Risoluzione dei problemi dei flap del protocollo di routing intermittente con EEM ed EPC

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Panoramica del problema
  - Metodologia di risoluzione dei problemi
- Panoramica della configurazione
  - Modello di configurazione ACL
  - Modello Parametri EPC
  - Modello di configurazione EEM
- Risoluzione Dei Problemi Dei Flap Del Protocollo Di Routing Intermittente
  - Esempio - EIGRP
    - Topologia
    - Configurazione
    - Analisi
  - OSPF
  - BGP
- Risoluzione dei problemi dei flash BFD intermittenti
  - Topologia
  - Esempio - Modalità eco BFD
    - Configurazione
    - Analisi
  - Modalità asincrona BFD

Introduzione

In questo documento viene descritto come risolvere i problemi relativi ai flap del protocollo di routing intermittente e ai flap BFD in Cisco IOS® XE con EEM ed EPC.

Prerequisiti

Requisiti

Si consiglia di familiarizzare con le specifiche di Embedded Event Manager (EEM) e Embedded Packet Capture (EPC) per le piattaforme coinvolte nella risoluzione dei problemi, nonché con Wireshark. Si consiglia inoltre di acquisire familiarità con le funzionalità di base hello e keepalive per i protocolli di routing e il rilevamento dell'inoltro bidirezionale (BFD).

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica del problema

I flap del protocollo di routing intermittenti sono un problema comune nelle reti di produzione, ma a causa della loro natura imprevedibile, possono essere difficili da risolvere in tempo reale. EEM consente di automatizzare la raccolta dei dati attivando l'acquisizione dei dati con stringhe di syslog quando si verificano i flap. Con EEM ed EPC, i dati di acquisizione dei pacchetti possono essere raccolti da entrambe le estremità dell'adiacenza per isolare la potenziale perdita di pacchetti prima del momento del flap.

I link flap del protocollo di routing intermittente sono per natura dovuti sempre a un timeout di hello o keepalive (a meno che non si tratti di un problema fisico chiaro, ad esempio i link flap, che apparirebbero nei log). Di conseguenza, è questa la logica del presente documento.

Metodologia di risoluzione dei problemi

La cosa più importante per determinare quando si verifica un flap del protocollo di routing è se i pacchetti hello o keepalive sono stati inviati e ricevuti su entrambi i dispositivi al momento del problema. Questo metodo di risoluzione dei problemi prevede l'utilizzo di un EPC continuo su un buffer circolare fino al momento in cui si verifica il flap, in cui EEM utilizza la stringa di syslog pertinente per attivare un set di comandi da eseguire, uno dei quali arresta l'EPC. L'opzione del buffer circolare consente all'EPC di continuare a catturare nuovi pacchetti mentre sovrascrive i pacchetti più vecchi nel buffer, il che assicura che l'evento venga acquisito e che il buffer non si riempia e si arresti in anticipo. I dati di acquisizione dei pacchetti possono quindi essere correlati all'indicatore orario del link flap per determinare se i pacchetti necessari sono stati inviati e ricevuti su entrambe le estremità prima dell'evento.

Questo problema si verifica in genere per i dispositivi che formano un'adiacenza su una rete intermedia, ad esempio un provider di servizi Internet (ISP), ma la stessa metodologia può essere applicata a qualsiasi scenario di flap del protocollo di routing intermittente, indipendentemente dai dettagli specifici della topologia. La stessa operazione può essere eseguita nei casi in cui il dispositivo adiacente è gestito da una terza parte e non è accessibile. In questi casi, il metodo di risoluzione dei problemi descritto in questo documento può essere applicato solo al dispositivo a cui è possibile accedere per provare se ha inviato e ricevuto i pacchetti richiesti prima del link flap. Una volta confermato, i dati possono essere mostrati alla parte che gestisce il vicino per risolvere il problema dall'altra parte, se necessario.

Panoramica della configurazione

In questa sezione viene fornita una serie di modelli di configurazione che è possibile utilizzare per

impostare l'acquisizione automatica dei dati. Modificare gli indirizzi IP, i nomi delle interfacce e i nomi dei file in base alle esigenze.

Modello di configurazione ACL

Nella maggior parte dei casi, l'unico traffico proveniente dall'indirizzo IP dell'interfaccia su entrambe le estremità di una adiacenza di routing è il traffico di controllo del routing stesso. Di conseguenza, un ACL che permette il traffico sia dall'indirizzo IP dell'interfaccia locale sia dall'indirizzo IP del router adiacente verso qualsiasi destinazione soddisfa il requisito di qualsiasi protocollo di routing, oltre al BFD. Se è necessario un filtro aggiuntivo, è possibile specificare anche l'IP di destinazione pertinente basato sul protocollo di routing o sulla modalità BFD. Definire i parametri ACL in modalità di configurazione:

```
config t

ip access-list extended




permit ip host



         any

permit ip host



          any

end
```

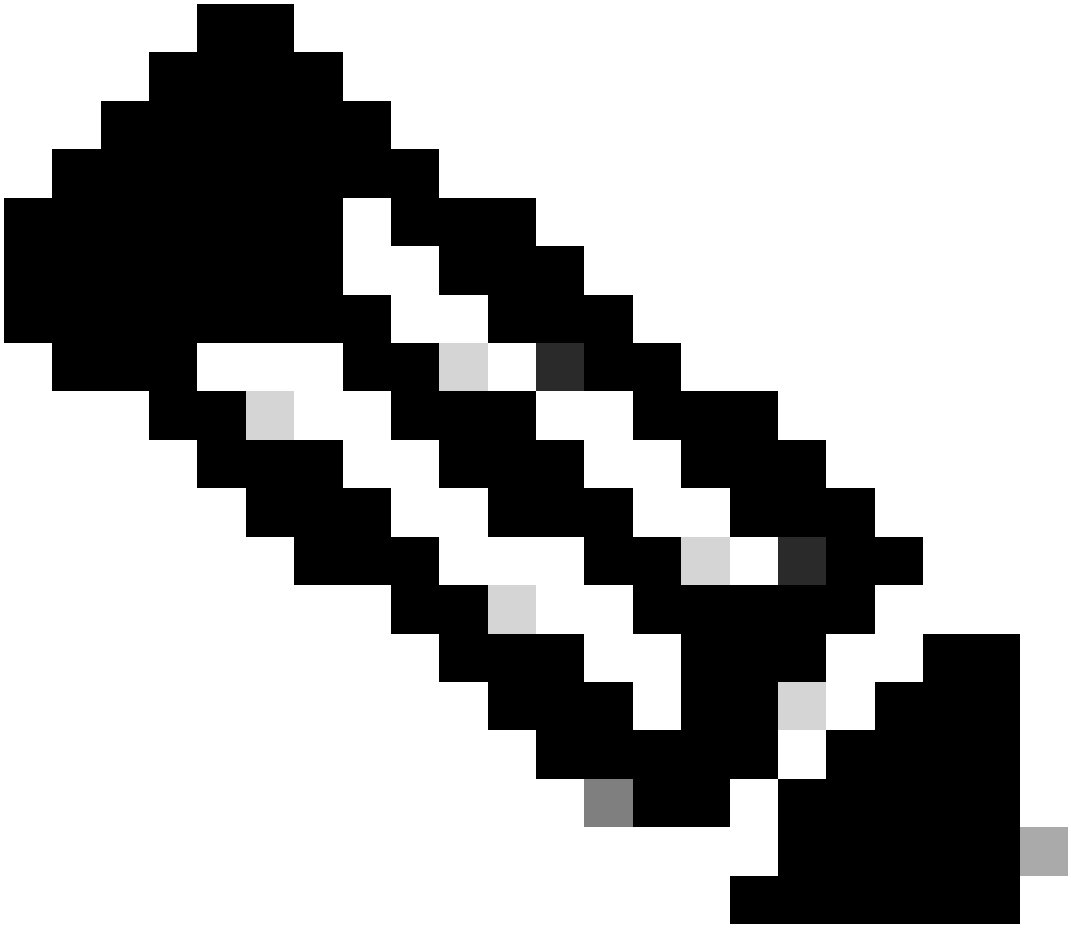
Modello Parametri EPC

I parametri EPC vengono creati in modalità di esecuzione privilegiata, non in modalità di configurazione. Accertarsi di consultare le guide alla configurazione specifiche della piattaforma per determinare se vi sono restrizioni con EPC. Creare i parametri per l'interfaccia desiderata e associarli all'ACL per filtrare il traffico desiderato:

- monitor capture <nome EPC> interface <interfaccia> both
- monitor capture <nome EPC> access-list <nome ACL>

- monitoraggio acquisizione <nome EPC> dimensione buffer 5 circolare

---



Nota: In alcune versioni del software, il traffico generato localmente non è visibile con un EPC a livello di interfaccia. In questi scenari, i parametri di acquisizione possono essere modificati per acquisire entrambe le direzioni del traffico sulla CPU:

- monitor capture <nome EPC> control-plane both
- monitor capture <nome EPC> access-list <nome ACL>
- monitoraggio acquisizione <nome EPC> dimensione buffer 5 circolare

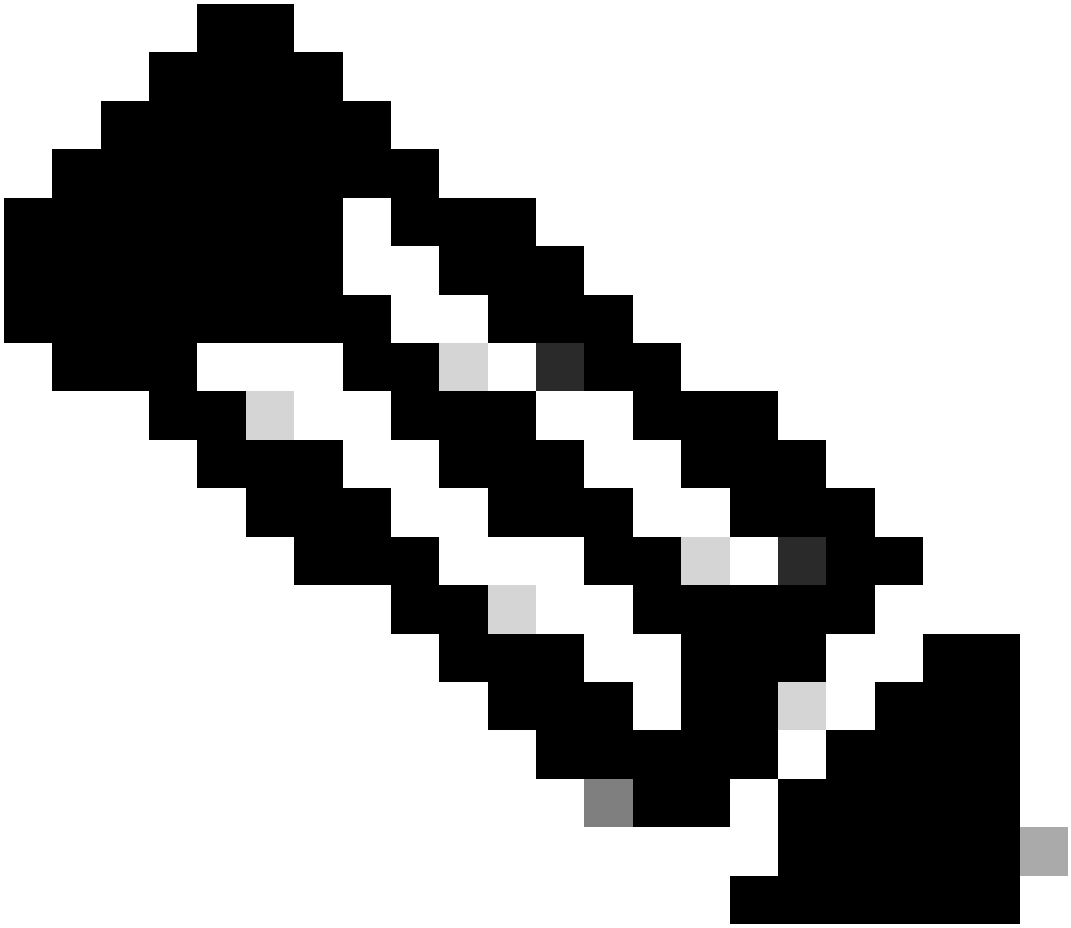
Una volta configurata, avviare l'EPC:

- avvio acquisizione monitor <nome EPC>

L'EEM è impostato in modo da interrompere l'acquisizione quando si verifica il flap.

Per assicurarsi che i pacchetti vengano acquisiti in entrambe le direzioni, controllare il buffer di acquisizione:

```
show monitor capture

        buffer brief
```



Nota: Sulle piattaforme di switching Catalyst (ad esempio Cat9k e Cat3k), è necessario arrestare l'acquisizione prima di poter visualizzare il buffer. Per verificare che l'acquisizione funzioni, arrestare l'acquisizione con il comando monitor capture stop, visualizzare il buffer e quindi riavviarlo per raccogliere i dati.

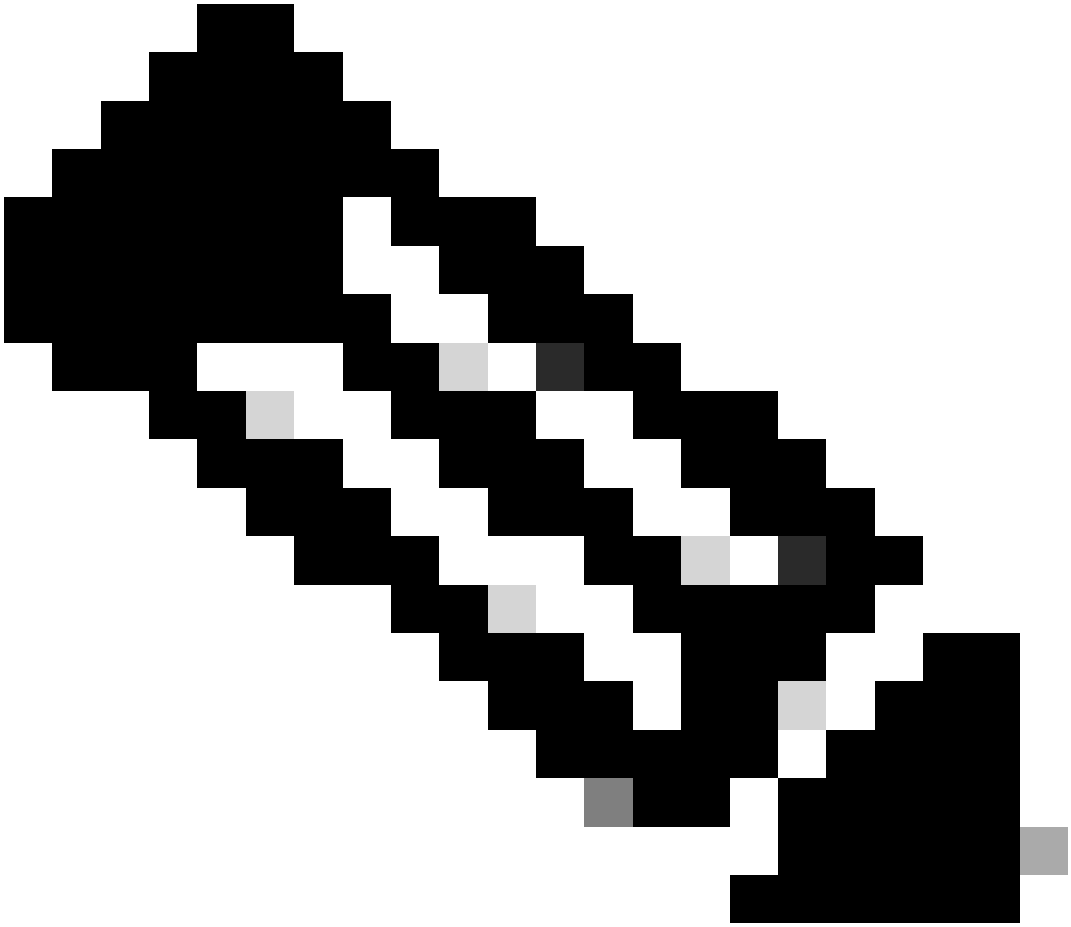
Modello di configurazione EEM

Lo scopo principale dell'EEM è arrestare l'acquisizione dei pacchetti e salvarli insieme al buffer di

syslog. È possibile includere comandi aggiuntivi per controllare altri fattori, quali CPU, interruzioni dell'interfaccia o utilizzo delle risorse e contatori di perdite specifici della piattaforma. Creare l'applet EEM in modalità di configurazione:

```
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 | append bootflash:



         .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: Sulle piattaforme di switching Catalyst (ad esempio Cat9k e Cat3k), il comando per esportare l'acquisizione è leggermente diverso. Per queste piattaforme, modificare il comando CLI usato nell'azione 035:

```
action 035 cli command "monitor capture

        export location bootflash:

        .pcap"
```

Il valore di limite di velocità nell'EEM è espresso in secondi e indica il tempo che deve trascorrere prima che l'EEM possa essere eseguito nuovamente. Nell'esempio, questo valore è impostato su 100000 secondi (27,8 ore) per consentire all'amministratore di rete di verificare il completamento dell'operazione e di estrarre i file dal dispositivo prima di eseguirlo di nuovo. Se l'EEM viene eseguito di nuovo autonomamente dopo questo periodo di tempo limite di velocità, non vengono raccolti nuovi dati di acquisizione dei pacchetti, in quanto l'EPC deve essere avviato manualmente. Tuttavia, i nuovi output del comando show vengono aggiunti ai file di testo.

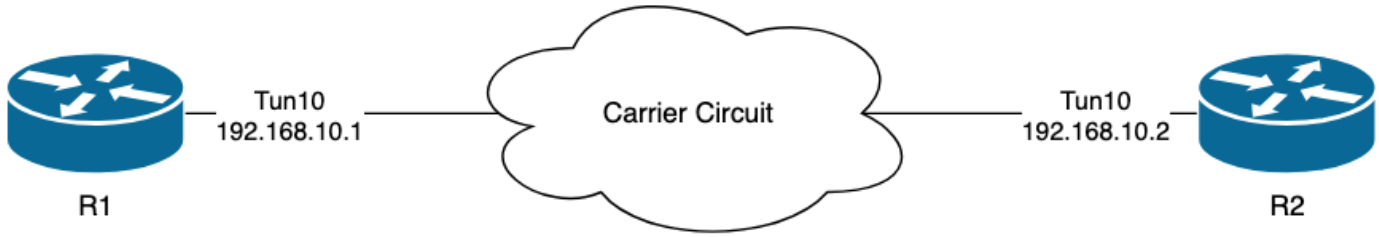
L'EEM può essere modificato in base alle esigenze per raccogliere informazioni specifiche della piattaforma e ottenere ulteriori funzionalità richieste dallo scenario.

Risoluzione Dei Problemi Dei Flap Del Protocollo Di Routing Intermittente

Esempio - EIGRP

In questo esempio, tutti i timer sono impostati sul valore predefinito (5 secondi di attesa, 15 secondi di attesa).

Topologia



I registri in R1 indicano che vi sono stati lembi EIGRP intermittenti che si sono verificati a distanza di diverse ore l'uno dall'altro:

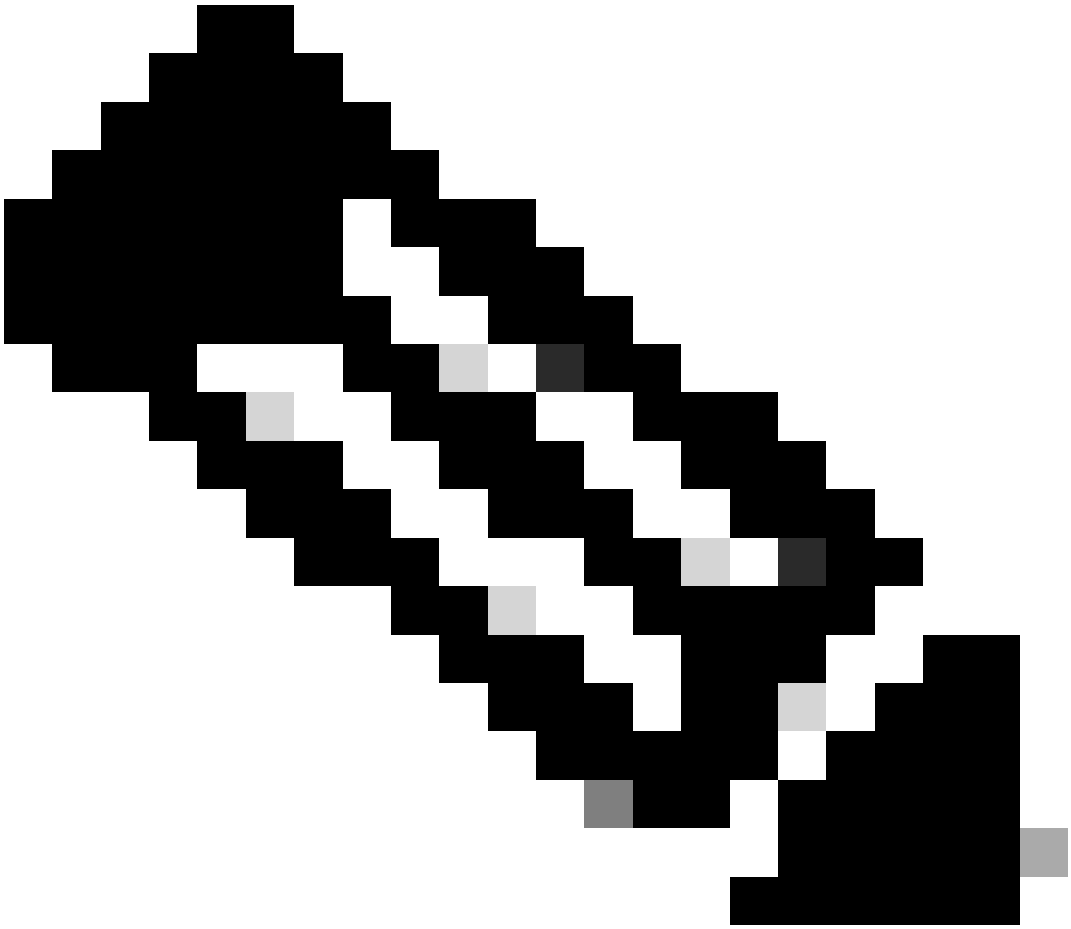
```
R1#show logging | i EIGRP
*Jul 16 20:45:08.019: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is down: Interf
*Jul 16 20:45:12.919: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is up: new adja
*Jul 17 10:25:42.970: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 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 perdita del pacchetto potrebbe avvenire in entrambe le direzioni; il tempo di attesa scaduto indica che il dispositivo non ha ricevuto o elaborato un saluto dal peer entro il tempo di attesa, mentre l'opzione Interface PEER-TERMINATION ricevuta indica che il peer ha terminato l'adiacenza perché non ha ricevuto o elaborato un saluto entro il tempo di attesa.

Configurazione

1. Configurare l'ACL con gli indirizzi IP dell'interfaccia del tunnel, in quanto sono gli indirizzi IP di origine degli helper:

```
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: Le configurazioni mostrate provengono da R1. Lo stesso avviene su R2 per le interfacce interessate e con i nomi di file modificati per l'EEM. Se è richiesta ulteriore specificità, configurare l'ACL con l'indirizzo multicast EIGRP 224.0.0.10 come indirizzo IP di destinazione per l'acquisizione degli helper.

---

2. Creare l'EPC e associarlo all'interfaccia e all'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. Avviare l'EPC e confermare che i pacchetti sono acquisiti in entrambe le direzioni:

```
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. Configurare l'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. Attendere che si verifichi il successivo flap e copiare i file da bootflash utilizzando il metodo di trasferimento preferito per l'analisi:

```
R1#show logging
```

```
*Jul 17 16:51:47.154: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is down: Interf
*Jul 17 16:51:48.015: %BUFCAP-6-DISABLE: Capture Point CAP disabled.
*Jul 17 16:51:48.283: %HA_EM-6-LOG: EIGRP_FLAP: Saved logs to bootflash:EIGRP_FLAP.txt and saved packet
*Jul 17 16:51:51.767: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.2 (Tunnel10) is up: new adja
R1#
```

```
R1#dir bootflash: | i EIGRP
23      -rw-           147804  Jul 17 2024 16:51:48 +00:00  EIGRP_CAP.pcap
22      -rw-            74450  Jul 17 2024 16:51:47 +00:00  EIGRP_FLAP.txt
```

- Il buffer di registro sul router indica che si è verificato un flap EIGRP e i file sono stati salvati dall'EEM.

Analisi

A questo punto, correlare l'ora del flap trovato nel buffer di log con le acquisizioni dei pacchetti raccolte per determinare se i pacchetti hello sono stati inviati e ricevuti su entrambe le estremità quando si è verificato il flap. Poiché l'interfaccia PEER-TERMINATION ricevuta è stata rilevata su R1, R2 deve aver rilevato perdite di hellos e quindi il tempo di attesa è scaduto, come indicato nel file di log:

```
*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
```

Poiché R2 ha rilevato che il tempo di attesa è scaduto, confermare se sono stati inviati dei colpi da R1 nei 15 secondi precedenti all'acquisizione del flap in 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	✓

- L'acquisizione mostra gli hellop sia da 192.168.10.1 (R1) che da 192.168.10.2 (R2) nei 15 secondi precedenti il pacchetto di saluto PEER-TERMINATION che R2 invia alle 16:51:47 (pacchetto 513).
- In particolare, i pacchetti 503, 505, 508 e 511 (indicati dalle frecce verdi) erano tutti hellos inviati da R1 in questo periodo di tempo.

Il passo successivo consiste nel confermare se tutti gli hellop inviati da R1 sono stati ricevuti da R2 in quel momento, quindi la cattura raccolta da R2 deve essere controllata:

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
```

- La cattura mostra che l'ultimo saluto ricevuto da 192.168.10.1 (R1) era alle 16:51:32 (indicato dalla freccia verde). Dopo questa operazione, nei successivi 15 secondi vengono visualizzati solo gli hellos inviati da R2 (indicati dal riquadro rosso). I pacchetti 505, 508 e 511 nell'acquisizione da R1 non vengono visualizzati nell'acquisizione su R2. In questo modo, R2 rileva la scadenza del timer di attesa e invia il pacchetto di pronto soccorso PEER-TERMINATION alle 16:51:47 (pacchetto 502).

La conclusione tratta da questi dati è che la perdita di pacchetti si verifica in qualche punto della rete di portanti tra R1 e R2. In questo caso, la perdita si è verificata nella direzione da R1 a R2. Per indagare ulteriormente, il vettore deve essere coinvolto per controllare il percorso per individuare eventuali cadute.

OSPF

La stessa logica può essere utilizzata per risolvere i problemi relativi ai flap OSPF intermittenti. In questa sezione vengono descritti i fattori chiave che la distinguono dagli altri protocolli di routing per timer, filtri di indirizzi IP e messaggi di log.

- I timer predefiniti sono hellos da 10 secondi e un timer inattivo da 40 secondi. Confermare sempre i timer in uso nella rete quando si risolvono i problemi di flash scaduti del timer.
- I pacchetti Hello provengono dagli indirizzi IP dell'interfaccia. Se è necessaria una specifica ACL aggiuntiva, l'indirizzo di destinazione multicast per gli hellop OSPF è 224.0.0.5.
- I messaggi di registro sui dispositivi sono leggermente diversi. Contrariamente a EIGRP, con OSPF non esiste il concetto di messaggio di terminazione peer. Al contrario, il dispositivo che rileva il timer inattivo scaduto lo registra come motivo del link flap e quindi gli helper inviati non contengono più l'ID router del peer, il che fa sì che il peer passi allo stato INIT. Quando gli hellos vengono rilevati di nuovo, l'adiacente passa attraverso finché non raggiunge lo stato FULL. Ad esempio:

R1 rileva la scadenza del timer:

```
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
```

R2, tuttavia, visualizza i messaggi di log solo quando OSPF torna a FULL. Quando lo stato viene impostato su INIT, non viene visualizzato alcun messaggio di registro:

```
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
```

Per attivare EEM su entrambi i dispositivi, utilizzare "%OSPF-5-ADJCHG" come modello syslog. In questo modo, l'EEM viene attivato su entrambi i dispositivi finché non viene disattivato e non viene riattivato. Il valore ratelimit configurato garantisce che non venga attivato due volte in un breve periodo quando vengono rilevati più registri con questa stringa. La chiave è confermare se i pacchetti hellop vengono inviati e ricevuti nelle clip su entrambi i lati.

BGP

La stessa logica può essere utilizzata per risolvere i problemi di flap BGP intermittenti. In questa sezione vengono descritti i fattori chiave che la distinguono dagli altri protocolli di routing per timer, filtri di indirizzi IP e messaggi di log.

- I timer predefiniti sono keepalive di 60 secondi e un tempo di attesa di 180 secondi. Confermare sempre i timer in uso nella rete quando la risoluzione dei problemi di flap tempo di attesa scaduto.
- I pacchetti keepalive vengono inviati in formato unicast tra gli indirizzi IP dei router adiacenti e la porta di destinazione TCP 179. Se è necessaria una maggiore specificità ACL, autorizzare il traffico TCP tra gli indirizzi IP di origine e la porta TCP di destinazione 179.
- I messaggi di log per BGP sono simili su entrambi i dispositivi, ma il dispositivo che rileva la scadenza del tempo di attesa indica che ha inviato la notifica al router adiacente, mentre il secondo indica che ha ricevuto il messaggio di notifica. Ad esempio:

R1 rileva che il tempo di attesa è scaduto e invia la notifica 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 riceve la notifica da R1 perché R1 ha rilevato un tempo di attesa scaduto:

```
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
```

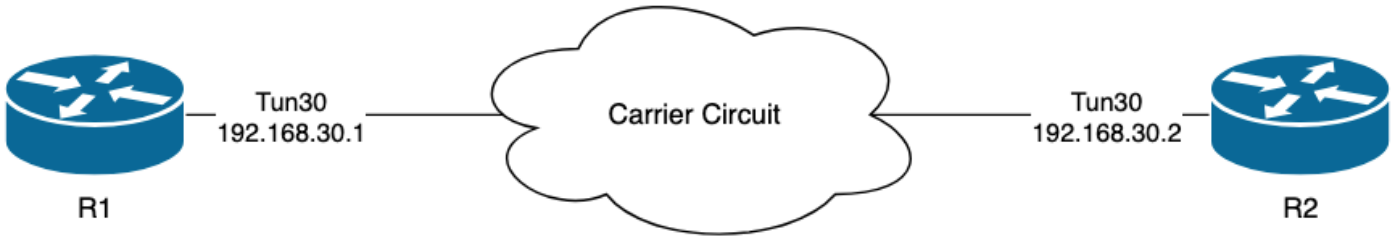
Per attivare EEM per un flap BGP, utilizzare "%BGP_SESSION-5-ADJCHANGE" come modello di syslog. Tutti gli altri messaggi syslog "%BGP" registrati dopo il flap possono essere utilizzati per attivare l'EEM.

Risoluzione dei problemi dei flash BFD intermittenti

La stessa metodologia può essere applicata per risolvere i problemi di flap BFD intermittenti, con alcune differenze minime da applicare all'analisi. In questa sezione vengono descritte alcune funzionalità di base dei DCF e viene fornito un esempio di come utilizzare EEM ed EPC per la risoluzione dei problemi. Per informazioni più dettagliate sulla risoluzione dei problemi relativi ai dati di configurazione di avvio, consultare il documento sulla risoluzione dei problemi di rilevamento dell'inoltro bidirezionale in Cisco IOS XE.

In questo esempio, i timer BFD sono impostati su 300 ms con un moltiplicatore di 3, il che significa che gli echo vengono inviati ogni 300 ms e che viene rilevato un errore echo quando non vengono restituiti 3 pacchetti echo in una riga (pari a un tempo di attesa di 900 ms).

Topologia



Esempio - Modalità eco BFD

In modalità Eco BFD (modalità predefinita), i pacchetti echo BFD vengono inviati con l'indirizzo IP dell'interfaccia locale come origine e destinazione. In questo modo, il router adiacente può elaborare il pacchetto nel piano dati e restituirlo al dispositivo di origine. Ogni eco BFD viene inviata con un ID echo nell'intestazione del messaggio echo BFD. Queste opzioni possono essere utilizzate per determinare se un pacchetto echo BFD inviato è stato ricevuto indietro. Infatti, devono essere presenti due occorrenze di ogni pacchetto echo BFD inviato se è stato effettivamente restituito dal router adiacente. I pacchetti di controllo BFD, utilizzati per controllare lo stato della sessione BFD, vengono inviati in modalità unicast tra gli indirizzi IP dell'interfaccia.

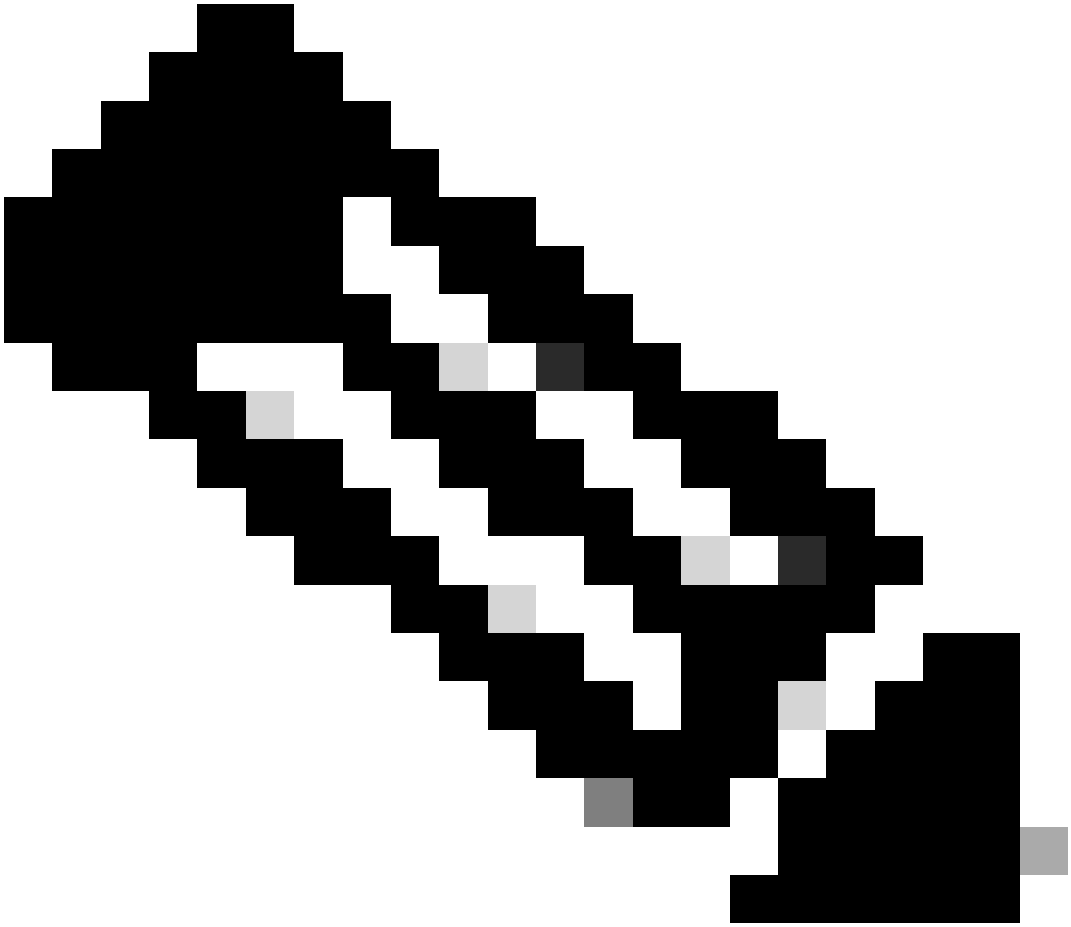
I log di R1 indicano che l'adiacenza del BFD è scesa più volte a causa di un ERRORE ECHO, il che significa che durante questi intervalli, R1 non ha ricevuto o elaborato 3 pacchetti echo di sua proprietà da R2.

```
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
```

Configurazione

1. Configurare l'ACL con gli indirizzi IP dell'interfaccia del tunnel, come questi sono gli indirizzi IP di origine dei pacchetti echo BFD e dei pacchetti di controllo:

```
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: Le configurazioni mostrate provengono da R1. Lo stesso avviene su R2 per le interfacce interessate e con i nomi di file modificati per l'EEM. Se è richiesta ulteriore specificità, configurare l'ACL per UDP con le porte di destinazione 3785 (pacchetti echo) e 3784 (pacchetti di controllo).

2. Creare l'EPC e associarlo all'interfaccia e all'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. Avviare l'EPC e confermare che i pacchetti sono acquisiti in entrambe le direzioni:

```
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. Configurare l'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. Attendere che si verifichi il successivo flap e copiare i file da bootflash utilizzando il metodo di trasferimento preferito per l'analisi:

```
R1#show logging
```

```
*Jul 18 19:09:47.482: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going Down R
*Jul 18 19:09:47.483: %BGP-5-NBR_RESET: Neighbor 192.168.30.2 reset (BFD adjacency down)
*Jul 18 19:09:47.487: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Down BFD adjacency down
*Jul 18 19:09:47.487: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.30.2 IPv4 Unicast topology base remove
*Jul 18 19:09:47.487: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed,  ld:4097 neigh proc
*Jul 18 19:09:48.191: %BUFCAP-6-DISABLE: Capture Point CAP disabled.
*Jul 18 19:09:48.668: %HA_EM-6-LOG: R1_BFD_FLAP: Saved logs to bootflash:R1_BFD_FLAP.txt and saved pack
*Jul 18 19:09:50.165: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4097 handle:1 is going UP
*Jul 18 19:09:54.386: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 192.168.30.2 proc
*Jul 18 19:09:54.386: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Up
*Jul 18 19:09:55.178: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4097 handle:1 is going UP
R1#
R1#dir | i BFD
25      -rw-          1591803  Jul 18 2024 19:09:48 +00:00  R1_BFD_CAP.pcap
24      -rw-            84949  Jul 18 2024 19:09:48 +00:00  R1_BFD_FLAP.txt
```

- Il buffer di log indica che c'è stato un flap BFD alle 19:09:47 e che i file sono stati salvati dall'EEM.

Analisi

A questo punto, correlare l'ora del flap trovato nel buffer di log con le acquisizioni dei pacchetti raccolte per determinare se gli echo dei BFD sono stati inviati e ricevuti su entrambe le estremità quando si è verificato il problema. Poiché la causa dell'instabilità su R1 è il GUASTO ECHO, questo significa che avrebbe anche inviato un pacchetto di controllo a R2 per terminare la sessione BFD, e questo si riflette nel file di log raccolto da R2, dove è visibile il motivo dell'inattività 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
```

Poiché R1 ha rilevato un ERRORE ECHO, controllare l'acquisizione del pacchetto raccolta su R1 per verificare se ha inviato e ricevuto eco BFD nei 900 ms precedenti l'errore.

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	000000000000100200000041f	Originator specific content
136	2024-07-18 19:09:46.484581	192.168.30.2	192.168.30.2	BFD Echo	78	000000000000100200000041f	Originator specific content
137	2024-07-18 19:09:46.707712	192.168.30.1	192.168.30.1	BFD Echo	78	000000000000100100000041d	Originator specific content
138	2024-07-18 19:09:46.970921	192.168.30.1	192.168.30.1	BFD Echo	78	000000000000100100000041e	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	000000000000100100000041f	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

- L'acquisizione mostra che R1 ha inviato attivamente pacchetti echo BFD fino al momento del flap, ma non sono stati restituiti da R2, quindi R1 invia un pacchetto di controllo per terminare la sessione alle 19:09:47.468.
- Ciò è evidente dal fatto che i pacchetti 137, 138 e 140 (indicati dalle frecce verdi) vengono visti solo una volta nella cattura, che può essere determinata dagli Echo ID dei BFD (nel riquadro rosso). Se l'echo fosse stato restituito, ci sarebbe stata una seconda copia di ciascuno di quei pacchetti con lo stesso ID echo BFD. Anche il campo Identificazione IP nell'intestazione IP (non presente in questa immagine) può essere utilizzato per verificare questa condizione.
- Questa acquisizione mostra anche che non sono stati ricevuti echo BFD da R2 dopo il pacchetto 136, il che è un'altra indicazione di perdita di pacchetto nella direzione da R2 a R1.

Il passaggio successivo consiste nel confermare se tutti i pacchetti echo BFD inviati da R1 sono stati ricevuti e restituiti da R2, quindi è necessario controllare l'acquisizione raccolta da 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	000000000000010010000041d	Originator specific content
108	2024-07-18 19:09:46.708430	192.168.30.1	192.168.30.1	BFD Echo	78	000000000000010010000041d	Originator specific content
110	2024-07-18 19:09:46.774829	192.168.30.2	192.168.30.2	BFD Echo	78	000000000000100200000420	Originator specific content
111	2024-07-18 19:09:46.971240	192.168.30.1	192.168.30.1	BFD Echo	78	000000000000010010000041e	Originator specific content
112	2024-07-18 19:09:46.971542	192.168.30.1	192.168.30.1	BFD Echo	78	000000000000010010000041e	Originator specific content
113	2024-07-18 19:09:47.015058	192.168.30.2	192.168.30.2	BFD Echo	78	000000000000100200000421	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	000000000000010010000041f	Originator specific content
117	2024-07-18 19:09:47.204021	192.168.30.1	192.168.30.1	BFD Echo	78	000000000000010010000041f	Originator specific content
118	2024-07-18 19:09:47.286688	192.168.30.2	192.168.30.2	BFD Echo	78	000000000000100200000422	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

- Questa acquisizione mostra che tutti gli echo BFD inviati da R1 sono stati ricevuti e restituiti da R2 (indicati con frecce verdi); I pacchetti 107 e 108 sono la stessa eco BFD, i pacchetti 111 e 112 sono la stessa eco BFD e i pacchetti 116 e 117 sono la stessa eco BFD.
- Questa acquisizione mostra anche che R2 invia attivamente pacchetti echo (indicati con caselle rosse) che non sono visibili nell'acquisizione su R1, il che indica ulteriormente la perdita di pacchetti tra i dispositivi nella direzione da R2 a R1.

La conclusione tratta da questi dati è che la perdita del pacchetto si verifica in qualche punto della rete di vettori tra R1 e R2 e tutte le prove a questo punto indicano che la direzione della perdita va da R2 a R1. Per indagare ulteriormente, il vettore deve essere coinvolto per controllare il percorso per individuare eventuali cadute.

Modalità asincrona BFD

Lo stesso metodo può essere applicato quando è in uso la modalità asincrona dei dati configurazione di avvio (funzione echo disabilitata) e la configurazione EEM ed EPC può essere mantenuta invariata. La differenza nella modalità asincrona è che i dispositivi inviano tra loro pacchetti di controllo BFD unicast come pacchetti keepalive, analogamente a una tipica adiacenza del protocollo di routing. Ciò significa che vengono inviati solo pacchetti sulla porta UDP 3784. In questo scenario, il BFD rimane nello stato attivo finché viene ricevuto un pacchetto BFD dal router adiacente entro l'intervallo richiesto. Quando questo non accade, il motivo dell'errore è DETECT TIMER EXPIRED (TIMER RILEVAMENTO SCADUTO) e il router invia un pacchetto di controllo al peer per interrompere la sessione.

Per analizzare le acquisizioni sul dispositivo che ha rilevato il guasto, cercare i pacchetti BFD unicast ricevuti dal peer durante il tempo immediatamente precedente al flap. Ad esempio, se l'intervallo TX è impostato su 300 ms con un moltiplicatore di 3, se non ci sono pacchetti BFD ricevuti nei 900 ms precedenti al flap, il pacchetto potrebbe andare perso. Nella cattura raccolta dal vicino tramite l'EEM, controllare questa finestra temporale; se i pacchetti sono stati inviati durante quel periodo di tempo, allora conferma che c'è una perdita da qualche parte tra i dispositivi.

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).