Protocolflaps met intermitterende routing met EM en EPC oplossen

Inhoud

Inleiding

Dit document beschrijft hoe u intermitterende routingprotocolflaps en BFD-flaps in Cisco IOS® XE met EM en EPC kunt oplossen.

Voorwaarden

Vereisten

Het wordt aanbevolen om bekend te zijn met de specificaties van Embedded Event Manager (EEM) en Embedded Packet Capture (EPC) voor het platform (s) dat (die) betrokken is (zijn) bij het oplossen van problemen, evenals Wireshark. Bovendien wordt vertrouwdheid met basis-hello- en keepalive-functionaliteit voor routing van protocollen en bidirectionele doorsturen-detectie

(BFD) aanbevolen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem - Overzicht

Intermitterende routering protocol flaps zijn een veel voorkomend probleem in productienetwerken, maar vanwege hun onvoorspelbare aard, kunnen ze moeilijk in real time probleemoplossing. EEM biedt de mogelijkheid om gegevensverzameling te automatiseren door gegevensvastlegging met syslog-strings te activeren wanneer de flaps optreden. Met EEM en EPC kunnen pakketopnamegegevens worden verzameld aan beide uiteinden van de nabijheid om mogelijk pakketverlies te isoleren voorafgaand aan het tijdstip van de flap.

De aard van intermitterende routing protocol flaps is dat ze altijd te wijten zijn aan een hello of keepalive time-out (tenzij het een duidelijke fysieke kwestie is zoals link flaps die zou verschijnen in de logs). Daarom is dit de logica van dit document.

Methodologie voor probleemoplossing

Het belangrijkste om te bepalen wanneer een routingprotocol flap voorkomt is of de hello pakketten of keepalive pakketten werden verzonden en ontvangen op beide apparaten op het tijdstip van de kwestie. Deze probleemoplossingsmethode maakt gebruik van een continue EPC op een circulaire buffer totdat de flap optreedt, op welk punt EEM de relevante syslog string gebruikt om een set commando's te starten, waarvan er één de EPC stopt. De circulaire bufferoptie stelt de EPC in staat door te gaan met het opnemen van nieuwe pakketten, terwijl de oudste pakketten in de buffer worden overschreven, wat ervoor zorgt dat een gebeurtenis wordt opgenomen en de buffer niet vooraf wordt gevuld en stopgezet. De pakketopnamegegevens kunnen vervolgens gecorreleerd worden met de tijdstempel van de flap om te bepalen of de benodigde pakketten voorafgaand aan de gebeurtenis verzonden en ontvangen zijn op beide uiteinden.

Dit probleem doet zich het meest voor voor voor apparaten die een nabijheid over een tussenliggend netwerk zoals een Internet Service Provider (ISP) vormen, maar de zelfde methodologie kan voor om het even welk intermitterend routerings protocolflap scenario ongeacht de specifieke topologiedetails worden toegepast. Het zelfde kan in instanties worden gedaan waar het buurapparaat door een derde wordt beheerd en niet kan worden betreden. In dergelijke gevallen kan de probleemoplossingsmethode die in dit document wordt beschreven, worden toegepast op slechts één apparaat dat toegankelijk is om te bewijzen of het de vereiste pakketten vóór de flap heeft verzonden en ontvangen. Wanneer dit wordt bevestigd, kunnen de gegevens aan de partij worden getoond die de buur beheert om verder op het andere eind indien nodig problemen op te lossen.

Overzicht van configuratie

Deze sectie biedt een aantal configuratiesjablonen die kunnen worden gebruikt om deze geautomatiseerde gegevensvastlegging in te stellen. Wijzig desgewenst de IP-adressen, interfacenamen en bestandsnamen.

Sjabloon voor ACL-configuratie

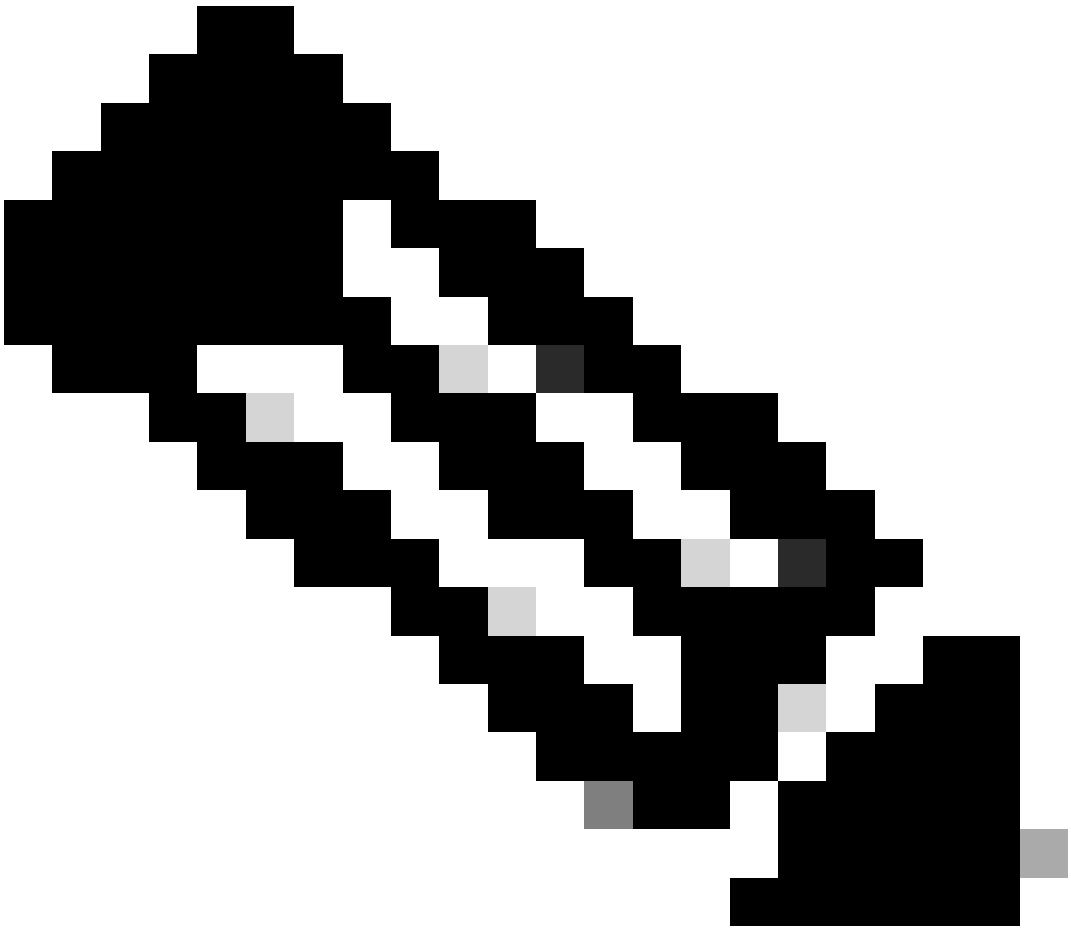
In de meeste gevallen, is het enige verkeer dat afkomstig is van het interfaceIP-adres aan beide uiteinden van een routeringsnabijheid het routing control verkeer zelf. Als dusdanig, een ACL die verkeer van zowel het lokale interfaceIP adres als het naburige IP adres aan om het even welke bestemming toestaat behandelt het vereiste voor om het even welk routeringsprotocol, evenals BFD. Als een extra filter nodig is, dan kan de relevante bestemming IP die op routeringsprotocol of BFD wijze wordt gebaseerd eveneens worden gespecificeerd. Definieer de ACL-parameters in de configuratiemodus:

```
config t

ip access-list extended




      permit ip host




       any permit ip host




        any end
```

Sjabloon EPC-parameters

De EPC-parameters worden gemaakt van de voorkeursexec-modus, niet van de configuratiemodus. Controleer de platformspecifieke configuratiehandleidingen om te bepalen of er beperkingen zijn met de EPC. Maak de parameters voor de gewenste interface en koppel deze aan de ACL om te filteren voor het gewenste verkeer:

- monitor-opname <EPC-naam>-interface <interface> beide
- monitor-opname <EPC-naam> - toegangslijst <ACL-naam>
- monitor Capture <EPC name>, buffergrootte 5, circulair



Opmerking: Op sommige softwareversies is lokaal gegenereerd verkeer niet zichtbaar met een EPC op interfaceniveau. In dergelijke scenario's kunnen de opnameparameters worden gewijzigd om beide richtingen van verkeer op de CPU op te nemen:

- <EPC name>-besturingsplane voor monitor
- monitor-opname <EPC-naam> - toegangslijst <ACL-naam>
- monitor Capture <EPC name>, buffergrootte 5, circulair

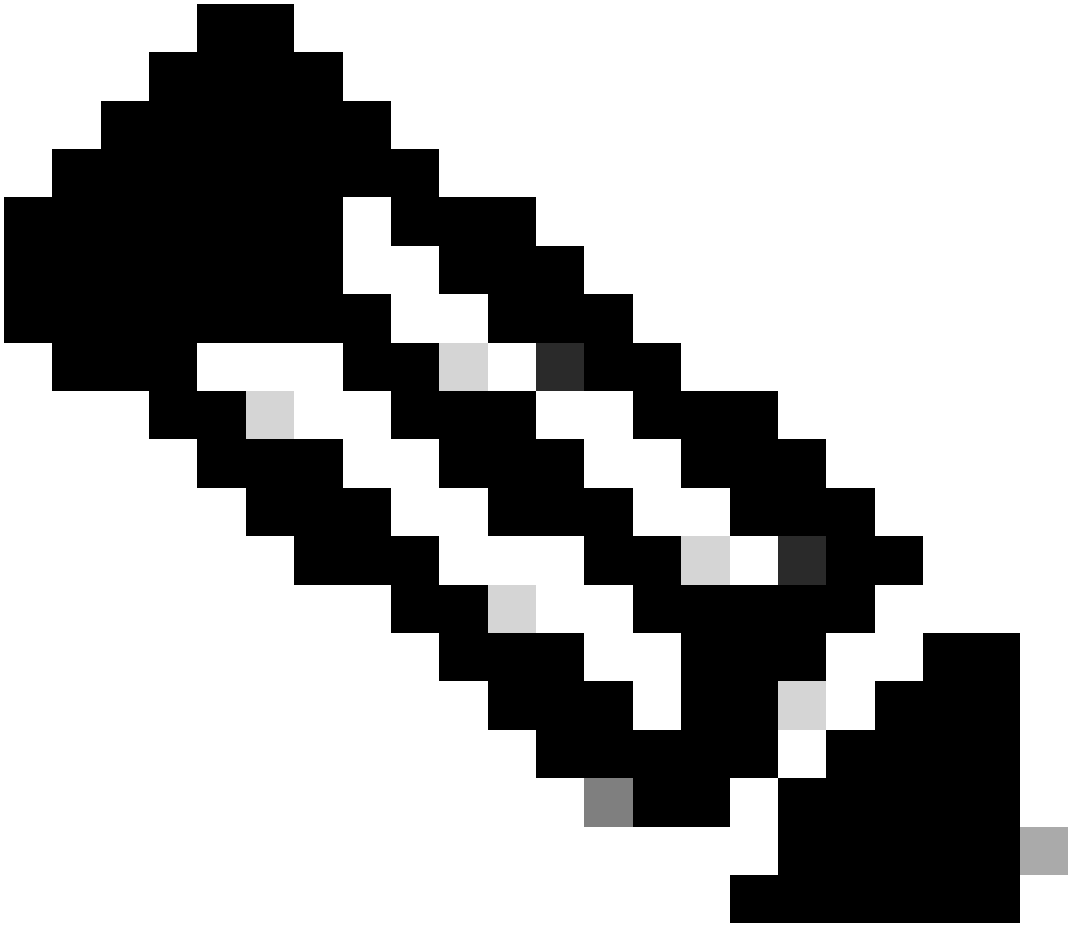
Start de EPC als deze eenmaal is geconfigureerd:

- Monitor Capture <EPC name> start

De EEM is ingesteld om de opname te stoppen wanneer de flap optreedt.

Controleer de opnamebuffer om er zeker van te zijn dat pakketten in beide richtingen worden opgenomen:

```
show monitor capture


      buffer brief
```



Opmerking: De Catalyst-switchingplatforms (zoals Cat9k en Cat3k) vereisen dat de opname wordt gestopt voordat de buffer kan worden bekeken. Om te bevestigen dat de opname werkt, stop de opname met de monitor stop bevel, bekijk de buffer, en start het opnieuw om gegevens te verzamelen.

EEM-configuratiesjabloon

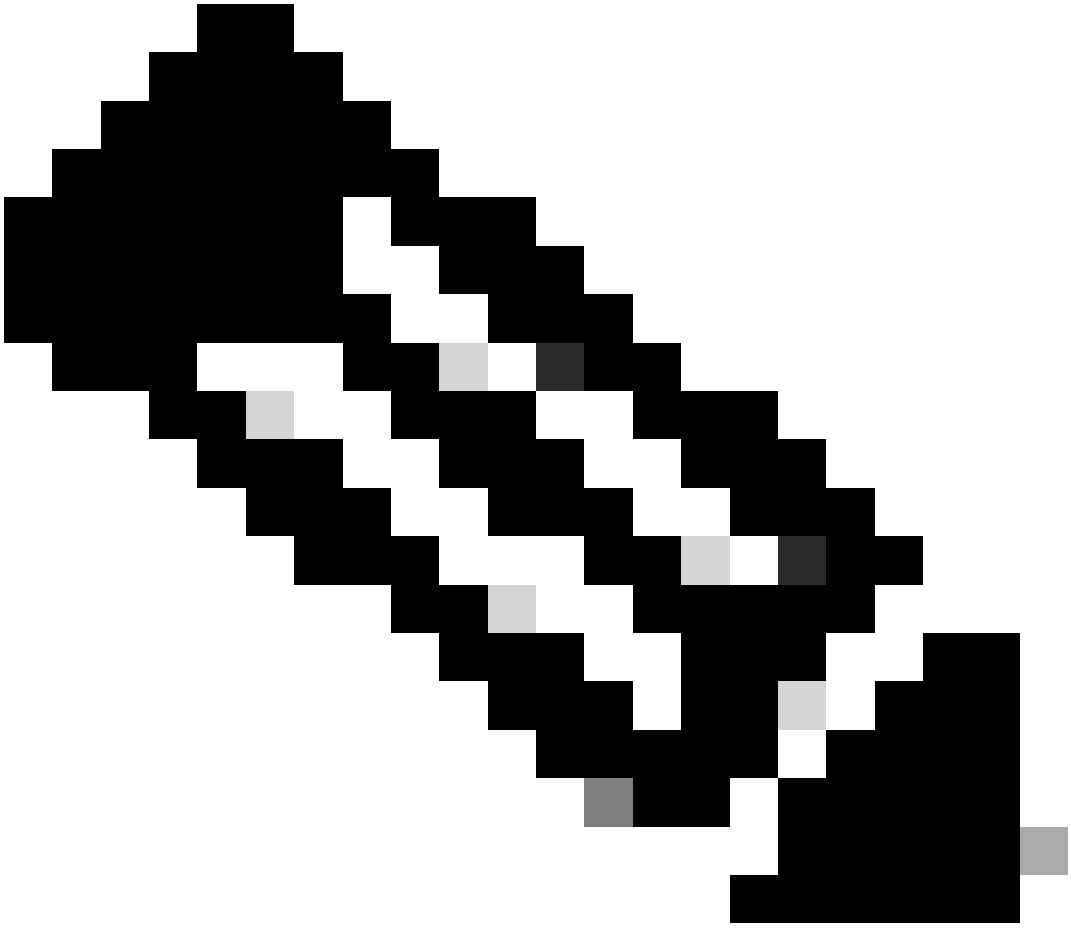
Het belangrijkste doel van de EEM is het pakket tegen te houden en het samen met de syslog buffer op te slaan. Er kunnen extra opdrachten worden opgenomen om andere factoren te controleren, zoals de CPU, de interfacedalingen of het platformspecifieke resourcegebruik en de valtellers. Maak de EEM applet in de configuratiemodus:

```
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



Opmerking: Op Catalyst-switchingplatforms (zoals Cat9k en Cat3k) is de opdracht voor het exporteren van de opname iets anders. Voor deze platforms kunt u de CLI-opdracht wijzigen die in actie 035 wordt gebruikt:

```
action 035 cli command "monitor capture

      export location bootflash:

       .pcap"
```

De snelheidswaarde in de EEM is in seconden en geeft aan hoeveel tijd moet verstrijken voordat de EEM weer kan lopen. In dit voorbeeld is de instelling ingesteld op 100000 seconden (27,8 uur) zodat de netwerkbeheerder voldoende tijd heeft om te identificeren dat hij de bestanden heeft voltooid en uit het apparaat heeft gehaald voordat het weer wordt uitgevoerd. Als de EEM na deze ratingperiode weer zelfstandig wordt uitgevoerd, worden er geen nieuwe pakketopnamegegevens verzameld, aangezien de EPC handmatig moet worden gestart. Er worden echter nieuwe output van showopdrachten aan de tekstbestanden toegevoegd.

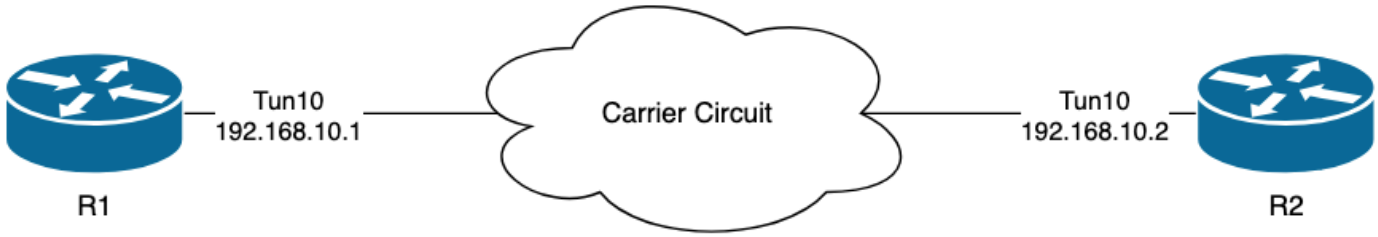
De EEM kan naar behoefte worden gewijzigd om platform-specifieke pakketdrop-informatie te verzamelen en extra functionaliteit te bereiken die voor uw scenario wordt vereist.

Protocolflappen voor intermitterende routing

Voorbeeld - EIGRP

Alle timers worden in dit voorbeeld ingesteld op de standaardwaarde (hellos van 5 seconden, houdtijd van 15 seconden).

Topologie



De logboeken op R1 wijzen erop dat er intermitterende EIGRP flaps zijn geweest die verscheidene uren apart van elkaar voorkwamen:

```
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
```

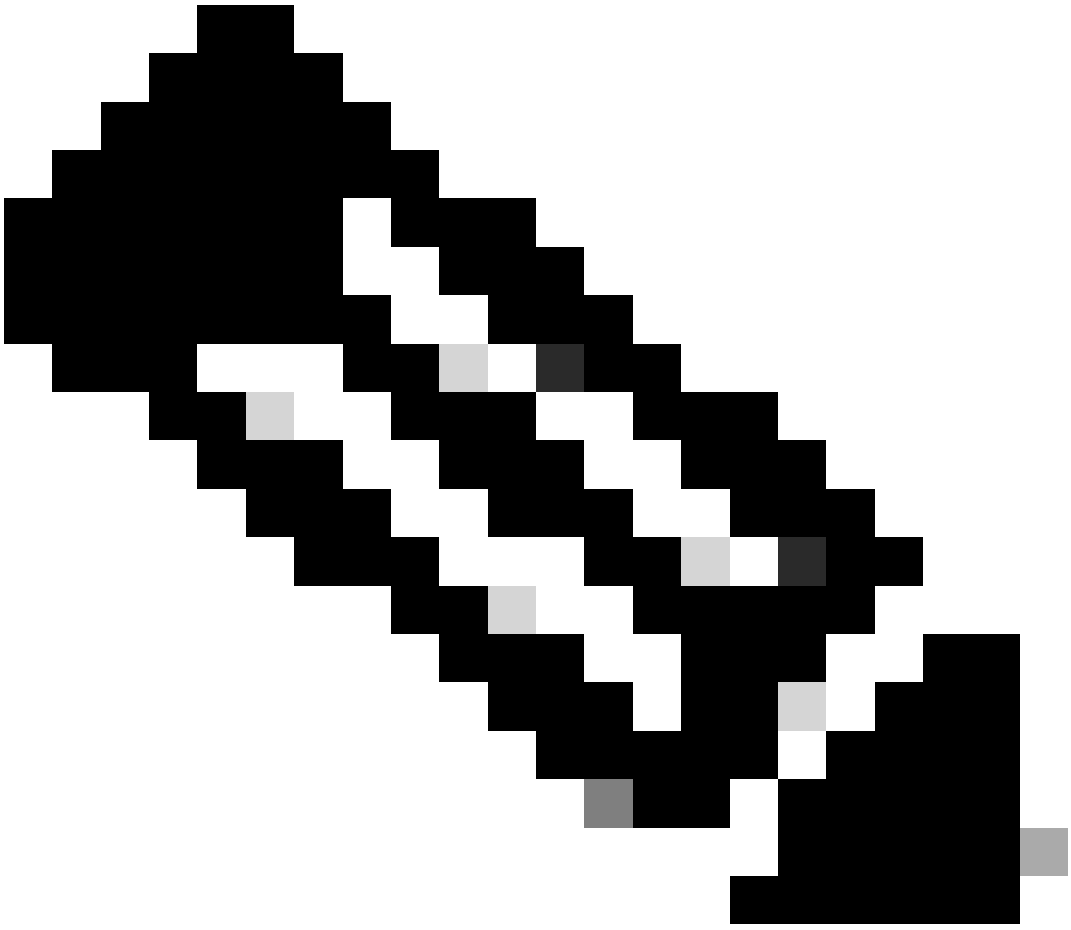
Het pakketverlies zou in beide richtingen kunnen zijn; De holdingstijd is verlopen, geeft aan dat dit apparaat geen hello van de peer binnen de greeptijd heeft ontvangen of verwerkt, en ontvangen

interface-PEER-BEËINDIGING geeft aan dat de peer de nabijheid eindigde omdat het geen hello binnen de greeptijd ontving of verwerkte.

Configuratie

1. Configureer de ACL met de IP-adressen van de tunnelinterface, aangezien dit de IP-adressen van de bronnen van de hellos zijn:

```
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
```



Opmerking: De getoonde configuraties zijn van R1. Hetzelfde wordt gedaan op R2 voor de relevante interfaces en met aangepaste bestandsnamen voor de EEM. Als extra

---

specificiteit wordt vereist, vorm ACL met EIGRP multicast adres 24.0.0.10 als bestemmingsIP adres om hellos te vangen.

2. Maak de EPC en koppel deze aan de interface en de 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. Start de EPC en bevestig dat pakketten in beide richtingen worden opgenomen:

```
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. De EEM configureren:

```
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. Wacht tot de volgende flap optreedt en kopieer de bestanden van bootflash via uw gewenste overdrachtsmethode voor analyse:

```
R1#show logging
```

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

- De logbuffer op de router geeft aan dat er een EIGRP-flap was en de bestanden zijn opgeslagen door de EEM.

Analyse

Op dit punt correleert u de tijd van de flap in de logbuffer met de pakketopnamen die werden verzameld om te bepalen of de hello-pakketten werden verzonden en ontvangen aan beide uiteinden toen de flap voorkwam. Aangezien ontvangen interface-PEER-BEËINDIGING op R1 werd gezien, betekent dit R2 verloren hellos moet ontdekt hebben en daarom is de houdstijd verlopen, wat in het logbestand wordt gezien:

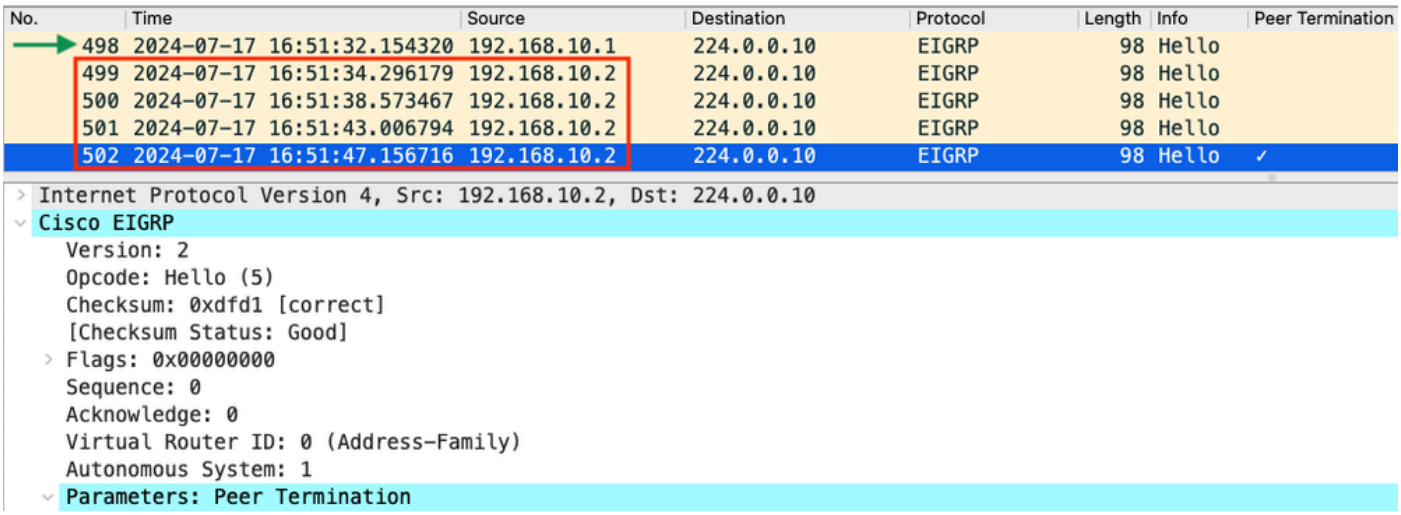
```
*Jul 17 16:51:47.156: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is down: holdin
*Jul 17 16:51:51.870: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is up: new adja
```

Omdat R2 detecteerde houdtijd is verlopen, moet u bevestigen of er hellos zijn verzonden door R1 in de 15 seconden voordat de flap in de opname op R1 is verzameld:

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	✓

- De opname toont hellos van zowel 192.168.10.1 (R1) als 192.168.10.2 (R2) in de 15 seconden vóór het PEER-TERMINATION hello-pakket dat R2 bij 16:51:47 verzendt (pakket 513).
- De pakketten 503, 505, 508 en 511 (aangegeven door de groene pijlen) waren alle hellos die door R1 in deze periode werden verzonden.

De volgende stap is te bevestigen of alle hellos die door R1 worden verzonden op het moment door R2 zijn ontvangen, zodat de opname die uit R2 is verzameld moet worden gecontroleerd:



- De opname laat zien dat de laatste hello ontvangen van 192.168.10.1 (R1) was om 16:51:32 (aangegeven door de groene pijl). De volgende 15 seconden tonen alleen hellos die door R2 worden verstuurd (aangegeven door het rode vak). De pakketten 505, 508 en 511 in de opname van R1 worden niet weergegeven in de opname op R2. Dit zorgt ervoor dat R2 de houdbaarheidstimer verliep en het PEER-TERMINATION hello-pakket verstuurde om 16:51:47 (pakket 502).

De conclusie uit deze gegevens is dat het pakketverlies zich ergens in het dragernetwerk tussen R1 en R2 bevindt. In dit geval lag het verlies in de richting van R1 naar R2. Om verder onderzoek te doen, moet de drager worden betrokken om het pad voor druppels te controleren.

OSPF

De zelfde logica kan worden gebruikt om intermitterende OSPF flaps problemen op te lossen. In deze sectie worden belangrijke factoren beschreven die het onderscheiden van andere routeringsprotocollen met betrekking tot timers, IP-adresfilters en logberichten.

- De standaardtimers zijn 10-secondenhellos en een dode timer van 40 seconden. Bevestig altijd de timers die in gebruik zijn in uw netwerk wanneer het oplossen van problemen dode timer verlopen flaps.
- De pakketten van Hello zijn afkomstig van de interfaceIP adressen. Als extra ACL-specificiteit nodig is, is het multicast doeladres voor OSPF-hellos 24.0.0.5.
- De logberichten op de apparaten zijn lichtjes verschillend. In tegenstelling tot EIGRP is er geen concept van een peer beëindigingsbericht met OSPF. Het apparaat dat de verlopen dode timer detecteert, registreert dit als de reden van de flap en vervolgens de hellos die het verstuurt, bevat niet langer de router-ID van de peer, die ervoor zorgt dat de peer naar de INIT-staat gaat. Wanneer de hellos opnieuw worden gedetecteerd, gaat de nabijheid door tot het de VOLLEDIGE staat bereikt. Voorbeeld:

R1 detecteert verlopen dode 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
```

Echter, R2, toont alleen de logberichten wanneer OSPF teruggaat naar FULL. Er wordt geen logbericht weergegeven wanneer de status verandert in 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
```

Als u de EM op beide apparaten wilt activeren, gebruikt u "%OSPF-5-ADJCHG" als syslog-patroon. Dit zorgt ervoor dat de EEM op beide apparaten activeert zolang het naar beneden ging en weer omhoog kwam. De ingestelde snelheidswaarde zorgt ervoor dat het niet tweemaal binnen een korte periode teweegbrengt wanneer de veelvoud logt met dit koord wordt gezien. De sleutel is om te bevestigen of hellos worden verzonden en ontvangen in het pakket vangt aan beide kanten.

BGP

Dezelfde logica kan worden gebruikt om intermitterende BGP-flappen op te lossen. In deze sectie worden belangrijke factoren beschreven die het onderscheiden van andere routeringsprotocollen met betrekking tot timers, IP-adresfilters en logberichten.

- De standaardtimers zijn keepalives van 60 seconden en een houdtijd van 180 seconden. Bevestig altijd de timers die in gebruik zijn in uw netwerk wanneer de wachttijd voor probleemoplossing is verlopen.
- Keepalive-pakketten worden unicast tussen de IP-adressen van de buur naar TCP-bestemmingshaven 179 verzonden. Als extra ACL-specificiteit nodig is, moet u TCP-verkeer vanaf de IP-adressen van de bron naar de TCP-poort 179 van de bestemming toestaan.
- De logberichten voor BGP zien er op beide apparaten hetzelfde uit, maar het apparaat dat de wachttijd detecteert, toont aan dat het bericht naar de buur is verstuurd, terwijl het andere aangeeft dat het bericht is ontvangen. Voorbeeld:

R1 detecteert de verlopen wachttijd en verstuurt de melding naar 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 ontvangt het bericht van R1 omdat R1 ontdekte houdtijd is verlopen:

```
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
```

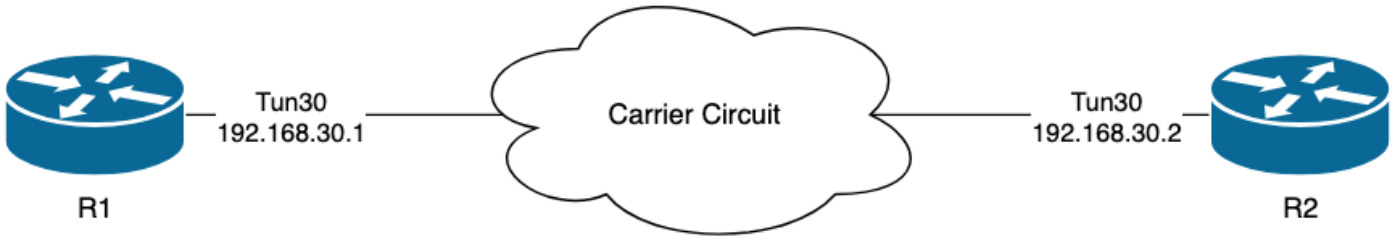
Als u de EM voor een BGP-flap wilt activeren, gebruikt u "%BGP_SESSION-5-ADJCHANGE" als syslog-patroon. Alle andere "%BGP" syslog berichten die ook na de flap worden vastgelegd, kunnen ook worden gebruikt om de EEM te activeren.

Intermitterende BFD-kleppen voor probleemoplossing

Dezelfde methodologie kan toegepast worden op het oplossen van problemen met intermitterende BFD flaps, waarbij enkele kleine verschillen toegepast kunnen worden op de analyse. In deze paragraaf wordt een aantal basisfuncties van de BFD besproken en wordt een voorbeeld gegeven van hoe EEM en EPC kunnen worden gebruikt voor probleemoplossing. Raadpleeg voor gedetailleerdere informatie over BFD-probleemoplossing Probleemoplossing bij detectie van bidirectionele doorsturen in Cisco IOS XE.

In dit voorbeeld, worden de BFD timers geplaatst aan 300ms met een multiplier van 3, wat betekent dat de echo's elke 300ms worden verzonden, en een echomislukking wordt ontdekt wanneer 3 echopakketten in een rij niet zijn teruggekeerd (gelijk aan een 900ms houdtijd).

Topologie



Voorbeeld - BFD-echomodus

In de BFD Echo Mode (de standaardmodus) worden de BFD-echopakketten verzonden met de lokale IP-interface als bron en bestemming. Dit staat de buur toe om het pakket in het gegevensvliegtuig te verwerken en het terug te keren naar het bronapparaat. Elke BFD echo wordt verzonden met een echo-id in de BFD Echo Message header. Deze kunnen worden gebruikt om te bepalen of een verzonden BFD echopakket terug werd ontvangen, aangezien er twee voorkomen van om het even welk bepaald BFD echopakket moeten zijn als het inderdaad door de buur was teruggekeerd. De BFD-controlepakketten die worden gebruikt om de status van de BFD-sessie te bepalen, worden unicast verzonden tussen de IP-interfaceadressen.

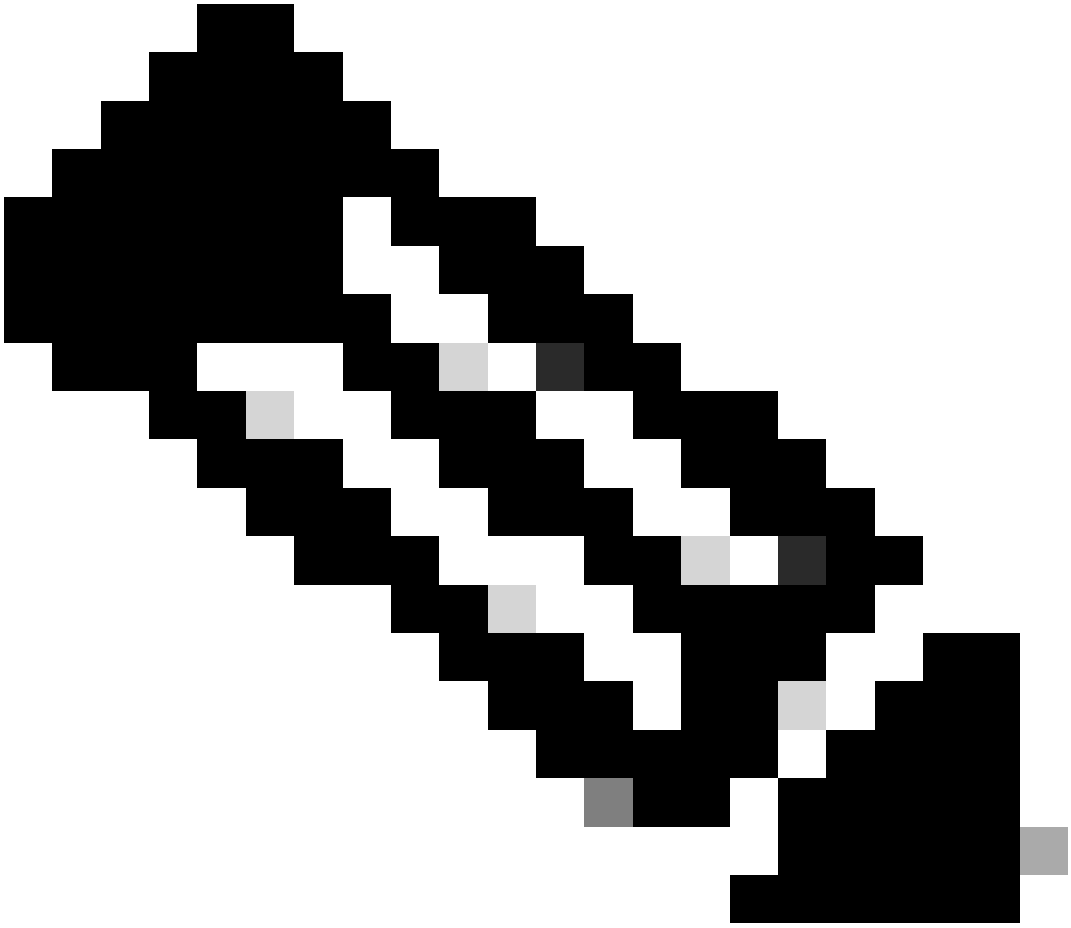
De logboeken van R1 wijzen erop dat de BFD nabijheid meerdere malen is gedaald toe te schrijven aan ECHO MISLUKKING, wat betekent dat tijdens die intervallen, R1 ontving of geen 3 van zijn eigen echopakketten terug van R2 verwerkt.

```
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
```

Configuratie

1. Configureer de ACL met de IP-adressen van de tunnelinterface, aangezien dit de IP-adressen van de bron van de BFD-echopakketten en -controlepakketten zijn:

```
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
```



Opmerking: De getoonde configuraties zijn van R1. Hetzelfde wordt gedaan op R2 voor de relevante interfaces en met aangepaste bestandsnamen voor de EEM. Als extra specificiteit is vereist, configureer dan de ACL voor UDP met bestemmingspoorten 3785 (echopakketten) en 3784 (controlepakketten).

2. Maak de EPC en koppel deze aan de interface en de 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. Start de EPC en bevestig dat pakketten in beide richtingen worden opgenomen:

```
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. De EEM configureren:

```
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. Wacht tot de volgende flap optreedt en kopieer de bestanden van bootflash via uw gewenste overdrachtsmethode voor analyse:

```
R1#show logging

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

- De log buffer geeft aan dat er een BFD flap was op 19:09:47, en de bestanden zijn opgeslagen door de EEM.

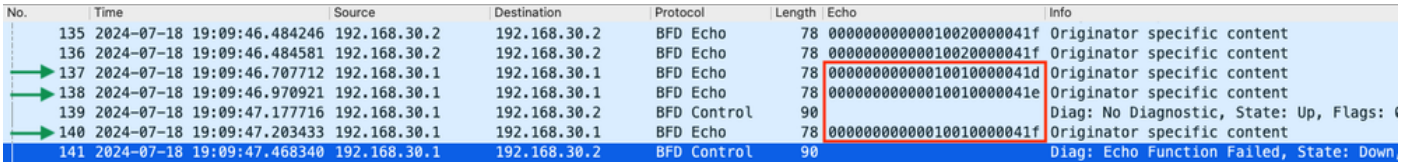
Analyse

Op dit punt correleert u de tijd van de flap in de logbuffer met de pakketopnamen die werden

verzameld om te bepalen of de BFD-echo's op beide uiteinden werden verzonden en ontvangen toen het probleem zich voordeed. Aangezien de reden van de flap op R1 ECHO-FOUT is, betekent dit dat er ook een controlepakket naar R2 verzonden zou zijn om de BFD-sessie te beëindigen. Dit wordt weerspiegeld in het logbestand dat is verzameld uit R2 waar de BFD omlaag reden RX DOWN wordt gezien:

```
*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
```

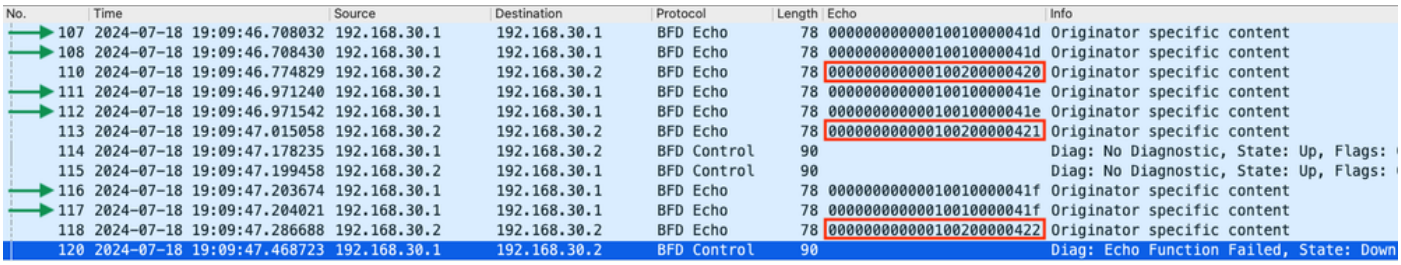
Omdat R1 een ECHO-FOUT heeft gedetecteerd, controleert u de pakketopname die op R1 is verzameld om te zien of BFD-echo's zijn verzonden en ontvangen in de 900ms vóór de flap.



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

- De opname laat zien dat R1 actief BFD-echopakketten zond tot op het moment van de flap, maar ze werden niet teruggestuurd door R2, dus R1 stuurt een controlepakket om de sessie te beëindigen op 19:09:47.468.
- Dit blijkt uit het feit dat de pakketten 137, 138, en 140 (aangegeven door de groene pijlen) slechts één keer in de opname worden gezien, die kan worden bepaald uit de BFD Echo IDs (in de rode doos). Als de echo's waren teruggekeerd, dan zou er een tweede exemplaar van elk van die pakketten met zelfde BFD echo-id zijn. Het veld IP-identificatie in de IP-header (hier niet weergegeven) kan worden gebruikt om dit ook te verifiëren.
- Deze opname laat ook zien dat er geen BFD-echo's zijn ontvangen van R2 na pakket 136, wat een andere indicatie is van pakketverlies in de richting van R2 naar R1.

De volgende stap is te bevestigen of alle BFD-echopakketten die door R1 zijn verzonden, door R2 zijn ontvangen en geretourneerd, zodat de uit R2 verzamelde opname moet worden gecontroleerd:



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

- Deze opname laat zien dat alle BFD-echo's die door R1 zijn verzonden, zijn ontvangen en geretourneerd door R2 (aangeduid met groene pijlen); De pakketten 107 en 108 zijn de zelfde BFD echo, pakketten 111 en 112 zijn de zelfde BFD echo, en de pakketten 116 en 117 zijn de zelfde BFD echo.

- Deze opname laat ook zien dat R2 actief echopakketten zond (aangeduid met rode vakjes) die niet worden gezien in de opname op R1, wat verder wijst op pakketverlies tussen de apparaten in de richting van R2 naar R1.

De conclusie uit deze gegevens is dat het pakketverlies ergens in het dragernetwerk tussen R1 en R2 zit, en al het bewijs op dit punt geeft aan dat de richting van het verlies van R2 naar R1 is. Om verder te onderzoeken, moet de drager worden betrokken om het pad voor druppels te controleren.

BFD asynchrone modus

Dezelfde methode kan worden toegepast wanneer de BFD asynchrone modus in gebruik is (echofunctie uitgeschakeld), en de EEM en EPC configuratie kunnen hetzelfde worden gehouden. Het verschil op asynchrone wijze is dat de apparaten unicast BFD controlepakketten naar elkaar als keepalives verzenden, analoog aan een typische routingprotocolnabijheid. Dit betekent dat alleen UDP-poort 3784-pakketten worden verzonden. In dit scenario blijft BFD in de status up zolang er binnen het vereiste interval een BFD-pakket van de buur wordt ontvangen. Wanneer dit niet gebeurt, is de mislukkingsreden de ONTDEKKINGSTIMER VERLOPEN, en de router verzendt een controlepakket naar de peer om de zitting neer te halen.

Om de opnamen op het apparaat te analyseren dat de fout heeft gedetecteerd, zoekt u de unicast BFD-pakketten die u van de peer hebt ontvangen tijdens de tijd vlak voor de flap. Als het TX-interval bijvoorbeeld is ingesteld op 300ms met een multiplier van 3, dan geeft dit, als er geen BFD-pakketten worden ontvangen in de 900ms voorafgaand aan de flap, het potentiële pakketverlies aan. In de opname die via de EEM van de buur is verzameld, controleer dit zelfde tijdvenster; als de pakjes in die tijd zijn verzonden, bevestigt het dat er ergens tussen de apparaten verlies is.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.