Dépannage des défaillances du protocole de routage intermittent avec EEM et EPC

Table des matières

Introduction

Ce document décrit comment dépanner les volets de protocole de routage intermittent et les volets BFD dans Cisco IOS® XE avec EEM et EPC.

Conditions préalables

Exigences

Il est recommandé de connaître les caractéristiques d'Embedded Event Manager (EEM) et d'Embedded Packet Capture (EPC) pour la ou les plates-formes impliquées dans le dépannage, ainsi que Wireshark. En outre, il est recommandé de se familiariser avec les fonctionnalités Hello et de test d'activité de base des protocoles de routage et de la détection de transfert bidirectionnel

(BFD).

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Présentation du problème

Les défaillances de protocole de routage intermittent sont un problème courant dans les réseaux de production, mais en raison de leur nature imprévisible, elles peuvent être difficiles à résoudre en temps réel. EEM permet d'automatiser la collecte des données en déclenchant la capture des données à l'aide de chaînes syslog lorsque les défaillances se produisent. Avec EEM et EPC, les données de capture de paquets peuvent être collectées à partir des deux extrémités de la contiguïté pour isoler la perte de paquets potentielle avant le moment du battement.

La nature des failles de protocole de routage intermittentes est qu'elles sont toujours dues à un délai d'attente Hello ou keepalive (à moins qu'il ne s'agisse d'un problème physique clair tel que des failles de liaison qui apparaîtraient dans les journaux). C'est donc ce que recouvre la logique de ce document.

Méthodologie de dépannage

La chose la plus importante à déterminer quand un défaut de protocole de routage se produit est si les paquets Hello ou les paquets de test d'activité ont été envoyés et reçus sur les deux périphériques au moment du problème. Cette méthode de dépannage consiste à utiliser un EPC continu sur une mémoire tampon circulaire jusqu'à ce que le battement se produise. EEM utilise alors la chaîne syslog appropriée pour déclencher un ensemble de commandes à exécuter, dont l'une arrête l'EPC. L'option de mémoire tampon circulaire permet à l'EPC de continuer à capturer les nouveaux paquets tout en écrasant les paquets les plus anciens dans la mémoire tampon, ce qui garantit que l'événement est capturé et que la mémoire tampon ne se remplit pas et ne s'arrête pas au préalable. Les données de capture de paquets peuvent ensuite être corrélées avec l'horodatage du volet pour déterminer si les paquets nécessaires ont été envoyés et reçus aux deux extrémités avant l'événement.

Ce problème se produit le plus souvent pour les périphériques qui forment une contiguïté sur un réseau intermédiaire tel qu’un fournisseur d’accès Internet (FAI), mais la même méthodologie peut être appliquée à n’importe quel scénario de battement de protocole de routage intermittent, quels que soient les détails de la topologie. Il en va de même dans les cas où le périphérique voisin est géré par un tiers et n'est pas accessible. Dans de tels cas, la méthode de dépannage décrite dans ce document peut être appliquée au seul périphérique accessible afin de prouver s'il a envoyé et reçu les paquets requis avant le volet. Lorsque cela est confirmé, les données peuvent être affichées à la partie qui gère le voisin afin de poursuivre le dépannage à l'autre extrémité si nécessaire.

Présentation de la configuration

Cette section fournit un ensemble de modèles de configuration qui peuvent être utilisés pour configurer cette capture de données automatisée. Modifiez les adresses IP, les noms d'interface et les noms de fichiers selon vos besoins.

Modèle de configuration ACL

Dans la plupart des cas, le seul trafic provenant de l'adresse IP de l'interface aux deux extrémités d'une contiguïté de routage est le trafic de contrôle de routage lui-même. Ainsi, une liste de contrôle d’accès qui autorise le trafic à partir de l’adresse IP de l’interface locale et de l’adresse IP du voisin vers n’importe quelle destination couvre la nécessité de n’importe quel protocole de routage, ainsi que BFD. Si un filtre supplémentaire est nécessaire, l’adresse IP de destination appropriée basée sur le protocole de routage ou le mode BFD peut également être spécifiée. Définissez les paramètres ACL en mode de configuration :

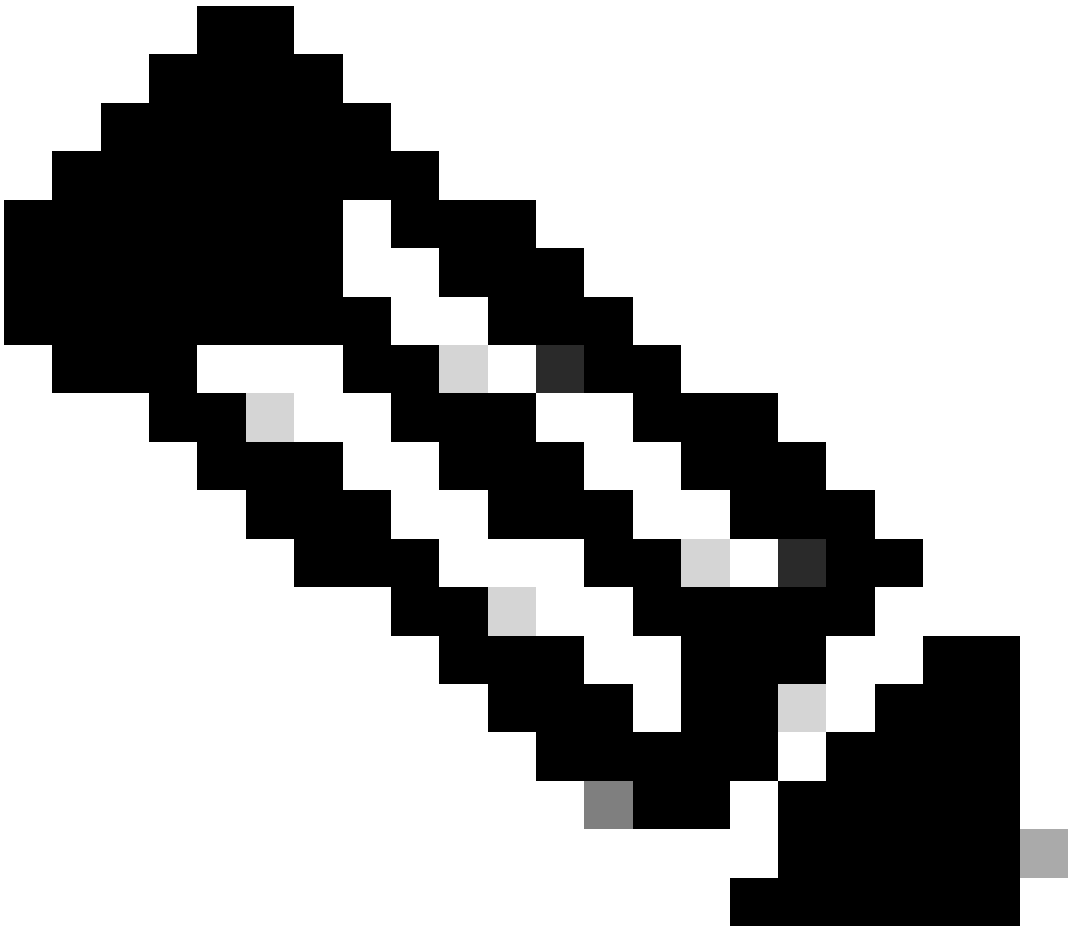
```
config t

ip access-list extended




      permit ip host




       any permit ip host




        any end
```

Modèle de paramètres EPC

Les paramètres EPC sont créés à partir du mode d'exécution privilégié et non du mode de configuration. Consultez les guides de configuration spécifiques à la plate-forme pour déterminer s'il existe des restrictions avec EPC. Créez les paramètres de l'interface souhaitée et associez-la à la liste de contrôle d'accès pour filtrer le trafic souhaité :

- monitor capture <EPC name> interface <interface> les deux
- monitor capture <EPC name> access-list <ACL name>
- <EPC name> taille de tampon 5 circulaire pour la capture de moniteur

---



Remarque : Sur certaines versions logicielles, le trafic généré localement n'est pas visible avec un EPC au niveau de l'interface. Dans de tels scénarios, les paramètres de capture peuvent être modifiés pour capturer les deux sens du trafic au niveau du processeur :

- monitor capture <EPC name> control-plane both
- monitor capture <EPC name> access-list <ACL name>
- <EPC name> taille de tampon 5 circulaire pour la capture de moniteur

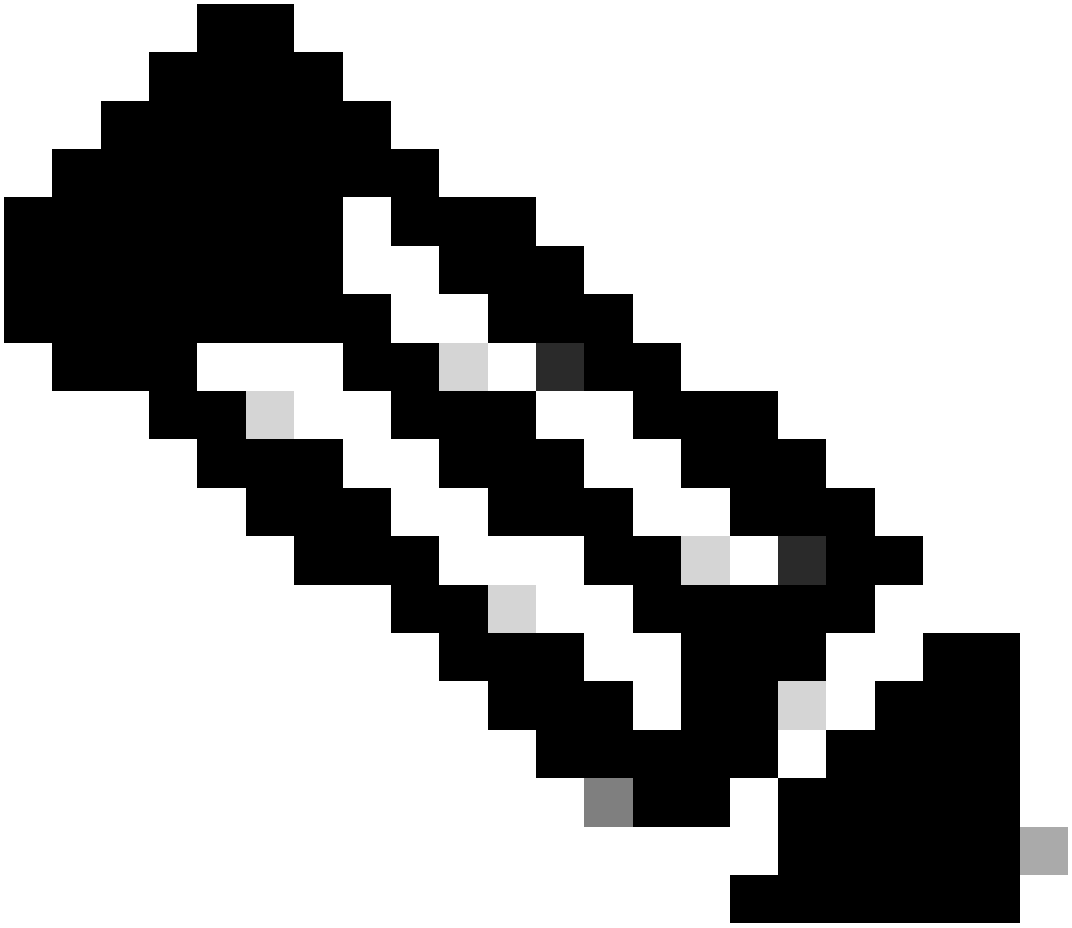
Une fois configuré, démarrez l'EPC :

- monitor capture <EPC name> start

Le module EEM est configuré pour arrêter la capture lorsque le volet se produit.

Pour vous assurer que les paquets sont capturés dans les deux directions, vérifiez la mémoire tampon de capture :

```
show monitor capture


      buffer brief
```



Remarque : Les plates-formes de commutation Catalyst (telles que Cat9k et Cat3k) nécessitent l'arrêt de la capture avant que la mémoire tampon puisse être affichée. Pour confirmer que la capture fonctionne, arrêtez-la à l'aide de la commande monitor capture stop, affichez la mémoire tampon, puis redémarrez-la pour collecter des données.

Modèle de configuration EEM

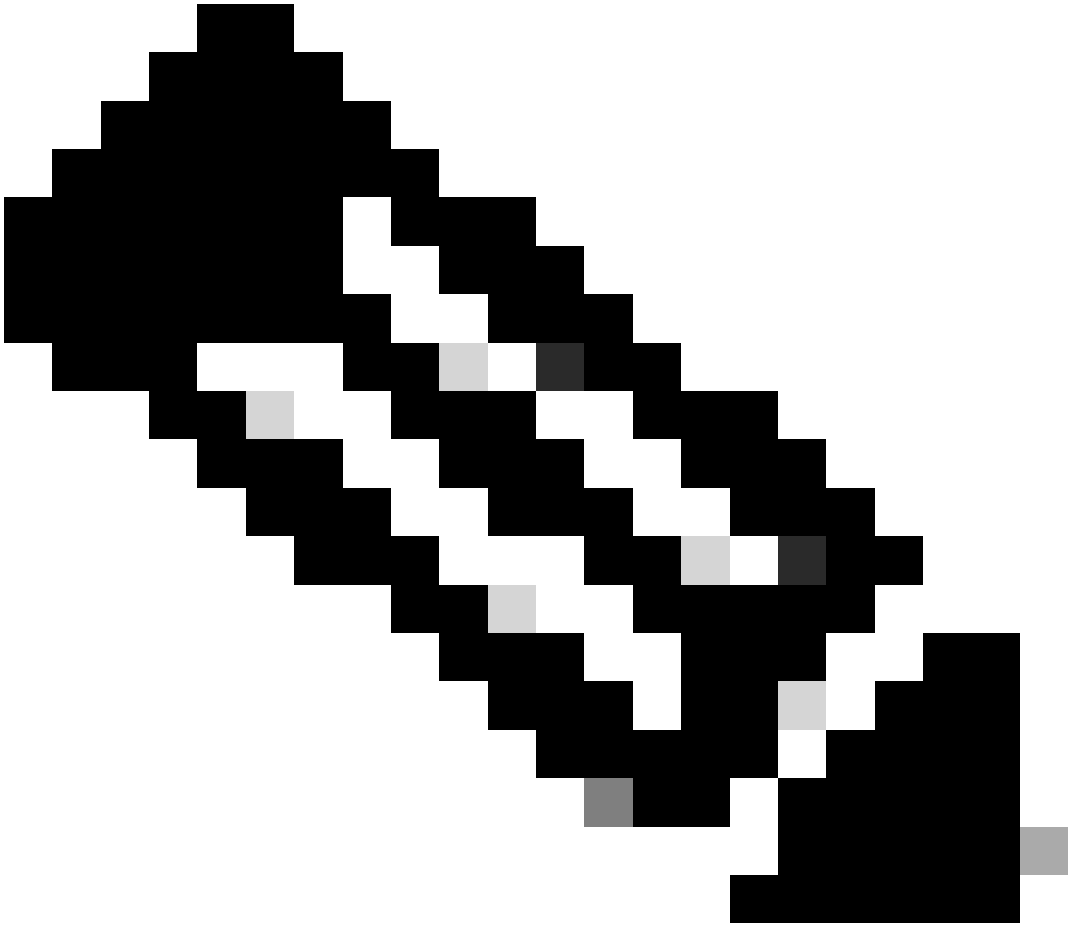
L'objectif principal de l'EEM est d'arrêter la capture de paquets et de l'enregistrer avec la mémoire tampon Syslog. Des commandes supplémentaires peuvent être incluses pour vérifier d'autres facteurs tels que le processeur, les abandons d'interface ou l'utilisation des ressources spécifiques à la plate-forme et les compteurs d'abandon. Créez l'applet EEM en mode de configuration :

```
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



Remarque : Sur les plates-formes de commutation Catalyst (telles que Cat9k et Cat3k), la commande d'exportation de la capture est légèrement différente. Pour ces plates-formes, modifiez la commande CLI utilisée dans l'action 035 :

```
action 035 cli command "monitor capture

      export location bootflash:

       .pcap"
```

La valeur de la limite de débit dans l'EEM est exprimée en secondes et indique le temps qui doit s'écouler avant que l'EEM puisse s'exécuter à nouveau. Dans cet exemple, il est défini sur 100000 secondes (27,8 heures) pour laisser suffisamment de temps à l'administrateur réseau pour identifier qu'il a terminé et extraire les fichiers du périphérique avant qu'il ne s'exécute à nouveau. Si l'EEM est de nouveau exécuté seul après cette période de limitation de débit, aucune nouvelle donnée de capture de paquet n'est collectée, car l'EPC doit être démarré manuellement. Cependant, les nouvelles sorties de la commande show sont ajoutées aux fichiers texte.

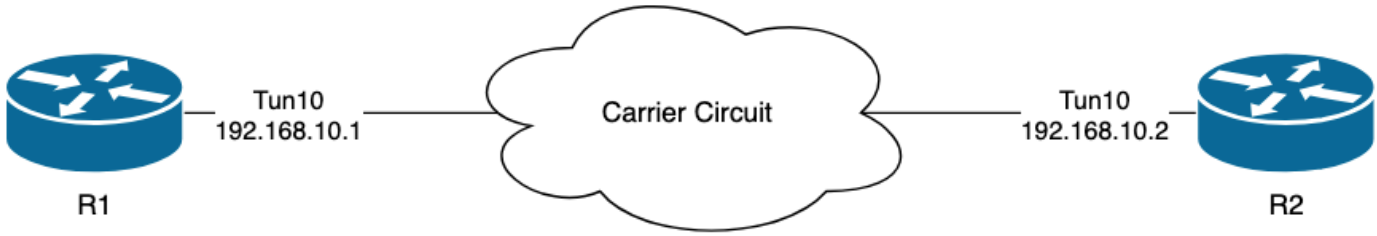
L'EEM peut être modifié selon les besoins pour collecter des informations d'abandon de paquets spécifiques à la plate-forme et obtenir les fonctionnalités supplémentaires requises pour votre scénario.

Dépannage des défaillances du protocole de routage intermittent

Exemple - EIGRP

Tous les minuteurs sont définis sur la valeur par défaut dans cet exemple (HELLO 5 secondes, temps d'attente 15 secondes).

Topologie



Les journaux sur R1 indiquent qu'il y a eu des volets EIGRP intermittents qui se sont produits à plusieurs heures d'intervalle :

```
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
```

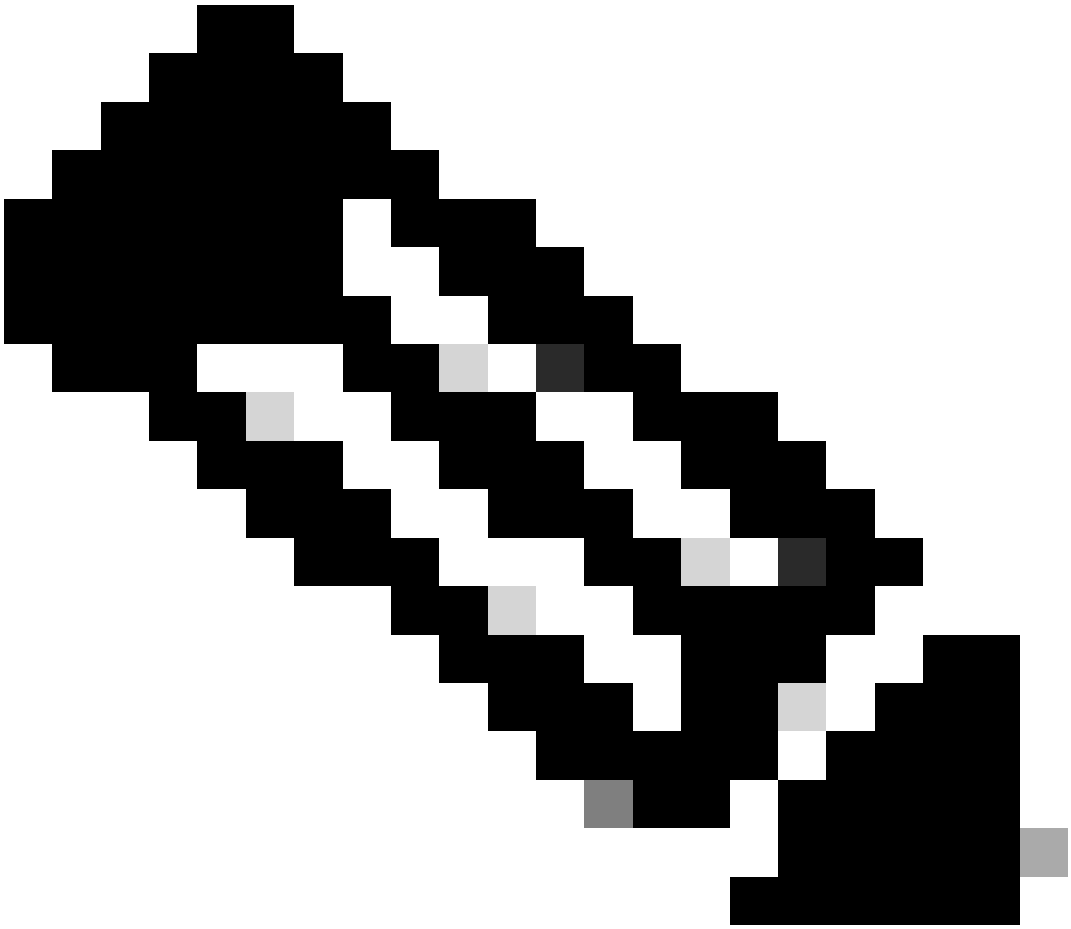
La perte de paquets peut être dans les deux sens ; le délai d'attente expiré indique que ce

périphérique n'a pas reçu ou traité de paquet Hello de l'homologue pendant le délai d'attente, et le message Interface PEER-TERMINATION received indique que l'homologue a mis fin à la contiguïté car il n'a pas reçu ou traité de paquet Hello pendant le délai d'attente.

Configuration

1. Configurez la liste de contrôle d’accès avec les adresses IP de l’interface du tunnel, car il s’agit des adresses IP source des HELLO :

```
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
```



Remarque : Les configurations présentées proviennent de R1. Il en est de même sur R2

---

pour les interfaces concernées et avec des noms de fichiers modifiés pour l'EEM. Si une spécificité supplémentaire est requise, configurez la liste de contrôle d'accès avec l'adresse de multidiffusion EIGRP 224.0.0.10 comme adresse IP de destination pour capturer les paquets Hello.

---

2. Créez l'EPC et associez-le à l'interface et à la liste de contrôle d'accès :

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

3. Démarrez l'EPC et vérifiez que les paquets sont capturés dans les deux directions :

```
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. Configurez 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. Attendez que le prochain battement se produise, et copiez les fichiers de bootflash via votre méthode de transfert préférée pour l'analyse :

```
R1#show logging
```

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

- La mémoire tampon du journal sur le routeur indique qu'il y avait un volet EIGRP et que les fichiers ont été enregistrés par l'EEM.

Analyse

À ce stade, établissez une corrélation entre l'heure du battement détecté dans la mémoire tampon du journal et les captures de paquets collectées pour déterminer si les paquets Hello ont été envoyés et reçus aux deux extrémités lorsque le battement s'est produit. Puisque l'interface PEER-TERMINATION reçue a été vue sur R1, cela signifie que R2 doit avoir détecté des paquets Hello perdus et donc que le temps d'attente a expiré, ce qui est ce qui est vu dans le fichier journal :

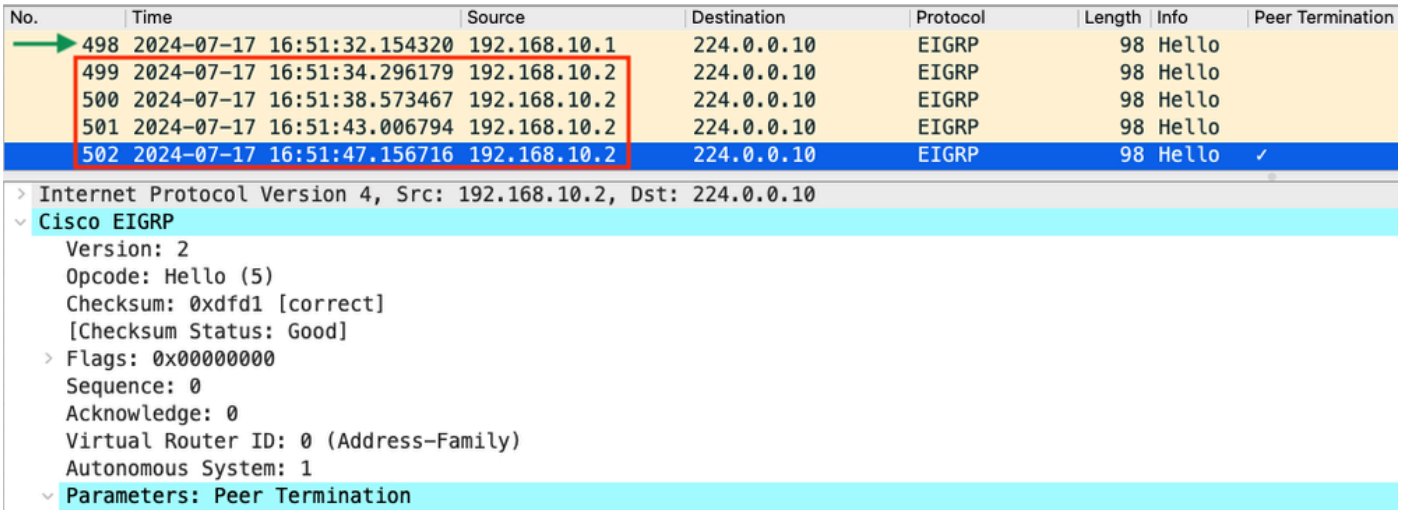
```
*Jul 17 16:51:47.156: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is down: holdin
*Jul 17 16:51:51.870: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is up: new adja
```

Étant donné que R2 a détecté que le temps d'attente a expiré, vérifiez si des messages Hello ont été envoyés par R1 dans les 15 secondes précédant le volet de la capture collectée sur R1 :

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

- La capture affiche les paquets Hello de 192.168.10.1 (R1) et 192.168.10.2 (R2) dans les 15 secondes précédant le paquet Hello TERMINATION D'HOMOLOGUE que R2 envoie à 16:51:47 (paquet 513).
- Plus précisément, les paquets 503, 505, 508 et 511 (indiqués par les flèches vertes) étaient tous des paquets Hello envoyés par R1 au cours de cette période.

L'étape suivante consiste à confirmer si tous les messages Hello envoyés par R1 ont été reçus par R2 à ce moment-là, de sorte que la capture collectée à partir de R2 doit être vérifiée :



- La capture montre que le dernier Hello reçu de 192.168.10.1 (R1) était à 16:51:32 (indiqué par la flèche verte). Après cela, les 15 secondes suivantes affichent uniquement les messages Hello envoyés par R2 (indiqués par la zone rouge). Les paquets 505, 508 et 511 de la capture de R1 n'apparaissent pas dans la capture de R2. R2 détecte alors que le minuteur de mise en attente a expiré et envoie le paquet Hello TERMINATION D'HOMOLOGUE à 16:51:47 (paquet 502).

La conclusion de ces données est que la perte de paquets se situe quelque part dans le réseau de l'opérateur entre R1 et R2. Dans ce cas, la perte s'est produite dans la direction de R1 à R2. Pour approfondir l'étude, l'opérateur doit être impliqué pour vérifier le chemin à la recherche de pertes.

OSPF

La même logique peut être utilisée pour dépanner les volets OSPF intermittents. Cette section décrit les facteurs clés qui le distinguent des autres protocoles de routage en ce qui concerne les compteurs, les filtres d'adresses IP et les messages de journal.

- Les minuteurs par défaut sont des HELLO de 10 secondes et un minuteur Dead de 40 secondes. Vérifiez toujours les minuteurs qui sont utilisés sur votre réseau lors du dépannage des volets expirés des minuteurs morts.
- Les paquets Hello proviennent des adresses IP de l'interface. Si une spécificité ACL supplémentaire est nécessaire, l'adresse de destination de multidiffusion pour les HELLO OSPF est 224.0.0.5.
- Les messages du journal sur les périphériques sont légèrement différents. Contrairement au protocole EIGRP, il n'existe aucun concept de message de terminaison d'homologue avec OSPF. Au contraire, le périphérique qui détecte le minuteur d'arrêt expiré consigne cette erreur comme la raison du battement, puis les messages Hello qu'il envoie ne contiennent plus l'ID de routeur de l'homologue, ce qui entraîne le passage de l'homologue à l'état INIT. Lorsque les paquets Hello sont détectés à nouveau, la contiguïté passe à travers jusqu'à ce qu'elle atteigne l'état FULL. Exemple :

R1 détecte que le délai d'arrêt a expiré :

```
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
```

Cependant, R2 n'affiche les messages de journal que lorsque le protocole OSPF revient à la valeur FULL. Il n'affiche pas de message de journal lorsque l'état passe à 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
```

Pour déclencher le module EEM sur les deux périphériques, utilisez « %OSPF-5-ADJCHG » comme modèle syslog. Cela garantit que l'EEM se déclenche sur les deux périphériques tant qu'il est tombé en panne et qu'il s'est rétabli. La valeur ratelimit configurée garantit qu'elle ne se déclenche pas deux fois dans une courte période lorsque plusieurs journaux avec cette chaîne sont vus. La clé consiste à confirmer si les paquets Hello sont envoyés et reçus dans les captures de paquets des deux côtés.

BGP

La même logique peut être utilisée pour dépanner les défaillances BGP intermittentes. Cette section décrit les facteurs clés qui le distinguent des autres protocoles de routage en ce qui concerne les compteurs, les filtres d’adresses IP et les messages de journal.

- Les minuteurs par défaut sont des keepalives de 60 secondes et un temps d'attente de 180 secondes. Vérifiez toujours les minuteurs utilisés sur votre réseau lors du dépannage des volets d'expiration du délai d'attente.
- Les paquets Keepalive sont envoyés en monodiffusion entre les adresses IP voisines vers le port de destination TCP 179. Si une spécificité ACL supplémentaire est nécessaire, autorisez le trafic TCP des adresses IP source vers le port TCP de destination 179.
- Les messages de journal pour BGP semblent similaires sur les deux périphériques, mais le périphérique qui détecte le temps d'attente expire montre qu'il a envoyé la notification au voisin, tandis que l'autre indique qu'il a reçu le message de notification. Exemple :

R1 détecte que le délai d'attente a expiré et envoie la notification à 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 reçoit la notification de R1 car le délai d'attente détecté par R1 a expiré :

```
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
```

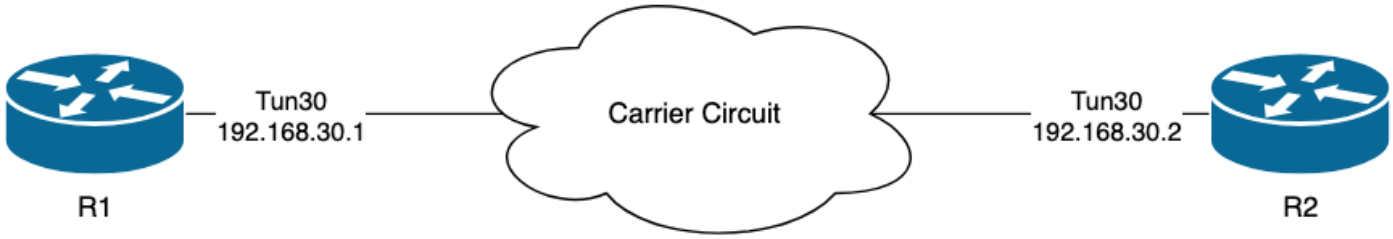
Pour déclencher l'EEM pour un rabat BGP, utilisez « %BGP_SESSION-5-ADJCHANGE » comme modèle syslog. Tous les autres messages syslog « %BGP » qui sont également consignés après le rabat peuvent également être utilisés pour déclencher l'EEM.

Dépannage des volets BFD intermittents

La même méthodologie peut être appliquée au dépannage des volets BFD intermittents, avec quelques différences mineures à appliquer à l'analyse. Cette section couvre certaines fonctionnalités BFD de base et fournit un exemple d'utilisation d'EEM et d'EPC pour le dépannage. Pour plus d'informations détaillées sur le dépannage BFD, référez-vous à Dépannage de la détection de transfert bidirectionnel dans Cisco IOS XE.

Dans cet exemple, les compteurs BFD sont définis sur 300 ms avec un multiplicateur de 3, ce qui signifie que des échos sont envoyés toutes les 300 ms, et une défaillance d'écho est détectée lorsque 3 paquets d'écho dans une ligne ne sont pas renvoyés (ce qui équivaut à un temps d'attente de 900 ms).

Topologie



Exemple - Mode d'écho BFD

En mode d’écho BFD (mode par défaut), les paquets d’écho BFD sont envoyés avec l’adresse IP de l’interface locale comme source et destination. Cela permet au voisin de traiter le paquet dans le plan de données et de le renvoyer au périphérique source. Chaque écho BFD est envoyé avec un ID d'écho dans l'en-tête du message d'écho BFD. Ceux-ci peuvent être utilisés pour déterminer si un paquet d'écho BFD envoyé a été reçu en retour, car il doit y avoir deux occurrences d'un paquet d'écho BFD donné s'il a bien été retourné par le voisin. Les paquets de contrôle BFD, qui sont utilisés pour contrôler l'état de la session BFD, sont envoyés en monodiffusion entre les adresses IP de l'interface.

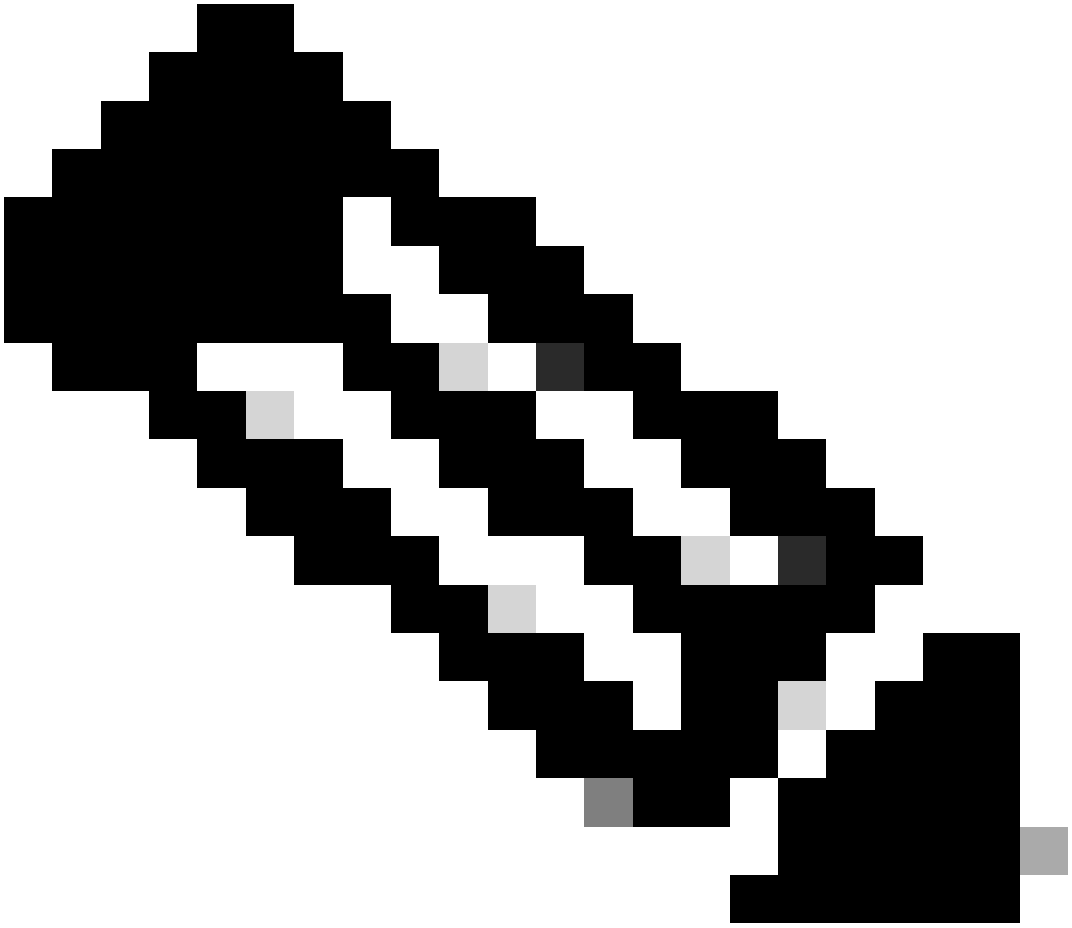
Les journaux de R1 indiquent que la contiguïté BFD s'est désactivée plusieurs fois en raison de ECHO FAILURE, ce qui signifie qu'au cours de ces intervalles, R1 n'a pas reçu ni traité 3 de ses propres paquets d'écho de R2.

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

Configuration

1. Configurez la liste de contrôle d’accès avec les adresses IP de l’interface de tunnel, car il s’agit des adresses IP source des paquets d’écho BFD et des paquets de contrôle :

```
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
```



Remarque : Les configurations présentées proviennent de R1. Il en est de même sur R2 pour les interfaces concernées et avec des noms de fichiers modifiés pour l'EEM. Si une spécificité supplémentaire est requise, configurez la liste de contrôle d'accès pour UDP avec les ports de destination 3785 (paquets d'écho) et 3784 (paquets de contrôle).

2. Créez l'EPC et associez-le à l'interface et à la liste de contrôle d'accès :

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

3. Démarrez l'EPC et vérifiez que les paquets sont capturés dans les deux directions :

```
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. Configurez 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. Attendez que le prochain battement se produise, et copiez les fichiers de bootflash via votre méthode de transfert préférée pour l'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
```

- La mémoire tampon du journal indique qu'il y avait un volet BFD à 19:09:47 et que les fichiers ont été enregistrés par l'EEM.

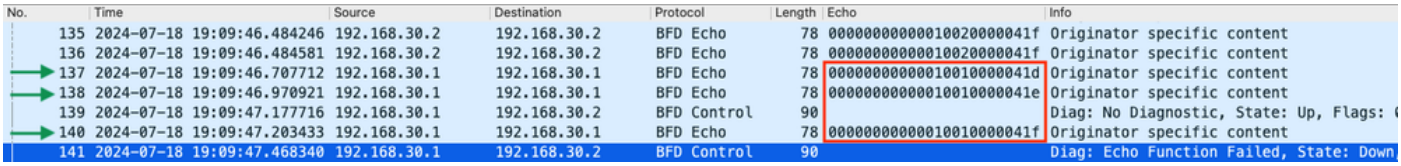
Analyse

À ce stade, établissez une corrélation entre l'heure du battement détecté dans le tampon du

journal et les captures de paquets collectées pour déterminer si les échos BFD ont été envoyés et reçus aux deux extrémités lorsque le problème s'est produit. Puisque la raison du battement sur R1 est ECHO FAILURE, cela signifie qu'il aurait également envoyé un paquet de contrôle à R2 pour mettre fin à la session BFD, et ceci est reflété dans le fichier journal collecté à partir de R2 où la raison BFD down RX DOWN est vue :

```
*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
```

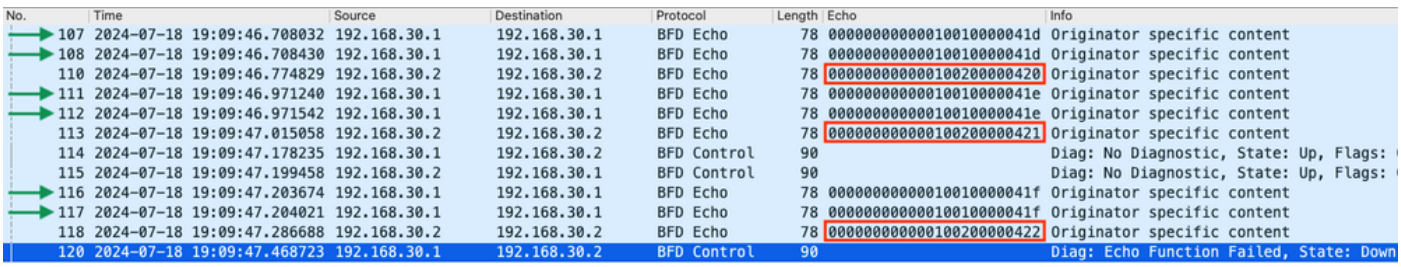
Étant donné que R1 a détecté une ECHO FAILURE, vérifiez la capture de paquets collectée sur R1 pour voir si elle a envoyé et reçu des échos BFD dans les 900 ms précédant le battement.



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

- La capture montre que R1 a envoyé activement des paquets d'écho BFD jusqu'au moment du battement, mais qu'ils n'ont pas été renvoyés par R2, de sorte que R1 envoie un paquet de contrôle pour mettre fin à la session à 19:09:47.468.
- Cela ressort du fait que les paquets 137, 138 et 140 (indiqués par les flèches vertes) ne sont vus qu'une seule fois dans la capture, ce qui peut être déterminé à partir des Echo ID BFD (dans la zone rouge). Si les échos avaient été renvoyés, il y aurait alors une deuxième copie de chacun de ces paquets avec le même ID d'écho BFD. Le champ d'identification IP de l'en-tête IP (non illustré ici) peut également être utilisé pour vérifier cela.
- Cette capture montre également qu'aucun écho BFD n'a été reçu de R2 après le paquet 136, ce qui est une autre indication de perte de paquet dans la direction de R2 vers R1.

L'étape suivante consiste à confirmer si tous les paquets d'écho BFD envoyés par R1 ont été reçus et renvoyés par R2, de sorte que la capture collectée à partir de R2 doit être vérifiée :



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	0000000000001002000420	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	0000000000001002000421	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	0000000000001002000422	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

- Cette capture montre que tous les échos BFD envoyés par R1 ont été reçus et renvoyés par R2 (indiqués par des flèches vertes) ; Les paquets 107 et 108 sont le même écho BFD, les paquets 111 et 112 sont le même écho BFD et les paquets 116 et 117 sont le même écho BFD.
- Cette capture montre également que R2 a envoyé activement des paquets d'écho (indiqués

par des cases rouges) qui ne sont pas visibles dans la capture sur R1, ce qui indique en outre une perte de paquets entre les périphériques dans la direction allant de R2 à R1.

La conclusion de ces données est que la perte de paquets se situe quelque part dans le réseau de l’opérateur entre R1 et R2, et toutes les preuves à ce stade indiquent que la direction de la perte est de R2 à R1. Pour approfondir l’étude, l’opérateur doit être impliqué pour vérifier le chemin des pertes.

Mode asynchrone BFD

La même méthode peut être appliquée lorsque le mode asynchrone BFD est utilisé (fonction d'écho désactivée), et la configuration EEM et EPC peut être conservée. La différence dans le mode asynchrone est que les périphériques envoient des paquets de contrôle BFD monodiffusion les uns aux autres en tant que keepalives, de manière analogue à une contiguïté de protocole de routage typique. Cela signifie que seuls les paquets du port UDP 3784 sont envoyés. Dans ce scénario, BFD reste à l'état up tant qu'un paquet BFD est reçu du voisin dans l'intervalle requis. Lorsque cela ne se produit pas, la raison de l'échec est DETECT TIMER EXPIRED et le routeur envoie un paquet de contrôle à l'homologue pour arrêter la session.

Pour analyser les captures sur le périphérique qui a détecté la défaillance, recherchez les paquets BFD de monodiffusion reçus de l'homologue pendant le temps juste avant le battement. Par exemple, si l'intervalle TX est défini sur 300 ms avec un multiplicateur de 3, alors s'il n'y a aucun paquet BFD reçu dans les 900 ms avant le battement, cela indique une perte de paquet potentielle. Dans la capture collectée auprès du voisin via l'EEM, vérifiez cette même fenêtre temporelle ; si les paquets ont été envoyés pendant ce temps, cela confirme qu'il y a une perte quelque part entre les périphériques.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.