Identificar e solucionar problemas de oscilações do protocolo de roteamento intermitente com EEM e EPC

Contents

Introdução

Este documento descreve como solucionar problemas de sincronismo de protocolo de roteamento intermitente e sincronismo de BFD no Cisco IOS® XE com EEM e EPC.

Pré-requisitos

Requisitos

Recomenda-se que você esteja familiarizado com os detalhes do Embedded Event Manager

(EEM) e do Embedded Packet Capture (EPC) para a(s) plataforma(s) envolvida(s) na solução de problemas, bem como com o Wireshark. Além disso, recomenda-se a familiaridade com a funcionalidade básica de hello e keepalive dos protocolos de roteamento e da detecção de encaminhamento bidirecional (BFD).

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral do problema

Flaps de protocolo de roteamento intermitentes são um problema comum em redes de produção, mas devido à sua natureza imprevisível, eles podem ser difíceis de resolver em tempo real. O EEM oferece a capacidade de automatizar a coleta de dados, disparando a captura de dados com cadeias de caracteres de syslog quando ocorrem oscilações. Com o EEM e o EPC, os dados de captura de pacotes podem ser coletados de ambas as extremidades da adjacência para isolar a possível perda de pacotes antes do momento da oscilação.

A natureza das oscilações intermitentes do protocolo de roteamento é que elas sempre se devem a um tempo limite de hello ou keepalive (a menos que seja um problema físico claro, como oscilações de link, que apareceriam nos logs). Portanto, é isso que a lógica neste documento aborda.

Metodologia de Troubleshooting

O mais importante para determinar quando ocorre um flap do protocolo de roteamento é se os pacotes hello ou os pacotes keepalive foram enviados e recebidos em ambos os dispositivos no momento do problema. Este método de Troubleshooting envolve o uso de um EPC contínuo em um buffer circular até que o flap ocorra, momento em que o EEM usa a string de syslog relevante para acionar um conjunto de comandos a serem executados, um dos quais interrompe o EPC. A opção de buffer circular permite que o EPC continue a capturar novos pacotes enquanto sobrescreve os pacotes mais antigos no buffer, o que garante que o evento seja capturado e que o buffer não seja preenchido e parado com antecedência. Os dados de captura de pacote podem então ser correlacionados com o carimbo de data e hora do flap para determinar se os pacotes necessários foram enviados e recebidos em ambas as extremidades antes do evento.

Esse problema ocorre mais comumente para dispositivos que formam uma adjacência em uma rede intermediária, como um ISP (Provedor de serviços de Internet), mas a mesma metodologia pode ser aplicada para qualquer cenário de flap de protocolo de roteamento intermitente, independentemente dos detalhes da topologia específica. O mesmo pode ser feito em instâncias onde o dispositivo vizinho é gerenciado por terceiros e não pode ser acessado. Nesses casos, o método de identificação e solução de problemas descrito neste documento pode ser aplicado apenas a um dispositivo que esteja acessível para provar se ele enviou e recebeu os pacotes

necessários antes da oscilação. Quando isso é confirmado, os dados podem ser mostrados para a parte que gerencia o vizinho para fazer troubleshooting adicional na outra extremidade, se necessário.

Visão geral sobre a configuração

Esta seção fornece um conjunto de modelos de configuração que podem ser usados para configurar essa captura de dados automatizada. Modifique os endereços IP, os nomes de interface e os nomes de arquivo conforme necessário.

Modelo de configuração da ACL

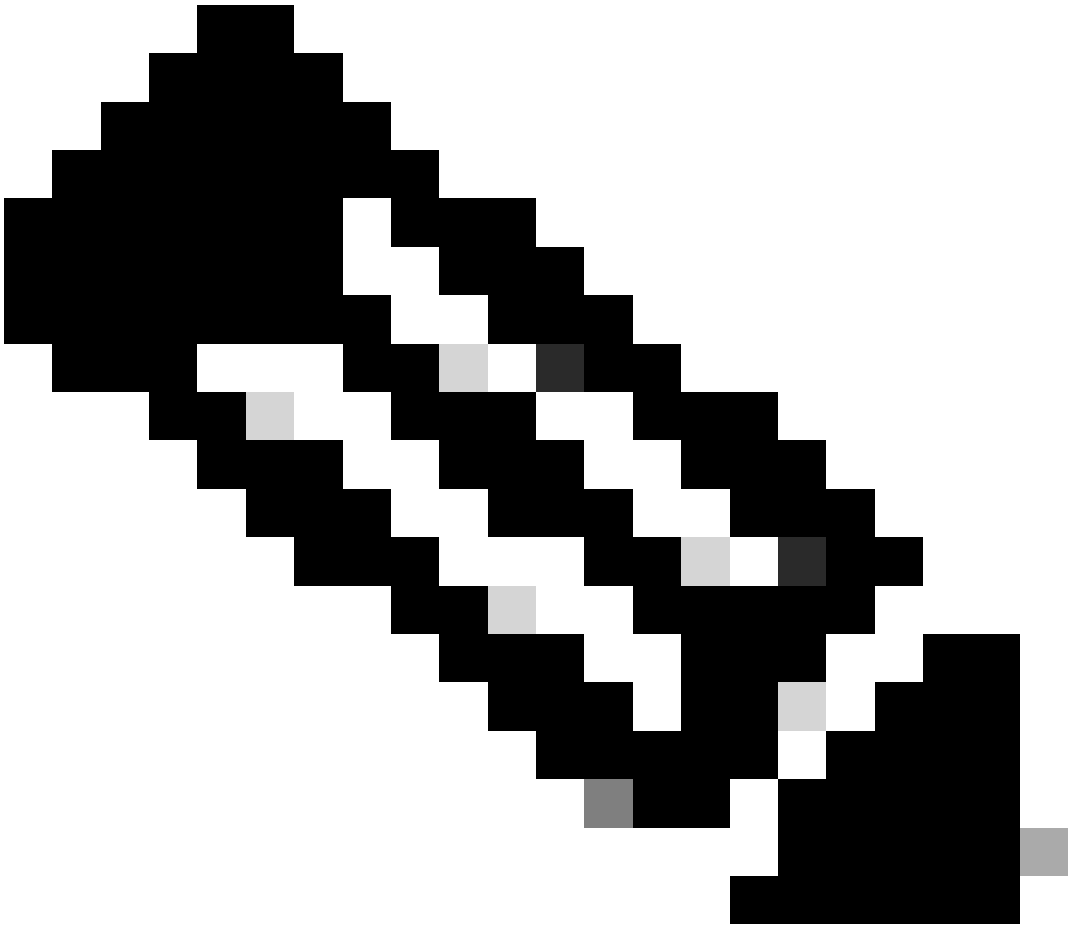
Na maioria dos casos, o único tráfego originado do endereço IP da interface em ambas as extremidades de uma adjacência de roteamento é o próprio tráfego de controle de roteamento. Como tal, uma ACL que permite o tráfego do endereço IP da interface local e do endereço IP vizinho para qualquer destino cobre o requisito de qualquer protocolo de roteamento, bem como BFD. Se um filtro adicional for necessário, o IP de destino relevante baseado no protocolo de roteamento ou no modo BFD também poderá ser especificado. Defina os parâmetros da ACL no modo de configuração:

```
config t

ip access-list extended




      permit ip host




       any permit ip host




        any end
```

Modelo de Parâmetros EPC

Os parâmetros EPC são criados no modo exec privilegiado, não no modo config. Verifique os guias de configuração específicos da plataforma para determinar se há restrições com o EPC. Crie os parâmetros para a interface desejada e associe-a à ACL para filtrar o tráfego desejado:

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



Note: Em algumas versões de software, o tráfego gerado localmente não é visível com um EPC de nível de interface. Nesses cenários, os parâmetros de captura podem ser alterados para capturar ambas as direções do tráfego na CPU:

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

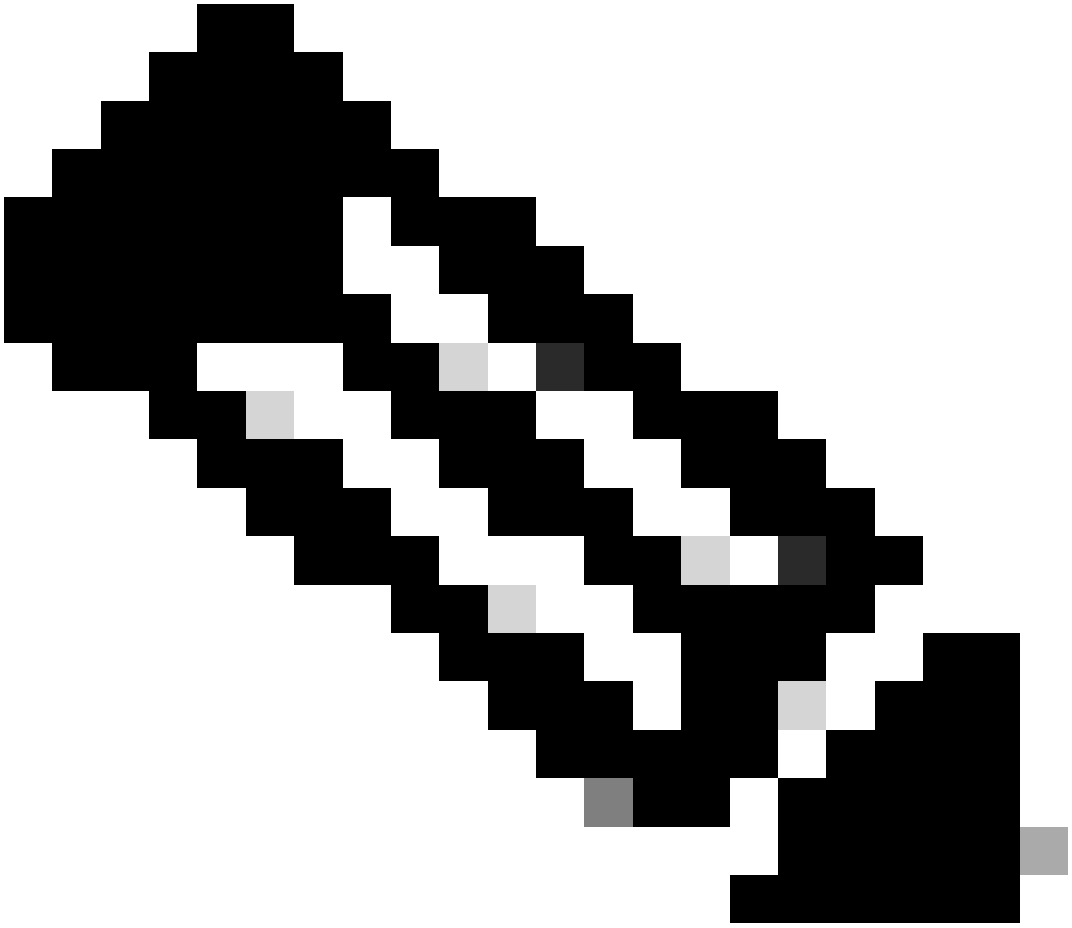
Uma vez configurado, inicie o EPC:

- monitor capture <EPC name> start

O EEM é configurado para interromper a captura quando a oscilação ocorrer.

Para garantir que os pacotes sejam capturados em ambas as direções, verifique o buffer de captura:

```
show monitor capture

      buffer brief
```



Note: As plataformas de switching Catalyst (como Cat9k e Cat3k) exigem que a captura seja interrompida antes que o buffer possa ser visualizado. Para confirmar se a captura funciona, interrompa a captura com o comando monitor capture stop, exiba o buffer e inicie-o novamente para coletar dados.

Modelo de configuração de EEM

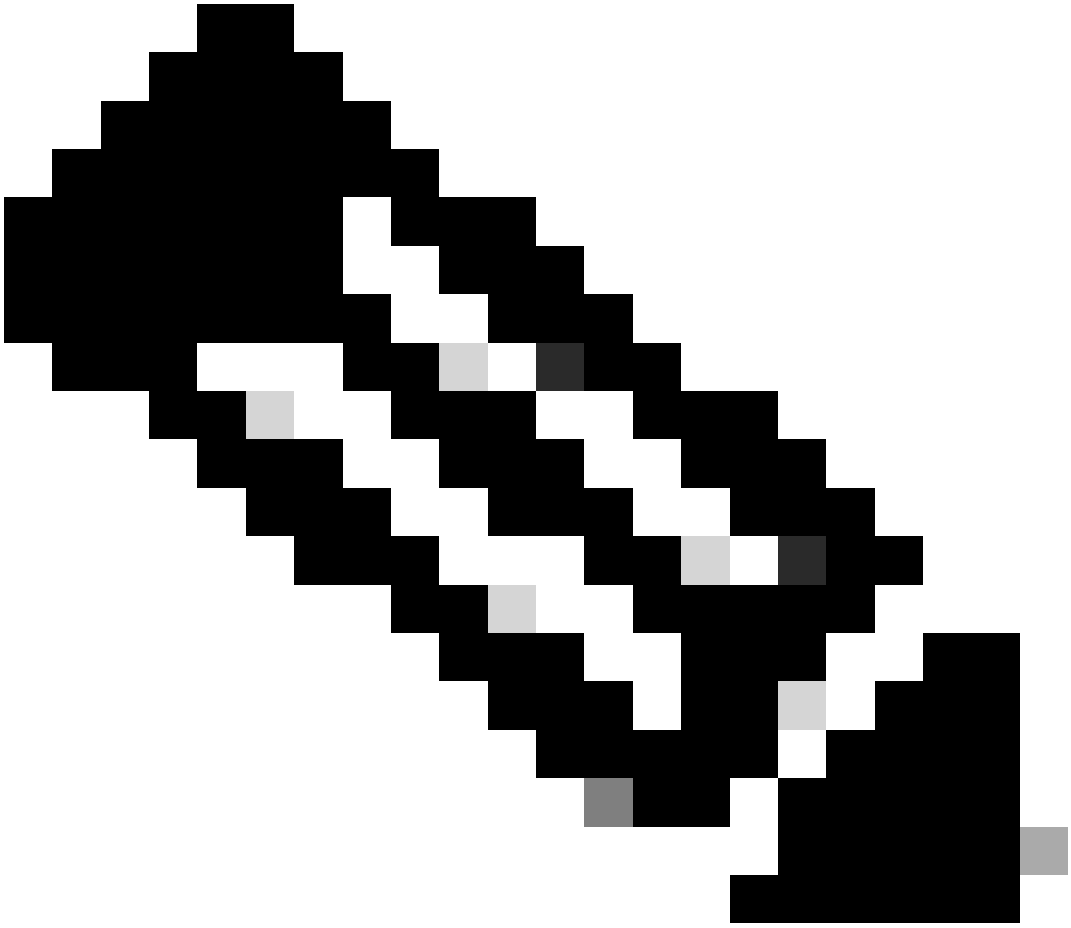
A principal finalidade do EEM é interromper a captura de pacotes e salvá-la junto com o buffer de syslog. Comandos adicionais podem ser incluídos para verificar outros fatores, como CPU, quedas de interface ou utilização de recursos específicos da plataforma e contadores de quedas. Crie o miniaplicativo EEM no modo de configuração:

```
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



Note: Nas plataformas de switching Catalyst (como Cat9k e Cat3k), o comando para exportar a captura é ligeiramente diferente. Para essas plataformas, modifique o comando CLI usado na ação 035:

```
action 035 cli command "monitor capture

      export location bootflash:

       .pcap"
```

O valor limite de taxa no EEM é em segundos e indica quanto tempo deve decorrer antes que o EEM possa ser executado novamente. Neste exemplo, ele é definido como 100000 segundos (27,8 horas) para permitir tempo suficiente para que o administrador de rede identifique que ele concluiu e extraia os arquivos do dispositivo antes que ele seja executado novamente. Se o EEM for executado novamente sozinho após esse período de limite de taxa, nenhum novo dado de captura de pacotes será coletado, pois o EPC deve ser iniciado manualmente. No entanto, as novas saídas do comando show são anexadas aos arquivos de texto.

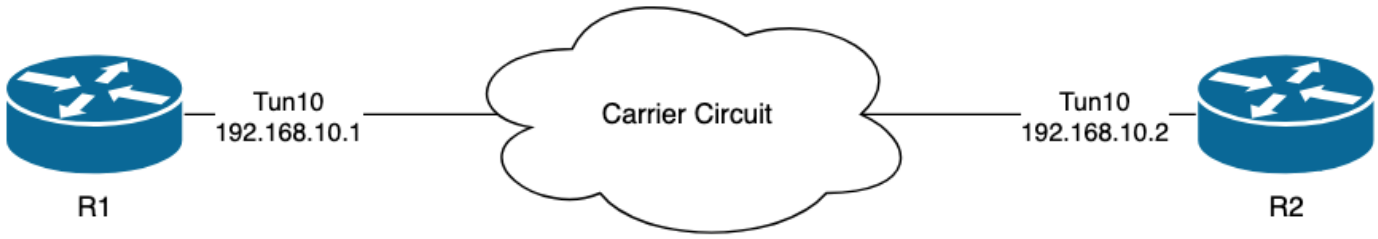
O EEM pode ser modificado conforme necessário para reunir informações de descarte de pacotes específicas da plataforma e obter a funcionalidade adicional necessária para seu cenário.

Identificar e Solucionar Problemas de Flaps de Protocolo de Roteamento Intermitente

Exemplo - EIGRP

Todos os temporizadores são definidos como o padrão neste exemplo (saudações de 5 segundos, tempo de espera de 15 segundos).

Topologia



Os logs em R1 indicam que houve oscilações de EIGRP intermitentes que ocorreram com várias horas de distância um do outro:

```
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: Interfa
*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
```

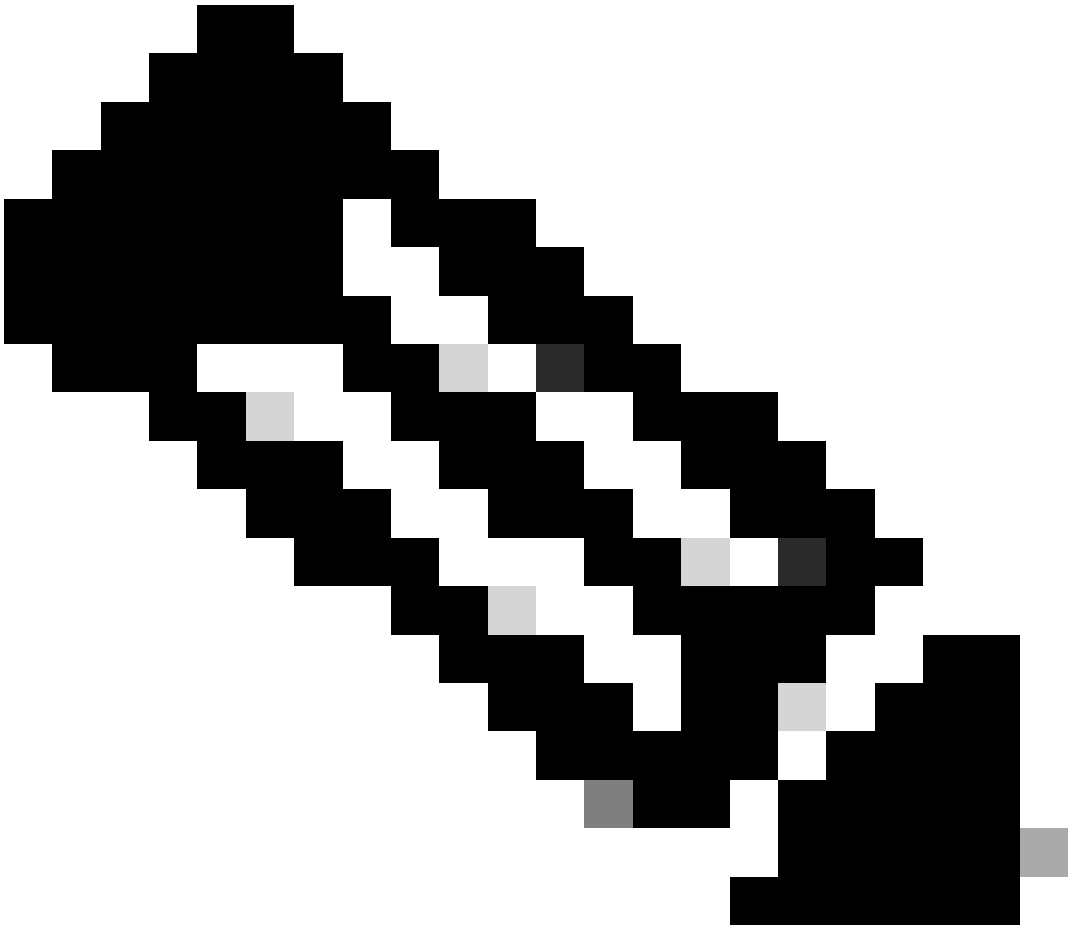
A perda de pacotes pode ocorrer em ambas as direções; o tempo de espera expirado indica que

esse dispositivo não recebeu ou processou uma saudação do peer dentro do tempo de espera, e a interface PEER-TERMINATION recebida indica que o peer encerrou a adjacência porque não recebeu ou processou uma saudação dentro do tempo de espera.

Configuração

1. Configure a ACL com os endereços IP da interface de túnel, já que estes são os endereços IP origem das mensagens 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
```



Note: As configurações mostradas são de R1. O mesmo é feito em R2 para as interfaces

---

relevantes e com nomes de arquivo modificados para o EEM. Se for necessária uma especificidade adicional, configure a ACL com o endereço multicast 224.0.0.10 do EIGRP como o endereço IP destino para capturar saudações.

2. Crie o EPC e associe-o à interface e à ACL:

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

3. Inicie o EPC e confirme se os pacotes foram capturados em ambas as direções:

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

4. Configure o 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. Aguarde até que ocorra a próxima oscilação e copie os arquivos do bootflash através do método de transferência preferido para análise:

```
R1#show logging
```

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

- O buffer de registro no roteador indica que houve uma oscilação de EIGRP e que os arquivos foram salvos pelo EEM.

Análise

Nesse ponto, correlacione o tempo do flap encontrado no buffer de registro com as capturas de pacotes que foram coletadas para determinar se os pacotes de hello foram enviados e recebidos em ambas as extremidades quando o flap ocorreu. Como a interface PEER-TERMINATION recebida foi vista em R1, isso significa que R2 deve ter detectado saudações perdidas e, portanto, o tempo de espera expirou, que é o que é visto no arquivo de log:

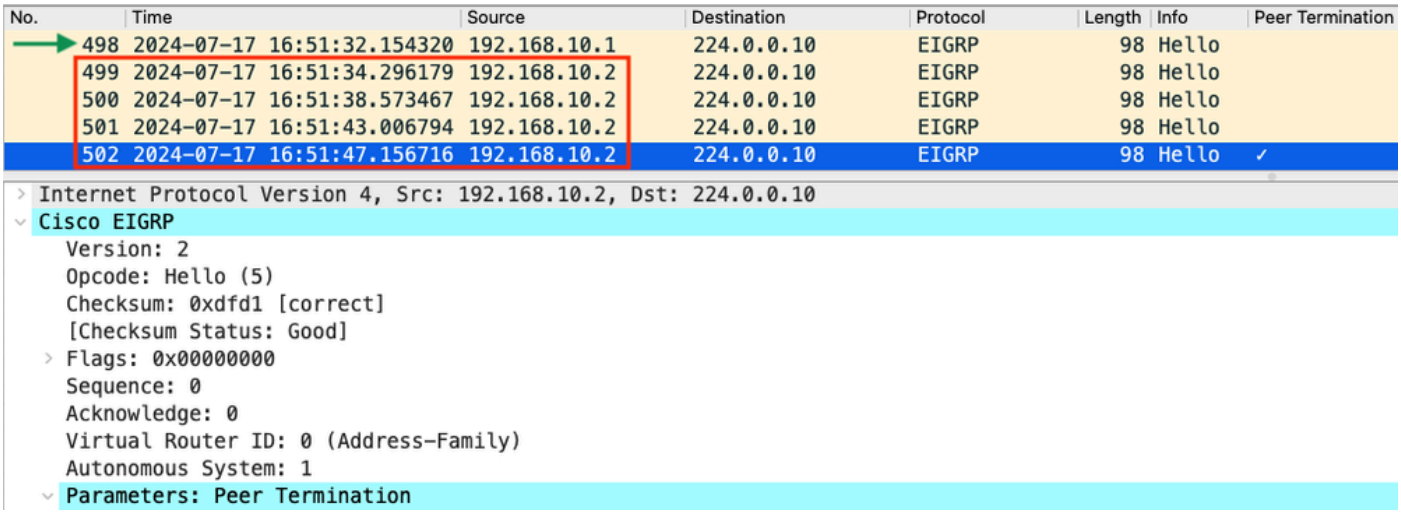
```
*Jul 17 16:51:47.156: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is down: holdin
*Jul 17 16:51:51.870: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.168.10.1 (Tunnel10) is up: new adja
```

Como R2 detectou que o tempo de espera expirou, confirme se houve saudações enviadas por R1 nos 15 segundos antes da oscilação na captura coletada em 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	✓

- A captura mostra saudações de 192.168.10.1 (R1) e 192.168.10.2 (R2) nos 15 segundos anteriores ao pacote hello PEER-TERMINATION que R2 envia às 16:51:47 (pacote 513).
- Especificamente, os pacotes 503, 505, 508 e 511 (indicados pelas setas verdes) foram todos pacotes de hello enviados por R1 nesse período.

A próxima etapa é confirmar se todas as saudações enviadas por R1 foram recebidas por R2 no momento, portanto, a captura coletada de R2 deve ser verificada:



- A captura mostra que o último hello recebido de 192.168.10.1 (R1) foi às 16:51:32 (indicado pela seta verde). Depois disso, os próximos 15 segundos mostram apenas mensagens hello enviadas por R2 (indicadas pela caixa vermelha). Os pacotes 505, 508 e 511 na captura de R1 não aparecem na captura em R2. Isso faz com que R2 detecte o temporizador de espera expirado e envie o pacote hello PEER-TERMINATION às 16:51:47 (pacote 502).

A conclusão desses dados é que a perda de pacotes está em algum lugar na rede da portadora entre R1 e R2. Nesse caso, a perda foi na direção de R1 para R2. Para investigar mais, a portadora precisa estar envolvida para verificar o caminho para quedas.

OSPF

A mesma lógica pode ser usada para solucionar problemas de oscilações OSPF intermitentes. Esta seção descreve os principais fatores que a diferenciam de outros protocolos de roteamento com relação a temporizadores, filtros de endereço IP e mensagens de registro.

- Os temporizadores padrão são pacotes de hello de 10 segundos e um temporizador dead de 40 segundos. Sempre confirme os temporizadores que estão em uso na sua rede ao solucionar problemas de oscilações de temporizadores inativos expirados.
- Os pacotes Hello são originados dos endereços IP da interface. Se for necessária uma especificidade adicional da ACL, o endereço de destino multicast para saudações do OSPF é 224.0.0.5.
- As mensagens de log nos dispositivos são ligeiramente diferentes. Ao contrário do EIGRP, não há conceito de uma mensagem de terminação de peer com OSPF. Em vez disso, o dispositivo que detecta o temporizador dead expirado registra isso como a razão da oscilação e, em seguida, as saudações que ele envia não contêm mais o ID do roteador do peer, o que faz com que o peer passe para o estado INIT. Quando as saudações são detectadas novamente, a adjacência passa pelo estado FULL. Por exemplo:

O R1 detecta que o temporizador de Dead expirou:

```
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
```

No entanto, R2 mostra apenas as mensagens de log quando o OSPF volta para FULL. Ele não mostra uma mensagem de log quando o estado é alterado para INIT:

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

Para disparar o EEM em ambos os dispositivos, use "%OSPF-5-ADJCHG" como padrão de syslog. Isso garante que o EEM seja acionado em ambos os dispositivos, desde que tenha sido desativado e reativado. O valor de limite de taxa configurado garante que ele não seja disparado duas vezes em um curto período quando vários logs com essa cadeia de caracteres são vistos. O segredo é confirmar se as saudações são enviadas e recebidas nas capturas de pacotes em ambos os lados.

BGP

A mesma lógica pode ser usada para identificar e solucionar problemas de oscilações de BGP intermitentes. Esta seção descreve os principais fatores que a diferenciam de outros protocolos de roteamento com relação a temporizadores, filtros de endereço IP e mensagens de registro.

- Os temporizadores padrão são manutenções de atividades de 60 segundos e um tempo de espera de 180 segundos. Sempre confirme os temporizadores que estão em uso na rede ao solucionar problemas de oscilações de tempo de espera expirado.
- Os pacotes de manutenção de atividade são enviados em unicast entre os endereços IP vizinhos para a porta de destino 179 do TCP. Se for necessária uma especificidade adicional da ACL, permita o tráfego TCP dos endereços IP de origem para a porta 179 do TCP de destino.
- As mensagens de log para o BGP parecem semelhantes em ambos os dispositivos, mas o dispositivo que detecta o tempo de espera expira mostra que enviou a notificação ao vizinho, enquanto o outro indica que recebeu a mensagem de notificação. Por exemplo:

O R1 detecta o tempo de espera expirado e envia a notificação ao 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 recebe a notificação de R1 porque R1 detectou que o tempo de espera expirou:

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

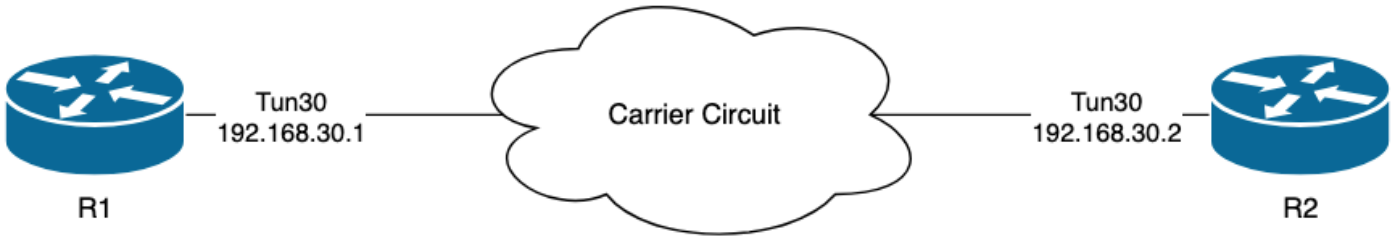
Para disparar o EEM para um flap BGP, use "%BGP_SESSION-5-ADJCHANGE" como o padrão de syslog. Qualquer uma das outras mensagens do syslog "%BGP" que também são registradas após o flap também pode ser usada para disparar o EEM.

Identificar e solucionar problemas de oscilações intermitentes de BFD

A mesma metodologia pode ser aplicada para solucionar problemas de flaps de BFD intermitentes, com algumas diferenças mínimas a serem aplicadas à análise. Esta seção aborda algumas funcionalidades básicas do BFD e fornece um exemplo de como usar o EEM e o EPC para solucionar problemas. Para obter informações mais detalhadas sobre Troubleshooting de BFD, consulte Troubleshooting de Detecção de Encaminhamento Bidirecional no Cisco IOS XE.

Neste exemplo, os temporizadores BFD são definidos como 300 ms com um multiplicador de 3, o que significa que os ecos são enviados a cada 300 ms, e uma falha de eco é detectada quando 3 pacotes de eco em uma linha não são retornados (igual a um tempo de espera de 900 ms).

Topologia



Exemplo - Modo de eco BFD

No modo de eco BFD (o modo padrão), os pacotes de eco BFD são enviados com o IP da interface local como origem e destino. Isso permite que o vizinho processe o pacote no plano de dados e o retorne ao dispositivo de origem. Cada eco BFD é enviado com um ID de eco no cabeçalho da Mensagem de Eco BFD. Eles podem ser usados para determinar se um pacote de eco BFD enviado foi recebido de volta, pois deve haver duas ocorrências de qualquer pacote de eco BFD se ele foi realmente retornado pelo vizinho. Os pacotes de controle BFD, que são usados para controlar o estado da sessão BFD, são enviados unicast entre os endereços IP da interface.

Os logs de R1 indicam que a adjacência BFD foi desativada várias vezes devido a FALHA DE ECO, o que significa que, durante esses intervalos, R1 não recebeu nem processou 3 de seus

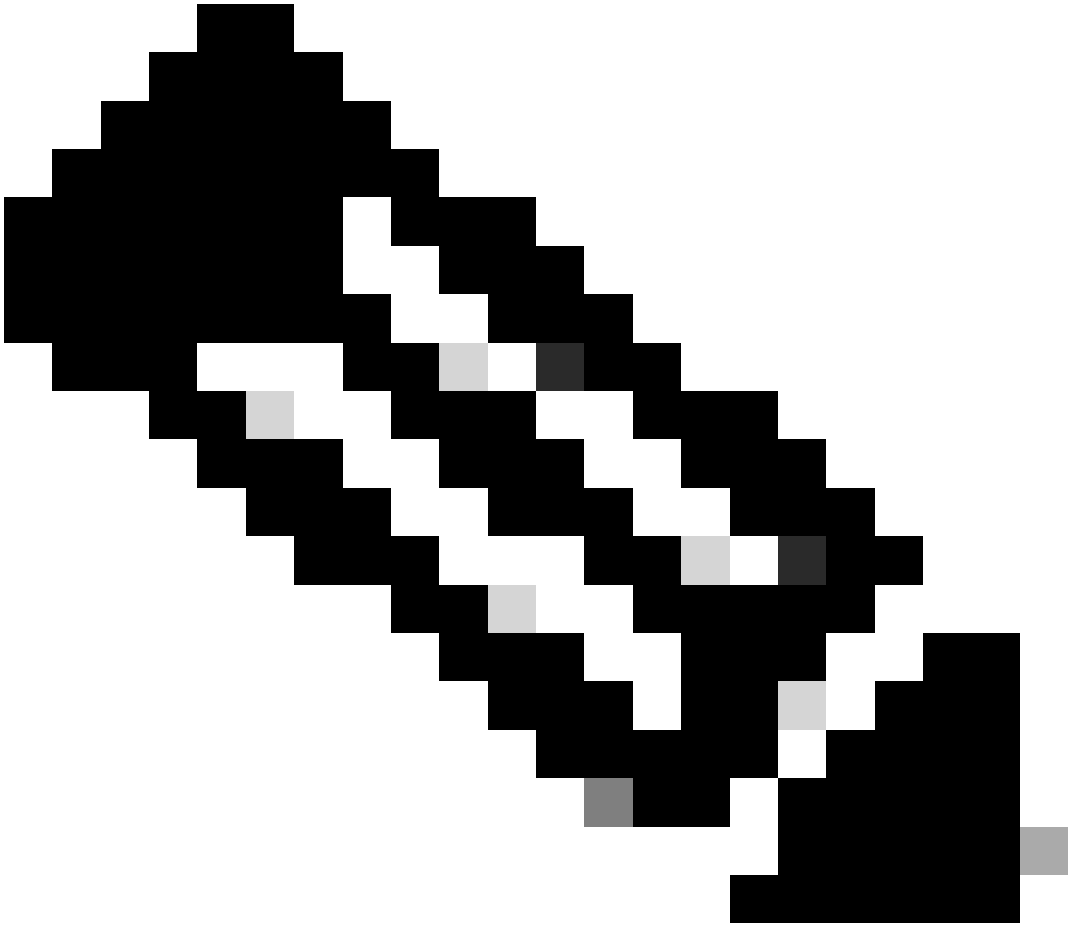
próprios pacotes de eco de volta de R2.

```
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
```

Configuração

1. Configure a ACL com os endereços IP da interface de túnel, já que estes são os endereços IP origem dos pacotes de eco BFD e dos pacotes de controle:

```
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
```



Note: As configurações mostradas são de R1. O mesmo é feito em R2 para as interfaces relevantes e com nomes de arquivo modificados para o EEM. Se for necessária uma especificidade adicional, configure a ACL para UDP com as portas de destino 3785 (pacotes de eco) e 3784 (pacotes de controle).

2. Crie o EPC e associe-o à interface e à ACL:

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

3. Inicie o EPC e confirme se os pacotes foram capturados em ambas as direções:

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

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

4. Configure o 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. Aguarde até que ocorra a próxima oscilação e copie os arquivos do bootflash através do método de transferência preferido para análise:

```
R1#show logging

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

- O buffer de registro indica que houve uma oscilação de BFD às 19:09:47, e os arquivos foram salvos pelo EEM.

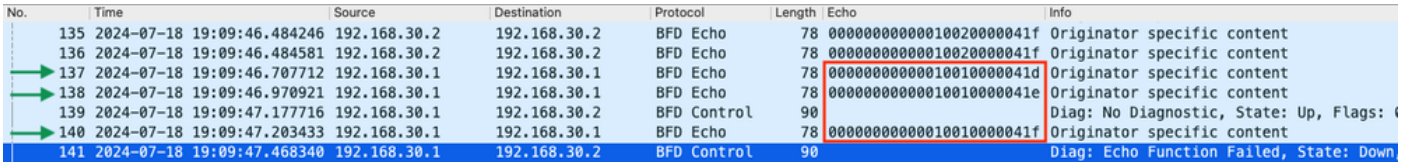
Análise

Nesse ponto, correlacione o tempo do flap encontrado no buffer de registro com as capturas de

pacotes que foram coletadas para determinar se os ecos BFD foram enviados e recebidos em ambas as extremidades quando o problema ocorreu. Como a razão da oscilação em R1 é FALHA de ECO, isso significa que ele também teria enviado um pacote de controle para R2 para encerrar a sessão BFD, e isso é refletido no arquivo de log coletado de R2, onde a razão da desativação do BFD RX DOWN é vista:

```
*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
```

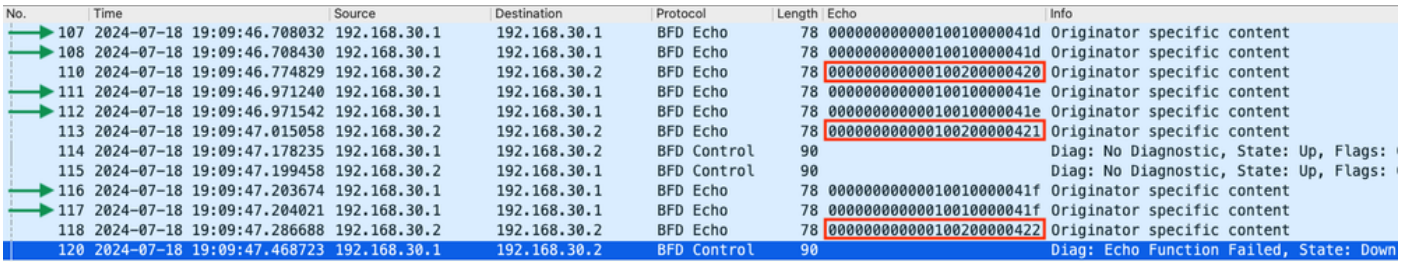
Como R1 detectou uma FALHA de ECO, verifique a captura de pacote coletada em R1 para ver se ele enviou e recebeu ecos BFD nos 900 ms antes da oscilação.



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

- A captura mostra que R1 enviou ativamente pacotes de eco BFD até o momento da oscilação, mas eles não foram retornados por R2, portanto R1 envia um pacote de controle para encerrar a sessão em 19:09:47.468.
- Isso é evidente pelo fato de que os pacotes 137, 138 e 140 (indicados pelas setas verdes) são vistos apenas uma vez na captura, que pode ser determinada a partir das IDs de eco BFD (na caixa vermelha). Se os ecos tivessem sido devolvidos, haveria uma segunda cópia de cada um desses pacotes com o mesmo ID de eco BFD. O campo IP Identification (Identificação de IP) no cabeçalho IP (não mostrado aqui) também pode ser usado para verificar isso.
- Essa captura também mostra que nenhum eco BFD foi recebido de R2 após o pacote 136, que é outra indicação de perda de pacote na direção de R2 para R1.

A próxima etapa é confirmar se todos os pacotes de eco BFD enviados por R1 foram recebidos e retornados por R2, portanto, a captura coletada de R2 deve ser verificada:



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

- Essa captura mostra que todos os ecos BFD enviados por R1 foram recebidos e retornados por R2 (indicados com setas verdes); Os pacotes 107 e 108 são o mesmo eco BFD, os pacotes 111 e 112 são o mesmo eco BFD e os pacotes 116 e 117 são o mesmo eco BFD.
- Essa captura também mostra que R2 enviou ativamente pacotes de eco (indicados com

caixas vermelhas) que não são vistos na captura em R1, o que indica ainda mais a perda de pacotes entre os dispositivos na direção de R2 para R1.

A conclusão desses dados é que a perda de pacotes está em algum lugar na rede da portadora entre R1 e R2, e todas as evidências nesse ponto indicam que a direção da perda é de R2 para R1. Para investigar mais, a portadora precisa estar envolvida para verificar o caminho para quedas.

Modo assíncrono de BFD

O mesmo método pode ser aplicado quando o modo assíncrono BFD está em uso (função de eco desativada), e a configuração do EEM e do EPC pode ser mantida a mesma. A diferença no modo assíncrono é que os dispositivos enviam pacotes de controle BFD unicast uns aos outros como keepalives, análogo a uma adjacência típica de protocolo de roteamento. Isso significa que somente os pacotes da porta UDP 3784 são enviados. Neste cenário, o BFD permanece no estado ativado enquanto um pacote BFD é recebido do vizinho dentro do intervalo necessário. Quando isso não acontece, o motivo da falha é DETECT TIMER EXPIRED e o roteador envia um pacote de controle ao peer para desativar a sessão.

Para analisar as capturas no dispositivo que detectou a falha, procure os pacotes BFD unicast recebidos do peer durante o tempo que antecedeu o flap. Por exemplo, se o intervalo de TX for definido como 300 ms com um multiplicador de 3, então se não houver pacotes BFD recebidos nos 900 ms anteriores ao flap, isso indica perda potencial de pacotes. Na captura obtida do vizinho por meio do EEM, verifique essa mesma janela de tempo; se os pacotes foram enviados durante esse tempo, ele confirma que há perda em algum lugar entre os dispositivos.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.