

# Identificar e Solucionar Problemas de Detecção de Encaminhamento Bidirecional no Cisco IOS XE

## Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Componentes Utilizados](#)
- [Visão geral do BFD](#)
- [Modos de operação da BFD](#)
- [Solucionar problemas de BFD](#)
- [BFD para baixo](#)
- [Flaps de vizinhos BFD](#)
- [Flaps de vizinhos devido à perda de pacotes](#)
- [Flaps de Vizinhos Devido a Parâmetros Definidos Muito Baixos](#)
- [O BFD não falha quando o modo estrito não está configurado](#)
- [Comandos show úteis](#)
- [Mostrar detalhes do vizinho BFD](#)
- [Mostrar resumo de BFD](#)
- [Mostrar quedas de BFD](#)
- [Mostrar histórico de vizinhos BFD](#)
- [Informações Relacionadas](#)

## Introduction

Este documento descreve como solucionar problemas com a detecção de encaminhamento bidirecional (BFD) no Cisco IOS® XE.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não é restrito a versões de software ou hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

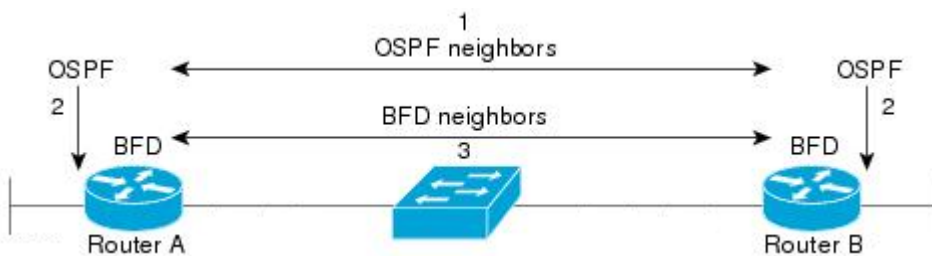
## Visão geral do BFD

A Detecção de Encaminhamento Bidirecional (BFD - Bidirectional Forwarding Detection) é um protocolo de detecção projetado para fornecer tempos rápidos de detecção de falhas de caminho de encaminhamento para todos os tipos de mídia, encapsulamentos, topologias e protocolos de roteamento. Além da detecção

rápida de falhas de caminho de encaminhamento, o BFD oferece um método consistente de detecção de falhas para administradores de rede. Como o administrador de rede pode usar o BFD para detectar falhas de caminho de encaminhamento em uma taxa uniforme, em vez de taxas variáveis para diferentes mecanismos de saudação de protocolo de roteamento, os perfis e planos de rede são mais fáceis e o tempo de reconvergência é consistente e previsível.

Um par de sistemas transmite pacotes BFD periodicamente sobre cada caminho entre os dois sistemas e, se um sistema interrompe o recebimento de pacotes BFD por tempo suficiente, presume-se que algum componente nesse caminho bidirecional específico para o sistema vizinho falhou. Em algumas condições, os sistemas podem negociar o não envio de pacotes BFD periódicos para reduzir a sobrecarga. A redução do número e da frequência de atualizações pode, no entanto, afetar a sensibilidade da BFD.

A imagem mostra o estabelecimento de BFD em uma rede simples com dois roteadores configurados para OSPF e BFD. Quando o OSPF descobre um vizinho (1), ele envia uma solicitação ao processo BFD local para iniciar uma sessão de vizinho BFD com o roteador vizinho OSPF (2). A sessão do vizinho BFD com o roteador vizinho OSPF é estabelecida (3). A mesma progressão é usada com outros protocolos de roteamento quando o BFD está ativado.



## Modos de operação da BFD

**Modo de eco BFD** - O modo de eco é ativado por padrão e é executado com BFD assíncrono. Ele pode ser desativado em um lado para executar com assimetria, ou executar em ambos os lados de uma vizinhança. Os pacotes de eco são enviados pelo mecanismo de encaminhamento e encaminhados de volta ao longo do mesmo caminho. Um pacote de eco é definido com um endereço origem e destino da própria interface e uma porta UDP destino de 3785. O vizinho reflete o eco de volta para o originador, o que minimiza sua carga de processo do pacote e aumenta a sensibilidade possível do BFD. Em geral, os ecos não são encaminhados para o plano de controle do vizinho, a fim de reduzir atrasos e carga de CPU.

**Modo assíncrono BFD** - O modo assíncrono rastreia a disponibilidade do vizinho pela troca de pacotes de controle entre os dois vizinhos, o que requer a configuração estática do BFD em ambos os lados.

## Solucionar problemas de BFD

### BFD para baixo

As mensagens de log de inatividade do BFD são cruciais para o isolamento de uma sessão inativa. Há várias causas diferentes que podem ser vistas:

**TEMPORIZADOR DE DETECÇÃO EXPIRADO** - O roteador não recebe mais tráfego de manutenção de atividade BFD e expira.

**FALHA DE ECO** - O roteador não recebe mais seus ecos BFD do outro lado.

**RX DOWN** - O roteador recebe notificação de seu vizinho de que foi desativado.

## **RX ADMINDOWN - O BFD foi desabilitado no dispositivo vizinho.**

```
*Mar 31 19:35:51.809: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4111 handle:3,is going Down Re
*Mar 31 19:35:51.811: %BGP-5-NBR_RESET: Neighbor 10.1.1.2 reset (BFD adjacency down)
*Mar 31 19:35:51.812: %BGP-5-ADJCHANGE: neighbor 10.1.1.2 Down BFD adjacency down
*Mar 31 19:35:51.813: %BGP_SESSION-5-ADJCHANGE: neighbor 10.1.1.2 IPv4 Unicast topology base removed fro
*Mar 31 19:35:51.813: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, ld:4111 neigh proc:
*Mar 31 19:36:33.377: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4113 handle:1,is going Down Re
*Mar 31 19:36:33.380: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, ld:4113 neigh proc:
*Mar 31 19:36:33.381: %OSPF-5-ADJCHG: Process 1, Nbr 10.30.30.30 on GigabitEthernet3 from FULL to DOWN,
*Mar 31 19:35:59.483: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4110 handle:2,is going Down Re
*Mar 31 19:36:02.220: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 10.1.1.2 proc:BGP,
```

Após a confirmação do motivo pelo qual a sessão BFD foi interrompida e o direcionamento do problema, você pode começar a isolar as possíveis causas:

- Falha de mídia unidirecional
- Alterações de configuração
- BFD bloqueado no caminho
- Falhas de CPU ou encaminhamento em um dispositivo

## **Flaps de vizinhos BFD**

### **Flaps de vizinhos devido à perda de pacotes**

Os flaps frequentes de BFD podem geralmente ser causados por um link com perdas que faz com que os pacotes de controle de BFD ou ecos sejam perdidos. Se houver vários motivos diferentes de inatividade da sessão, isso seria mais indicativo de perda de pacotes.

```
*Apr 4 17:18:25.931: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going Down Re
*Apr 4 17:18:25.933: %BGP-5-NBR_RESET: Neighbor 10.1.1.2 reset (BFD adjacency down)
*Apr 4 17:18:25.934: %BGP-5-ADJCHANGE: neighbor 10.1.1.2 Down BFD adjacency down
*Apr 4 17:18:25.934: %BGP_SESSION-5-ADJCHANGE: neighbor 10.1.1.2 IPv4 Unicast topology base removed fro
*Apr 4 17:18:25.934: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, ld:4097 neigh proc:
*Apr 4 17:18:27.828: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4097 handle:1 is going UP
*Apr 4 17:18:32.304: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 10.1.1.2 proc:BGP,
*Apr 4 17:18:32.304: %BGP-5-ADJCHANGE: neighbor 10.1.1.2 Up
*Apr 4 17:18:34.005: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4100 handle:1 is going UP
*Apr 4 17:18:34.418: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4100 handle:1,is going Down Re
*Apr 4 17:18:34.420: %BGP-5-NBR_RESET: Neighbor 10.1.1.2 reset (BFD adjacency down)
*Apr 4 17:18:34.422: %BGP-5-ADJCHANGE: neighbor 10.1.1.2 Down BFD adjacency down
*Apr 4 17:18:34.422: %BGP_SESSION-5-ADJCHANGE: neighbor 10.1.1.2 IPv4 Unicast topology base removed fro
*Apr 4 17:18:34.422: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, ld:4100 neigh proc:
*Apr 4 17:18:42.529: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 10.1.1.2 proc:BGP,
*Apr 4 17:18:42.529: %BGP-5-ADJCHANGE: neighbor 10.1.1.2 Up
*Apr 4 17:18:43.173: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:4100 handle:1 is going UP
```

Para isolar a perda de pacotes, é útil fazer uma captura de pacote incorporada da interface envolvida. Os comandos básicos são:

```
monitor capture <name> interface <interface> <in|out|both>  
monitor capture <name> match ipv4 protocol udp any any eq <3784|3785>
```

Você também pode filtrar com uma lista de acesso para corresponder tanto o controle BFD quanto os pacotes de eco.

```
config t  
ip access-list extended <ACLname>  
permit udp any any eq 3784  
permit udp any any eq 3785  
fin  
monitor capture <name> interface <interface> <in|out|both>  
monitor capture <name> access-list <ACLname>
```

Neste exemplo, as capturas na interface de entrada mostram que os pacotes de controle BFD são recebidos consistentemente, mas os ecos são intermitentes. Dos timestamps de 5 segundos a 15 segundos, não há pacotes de eco para o sistema local 10.1.1.1 visto como retornado. Isso indicaria que há perda do roteador BFD em direção ao seu vizinho.

```
BFDrouter#show run | section access-list extended  
ip access-list extended BFDcap  
 10 permit udp any any eq 3784  
 20 permit udp any any eq 3785  
BFDrouter#mon cap BFD interface Gi1 in  
BFDrouter#mon cap BFD access-list BFDcap  
BFDrouter#mon cap BFD start  
Started capture point : BFD  
BFDrouter#mon cap BFD stop  
Stopped capture point : BFD  
BFDrouter#show mon cap BFD buffer brief
```

#	size	timestamp	source	destination	dscp	protocol
...						
212	54	4.694016	10.1.1.1	-> 10.1.1.1	48 CS6	UDP
213	54	4.733016	10.1.1.2	-> 10.1.1.2	48 CS6	UDP
214	54	4.735014	10.1.1.1	-> 10.1.1.1	48 CS6	UDP
215	54	4.789012	10.1.1.1	-> 10.1.1.1	48 CS6	UDP
216	54	4.808009	10.1.1.2	-> 10.1.1.2	48 CS6	UDP
217	54	4.838006	10.1.1.1	-> 10.1.1.1	48 CS6	UDP
218	66	4.857002	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
219	66	5.712021	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
220	66	6.593963	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
221	66	7.570970	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
222	66	8.568971	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
223	66	9.354977	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
224	66	10.250979	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
225	66	11.154991	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
226	66	11.950000	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
227	66	12.925007	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
228	66	13.687013	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
229	66	14.552965	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
230	66	15.537967	10.1.1.2	-> 10.1.1.1	48 CS6	UDP
231	66	15.641965	10.1.1.2	-> 10.1.1.1	48 CS6	UDP

232	66	15.656964	10.1.1.2	->	10.1.1.1	48	CS6	UDP
233	54	15.683015	10.1.1.1	->	10.1.1.1	48	CS6	UDP
234	54	15.702011	10.1.1.2	->	10.1.1.2	48	CS6	UDP
235	54	15.731017	10.1.1.1	->	10.1.1.1	48	CS6	UDP
236	54	15.752012	10.1.1.2	->	10.1.1.2	48	CS6	UDP

## Flaps de Vizinhos Devido a Parâmetros Definidos Muito Baixos

Em links de velocidade mais baixa, é importante ter em mente os parâmetros BFD apropriados. Os valores de intervalo e de recebimento mínimo são definidos em milissegundos. Se o atraso entre vizinhos estiver dentro ou perto desses valores, os atrasos normais causados pelas condições de tráfego acionam flaps de BFD. Por exemplo, se o atraso fim-a-fim normal entre vizinhos for de 100 ms e o intervalo BFD for definido como o mínimo de 50 ms com um multiplicador de 3, um único pacote BFD perdido disparará um evento de vizinho inativo, pois os próximos dois ainda estão em trânsito.

Você pode validar o atraso para o vizinho através de um ping simples entre os dois endereços IP vizinhos.

Além disso, os temporizadores mínimos suportados variam por plataforma e devem ser confirmados antes da configuração do BFD.

## O BFD não falha quando o modo estrito não está configurado

É importante observar que quando o modo estrito BFD não está ativado, a ausência de uma sessão BFD não impede o estabelecimento do protocolo de roteamento associado.

Isso pode permitir a reconvergência em cenários indesejáveis. No exemplo, o BFD remove com êxito o BGP, mas como a comunicação TCP permanece bem-sucedida, o vizinho volta a ficar ativo.

```
*Mar 31 18:53:08.997: %BDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going Down Re
*Mar 31 18:53:08.999: %BGP-5-NBR_RESET: Neighbor 10.1.1.1 reset (BFD adjacency down)
*Mar 31 18:53:09.000: %BGP-5-ADJCHANGE: neighbor 10.1.1.1 Down BFD adjacency down
*Mar 31 18:53:09.000: %BGP_SESSION-5-ADJCHANGE: neighbor 10.1.1.1 IPv4 Unicast topology base removed fro
BGPpeer#
*Mar 31 18:53:09.000: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, ld:4097 neigh proc:
*Mar 31 18:53:10.044: %SYS-5-CONFIG_I: Configured from console by console
BGPpeer#
*Mar 31 18:53:15.245: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 10.1.1.1 proc:BGP,
*Mar 31 18:53:15.245: %BGP-5-ADJCHANGE: neighbor 10.1.1.1 Up
BGPpeer#show bfd neighbor
```

IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
10.1.1.1	4097/0	Down	Down	Gi1

Como o BGP está ativado antes da vizinhança de BFD, a rede converge novamente. Se o BFD permanecer inativo, a única maneira de desativar o vizinho é quando o temporizador de espera de dois minutos expira, o que atrasa o failover.

```
*Mar 31 18:59:01.539: %BGP-3-NOTIFICATION: sent to neighbor 10.1.1.1 4/0 (hold time expired) 0 bytes
*Mar 31 18:59:01.540: %BGP-5-NBR_RESET: Neighbor 10.1.1.1 reset (BGP Notification sent)
*Mar 31 18:59:01.541: %BGP-5-ADJCHANGE: neighbor 10.1.1.1 Down BGP Notification sent
```

\*Mar 31 18:59:01.541: %BGP\_SESSION-5-ADJCHANGE: neighbor 10.1.1.1 IPv4 Unicast topology base removed from  
\*Mar 31 18:59:01.541: %BFD-6-BFD\_SESS\_DESTROYED: BFD-SYSLOG: bfd\_session\_destroyed, ld:4097 neigh proc:

## Comandos show úteis

### Mostrar detalhes do vizinho BFD

Esse comando fornece detalhes dos vizinhos BFD configurados conforme descrito abaixo. Isso inclui todos os vizinhos, independentemente do estado atual.

```
BFDrouter#show bfd neighbor details
```

```
IPv4 Sessions
```

NeighAddr	LD/RD	RH/RS	State	Int
10.1.1.2	4104/4097	Up	Up	Gi1

```
Session state is UP and using echo function with 50 ms interval.
```

```
Session Host: Software
```

```
OurAddr: 10.1.1.1
```

```
Handle: 3
```

```
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
```

```
Received MinRxInt: 1000000, Received Multiplier: 3
```

```
Holddown (hits): 0(0), Hello (hits): 1000(36)
```

```
Rx Count: 38, Rx Interval (ms) min/max/avg: 2/1001/827 last: 493 ms ago
```

```
Tx Count: 39, Tx Interval (ms) min/max/avg: 4/988/809 last: 402 ms ago
```

```
Echo Rx Count: 534, Echo Rx Interval (ms) min/max/avg: 23/68/45 last: 26 ms ago
```

```
Echo Tx Count: 534, Echo Tx Interval (ms) min/max/avg: 39/63/45 last: 27 ms ago
```

```
Elapsed time watermarks: 0 0 (last: 0)
```

```
Registered protocols: BGP CEF
```

```
Uptime: 00:00:24
```

```
Last packet: Version: 1
```

```
- Diagnostic: 0
```

```
State bit: Up - Demand bit: 0
```

```
Poll bit: 0 - Final bit: 0
```

```
C bit: 0
```

```
Multiplier: 3 - Length: 24
```

```
My Discr.: 4097 - Your Discr.: 4104
```

```
Min tx interval: 1000000 - Min rx interval: 1000000
```

```
Min Echo interval: 50000
```

```
IPv4 Sessions
```

NeighAddr	LD/RD	RH/RS	State	Int
10.2.2.2	4102/4097	Up	Up	Gi2

```
Session state is UP and using echo function with 50 ms interval.
```

```
Session Host: Software
```

```
OurAddr: 10.2.2.1
```

```
Handle: 2
```

```
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
```

```
Received MinRxInt: 1000000, Received Multiplier: 3
```

```
Holddown (hits): 0(0), Hello (hits): 1000(2637)
```

```
Rx Count: 2639, Rx Interval (ms) min/max/avg: 3/1012/879 last: 10 ms ago
```

```
Tx Count: 2639, Tx Interval (ms) min/max/avg: 2/1006/879 last: 683 ms ago
```

```
Echo Rx Count: 51504, Echo Rx Interval (ms) min/max/avg: 1/98/45 last: 32 ms ago
```

```
Echo Tx Count: 51504, Echo Tx Interval (ms) min/max/avg: 39/98/45 last: 34 ms ago
```

```
Elapsed time watermarks: 0 0 (last: 0)
```

```
Registered protocols: EIGRP CEF
```

```
Uptime: 00:38:37
```

```

Last packet: Version: 1          - Diagnostic: 0
              State bit: Up      - Demand bit: 0
              Poll bit: 0        - Final bit: 0
              C bit: 0
              Multiplier: 3      - Length: 24
              My Discr.: 4097    - Your Discr.: 4102
              Min tx interval: 1000000 - Min rx interval: 1000000
              Min Echo interval: 50000

```

#### IPv4 Sessions

```

NeighAddr          LD/RD          RH/RS          State          Int
10.3.3.2           4100/4097         Up             Up             Gi3

```

Session state is UP and using echo function with 50 ms interval.

Session Host: Software

OurAddr: 10.3.3.1

Handle: 1

Local Diag: 0, Demand mode: 0, Poll bit: 0

MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3

Received MinRxInt: 1000000, Received Multiplier: 3

Holddown (hits): 0(0), Hello (hits): 1000(10120)

Rx Count: 10137, Rx Interval (ms) min/max/avg: 1/2761/878 last: 816 ms ago

Tx Count: 10136, Tx Interval (ms) min/max/avg: 1/2645/877 last: 904 ms ago

Echo Rx Count: 197745, Echo Rx Interval (ms) min/max/avg: 1/4126/45 last: 15 ms ago

Echo Tx Count: 197745, Echo Tx Interval (ms) min/max/avg: 39/4227/45 last: 16 ms ago

Elapsed time watermarks: 0 0 (last: 0)

Registered protocols: CEF OSPF

Uptime: 00:38:39

```

Last packet: Version: 1          - Diagnostic: 0
              State bit: Up      - Demand bit: 0
              Poll bit: 0        - Final bit: 0
              C bit: 0
              Multiplier: 3      - Length: 24
              My Discr.: 4097    - Your Discr.: 4100
              Min tx interval: 1000000 - Min rx interval: 1000000
              Min Echo interval: 50000

```

#### Campos-chave:

Host da sessão	Este campo especifica se a sessão está hospedada no software ou descarregada no hardware. O descarregamento de hardware está disponível em algumas plataformas para evitar a instabilidade do BFD devido ao congestionamento da CPU.
MinTxInt/MinRxInt/Multiplicador	Os valores locais para intervalos mínimos de transmissão e recepção e multiplicador
MinRxInt recebido/Multiplicador recebido	Os valores de par para o intervalo mínimo de recebimento e o multiplicador
Contagem Rx/Tx	Contadores dos pacotes BFD enviados e recebidos
Contagem Rx/Tx De Eco	Contadores para ecos BFD enviados e recebidos
Protocolos registrados	Protocolo de roteamento usado pela sessão BFD
Tempo de atividade	Tempo de atividade da sessão
LD/RD	Discriminador local e Discriminador remoto para a sessão





## Mostrar histórico de vizinhos BFD

Esse comando mostra logs BFD recentes para cada vizinho, juntamente com seu estado atual.

```
BFDrouter# show bfd neighbors history
```

### IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
10.1.1.2	4101/4097	Down	Init	Gi1

#### History information:

```
[Apr 4 15:56:21.346] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:20.527] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:19.552] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:18.776] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:17.823] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:16.816] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:15.886] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:14.920] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:14.023] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:13.060] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:12.183] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:11.389] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:10.600] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:09.603] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:08.750] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:07.808] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:06.825] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:05.877] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
```

### IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
[Apr 4 15:56:04.917]	Event: V1 FSM ld:4101 handle:3 event:RX	DOWN	state:INIT	
[Apr 4 15:56:03.920]	Event: V1 FSM ld:4101 handle:3 event:RX	DOWN	state:INIT	

10.2.2.2	104/4097	Up	Up	Gi2
----------	----------	----	----	-----

#### History information:

```
[Apr 4 15:10:41.820] Event: V1 FSM ld:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.803] Event: V1 FSM ld:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.784] Event: V1 FSM ld:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.770] Event: notify client(CEF) IP:10.2.2.2, ld:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: notify client(EIGRP) IP:10.2.2.2, ld:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: notify client(CEF) IP:10.2.2.2, ld:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: resetting timestamps ld:104 handle:1
[Apr 4 15:10:41.768] Event: V1 FSM ld:104 handle:1 event:RX INIT state:DOWN
[Apr 4 15:10:41.751] Event: V1 FSM ld:104 handle:1 event:Session create state:DOWN
[Apr 4 15:10:41.751]
bfd_session_created, proc:EIGRP, idb:GigabitEthernet2 handle:1 act
```

10.3.3.2	4198/4097	Up	Up	Gi3
----------	-----------	----	----	-----

#### History information:

### IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
[Apr 4 15:26:01.779]	Event: notify client(CEF) IP:10.3.3.2, ld:4198, handle:2, event:UP,			
[Apr 4 15:26:01.779]	Event: notify client(OSPF) IP:10.3.3.2, ld:4198, handle:2, event:UP,			
[Apr 4 15:26:01.778]	Event: V1 FSM ld:4198 handle:2 event:RX	UP	state:UP	
[Apr 4 15:26:01.777]	Event: notify client(OSPF) IP:10.3.3.2, ld:4198, handle:2, event:UP,			
[Apr 4 15:26:01.777]	Event: V1 FSM ld:4198 handle:2 event:RX	INIT	state:DOWN	
[Apr 4 15:26:01.776]	Event: V1 FSM ld:4198 handle:2 event:Session create		state:ADMIN DOWN	
[Apr 4 15:25:59.309]	Event:			

```
bfd_session_destroyed, proc:CEF, handle:2 act
[Apr 4 15:25:59.309] Event: V1 FSM ld:4198 handle:2 event:Session delete state:UP
[Apr 4 15:25:59.308] Event:
bfd_session_destroyed, proc:OSPF, handle:2 act
[Apr 4 15:22:48.912] Event: V1 FSM ld:4198 handle:2 event:RX UP state:UP
[Apr 4 15:22:48.911] Event: notify client(CEF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
[Apr 4 15:22:48.911] Event: notify client(OSPF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
[Apr 4 15:22:48.911] Event: notify client(CEF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
IPv4 Sessions
NeighAddr                LD/RD          RH/RS      State      Int
[Apr 4 15:22:48.911] Event: V1 FSM ld:4198 handle:2 event:RX INIT state:DOWN
[Apr 4 15:22:48.910] Event: V1 FSM ld:4198 handle:2 event:Session create state:DOWN
[Apr 4 15:22:48.909]
bfd_session_created, proc:OSPF, idb:GigabitEthernet3 handle:2 act
```

## Informações Relacionadas

[Referência BFD do Cisco IOS](#)

[Guia de configuração de BFD, Cisco IOS XE 17.x](#)

[IETF RFC 5880 para BFD](#)

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.