

Cisco IOS XEの双方向フォワーディング検出の トラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[BFDの概要](#)

[BFD動作モード](#)

[BFD問題のトラブルシューティング](#)

[BFDダウン](#)

[BFDネイバーフラップ](#)

[パケット損失によるネイバーフラップ](#)

[設定されたパラメータが小さすぎるために発生するネイバーフラップ](#)

[ストリクトモードが設定されていないとBFDがフェールオーバーしない](#)

[便利な show コマンド](#)

[BFDネイバーの詳細の表示](#)

[BFDの概要を表示](#)

[BFDドロップの表示](#)

[BFDネイバー履歴の表示](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco IOS® XEの双方向フォワーディング検出(BFD)に関する問題をトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

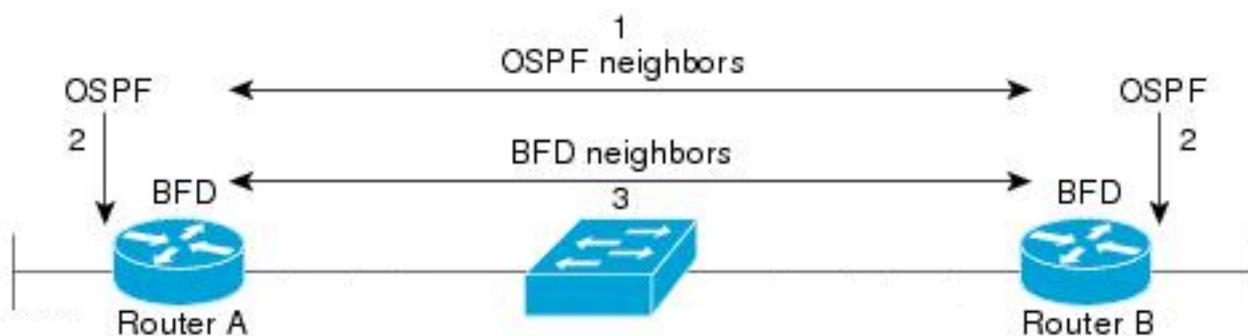
ください。

BFDの概要

双方向フォワーディング検出(BFD)は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルに対して高速なフォワードパス障害検出時間を提供するように設計された検出プロトコルです。BFDは、ファストフォワードパスの障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は、異なるルーティングプロトコルhelloメカニズムの可変レートではなく、均一なレートで転送パスの障害を検出するためにBFDを使用できるため、ネットワークプロファイルと計画が簡単になり、再コンバージェンス時間が一貫して予測可能になります。

一対のシステムが、2つのシステム間の各パスを通じて定期的にBFDパケットを送信します。システムがBFDパケットの受信を十分長く停止した場合は、ネイバーシステムへの特定の双方向パスの一部のコンポーネントに障害が発生したと見なされます。状況によっては、オーバーヘッドを減らすために、システムは定期的なBFDパケットを送信しないようにネゴシエートできます。ただし、アップデートの数と頻度を減らすと、BFDの感度に影響する可能性があります。

次の図は、OSPFとBFD用に設定された2台のルータを使用した単純なネットワークでのBFD確立を示しています。OSPFはネイバー(1)を検出すると、ローカルBFDプロセスに要求を送信して、OSPFネイバールータ(2)とのBFDネイバーセッションを開始します。OSPFネイバールータとのBFDネイバーセッションが確立されます(3)。BFDが有効になっている場合、他のルーティングプロトコルでも同じ処理が行われます。



BFD動作モード

BFDエコモード：エコモードはデフォルトで有効になっており、非同期BFDで実行されます。一方の側でエコモードを無効にして非対称で実行することも、ネイバーシップの両側で実行することもできます。エコパケットは転送エンジンによって送信され、同じパスに沿って転送されます。エコパケットは、インターフェイス自体の送信元アドレスと宛先アドレス、および宛先UDPポート3785を使用して設定されます。ネイバーがエコを発信元に反映するため、パケットのプロセス負荷が最小限に抑えられ、BFDの感度が向上します。一般に、遅延とCPU負荷を軽減するために、エコはネイバーのコントロールプレーンに転送されません。

BFD非同期モード：非同期モードでは、2つのネイバー間で制御パケットが交換されることにより、ネイバーの可用性が追跡されます。このため、両側でBFDをスタティックに設定する必要があります。

BFD問題のトラブルシューティング

BFDダウン

BFDダウンログメッセージは、ダウンセッションを切り分けるために不可欠です。 次のような複数の異なる原因が考えられます。

DETECT TIMER EXPIRED – ルータはBFDキープアライブトラフィックを受信しなくなり、タイムアウトします。

ECHO FAILURE – ルータはもう相手側からのBFDエコーを受信しません。

RX DOWN : ルータは、ダウンしたという通知をネイバーから受信します。

RX ADMINDOWN : ネイバーデバイスでBFDが無効になっています。

```
*Mar 31 19:35:51.809: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session 1d:4111 handle:3,is going Down R
*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 fr
*Mar 31 19:35:51.813: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, 1d:4111 neigh proc
```

```
*Mar 31 19:36:33.377: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session 1d:4113 handle:1,is going Down R
*Mar 31 19:36:33.380: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, 1d: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 1d:4110 handle:2,is going Down R
*Mar 31 19:36:02.220: %BFD-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh 10.1.1.2 proc:BGP
```

BFDセッションが切断された理由と問題の方向性を確認した後、考えられる原因の切り分けを開始できます。

- 片方向メディア障害
- 設定変更
- パスでブロックされたBFD
- 1台のデバイス上のCPUまたは転送の障害

BFDネイバーフラップ

パケット損失によるネイバーフラップ

BFDのフラップが頻繁に発生する原因は、BFD制御パケットやエコーが失われる原因となるリンクの損失である可能性があります。 セッションダウンの原因が複数存在する場合は、パケット損失の可能性が高くなります。

```

*Apr 4 17:18:25.931: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session Id:4097 handle:1,is going Down R
*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 fr
*Apr 4 17:18:25.934: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, Id:4097 neigh proc
*Apr 4 17:18:27.828: %BFDFSM-6-BFD_SESS_UP: BFD-SYSLOG: BFD session Id: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 Id:4100 handle:1 is going UP
*Apr 4 17:18:34.418: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session Id:4100 handle:1,is going Down R
*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 fr
*Apr 4 17:18:34.422: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, Id: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 Id:4100 handle:1 is going UP

```

パケット損失を切り分けるには、関連するインターフェイスの組み込みパケットキャプチャを取得すると役立ちます。

基本的なコマンドを次に示します。

```

monitor capture <名前> interface <インターフェイス> <in|out|both>
monitor capture <名前> match ipv4 protocol udp any eq <3784|3785>

```

アクセスリストを使用してフィルタリングを行い、BFD制御パケットとエコーパケットの両方に一致させることもできます。

```

config t
ip access-list extended <ACL名>
permit udp any any eq 3784 ( 任意のudpを許可 )
permit udp any any eq 3785
最後
monitor capture <名前> interface <インターフェイス> <in|out|both>
monitor capture <名前> access-list <ACLname>

```

この例では、着信インターフェイスのキャプチャにより、BFD制御パケットが一貫して受信されているにもかかわらず、エコーが断続的に発生することがわかります。5秒から15秒のタイムスタンプでは、ローカルシステム10.1.1.1に対するエコーパケットは返されません。これは、BFDルータからそのネイバーに向かって損失があることを示します。

```

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

設定されたパラメータが小さすぎるために発生するネイバーフラップ

低速リンクでは、適切なBFDパラメータに注意することが重要です。インターバルと最小受信値はミリ秒単位で設定されます。ネイバー間の遅延がこの値に近い場合、トラフィック状態による通常の遅延によってBFDフラップがトリガーされます。たとえば、ネイバー間の通常のエンドツーエンド遅延が100ミリ秒で、BFD間隔が乗算器3で50ミリ秒以上に設定されている場合、次の2つのパケットがまだ転送中であるときに、1つのBFDパケットが失われただけでネイバーダウンイベントがトリガーされます。

2つのネイバーIPアドレス間でpingを発行するだけで、ネイバーへの遅延を検証できます。

また、サポートされる最小タイマーはプラットフォームごとに異なるため、BFDを設定する前に確認する必要があります。

ストリクトモードが設定されていないとBFDがフェールオーバーしない

BFDストリクトモードが有効でない場合、BFDセッションがないと、関連するルーティングプロトコルの確立が妨げられないことに注意してください。

これにより、望ましくないシナリオでの再コンバージェンスが可能になる場合があります。この例では、BFDが正常にBGPを切断していますが、TCP通信は正常に維持されているため、ネイバーは復帰します。

```

*Mar 31 18:53:08.997: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session 1d:4097 handle:1, is going Down R
*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 fr
BGPpeer#
*Mar 31 18:53:09.000: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, 1d: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

BGPはBFDネイバーシップよりも先にアップしているため、ネットワークは再収束します。BFDがダウン状態のままである場合、ネイバーをダウンさせる唯一の方法は、2分間のホールドタイムが時間切れになり、フェールオーバーが遅延することです。

```

*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 fr
*Mar 31 18:59:01.541: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, 1d:4097 neigh proc

```

便利な show コマンド

BFDネイバーの詳細の表示

このコマンドは、次に示すように、設定されているBFDネイバーの詳細を提供します。これには、現在の状態から独立したすべてのネイバーが含まれます。

```
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	

キーフィールド :

セッションホスト	このフィールドは、セッションをソフトウェアでホストするか、ハードウェアにオフロードするかを指定します。一部のプラットフォームでは、CPUの輻輳によるBFDの不安定性を防ぐために、ハードウェアオフロードを使用できます。
MinTxInt/MinRxInt/乗数	最小送受信間隔および乗数のローカル値。
受信MinRxInt/受信乗数	最小受信間隔および乗数のピア値。
Rx/Txカウント	送受信されたBFDパケットのカウント。
エコーRx/Txカウント	送受信BFDエコーのカウント。
登録済みプロトコル	BFDセッションで使用されるルーティングプロトコル。
Uptime	セッションアップタイム
保持/rd	セッションのローカル識別子とリモート識別子。
相対湿度/相対湿度	リモートのヒアリングおよびリモート状態

BFDの概要を表示

show bfd summary コマンドを使用すると、アクティブなクライアントプロトコル、IPプロトコルセッション、またはハードウェアとソフトウェアでホストされたBFDセッションを複数の出力ですばやく表示できます。この情報は、完全な詳細の出力が長く扱いにくい場合に役立ちます。

```
BFDrouter#show bfd summary client
```

Client	Session	Up	Down
BGP	1	1	0
EIGRP	1	1	0
OSPF	1	1	0
CEF	3	3	0
Total	3	3	0

```
BFDrouter#show bfd summary session
```

Protocol	Session	Up	Down
IPV4	3	3	0
Total	3	3	0

```
BFDrouter#show bfd summary host
```

Host	Session	Up	Down
Software	3	3	0
Hardware	0	0	0
Total	3	3	0

BFDドロップの表示

このコマンドは、ローカルデバイスでドロップされたBFDパケットとその理由を表示します。ローカルドロップが増加すると、セッションのフラップが発生する可能性があります。

```
BFDrouter#show bfd drops
```

```
BFD Drop Statistics
```

	IPV4	IPV6	IPV4-M	IPV6-M	MPLS_PW	MPLS_TP_LSP	MPLS_TE_GAL_LSP	MPLS_TE_SR
Invalid TTL	0	0	0	0	0	0	0	0
BFD Not Configured	0	0	0	0	0	0	0	0
No BFD Adjacency	12	0	0	0	0	0	0	0
Invalid Header Bits	0	0	0	0	0	0	0	0
Invalid Discriminator	3	0	0	0	0	0	0	0
Session AdminDown	2222	0	0	0	0	0	0	0
Authen invalid BFD ver	0	0	0	0	0	0	0	0
Authen invalid len	0	0	0	0	0	0	0	0
Authen invalid seq	0	0	0	0	0	0	0	0
Authen failed	0	0	0	0	0	0	0	0
Dampenend Down	0	0	0	0	0	0	0	0
SBFD Srcip Invalid	0	0	0	0	0	0	0	0
Invalid SBFD_SPORT	0	0	0	0	0	0	0	0
Source Port not valid	0	0	0	0	0	0	0	0

BFDネイバー履歴の表示

このコマンドは、各ネイバーの最新のBFDログを現在の状態とともに表示します。

```
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 Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:20.527] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:19.552] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:18.776] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:17.823] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:16.816] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:15.886] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:14.920] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:14.023] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT  
[Apr 4 15:56:13.060] Event: V1 FSM Id:4101 handle:3 event:RX DOWN state:INIT
```

```
[Apr 4 15:56:12.183] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:11.389] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:10.600] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:09.603] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:08.750] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:07.808] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:06.825] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:05.877] Event: V1 FSM lId: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 lId:4101 handle:3	event:RX	DOWN	state:INIT
[Apr 4 15:56:03.920]	Event: V1 FSM lId: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 lId:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.803] Event: V1 FSM lId:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.784] Event: V1 FSM lId:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.770] Event: notify client(CEF) IP:10.2.2.2, lId:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: notify client(EIGRP) IP:10.2.2.2, lId:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: notify client(CEF) IP:10.2.2.2, lId:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: resetting timestamps lId:104 handle:1
[Apr 4 15:10:41.768] Event: V1 FSM lId:104 handle:1 event:RX INIT state:DOWN
[Apr 4 15:10:41.751] Event: V1 FSM lId: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, lId:4198, handle:2, event:UP,			
[Apr 4 15:26:01.779]	Event: notify client(OSPF) IP:10.3.3.2, lId:4198, handle:2, event:UP,			
[Apr 4 15:26:01.778]	Event: V1 FSM lId:4198 handle:2 event:RX UP state:UP			
[Apr 4 15:26:01.777]	Event: notify client(OSPF) IP:10.3.3.2, lId:4198, handle:2, event:UP,			
[Apr 4 15:26:01.777]	Event: V1 FSM lId:4198 handle:2 event:RX INIT state:DOWN			
[Apr 4 15:26:01.776]	Event: V1 FSM lId: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 lId: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 lId:4198 handle:2 event:RX UP state:UP			
[Apr 4 15:22:48.911]	Event: notify client(CEF) IP:10.3.3.2, lId:4198, handle:2, event:UP,			
[Apr 4 15:22:48.911]	Event: notify client(OSPF) IP:10.3.3.2, lId:4198, handle:2, event:UP,			
[Apr 4 15:22:48.911]	Event: notify client(CEF) IP:10.3.3.2, lId:4198, handle:2, event:UP,			

IPv4 Sessions

NeighAddr	LD/RD	RH/RS	State	Int
[Apr 4 15:22:48.911]	Event: V1 FSM lId:4198 handle:2 event:RX INIT state:DOWN			
[Apr 4 15:22:48.910]	Event: V1 FSM lId:4198 handle:2 event:Session create state:DOWN			
[Apr 4 15:22:48.909]	Event:			
	bfd_session_created, proc:OSPF, idb:GigabitEthernet3 handle:2 act			

関連情報

- [Cisco IOS BFDリファレンス](#)
- [BFDコンフィギュレーションガイド、Cisco IOS XE 17.x](#)

- [BFD用のIETF RFC 5880](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。