

# Nexus 9000スイッチでのBFDの設定と確認

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [ネットワーク図](#)

#### [設定](#)

#### [Syslog BFDのダウンの理由](#)

### [ルーティングプロトコルでのBFDの設定](#)

#### [OSPFでのBFDの設定](#)

#### [OSPFでのBFDの設定例](#)

#### [EIGRPでのBFDの設定](#)

#### [EIGRPでのBFDの設定例](#)

#### [BGPでのBFDの設定](#)

#### [BGPでのBFDの設定例](#)

### [確認](#)

#### [セッションの詳細を使用した検証](#)

#### [アクセスリストを使用した確認](#)

#### [Ethanalyzerを使用した検証](#)

---

## はじめに

このドキュメントでは、Cisco Nexus NXOS®ベースのスイッチ全体で双方向フォワーディング検出(BFD)セッションを設定および確認する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- 双方向フォワーディング検出(BFD)
- Nexus NX-OS ソフトウェア
- ルーティングプロトコル : Open Shortest Path First(OSPF)、ボーダーゲートウェイプロトコル(BGP)、Enhanced Interior Gateway Routing Protocol(EIGRP)。

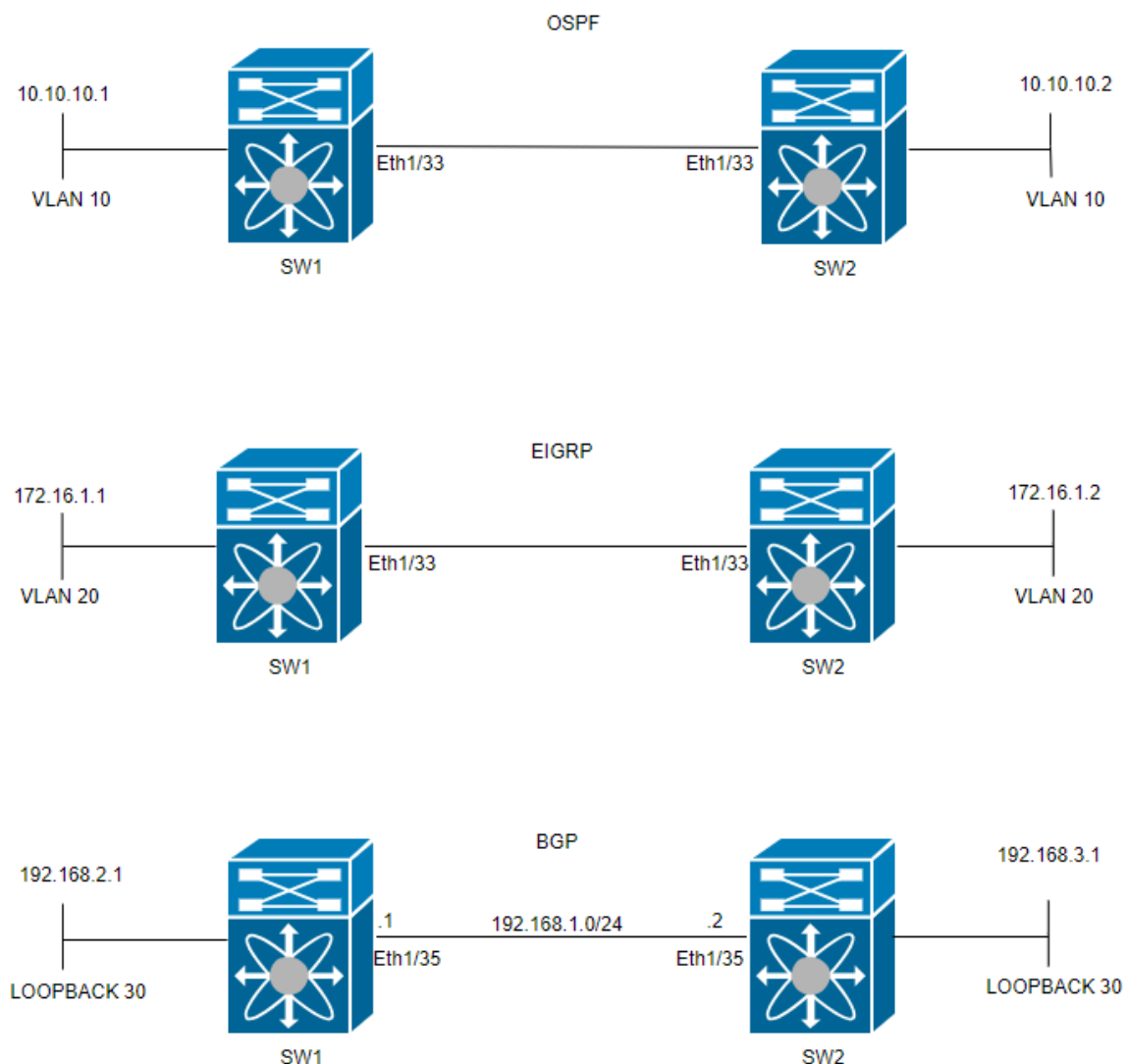
## 使用するコンポーネント

このドキュメントの情報は、NXOSバージョン10.3(4a).Mが稼働するCisco Nexus 9000に基づくものです。

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。

## 設定

### ネットワーク図



## 設定

BFDを設定する目的は、さまざまなルーティングプロトコルの設定間の違いを検出して理解することです。

ステップ1：インターフェイスおよびプロトコルでBFDを設定する前に、BFD機能を有効にする必要があります。

スイッチ 1	スイッチ 2
SW1(config)# feature bfd	SW2(config)# feature bfd

ステップ2：グローバルBFDの設定

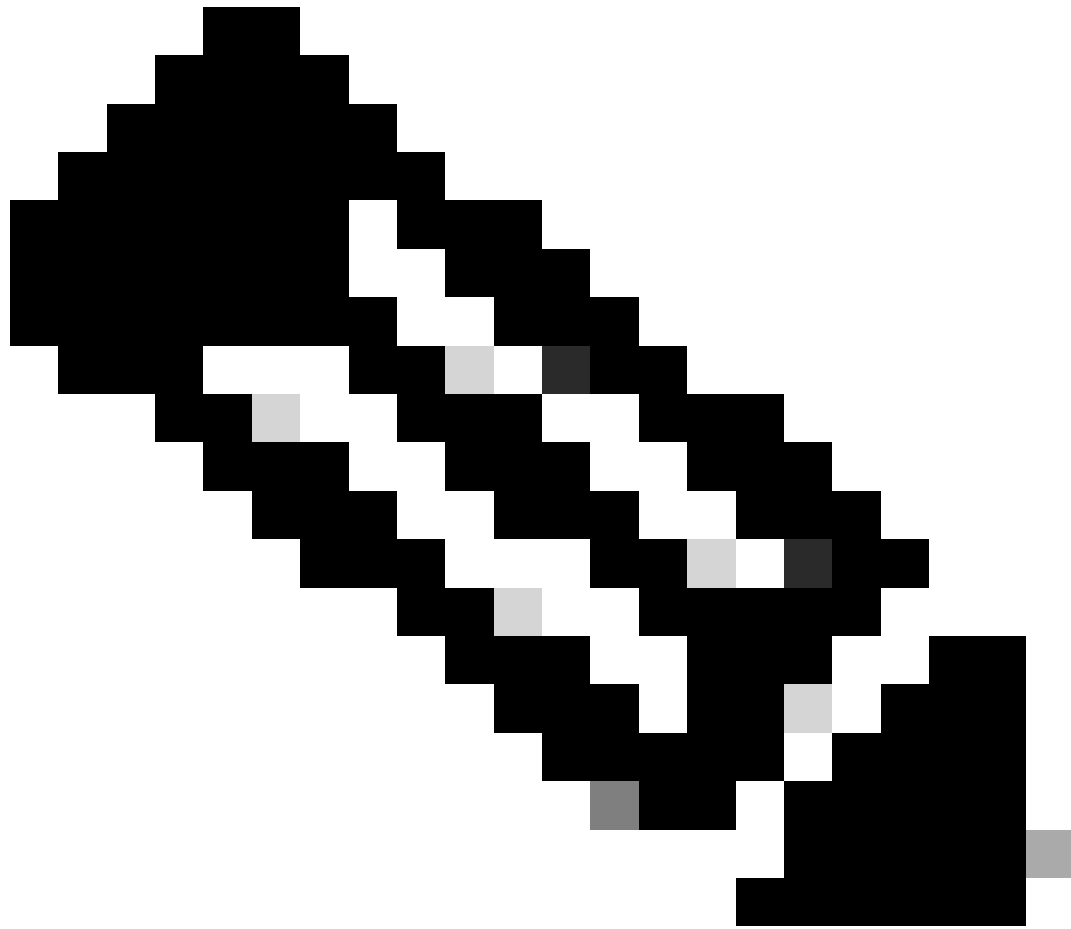
スイッチ 1	スイッチ 2
SW1(config)# bfd interval 500 min_rx 500 multiplier 3	SW2(config)# bfd interval 500 min_rx 500 multiplie



注：min\_txとmsecの範囲は50～999ミリ秒で、デフォルトは50です。乗数の範囲は1～50です。乗数のデフォルトは3です。

---

ステップ3：インターフェイスでBFDを設定する



注：インターフェイス上のすべてのBFDセッションに対してBFDセッションパラメータを設定できます。

---



警告: BFD対応インターフェイスでインターネット制御メッセージプロトコル(ICMP)リダイレクトメッセージが無効になっていることを確認してください。インターフェイスでno ip redirectsコマンドまたはno ipv6 redirectsコマンドを使用します。

スイッチ 1	スイッチ 2
<pre>SW1(config)# interface vlan 20 SW1(config-if)# bfd interval 500 min_rx 500 multiplier 3 SW1(config-if)# no ip redirects SW1(config-if)# no ipv6 redirects</pre>	<pre>SW2(config)# interface vlan 20 SW2(config-if)# bfd interval 500 min_rx 500 multiplier 3 SW2(config-if)# no ip redirects SW2(config-if)# no ipv6 redirects</pre>

BFD非同期モードは、2台のデバイス間で接続を強かに維持するためのハンドシェイクに似ています。両方のデバイスで設定すると、そのデバイスがオンになると、設定した時間に相互に特殊なメッセージの送信を開始します。これらのメッセージには、メッセージの送信頻度や、一方のデバイスがもう一方に回答できる速度など、いくつかの重要な設定があります。また、接続に問題が

発生する可能性があることを1台のデバイスが認識するのに必要な不在時のメッセージ数を決定する設定もあります。

BFDエコー機能は、テストパケットをネイバーに送信し、パケット転送にネイバーを関与させずに、テストパケットをネイバーに返送して問題をチェックします。低速タイマーを使用して制御パケットトラフィックを減らし、ネイバーを煩わせることなくネイバーシステムの転送パスをテストすることで、検出を高速化できます。両方のネイバーがエコー機能を使用する場合、非対称はありません。

#### Syslog BFDのダウンの理由

- **パスダウン**：これは、おそらくネットワークの輻輳、ハードウェアの障害、またはその他の問題が原因で、2つのBFDネイバー間の転送パスが動作していないことを示します。

```
2024 Apr 11 22:07:07 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519062 to neighbor 172.16.1.1
```

- **Echo Function Failed**：接続を確認するためにエコーパケットが送受信されるBFDの機能であるecho機能の障害。これらのパケットが正常に送受信されない場合は、問題があることを示しています。

```
2024 Apr 11 22:17:45 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519174 to neighbor 10.10.10.1
```

- **ネイバーから報告されたセッションのダウン**：ネイバーデバイスから、BFDセッションがダウンしているという信号が送られます。これは通常、接続の終了に関する問題を検出したことが原因です。

```
2024 Apr 11 22:03:48 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519058 to neighbor 172.16.1.1
```

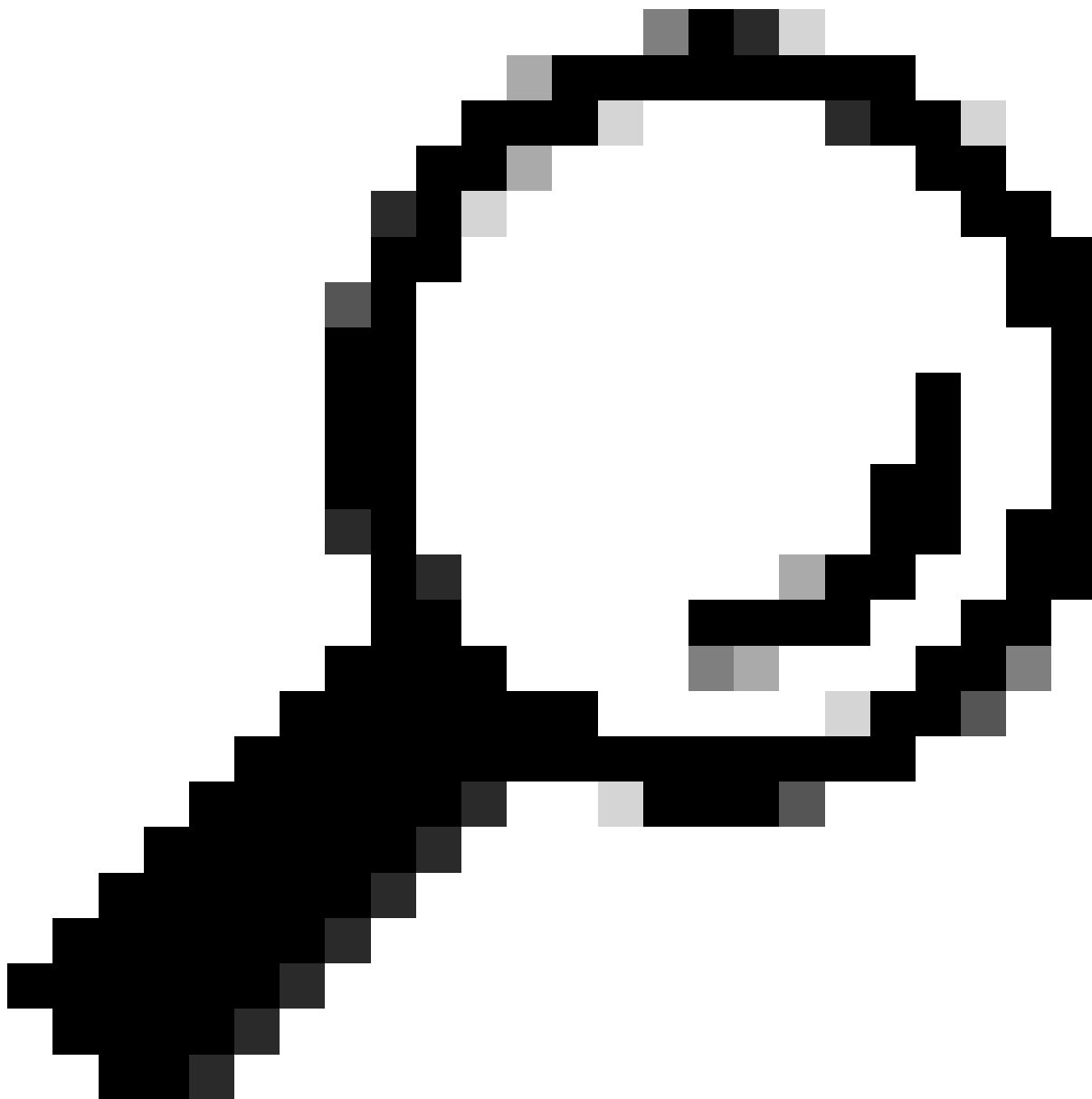
- **Control Detection Time Expired**：これは、ネイバーから予期された応答を受信する前に制御検出タイマーが時間切れになった場合に発生します。これは、接続に問題がある可能性を示しています。

```
2024 Apr 11 22:19:31 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519061 to neighbor 192.168.2.1
```

- **管理上ダウン**：BFDセッションは、メンテナンスの目的で、または設定の変更によって、管理者によって意図的にダウンにされています。

```
2024 Apr 11 22:13:15 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519064 to neighbor 10.10.10.1
```

#### ルーティングプロトコルでのBFDの設定



ヒント: OSPFでBFDが有効になっている場合は、OSPFを使用しているすべてのインターフェイスでそのBFDがアクティブになります。インターフェイスは、グローバルに設定された値を採用します。これらの値を調整する必要がある場合は、ステップ3「インターフェイスでのBFD設定」を参照してください。

---

スイッチ 1	スイッチ 2
--------	--------



SW1(config)# router ospf 1 SW1(config-router)# bfd	SW2(config)# router ospf 1 SW2(config-router)# bfd
---	---

また、コマンドを使用して、OSPFインターフェイスでBFDを有効にすることもできます `ip ospf bfd`

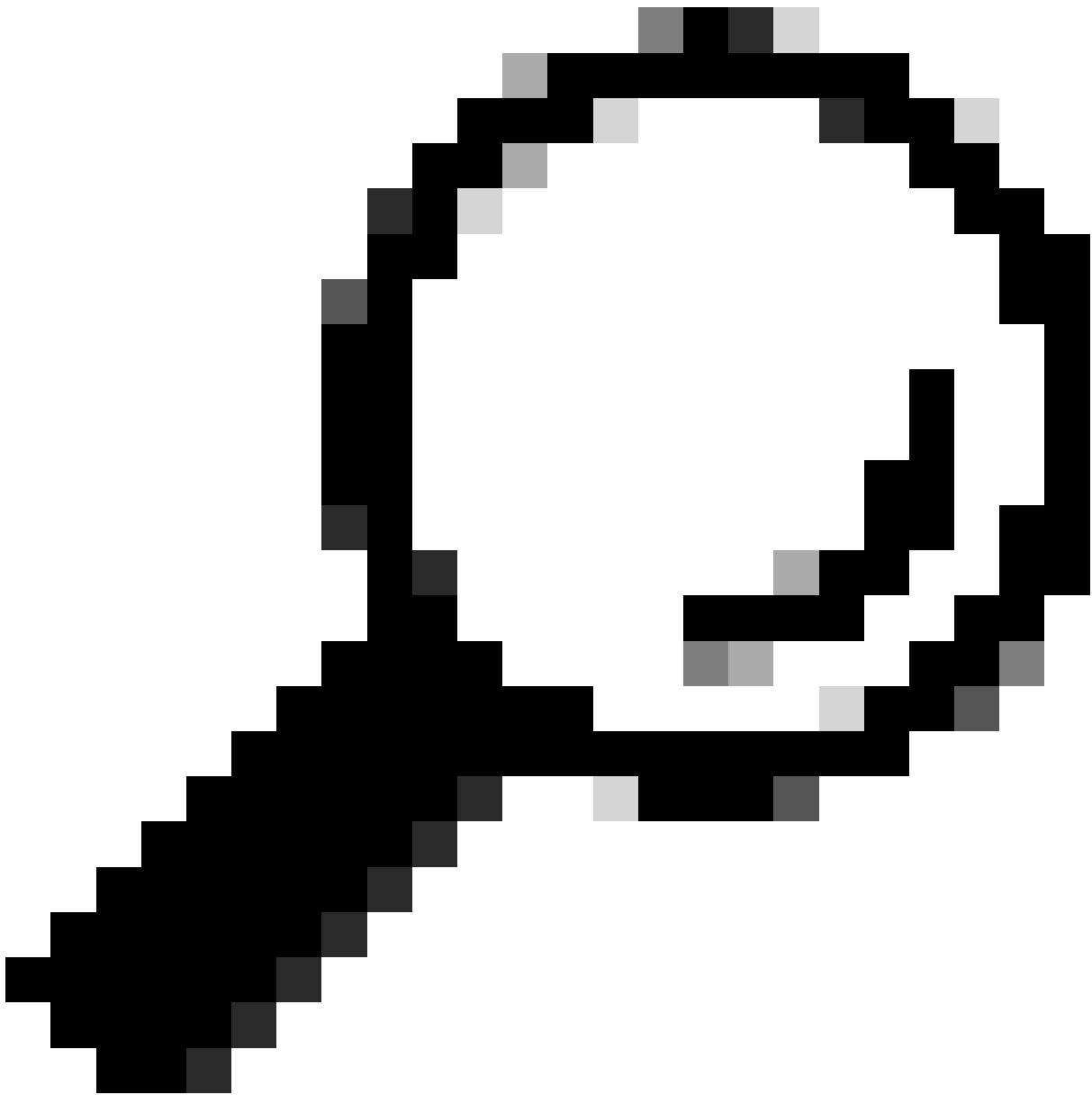
スイッチ 1	スイッチ 2
SW1(config)# interface vlan 10 SW1(config-if)# ip ospf bfd	SW2(config)# interface vlan 10 SW2(config-if)# ip ospf bfd

OSPFでのBFDの設定例

SW1# show running-config ospf !Command: show running-config ospf !Running configuration last done at: W

EIGRPでのBFDの設定

SW1(config)# interface vlan 20 SW1(config-if)# ip eigrp 2 bfd



ヒント:EIGRPでBFDが有効になっている場合は、EIGRPを使用しているすべてのインターフェイスでそのBFDがアクティブになります。インターフェイスは、グローバルに設定された値を採用します。これらの値を調整する必要がある場合は、ステップ3「インターフェイスでのBFD設定」を参照してください。

スイッチ 1	スイッチ 2
SW1(config)# router eigrp 2 SW1(config-router)# bfd	SW2(config)# router eigrp 2 SW2(config-router)# bfd

また、次のコマンドを使用して、EIGRPインターフェイスでBFDを有効にすることもできますip eigrp instance-tag bfd

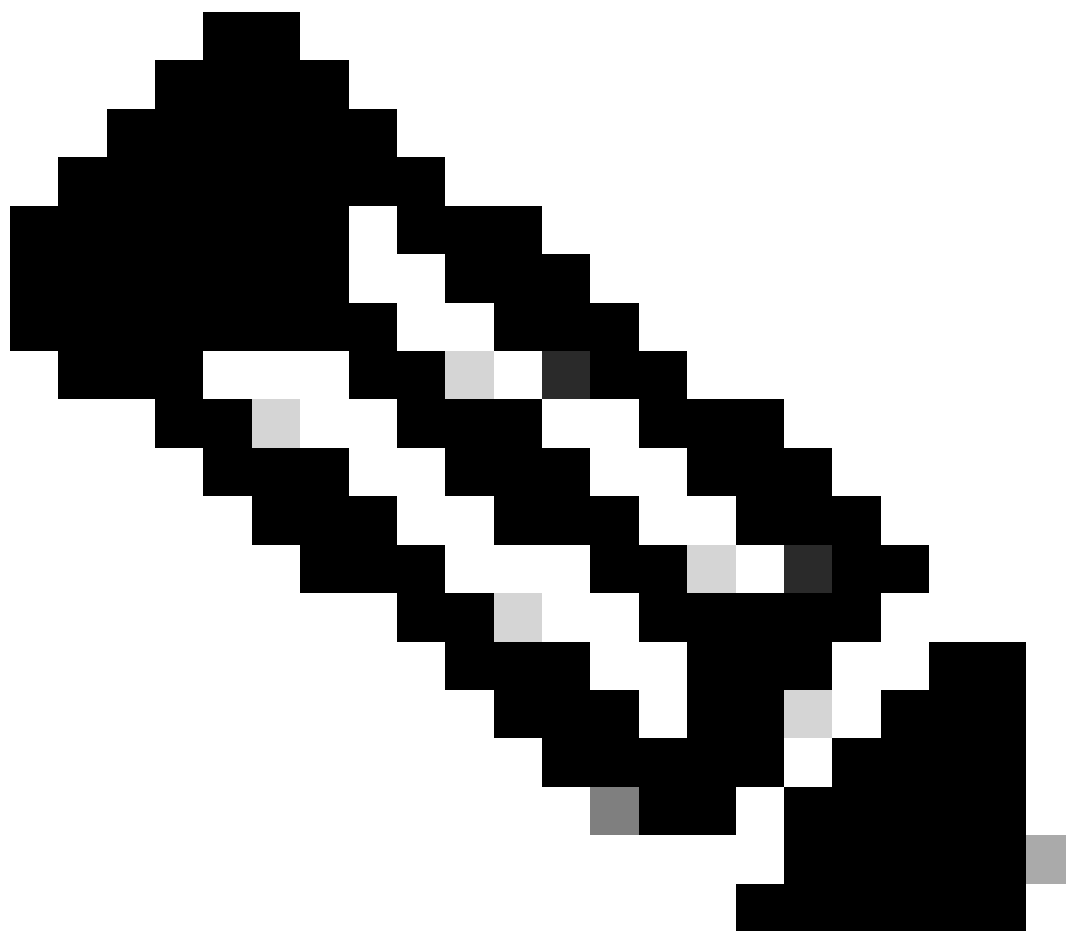
スイッチ 1	スイッチ 2
SW1(config)# interface vlan 20 SW1(config-if)# ip eigrp 2 bfd	SW2(config)# interface vlan 20 SW2(config-if)# ip eigrp 2 bfd

#### EIGRPでのBFDの設定例

```
SW1# show running-config eigrp !Command: show running-config eigrp !Running configuration last done at:
```

#### BGPでのBFDの設定

---

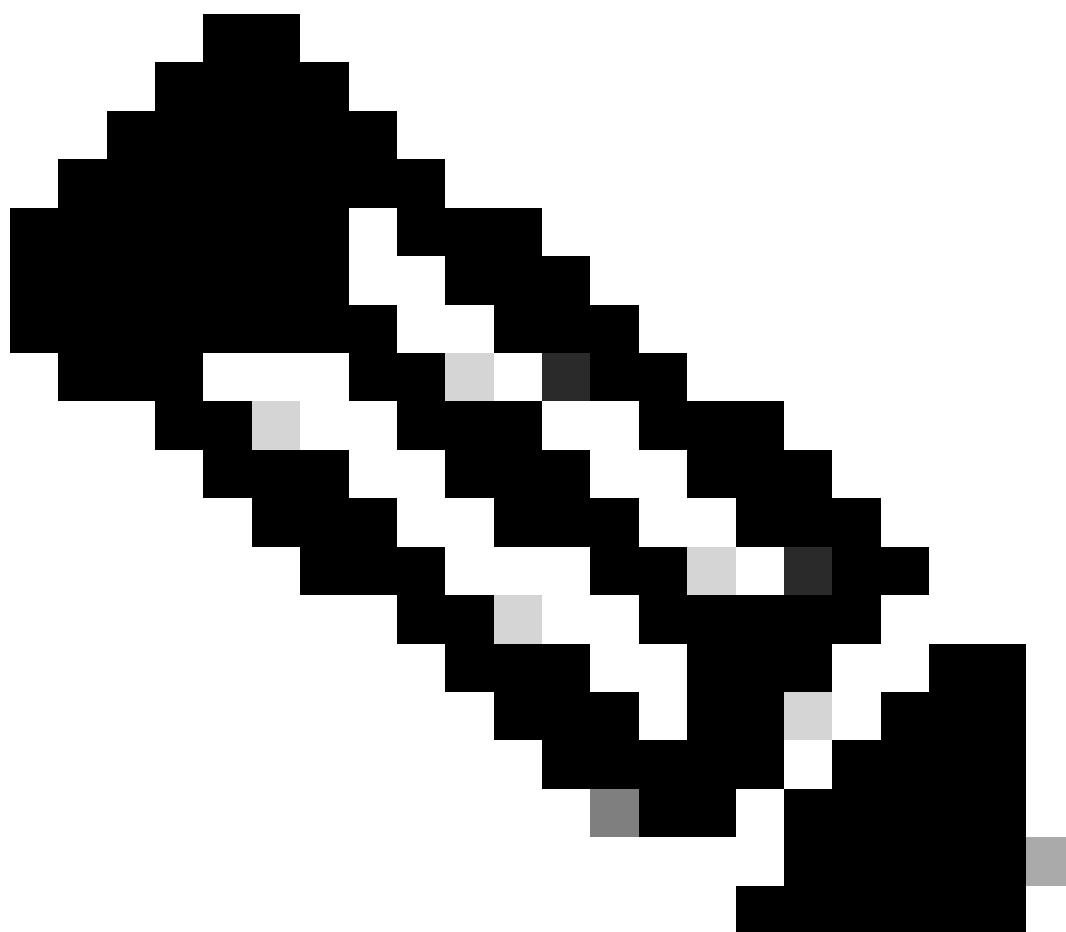


---

注:アップデートのソース機能により、ネイバーとのBGPセッションの確立中に、指定インターフェイスのプライマリIPアドレスをローカルアドレスとしてBGPセッションで使用できるようになります。さらに、BGPをクライアントとしてBFDに登録できます。

---

---



注:デバイスでBFDセッションを設定する場合は、「multihop」または「singlehop」を指定するとセッションタイプが決まります。キーワードを指定しない場合、ピアが直接接続されると、セッションタイプはデフォルトで「singlehop」になります。ピアが接続されていない場合、セッションタイプはデフォルトで「マルチホップ」に設定されます。

---

スイッチ 1	スイッチ 2
<pre>SW1(config)# router bgp 65001 SW1(config-router)# address-family ipv4 unicast SW1(config-router)# neighbor 192.168.3.1 SW1(config-router-neighbor)# bfd multihop SW1(config-router-neighbor)# update-source loopback30</pre>	<pre>SW2(config)# router bgp 65002 SW2(config-router)# address-family ipv4 unicast SW2(config-router)# neighbor 192.168.2.1 SW2(config-router-neighbor)# bfd multihop SW2(config-router-neighbor)# update-source loopback30</pre>

BGPでのBFDの設定例

```
SW1# show running-config bgp !Command: show running-config bgp !Running configuration last done at: Thu
```

確認

BFDを設定してOSPF、EIGRP、BGPなどのプロトコルと関連付けた後、BFDネイバーを自動的に特定する必要があります。これを確認するには、次のコマンドを使用します。

```
show bfd neighbors
```

スイッチ1

```
SW1# show bfd neighbors OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf Type BSID 172.16.1.1
```

スイッチ2

```
SW2# show bfd neighbors OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf Type BSID 172.16.1.2
```

これを確認して詳細な出力を取得するには、次のコマンドを使用します。

```
SW1# show bfd neighbors interface lo30 details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Vrf
```

```
SW2# show bfd neighbors interface v1an 20 details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
```

セッションの詳細を使用した検証

```
SW1# sh bfd clients Client : Number of sessions bgp : 1 ospf : 1 eigrp : 1 SW1# show system internal bf
```

アクセスリストを使用した確認

```
SW2# show system internal access-list v1an 10 input statistics slot 1 ===== INSTANCE 0x0 -----
```

Ethalyzerを使用した検証

もう1つのアプローチは、パケットキャプチャを実行して、UDPポート3785専用フィルタリングすることです。

```
SW1# ethalyzer local interface inband display-filter "udp.port==3785" limit-captured-frames 0 Capturi
```

これらのエコーパケットはローカルスイッチ自体から発信されるため、BFD Echoプロトコルからキャプチャされたパケット内には、同一の送信元IPアドレスと宛先IPアドレスが存在することが予想されます。



注:インターフェイスに「no bfd echo」文がない場合、キャプチャはBFD制御の確認とともに、ローカル発信IPアドレスとネイバー宛先IPアドレスの両方が含まれているパケットを明らかにします

---

```
SW2# ethanalyzer local interface inband display-filter "ip.addr==192.168.2.1" limit-captured-frames 0 C
```

## 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。