

Konfigurieren und Überprüfen von BFD auf Nexus 9000-Switches

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurieren](#)

[Gründe für BFD-Ausfall im Syslog](#)

[Konfigurieren von BFD für Routing-Protokolle](#)

[Konfigurieren von BFD auf OSPF](#)

[Beispielkonfigurationen für BFD in OSPF](#)

[Konfigurieren von BFD auf EIGRP](#)

[Beispielkonfigurationen für BFD auf EIGRP](#)

[Konfigurieren von BFD auf dem BGP](#)

[Beispielkonfigurationen für BFD auf BGP](#)

[Überprüfung](#)

[Überprüfung anhand von Sitzungsdetails](#)

[Überprüfen mithilfe der Zugriffsliste](#)

[Verifizieren mit Ethalyzer](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie BFD-Sitzungen (Bidirectional Forwarding Detection) für Cisco Nexus NX-OS®-basierte Switches konfigurieren und überprüfen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Bidirectional Forwarding Detection (BFD)
- Nexus NX-OS-Software

- Routing-Protokolle: Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP).

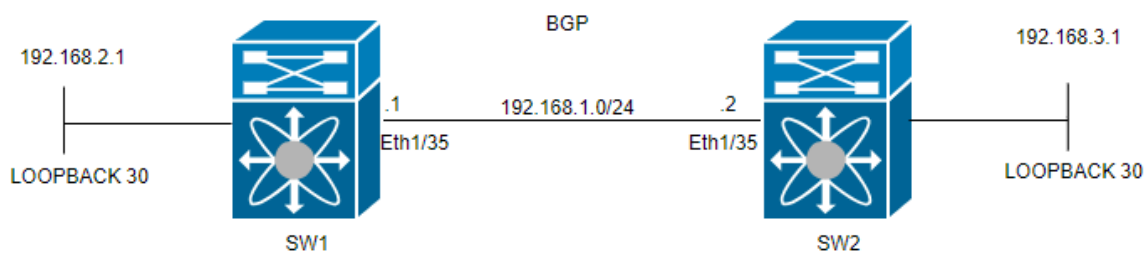
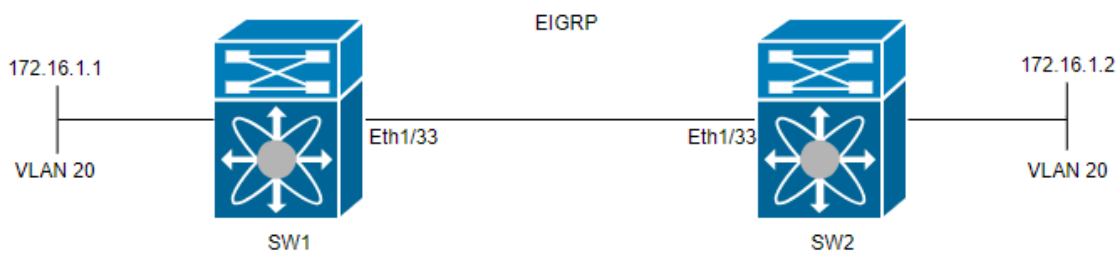
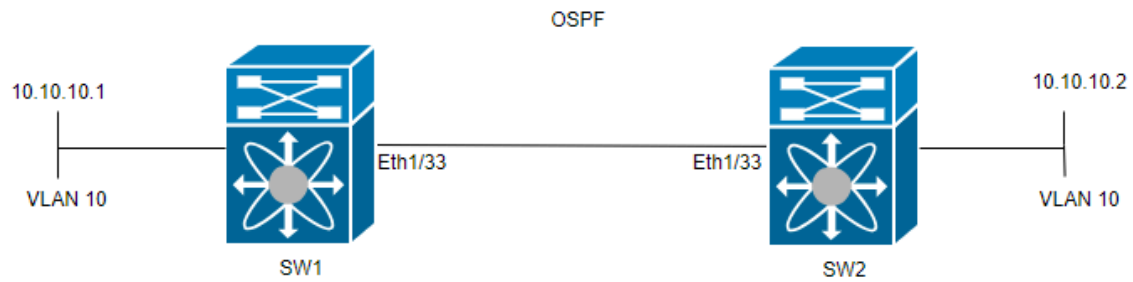
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Nexus 9000 mit NX-OS-Version 10.3(4a).M.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Konfigurieren

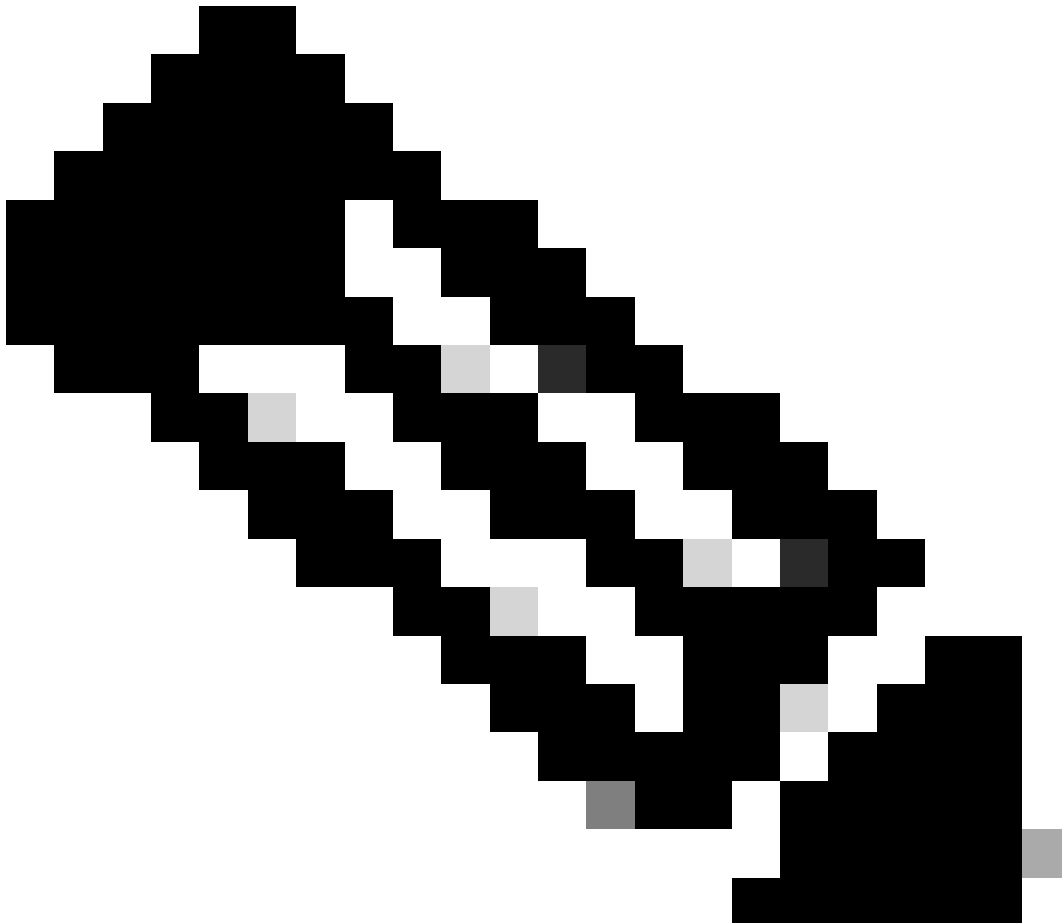
Der Zweck der BFD-Konfiguration besteht darin, die Unterschiede zwischen den Konfigurationen der verschiedenen Routing-Protokolle zu erkennen und zu verstehen.

SCHRITT 1: Sie müssen die BFD-Funktion aktivieren, bevor Sie BFD für eine Schnittstelle und ein Protokoll konfigurieren können.

SWITCH 1	SWITCH 2
SW1(config)# feature bfd	SW2(config)# feature bfd

SCHRITT 2: Konfigurieren von Global BFD

SWITCH 1	SWITCH 2
<pre>SW1(config)# bfd interval 500 min_rx 500 multiplier 3</pre>	<pre>SW2(config)# bfd interval 500 min_rx 500 multiplie</pre>



Hinweis: Der Bereich von min_tx und msec liegt zwischen 50 und 999 Millisekunden, und der Standardwert ist 50. Der Multiplikatorbereich liegt zwischen 1 und 50. Der Standardwert für den Multiplikator ist 3.

SCHRITT 3: Konfigurieren von BFD auf einer Schnittstelle



Hinweis: Sie können die BFD-Sitzungsparameter für alle BFD-Sitzungen einer Schnittstelle konfigurieren.



Warnung: Stellen Sie sicher, dass die ICMP-Umleitungsmeldungen (Internet Control Message Protocol) an BFD-fähigen Schnittstellen deaktiviert sind. Verwenden Sie den `no ip redirects` Befehl oder den `no ipv6 redirects` Befehl auf der Schnittstelle.

SWITCH 1	SWITCH 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>

Der asynchrone BFD-Modus ist wie ein Handshake zwischen zwei Geräten, um die Verbindung stabil zu halten. Sie richten es auf beiden Geräten ein, und sobald es eingeschaltet ist, senden sie sich zu einer bestimmten Zeit spezielle Nachrichten. Diese Nachrichten enthalten einige wichtige Einstellungen, z. B. wie oft sie gesendet werden und wie schnell ein Gerät auf das andere reagieren kann. Es gibt auch eine Einstellung,

die entscheidet, wie viele verpasste Nachrichten ein Gerät benötigt, um festzustellen, dass ein Problem mit der Verbindung vorliegen kann.

Die BFD-Echo-Funktion sendet Testpakete an einen Nachbarn und sendet diese zurück, um Probleme zu überprüfen, ohne diesen an der Paketweiterleitung zu beteiligen. Er kann einen langsameren Timer verwenden, um den Kontrollpaketverkehr zu reduzieren, und testet den Weiterleitungspfad auf dem Nachbarsystem, ohne den Nachbarn zu stören. Dies beschleunigt die Erkennung. Wenn beide Nachbarn die Echo-Funktion verwenden, gibt es keine Asymmetrie.

Gründe für BFD-Ausfall im Syslog

- Path Down: Zeigt an, dass der Weiterleitungspfad zwischen den beiden BFD-Nachbarn möglicherweise aufgrund von Netzwerküberlastung, Hardwareausfällen oder anderen Problemen nicht mehr funktioniert.

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

- Echo Function Failed: Fehler in der Echo-Funktion, einer Funktion von BFD, bei der Echo-Pakete gesendet und empfangen werden, um die Verbindung zu überprüfen. Wenn diese Pakete nicht erfolgreich übertragen oder empfangen werden können, weist dies auf ein Problem hin.

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

- Neighbor Signed Session Down (Benachbarte, signalisierte Sitzung unterbrochen): Das Nachbargerät signalisiert, dass die BFD-Sitzung unterbrochen ist, was in der Regel darauf zurückzuführen ist, dass am Ende der Verbindung ein Problem erkannt wurde.

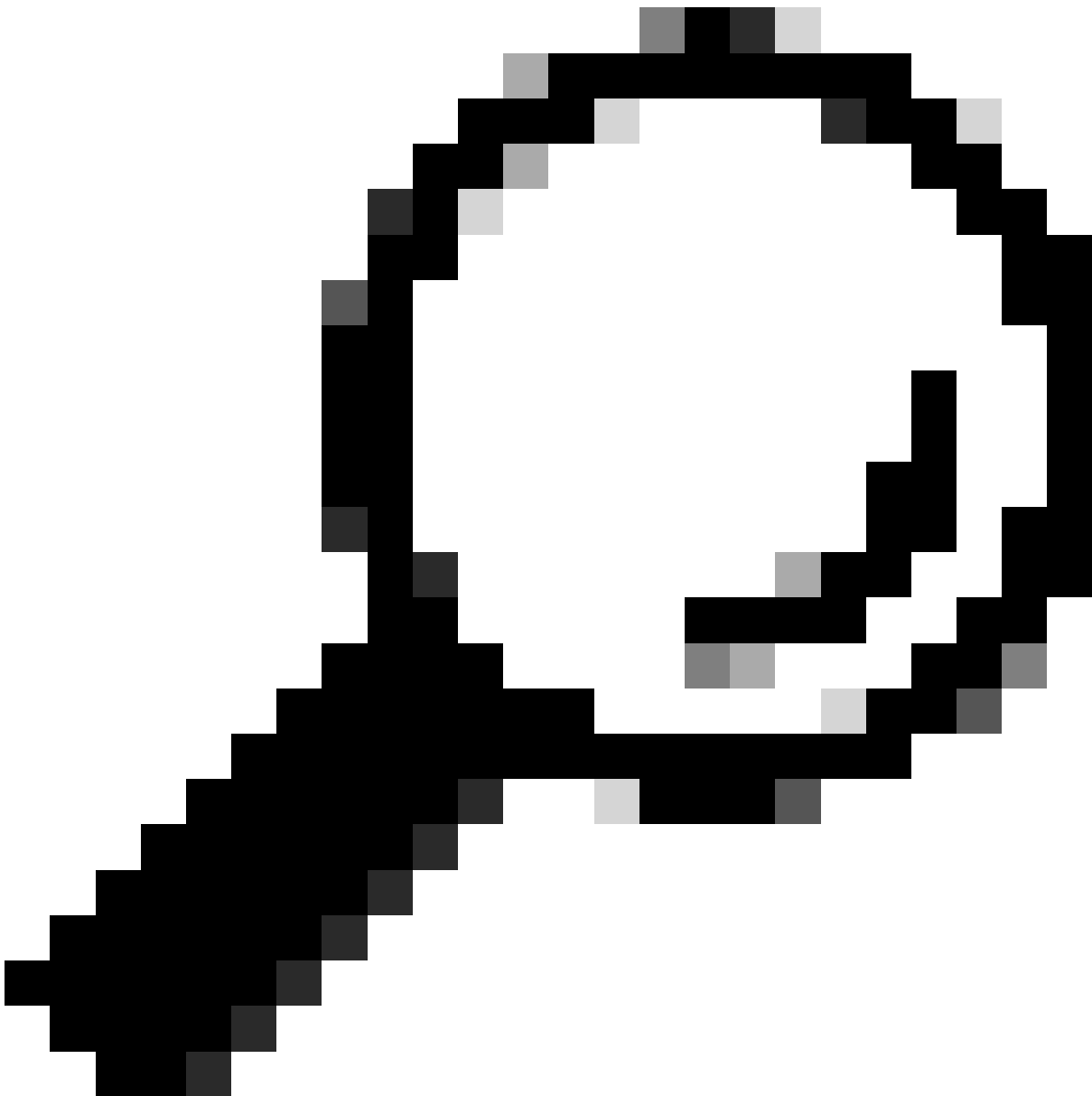
```
2024 Apr 11 22:03:48 SW2 %BFD-5-SESSION_STATE_DOWN: BFD session 1090519058 to neighbor 172.16.1.1
```

- Control Detection Time Expired (Erkennungszeit für Steuerung abgelaufen): Dieser Fehler tritt auf, wenn der Timer für die Steuerelementerkennung abläuft, bevor eine erwartete Antwort vom Nachbarn empfangen wird. Dies weist auf ein potenzielles Verbindungsproblem hin.

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

- Administrative Abschaltung: Die BFD-Sitzung wird von einem Administrator absichtlich abgeschaltet, entweder zu Wartungszwecken oder aufgrund von Konfigurationsänderungen.

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



Tipp: Wenn BFD unter OSPF aktiviert ist, wird es für alle Schnittstellen aktiviert, die OSPF verwenden. Die Schnittstellen übernehmen die global konfigurierten Werte. Wenn Anpassungen an diesen Werten erforderlich sind, lesen Sie Schritt 3, "BFD-Konfiguration auf einer Schnittstelle".

SWITCH 1

SWITCH 2

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

Außerdem kann BFD über die OSPF-Schnittstelle mithilfe des Befehls `ospf bfd`

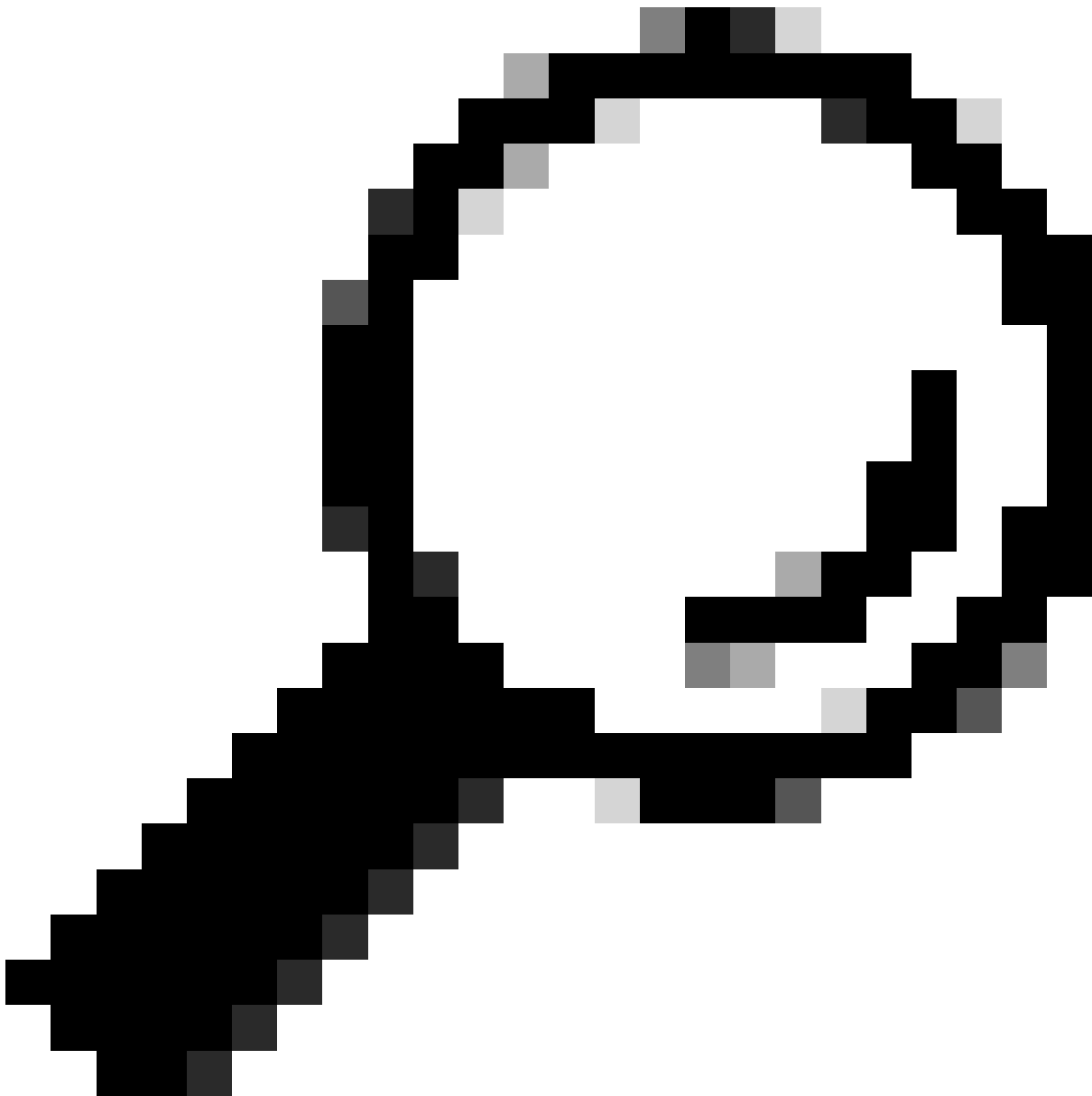
SWITCH 1	SWITCH 2
SW1(config)# interface vlan 10 SW1(config-if)# ip ospf bfd	SW2(config)# interface vlan 10 SW2(config-if)# ip ospf bfd

Beispielkonfigurationen für BFD in OSPF

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

Konfigurieren von BFD auf EIGRP

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



Tipp: Wenn BFD unter EIGRP aktiviert ist, wird es für alle Schnittstellen aktiviert, die EIGRP verwenden. Die Schnittstellen übernehmen die global konfigurierten Werte. Wenn Anpassungen an diesen Werten erforderlich sind, lesen Sie Schritt 3, "BFD-Konfiguration auf einer Schnittstelle".

SWITCH 1	SWITCH 2
<pre>SW1(config)# router eigrp 2 SW1(config-router)# bfd</pre>	<pre>SW2(config)# router eigrp 2 SW2(config-router)# bfd</pre>

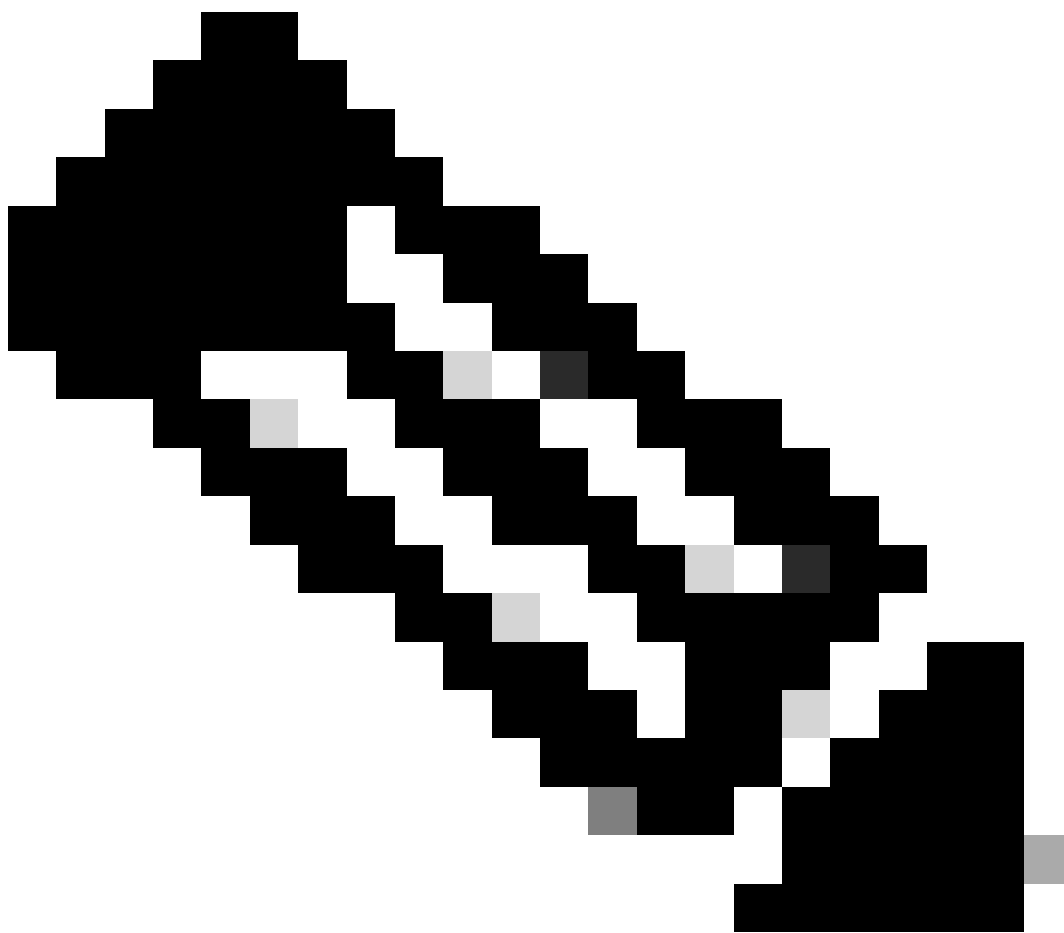
Darüber hinaus kann BFD über eine EIGRP-Schnittstelle mithilfe des Befehls `ip eigrp instance-tag bfd`

SWITCH 1	SWITCH 2
<pre>SW1(config)# interface vlan 20 SW1(config-if)# ip eigrp 2 bfd</pre>	<pre>SW2(config)# interface vlan 20 SW2(config-if)# ip eigrp 2 bfd</pre>

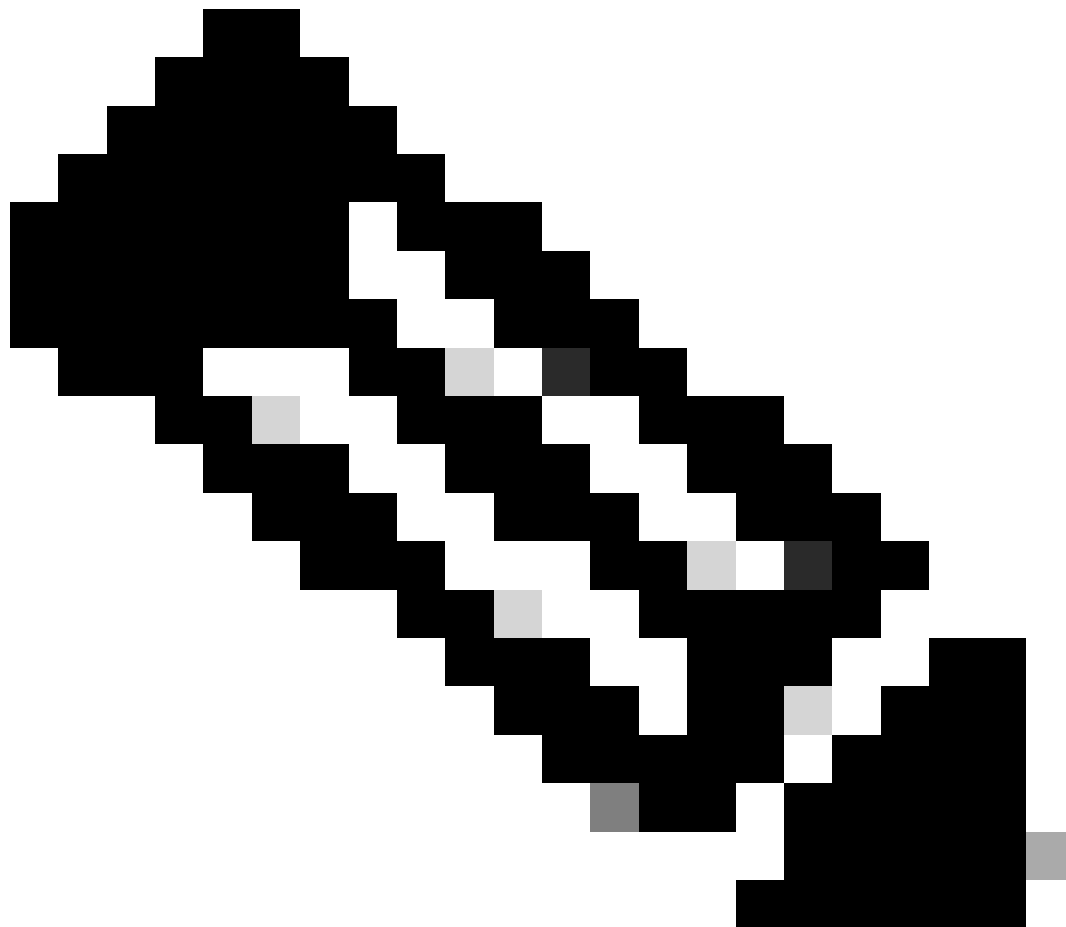
Beispielkonfigurationen für BFD auf EIGRP

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

Konfigurieren von BFD auf dem BGP



Hinweis: Die Funktion Update Source (Update-Adresse) erleichtert BGP-Sitzungen die Verwendung der primären IP-Adresse einer designierten Schnittstelle als lokale Adresse während des Aufbaus einer BGP-Sitzung mit einem Nachbarn. Darüber hinaus kann sich BGP als Client bei BFD registrieren.



Hinweis: Wenn Sie BFD-Sitzungen auf dem Gerät konfigurieren, bestimmt die Angabe von entweder 'multihop' oder 'singlehop' den Sitzungstyp. Wenn kein Schlüsselwort angegeben wird, wird für den Sitzungstyp standardmäßig 'Singlehop' verwendet, wenn der Peer direkt verbunden ist. Wenn der Peer nicht verbunden ist, lautet der Standardwert für den Sitzungstyp "multihop" (Multihop).

SWITCH 1	SWITCH 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>

Beispielkonfigurationen für BFD auf BGP

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

Überprüfung

Nach der Konfiguration von BFD und der Zuordnung zu einem Protokoll wie OSPF, EIGRP oder BGP müssen die BFD-Nachbarn automatisch identifiziert werden. Verwenden Sie den folgenden Befehl, um dies zu bestätigen:

```
show bfd neighbors
```

Auf Switch 1

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

Auf Switch 2

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

Um dies zu bestätigen und eine detaillierte Ausgabe zu erhalten, verwenden Sie den folgenden Befehl:

```
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
```

Überprüfung anhand von Sitzungsdetails

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

Überprüfen mithilfe der Zugriffsliste

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

Verifizieren mit Ethalyzer

Ein alternativer Ansatz besteht darin, eine Paketerfassung auszuführen, die speziell für den UDP-Port 3785 gefiltert wird.

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

Es wird erwartet, dass identische Quell- und Ziel-IP-Adressen in den erfassten Paketen vom BFD-Echo-Protokoll vorhanden sind, da diese Echo-Pakete vom lokalen Switch selbst stammen.



Hinweis: Wenn die "no bfd echo"-Anweisung unter der Schnittstelle nicht vorhanden ist, werden bei der Erfassung Pakete mit der lokal bezogenen IP-Adresse und der benachbarten Ziel-IP-Adresse angezeigt, zusammen mit der BFD-Kontrolle.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.