Configuration et vérification du BFD sur les commutateurs Nexus 9000

Table des matières

Introduction

Ce document décrit comment configurer et vérifier les sessions de détection de transfert bidirectionnel (BFD) sur les commutateurs Cisco Nexus basés sur NXOS®.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Détection de transfert bidirectionnel (BFD)
- Logiciel Nexus NX-OS.

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

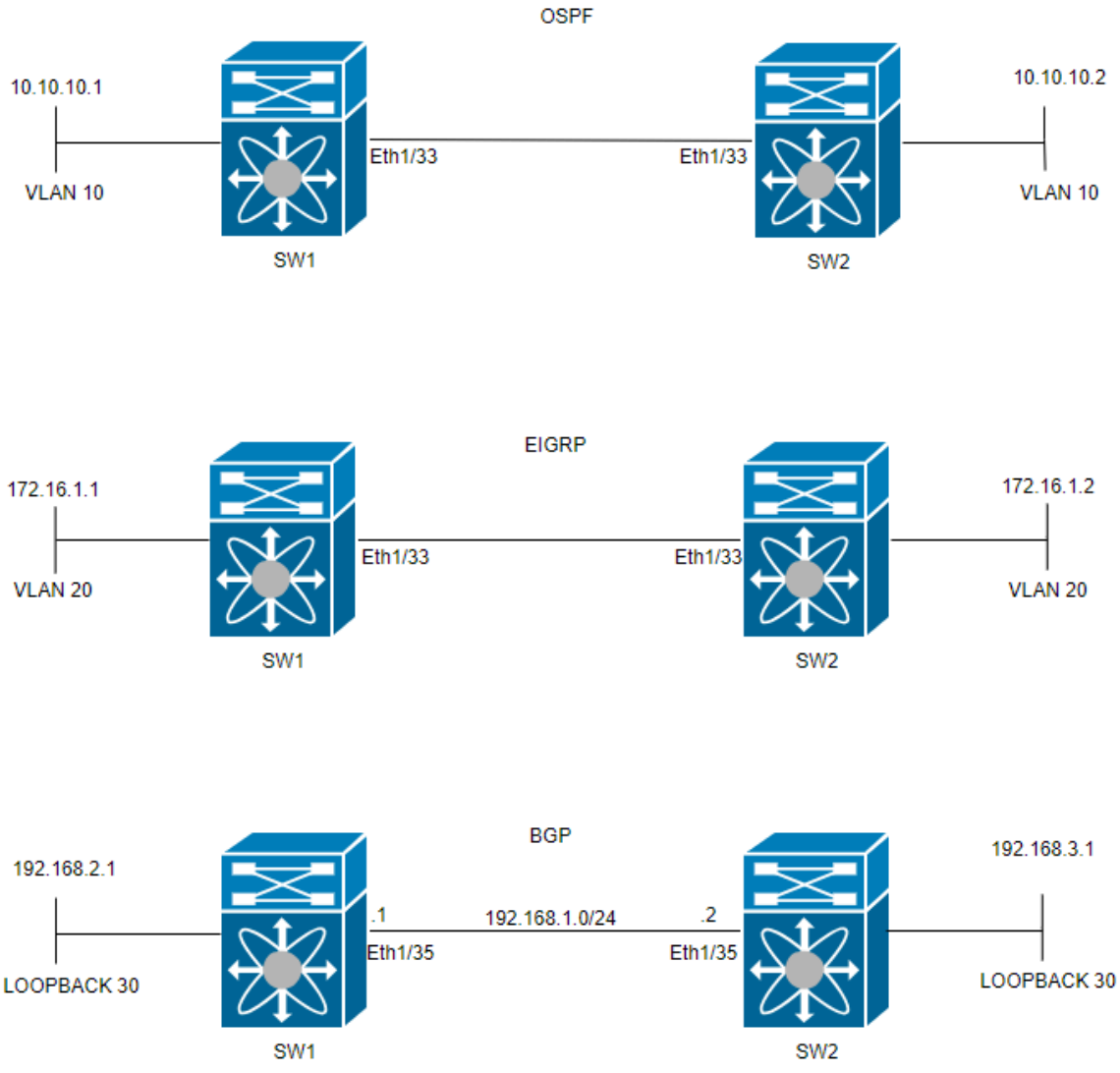
Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Nexus 9000 avec NXOS version 10.3(4a).M.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Configurer

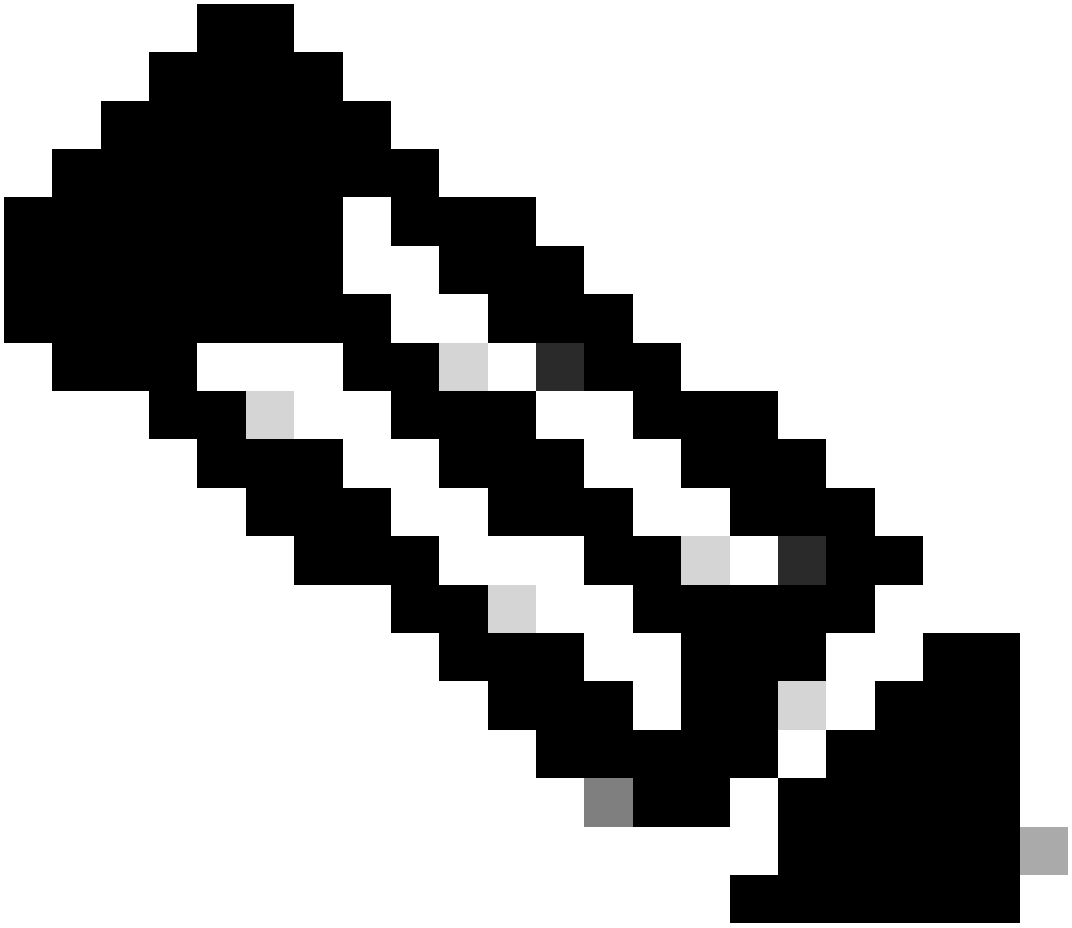
L’objectif de la configuration BFD est de détecter et de comprendre les différences entre les configurations des différents protocoles de routage.

ÉTAPE 1 : Vous devez activer la fonctionnalité BFD avant de pouvoir configurer BFD sur une interface et un protocole.

COMMUTATEUR 1	COMMUTATEUR 2
`SW1(config)# feature bfd`	`SW2(config)# feature bfd`

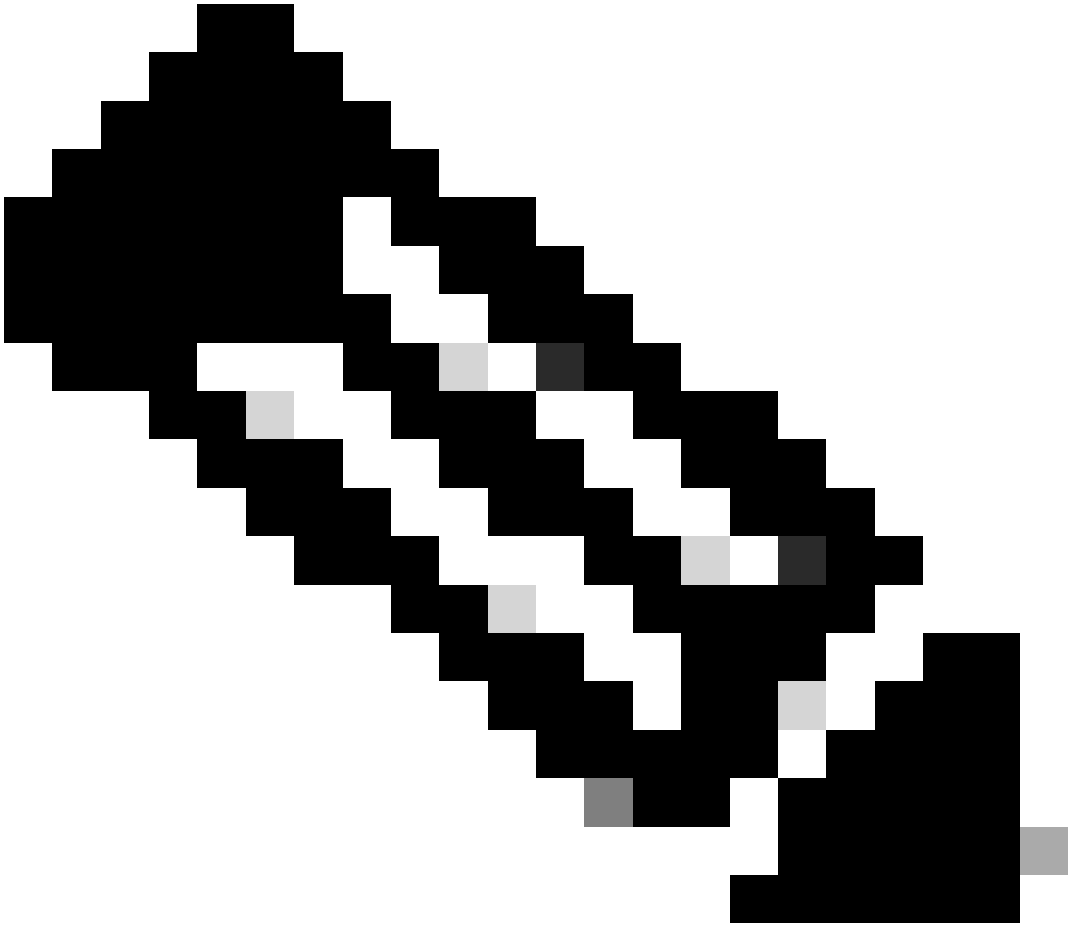
ÉTAPE 2 : Configuration du BFD global

COMMUTATEUR 1	COMMUTATEUR 2
`SW1(config)# bfd interval 500 min_rx 500 multiplier 3`	**`SW2(config)# bfd interval 500 min_rx 500 multiplie`**

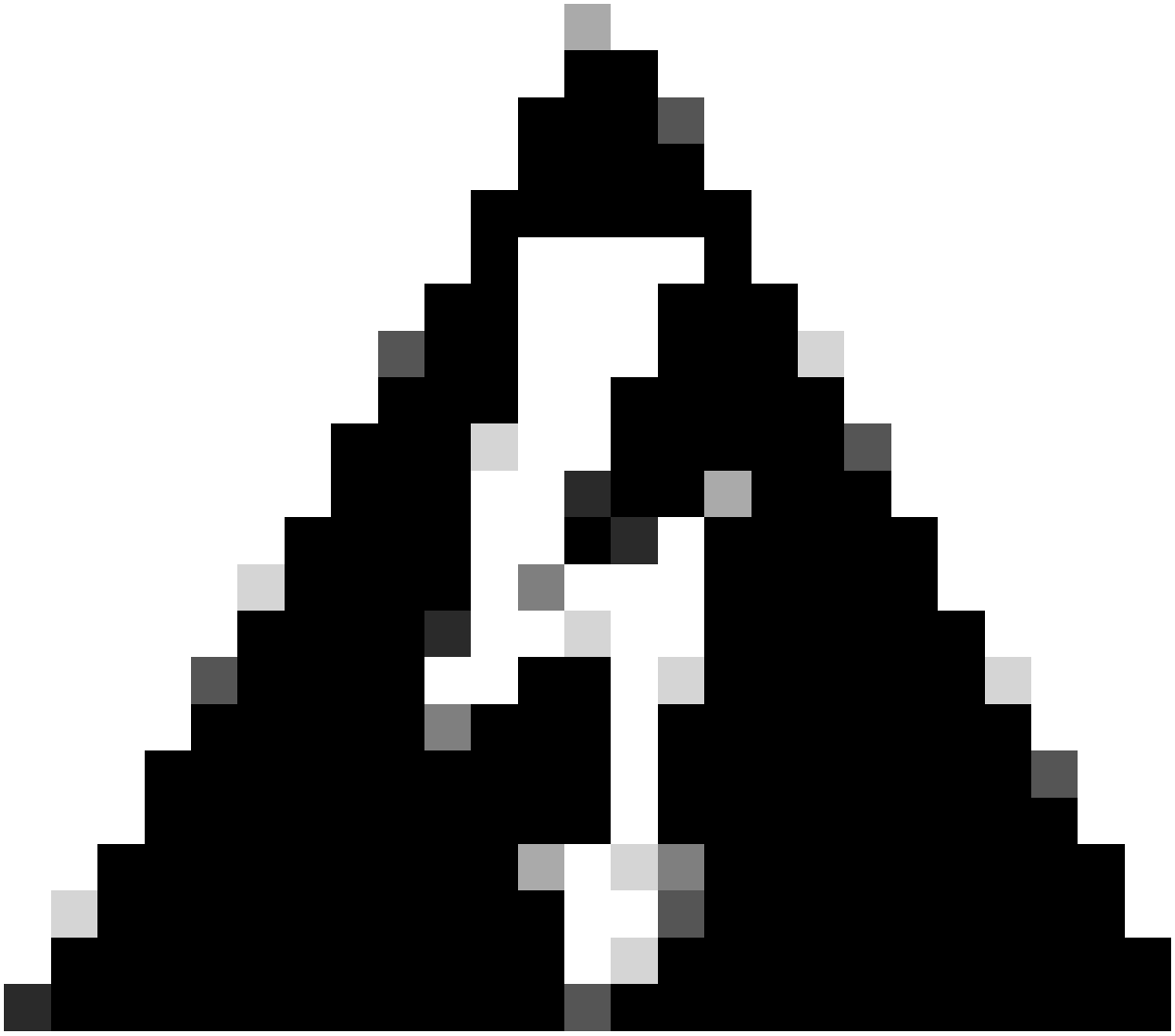


Remarque : la plage min_tx et msec est comprise entre 50 et 999 millisecondes et la valeur par défaut est 50. Le multiplicateur est compris entre 1 et 50. Le multiplicateur par défaut est 3.

ÉTAPE 3 : Configuration de BFD sur une interface



Remarque : vous pouvez configurer les paramètres de session BFD pour toutes les sessions BFD sur une interface.



Avertissement : assurez-vous que les messages de redirection ICMP (Internet Control Message Protocol) sont désactivés sur les interfaces compatibles BFD. Utilisez la no ip redirects commande ou la commandeno ipv6 redirects sur l'interface.

COMMUTATEUR 1	COMMUTATEUR 2
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	SW2(config)# interface vlan 20 SW2(config-if)# bfd interval 500 min_rx 500 mul SW2(config-if)# no ip redirects SW2(config-if)# no ipv6 redirects

Le mode asynchrone BFD est comme une connexion entre deux périphériques pour maintenir une connexion forte. Vous la configurez sur les deux périphériques et une fois qu'elle est activée, ils commencent à s'envoyer des messages spéciaux à un moment donné. Ces messages ont des paramètres importants, comme la fréquence à laquelle ils sont envoyés et la vitesse à laquelle un périphérique peut répondre à l'autre. Il existe

également un paramètre qui détermine le nombre de messages manqués nécessaires pour qu'un périphérique réalise qu'il peut y avoir un problème de connexion.

La fonction d'écho BFD envoie des paquets de test à un voisin et les renvoie pour vérifier les problèmes sans impliquer le voisin dans le transfert de paquets. Il peut utiliser un temporisateur plus lent pour réduire le trafic des paquets de contrôle et tester le chemin de transmission sur le système voisin sans déranger le voisin, ce qui accélère la détection. Si les deux voisins utilisent la fonction echo, il n'y a pas d'asymétrie.

Raisons de blocage BFD Syslog

- Path Down : indique que le chemin de transfert entre les deux voisins BFD n'est plus opérationnel, peut-être en raison d'un encombrement du réseau, d'une défaillance matérielle ou d'autres problèmes.

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

- Échec de la fonction d'écho : échec de la fonction d'écho, qui est une fonctionnalité de BFD où les paquets d'écho sont envoyés et reçus pour vérifier la connectivité. Si ces paquets ne parviennent pas à être transmis ou reçus, cela indique un problème.

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

- Neighbor Signaled Session Down : le périphérique voisin signale que la session BFD est désactivée, généralement en raison de la détection d'un problème sur la fin de la connexion.

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

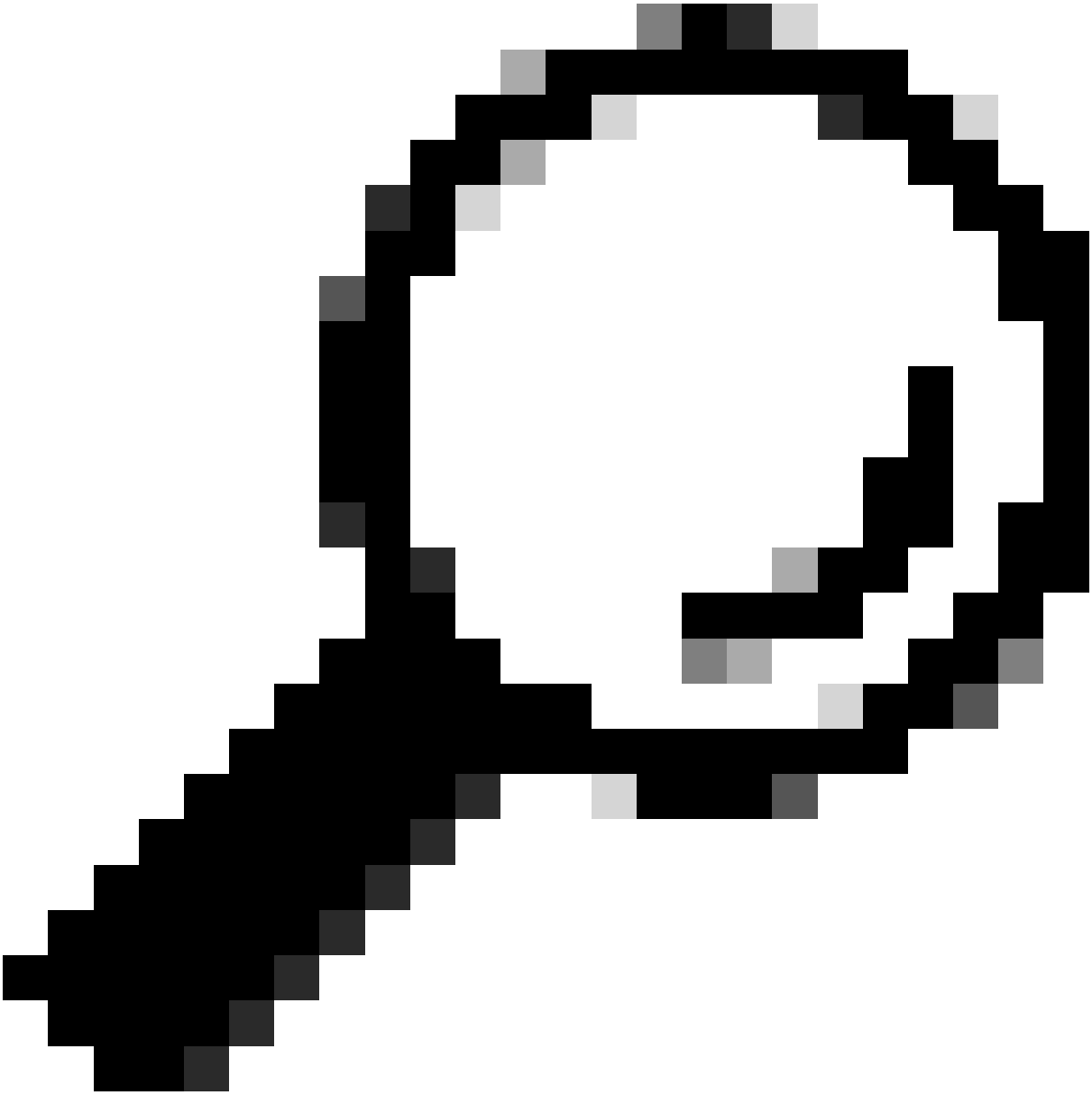
- Control Detection Time Expired : se produit lorsque le compteur de détection de contrôle s'exécute avant de recevoir une réponse attendue du voisin, indiquant un problème potentiel avec la connexion.

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

- Administrative Down : la session BFD est intentionnellement arrêtée par un administrateur, à des fins de maintenance ou en raison de modifications de configuration.

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

Configuration de BFD sur les protocoles de routage



Conseil : lorsque BFD est activé sous OSPF, il devient actif pour toutes les interfaces utilisant OSPF. Les interfaces adoptent les valeurs configurées globalement. Si des ajustements de ces valeurs sont nécessaires, reportez-vous à l'étape 3, « Configuration BFD sur une interface ».

COMMUTATEUR 1	COMMUTATEUR 2
`SW1(config)# router ospf 1`	`SW2(config)# router ospf 1`

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

Il peut également activer BFD sous l'interface OSPF avec la commandeip ospf bfd

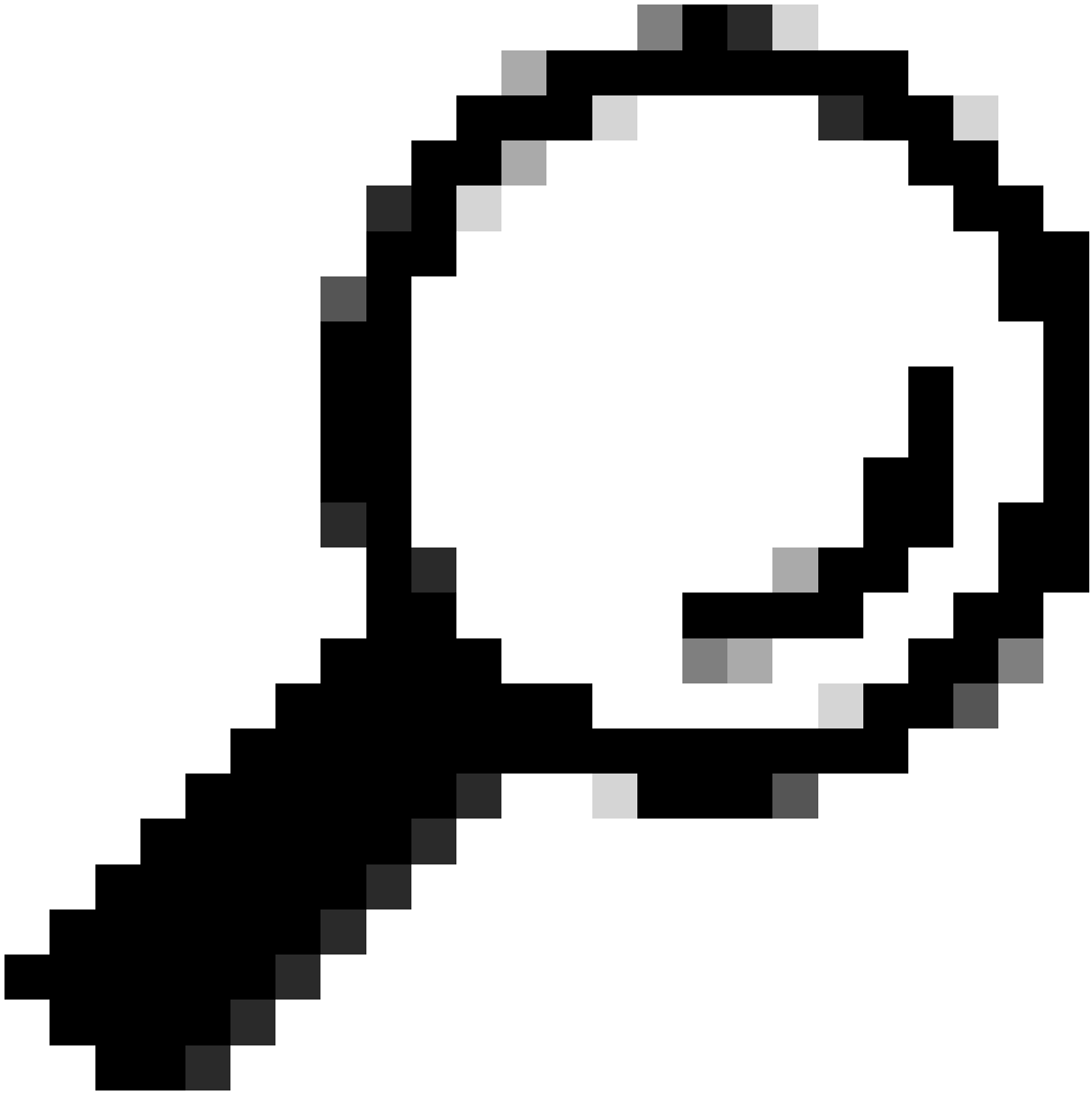
COMMUTATEUR 1	COMMUTATEUR 2
SW1(config)# interface vlan 10 SW1(config-if)# ip ospf bfd	SW2(config)# interface vlan 10 SW2(config-if)# ip ospf bfd

Exemples de configuration de BFD sur OSPF

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

Configuration de BFD sur EIGRP

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



Conseil : lorsque BFD est activé sous EIGRP, il devient actif pour toutes les interfaces utilisant EIGRP. Les interfaces adoptent les valeurs configurées globalement. Si des ajustements de ces valeurs sont nécessaires, reportez-vous à l'étape 3, « Configuration BFD sur une interface ».

COMMUTATEUR 1	COMMUTATEUR 2
SW1(config)# router eigrp 2 SW1(config-router)# bfd	SW2(config)# router eigrp 2 SW2(config-router)# bfd

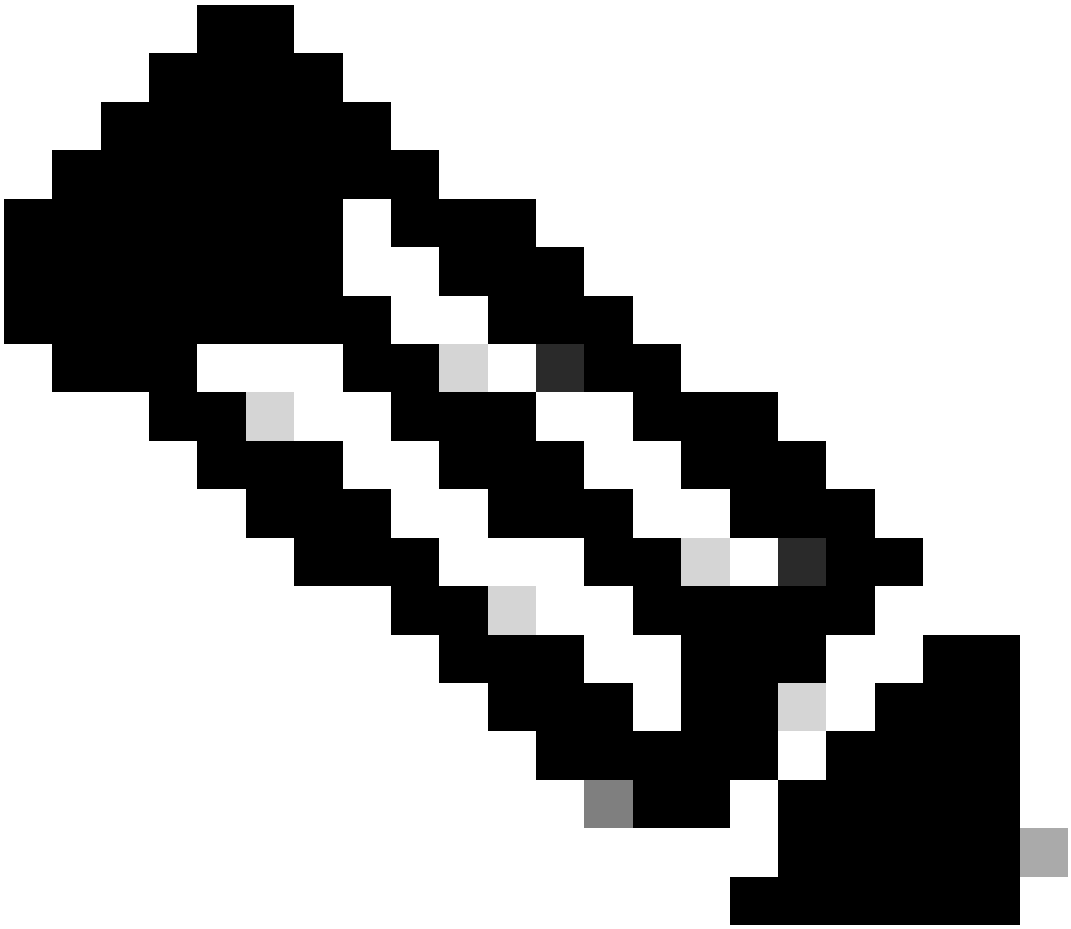
Il peut également activer BFD sous une interface EIGRP avec la commandeip eigrp instance-tag bfd

COMMUTATEUR 1	COMMUTATEUR 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

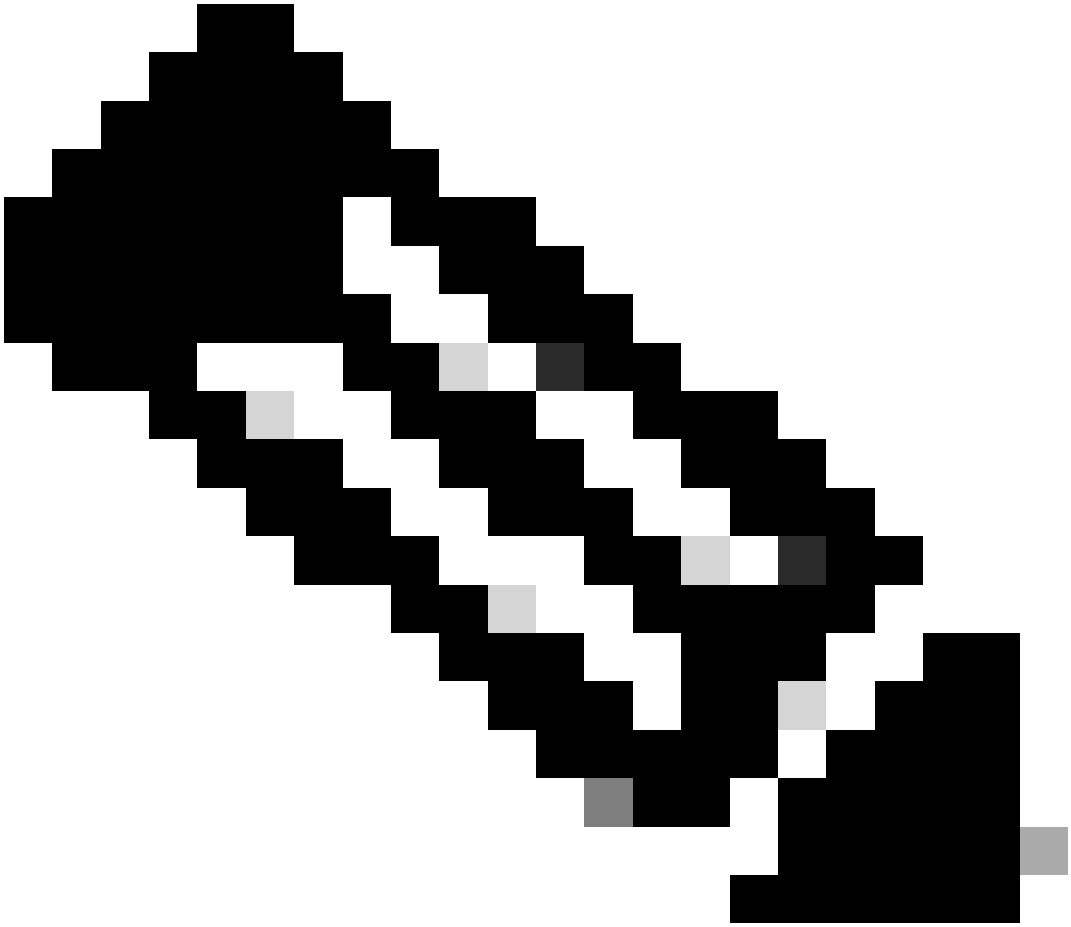
Exemples de configuration de BFD sur EIGRP

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

Configuration de BFD sur BGP



Remarque : la fonctionnalité de mise à jour de la source facilite les sessions BGP pour utiliser l'adresse IP principale d'une interface désignée comme adresse locale lors de l'établissement d'une session BGP avec un voisin. En outre, il permet à BGP de s'enregistrer en tant que client avec BFD.



Remarque : lors de la configuration des sessions BFD sur le périphérique, la spécification de 'multihop' ou 'single hop' détermine le type de session. Si aucun mot-clé n'est fourni, le type de session par défaut est 'singlehop' lorsque l'homologue est directement connecté. Si l'homologue n'est pas connecté, le type de session par défaut est 'multihop'.

COMMUTATEUR 1	COMMUTATEUR 2
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	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 loopbac

Exemples de configuration de BFD sur BGP

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

Vérifier

Après avoir configuré BFD et l'avoir associé à un protocole tel qu'OSPF, EIGRP ou BGP, les voisins BFD doivent être automatiquement identifiés. Pour le confirmer, utilisez la commande suivante :

```
show bfd neighbors
```

Sur le commutateur 1

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

Sur le commutateur 2

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

Pour le confirmer et obtenir des informations détaillées, utilisez la commande suivante :

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

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

Vérifier en utilisant les détails de session

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

Vérification à l'aide de Access-list

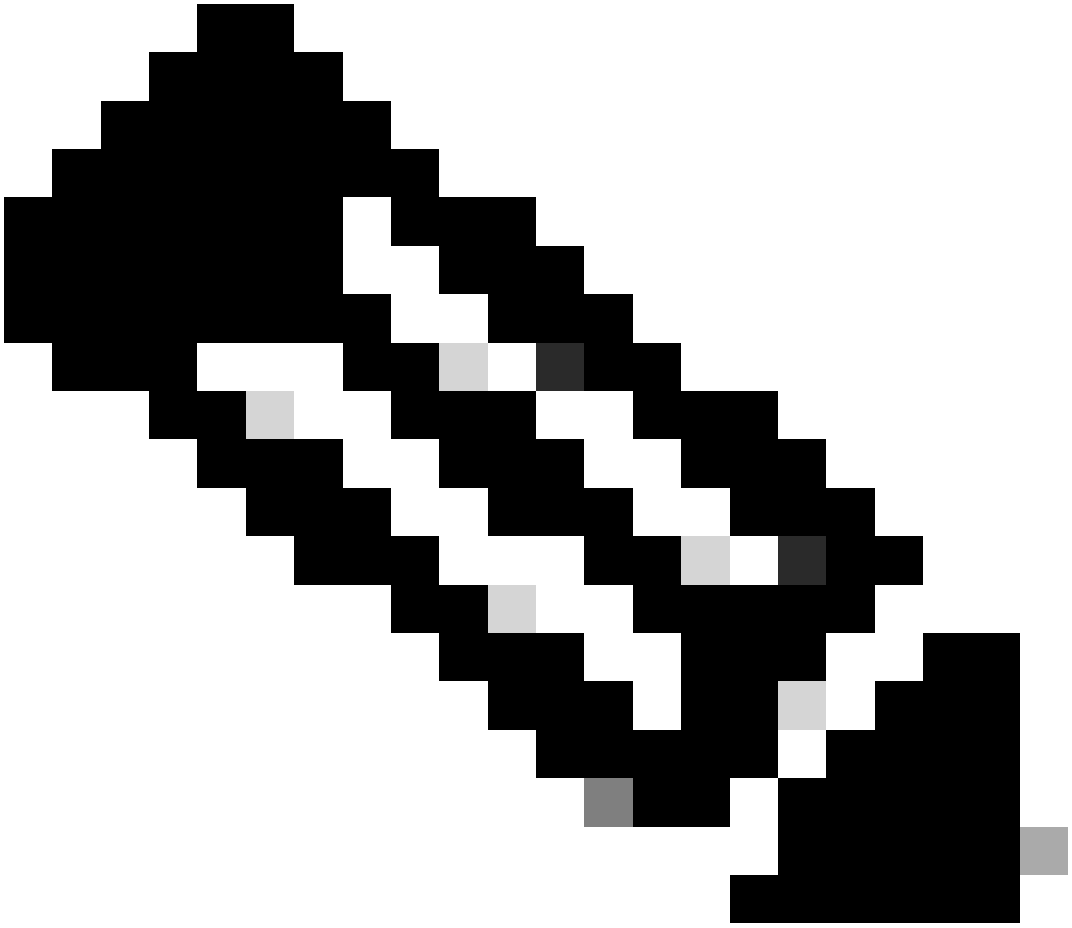
```
SW2# show system internal access-list vlan 10 input statistics slot 1 ======= INSTANCE 0x0 ----------
```

Vérification à l'aide d'Ethanalyzer

Une autre approche consiste à effectuer une capture de paquets, en filtrant spécifiquement le port UDP 3785.

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

La présence d'adresses IP source et de destination identiques dans les paquets capturés à partir du protocole BFD Echo est attendue, car ces paquets Echo proviennent du commutateur local lui-même.



Remarque : en l'absence de l'instruction « no bfd echo » sous l'interface, la capture révèle les paquets avec l'adresse IP source locale et l'adresse IP de destination voisine, ainsi que l'observation du contrôle BFD

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.