

Dépannage de la détection du transfert bidirectionnel dans Cisco IOS XE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Présentation de BFD](#)

[Modes de fonctionnement BFD](#)

[Résolution des problèmes BFD](#)

[BFD en baisse](#)

[Volets voisins BFD](#)

[Volets de voisinage dus à la perte de paquets](#)

[Volets de voisinage en raison de paramètres définis trop bas](#)

[BFD ne bascule pas lorsque le mode strict n'est pas configuré](#)

[Commandes show utiles](#)

[Afficher les détails du voisin BFD](#)

[Afficher le résumé BFD](#)

[Afficher les abandons BFD](#)

[Afficher l'historique des voisins BFD](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner les problèmes avec la détection de transfert bidirectionnel (BFD) dans Cisco IOS® XE.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel ou de logiciel spécifiques.

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.

Présentation de BFD

La détection de transfert bidirectionnel est un protocole de détection conçu pour fournir des temps de détection de défaillance du chemin de transfert rapide pour tous les types de supports, les encapsulations, les topologies et les protocoles de routage. En plus de la détection rapide des défaillances du chemin d'accès, BFD fournit une méthode de détection des défaillances cohérente pour les administrateurs réseau. Étant donné que l'administrateur réseau peut utiliser BFD pour détecter les défaillances du chemin de transfert à un taux uniforme, plutôt que les taux variables pour différents mécanismes Hello de protocole de routage, les profils et les plans réseau sont plus faciles et le temps de reconvergence est cohérent et prévisible.

Une paire de systèmes transmet périodiquement des paquets BFD sur chaque chemin entre les deux systèmes, et si un système arrête la réception de paquets BFD pendant suffisamment longtemps, un composant de ce chemin bidirectionnel particulier vers le système voisin est supposé avoir échoué. Dans certaines conditions, les systèmes peuvent négocier de ne pas envoyer de paquets BFD périodiques afin de réduire la surcharge. La réduction du nombre et de la fréquence des mises à jour peut toutefois avoir une incidence sur la sensibilité de la DFB.

L'image montre l'établissement de BFD dans un réseau simple avec deux routeurs configurés pour OSPF et BFD. Lorsque le protocole OSPF détecte un voisin (1), il envoie une requête au processus BFD local pour initier une session de voisinage BFD avec le routeur voisin OSPF (2). La session de voisinage BFD avec le routeur voisin OSPF est établie (3). La même progression est utilisée avec d'autres protocoles de routage lorsque BFD est activé.



Modes de fonctionnement BFD

Mode d'écho BFD : le mode d'écho est activé par défaut et s'exécute avec un BFD asynchrone. Il peut être désactivé sur un côté pour s'exécuter avec asymétrie ou sur les deux côtés d'un voisinage. Les paquets d'écho sont envoyés par le moteur de transfert et renvoyés le long du même chemin. Un paquet d'écho est défini avec une adresse source et de destination de l'interface elle-même, et un port UDP de destination de 3785. Le voisin renvoie l'écho à l'émetteur, ce qui réduit sa charge de traitement du paquet et augmente la sensibilité possible de BFD. En général, les échos ne sont pas transmis au plan de contrôle du voisin, afin de réduire les délais et la charge du processeur.

BFD Asynchronous Mode (Mode asynchrone BFD) : le mode asynchrone effectue le suivi de la disponibilité du voisin par l'échange de paquets de contrôle entre les deux voisins, ce qui

nécessite une configuration statique de BFD des deux côtés.

Résolution des problèmes BFD

BFD en baisse

Les messages BFD down log sont essentiels à l'isolation d'une session inactive. Il existe plusieurs causes différentes que l'on peut voir :

DETECT TIMER EXPIRED : le routeur ne reçoit plus de trafic de test d'activité BFD et expire.

ECHO FAILURE : le routeur ne reçoit plus d'écho BFD de l'autre côté.

RX DOWN : le routeur reçoit une notification de son voisin l'informant qu'il est en panne.

RX ADMINDOWN - BFD a été désactivé sur le périphérique voisin.

```
*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
```

Après confirmation de la raison pour laquelle la session BFD est interrompue et de la direction du problème, vous pouvez commencer à isoler les causes possibles :

- Panne de support unidirectionnelle
- Problèmes liés à la modification de la configuration
- BFD bloqué sur le chemin
- Défaillances du processeur ou du transfert sur un périphérique

Volets voisins BFD

Volets de voisinage dus à la perte de paquets

Les battements BFD fréquents peuvent souvent être dus à une liaison perdue qui entraîne la perte de paquets de contrôle BFD ou d'échos. S'il existe plusieurs raisons différentes d'interruption de session, cela indique davantage une perte de paquets.

```

*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

```

Pour isoler la perte de paquets, il est utile d'effectuer une capture de paquets intégrée de l'interface concernée.

Les commandes de base sont les suivantes :

```

surveillance capture <nom> interface <interface> <entrée|sortie|les deux>
monitor capture <name> match ipv4 protocol udp any any eq <3784|3785>

```

Vous pouvez également filtrer avec une liste d'accès pour faire correspondre les paquets de contrôle BFD et d'écho.

```

config t
ip access-list extended <ACLname>
permit udp any any eq 3784
permit udp any any eq 3785
tranche
surveillance capture <nom> interface <interface> <entrée|sortie|les deux>
monitor capture <name> access-list <ACLname>

```

Dans cet exemple, les captures sur l'interface entrante montrent que les paquets de contrôle BFD sont reçus de manière cohérente, mais que les échos sont intermittents. Des horodatages de 5 à 15 secondes, aucun paquet d'écho n'est renvoyé pour le système local 10.1.1.1. Cela indique une perte du routeur BFD vers son voisin.

```

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
```

Volets de voisinage en raison de paramètres définis trop bas

Sur les liaisons à faible vitesse, il est important de garder à l'esprit les paramètres BFD appropriés. Les valeurs d'intervalle et de réception minimale sont définies en millisecondes. Si le délai entre voisins est égal ou proche de ces valeurs, les délais normaux causés par les conditions de trafic déclenchent des flaps BFD. Par exemple, si le délai normal de bout en bout entre voisins est de 100 ms et que l'intervalle BFD est défini sur un minimum de 50 ms avec un multiplicateur de 3, un seul paquet BFD manqué déclencherait un événement de mise hors service du voisin, car les deux suivants sont toujours en transit.

Vous pouvez valider le délai pour le voisin via une simple requête ping entre les deux adresses IP voisines.

En outre, les minuteurs minimum pris en charge varient selon la plate-forme et doivent être confirmés avant la configuration BFD.

BFD ne bascule pas lorsque le mode strict n'est pas configuré

Il est important de noter que lorsque le mode strict BFD n'est pas activé, l'absence d'une session BFD n'empêche pas l'établissement du protocole de routage associé.

Cela peut permettre une nouvelle convergence dans des scénarios indésirables. Dans l'exemple,

BFD a réussi à arrêter le protocole BGP, mais comme la communication TCP réussit toujours, le voisin est rétabli.

```
*Mar 31 18:53:08.997: %BFD-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:BG
*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

Étant donné que le protocole BGP est actif avant le voisinage BFD, le réseau reconverge. Si le BFD reste inactif, la seule façon pour le voisin d'être inactif est lorsque le minuteur d'attente de deux minutes expire, ce qui retarde le basculement.

```
*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
```

Commandes show utiles

Afficher les détails du voisin BFD

Cette commande fournit des détails sur les voisins BFD configurés comme indiqué ci-dessous. Cela inclut tous les voisins indépendants de l'état actuel.

```
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	
Multiplieur: 3	- Length: 24
My Discr.: 4097	- Your Discr.: 4100
Min tx interval: 1000000	- Min rx interval: 1000000
Min Echo interval: 50000	

Champs clés :

Hôte de session	Ce champ indique si la session est hébergée dans un logiciel ou déchargée sur un matériel. Le déchargement matériel est disponible sur certaines plates-formes pour empêcher l'instabilité BFD due à l'encombrement du processeur.
MinTxInt/MinRxInt/Multiplicateur	Valeurs locales des intervalles et du multiplicateur d'émission et de réception minimaux.
MinRxInt reçu/Multiplicateur reçu	Valeurs d'homologue pour l'intervalle de réception minimal et le multiplicateur.
Nombre de Rx/Tx	Compteurs des paquets BFD envoyés et reçus.
Nombre D'Écho Rx/Tx	Compteurs pour les échos BFD envoyés et reçus.
Protocoles enregistrés	Protocole de routage utilisé par la session BFD.
Disponibilité	Durée de session
LD/RD	Discriminateur local et Discriminateur distant pour la session.
RH/RS	Entendu à distance et état distant

Afficher le résumé BFD

La commande show bfd summary fournit plusieurs sorties rapides des protocoles client actifs, des sessions de protocole IP ou des sessions BFD hébergées par matériel ou logiciel. Ces informations sont utiles lorsque la sortie de tous les détails est longue et complexe.

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

Afficher les abandons BFD

Cette commande affiche les paquets BFD abandonnés sur le périphérique local et la raison. Si les abandons locaux sont incrémentés, cela peut provoquer le basculement des sessions.

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

Afficher l'historique des voisins BFD

Cette commande affiche les journaux BFD récents pour chaque voisin, ainsi que son état actuel.

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 lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:16.816] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:15.886] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:14.920] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:14.023] Event: V1 FSM lId:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:13.060] Event: V1 FSM lId: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]
bfd_session_created, proc:OSPF, idb:GigabitEthernet3 handle:2 act

```

Informations connexes

- [Référence BFD Cisco IOS](#)
- [Guide de configuration BFD, Cisco IOS XE 17.x](#)
- [IETF RFC 5880 pour BFD](#)
- [Assistance technique de Cisco et téléchargements](#)

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.