

Risoluzione dei problemi di rilevamento dell'inoltro bidirezionale in Cisco IOS XE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica BFD](#)

[Modalità operative BFD](#)

[Risoluzione dei problemi relativi ai dati configurazione di avvio](#)

[BFD in basso](#)

[BFD Neighbor Flap](#)

[Flap del router adiacente a causa di perdita di pacchetti](#)

[Flag adiacenti dovuti a parametri impostati su un valore troppo basso](#)

[Failover Non Eseguito Quando Non È Configurata La Modalità Strict](#)

[Comandi Show](#)

[Mostra dettagli router adiacente BFD](#)

[Mostra riepilogo DCF](#)

[Mostra rilasci DCF](#)

[Mostra cronologia vicini DCF](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al rilevamento dell'inoltro bidirezionale (BFD) in Cisco IOS® XE.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Quanto riportato in questo documento non è limitato a versioni software o hardware specifiche.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

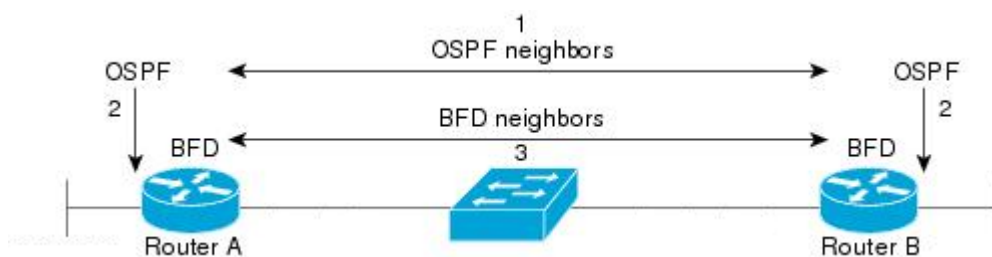
Panoramica BFD

BFD (Bidirectional Forwarding Detection) è un protocollo di rilevamento progettato per fornire tempi rapidi di rilevamento degli errori del percorso di inoltro per tutti i tipi di supporti, incapsulamenti, topologie e

protocolli di routing. Oltre al rilevamento rapido degli errori del percorso, il BFD fornisce un metodo coerente di rilevamento degli errori per gli amministratori di rete. Poiché l'amministratore di rete può utilizzare il BFD per rilevare gli errori dei percorsi di inoltra a una velocità uniforme, anziché le velocità variabili per i diversi meccanismi di hello dei protocolli di routing, i profili e i piani di rete sono più semplici e i tempi di riconversione sono coerenti e prevedibili.

Una coppia di sistemi trasmette periodicamente pacchetti BFD su ciascun percorso tra i due sistemi e, se un sistema interrompe la ricezione di pacchetti BFD per un periodo di tempo sufficiente, si presume che alcuni componenti del percorso bidirezionale specifico verso il sistema adiacente abbiano avuto un errore. In alcune condizioni, i sistemi possono negoziare di non inviare pacchetti BFD periodici al fine di ridurre il sovraccarico. La riduzione del numero e della frequenza degli aggiornamenti può tuttavia influire sulla sensibilità del BFD.

Nell'immagine viene mostrata la definizione del BFD in una rete semplice con due router configurati per OSPF e BFD. Quando OSPF individua un router adiacente (1), invia una richiesta al processo BFD locale per avviare una sessione BFD con il router adiacente OSPF (2). Viene stabilita la sessione BFD adiacente con il router adiacente OSPF (3). La stessa progressione viene usata con altri protocolli di routing quando è abilitato il BFD.



Modalità operative BFD

Modalità eco BFD: la modalità eco è attivata per impostazione predefinita ed è eseguita con un BFD asincrono. Può essere disattivato da un lato per funzionare in modo asimmetrico, o per funzionare da entrambi i lati di un vicinato. I pacchetti echo vengono inviati dal motore di inoltra e inoltrati nuovamente lungo lo stesso percorso. Un pacchetto echo viene impostato con un indirizzo di origine e di destinazione dell'interfaccia stessa e una porta UDP di destinazione di 3785. Il router adiacente riflette l'eco verso il mittente, riducendo al minimo il carico di elaborazione del pacchetto e aumentando la possibile sensibilità del BFD. In generale, gli echi non vengono inoltrati al control plane del router adiacente, al fine di ridurre i ritardi e il carico della CPU.

Modalità asincrona BFD: la modalità asincrona tiene traccia della disponibilità dei router adiacenti tramite lo scambio di pacchetti di controllo tra i due router adiacenti, che richiede la configurazione statica di BFD su entrambi i lati.

Risoluzione dei problemi relativi ai dati configurazione di avvio

BFD in basso

I messaggi di log di BFD inattivo sono fondamentali per l'isolamento di una sessione inattiva. Le cause possono essere diverse:

DETECT TIMER EXPIRED (TIMER RILEVATO SCADUTO) - Il router non riceve più il traffico keepalive BFD e scade il tempo di attesa.

ERRORE ECHO - Il router non riceve più gli echo BFD dall'altro lato.

RX DOWN - Il router riceve una notifica dal router adiacente che il router è guasto.

RX ADMINDOWN - BFD disabilitato sul dispositivo adiacente.

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

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

Dopo aver confermato il motivo per cui la sessione BFD viene interrotta e la direzionalità del problema, è possibile iniziare a isolare le possibili cause:

- Guasto del supporto unidirezionale
- Modifiche alla configurazione
- BFD bloccato nel percorso
- Errori di CPU o inoltro su un dispositivo

BFD Neighbor Flap

Flap del router adiacente a causa di perdita di pacchetti

I frequenti flap BFD possono essere causati spesso da un collegamento con perdita di segnale che causa la perdita di pacchetti di controllo BFD o di eco. Se vi sono più motivi di interruzione della sessione, ciò è più indicativo di una perdita di pacchetti.

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

Per isolare la perdita di pacchetti, è utile acquisire un pacchetto incorporato dell'interfaccia interessata. I comandi di base sono:

```
monitor capture <nome> interface <interfaccia> <in|out|both>  
monitor capture <name> corrisponde al protocollo ipv4 udp any eq <3784|3785>
```

È inoltre possibile filtrare i dati con un elenco degli accessi in modo che corrispondano sia al controllo BFD che ai pacchetti echo.

```
config t  
ip access-list extended <nomeACL>  
consenti udp qualsiasi eq 3784  
consenti udp qualsiasi eq 3785  
fine  
monitor capture <nome> interface <interfaccia> <in|out|both>  
monitor capture <name> access-list <ACLname>
```

In questo esempio, le clip sull'interfaccia in entrata mostrano che i pacchetti del controllo BFD vengono ricevuti coerentemente, ma gli echi sono intermittenti. Dai 5 secondi ai 15 secondi, non sono presenti pacchetti echo per il sistema locale 10.1.1.1 visto restituito. Ciò indicherebbe una perdita da parte del router BFD verso il router adiacente.

```
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

Flag adiacenti dovuti a parametri impostati su un valore troppo basso

Sui collegamenti a velocità inferiore, è importante prestare attenzione ai parametri BFD appropriati. I valori di intervallo e ricezione minima sono impostati in millisecondi. Se il ritardo tra i vicini è uguale o vicino a questi valori, i ritardi normali causati dalle condizioni del traffico attivano i BFD flap. Ad esempio, se il normale ritardo end-to-end tra router adiacenti è 100 ms e l'intervallo BFD è impostato su un minimo di 50 ms con un moltiplicatore di 3, un singolo pacchetto BFD perso attiverà un evento di mancato accesso per il router adiacente, poiché i due successivi sono ancora in transito.

È possibile convalidare il ritardo per il router adiacente tramite un semplice ping tra i due indirizzi IP adiacenti.

Inoltre, i timer minimi supportati variano a seconda della piattaforma e devono essere confermati prima della configurazione BFD.

Failover Non Eseguito Quando Non È Configurata La Modalità Strict

È importante notare che quando la modalità rigorosa BFD non è abilitata, l'assenza di una sessione BFD non impedisce la definizione del protocollo di routing associato.

Ciò può consentire una riconvergenza in scenari indesiderati. Nell'esempio, il BFD elimina il protocollo BGP, ma, poiché la comunicazione TCP continua a funzionare, il router adiacente ritorna in posizione.

```
*Mar 31 18:53:08.997: %BFDFSM-6-BFD_SESS_DOWN: BFD-SYSLOG: BFD session ld:4097 handle:1,is going Down Re
*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 fro
BGPpeer#
*Mar 31 18:53:09.000: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed, ld: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
```

Poiché BGP è attivo prima del vicinato BFD, la rete riconverge. Se il BFD rimane inattivo, l'unico modo per il router adiacente di essere disattivato è quando scade il timer di attesa di due minuti, che ritarda il failover.

```
*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, ld:4097 neigh proc
```

Comandi Show

Mostra dettagli router adiacente BFD

Questo comando fornisce i dettagli dei BFD adiacenti configurati, come descritto di seguito. Ciò include tutti i vicini indipendenti dallo stato corrente.

```
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

Campi chiave:

Host sessione	Questo campo specifica se la sessione è ospitata nel software o scaricata nell'hardware. L'offload hardware è disponibile su alcune piattaforme per prevenire l'instabilità BFD dovuta alla congestione della CPU.
MinTxInt/MinRxInt/Moltiplicatore	Valori locali per gli intervalli minimi di trasmissione e ricezione e moltiplicatore
MinRxInt/Moltiplicatore ricevuto	Valori peer per l'intervallo di ricezione minimo e il moltiplicatore
Conteggio Rx/Tx	Contatori dei pacchetti BFD inviati e ricevuti
Conteggio Rx/Tx Eco	Contatori per gli echi BFD inviati e ricevuti
Protocolli registrati	Protocollo di routing utilizzato dalla sessione BFD
Tempo di attività	Tempo di attività della sessione

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

Mostra cronologia vicini DCF

Con questo comando vengono visualizzati i registri BFD recenti per ogni router adiacente, insieme allo stato attuale.

```
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 ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:20.527] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:19.552] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:18.776] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:17.823] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:16.816] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:15.886] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:14.920] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:14.023] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:13.060] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:12.183] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:11.389] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:10.600] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:09.603] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:08.750] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:07.808] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:06.825] Event: V1 FSM ld:4101 handle:3 event:RX DOWN state:INIT
[Apr 4 15:56:05.877] Event: V1 FSM ld: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 ld:4101 handle:3	event:RX	DOWN	state:INIT
[Apr 4 15:56:03.920]	Event: V1 FSM ld: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 ld:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.803] Event: V1 FSM ld:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.784] Event: V1 FSM ld:104 handle:1 event:RX UP state:UP
[Apr 4 15:10:41.770] Event: notify client(CEF) IP:10.2.2.2, ld:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: notify client(EIGRP) IP:10.2.2.2, ld:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: notify client(CEF) IP:10.2.2.2, ld:104, handle:1, event:UP,
[Apr 4 15:10:41.770] Event: resetting timestamps ld:104 handle:1
[Apr 4 15:10:41.768] Event: V1 FSM ld:104 handle:1 event:RX INIT state:DOWN
[Apr 4 15:10:41.751] Event: V1 FSM ld: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, ld:4198, handle:2,	event:UP,		

```
[Apr 4 15:26:01.779] Event: notify client(OSPF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
[Apr 4 15:26:01.778] Event: V1 FSM ld:4198 handle:2 event:RX UP state:UP
[Apr 4 15:26:01.777] Event: notify client(OSPF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
[Apr 4 15:26:01.777] Event: V1 FSM ld:4198 handle:2 event:RX INIT state:DOWN
[Apr 4 15:26:01.776] Event: V1 FSM ld: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 ld: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 ld:4198 handle:2 event:RX UP state:UP
[Apr 4 15:22:48.911] Event: notify client(CEF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
[Apr 4 15:22:48.911] Event: notify client(OSPF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
[Apr 4 15:22:48.911] Event: notify client(CEF) IP:10.3.3.2, ld:4198, handle:2, event:UP,
IPv4 Sessions
NeighAddr          LD/RD          RH/RS          State          Int
[Apr 4 15:22:48.911] Event: V1 FSM ld:4198 handle:2 event:RX INIT state:DOWN
[Apr 4 15:22:48.910] Event: V1 FSM ld:4198 handle:2 event:Session create state:DOWN
[Apr 4 15:22:48.909]
bfd_session_created, proc:OSPF, idb:GigabitEthernet3 handle:2 act
```

Informazioni correlate

[Guida di riferimento al BFD di Cisco IOS](#)

[Guida alla configurazione del BFD, Cisco IOS XE 17.x](#)

[IETF RFC 580 per BFD](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).