Fehlerbehebung bei der Erkennung von bidirektionalen Weiterleitungen in Cisco IOS XE

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Probleme mit Bidirectional Forwarding Detection (BFD) in Cisco IOS® XE beheben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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.

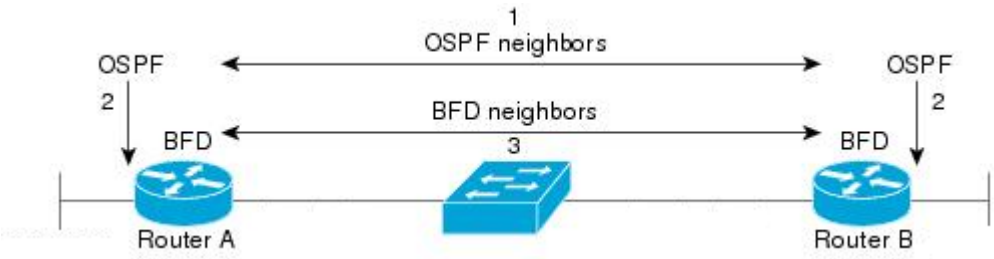
BFD - Übersicht

BFD (Bidirectional Forwarding Detection; bidirektionale Weiterleitungserkennung) ist ein Erkennungsprotokoll, das entwickelt wurde, um eine schnelle Erkennung von Weiterleitungspfadausfällen

für alle Medientypen, Kapselungen, Topologien und Routing-Protokolle zu ermöglichen. Zusätzlich zur schnellen Erkennung von Weiterleitungspfadausfällen bietet BFD Netzwerkadministratoren eine konsistente Fehlererkennungsmethode. Da der Netzwerkadministrator Weiterleitungspfadausfälle mit einheitlicher Geschwindigkeit und nicht mit variablen Raten für verschiedene Hello-Mechanismen der Routing-Protokolle erkennen kann, sind Netzwerkprofile und -pläne einfacher, und die Rekonvergenzzeit ist konsistent und vorhersehbar.

Ein Systempaar überträgt periodisch BFD-Pakete über jeden Pfad zwischen den beiden Systemen. Wenn ein System den Empfang von BFD-Paketen lange genug unterbricht, wird angenommen, dass eine Komponente dieses bidirektionalen Pfads zum benachbarten System ausgefallen ist. Unter bestimmten Bedingungen können Systeme aushandeln, keine periodischen BFD-Pakete zu senden, um den Overhead zu reduzieren. Die Reduzierung der Anzahl und Häufigkeit von Updates kann sich jedoch auf die Empfindlichkeit von BFD auswirken.

Das Bild zeigt die BFD-Einrichtung in einem einfachen Netzwerk mit zwei für OSPF und BFD konfigurierten Routern. Wenn OSPF einen Nachbarn (1) erkennt, sendet es eine Anforderung an den lokalen BFD-Prozess, um eine BFD-Nachbarsitzung mit dem OSPF-Nachbarrouter (2) zu initiieren. Die BFD-Nachbarsitzung mit dem OSPF-Nachbarrouter wird eingerichtet (3). Derselbe Verlauf wird bei aktiviertem BFD mit anderen Routing-Protokollen verwendet.



BFD-Betriebsmodi

BFD-Echomodus - Der Echomodus ist standardmäßig aktiviert und wird mit asynchronem BFD ausgeführt. Es kann auf einer Seite deaktiviert werden, um mit Asymmetrie zu laufen, oder auf beiden Seiten einer Nachbarschaft laufen. Echo-Pakete werden von der Weiterleitungs-Engine gesendet und über denselben Pfad zurückgeleitet. Ein Echo-Paket wird mit einer Quell- und Zieladresse der Schnittstelle selbst und einem UDP-Zielport von 3785 festgelegt. Der Nachbar reflektiert das Echo zurück zum Ausgangspunkt, wodurch die Prozesslast des Pakets minimiert und die mögliche Empfindlichkeit von BFD erhöht wird. Im Allgemeinen werden Echos nicht an die Steuerungsebene des Nachbarn weitergeleitet, um Verzögerungen und CPU-Last zu reduzieren.

BFD Asynchronous Mode (Asynchroner BFD-Modus): Der asynchrone Modus verfolgt die Verfügbarkeit des Nachbarn durch den Austausch von Steuerungspaketen zwischen den beiden Nachbarn, was eine statische Konfiguration von BFD auf beiden Seiten erfordert.

Fehlerbehebung bei BFD-Problemen

BFD Down

BFD-Downlog-Meldungen sind für die Isolierung einer Ausfallsitzung von entscheidender Bedeutung. Es gibt mehrere verschiedene Ursachen, die erkennbar sind:

DETECT TIMER EXPIRED - Der Router empfängt keinen BFD-Keepalive-Datenverkehr mehr und gibt keine Zeitüberschreitung mehr aus.

ECHO-FEHLER - Der Router empfängt seine BFD-Echos nicht mehr von der anderen Seite.

RX DOWN - Der Router erhält eine Benachrichtigung von seinem Nachbarn, dass er ausgefallen ist.

RX ADMINDOWN - BFD wurde auf dem benachbarten Gerät deaktiviert.

```
*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,
```

Nach Bestätigung des Grundes, aus dem die BFD-Sitzung abgebrochen wurde, und der Richtung des Problems können Sie beginnen, mögliche Ursachen zu isolieren:

- Einweg-Medienfehler
- Konfigurationsänderungen
- BFD im Pfad blockiert
- CPU- oder Weiterleitungsfehler auf einem Gerät

BFD Neighbor Flaps

Flaps beim Nachbarn aufgrund von Paketverlust

Häufige BFD-Flaps können durch einen Verbindungsverlust verursacht werden, bei dem BFD-Steuerungspakete oder Echos verloren gehen. Wenn mehrere Gründe für den Ausfall einer Sitzung vorliegen, ist dies eher ein Hinweis auf einen Paketverlust.

```
*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
```

Um einen Paketverlust zu isolieren, ist es hilfreich, eine eingebettete Paketerfassung der betreffenden Schnittstelle zu verwenden. Die grundlegenden Befehle sind:

monitor capture <Name> interface <Schnittstelle> <Eingang|Ausgang|beide>
monitor capture <name> match ipv4 protocol udp any any any eq <3784|3785>

Sie können auch anhand einer Zugriffsliste filtern, um sowohl BFD-Steuerungs- als auch Echo-Pakete abzugleichen.

config t
ip access-list extended <ACLname>
permit udp any eq 3784
permit udp any eq 3785
Ende
monitor capture <Name> interface <Schnittstelle> <Eingang|Ausgang|beide>
monitor capture <Name> access-list <ACLname>

In diesem Beispiel zeigen Erfassungen an der Eingangsschnittstelle, dass BFD-Steuerungspakete konsistent empfangen werden, Echos jedoch unregelmäßig auftreten. Es wurden keine Echopakete für das lokale System 10.1.1.1 zurückgegeben, die zwischen dem 5-Sekunden- und dem 15-Sekunden-Zeitstempel liegen. Dies würde auf einen Verlust des BFD-Routers gegenüber seinem Nachbarn hinweisen.

```
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
```

Nachbarklappen aufgrund zu niedriger Parameter

Bei Verbindungen mit geringerer Geschwindigkeit ist es wichtig, auf geeignete BFD-Parameter zu achten. Intervall und minimale Empfangswerte werden in Millisekunden festgelegt. Wenn die Verzögerung zwischen Nachbarn diesen Wert erreicht oder nahezu erreicht, lösen normale Verzögerungen durch Verkehrsbedingungen BFD-Flaps aus. Wenn beispielsweise die normale End-to-End-Verzögerung zwischen Nachbarn 100 ms beträgt und das BFD-Intervall mit einem Multiplikator von 3 auf das Minimum von 50 ms festgelegt wird, löst ein einzelnes verpasstes BFD-Paket ein "Neighbor Down"-Ereignis aus, da die nächsten beiden Pakete noch übertragen werden.

Sie können die Verzögerung für den Nachbarn durch einen einfachen Ping zwischen den beiden benachbarten IP-Adressen validieren.

Darüber hinaus variieren die unterstützten Timer pro Plattform und müssen vor der BFD-Konfiguration bestätigt werden.

BFD schlägt nicht fehl, wenn kein strikter Modus konfiguriert ist

Wenn der strikte BFD-Modus nicht aktiviert ist, verhindert das Fehlen einer BFD-Sitzung nicht die Einrichtung des zugehörigen Routing-Protokolls.

Dies kann eine erneute Konvergenz in unerwünschten Szenarien ermöglichen. In diesem Beispiel wird BGP erfolgreich abgebrochen. Da die TCP-Kommunikation jedoch erfolgreich bleibt, wird der Nachbar wieder aktiviert.

```
*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
```

Da BGP vor der BFD-Nachbarschaft eingerichtet wurde, wird das Netzwerk neu konvergiert. Wenn BFD ausgefallen bleibt, kann der Nachbar nur nach Ablauf des zweiminütigen Haltezeitgebers ausgefallen sein,

wodurch sich das Failover verzögert.

```
*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 fro
*Mar 31 18:59:01.541: %BFD-6-BFD_SESS_DESTROYED: BFD-SYSLOG: bfd_session_destroyed,  ld:4097 neigh proc:
```

Nützliche Show-Befehle

Details zum BFD-Nachbar anzeigen

Dieser Befehl stellt Details zu den konfigurierten BFD-Nachbarn bereit, wie unten beschrieben. Dies schließt alle Nachbarn unabhängig vom aktuellen Zustand ein.

```
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
```

Schlüsselfelder:

Sitzungshost	In diesem Feld wird angegeben, ob die Sitzung in einer Software gehostet oder auf Hardware ausgelagert wird. Auf einigen Plattformen ist Hardware-Offload verfügbar, um BFD-Instabilitäten aufgrund von CPU-Überlastung zu vermeiden.
MinTxInt/MinRxInt/Multiplikator	Lokale Werte für minimale Sende- und Empfangsintervalle und Multiplikator
Empfangener MinRxInt/Empfangener Multiplikator	Die Peer-Werte für das minimale Empfangsintervall und den Multiplikator
Rx/Tx-Anzahl	Zähler der gesendeten und empfangenen BFD-Pakete

Echo-Rx/Tx-Anzahl	Zähler für gesendete und empfangene BFD-Echos
Registrierte Protokolle	Von der BFD-Sitzung verwendetes Routing-Protokoll
Betriebszeit	Sitzungsverfügbarkeit
LD/RD	Lokaler Diskriminator und Remote-Diskriminator für die Sitzung
RH/RS	Remote-Heard und Remote-State

BFD-Zusammenfassung anzeigen

Der Befehl **show bfd summary** bietet mehrere Schnellausgaben der aktiven Clientprotokolle, IP-Protokollsitzungen oder Hardware- bzw. Software-gehosteten BFD-Sitzungen. Diese Informationen sind nützlich, wenn die Ausgabe der vollständigen Details lang und schwerfällig ist.

```
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
```

BFD-Drops anzeigen

Dieser Befehl zeigt die BFD-Pakete an, die auf dem lokalen Gerät verworfen wurden, und den Grund dafür. Wenn lokale Drops inkrementiert werden, kann dies zu Flapping-Ereignissen in den Sitzungen führen.

```
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_L
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
```

BFD-Nachbarschaftsverlauf anzeigen

Dieser Befehl zeigt aktuelle BFD-Protokolle für jeden Nachbarn sowie dessen aktuellen Status an.

```
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
```

Zugehörige Informationen

Cisco IOS BFD-Referenz

BFD-Konfigurationsleitfaden, Cisco IOS XE 17.x

IETF RFC 5880 für BFD

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.