Configurazione e verifica della funzionalità BFD sugli switch Nexus 9000

Sommario

Introduzione

In questo documento viene descritto come configurare e verificare le sessioni BFD (Bidirectional Forwarding Detection) su switch Cisco Nexus basati su NXOS®.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Rilevamento inoltro bidirezionale (BFD)
- Software Nexus NX-OS.

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

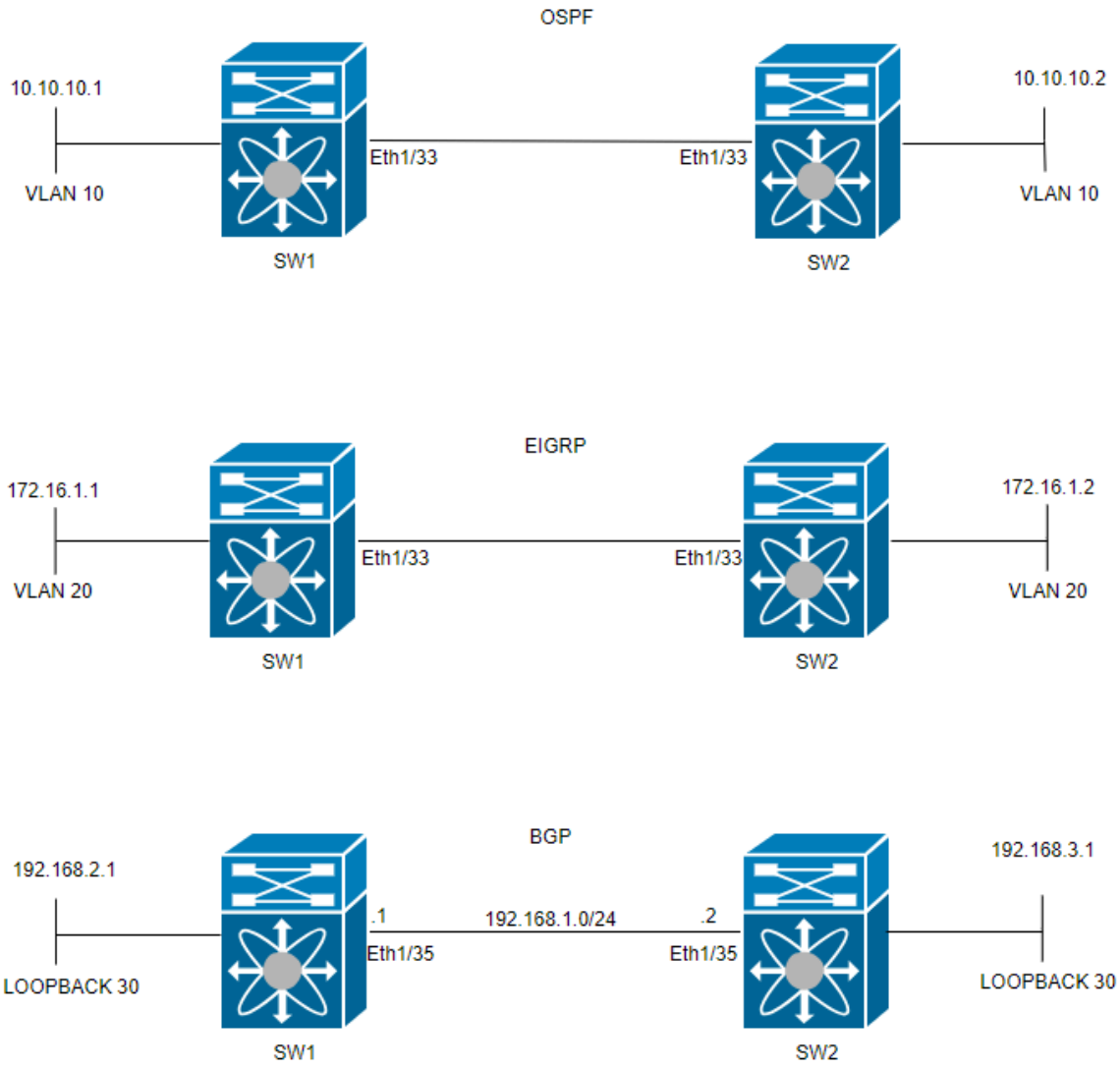
Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Nexus 9000 con NXOS versione 10.3(4a).M.

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.

Configurazione

Esempio di rete



Configurazione

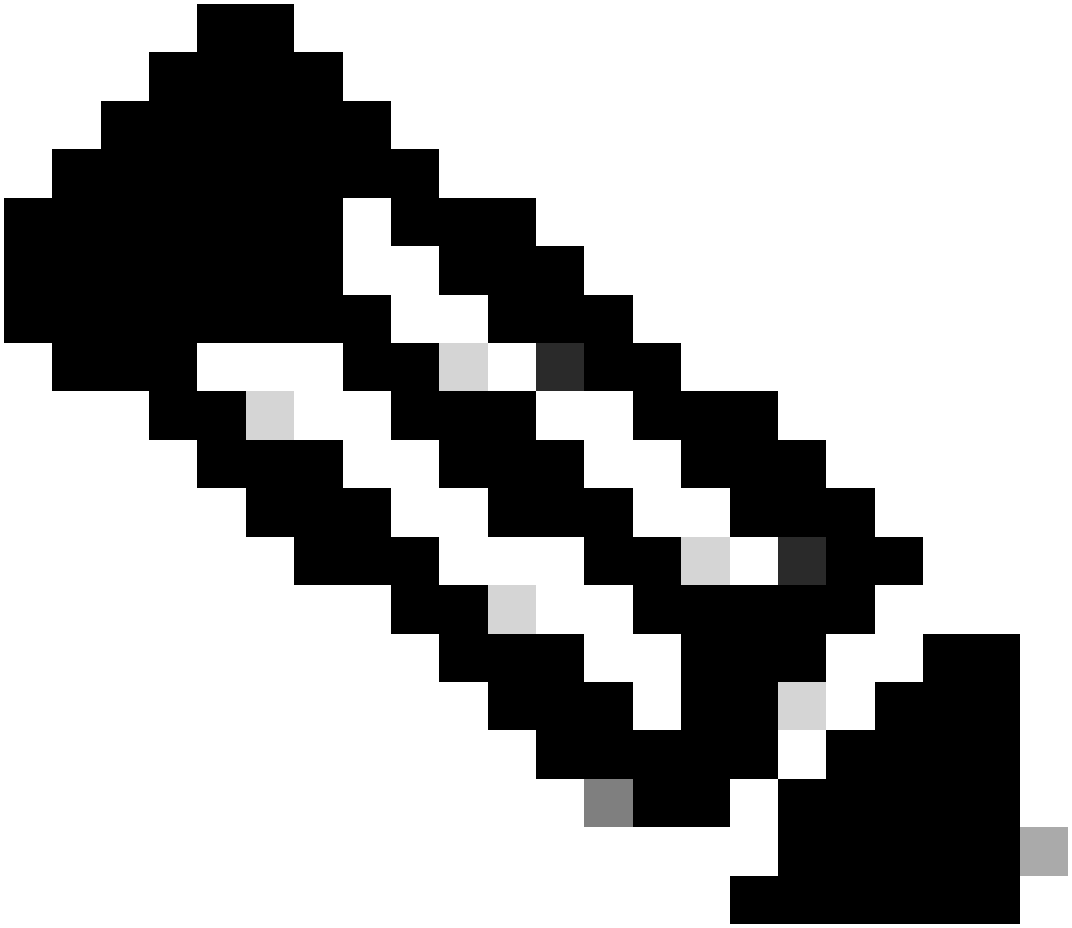
Lo scopo della configurazione del BFD è quello di rilevare e comprendere le differenze tra le configurazioni dei vari protocolli di routing.

PASSAGGIO 1: Prima di poter configurare il BFD su un'interfaccia e un protocollo, è necessario abilitare la funzione BFD.

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

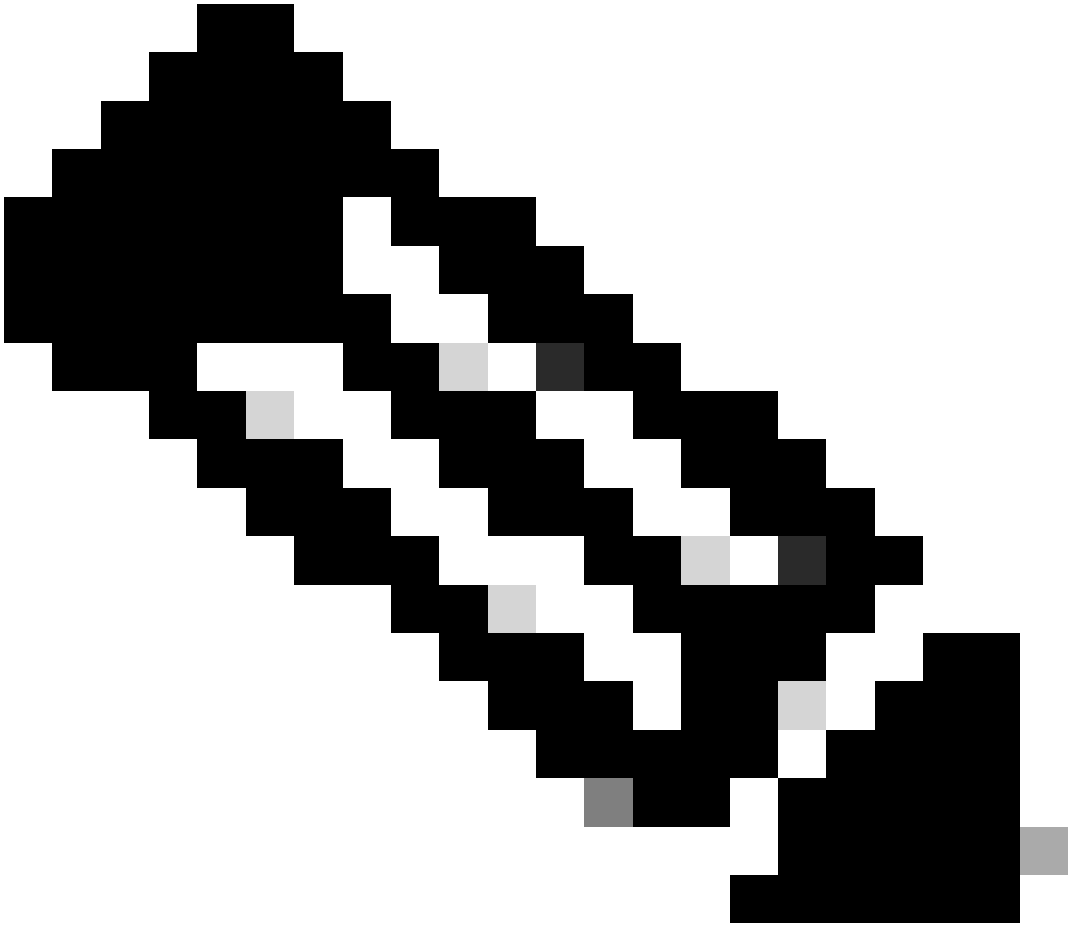
PASSO 2: Configurazione di BFD globale

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

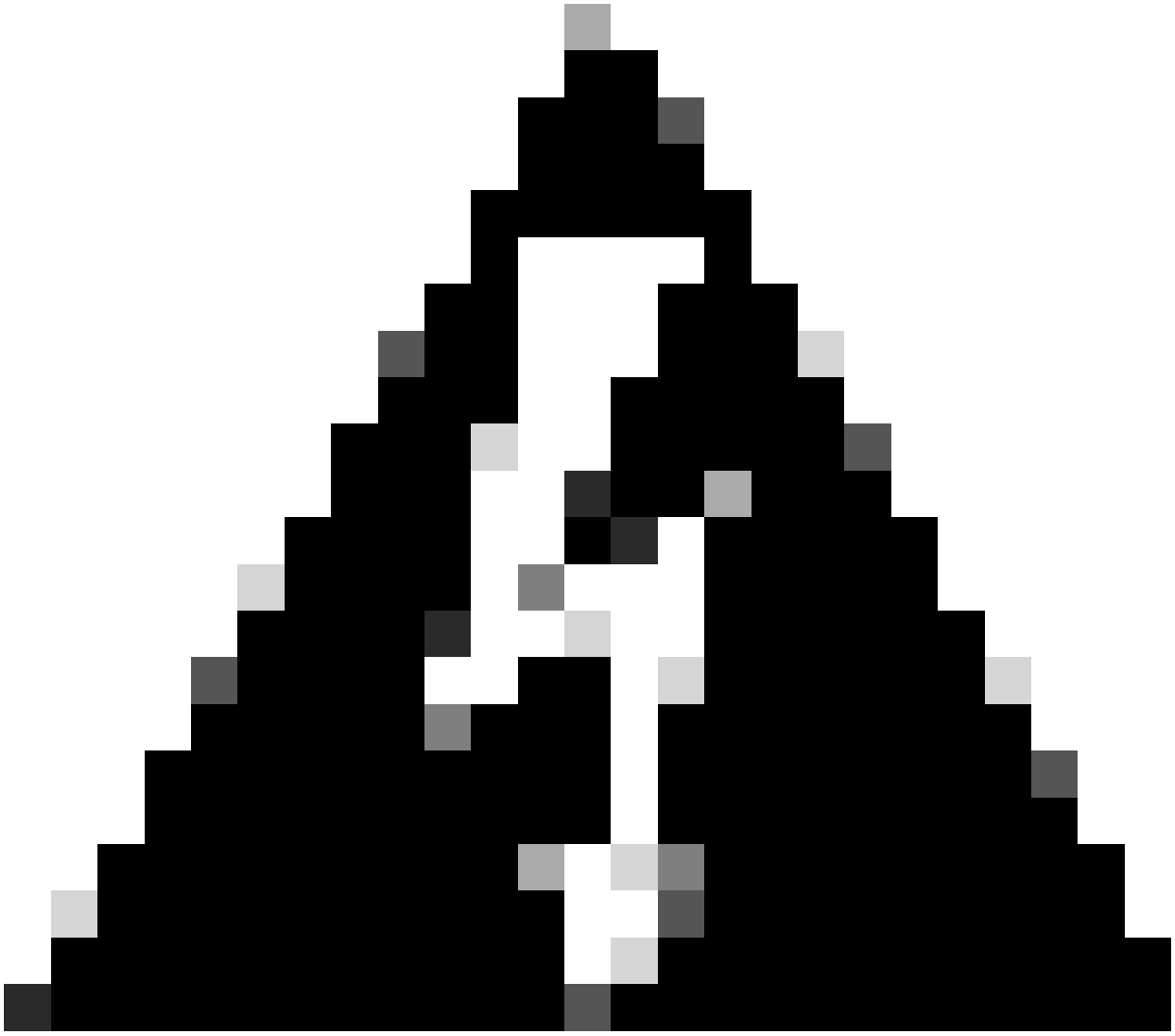


Nota: l'intervallo min_tx e msec è compreso tra 50 e 999 millisecondi e il valore predefinito è 50. L'intervallo del moltiplicatore è compreso tra 1 e 50. Il valore predefinito del moltiplicatore è 3.

PASSAGGIO 3: Configurazione di BFD su un'interfaccia



Nota: è possibile configurare i parametri della sessione BFD per tutte le sessioni BFD su un'interfaccia.



Avviso: verificare che i messaggi di reindirizzamento ICMP (Internet Control Message Protocol) siano disabilitati sulle interfacce abilitate per BFD. Usare il comando no ip redirects o il comando no ipv6 redirects sull'interfaccia.

SWITCH 1	SWITCH 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

La modalità asincrona BFD è come un handshake tra due dispositivi per mantenere elevata la connessione. La configurazione viene eseguita su entrambi i dispositivi e, una volta attivata, i due dispositivi iniziano a scambiarsi messaggi speciali a un'ora prestabilita. Questi messaggi hanno alcune impostazioni importanti, ad esempio la frequenza con cui vengono inviati e la velocità con cui un dispositivo può rispondere all'altro. È

inoltre disponibile un'impostazione che consente di stabilire il numero di messaggi non ricevuti necessari affinché un dispositivo possa rendersi conto della presenza di un problema nella connessione.

La funzione echo BFD invia i pacchetti di prova a un router adiacente e li restituisce per verificare la presenza di problemi senza coinvolgere il router adiacente nell'inoltro dei pacchetti. Può utilizzare un timer più lento per ridurre il traffico dei pacchetti di controllo e verificare il percorso di inoltro sul sistema adiacente senza disturbare il router adiacente, rendendo il rilevamento più veloce. Se entrambi i vicini utilizzano la funzione echo, non vi è asimmetria.

Motivi per la non disponibilità dei pacchetti Syslog

- Path Down: indica che il percorso di inoltro tra i due BFD adiacenti non è più operativo, probabilmente a causa di congestione della rete, errori hardware o altri problemi.

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

- Funzione echo non riuscita: errore della funzione echo, una funzione del BFD in cui vengono inviati e ricevuti i pacchetti echo per verificare la connettività. Se i pacchetti non vengono trasmessi o ricevuti correttamente, è possibile che si sia verificato un problema.

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

- Sessione segnalata router adiacente inattiva: il dispositivo adiacente segnala che la sessione BFD è inattiva, in genere a causa del rilevamento di un problema sul dispositivo stesso e della fine della connessione.

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

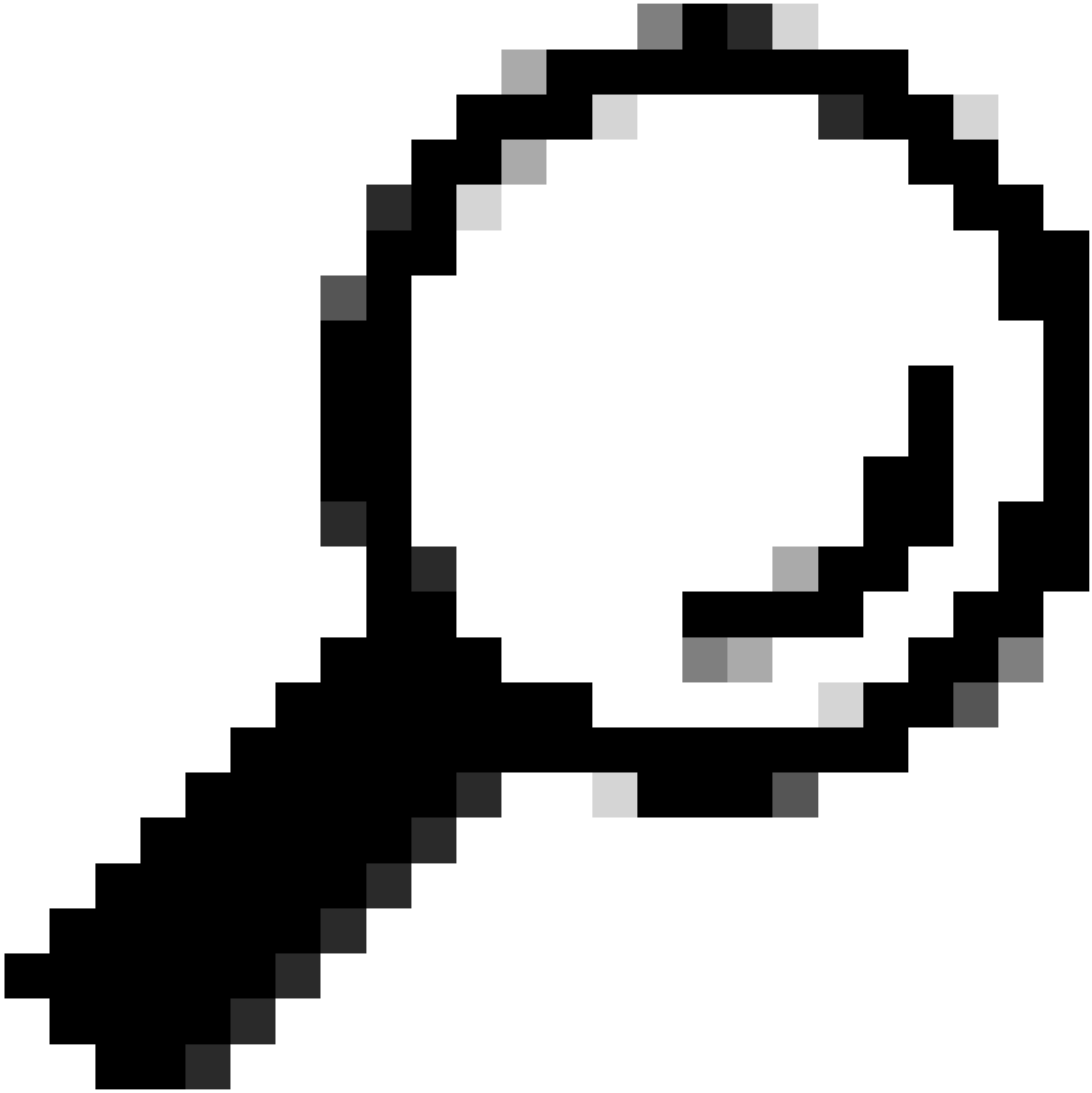
- Tempo scaduto rilevamento controllo: questo si verifica quando il timer di rilevamento controllo scade prima di ricevere una risposta prevista dal router adiacente, che indica un potenziale problema con la connessione.

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

- Inattività amministrativa: la sessione BFD viene interrotta intenzionalmente da un amministratore, a scopo di manutenzione o a causa di modifiche alla configurazione.

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

Configurazione di BFD sui protocolli di routing



Suggerimento: quando il BFD è abilitato in OSPF, diventa attivo per tutte le interfacce che utilizzano OSPF. Le interfacce adottano i valori configurati globalmente. Se è necessario regolare questi valori, fare riferimento al punto 3, "Configurazione BFD su un'interfaccia".

SWITCH 1	SWITCH 2

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

Può inoltre abilitare il BFD nell'interfaccia OSPF con il comandoip ospf bfd

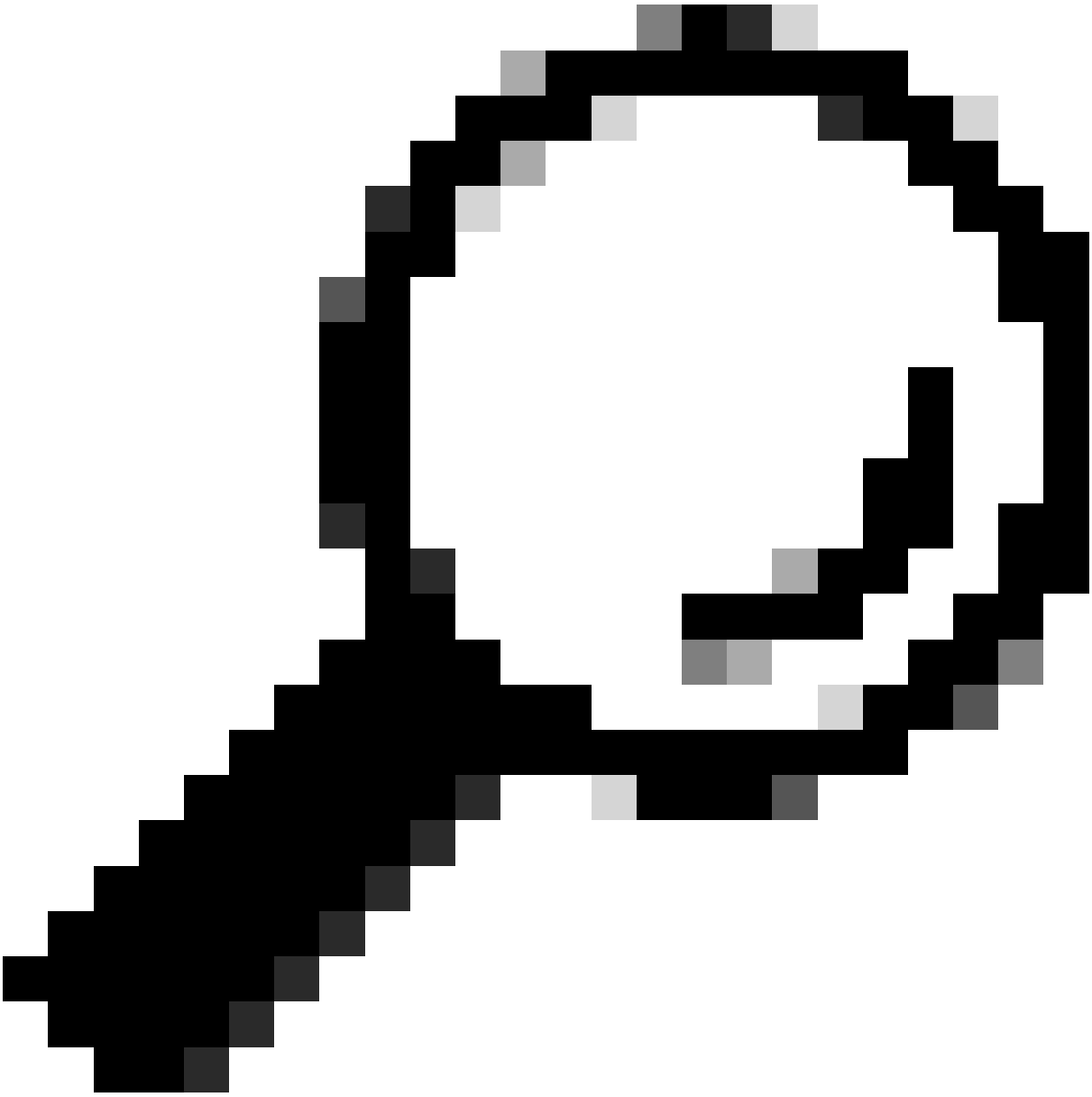
SWITCH 1	SWITCH 2
SW1(config)# interface vlan 10 SW1(config-if)# ip ospf bfd	SW2(config)# interface vlan 10 SW2(config-if)# ip ospf bfd

Configurazioni di esempio per BFD su OSPF

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

Configurazione di BFD su EIGRP

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



Suggerimento: quando il BFD è abilitato in EIGRP, diventa attivo per tutte le interfacce che usano EIGRP. Le interfacce adottano i valori configurati globalmente. Se è necessario regolare questi valori, fare riferimento al punto 3, "Configurazione BFD su un'interfaccia".

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

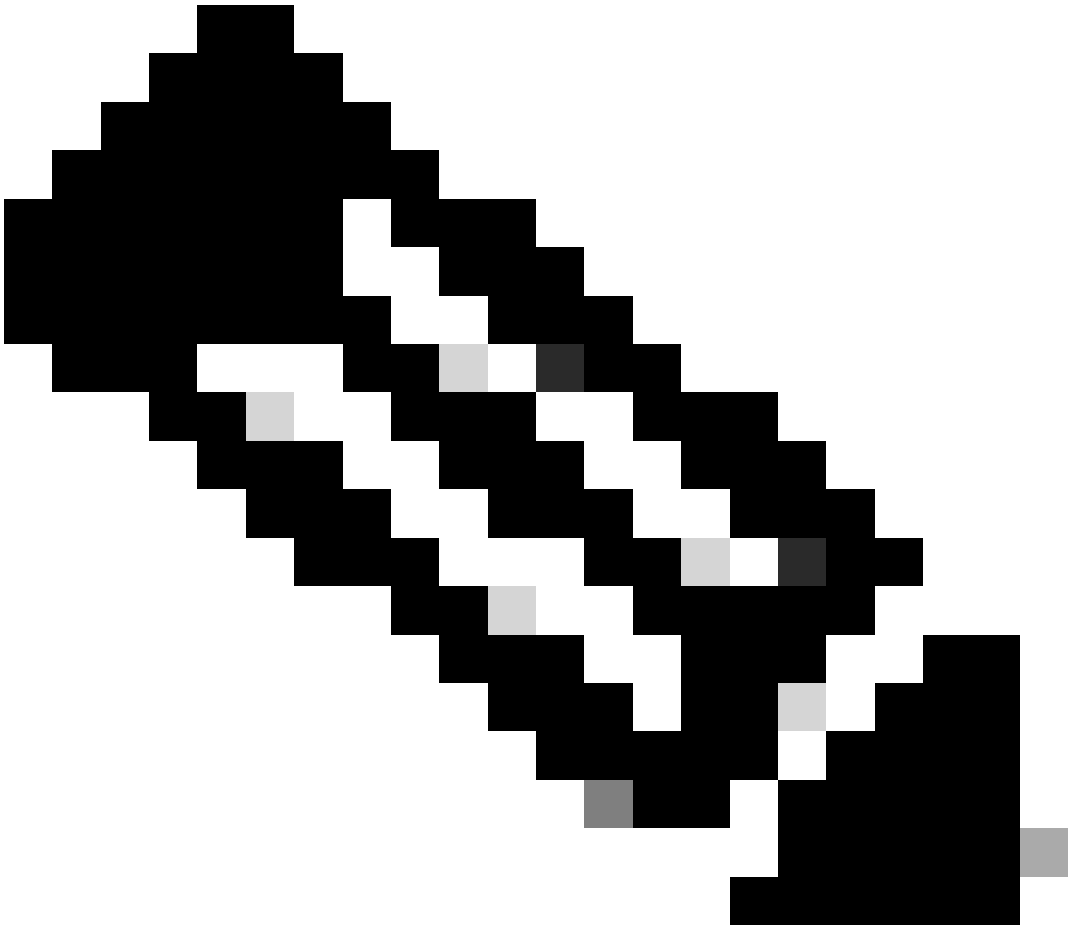
Inoltre, può abilitare il BFD su un'interfaccia EIGRP con il comandoip eigrp instance-tag bfd

SWITCH 1	SWITCH 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

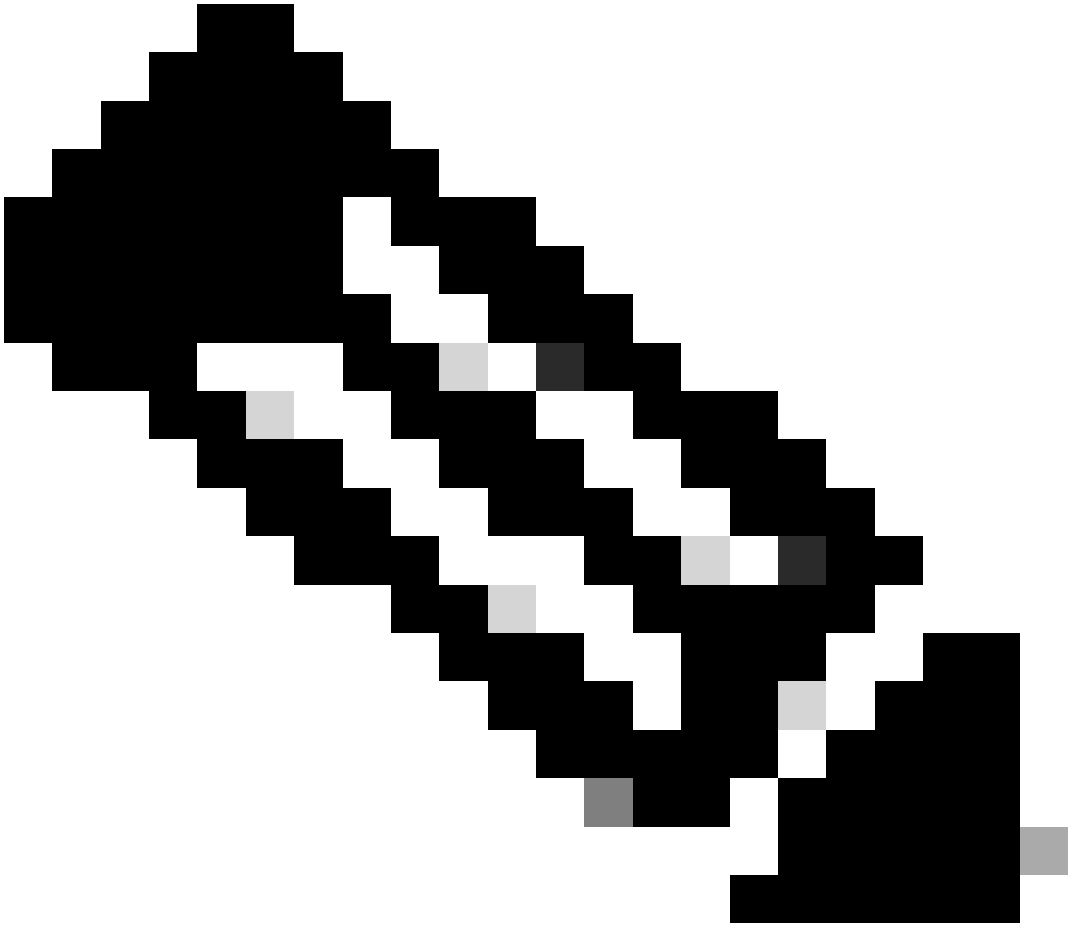
Configurazioni di esempio per BFD su EIGRP

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

Configurazione di BFD su BGP



Nota: la funzione di aggiornamento dell'origine facilita le sessioni BGP nell'utilizzare l'indirizzo IP primario di un'interfaccia designata come indirizzo locale durante la definizione di una sessione BGP con un router adiacente. Consente inoltre a BGP di registrarsi come client con BFD.



Nota: quando si configurano sessioni BFD sul dispositivo, il tipo di sessione viene determinato specificando 'multihop' o 'single hop'. Se non viene specificata alcuna parola chiave, il tipo di sessione viene impostato per impostazione predefinita su 'single hop' quando il peer è connesso direttamente. Se il peer non è connesso, il tipo di sessione predefinito è 'multihop'.

SWITCH 1	SWITCH 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

Configurazioni di esempio per BFD su BGP

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

Verifica

Dopo aver configurato il BFD e averlo associato a un protocollo come OSPF, EIGRP o BGP, i BFD adiacenti devono essere identificati automaticamente. Per verificare questa condizione, utilizzare il comando:

```
show bfd neighbors
```

On Switch 1

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

On Switch 2

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

Per verificare e ottenere un output dettagliato, utilizzare il comando:

```
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
```

Verifica tramite dettagli sessione

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

Verifica tramite Access-list

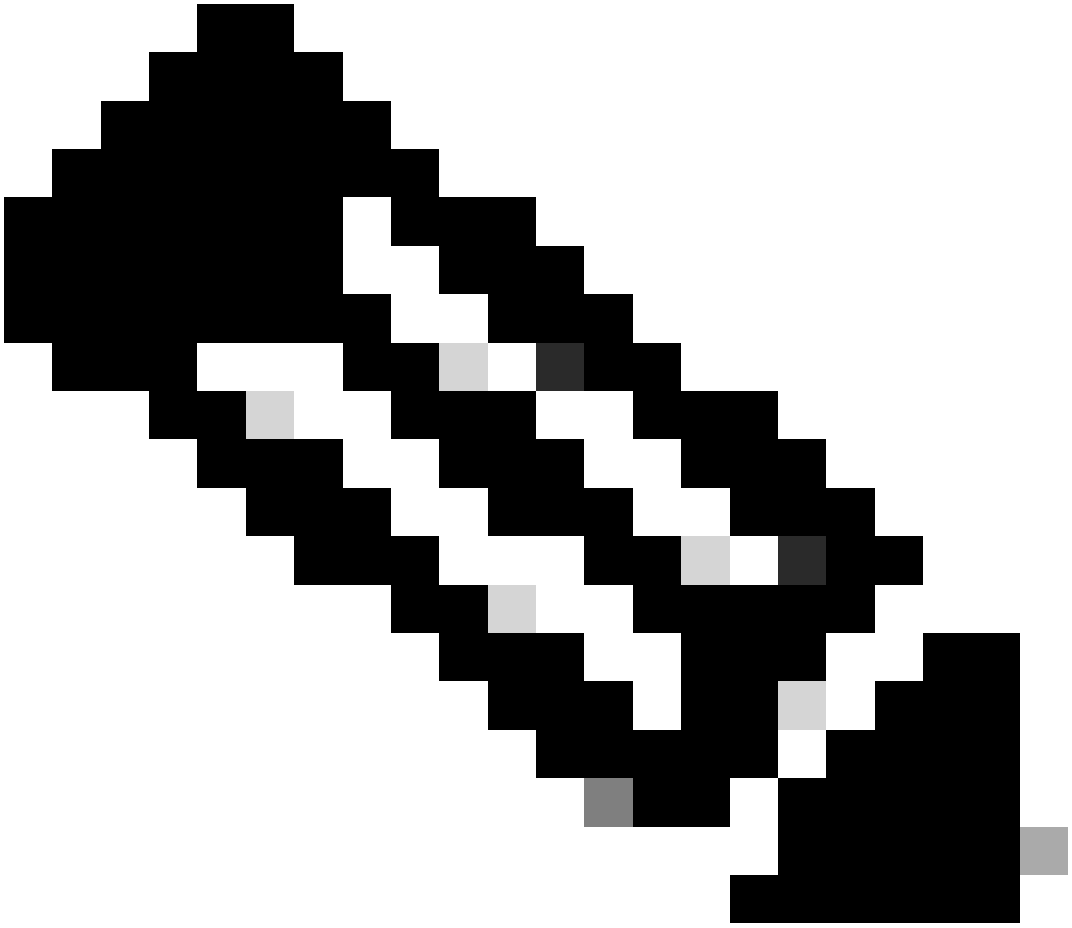
```
SW2# show system internal access-list vlan 10 input statistics slot 1 ======= INSTANCE 0x0 ----------
```

Verifica con Ethanalyzer

Un approccio alternativo consiste nell'eseguire un'acquisizione dei pacchetti, filtrando specificamente la porta UDP 3785.

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

Ci si aspetta che i pacchetti acquisiti dal protocollo Echo BFD contengano indirizzi IP di origine e destinazione identici, in quanto i pacchetti Echo provengono dallo switch locale stesso.



Nota: in assenza dell'istruzione 'no bfd echo' nell'interfaccia, l'acquisizione rivela i pacchetti con l'indirizzo IP di origine locale e l'indirizzo IP di destinazione adiacente, insieme all'osservazione del controllo BFD

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

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).