Risoluzione dei problemi comuni del protocollo EIGRP

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi più comuni relativi al protocollo Enhanced Interior Gateway Routing Protocol (EIGRP).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

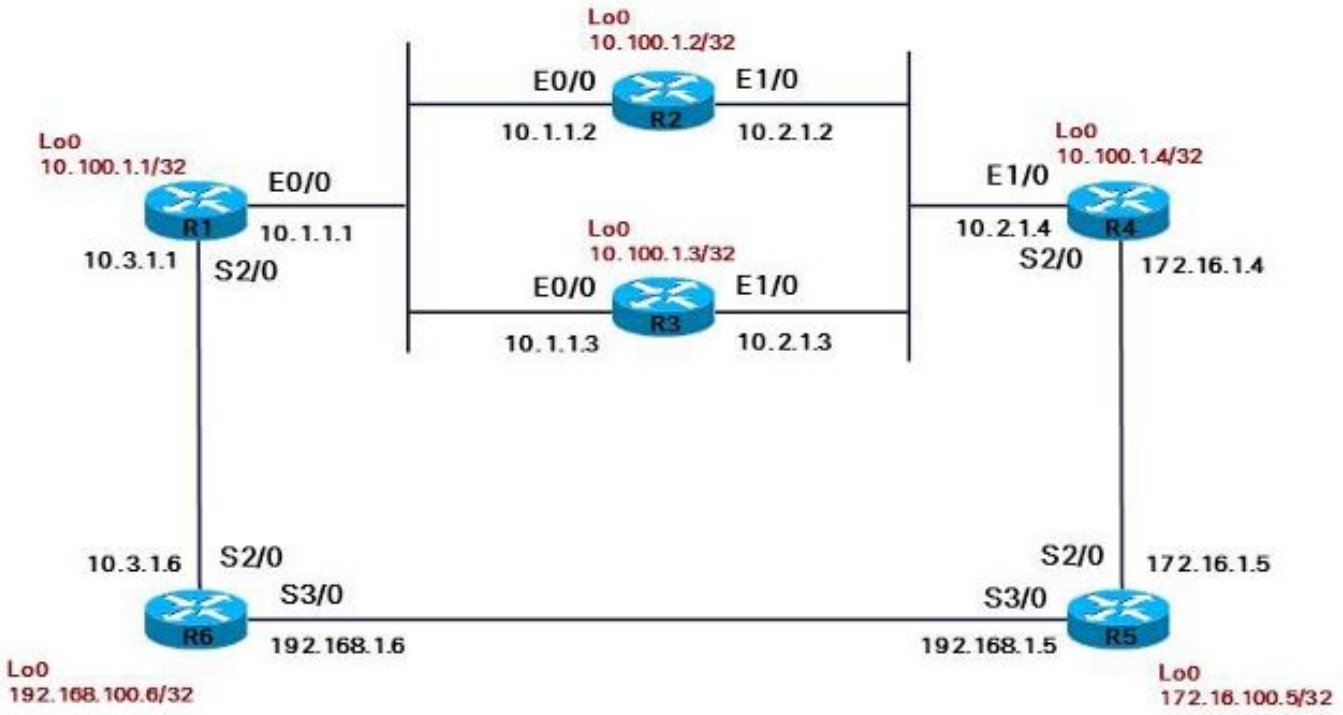
Componenti usati

Le informazioni di questo documento si basano su Cisco IOS® per illustrare i vari comportamenti che possono verificarsi con questo protocollo.

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.

Premesse

Questa è la topologia utilizzata nel presente documento:



Le sezioni seguenti descrivono alcuni dei problemi EIGRP più comuni e alcuni consigli per risolverli.

Instabilità del router vicino

Il problema più comune che si verifica con il protocollo EIGRP riguarda il collegamento con i router vicini. Le cause possono essere diverse:

- Problema dell'unità massima di trasmissione, o MTU (Maximum Transmission Unit)
- Comunicazione unidirezionale (collegamenti unidirezionali)
- Problema multicast sul collegamento
- Problemi unicast
- Problemi di qualità del collegamento
- Problemi di autenticazione
- Problemi di configurazione errata

Per visualizzare il router vicino, occorre ricevere un messaggio Hello del protocollo EIGRP. Immettere il comando show ip eigrp neighbors per visualizzare le informazioni sui router vicini e identificare il problema:

<#root>

```
R2#
```

show ip eigrp neighbors

```
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
```

```
3   10.1.1.1                Et0/0             12 00:00:48    1  5000

1

  0
2   10.1.1.3                Et0/0             12 02:47:13   22   200  0  339
1   10.2.1.4                Et1/0             12 02:47:13   24   200  0  318
0   10.2.1.3                Et1/0             12 02:47:13   20   200  0  338
```

Se si ritiene che il router adiacente sia stato formato, ma non si dispone dei prefissi che è necessario imparare dal router adiacente, controllare l'output del comando precedente: Se il conteggio Q è sempre diverso da zero, potrebbe essere un'indicazione del fatto che gli stessi pacchetti EIGRP vengono ritrasmessi continuamente. Immettere il comando show ip eigrp neighbors detail per verificare se viene inviato sempre lo stesso pacchetto. Se il numero di sequenza del primo pacchetto rimane invariato, lo stesso pacchetto viene ritrasmesso continuamente:

<#root>

```
R2#

show ip eigrp neighbors detail



IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Et0/0             11

00:00:08

    1  4500

1

  0
   Version 12.4/1.2, Retrans: 2, Retries: 2, Waiting for Init, Waiting for Init Ack
    UPDATE seq 350 ser 0-0 Sent 8040 Init Sequenced
2   10.1.1.3                Et0/0             11 02:47:56   22   200  0  339
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 10
1   10.2.1.4                Et1/0             10 02:47:56   24   200  0  318
   Version 12.4/1.2, Retrans: 10, Retries: 0, Prefixes: 8
0   10.2.1.3                Et1/0             11 02:47:56   20   200  0  338
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 2
```

L'output mostra un problema nel primo router il cui valore Uptime è stato azzerato.

È importante verificare che per il router EIGRP di processo sia specificato il comando eigrp log-neighbor-changes. In questo caso, tuttavia, il comando non compare nella configurazione, in quanto è stato incluso per impostazione predefinita a partire dall'ID bug Cisco CSCdx67706. Controllare la voce nei log di entrambi i router EIGRP vicini su ciascun lato del collegamento. In almeno uno dei registri deve essere presente una voce significativa.

Di seguito sono riportate alcune cause possibili che comportano una modifica del router EIGRP vicino e le relative voci di log:

- Non sono stati ricevuti pacchetti EIGRP durante il tempo di attesa:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 holding time expired
```

- Un pacchetto EIGRP affidabile non è stato riconosciuto per il numero di tentativi impostato:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 retry limit exceeded
```

- Il protocollo EIGRP vede l'interfaccia in stato down:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.3.1.6 (Serial2/0) is down:
 interface down
```

- Il router ha ricevuto un pacchetto Update iniziale e ha riavviato la ricerca dei router vicini:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 peer restarted
```

- Il router ha ricevuto un pacchetto Update iniziale e ha formato una nuova adiacenza:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is up:
 new adjacency
```

- È stato immesso il comando clear ip eigrp neighbor, che ha comportato un processo di eliminazione manuale delle relazioni stabilite con i router vicini:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.1.4 (Serial2/0) is down:
 manually cleared
```

- L'indirizzo IP dell'interfaccia è stato modificato:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.1.5 (Serial3/0) is down:
 address changed
```

- È stato modificato il valore del ritardo o della larghezza di banda dell'interfaccia:

> Nota: questo problema si verifica solo nelle versioni precedenti del codice. Non si verifica alcuna instabilità sui router vicini dopo l'ID bug Cisco CSCdp08764.

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.3.1.6 (Serial2/0) is down:
 metric changed
```

- I valori K non sono configurati correttamente oppure si è verificato un arresto normale:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.4.1.5 (Ethernet1/0) is down:
 K-value mismatch
```

- Si verifica un arresto normale:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 Interface Goodbye received
```

- Sull'interfaccia è stato configurato il comando ip authentication mode eigrp 1 md5:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.3 (Ethernet0/0) is down:
 authentication mode changed
```

- Si è verificato un riavvio normale/NSF (Non-Stop Forwarding):

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (FastEthernet1) is resync:
 peer graceful-restart
```

- I router vicini che non hanno risposto alle query loro inviate vengono disattivati:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.1.16 (Serial3/0) is down:
 stuck in active
```

Problemi di rete

Un problema di rete può essere causato da:

- Stato SIA (Stuck-In-Active)
- Timer di attesa scaduto
- Limite di tentativi superato
- Riavvio del peer
- Il pacchetto Update iniziale precede il pacchetto Hello

SIA

Fare riferimento alla sezione SIA di questo documento.

Timer di attesa scaduto

La scadenza del timer di attesa indica che il router non ha ricevuto alcun pacchetto EIGRP (né un pacchetto Hello né altri pacchetti EIGRP) durante il tempo di attesa. In questo caso, è molto probabile che si sia verificato un problema sul collegamento.

Verificare che i pacchetti Hello del protocollo EIGRP su questo collegamento vengano ricevuti dal router e inviati dall'altro lato del collegamento. Usare il comando debug eigrp packet hello a tale scopo. In alternativa al comando debug, eseguire il ping dell'indirizzo IP 224.0.0.10 e verificare se il router vicino risponde. Il problema multicast sul collegamento può essere dovuto a problemi di interfaccia, ad esempio i pacchetti Hello potrebbero essere bloccati da uno switch intermedio.

Per verificare la causa del problema, provare a usare un altro protocollo con un indirizzo IP multicast diverso. Ad esempio, è possibile configurare il protocollo Routing Information Protocol (RIP) versione 2 che usa l'indirizzo IP multicast 224.0.0.9.

Limite di tentativi superato

Il limite di tentativi superato indica che il pacchetto EIGRP, anche se affidabile, non è stato riconosciuto molte volte. I pacchetti EIGRP affidabili sono:

- Update
- Query
- Reply
- SIA-Query
- SIA-Reply

Il pacchetto EIGRP affidabile viene ritrasmesso almeno 16 volte. La frequenza di trasmissione è determinata dal timeout di ritrasmissione, o RTO (Retransmit Time Out), un valore che può essere compreso tra 200 ms e 5.000 ms. Il valore RTO aumenta o diminuisce in modo dinamico osservando la differenza temporale tra il momento in cui il pacchetto EIGRP affidabile viene inviato e il momento in cui ne viene confermato l'arrivo. Se la ricezione del pacchetto non è confermata, il valore RTO aumenta. Se il problema persiste, il valore RTO aumenta rapidamente

fino a cinque secondi, quindi il limite di tentativi può diventare 16 x 5 secondi = 80 secondi. Tuttavia, se il tempo di attesa del protocollo EIGRP è superiore a 80 secondi, il router vicino rimane attivo finché il tempo di attesa non si esaurisce. È la situazione che si verifica sui collegamenti WAN lenti in cui, ad esempio, il tempo di attesa predefinito è 180 secondi.

Nei collegamenti con tempi di attesa inferiori a 80 secondi, se il tempo di attesa non scade, è mantenuto attivo dal pacchetto Hello del protocollo EIGRP. Il limite di tentativi potrebbe quindi essere superato, segnalando la presenza di un problema MTU o unicast. I pacchetti EIGRP Hello sono piccoli; il (primo) pacchetto di aggiornamento EIGRP può avere una MTU massima. Se il numero di prefissi è sufficiente per completare l'aggiornamento, è possibile che le dimensioni della MTU siano complete. Il router adiacente può essere appreso tramite la ricezione dei pacchetti EIGRP Hello, ma l'adiacenza completa non riesce se il pacchetto EIGRP Update non viene riconosciuto.

In genere, questo è l'output visualizzato:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 retry limit exceeded
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is up:
 new adjacency
```

Nota: a partire dall'ID bug Cisco CSCsc72090, il protocollo EIGRP usa anche le impostazioni MTU IP dell'interfaccia. Prima di applicare questa correzione, i pacchetti EIGRP verrebbero frammentati se l'MTU dell'IP fosse configurata con un valore inferiore a 1500. Questo problema si può verificare in genere nelle reti DMVPN (Dynamic Multipoint VPN).

Una seconda possibilità è che i pacchetti EIGRP Hello lo facciano perché sono multicast all'indirizzo IP 24.0.0.10. Alcuni pacchetti di aggiornamento EIGRP possono farlo, in quanto possono essere multicast. Tuttavia, i pacchetti EIGRP affidabili vengono sempre ritrasmessi in modalità unicast. Se il percorso dati unicast al router vicino è interrotto, il pacchetto affidabile ritrasmesso non viene elaborato correttamente. Per verificarlo, eseguire il ping dell'indirizzo IP unicast del router vicino (con la dimensione del ping impostata alla dimensione MTU massima del collegamento e con il bit Do Not Fragment (DF-bit) impostato).

Anche un collegamento unidirezionale può causare questo problema. Il router EIGRP può ricevere i pacchetti EIGRP Hello, ma i pacchetti inviati da questo router adiacente non passano attraverso il collegamento. Se i pacchetti Hello non vengono inviati correttamente, il router non può conoscerne la causa. Impossibile riconoscere i pacchetti di aggiornamento EIGRP inviati.

I pacchetti EIGRP affidabili o il pacchetto di conferma ricezione possono danneggiarsi. Per verificare rapidamente questa situazione, eseguire un comando ping abilitando la conferma della risposta:

<#root>

```
R1#
```

ping

```
Protocol [ip]:
Target IP address: 10.1.1.2
Repeat count [5]: 10
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
```

Validate reply data? [no]: yes

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
Reply data will be validated
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/24/152 ms
```

Abilitare il comando debug eigrp packets per verificare almeno la trasmissione e la ricezione dei pacchetti Hello e dei pacchetti Update del protocollo EIGRP:

<#root>

```
R1#
```

debug eigrp packets ?

```
  SIAquery  EIGRP SIA-Query packets
  SIAreply  EIGRP SIA-Reply packets
  ack       EIGRP ack packets
  hello     EIGRP hello packets
  ipxsap    EIGRP ipxsap packets
  probe     EIGRP probe packets
  query     EIGRP query packets
  reply     EIGRP reply packets
  request   EIGRP request packets
  retry     EIGRP retransmissions
  stub      EIGRP stub packets
  terse     Display all EIGRP packets except Hellos
  update    EIGRP update packets
  verbose   Display all EIGRP packets
```

Ecco un esempio tipico di limite di tentativi superato:

<#root>

```
R2#
show ip eigrp neighbors


IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Et0/0             12 00:00:48    1  5000
1

  0
2   10.1.1.3                Et0/0             12 02:47:13   22   200  0  339
1   10.2.1.4                Et1/0             12 02:47:13   24   200  0  318
0   10.2.1.3                Et1/0             12 02:47:13   20   200  0  338
```

Nota: nella coda sono sempre presenti uno o più pacchetti (Q Cnt).

<#root>

```
R2#
show ip eigrp neighbors detail


IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Et0/0             10 00:00:59    1
5000



1

  0
   Version 12.4/1.2,
Retrans: 12
, Retries: 12,
Waiting for Init, Waiting for Init Ack



UPDATE seq 349
 ser 0-0 Sent 59472 Init Sequenced
2   10.1.1.3                Et0/0             11 02:47:23   22   200  0  339
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 10
1   10.2.1.4                Et1/0             11 02:47:23   24   200  0  318
   Version 12.4/1.2, Retrans: 10, Retries: 0, Prefixes: 8
0   10.2.1.3                Et1/0             10 02:47:23   20   200  0  338
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 2
```

Come mostrato nell'output, R2 attende il primo pacchetto di aggiornamento (init bit set) dal router adiacente all'indirizzo IP 10.1.1.1.

In questo output successivo, R2 attende la conferma del primo pacchetto di aggiornamento (init bit set) dal router adiacente all'indirizzo IP 10.1.1.1.

Nota: l'RTO è al massimo di 5.000 ms, il che indica che i pacchetti affidabili EIGRP non vengono riconosciuti entro i cinque secondi.

<#root>

```
R2#
```

show ip eigrp neighbors detail

```
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Et0/0             11 00:01:17    1
```

5000

1

```
  0
   Version 12.4/1.2,
```

Retrans: 16

```
, Retries: 16,
```

Waiting for Init, Waiting for Init Ack

UPDATE seq 349

```
 ser 0-0 Sent 77844 Init Sequenced
2   10.1.1.3                Et0/0              12 02:47:42   22   200  0  339
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 10
1   10.2.1.4                Et1/0              10 02:47:42   24   200  0  318
   Version 12.4/1.2, Retrans: 10, Retries: 0, Prefixes: 8
0   10.2.1.3                Et1/0              11 02:47:42   20   200  0  338
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 2
```

Il numero di ritrasmissioni aumenta costantemente. Nella coda (seq 349) è presente sempre lo stesso pacchetto. Dopo che R2 ha inviato lo stesso pacchetto 16 volte, il router vicino diventa inattivo:

```
R2#
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 retry limit exceeded
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is up:
 new adjacency
```

Il processo inizia di nuovo:

<#root>

```
R2#
```

show ip eigrp neighbors detail

```
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
3   10.1.1.1                Et0/0             11 00:00:08    1  4500  1  0
   Version 12.4/1.2, Retrans: 2, Retries: 2, Waiting for Init, Waiting for Init Ack
    UPDATE seq 350 ser 0-0 Sent 8040 Init Sequenced
2   10.1.1.3                Et0/0             11 02:47:56   22   200  0  339
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 10
1   10.2.1.4                Et1/0             10 02:47:56   24   200  0  318
   Version 12.4/1.2, Retrans: 10, Retries: 0, Prefixes: 8
0   10.2.1.3                Et1/0             11 02:47:56   20   200  0  338
   Version 12.4/1.2, Retrans: 11, Retries: 0, Prefixes: 2
```

L'output del comando debug eigrp packets terse mostra che R2 continua a inviare lo stesso pacchetto:

Nota: il valore retry aumenta, il valore Flags è 0x1 e il bit Init è impostato.

<#root>

```
R2#
```

debug eigrp packets terse

```
EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)

R2#
EIGRP: Sending UPDATE on Ethernet0/0 nbr 10.1.1.1,
```

retry 14

,

RTO 5000

AS 1,

```
Flags 0x1

, Seq 350/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
EIGRP: Sending UPDATE on Ethernet0/0 nbr 10.1.1.1,

retry 15

,

RTO 5000


 AS 1,

Flags 0x1

, Seq 350/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
```

Il tempo di attesa non scade perché i pacchetti Hello vengono inviati e ricevuti correttamente:

```
<#root>

R2#

debug eigrp packets hello


EIGRP Packets debugging is on
    (HELLO)

EIGRP: Received HELLO on Ethernet0/0 nbr 10.1.1.1
  AS 1, Flags 0x0, Seq 0/0 idbQ 0/0
```

Riavvio del peer

Se viene ripetutamente visualizzato peer restarted su un router, il router riceve i pacchetti Update iniziali dal router vicino: Prestare attenzione al Flag 1 nei pacchetti Update ricevuti.

```
<#root>

R2#

debug eigrp packets terse



EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)

R2#
EIGRP: Received Sequence TLV from 10.1.1.1
       10.1.1.2
       address matched
      clearing CR-mode
EIGRP: Received CR sequence TLV from 10.1.1.1, sequence 479
EIGRP: Received UPDATE on Ethernet0/0 nbr 10.1.1.1
```

```
  AS 1, Flags 0xA, Seq 479/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0,
   not in CR-mode, packet discarded
EIGRP: Received UPDATE on Ethernet0/0 nbr 10.1.1.1
  AS 1,
```

Flags 0x1

```
, Seq 478/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
```

peer restarted

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is up:
 new adjacency
EIGRP: Enqueueing UPDATE on Ethernet0/0 nbr 10.1.1.1 iidbQ un/rely 0/1
 peerQ un/rely 0/0
```

Il pacchetto Update iniziale precede il pacchetto Hello

In questo esempio, il pacchetto Update iniziale viene ricevuto prima del pacchetto Hello:

```
EIGRP: Received UPDATE on Ethernet0/0 nbr 10.1.1.2
  AS 1, Flags 0x1, Seq 3/0 idbQ 0/0
EIGRP: Neighbor(10.1.1.2) not yet found
```

Se si verifica questo problema dopo un problema di instabilità del router vicino, il comportamento può essere considerato normale. Tuttavia, se la frequenza con cui si verifica il problema aumenta, vuol dire che la trasmissione unicast sul collegamento è operativa mentre la trasmissione multicast è interrotta. In altre parole, il router riceve il pacchetto Update unicast, ma non i pacchetti Hello.

Altri problemi

Altri tipi di problemi:

- Modifiche alla configurazione
- Problemi di autenticazione
- Mancata corrispondenza tra gli indirizzi IP principale e secondario
- Problemi DMVPN

Questi problemi vengono spiegati più dettagliatamente nelle sezioni seguenti.

Modifiche alla configurazione

 Nota: i risultati dei comandi utilizzati in questa sezione sono gli stessi se si configura invece

---

la negazione (il comando no).

Quando si configura l'istruzione di riepilogo, o auto-summary, sull'interfaccia, sul router viene visualizzato il seguente messaggio:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.3 (Ethernet0/0) is resync:
 summary configured
```

Ecco un esempio di configurazione global distribute-list per il processo EIGRP:

<#root>

```
R1(config-router)#
```

distribute-list 1 out

```
R1(config-router)#
```

Sul router viene visualizzato questo messaggio:

Nota: la stessa situazione si verifica quando si configura una lista di distribuzione <> anche in.

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.3 (Ethernet0/0) is resync:
 route configuration changed
```

Tutti i router EIGRP vicini diventano inattivi quando si configura interface distribute-list per il processo EIGRP:

```
R1(config-router)#distribute-list 1 out ethernet 0/0
```

In questo caso, il reset riguarda solo i router EIGRP vicini sull'interfaccia.

Nota: dopo l'ID bug Cisco CSCdy20284, le risorse adiacenti non vengono reimpostate per le modifiche manuali come il riepilogo e i filtri.

Autenticazione

L'autenticazione potrebbe mancare o essere configurata in modo errato. Il router EIGRP vicino potrebbe quindi diventare inattivo per superamento del limite di tentativi. Usare il comando debug eigrp packets per controllare se il problema dipende dall'autenticazione Message Digest 5 (MD5):

<#root>

```
R1#
debug eigrp packets



EIGRP Packets debugging is on
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
     SIAREPLY)

EIGRP: Ethernet0/0: ignored packet from 10.1.1.3, opcode = 1 (missing
 authentication or key-chain missing)
```

Mancata corrispondenza tra gli indirizzi IP principale e secondario

Il protocollo EIGRP invia il pacchetto Hello e tutti gli altri pacchetti dall'indirizzo IP principale. I pacchetti vengono accettati dall'altro router se gli indirizzi IP di origine rientrano nell'intervallo di indirizzi IP principali o in uno degli intervalli di indirizzi IP secondari dell'interfaccia. In caso contrario, viene visualizzato questo messaggio di errore (con eigrp log-neighbor-warnings abilitato):

```
IP-EIGRP(Default-IP-Routing-Table:1): Neighbor 10.1.1.2 not on common subnet
 for Ethernet0/0
```

DMVPN

Controllare se sono presenti problemi IPSec nelle reti DMVPN. IPSec può causare l'instabilità del protocollo EIGRP se la crittografia non è pulita:

<#root>

```
 show crypto ipsec sa


   protected vrf:
   local  ident (addr/mask/prot/port):  (10.10.110.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port):  (10.10.101.1/255.255.255.255/47/0)
   current_peer: 144.23.252.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 190840467, #pkts encrypt: 190840467, #pkts digest 190840467
    #pkts decaps: 158102457, #pkts decrypt: 158102457, #pkts verify 158102457
```

```
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 5523, #recv errors 42
```

Spiegazione dei flag

Nell'intestazione del pacchetto EIGRP è presente un campo Flags a 32 bit di cui è utile conoscere i vari valori.

- Flag 0x1 Init bit

  Questo flag è impostato nel pacchetto Update iniziale.

  <#root>

  ```
  EIGRP: Received UPDATE on Ethernet0/0 nbr 10.1.1.1
   AS 1,
  Flags 0x1
  , Seq 478/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
  ```

- Flag 0x2

  Questo flag indica la modalità di ricezione condizionale, o CR (Conditional Receive). Questa modalità fa parte del processo EIGRP multicast affidabile ed è utilizzata per consentire ai router vicini che non hanno confermato la ricezione di un pacchetto affidabile precedente di raggiungere un collegamento condiviso. Gli indirizzi nel TLV (Type Length Value) della sequenza sono i peer che devono ignorare i pacchetti multicast finché non vengono recuperati tramite pacchetti unicast.

  <#root>

  ```
  EIGRP: Received UPDATE on Ethernet0/0 nbr 10.1.1.2
    AS 1,
  Flags 0x2
  , Seq 21/0 idbQ 1/0 iidbQ un/rely 0/0 peerQ un/rely 0/1,
    not in CR-mode, packet discarded
  ```

- Flag 0x4

  Questo flag è il bit di riavvio (bit RS). È impostato nei pacchetti Hello e nei pacchetti Update quando si usa la funzionalità NSF. Un router con funzionalità NSF visualizza questo bit per

rilevare se il router vicino viene riavviato. Il router vicino sa quindi che deve mantenere l'adiacenza EIGRP attiva. Il router che si riavvia visualizza questo flag per stabilire se il peer partecipa al riavvio.

<#root>

```
EIGRP: Received HELLO on Ethernet0/0 nbr 10.1.1.2
 AS 1,
```

Flags 0x4

```
, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
```

- Flag 0x8

  Questo è il bit di fine tabella, o EOT (End-of-Table). Questo bit indica che al router vicino è stata inviata la tabella di routing completa. Un router NSF visualizza questo bit per stabilire se il router vicino ha completato il riavvio. Un router NSF attende questo bit prima di rimuovere le route obsolete dal router che viene riavviato.

  <#root>

```
EIGRP: Received UPDATE on Ethernet0/0 nbr 10.1.1.2
  AS 1,
```

Flags 0x8

```
, Seq 4/33 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
EIGRP: NSF: AS1. Receive EOT from 10.1.1.2
```

I flag sono espressi con un numero esadecimale. Pertanto, il flag 0x5 indica che i flag 4 e 1 sono impostati; il flag 0x9 indica che i flag 8 e 1 sono impostati; il flag 0xA indica che i flag 8 e 2 sono impostati.

Per risolvere i problemi relativi all'instabilità dei router vicini, usare questi comandi:

- show eigrp interface detail
- show ip eigrp neighbor detail
- ping unicast
- ping with size full MTU
- ping con verifica dati risposta
- ping multicast
- debug eigrp packet (hello)
- show ip eigrp traffic
- show ip traffic | iniziare EIGRP

SIA

In questa sezione viene fornita una panoramica dello stato SIA, alcuni possibili sintomi e cause e come risolverlo.

Definizione dello stato SIA

Lo stato SIA indica che un router EIGRP non ha ricevuto una risposta a una query inviata da uno o più router vicini entro il tempo assegnato (circa tre minuti). In questo caso, il protocollo EIGRP disattiva la relazione stabilita con i router vicini che non hanno inviato la risposta e registra un messaggio di errore DUAL-3-SIA per la route che era attiva.

Sintomi

Questi messaggi possono essere visualizzati su uno o più router:

```
%DUAL-3-SIA: Route 10.100.1.1/32 stuck-in-active state in IP-EIGRP(0) 1.  Cleaning up

%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.1.6 (Serial3/0) is down:
 stuck in active
```

Se il problema si verifica solo saltuariamente, può essere ignorato. Se si verifica di frequente, indica un problema di rete persistente.

Possibili cause

Ecco alcune cause possibili di uno stato SIA:

- Instabilità dei collegamenti
- Collegamenti non validi
- Instabilità delle route
- Collegamenti congestionati
- Diametro della rete grande (ampio intervallo di query)
- Memoria insufficiente
- Elevato consumo della CPU
- Configurazione errata (valore della larghezza di banda errato)

Suggerimenti per la risoluzione dei problemi

Lo stato SIA indica la presenza di un problema nella rete, la cui causa non è sempre facilmente individuabile. Possiamo usare due metodi:

- Visualizzare i prefissi che hanno riportato uno stato SIA e studiarne eventuali caratteristiche comuni.
- Individuare il router che non rispondono alle query su queste route.

Stabilire se tutti i prefissi per cui viene segnalato uno stato SIA hanno caratteristiche comuni. Ad

esempio, possono essere tutte route /32 dal bordo della rete, ad esempio nelle reti remote. In tal caso, può indicare la posizione del problema nella rete (vale a dire, dove hanno avuto origine questi prefissi).

In definitiva, si tratta di capire dove uno o più router inviano query senza ricevere risposta, mentre il router downstream non è in questo stato. Ad esempio, il router potrebbe inviare query la cui ricezione è confermata, ma senza ricevere risposta dal router downstream.

Per risolvere un problema SIA, usare il comando show ip eigrp topology active. Cercare la r minuscola nell'output del comando, che indica un router in attesa di risposta a una query per quel prefisso dal router vicino.

Ecco un esempio. Esaminiamo la topologia. I collegamenti R1-R6 e R1-R5 sono disattivati. Quando l'interfaccia di loopback del router R1 viene chiusa, R1 invia una query per il prefisso 10.100.1.1/32 a R2 e R3. Il router R1 è ora attivo per questo prefisso. I router R2 e R3 diventano attivi ed eseguono una query sul router R4, che diventa attivo e invia una query a R5. Il router R5 diventa finalmente attivo e invia una query a R6. Il router R6 deve restituire una risposta a R5. Il router R5 diventa passivo e risponde a R4, che a sua volta diventa passivo e invia una risposta a R2 e R3. Infine, R2 e R3 diventano passivi e inviano una risposta a R1, che diventa nuovamente passivo.

Se si verifica un problema, un router può rimanere attivo per un periodo di tempo prolungato in attesa di una risposta. Per impedire al router di attendere una risposta che non potrà mai essere ricevuta, può dichiarare sia e uccidere il router attraverso cui attende la risposta. Per risolvere il problema, visualizzare l'output del comando show ip eigrp topology active e seguire il percorso della r.

Ecco l'output del router R1:

<#root>

```
R1#

show ip eigrp topology active


IP-EIGRP Topology Table for AS 1)/ID(10.100.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

A 10.100.1.1/32, 1 successors, FD is Inaccessible
    1 replies, active 00:01:11, query-origin: Local origin
        via Connected (Infinity/Infinity), Loopback0
      Remaining replies:
         via 10.1.1.2,

r

, Ethernet0/0
```

Il router R1 è attivo e attende una risposta da R2. Di seguito è riportato l'output per il router R2:

<#root>

```
R2#
```

show ip eigrp topology active

```
IP-EIGRP Topology Table for AS(1)/ID(10.100.1.2)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

A 10.100.1.1/32, 1 successors, FD is Inaccessible
    1 replies, active 00:01:01, query-origin: Successor Origin
        via 10.1.1.1 (Infinity/Infinity), Ethernet0/0
        via 10.2.1.4 (Infinity/Infinity),
```

r

```
, Ethernet1/0, serno 524
        via 10.2.1.3 (Infinity/Infinity), Ethernet1/0, serno 523
```

Il router R2 è attivo e attende una risposta da R4. Di seguito è riportato l'output per il router R4:

<#root>

```
R4#
```

show ip eigrp topology active

```
IP-EIGRP Topology Table for AS(1)/ID(10.100.1.4)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

A 10.100.1.1/32, 1 successors, FD is Inaccessible
    1 replies, active 00:00:56, query-origin: Successor Origin
        via 10.2.1.2 (Infinity/Infinity), Ethernet1/0
        via 172.16.1.5 (Infinity/Infinity),
```

r

```
, Serial2/0, serno 562
        via 10.2.1.3 (Infinity/Infinity), Ethernet1/0, serno 560
```

Il router R4 è attivo e attende una risposta da R5. Di seguito è riportato l'output per il router R5:

<#root>

```
R5#
```

show ip eigrp topology active

```
IP-EIGRP Topology Table for AS(1)/ID(172.16.1.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - reply Status

, s - sia Status

A 10.100.1.1/32, 1 successors, FD is Inaccessible, Q
    1 replies, active 00:00:53, query-origin: Successor Origin
        via 172.16.1.4 (Infinity/Infinity), Serial2/0
      Remaining replies:
         via 192.168.1.6,

r

, Serial3/0
```

Il router R5 è attivo e attende una risposta da R6. Di seguito è riportato l'output per il router R6:

<#root>

```
R6#

show ip eigrp topology active


IP-EIGRP Topology Table for AS(1)/ID(192.168.1.6)
R6#
```

Come mostrato, il router R6 non è attivo per il prefisso, quindi il problema deve essere tra i router R5 e R6. Dopo un po' di tempo, vediamo che la R5 uccide il vicinato della R6 e dichiara uno stato SIA:

```
R5#
%DUAL-3-SIA: Route 10.100.1.1/32 stuck-in-active state in IP-EIGRP(0) 1.
  Cleaning up
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.1.6 (Serial3/0) is down:
 stuck in active
```

Quando si visualizza l'output del router R5, si possono notare problemi sul collegamento al router R6.

Questo è il nuovo meccanismo SIA e, come tale, lo stato SIA ha riguardato un router accanto al router su cui si è verificato il problema. Nell'esempio, questo è il collegamento tra i router R5 e R6. Nelle versioni di codice meno recenti, l'ASI può essere dichiarata su qualsiasi router del percorso (ad esempio su R2), che può essere distante dal problema. Il timer del SIA era tre minuti. Qualsiasi router del percorso poteva essere il primo a passare allo stato SIA e disattivare il

collegamento ai router vicini. Nelle nuove versioni, il router attende una risposta, invia intanto una query SIA al router vicino e il router vicino risponde immediatamente con una risposta SIA. Ad esempio, mentre è nello stato attivo, il router R4 invia una query SIA al router R5 e il router R5 risponde con una risposta SIA.

```
R5#
EIGRP: Received SIAQUERY on Serial2/0 nbr 172.16.1.4
  AS 1, Flags 0x0, Seq 456/447 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
EIGRP: Enqueueing SIAREPLY on Serial2/0 nbr 172.16.1.4 iidbQ un/rely 0/1
  peerQ un/rely 0/0 serno 374-374
EIGRP: Sending SIAREPLY on Serial2/0 nbr 172.16.1.4
  AS 1, Flags 0x0, Seq 448/456 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/1
  serno 374-374
```

Il router R5 invia le query SIA anche al router R6, ma non riceve risposta.

```
R5#
EIGRP: Enqueueing SIAQUERY on Serial3/0 nbr 192.168.1.6 iidbQ un/rely 0/2
 peerQ un/rely 5/0 serno 60-60
```

Dopo aver inviato la query SIA senza ricevere risposta, il router viene contrassegnato dalla lettera s:

<#root>

```
R5#
```

show ip eigrp topology active

```
IP-EIGRP Topology Table for AS(1)/ID(172.16.1.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status,
```

s - sia Status

```
A 10.100.1.1/32, 1 successors, FD is Inaccessible, Qqr
    1 replies, active 00:02:36, query-origin: Successor Origin, retries(1)
        via 1172.16.1.4 (Infinity/Infinity), Serial2/0, serno 61
        via 192.168.1.6 (Infinity/Infinity), r
```

s

```
, q, Serial3/0, serno 60, anchored
```

Con il nuovo codice SIA, è necessario dichiarare il SIA sul router R5 quando non riceve una

risposta SIA. È quindi necessario attivare il debug per questi due pacchetti SIA EIGRP:

<#root>

```
R2#
debug eigrp packets SIAquery SIAreply


EIGRP Packets debugging is on
    (SIAQUERY, SIAREPLY)

R2#
show debug


EIGRP:
  EIGRP Packets debugging is on
    (SIAQUERY, SIAREPLY)
```

In breve, per risolvere il problema SIA, usare questi comandi:

- show ip eigrp topology active
- show ip eigrp event (può aumentare le dimensioni del log eventi)
- show ip eigrp traffic (cerca le query SIA e le risposte SIA)
- show proc mem
- show mem sum

Ecco alcune possibili soluzioni al problema SIA:

- Risolvere il problema del collegamento.
- Usare la funzionalità di riepilogo (manuale o automatico) sulle reti con molti prefissi o intervalli di query troppo specifici.
- Usare distribute-lists per diminuire l'intervallo di query.
- Definire i router remoti come stub.

Prefissi mancanti

Esistono due tipi di prefissi mancanti: quelli mancanti nella tabella di routing (o nella base RIB (Routing Information Base)) e quelli mancanti nella tabella di topologia.

Prefissi mancanti nella tabella RIB

Le cause per cui i prefissi non sono presenti nella tabella RIB sono diverse:

- Il prefisso viene installato nella tabella di routing da un altro protocollo di routing con una distanza amministrativa più bassa.
- Il prefisso è bloccato da una lista di distribuzione (distribute-list).

- Il prefisso è bloccato dal meccanismo split-horizon.

Prefisso installato dal protocollo di routing con distanza amministrativa più bassa

In questo esempio, il prefisso è installato nella tabella di routing da una route statica o da un protocollo di routing con distanza amministrativa più bassa.

In genere, in questo caso, il prefisso si trova nella tabella della topologia, ma non ha percorsi migliori (Successor) per raggiungere la destinazione. Per visualizzare tutte le voci, usare il comando show ip eigrp topology zero-successors. La Distanza realizzabile (FD) deve avere un valore infinito.

Immettere il comando show ip route <prefix> e verificare i protocolli di routing usati sulla route nella tabella RIB:

<#root>

```
R1#
show ip eigrp topology 192.168.100.6 255.255.255.255


IP-EIGRP (AS 1): Topology entry for 192.168.100.6/32
  State is Passive, Query origin flag is 1,
0 Successor(s), FD is 4294967295


  Routing Descriptor Blocks:
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (2297856/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

<#root>

```
R1#
show ip eigrp topology zero-successors


IP-EIGRP Topology Table for AS(1)/ID(10.100.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.1.0/24, 0 successors, FD is Inaccessible
        via 10.3.1.6 (2681856/2169856), Serial2/0
P 192.168.100.6/32, 0 successors, FD is Inaccessible
        via 10.3.1.6 (2297856/128256), Serial2/0
```

Blocco del prefisso da parte di distribute-list

L'EIGRP è un protocollo di routing di tipo distance-vector. Per bloccare i prefissi, è possibile usare una lista di distribuzione (distribute-list) su un router. È possibile usarlo su un'interfaccia per interrompere la trasmissione o la ricezione dei prefissi, oppure configurare la lista di distribuzione globalmente con il processo EIGRP del router in modo da applicare il filtro di routing su tutte le interfacce abilitate per EIGRP.

Di seguito è riportato un esempio:

<#root>

```
R1#
show running-config | begin router eigrp


router eigrp 1
 network 10.0.0.0

distribute-list 1 in


 no auto-summary
!
access-list 1 deny   192.168.100.6
access-list 1 permit any
```

Prefissi mancanti nella tabella della topologia

In questa sezione vengono descritti alcuni dei motivi per cui un prefisso potrebbe non essere presente nella tabella della topologia.

Specifica della maschera per un output corretto

Non commettere l'errore tipico; quando si verifica un prefisso nella tabella della topologia, specificare sempre la maschera. Se non si specifica la maschera, l'output visualizza:

<#root>

```
R1#
show ip eigrp topology 192.168.100.6


% IP-EIGRP (AS 1): Route not in topology table
```

Se la maschera viene specificata, l'output del comando show ip eigrp topology è:

<#root>

```
R1#
show ip eigrp topology 192.168.100.6 255.255.255.255


IP-EIGRP (AS 1): Topology entry for 192.168.100.6/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
  Routing Descriptor Blocks:
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (2297856/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.4.1.5 (Ethernet1/0), from 10.4.1.5, Send flag is 0x
      Composite metric is (2323456/2297856), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 26000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Come mostrato, il prefisso è presente nella tabella della topologia.

Blocco del prefisso da parte dello split-horizon

In questa sezione viene descritto un altro errore comune. Il protocollo EIGRP non si basa sullo stato del collegamento (link-state), ma sul vettore delle distanze (distance-vector). La tabella della topologia deve essere utilizzata per il corretto funzionamento dell'algoritmo di aggiornamento diffusione (DUAL), non perché l'EIGRP sia un protocollo di routing allo stato di collegamento, ma perché richiede un database. La tabella della topologia è necessaria perché solo le route giudicate migliori sono installate nella tabella di routing, mentre l'algoritmo DUAL richiede che vengano monitorate anche le altre route percorribili. Queste route FD sono quindi memorizzate nella tabella della topologia.

Nella tabella della topologia è sempre necessario specificare la route successore e le route possibili. In caso contrario, viene generato un bug. Tuttavia, la tabella della topologia potrebbero includere anche route alternative non ottimali in quanto ricevute come tali. Se non sono state ricevute da un router vicino, potrebbe essere stato applicato il metodo split-horizon che blocca il prefisso.

L'output del comando show ip eigrp topology mostra solo le voci dei prefissi che puntano alle route Successor e alle route Successor alternative, o route Feasible Successor. Per visualizzare i

prefissi che vengono ricevuti su tutti i percorsi, anche i percorsi non ottimali, immettere il comando show ip eigrp topology all-links.

Di seguito è riportato un esempio:

<#root>

```
R1#
```

show ip eigrp topology

```
IP-EIGRP Topology Table for AS(1)/ID(10.100.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.3.1.0/24, 1 successors, FD is 2169856
        via Connected, Serial2/0
P 10.2.1.0/24, 2 successors, FD is 307200
        via 10.1.1.2 (307200/281600), Ethernet0/0
        via 10.1.1.3 (307200/281600), Ethernet0/0
P 10.1.1.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 2195456
        via 10.4.1.5 (2195456/2169856), Ethernet1/0
P 192.168.1.0/24, 1 successors, FD is 2195456
        via 10.4.1.5 (2195456/2169856), Ethernet1/0
        via 10.3.1.6 (2681856/2169856), Serial2/0
P 10.4.1.0/24, 1 successors, FD is 281600
        via Connected, Ethernet1/0
P 172.16.100.5/32, 1 successors, FD is 409600
        via 10.4.1.5 (409600/128256), Ethernet1/0
P 10.100.1.4/32, 2 successors, FD is 435200
        via 10.1.1.2 (435200/409600), Ethernet0/0
        via 10.1.1.3 (435200/409600), Ethernet0/0
P 10.100.1.3/32, 1 successors, FD is 409600
        via 10.1.1.3 (409600/128256), Ethernet0/0
P 10.100.1.2/32, 1 successors, FD is 409600
        via 10.1.1.2 (409600/128256), Ethernet0/0
P 10.100.1.1/32, 1 successors, FD is 128256
        via Connected, Loopback0
P 192.168.100.6/32, 1 successors, FD is 2297856
        via 10.3.1.6 (2297856/128256), Serial2/0
```

Come si evince da questo output, la porzione all-links del comando include più percorsi:

<#root>

```
R1#
```

show ip eigrp topology all-links

```
IP-EIGRP Topology Table for AS(1)/ID(10.100.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
```

```
       r - reply Status, s - sia Status

P 10.3.1.0/24, 1 successors, FD is 2169856, serno 43
        via Connected, Serial2/0
P 10.2.1.0/24, 2 successors, FD is 307200, serno 127
        via 10.1.1.2 (307200/281600), Ethernet0/0
        via 10.1.1.3 (307200/281600), Ethernet0/0
P 10.1.1.0/24, 1 successors, FD is 281600, serno 80
        via Connected, Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 2195456, serno 116
        via 10.4.1.5 (2195456/2169856), Ethernet1/0


 via 10.3.1.6 (3193856/2681856), Serial2/0



        via 10.1.1.2 (2221056/2195456), Ethernet0/0



        via 10.1.1.3 (2221056/2195456), Ethernet0/0


P 192.168.1.0/24, 1 successors, FD is 2195456, serno 118
        via 10.4.1.5 (2195456/2169856), Ethernet1/0
        via 10.3.1.6 (2681856/2169856), Serial2/0
P 10.4.1.0/24, 1 successors, FD is 281600, serno 70
        via Connected, Ethernet1/0
P 172.16.100.5/32, 1 successors, FD is 409600, serno 117
        via 10.4.1.5 (409600/128256), Ethernet1/0


via 10.3.1.6 (2809856/2297856), Serial2/0


P 10.100.1.4/32, 2 successors, FD is 435200, serno 128
        via 10.1.1.2 (435200/409600), Ethernet0/0
        via 10.1.1.3 (435200/409600), Ethernet0/0
P 10.100.1.3/32, 1 successors, FD is 409600, serno 115
        via 10.1.1.3 (409600/128256), Ethernet0/0
P 10.100.1.2/32, 1 successors, FD is 409600, serno 109
        via 10.1.1.2 (409600/128256), Ethernet0/0
P 10.100.1.1/32, 1 successors, FD is 128256, serno 4
        via Connected, Loopback0
P 192.168.100.6/32, 1 successors,

FD is 2297856

, serno 135
        via 10.3.1.6 (2297856/128256), Serial2/0


 via 10.4.1.5 (2323456/2297856), Ethernet1/0
```

Considerare l'ultimo prefisso nell'output precedente. Il percorso tramite 10.4.1.5 ha (2323456/2297856). La distanza (metrica) annunciata è 2297856, che non è più bassa della metrica FD di 2297856, quindi il percorso non è quello ottimale.

```
P 192.168.100.6/32, 1 successors, FD is 2297856, serno 135
        via 10.3.1.6 (2297856/128256), Serial2/0


 via 10.4.1.5 (2323456/2297856), Ethernet1/0
```

Ecco un esempio in cui lo split-horizon fa sì che un percorso venga escluso dalla tabella della topologia di una route. Quando si visualizza la topologia, si nota come il router R1 abbia il prefisso 192.168.100.6/32 tramite i router R6 e R5 nella tabella della topologia, ma non tramite i router R2 o R3:

<#root>

```
R1#

show ip eigrp topology 192.168.100.6 255.255.255.255


IP-EIGRP (AS 1): Topology entry for 192.168.100.6/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
  Routing Descriptor Blocks:
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (2297856/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.4.1.5 (Ethernet1/0), from 10.4.1.5, Send flag is 0x0
      Composite metric is (2323456/2297856), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 26000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Ciò avviene perché il router R1 non ha mai ricevuto il prefisso 192.168.100.6/32 tramite il router R2 o R3, in quanto questi hanno il prefisso 192.168.100.6/32 tramite il router R1 nella tabella di routing.

<#root>

```
R2#

show ip route 192.168.100.6 255.255.255.255


Routing entry for 192.168.100.6/32
  Known via "eigrp 1", distance 90, metric 2323456, type internal
  Redistributing via eigrp 1
```

```
  Last update from 10.1.1.1 on Ethernet0/0, 00:02:07 ago
  Routing Descriptor Blocks:
  * 10.1.1.1, from 10.1.1.1, 00:02:07 ago, via Ethernet0/0
      Route metric is 2323456, traffic share count is 1
      Total delay is 26000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2

R3#
```

show ip route 192.168.100.6 255.255.255.255

```
Routing entry for 192.168.100.6/32
  Known via "eigrp 1", distance 90, metric 2323456, type internal
  Redistributing via eigrp 1
  Last update from 10.1.1.1 on Ethernet0/0, 00:01:58 ago
  Routing Descriptor Blocks:
  * 10.1.1.1, from 10.1.1.1, 00:01:58 ago, via Ethernet0/0
      Route metric is 2323456, traffic share count is 1
      Total delay is 26000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

Per verificarlo, usare la parola chiave all-links sul router R1 per esaminare la tabella della topologia. In questo modo vengono visualizzati tutti i percorsi di tutti i prefissi, inclusi i percorsi i cui costi non sono ottimali. Si può notare anche che il router R1 non ha appreso il prefisso 192.168.100.6/32 dai router R2 o R3.

Metriche

Nota: l'MTU e il conteggio hop non sono inclusi nel calcolo della metrica.

Queste sono le formule usate per calcolare la metrica di una route:

- Se K5 è un valore diverso da zero:

  Metrica EIGRP = 256*(((K1*Larghezza di banda) + (K2*Larghezza di banda)/(256-Carico) + (K3*Ritardo))*(K5/(Affidabilità+ K4)))

- Se K5 è uguale a zero:

  Metrica EIGRP = 256*((K1*Larghezza di banda) + (K2*Larghezza di banda)/(256-Carico) + (K3*Ritardo))

I valori K sono pesi utilizzati per ponderare i quattro componenti della metrica EIGRP: ritardo, larghezza di banda, affidabilità e carico. Questi sono i valori K predefiniti:

- K1 = 1
- K2 = 0

- K3 = 1
- K4 = 0
- K5 = 0

Con i valori K predefiniti (solo con larghezza di banda e ritardo), la formula diventa:

Metrica EIGRP = 256 * (Larghezza di banda + Ritardo)

Larghezza di banda = (10^7/Larghezza di banda minima in kilobit al secondo)

Nota: il ritardo viene misurato in decine di microsecondi; tuttavia, sull'interfaccia, viene misurato in microsecondi.

Tutti e quattro i parametri possono essere verificati con il comando show interface:

<#root>

```
 R1#
show interface et 0/0


  Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.0100 (bia aabb.cc00.0100)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes,
BW 10000 Kbit
,
DLY 1000 usec
,

reliability 255/255
,
txload 1/255
,
rxload 1/255


  Encapsulation ARPA, loopback not set  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00  Last input 00:00:02, output 00:00:02,
   output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
  5 minute output rate 0 bits/sec, 0 packets/sec
     789 packets input, 76700 bytes, 0 no buffer
     Received 707 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     548 packets output, 49206 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Il ritardo è cumulativo, quindi vengono sommati i ritardi di ciascun collegamento presente sul percorso. La larghezza di banda non è cumulativa, quindi il valore usato nella formula corrisponde alla larghezza di banda più bassa tra quelle dei collegamenti presenti sul percorso.

ID router duplicato

Per visualizzare l'ID router usato dal protocollo EIGRP, immettere il comando show ip eigrp topology sul router e visualizzare la prima riga dell'output:

```
<#root>

R1#

show ip eigrp topology


IP-EIGRP Topology Table for AS(1)/

ID(10.100.1.1)



Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.3.1.0/24, 1 successors, FD is 2169856
        via Connected, Serial2/0
```

L'ID del router EIGRP non viene usato per tutte le route interne nelle versioni precedenti di Cisco IOS. Un ID di router duplicato per EIGRP non deve causare problemi se vengono utilizzate solo route interne. Nel software Cisco IOS più recente, l'ID del router EIGRP è trasportato sulle route interne.

L'ID router delle route esterne può essere visualizzato in questo output:

```
<#root>

R1#

show ip eigrp topology 192.168.1.4 255.255.255.255
```

```
IP-EIGRP (AS 1): Topology entry for 192.168.1.4/32
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 435200
  Routing Descriptor Blocks:
  10.1.1.2 (Ethernet0/0), from 10.1.1.2, Send flag is 0x0
      Composite metric is (435200/409600), Route is External
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 7000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
      External data&colon;
```

Originating router is 10.100.1.4

```
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

Se viene ricevuta una route EIGRP (esterna) con lo stesso ID router EIGRP, non viene generata una voce di log. Tuttavia, l'evento viene acquisito nel log degli eventi EIGRP. Quando si controlla la route EIGRP (esterna), questa non viene visualizzata nella tabella della topologia.

Controllare se nel log degli eventi EIGRP sono presenti messaggi di ID router duplicati:

<#root>

R1#

show ip eigrp events

```
Event information for AS 1:
1    08:36:35.303 Ignored route, metric: 10.33.33.33 3347456
2    08:36:35.303 Ignored route, neighbor info: 10.3.1.6 Serial2/1
3    08:36:35.303
```

Ignored route, dup router: 10.100.1.1

```
4    08:36:35.303 Rcv EOT update src/seq: 10.3.1.6 143
5    08:36:35.227 Change queue emptied, entries: 2
6    08:36:35.227 Route OBE net/refcount: 10.100.1.4/32 3
7    08:36:35.227 Route OBE net/refcount: 10.2.1.0/24 3
8    08:36:35.227 Metric set: 10.100.1.4/32 435200
9    08:36:35.227 Update reason, delay: nexthop changed 179200
10   08:36:35.227 Update sent, RD: 10.100.1.4/32 435200
11   08:36:35.227 Route install: 10.100.1.4/32 10.1.1.3
12   08:36:35.227 Route install: 10.100.1.4/32 10.1.1.2
13   08:36:35.227 RDB delete: 10.100.1.4/32 10.3.1.6
```

Mancata corrispondenza dei valori K/arresto normale

Quando i valori K non corrispondono sui router vicini, viene visualizzato questo messaggio:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.4.1.5 (Ethernet1/0) is down:
 K-value mismatch
```

I valori K vengono configurati con questo comando (con valori K compresi tra 0 e 255):

<#root>

```
metric weights

 tos k1 k2 k3 k4 k5

!
router eigrp 1
 network 10.0.0.0
 metric weights 0 1 2 3 4 5
!
```

Il messaggio indica che il collegamento ai router EIGRP vicini non è stato stabilito a causa di una mancata corrispondenza dei valori K. I valori K devono essere uguali su tutti i router EIGRP di un sistema autonomo per evitare problemi di routing quando router diversi usano calcoli metrici diversi.

Controllare se i valori K sono uguali sui router vicini. Se i valori K sono gli stessi, il problema può essere causato dalla funzione di chiusura normale di EIGRP. In tal caso, un router EIGRP invia un pacchetto Hello con i valori K impostati a 255 in modo che la mancata corrispondenza dei valori K sia intenzionale. In questo modo si indica al router EIGRP adiacente di non funzionare. Sul router vicino, si dovrebbe ricevere un goodbye message:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down:
 Interface Goodbye received
```

Tuttavia, se il router vicino ha un software precedente all'ID bug Cisco CSCdr96531, non riconosce questo messaggio come arresto normale e pensa si tratti di una mancata corrispondenza dei valori K:

```
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.4.1.5 (Ethernet1/0) is down:
 K-value mismatch
```

Questo è lo stesso messaggio che viene visualizzato in caso di mancata corrispondenza dei valori K su router vicini.

Questi sono i fattori che determinano l'arresto normale:

- Uso del comando no router eigrp.
- Uso del comando no network.
- Uso del comando clear ip eigrp neighbor.
- Ricaricamento del router.

L'arresto normale viene usato per accelerare il rilevamento dello stato inattivo del router vicino. Senza un arresto normale, il router vicino deve attendere che il tempo di attesa scada prima di dichiarare che il router vicino è inattivo.

Bilanciamento del carico su percorsi con metriche diverse (variance)

Nel protocollo EIGRP è possibile bilanciare il carico su percorsi con metriche diverse usando la funzionalità UCLB (Unequal Cost Load Balancing) e il comando variance, a condizione che sia soddisfatta la condizione di varianza e che siano disponibili route Feasible Successor.

Per soddisfare la condizione di varianza, la metrica della route non deve essere più grande della metrica migliore moltiplicata per la varianza. Affinché una route sia considerata Feasible Successor, è necessario che la metrica annunciata sia inferiore alla metrica FD (Feasible Distance). Di seguito è riportato un esempio:

<#root>

```
!
router eigrp 1

variance 2


 network 10.0.0.0
 no auto-summary
!
```

Il valore della varianza configurato per il router R1 è variance 2. Ciò significa che se il router ha un altro percorso per la route con una metrica che non è più grande del doppio della metrica migliore per quella route, deve esistere un bilanciamento del carico di costo ineguale per quella route.

<#root>

```
R1#

show ip eigrp topology 172.16.100.5 255.255.255.255
```

```
IP-EIGRP (AS 1): Topology entry for 172.16.100.5/32
  State is Passive, Query origin flag is 1, 1 Successor(s),
```

FD is 409600

```
  Routing Descriptor Blocks:
  10.4.1.5 (Ethernet1/0), from 10.4.1.5, Send flag is 0x0
      Composite metric is (
```

409600

```
/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (
```

435200/409600

```
), Route is Internal <<< RD = 409600
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 7000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Se la seconda voce della topologia è installata nella tabella di routing, la metrica della seconda voce della topologia è 435200. Poiché il doppio della metrica migliore è 2 x 409600 = 819200 e 435200 < 819200, la seconda voce della topologia è compresa nell'intervallo di varianza. La distanza riportata della seconda voce della topologia è 409600, che non è inferiore a FD = 409600. La seconda condizione (fattibilità) non è soddisfatta e non è possibile installare la seconda voce nel RIB.

<#root>

```
R1#
```

show ip route 172.16.100.5

```
Routing entry for 172.16.100.5/32
  Known via "eigrp 1", distance 90, metric 409600, type internal
  Redistributing via eigrp 1
  Last update from 10.4.1.5 on Ethernet1/0, 00:00:16 ago
  Routing Descriptor Blocks:
  * 10.4.1.5, from 10.4.1.5, 00:00:16 ago, via Ethernet1/0
      Route metric is 409600, traffic share count is 1
      Total delay is 6000 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Se la metrica annunciata RD della seconda voce di topologia è più piccola della metrica FD, come nell'esempio successivo, è possibile bilanciare il carico tra route con metriche diverse.

```
<#root>

R1#

show ip eigrp topology 172.16.100.5 255.255.255.255


IP-EIGRP (AS 1): Topology entry for 172.16.100.5/32
  State is Passive, Query origin flag is 1, 1 Successor(s),

FD is 409600


  Routing Descriptor Blocks:
  10.4.1.5 (Ethernet1/0), from 10.4.1.5, Send flag is 0x0
      Composite metric is (409600/128256), Route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (434944/

409344

), Route is Internal <<< RD = 409344
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 6990 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 2
```

Entrambe le voci della topologia sono ora nella tabella di routing:

```
<#root>

R1#

show ip route 172.16.100.5


Routing entry for 172.16.100.5/32
  Known via "eigrp 1", distance 90, metric 409600, type internal
  Redistributing via eigrp 1
  Last update from 10.3.1.6 on Serial2/0, 00:00:26 ago
  Routing Descriptor Blocks:
  * 10.4.1.5, from 10.4.1.5, 00:00:26 ago, via Ethernet1/0
      Route metric is 409600, traffic share count is 120
      Total delay is 6000 microseconds, minimum bandwidth is 10000 Kbit
```

```
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    10.3.1.6, from 10.3.1.6, 00:00:26 ago, via Serial2/0
      Route metric is 434944, traffic share count is 113
      Total delay is 6990 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

Routing statico

Il protocollo EIGRP supporta le configurazioni con uno o più router vicini statici sulla stessa interfaccia. Non appena si configura un router adiacente EIGRP statico sull'interfaccia, il router non invia più i pacchetti EIGRP come multicast su tale interfaccia né elabora i pacchetti EIGRP multicast ricevuti. Ciò significa che i pacchetti Hello, Update e Query sono ora unicast. Non è possibile stabilire adiacenze con gli altri router vicini finché non si configura esplicitamente il comando static neighbor sull'interfaccia.

Ecco come configurare il routing statico per i router EIGRP vicini:

<#root>

```
router eigrp 1
 passive-interface Loopback0
 network 10.0.0.0
 no auto-summary
```

neighbor 10.1.1.1 Ethernet0/0

```
!
```

Quando i router su entrambi i lati del collegamento hanno il comando static neighbor, viene visualizzato quanto segue:

<#root>

```
R1#
```

show ip eigrp neighbors detail

```
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.1.1.2                Et0/0             14 00:00:23   27   200  0  230
```

Static neighbor

```
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 1
```

```
0   10.3.1.6                Se2/0             14 1d02h      26   200  0  169
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 12
3   10.4.1.5                Et1/0             10 1d02h      16   200  0  234
   Version 12.4/1.2, Retrans: 0, Retries: 0, Prefixes: 7
```

Se solo un router ha il comando statico neighbors configurato, è possibile notare che il router ignora i pacchetti EIGRP multicast e l'altro router ignora i pacchetti EIGRP unicast:

```
R1#
EIGRP: Received HELLO on Ethernet0/0 nbr 10.1.1.2
  AS 1, Flags 0x0, Seq 0/0 idbQ 0/0
EIGRP: Ignore multicast Hello Ethernet0/0 10.1.1.2
```

```
R2#
EIGRP: Received HELLO on Ethernet0/0 nbr 10.1.1.1
  AS 1, Flags 0x0, Seq 0/0 idbQ 0/0
EIGRP: Ignore unicast Hello from Ethernet0/0 10.1.1.1
```

Per i router EIGRP vicini statici, è disponibile un comando debug speciale:

<#root>

```
R2#

debug eigrp neighbors static


EIGRP Static Neighbors debugging is on

R2#

conf t


Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#neighbor 10.1.1.1 et 0/0
R2(config-router)#end
R2#

EIGRP: Multicast Hello is disabled on Ethernet0/0!
EIGRP: Add new static nbr 10.1.1.1 to AS 1 Ethernet0/0
```

Di seguito sono riportati alcuni motivi per cui è possibile configurare i router adiacenti EIGRP statici:

- Si desidera limitare o evitare le trasmissioni su reti NBMA (Non-Broadcast Multi-Access).
- Si desidera limitare o evitare i pacchetti multicast sulle trasmissioni broadcast (Ethernet).

- Usare per risolvere i problemi (con unicast anziché multicast).

⚠ Attenzione: non configurare il comando interfaccia passiva insieme al comando EIGRP statico adiacente.

Ridistribuzione delle route statiche

Quando si configura una route statica che punta a un'interfaccia e la route è coperta da un'istruzione di rete nel router EIGRP, la route statica viene annunciata dal protocollo EIGRP come route connessa. In questo caso, non è necessario usare il comando redistribute static o una metrica predefinita.

```
router eigrp 1
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
!
ip route 172.16.0.0 255.255.0.0 Serial2/0
!
```

<#root>

R1#

show ip eigrp top 172.16.0.0 255.255.0.0

```
IP-EIGRP (AS 1): Topology entry for 172.16.0.0/16
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2169856
  Routing Descriptor Blocks:
  0.0.0.0, from Rstatic, Send flag is 0x0
      Composite metric is (2169856/0),
```

Route is Internal

```
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 20000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 0
```

Affidabilità e carico nel calcolo delle metriche

⚠ Attenzione: non utilizzare affidabilità e/o carico per calcolare le metriche.

I parametri di affidabilità e carico vengono visualizzati nell'output del comando show interface. Se carico o affidabilità cambiano, questi parametri non vengono aggiornati in modo dinamico e quindi non viene innescata una modifica immediata della metrica. Solo se l'EIGRP decide di inviare aggiornamenti ai propri vicini a causa di modifiche della topologia, possono verificarsi cambiamenti nel carico e nell'affidabilità. Inoltre, l'uso del carico e dell'affidabilità per calcolare la metrica può introdurre instabilità, poiché viene eseguito un routing adattivo. Se si desidera modificare il routing in base al carico del traffico, è necessario prendere in considerazione l'uso di MPLS (Multiprotocol Label Switching) o PfR (Performance Routing).

Elevato consumo della CPU

Nel protocollo EIGRP vengono eseguiti tre processi contemporaneamente:

- Router – Occupa i pool di memoria condivisi.
- Hello – Invia e riceve i pacchetti Hello e gestisce i collegamenti tra i peer.
- Protocol Dependent Module (PDM): EIGRP supporta quattro suite di protocolli: IP, IPv6, IPX e AppleTalk. Ogni suite ha il proprio modulo PDM. Il modulo PDM svolge le seguenti funzioni principali:
    - Gestisce le tabelle della topologia e dei router vicini per i router EIGRP vicini che appartengono alla suite di protocolli.
    - Crea e converte i pacchetti specifici del protocollo per l'algoritmo DUAL (trasmissione e ricezione di pacchetti EIGRP).
    - Interfacce DUAL sulla tabella di routing specifica del protocollo.
    - Calcola la metrica e trasmette le informazioni all'algoritmo DUAL (DUAL seleziona solo le route Successor e Feasible Successor).
    - Implementa il filtraggio e gli elenchi di accesso.
    - Esegue le funzioni di ridistribuzione da e verso gli altri protocolli di routing.

Ecco un esempio di output che mostra i tre processi:

<#root>

```
R1#
show process cpu | include EIGRP

  89           4        24        166  0.00%  0.00%  0.00%   0 IP-EIGRP
Router

  90        1016      4406        230  0.00%  0.03%  0.00%   0 IP-EIGRP:
PDM

  91        2472      6881        359  0.00%  0.07%  0.08%   0 IP-EIGRP:
HELLO
```

Un consumo elevato della CPU nel protocollo EIGRP non è normale. Se si verifica, il carico di lavoro sul protocollo EIGRP è eccessivo oppure il protocollo EIGRP ha un bug. Nel primo caso, controllare il numero di prefissi nella tabella della topologia e il numero di peer. Controllare che le route EIGRP e i router vicini non siano instabili.

Protocollo EIGRP nelle reti frame relay (coda di trasmissione)

Nelle reti frame relay in cui sono presenti più router vicini su un'interfaccia point-to-multipoint, possono essere presenti molti pacchetti broadcast o multicast che devono essere trasmessi. Per questo motivo, esiste una coda di trasmissione separata con propri buffer. La coda di trasmissione ha la priorità quando trasmette a una velocità inferiore al massimo configurato e ha una allocazione della larghezza di banda minima garantita.

Ecco il comando usato in questo scenario:

<#root>

```
frame-relay broadcast-queue size byte-rate packet-rate
```

In genere, iniziare con venti pacchetti per Data Link Connection Identifier (DLCI). La velocità in byte deve essere minore di entrambe le seguenti:

- N/4 volte la velocità di accesso remoto minima (misurata in byte al secondo), dove N è il numero di DLCI su cui deve essere replicata la trasmissione.
- Un quarto della velocità di accesso locale (misurata in byte al secondo).

Se si osservano eventi di instabilità su un numero elevato di router EIGRP vicini, aumentare la dimensione della coda di trasmissione del frame relay. Questo problema non si verifica se sono presenti sottointerfacce frame relay, poiché ogni router vicino si trova su una sottointerfaccia con una subnet IP diversa. Ciò può tornare utile come soluzione provvisoria quando la rete frame relay è magliata e di grandi dimensioni.

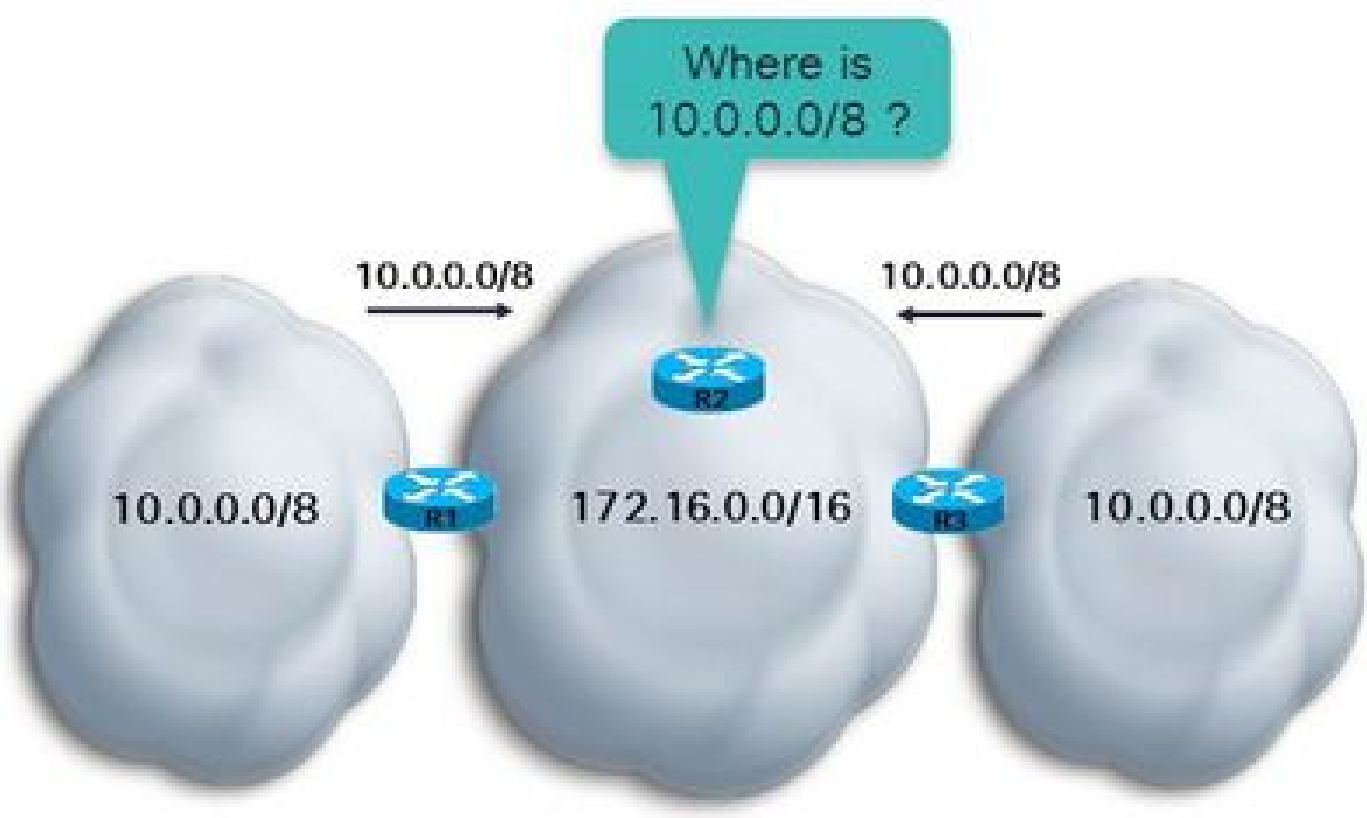
Mancata corrispondenza dei numeri AS

Il comando debug eigrp packets hello permette di verificare che il router non riceve i pacchetti Hello.

Riepilogo automatico

Il protocollo EIGRP viene usato per eseguire il riepilogo sui principali confini della rete (reti A, B e C) per impostazione predefinita. Ciò significa che le route più specifiche dei prefissi /8 della rete principale di tipo A, le route più specifiche dei prefissi /16 della rete principale di tipo B e le route più specifiche dei prefissi /24 delle reti principali di tipo C si perdono quando si attraversano i

confini. Ecco un esempio in cui il riepilogo automatico causa un problema:



Come mostrato, il parametro auto-summary è specificato per i router R1 e R3. Il router R2 riceve 10.0.0.0/8 da entrambi i router R2 e R3 perché entrambi sono router di confine tra la rete 10.0.0.0/8 e 172.16.0.0/16 della classe A principale. Il router R2 può avere la route 10.0.0.0/8 tramite R1 e R3 se la metrica è la stessa. In caso contrario, il router R2 riceve la route 10.0.0.0/8 tramite R1 o R3, a seconda del percorso con il costo minore. In entrambi i casi, se il router R2 deve inviare il traffico a determinate subnet di 10.0.0.0/8, non può essere completamente sicuro che il traffico raggiunga la destinazione, poiché una subnet di 10.0.0.0/8 può essere solo su un lato del cloud di rete.

Per risolvere il problema, immettere il comando no auto-summary nel processo del router EIGRP. Il router quindi propaga le subnet delle reti principali oltre il confine. Nelle versioni Cisco IOS più recenti, il parametro no auto-summary è specificato per impostazione predefinita.

Log degli eventi EIGRP

Il log degli eventi EIGRP acquisisce gli eventi EIGRP analogamente a quanto avviene con i debug. Tuttavia, è meno distruttivo e viene eseguito per impostazione predefinita. Può essere usato per acquisire gli eventi più difficili da risolvere o gli eventi che si verificano saltuariamente. Per impostazione predefinita, il log ha solo 500 righe. Per aumentarle, usare il comando eigrp event-log-sise<0 – 209878>. È possibile aumentare le dimensioni del log in base alle proprie esigenze, ma tenere sempre presente la quantità di memoria che il router deve dedicare al log. Per cancellare il log degli eventi EIGRP, immettere il comando clear ip eigrp events.

Di seguito è riportato un esempio:

<#root>

```
R1#
```

show ip eigrp events

```
Event information for AS 1:
1    09:01:36.107 Poison squashed: 10.100.1.3/32 reverse
2    09:01:35.991 Update ACK: 10.100.1.4/32 Serial2/0
3    09:01:35.967 Update ACK: 10.100.1.4/32 Ethernet0/0
4    09:01:35.967 Update ACK: 10.100.1.4/32 Ethernet1/0
5    09:01:35.943 Update delay/poison: 179200 FALSE
6    09:01:35.943 Update transmitted: 10.100.1.4/32 Serial2/0
7    09:01:35.943 Update delay/poison: 179200 TRUE
8    09:01:35.943 Update transmitted: 10.100.1.4/32 Ethernet0/0
9    09:01:35.943 Update delay/poison: 179200 FALSE
10   09:01:35.943 Update transmitted: 10.100.1.4/32 Ethernet1/0
11   09:01:35.923 Update packetized: 10.100.1.4/32 Ethernet0/0
12   09:01:35.923 Update packetized: 10.100.1.4/32 Ethernet1/0
13   09:01:35.923 Update packetized: 10.100.1.4/32 Serial2/0
14   09:01:35.903 Change queue emptied, entries: 1
15   09:01:35.903 Route OBE net/refcount: 10.100.1.4/32 3
16   09:01:35.903 Metric set: 172.16.1.0/24 2195456
17   09:01:35.903 Route install: 172.16.1.0/24 10.4.1.5
18   09:01:35.903 FC sat rdbmet/succmet: 2195456 2169856
19   09:01:35.903 FC sat nh/ndbmet: 10.4.1.5 2195456
20   09:01:35.903 Find FS: 172.16.1.0/24 2195456
```

Gli eventi più recenti vengono visualizzati all'inizio del log. È possibile filtrare alcuni tipi di eventi EIGRP, come DUAL, Xmit e transport:

```
eigrp log-event-type {dual | xmit | transport}
```

Inoltre, è possibile abilitare la registrazione per uno solo di questi tipi, per due tipi o per tutti e tre. Ecco un esempio in cui sono abilitati due tipi di registrazione:

<#root>

```
router eigrp 1
 redistribute connected
 network 10.0.0.0
 no auto-summary
```

eigrp log-event-type dual xmit

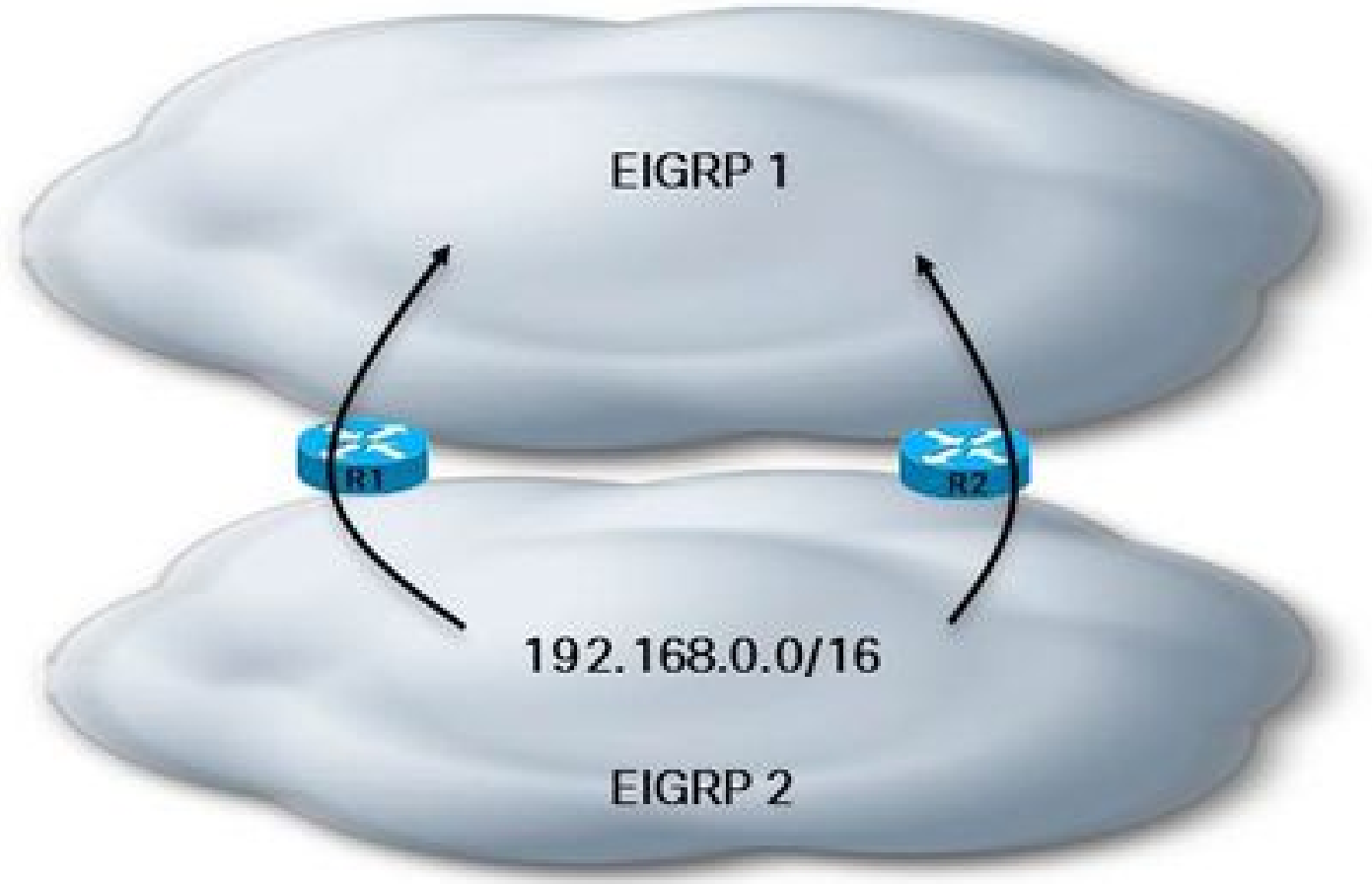
```
 eigrp event-logging
 eigrp event-log-size 100000
!
```

⚠ Attenzione: quando si abilita la registrazione degli eventi EIGRP, questa viene stampata e memorizzata nella tabella degli eventi. Ciò può aumentare l'output restituito sulla console, analogamente a quanto accade con i comandi debug del protocollo EIGRP.

Due sistemi autonomi EIGRP acquisiscono la stessa rete

Se una route viene acquisita tramite due processi EIGRP, solo uno dei processi EIGRP può installare la route nella tabella RIB, ossia il processo con la distanza amministrativa più bassa. A parità di distanza amministrativa, la route viene installata dal processo con la metrica più economica. A parità di metrica, la route viene installata nella tabella RIB dal processo EIGRP con l'ID processo EIGRP più basso. La tabella di topologia dell'altro processo EIGRP può avere la route installata con zero successori e un valore FD infinito.

Di seguito è riportato un esempio:



<#root>

R1#

show ip eigrp topology 192.168.1.0 255.255.255.0

IP-EIGRP (

AS 1

```
): Topology entry for 192.168.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2681856
  Routing Descriptor Blocks:
  10.3.1.6 (Serial2/0), from 10.3.1.6, Send flag is 0x0
      Composite metric is (2681856/2169856), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 40000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
IP-EIGRP (
```

AS 2

```
): Topology entry for 192.168.1.0/24
  State is Passive, Query origin flag is 1,
```

0 Successor(s)

,

FD is 4294967295

```
  Routing Descriptor Blocks:
  10.4.1.5 (Ethernet1/0), from 10.4.1.5, Send flag is 0x0
      Composite metric is (2681856/2169856), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 40000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

<#root>

```
R1#
```

show ip route 192.168.1.0 255.255.255.0

```
Routing entry for 192.168.1.0/24
  Known via "eigrp 1", distance 90, metric 2681856, type internal
  Redistributing via eigrp 1
  Last update from 10.3.1.6 on Serial2/0, 00:04:16 ago
  Routing Descriptor Blocks:
  * 10.3.1.6, from 10.3.1.6, 00:04:16 ago, via Serial2/0
      Route metric is 2681856, traffic share count is 1
      Total delay is 40000 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
```

Informazioni correlate

- Supporto tecnico Cisco e download

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).