

# Resuelva problemas comunes de EIGRP

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Intermitencia de vecinos](#)

[Problemas de red](#)

[SIA](#)

[Temporizador de espera caducado](#)

[Límite de reintentos excedido](#)

[Par reiniciado](#)

[Actualización inicial antes del paquete de saludo](#)

[Problemas adicionales](#)

[Cambios de configuración](#)

[Autenticación](#)

[Direcciones IP principales y secundarias no coincidentes](#)

[DMVPN](#)

[Explicación de los indicadores](#)

[SIA](#)

[Definición de SIA](#)

[Síntomas](#)

[Posibles Causas](#)

[Consejos para Troubleshooting](#)

[Prefijos faltantes](#)

[Prefijos faltantes en RIB](#)

[Prefijo instalado mediante el protocolo de routing con la menor distancia administrativa](#)

[El comando distribute-list bloquea el prefijo](#)

[Prefijos faltantes en la tabla de topología](#)

[Especificación de máscara para el resultado correcto del comando](#)

[El comando split-horizon bloquea el prefijo](#)

[Métrica](#)

[ID de router duplicado](#)

[Valores de K no coincidentes/Apagado correcto](#)

[Balance de carga de costo distinto \(variación\)](#)

[Vecinos estáticos](#)

[Redistribución de rutas estáticas](#)

[Confiabilidad y carga para el cálculo de métricas](#)

[Uso elevado de la CPU](#)

[EIGRP en las redes de Frame Relay \(cola de difusión\)](#)

[Números AS no coincidentes](#)

[Auto-Summary \(Resumen automático\)](#)

---

## Introducción

Este documento describe cómo solucionar los problemas más comunes del protocolo EIGRP (Enhanced Interior Gateway Routing Protocol).

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

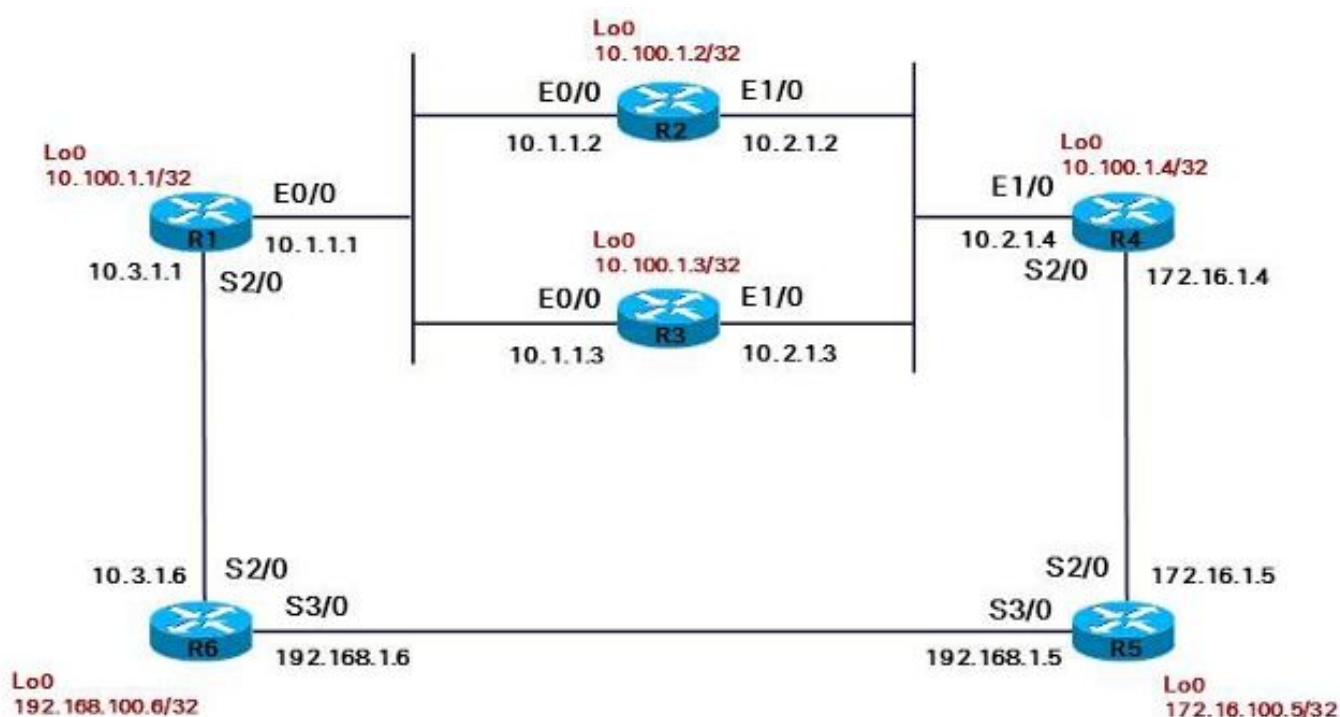
### Componentes Utilizados

La información de este documento se basa en Cisco IOS® para ilustrar los diversos comportamientos que se pueden encontrar con este protocolo.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Esta es la topología que se utiliza en este documento:



En las siguientes secciones se describen algunos de los problemas más comunes de EIGRP y se ofrecen algunas sugerencias sobre cómo solucionar los problemas.

## Intermitencia de vecinos

El único problema más común que se encuentra en el uso de EIGRP es que no establece correctamente un vecino. Existen varias causas posibles de esto:

- Problema en la unidad máxima de transferencia (MTU)
- Comunicación unidireccional (enlaces unidireccionales)
- Hay un problema de multidifusión en el enlace
- Problemas de unidifusión
- Problemas de calidad del enlace
- Problemas de autenticación
- Problemas de configuración errónea

Si no recibe un mensaje de saludo de EIGRP, no podrá ver al vecino en la lista de vecinos. Introduzca el comando `show ip eigrp neighbors` para ver la información del vecino de EIGRP e identificar el problema:

```
<#root>
```

```
R2#
```

```
show ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1
H  Address                Interface      Hold Uptime    SRTT   RTT  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
```

Si usted piensa que se ha formado la vecindad, pero no tiene los prefijos que debe aprender de ese vecino, verifique la salida del comando anterior: Si el Q-count es siempre distinto de cero, podría ser una indicación de que los mismos paquetes EIGRP se retransmiten continuamente. Introduzca el comando `show ip eigrp neighbors detail` para verificar si siempre se envía el mismo paquete. Si el número de secuencia del primer paquete es siempre el mismo, el mismo paquete se retransmite indefinidamente:

```
<#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
```

En el resultado, puede ver que el primer vecino tiene un problema y que el tiempo de actividad se restablece.

Es importante que verifique si el router de proceso EIGRP tiene el comando `eigrp log-neighbor-changes`. Sin embargo, este comando se incluye de manera predeterminada desde el error de Cisco [CSCdx67706](#), por lo que no aparece en la configuración en ese caso. Verifique la entrada de los registros de los dos vecinos EIGRP a cada lado del enlace. En al menos uno de los registros, debe haber una entrada significativa.

Estas son todas las razones posibles para un cambio de vecino EIGRP y sus entradas de registro:

- No se recibió ningún paquete de EIGRP durante el tiempo de espera:

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

- No se confirmó un paquete confiable de EIGRP dentro del límite de reintentos:

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

- El EIGRP ve la interfaz en estado inactivo:

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

- El router recibió un paquete de actualización inicial y reinició al vecino:

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

- El router recibió un paquete de actualización inicial y formó una nueva adyacencia:

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

- Se introdujo el comando `clear ip eigrp neighbor`, que dio lugar a un borrado manual:

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

- Se cambió la dirección IP en la interfaz:

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

- Hubo un cambio de demora/ancho de banda en la interfaz:



Nota: Esto sólo ocurre en versiones de código anteriores. No hay intermitencia de vecinos a partir de la ID de error de Cisco [CSCdp08764](https://www.cisco.com/cisco/web/errata/CSCdp08764).

---

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

- Los valores de K están mal configurados o se produce un apagado correcto :

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

- Se produce un apagado correcto:

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

- El comando ip authentication mode eigrp 1 md5 se configuró en la interfaz:

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

- Se produjo un reinicio correcto/Non-Stop Forwarding (NSF):

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

- Los vecinos a los que se enviaron consultas sin recibir respuesta se borran:

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

## Problemas de red

Estos cinco problemas indican un problema de red:

- Estado Stuck-In-Active (SIA)
- Un temporizador de espera caducado
- Un límite de reintentos excedido
- Un par reiniciado
- Se envía una actualización inicial antes del paquete de saludo.

### SIA

Consulte la sección [SIA de este documento](#).

### Temporizador de espera caducado

Un temporizador de espera caducado indica que el router no recibió ningún paquete EIGRP (es decir, un paquete de saludo EIGRP o cualquier otro paquete EIGRP) durante el intervalo de

tiempo de espera. En este caso, es más que probable que haya un problema en el enlace.

Verifique que el router reciba los paquetes de saludo de EIGRP en este enlace y que el otro lado los envíe. Para verificar esto, introduzca el comando `debug eigrp packet hello`. Como alternativa al uso del comando `debug`, puede hacer ping a la dirección IP 224.0.0.10 y verificar si ese vecino responde. Las causas posibles del problema de multidifusión en el enlace son problemas de interfaz, como si un switch intermedio bloquea los paquetes de saludo de EIGRP.

Otra prueba rápida que puede realizar es probar con otro protocolo que use otra dirección IP de multidifusión. Por ejemplo, puede configurar la versión 2 del Protocolo de Información de Enrutamiento (RIP), que utiliza la dirección IP de multidifusión 224.0.0.9.

### Límite de reintentos excedido

Un límite de reintentos excedido indica que un paquete confiable de EIGRP no se confirmó varias veces. Un paquete confiable de EIGRP es uno de estos cinco tipos de paquetes:

- Actualización
- Consulta
- Respuesta
- SIA-Query
- SIA-Reply

El paquete de EIGRP confiable se retransmitió al menos 16 veces. Un paquete se retransmite cada Tiempo de Espera de Retransmisión (RTO). El RTO mínimo es de 200 ms y el máximo es de 5.000 ms. El RTO aumenta o disminuye dinámicamente a través de la observación de la diferencia de tiempo entre el momento en que se envía el paquete de EIGRP confiable y el momento en que se recibe el acuse de recibo. Cuando el paquete confiable no se confirma, el RTO aumenta. Si esto continúa, el RTO aumenta hasta cinco segundos rápidamente, por lo que el límite de reintentos puede llegar a  $16 \times 5$  segundos = 80 segundos. Sin embargo, si el tiempo de espera de EIGRP es superior a 80 segundos, la proximidad quedará inactiva cuando el tiempo de espera haya expirado. Esto puede ocurrir en los enlaces WAN lentos donde, por ejemplo, el tiempo de espera predeterminado es de 180 segundos.

En el caso de los enlaces con tiempos de espera inferiores a 80 segundos, esto significa que, si el tiempo de espera no expira, sino que lo mantienen los paquetes de saludo de EIGRP. Luego, se puede exceder el límite de reintentos. Esto indica que hay un problema de MTU o un problema de unidifusión. Los paquetes Hello de EIGRP son pequeños; el (primer) paquete de actualización de EIGRP puede alcanzar la MTU completa. Puede ser de tamaño MTU completo si hay suficientes prefijos para llenar la actualización. El vecino se puede aprender a través de la recepción de los paquetes Hello de EIGRP, pero la adyacencia completa no puede tener éxito si no se reconoce el paquete de actualización de EIGRP.

Por lo general, este es el resultado que aparece:

```
%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 partir del ID de bug de Cisco [CSCsc72090](https://www.cisco.com/cisco/web/bugtools/bugdetail.do?moduleId=3&bugtypeID=5062&bugid=72090), el EIGRP también utiliza la configuración de IP MTU de la interfaz. Antes de aplicar esta corrección, los paquetes EIGRP se fragmentarían si la MTU IP se configurara con un valor inferior a 1500. En general, este problema puede ocurrir en redes Dynamic Multipoint VPN (DMVPN).

Una segunda posibilidad es que los paquetes Hello de EIGRP lo logren porque son multicast a la dirección IP 224.0.0.10. Algunos paquetes de actualización EIGRP pueden hacerlo, ya que pueden ser de multidifusión. Sin embargo, los paquetes confiables retransmitidos EIGRP siempre son de unidifusión. Si la ruta de datos de unidifusión al vecino está dañada, el paquete confiable retransmitido no se procesa correctamente. Haga ping a la dirección IP de unidifusión de vecinos EIGRP (con el ping del tamaño de la MTU total del enlace y el bit Do Not Fragment (DF-bit) configurados) para verificarlo.

Un enlace unidireccional también puede causar este problema. El router EIGRP puede recibir los paquetes Hello de EIGRP, pero los paquetes que se envían desde este vecino no cruzan el link. Si los paquetes de saludo no se envían a través del enlace, el router no es consciente porque los paquetes de saludo no se envían de manera confiable. Los paquetes de actualización EIGRP que se envían no se pueden confirmar.

Los paquetes confiables de EIGRP o el acuse de recibo pueden estar dañados. Una prueba rápida consiste en enviar pings con la validación de respuestas habilitada:

```
<#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
```



Habilite el comando debug eigrp packets para verificar la transmisión y la recepción de los paquetes de saludo de EIGRP y los paquetes de actualización de EIGRP como mínimo:

<#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
```

Este es un ejemplo típico del problema del límite de reintentos excedido:

<#root>

R2#

show ip eigrp neighbors

IP-EIGRP neighbors for process 1

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq 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: Siempre hay uno o más paquetes en la cola (Q Cnt).

---

<#root>

R2#

```
show ip eigrp neighbors detail
```

IP-EIGRP neighbors for process 1

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq 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						

Como se muestra en la salida, R2 espera el primer paquete de actualización (*init bit set*) del vecino en la dirección IP 10.1.1.1.

En esta siguiente salida, R2 espera el reconocimiento del primer paquete de actualización (*init bit set*) del vecino en la dirección IP 10.1.1.1.

---

 Nota: El RTO está en su máximo de 5.000 ms, lo que indica que los paquetes confiables EIGRP no se reconocen en los cinco segundos.

---

<#root>

R2#

```
show ip eigrp neighbors detail
```

IP-EIGRP neighbors for process 1

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq 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
```

El número de retransmisiones aumenta de manera constante. Siempre es el mismo paquete en la cola (sec. 349). Después de que el R2 envía el mismo paquete 16 veces, la proximidad queda inactiva:

```
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
```

El proceso comienza una vez más:

```
<#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						

El resultado del comando `debug eigrp packets terse` muestra que el R2 envía el mismo paquete una y otra vez:

---

 Nota: el valor de reintento aumenta, el valor de Indicadores es 0x1 y se establece el bit Init.

---

<#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

El tiempo de espera no expira porque los paquetes de saludo se envían y se reciben correctamente:

<#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
```

Par reiniciado

Si observa que un par se reinicia repetidamente en un router, el router recibe los paquetes de actualización iniciales de su vecino. Tenga en cuenta el indicador 1 en los paquetes de actualización recibidos.

<#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
```

## Actualización inicial antes del paquete de saludo

Este es un ejemplo en el que se recibe el paquete de actualización inicial antes que el paquete de saludo:

```
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
```

Si esto ocurre una vez después de la intermitencia de un vecino, esta situación no es un problema. Sin embargo, si lo experimenta con frecuencia, indica que la unidifusión en el enlace está en funcionamiento, pero la multidifusión en el enlace se ha roto. En otras palabras, el router recibe el paquete de actualización de unidifusión, pero no los paquetes de saludo.

## Problemas adicionales


Algunos otros tipos de problemas incluyen:

- Cambios de configuración
- Problemas de autenticación
- Direcciones IP principales y secundarias no coincidentes
- Problemas de DMVPN

Estos problemas se explican con más detalle en las siguientes secciones.

## Cambios de configuración

---

 Nota: Los resultados de los comandos que se utilizan en esta sección son los mismos si configura la negación en su lugar (el comando no).

---

Al configurar la instrucción resumida (o el resumen automático) en la interfaz, observará este mensaje en el router:

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

Este es un ejemplo que muestra la configuración de un comando distribute-list global para el proceso de EIGRP:

```
<#root>
```

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

```
distribute-list 1 out
```

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

Este mensaje se observa en el router:

---

 Nota: lo mismo ocurre cuando configura una lista de distribución <> en también.

---


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

Luego, todos los vecinos EIGRP desaparecen al configurar un comando distribute-list de interfaz para el proceso EIGRP:

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

En este caso, solo se restablecen las proximidades de EIGRP en esta interfaz.

---

 Nota: Después del ID de bug Cisco [CSCdy20284](https://tools.cisco.com/bugcenter/bug/?bugID=CSCdy20284), las vecindades no se restablecen para cambios manuales como resumen y filtros.

---

## Autenticación

La autenticación puede estar mal configurada o ausente. Esto puede generar que la proximidad de EIGRP quede inactiva debido a que el límite de reintentos fue excedido. Habilite el comando debug eigrp packets para confirmar que es la autenticación Message Digest 5 (MD5) la que causa el problema:

```
<#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)
```

## Direcciones IP principales y secundarias no coincidentes

El EIGRP envía el saludo y todos los demás paquetes desde la dirección IP principal. Los paquetes se aceptan desde el otro router si las direcciones IP de origen caen en el rango de direcciones IP principales o en uno de los rangos de direcciones IP secundarias en la interfaz. De lo contrario, se observa este mensaje (cuando se habilita el comando `eigrp log-neighbor-warnings`):

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

## DMVPN

Verifique los problemas de IPsec en las redes DMVPN. El IPsec puede generar intermitencia en el EIGRP si el cifrado no fue borrado:

<#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
```

## Explicación de los indicadores

Hay un campo de indicadores de 32 bits en el encabezado del paquete EIGRP, y es útil comprender las indicaciones de los diversos valores de los indicadores.

- Indicador 0x1 init bit

Este indicador se establece en el paquete de actualización inicial.



<#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

- Indicador 0X2

Este indicador indica el modo de recepción condicional (modo CR). Esta es una parte del proceso de multidifusión de EIGRP confiable y se utiliza para permitir que los vecinos que no hayan confirmado un paquete confiable anterior puedan ponerse al día en un enlace compartido. Las direcciones en el valor de longitud de tipo (TLV) de secuencia son los pares que deben ignorar los paquetes multicast hasta que se pongan al día a través de los paquetes 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

- Indicador 0x4

Este indicador es el bit de reinicio (RS bit). Se establece en los paquetes de saludo y los paquetes de actualización cuando se señala la función NSF. Un router con reconocimiento de NSF ve este bit para detectar si el router vecino se reinicia. Entonces, el vecino que detecta sabe mantener la adyacencia de EIGRP. El router que reinicia ve este indicador para determinar si el par ayuda con el reinicio.

<#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

- Indicador 0x8

Este es el bit de fin de tabla (EOT). Este bit indica que se ha enviado la tabla de enrutamiento completa al vecino. Un router con capacidad de NSF ve este bit para determinar si el router vecino terminó de reiniciarse. Un router con capacidad de NSF

espera este bit antes de eliminar las rutas obsoletas del router que se reinicia.

```
<#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
```

Los indicadores se imprimen en un número hexadecimal. Por lo tanto, Indicador 0x5 significa que los Indicadores 4 y 1 están establecidos; Indicador 0x9 significa que los Indicadores 8 y 1 están establecidos; Indicador 0xA significa que los Indicadores 8 y 2 están establecidos.

Puede utilizar estos comandos para solucionar problemas de intermitencia en los vecinos:

- show eigrp interface detail
- show ip eigrp neighbor detail
- ping unicast
- ping with size full MTU
- ping con datos de respuesta de verificación
- ping multicast
- debug eigrp packet (hello)
- show ip eigrp traffic
- show ip traffic | begin EIGRP

## SIA

En esta sección, se proporciona una descripción general del estado SIA, algunos síntomas y causas posibles de problemas, y la manera de resolverlos.

### Definición de SIA

El estado SIA significa que un router EIGRP no ha recibido respuesta a una consulta de uno o más vecinos dentro del tiempo asignado (aproximadamente 3 minutos). Cuando esto sucede, el EIGRP borra a los vecinos que no envían una respuesta y registra un mensaje de error DUAL-3-SIA para la ruta que se activó.

### Síntomas

Estos mensajes pueden verse en uno o varios routers:

```
%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
```

Si esto solo ocurre esporádicamente, puede ignorarse. Si ocurre con frecuencia, indica que hay un problema de red persistente.

## Posibles Causas

Estas son algunas causas posibles de un estado SIA:

- Enlaces intermitentes
- Enlaces incorrectos
- Rutas intermitentes
- Enlaces congestionados
- Diámetro de red grande (rango de consultas grandes)
- Escasez de memoria
- Uso elevado de la CPU
- Configuración incorrecta (valor de ancho de banda incorrecto)

## Consejos para Troubleshooting

Cuando ocurre una situación SIA, hay un problema en alguna parte de la red. La causa exacta puede ser difícil de descubrir. Existen dos enfoques:

- Vea los prefijos que se informan sistemáticamente como SIA y determine las similitudes.
- Ubique el router que sistemáticamente no responde las consultas de estas rutas.

Determine si todos los prefijos que se informan como SIA tienen similitudes. Por ejemplo, todas pueden ser /32 rutas desde el borde de la red (como en las redes de acceso telefónico). Si es así, puede indicar la ubicación del problema en la red (es decir, dónde se originaron estos prefijos).

En última instancia, debe descubrir la ubicación desde la cual uno o más routers envían consultas y no reciben respuestas mientras el router que recibe la información no está en este estado. Por ejemplo, el router puede enviar consultas que son confirmadas, pero no se recibe respuesta del router que recibe la información.

Puede utilizar el comando `show ip eigrp topology active` para resolver más fácilmente el problema de SIA. Busque la pequeña `r` en el resultado del comando. Esto significa que el router espera una respuesta a una consulta de ese prefijo, de ese vecino.

Aquí está un ejemplo. Consulte la topología. Los enlaces R1-R6 y R1-R5 se apagan. Cuando la interfaz de bucle invertido del router R1 se apaga, el R1 envía una consulta para el prefijo 10.100.1.1/32 al R2 y al R3. El router R1 ahora está activo para este prefijo. Los routers R2 y R3 se activan y consultan a su vez el router R4, que se activa y envía una consulta al R5. Finalmente, el router R5 se activa y envía una consulta a R6. El router R6 debe devolver una respuesta al R5. El router R5 queda pasivo y responde al R4, que a su vez se torna pasivo y envía una respuesta al R2 y al R3. Por último, el R2 y el R3 quedan en modo pasivo y envían una

respuesta al R1, que vuelve a tornarse pasivo.

Si se encuentra un problema, un router puede permanecer activo durante un tiempo prolongado, ya que debe esperar una respuesta. Para evitar que el router espere una respuesta que nunca se puede recibir, el router puede declarar SIA y eliminar la vecindad a través de la cual espera la respuesta. Para solucionar el problema, consulte el resultado del comando show ip eigrp topology active y siga el rastro de la r.

Este es el resultado 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
```

El router R1 está activo y espera una respuesta del R2. Este es el resultado del 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
```

El router R2 está activo y espera una respuesta del R4. Este es el resultado del 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
```

El router R4 está activo y espera una respuesta del R5. Este es el resultado del 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
```

El router R5 está activo y espera una respuesta de R6. Este es el resultado del router R6:

```
<#root>
```

R6#

```
show ip eigrp topology active
```

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

R6#

Como se muestra, el router R6 no está activo para el prefijo, por lo que el problema debe estar entre los routers R5 y R6. Después de un tiempo, vemos que R5 elimina la proximidad con R6 y declara un estado de 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
```

Al ver el resultado del router R5, puede ver que hay problemas en el enlace hacia R6.

Este es el código de SIA nuevo, y como tal, el estado SIA se declaró en un router que estaba junto al del problema. En este ejemplo, es el enlace entre los routers R5 y R6. En las versiones de código anteriores, el SIA se podía declarar en cualquier router a lo largo de la trayectoria (como en R2), que puede estar distante del problema. El temporizador de SIA fue de tres minutos. Cualquier router a lo largo de la ruta podría ser el primero en declarar el SIA y eliminar a los vecinos. Con el código más reciente, el router espera una respuesta, a nivel intermedio, envía una consulta de SIA a su vecino y el vecino responde inmediatamente con una respuesta de SIA. Por ejemplo, mientras está en el estado activo, el router R4 envía una consulta de SIA al R5 y R5 envía una respuesta de 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
```

El router R5 también envía consultas de SIA a R6, pero no recibe una respuesta de SIA de R6.

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
```

Una vez que el router envía una consulta de SIA pero no recibe una respuesta de SIA, aparece la s para ese vecino:

```
<#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 el nuevo código SIA, el SIA debe declararse en el router R5 cuando no recibe una respuesta SIA. Luego debe habilitar la depuración para estos dos paquetes EIGRP SIA:

```
<#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)
```

En resumen, puede utilizar estos comandos para resolver problemas de SIA:

- show ip eigrp topology active
- show ip eigrp event (posiblemente aumente el tamaño del registro de eventos)

- show ip eigrp traffic (buscar muchas consultas de SIA y respuestas de SIA)
- show proc mem
- show mem sum

Estas son algunas soluciones posibles para el problema de SIA:

- Solucionar el problema del enlace.
- Aplicar el resumen (manual o automático) en las redes con muchos prefijos o un rango de consulta profundo.
- Utilizar listas de distribución para reducir el rango de consulta.
- Definir los routers remotos como stubs.

## Prefijos faltantes

Hay dos tipos de prefijos que faltan: los que faltan en la tabla de routing (o en la Base de información de routing [RIB]) y los que faltan en la tabla de topología.

### Prefijos faltantes en RIB

Puede haber varios motivos por los cuales un prefijo no se incluye en la RIB:

- El prefijo está instalado en la tabla de enrutamiento mediante otro protocolo de enrutamiento, con una menor distancia administrativa.
- El comando distribute-list bloquea el prefijo.
- El comando split-horizon bloquea el prefijo.

Prefijo instalado mediante el protocolo de routing con la menor distancia administrativa

En este ejemplo, el prefijo se instala en la tabla de enrutamiento mediante una ruta estática o un protocolo de enrutamiento con una distancia administrativa menor.

En general, cuando ocurre esto, el prefijo está en la tabla de topología, pero no tiene un sucesor. Puede ver todas estas entradas con el comando show ip eigrp topology zero-successors. La distancia factible (FD) debe tener un valor infinito.

Introduzca el comando show ip route <prefix> y verifique los protocolos de enrutamiento que poseen la ruta en la 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
```

El comando distribute-list bloquea el prefijo

El EIGRP es un protocolo de enrutamiento del vector de distancia. Puede utilizar un comando distribute-list en cualquier router para bloquear los prefijos. Puede utilizarlo en una interfaz para detener la transmisión o recepción de prefijos, o puede configurar la lista de distribución globalmente bajo el proceso EIGRP del router para aplicar el filtro de ruteo en todas las interfaces habilitadas para EIGRP.

Aquí tiene un ejemplo:

<#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
```

## Prefijos faltantes en la tabla de topología

En esta sección se describen algunas de las razones por las que puede faltar un prefijo en la tabla de topología.

Especificación de máscara para el resultado correcto del comando

No cometa el error típico; cuando verifique un prefijo en la tabla de topología, especifique siempre la máscara. Si no utiliza la máscara, ocurre lo siguiente:

```
<#root>  
  
R1#  
  
show ip eigrp topology 192.168.100.6  
  
% IP-EIGRP (AS 1): Route not in topology table
```

Este es el resultado del comando show ip eigrp topology cuando se especifica la máscara:

```
<#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
```

Como se muestra, el prefijo está presente en la tabla de topología.

El comando split-horizon bloquea el prefijo

En esta sección, se describe otro error común. EIGRP no es un protocolo de enrutamiento de estado de enlace, sino que es un protocolo de enrutamiento de vector de distancia. La tabla de topología se debe utilizar para el funcionamiento correcto del algoritmo de actualización difusa (DUAL), no porque el EIGRP sea un protocolo de ruteo de estado de link; por lo tanto, requiere una base de datos. Se requiere la tabla de topología porque solo las mejores rutas se instalan en la tabla de enrutamiento, mientras que el DUAL exige que también se supervisen las rutas factibles. Estas se almacenan en la tabla de topología.

Siempre debe tener la ruta sucesora y las rutas factibles en la tabla de topología. De lo contrario, se produce un error. Sin embargo, también podría haber rutas no factibles en la tabla de topología, siempre que se reciban. Si no se reciben de un vecino, podría haber un comando split-horizon que bloquea el prefijo.

El resultado del comando `show ip eigrp topology` muestra solo las entradas de prefijo que apuntan a sucesores y sucesores factibles. En cambio, si desea ver los prefijos que se reciben en todas las rutas (también las rutas no factibles), introduzca el comando `show ip eigrp topology all-links`.

Aquí tiene un ejemplo:

```
<#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
```

En esta salida, puede ver que la porción all-links del comando incluye más rutas:

```
<#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
```

Considere el último prefijo en la salida anterior; la trayectoria vía 10.4.1.5 tiene (2323456/2297856). La distancia notificada (métrica anunciada) es 2297856, que no es más pequeña que la FD de 2297856, por lo cual, la ruta no es factible.

```
<#root>
```

```
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
```

En este ejemplo, un comando split-horizon hace que la ruta de un enrutado se excluya de la tabla de topología. Cuando vea la topología, podrá ver que el router R1 tiene el prefijo 192.168.100.6/32 a través de R6 y R5 en la tabla de topología, pero no a través de 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
```

Esto se debe a que el router R1 nunca recibió el prefijo 192.168.100.6/32 a través del R2 o el R3, ya que estos obtienen el prefijo 192.168.100.6/32 a través del R1 en la tabla de enrutamiento.

<#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

Para verificar esto, utilice la palabra clave all-links en el R1 cuando vea la tabla de topología. Esto muestra todas las rutas de todos los prefijos, lo que incluye las rutas que no son factibles. A continuación, puede ver que el router R1 no ha detectado el prefijo 192.168.100.6/32 desde el R2 o el R3.

## Métrica



Nota: La MTU y el recuento de saltos no se incluyen en el cálculo de la métrica.

---

Estas son las fórmulas que se utilizan para calcular la métrica de ruta de un enrutado:

- Si K5 es un valor distinto de cero:

$$\text{Métrica de EIGRP} = 256 * (((K1 * AB) + (K2 * AB) / (256 - \text{carga}) + (K3 * \text{demora})) * (K5 / (\text{confiabilidad} + K4)))$$

- Si K5 es igual a cero:

$$\text{Métrica de EIGRP} = 256 * ((K1 * AB) + (K2 * AB) / (256 - \text{carga}) + (K3 * \text{demora}))$$

Los valores K son pesos que se utilizan para ponderar los cuatro componentes de la métrica EIGRP: retraso, ancho de banda, confiabilidad y carga. Estos son los valores K predeterminados:


- K1 = 1
- K2 = 0
- K3 = 1
- K4 = 0
- K5 = 0

Con los valores K predeterminados (sólo con ancho de banda y retraso), la fórmula se convierte en:

$$\text{Métrica de EIGRP} = 256 * (AB + \text{demora})$$

$$AB = (10^7 / \text{tamaño mínimo de AB en kilobits por segundo})$$

---

 Nota: El retardo se mide en decenas de microsegundos; sin embargo, en la interfaz, se mide en microsegundos.

---

Los cuatro componentes pueden verificarse con el 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
```

La demora es acumulativa, lo que significa que usted agrega la demora de cada enlace a lo largo de la ruta. El ancho de banda no es acumulativo, por lo que el ancho de banda que se utiliza en la fórmula es el ancho de banda más pequeño de cualquier enlace a lo largo de la ruta.

## ID de router duplicado

Para ver la ID de router que utiliza el EIGRP, introduzca el comando `show ip eigrp topology` en el router y vea la primera línea del resultado:

```
<#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
```

La ID de router del EIGRP no se utiliza en absoluto para las rutas internas en versiones anteriores de Cisco IOS. Un ID de router duplicado para el EIGRP no debe causar ningún problema si sólo se utilizan rutas internas. En el software Cisco IOS más reciente, las rutas internas de EIGRP tienen la ID de router de EIGRP.

La ID de router de las rutas externas puede verse en este resultado:

```
<#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:;  
  
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)
```

Si se recibe una ruta de EIGRP (externa) con la misma ID de router de EIGRP que el router, no se genera una entrada de registro. Sin embargo, el registro de eventos de EIGRP lo captura. Cuando se busca la ruta de EIGRP (externa), esta no aparece en la tabla de topología.

Revise el registro de eventos de EIGRP para buscar posibles mensajes de ID de router duplicado:

```
<#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
```

## Valores de K no coincidentes/Apagado correcto

Cuando los valores K no son los mismos en los routers vecinos, se observa este mensaje:

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

Los valores K se configuran con este comando (con los valores posibles de K entre 0 y 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
```

```
!
```

El mensaje indica que el vecino EIGRP no se estableció debido a una incompatibilidad en los valores K. Los valores K deben ser los mismos en todos los routers EIGRP, en un sistema autónomo, para evitar problemas de enrutamiento cuando diferentes routers utilizan cálculos de métricas diferentes.

Verifique si los valores K son los mismos en los routers vecinos. Si los valores K son iguales, el problema puede ser causado por la función de cierre de gracia EIGRP. En ese caso, un router

envía un paquete de saludo de EIGRP con los valores K establecidos en 255 para que se produzca la falta de coincidencia de los valores K intencionalmente. Esto es para indicar al router EIGRP vecino que se desactiva. En el router vecino, debería recibirse este mensaje de despedida:

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

Sin embargo, si el router vecino ejecuta una versión de código más antigua (antes de la ID de error de Cisco [CSCdr96531](#)), no reconoce esto como un mensaje de apagado correcto, sino como una incompatibilidad en los valores K:

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

Este es el mismo mensaje que en el caso de una verdadera incompatibilidad de valores K en los routers vecinos.

Estos son los desencadenantes de un apagado correcto:

- Se introduce el comando no router eigrp.
- Se introduce el comando no network.
- Se introduce el comando clear ip eigrp neighbor.
- Se vuelve a cargar el router.

Se utiliza el apagado correcto para acelerar la detección del estado de inactividad de un vecino. Sin un apagado correcto, un vecino debe esperar que finalice el tiempo de espera para declarar que el vecino está inactivo.

## Balance de carga de costo distinto (variación)

El balance de carga de costo distinto es posible en EIGRP con el comando variance, pero deben cumplirse las condiciones de variación y factibilidad.

La condición de variación significa que la métrica de la ruta no es superior a la mejor métrica multiplicada por la variación. Para que una ruta se considere factible, se debe haber anunciado la ruta con una distancia notificada inferior a la distancia factible (FD). Aquí tiene un ejemplo:

```
<#root>
```

```
!
router eigrp 1
```

variance 2

```
network 10.0.0.0
no auto-summary
!
```

El router R1 tiene configurada una variación 2. Esto significa que si el router tiene otra trayectoria para la ruta con una métrica que no es mayor que el doble de la mejor métrica para esa ruta, debe haber un balanceo de carga de costo desigual para esa ruta.

<#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
```

Si la segunda entrada de topología está instalada en la tabla de enrutamiento, la métrica de la segunda entrada de topología es 435200. Dado que el doble de la mejor métrica es  $2 \times 409600 = 819200$ , y  $435200 < 819200$ , la segunda entrada de topología está dentro del rango de variación. La distancia notificada de la segunda entrada de topología es 409600, que no es inferior a la  $FD =$

409600. La segunda condición (factibilidad) no se cumple y la segunda entrada no puede instalarse en la 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
```

Si la RD de la segunda entrada de topología es inferior a la FD, como en el siguiente ejemplo, habría un balance de carga de costo distinto.

```
<#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
```

Ambas entradas de topología ahora están en la tabla de enrutamiento:

```
<#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
```

## Vecinos estáticos

El EIGRP admite configuraciones con uno o más vecinos estáticos en la misma interfaz. Tan pronto como configura un vecino EIGRP estático en la interfaz, el router ya no envía los paquetes EIGRP como multidifusión en esa interfaz o procesa los paquetes EIGRP de multidifusión recibidos. Esto significa que los paquetes de saludo, actualización y consulta ahora son de unidifusión. No se pueden formar proximidades adicionales a menos que el comando `static neighbor` esté configurado explícitamente para esos vecinos en esa interfaz.

Aquí se describe cómo configurar un vecino EIGRP estático:

```
<#root>
```

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

```
neighbor 10.1.1.1 Ethernet0/0
```

```
!
```

Cuando los routers de ambos lados del enlace tienen el comando static neighbor, se forma la proximidad:

```
<#root>
```

```
R1#
```

```
show ip eigrp neighbors detail
```

```
IP-EIGRP neighbors for process 1
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RT0	Q Cnt	Seq Num
1	10.1.1.2	Et0/0	14	00:00:23	27	200	0	230

```
Static neighbor
```

0	10.3.1.6	Se2/0	14	1d02h	26	200	0	169
3	10.4.1.5	Et1/0	10	1d02h	16	200	0	234

Si sólo un router tiene configurado el comando static neighbor, puede observar que el router ignora los paquetes EIGRP multicast y que el otro router ignora los paquetes 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
```

Hay un comando de depuración especial para vecinos EIGRP estáticos:

```
<#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
```

A continuación se indican algunas razones por las que se pueden configurar los vecinos EIGRP estáticos:

- Desea limitar o evitar difusiones en redes de acceso múltiple sin difusión (NBMA).
- Desea limitar o evitar multidifusiones en medios de difusión (Ethernet).
- Utilícelo para solucionar problemas (con unidifusión en lugar de multidifusión).

---

 Precaución: no configure el comando `passive-interface` junto con el comando `static EIGRP neighbor`.

---

## Redistribución de rutas estáticas

Cuando configura una ruta estática que apunta a una interfaz, y la ruta está sujeta a una instrucción de red en el router EIGRP, la ruta estática es anunciada por el EIGRP como si fuera una ruta conectada. En este caso, no se requiere el comando `redistribute static` ni una métrica predeterminada.

```
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
```

## Confiabilidad y carga para el cálculo de métricas

---

 Precaución: no utilice confiabilidad y/o carga para calcular métricas.

---

Los parámetros de confiabilidad y de carga aparecen en el resultado del comando show interface. No hay actualizaciones dinámicas para estos parámetros cuando cambia la carga y la confiabilidad. Si la carga y la confiabilidad cambian, no se desencadena un cambio inmediato en la métrica. Solo si el EIGRP decide enviar actualizaciones a sus vecinos debido a los cambios de topología, puede producirse un cambio en la carga y la confiabilidad. Además, el uso de la carga y la confiabilidad para calcular la métrica puede generar inestabilidad, ya que se realiza un enrutamiento adaptable. Si desea cambiar el routing de acuerdo con la carga de tráfico, debe considerar el uso de ingeniería de tráfico de switching de etiquetas multiprotocolo (MPLS) o routing de rendimiento (PfR).

## Uso elevado de la CPU

Existen tres procesos de EIGRP que se ejecutan simultáneamente:

- Router: Este proceso contiene los conjuntos de memoria compartidos.
- Hello: Este proceso envía y recibe los paquetes de saludo y mantiene las conexiones entre pares.
- Módulo dependiente del protocolo (PDM): el EIGRP admite cuatro conjuntos de protocolos: IP, IPv6, IPX y AppleTalk. Cada familia tiene su propio PDM. Estas son las funciones principales de PDM:
  - Mantiene a los vecinos y las tablas de topología de los routers EIGRP que pertenecen a esa familia de protocolos.
  - Crea y traduce paquetes específicos del protocolo para DUAL (transmisión y recepción de paquetes EIGRP).
  - Conecta a DUAL con la tabla de enrutamiento específica del protocolo.
  - Calcula la métrica y transmite la información a DUAL (DUAL solo selecciona los sucesores y los sucesores factibles).
  - Implementa listas de filtrado y acceso.
  - Realiza funciones de redistribución hacia otros protocolos de enrutamiento y desde ellos.

El siguiente modelo de resultado muestra estos tres procesos:

```
<#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
```

El uso elevado de la CPU en el EIGRP no es normal. Si esto ocurre, el EIGRP tiene demasiada actividad o hay un error en EIGRP. En el primer caso, verifique la cantidad de prefijos en la tabla de topología y la cantidad de pares. Verifique la inestabilidad entre las rutas y los vecinos EIGRP.

## EIGRP en las redes de Frame Relay (cola de difusión)

En las redes Frame Relay en las que hay varios routers vecinos en una interfaz punto a multipunto, puede haber muchos paquetes de difusión o de multidifusión que deben transmitirse. Por este motivo, hay una cola de transmisión separada con sus propios búferes. La cola de broadcast tiene prioridad cuando transmite a una velocidad por debajo del máximo configurado y tiene una asignación de ancho de banda mínima garantizada.

Este es el comando que se utiliza en esta situación:

```
<#root>
frame-relay broadcast-queue size byte-rate packet-rate
```

Como regla general, comience con 20 paquetes por identificador de conexión de enlace de datos (DLCI). La velocidad de bytes debe ser menor que ambos:

- $N/4$  veces la velocidad mínima de acceso remoto (medida en bytes por segundo), donde  $N$  es la cantidad de identificadores DLCI en los que debe replicarse la difusión.
- $1/4$  la velocidad de acceso local (medida en bytes por segundo).

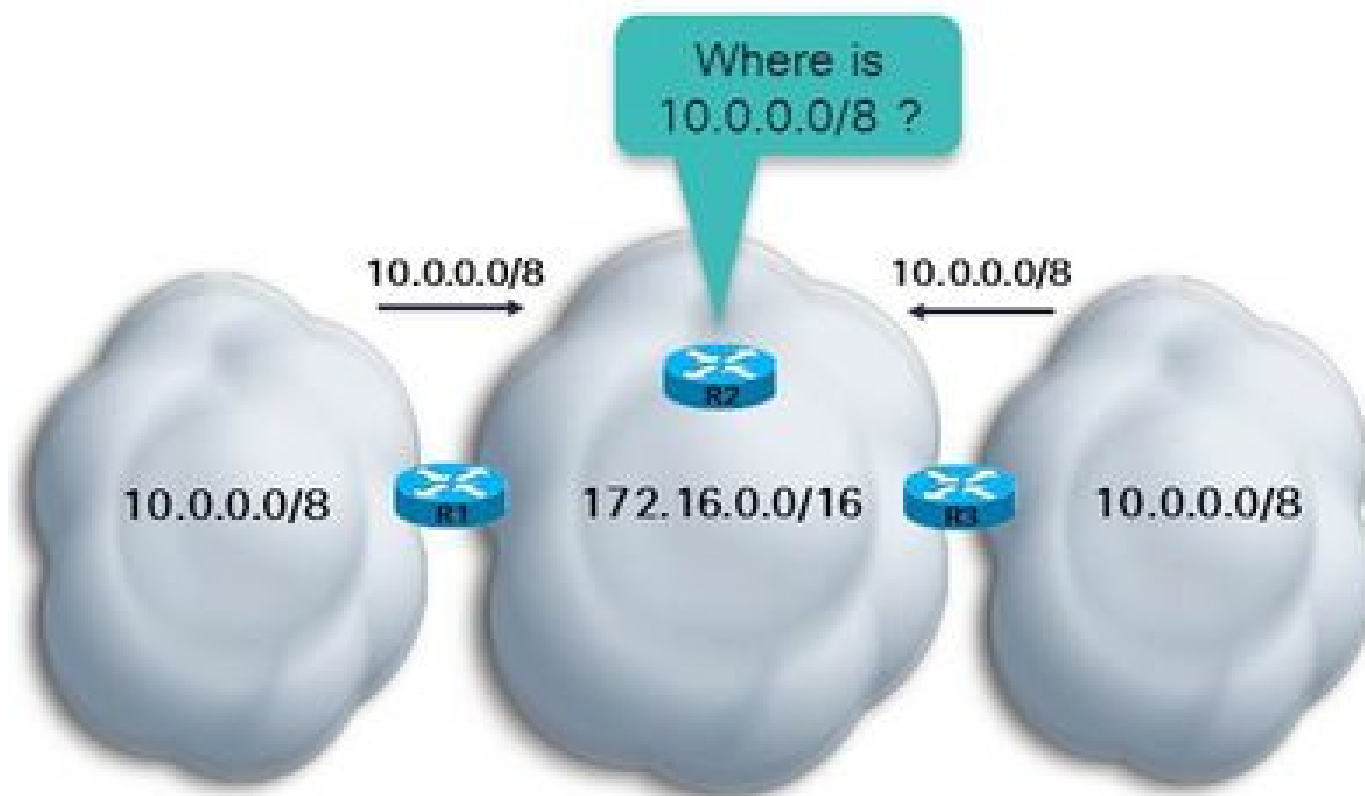
Si observa una gran cantidad de vecinos EIGRP con intermitencia, aumente el tamaño de la cola de difusión de Frame Relay. Este problema no se produce si hay subinterfaces de Frame Relay, porque cada router vecino está en una subinterfaz con una subred IP diferente. Considere esto como una solución alternativa cuando hay una red de Frame Relay de malla completa.

## Números AS no coincidentes

Cuando ingresa el comando `debug eigrp packets hello`, se revela que el router no recibe los paquetes de saludo.

## Auto-Summary (Resumen automático)

El EIGRP solía realizar el resumen en los límites de la red principal (redes A, B y C) de modo predeterminado. Esto significa que las rutas más específicas que los prefijos /8 para el tipo de red principal A, las rutas más específicas que los prefijos /16 para el tipo de red principal B y las rutas más específicas que los prefijos /24 para el tipo de red principal C, se pierden cuando cruzan los límites. En este ejemplo, el comando `auto-summary` causa un problema:



Como se muestra, los routers R1 y R3 tienen el comando `auto-summary` en el router de EIGRP. El router R2 recibe 10.0.0.0/8 de los routers R1 y R3, ya que tanto el R1 como el R3 son routers de límite entre la red principal de clase A 10.0.0.0/8 y 172.16.0.0/16. El router R2 puede tener la ruta 10.0.0.0/8 a través del R1 y el R3 si la métrica es la misma. De lo contrario, el R2 tiene la ruta 10.0.0.0/8 a través del R1 o a través del R3, según la ruta que genera el menor costo. En cualquier caso, si el R2 debe enviar tráfico a ciertas subredes de 10.0.0.0/8, no puede estar completamente seguro de que el tráfico llega a su destino, ya que una subred de 10.0.0.0/8 solo

puede estar en la nube de la red izquierda o derecha.

Para mitigar este problema, simplemente escriba `no auto-summary` en el proceso EIGRP del router. Luego, el router propaga las subredes de las redes principales a través del límite. En las versiones de Cisco IOS más recientes, la configuración `no auto-summary` es el comportamiento predeterminado.

## Registro de eventos de EIGRP

El registro de eventos de EIGRP captura los eventos de EIGRP. Es similar a cuando se habilitan las depuraciones de EIGRP. Sin embargo, es menos disruptiva y se ejecuta de manera predeterminada. Se puede utilizar para capturar eventos que son más difíciles de resolver o eventos más intermitentes. De manera predeterminada, este registro tiene solo 500 líneas. Para agrandarlo, introduzca el comando `eigrp event-log-size<0 – 209878>`. Puede aumentar el tamaño del registro tanto como lo desee, pero tenga en cuenta la cantidad de memoria que el router tiene para este registro. Para borrar el registro de eventos de EIGRP, ingrese el comando `clear ip eigrp events`.

Aquí tiene un ejemplo:

```
<#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
```

Los eventos más recientes aparecen en la parte superior del registro. Puede filtrar ciertos tipos de eventos de EIGRP, como DUAL, Xmit y transporte:

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

Además, puede habilitar el registro para uno de estos tres tipos, una combinación de dos tipos o para los tres. Este es un ejemplo en el que se habilitan dos tipos de registro:


```
<#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
!
```

---

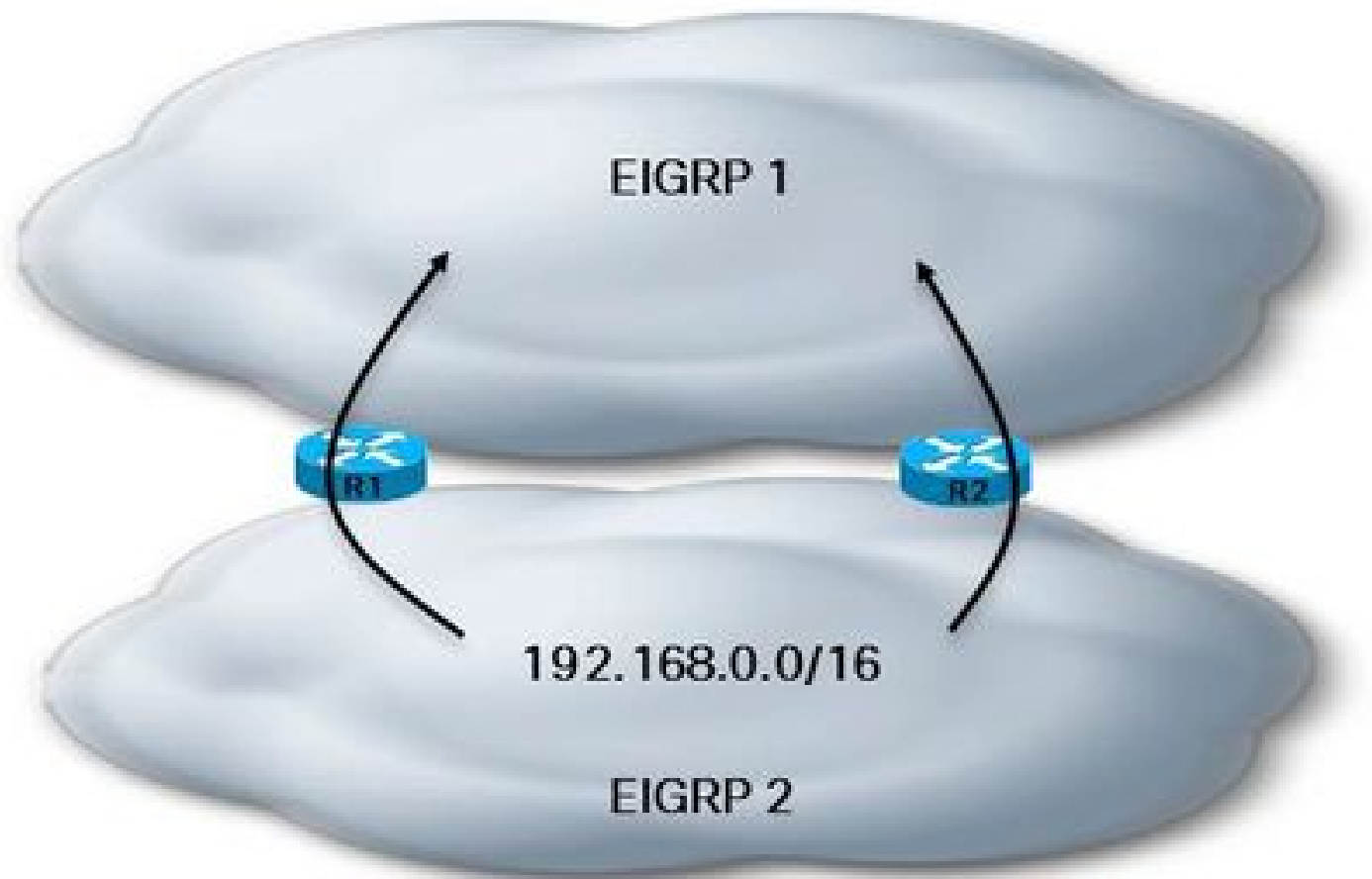
 **Precaución:** Cuando habilita el registro de eventos eigrp, imprime el registro de eventos y lo almacena en la tabla de eventos. Esto puede generar a una gran cantidad de resultados impresos en la consola, de manera similar a cuando se habilita la depuración intensa de EIGRP.

---

## Misma red detectada por dos sistemas autónomos de EIGRP

Si se detecta una ruta a través de dos procesos de EIGRP, solo uno de los procesos de EIGRP puede instalar la ruta en la RIB. Este proceso con la menor distancia administrativa instala la ruta. Si la distancia administrativa es la misma, el proceso con la métrica más baja instala la ruta. Si la métrica también es la misma, el proceso de EIGRP con la ID de proceso de EIGRP más baja instala la ruta en la RIB. La tabla de topología del otro proceso EIGRP puede tener la ruta instalada con cero sucesores y un valor FD infinito.

Aquí tiene un ejemplo:



```
<#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

## Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).