

SAPS

Riešenie problémov s EIGRP pre IPv4

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

*Katedra počítačov a informatiky
Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach*



Kapitola 4 Obsah

Táto kapitola zahŕňa nasledujúci obsah:

- **Riešenie problémov so susedskými vzťahmi EIGRP pre IPv4** - Táto časť sa zaoberá dôvodmi, prečo sa susedské vzťahy EIGRP pre IPv4 nemusia vytvoriť, a spôsobmi ich identifikácie.
- **Riešenie problémov s trasami EIGRP pre IPv4** - V tejto časti sa skúmajú dôvody, prečo môžu trasy EIGRP pre IPv4 chýbať v tabuľke EIGRP alebo smerovacej tabuľke smerovača a ako zistiť, prečo chýbajú.
- **Riešenie rôznych problémov EIGRP pre IPv4** - V tejto časti sú uvedené niektoré ďalšie problémy, s ktorými sa môžete stretnúť pri používaní EIGRP, ako ich identifikovať a ako ich vyriešiť.
- **EIGRP pre IPv4 Trouble Tickets** - Táto časť obsahuje tri hlásenia problémov, ktoré ukazujú, ako použiť štruktúrovaný proces riešenia problémov na vyriešenie nahláseného problému.

pril'ahlými susedmi protokolu EIGRP pre IPv4

- EIGRP nadväzuje susedské vzťahy odosielaním paketov hello na multicastovú adresu 224.0.0.10, z rozhraní zapojených do procesu EIGRP.
- Táto časť sa zameriava na dôvody, prečo sa vzťahy susedov EIGRP nemusia vytvoriť, a na to, ako ich môžete identifikovať počas procesu odstraňovania problémov.

Riešenie problémov s príľahlými susedmi protokolu EIGRP pre IPv4

Susedia EIGRP

Proces EIGRP sa spolieha na úspešné nadviazanie susedských vzťahov s ostatnými smerovačmi v tom istom autonómnom systéme. Niekedy sa z rôznych dôvodov susedské vzťahy úspešne nevytvoria.

Na overenie susedov EIGRP použijete príkaz **show ip eigrp neighbors**. Vo výstupe príkazu je uvedená adresa IPv4 rozhrania susedného zariadenia, ktoré odoslalo paket hello, miestne rozhranie na smerovači použité na dosiahnutie tohto suseda, ako dlho bude miestny smerovač považovať susedný smerovač za suseda, ako dlho sú smerovače susedmi, čas, za ktorý susedia v priemere komunikujú, počet paketov EIGRP vo fronte čakajúcich na odoslanie susedovi a sekvenčné číslo na sledovanie paketov EIGRP s cieľom zabezpečiť, aby sa prijali a spracovali len novšie pakety od suseda.

Example 4-1 *Verifying EIGRP Neighbors with show ip eigrp neighbors*

```
R2# show ip eigrp neighbors
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.1.23.3	Gi1/0	14	10:01:09	72	432	0	3
0	10.1.12.1	Gi0/0	11	10:32:14	75	450	0	8

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4

Základné témy

Vzťahy so susedmi EIGRP sa nemusia vytvoriť z rôznych dôvodov vrátane nasledujúcich:

- **Interface is down** - Rozhranie musí byť zapnuté/vypnuté.
- **Nesúlad čísel autonómnych systémov** - oba smerovače musia používať rovnaké číslo autonómneho systému.
- **Nesprávny príkaz siete** - príkaz siete musí identifikovať IP adresu rozhrania, ktoré chcete zahrnúť do procesu EIGRP.
- **Nesúlad hodnôt K** - oba smerovače musia používať presne rovnaké hodnoty K.
- **Pasívne rozhranie** - funkcia pasívneho rozhrania potláča odosielanie a prijímanie paketov hello, pričom stále umožňuje inzerovať sieť rozhrania.
- **Rôzne podsiete** - Výmena paketov hello sa musí uskutočňovať v tej istej podsieti;
- ak nie je, pakety hello sa ignorujú.
- **Overovanie** - Ak sa používa overovanie, ID kľúča a reťazec kľúča sa musia zhodovať a kľúč musí byť platný (ak boli nakonfigurované platné časy).
- **ACL** - Zoznam riadenia prístupu (ACL) môže odmietať pakety na multicastovú adresu EIGRP 224.0.0.10.
- **Časovače** - časovače sa nemusia zhodovať, ak však nie sú správne nakonfigurované, susedné adjacency sa mohli rozpadnúť.

Riešenie problémov s prilahlými susedmi protokolu EIGRP pre IPv4

Nesúhlasné čísla autonómnych systémov

Rozhranie je vypnuté

Rozhranie musí byť zapnuté, ak plánujete vytvoriť susedské spojenie EIGRP. Stav rozhrania môžete overiť príkazom **show ip interface brief**. Stav by mal byť uvedený ako **up** a protokol by mal byť uvedený ako **up**.

Nesúhlasné čísla autonómnych systémov

Na vytvorenie susedského vzťahu EIGRP musia byť oba smerovače v tom istom autonómnom systéme. Číslo autonómneho systému zadáte, keď v režime globálnej konfigurácie vydáte príkaz **router eigrp autonomous_system_number**. Najlepší príkaz na zobrazenie čísla autonómneho systému je **show ip protocols**, ktorý zobrazí neuveriteľné množstvo informácií na riešenie problémov, ako je uvedené v príklade 4-2.

Example 4-2 Verifying the Autonomous System Number with show ip protocols

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"

  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
```

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4 Nesúhlasné čísla AS (pokračovanie)

Výstup príkazu **debug eigrp packets** uvedený v príklade 4-3 naznačuje, že smerovač neprijíma žiadne pakety hello od susedov s nezhodným číslom autonómneho systému.

V tomto príklade R1 posiela pakety ahoj z Gi0/0 a Gi1/0. Neprijíma však žiadne pozdravné pakety. Dôvodom môže byť nezhoda autonómneho systému spôsobená tým, že niektorý zo smerovačov má nakonfigurované nesprávne číslo autonómneho systému.

Example 4-3 Sample Output of debug eigrp packets When an Autonomous System Mismatch Exists

```
R1# debug eigrp packets
(UPDATE, REQUEST, QUERY, REPLY, HELLO, UNKNOWN, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
EIGRP Packet debugging is on
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
      AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1#
EIGRP: Sending HELLO on Gi1/0 - paklen 20
      AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1#
EIGRP: Sending HELLO on Gi0/0 - paklen 20
      AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# 1
EIGRP: Sending HELLO on Gi1/0 - paklen 20
      AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# 1
EIGRP: Sending HELLO on Gi0/0 - paklen 20
      AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0
R1# u all
All possible debugging has been turned off
```

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4

Nesprávny výpis siete

Ak je **siet'ový** príkaz zle nakonfigurovaný, EIGRP nemusí byť povolený na správnych rozhraniach,

a v dôsledku toho nebudú odosielané pakety ahoj a nebudú vytvorené susedské vzťahy. Príkaz **show ip eigrp interfaces** zobrazí rozhrania, ktoré sa zúčastňujú na procese EIGRP . V príklade 4-4 napríklad vidíte, že na procese EIGRP pre autonómny systém 100 sa zúčastňujú dve rozhrania. Gi0/0 nemá partnera EIGRP a Gi1/0 má partnera EIGRP.

Example 4-4 Verifying EIGRP Interfaces with show ip eigrp interfaces

```
R2# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Gi0/0	0	0/0	0	0/0	0	0
Gi1/0	1	0/0	78	0/0	300	0

Nezabudnite, že pasívne rozhrania EIGRP sa v tomto výstupe nezobrazujú. Ak rozhranie chýba, je možné, že je nakonfigurované ako pasívne.

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4 Nesprávny výpis siete (pokračovanie)

Výstup príkazu **show ip protocols** zobrazuje rozhrania, na ktorých je spustený protokol EIGRP ako výsledok **sieťových** príkazov. Zamerajte sa na zvýraznený text v príklade 4-5. Výstup v časti *Smerovanie pre siete* uvádza adresy rozhraní, na ktorých bude EIGRP povolený na základe **sieťových** príkazov. V tomto prípade **10.1.1.1/32** v skutočnosti znamená **sieť 10.1.1.1 0.0.0.0** a **10.1.12.1/32** v skutočnosti znamená **sieť 10.1.12.1 0.0.0.0**. Preto je lepšou možnosťou použiť príkaz **show run | section router eigrp**, ako je zobrazené v príklade 4-6. Na identifikáciu rozhraní, ktoré nedosielajú pakety hello z dôvodu nesprávne nakonfigurovaných sieťových príkazov, môžete použiť aj funkciu **debug eigrp packets**.

Example 4-6 *Verifying network Statements with show run | section router eigrp*

```
R1# show run | section router eigrp
router eigrp 100
network 10.1.1.1 0.0.0.0
network 10.1.12.1 0.0.0.0
```

Example 4-5 *Verifying Network Statements with show ip protocols*

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  10.1.1.1/32
  10.1.12.1/32
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.12.2             90      09:54:36
Distance: internal 90 external 170
```

Riešenie problémov s prilahlými susedmi protokolu EIGRP pre IPv4

Nesúlad hodnôt K

Hodnoty K, ktoré sa používajú na výpočet metriky, sa musia medzi susedmi zhodovať, aby sa vytvorila adjacencia. Zvyčajne nie je potrebné hodnoty K meniť. Ak sa zmenia, musíte overiť, či sú rovnaké na každom smerovači v autonómnom systéme. To, či sa hodnoty K zhodujú, môžete overiť pomocou príkazu **show ip protocols**, ako je uvedené v príklade 4-7. Predvolené hodnoty K sú zvýraznené.

Nesúhlasné hodnoty K generujú správu syslogu s úrovňou závažnosti 5, ak je povolené protokolovanie.

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100:Neighbor
10.1.12.2
(GigabitEthernet1/0) je vypnutý: Nesúlad hodnôt
K
```

Example 4-7 Verifying K Values with show ip protocols

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.1.1.1/32
    10.1.12.1/32
  Routing Information Sources:
    Gateway      Distance    Last Update
    10.1.12.2          90    09:54:36
  Distance: internal 90 external 170
```

Riešenie problémov s príľahlými susedmi protokolu EIGRP pre IPv4

Pasívne rozhranie

Funkcia pasívneho rozhrania je nevyhnutná pre všetky organizácie. Umožňuje dve veci:

- Znižuje prevádzku súvisiacu s EIGRP v sieti
- Zlepšuje zabezpečenie EIGRP

Funkcia pasívneho rozhrania vypne odosielanie a prijímanie paketov EIGRP na rozhraní, pričom stále umožňuje, aby sa sieťové ID rozhrania vkladalo do procesu EIGRP a inzerovalo ostatným susedom EIGRP. Ak nakonfigurujete nesprávne rozhranie ako pasívne, legitímny susedský vzťah EIGRP sa nevytvorí. Ako ukazuje výstup **show ip protocols** v príklade 4-8, Gigabit Ethernet 0/0 je pasívne rozhranie.

Example 4-8 Verifying Passive Interfaces with show ip protocols

```
RI# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  10.1.1.1/32
  10.1.12.1/32
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway         Distance      Last Update
  10.1.12.2             90           11:00:14
Distance: internal 90 external 170
```

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4

Rôzne podsiete

Ak chcete vytvoriť susedské spojenie EIGRP, musia byť rozhrania smerovačov v rovnakej podsieti. Najjednoduchším spôsobom overenia podsietí je pozrieť sa na konfiguráciu rozhrania v bežiacom nastavení pomocou príkazu **show run interface interface_type interface_number**. Môžete tiež použiť príkaz **show ip interface_type interface_number** alebo príkaz **show interface_type interface_number**. Príklad 4-9 ukazuje konfiguráciu Gig1/0 na R1 a Gig0/0 na R2. Obe adresy IP sú v rovnakej podsieti.

Example 4-9 Verifying IPv4 Addresses and Masks on Router Interfaces

```
R1# show running-config interface gigabitEthernet 1/0
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 negotiation auto
end

R2# show running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/0
 ip address 10.1.12.2 255.255.255.0
 negotiation auto
end
```

Ak nie sú v rovnakej podsieti a syslog je nastavený na úroveň závažnosti 6, vygeneruje sa syslog správa.

```
%DUAL-6-NBRINFO: EIGRP-IPv4 100: Sused 10.1.21.2 (GigabitEthernet1/0)
je blokováný: nie je v spoločnej podsieti (10.1.12.1/24)
```

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4

Overovanie

Overovanie sa používa na zabezpečenie toho, aby smerovače EIGRP vytvárali susedské vzťahy len s legitímnymi smerovačmi a aby prijímali pakety EIGRP len od legitímnych smerovačov.

Príklad 4-10 ukazuje výstup príkazov **show run interface interface_type interface_number** a **show ip eigrp interfaces detail interface_type interface_number**, ktoré určujú, či je na rozhraní povolené overovanie EIGRP. Všimnite si, že overovanie musí byť nakonfigurované na správnom rozhraní a že musí byť viazané na správne číslo autonómneho systému.

Uistite sa, že ste zadali správny zväzok kľúčov, ktorý sa použije na overenie hash protokolu MD5 (Message Digest 5). Kľúčenku môžete overiť príkazom **show key chain**, ako je uvedené v príklade 4-11.

Example 4-10 Verifying EIGRP Authentication on an Interface

```
R1# show run interface gig 1/0
Building configuration...

Current configuration : 178 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRP_AUTH
 negotiation auto
end

R1# show ip eigrp interfaces detail gigabitEthernet 1/0
EIGRP-IPv4 Interfaces for AS(100)

```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Gil/0	1	0/0	0/0	87	0/0	376	0

```

Hello-interval is 5, Hold-time is 15
Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 2/0
Hello's sent/expedited: 17/2
Un/reliable mcasts: 0/3 Un/reliable ucasts: 2/2
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 1 Out-of-sequence rcvd: 1
Topology-ids on interface - 0
Authentication mode is md5, key-chain is "EIGRP_AUTH"
```

Example 4-11 Verifying the Keychain Used for EIGRP Authentication

```
R1# show key chain
Key-chain EIGRP_AUTH:
  key 1 -- text "ENARSI"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
```

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4 ACL

Zoznamy riadenia prístupu (ACL) sú mimoriadne výkonné. To, ako sú implementované, určuje, čo v sieti kontrolujú. Ak je na rozhranie aplikovaný zoznam ACL a tento zoznam ACL odmieta pakety EIGRP alebo ak sa paket EIGRP stane obeťou implicitného deny all na konci zoznamu ACL, vzťah so susedom sa nevytvorí.

Ak chcete zistiť, či je na rozhranie použitý ACL, použijete príkaz **show ip interface interface_type interface_number**, ako je znázornené v príklade 4-14. Všimnite si, že ACL 100 je aplikovaný na prichádzajúce rozhranie Gig1/0. Ak chcete overiť položky ACL 100, zadajte príkaz **show access-lists 100**, ako je uvedené v príklade 4-15. V tomto prípade môžete vidieť, že ACL 100 odmieta prevádzku EIGRP; to zabraňuje vytvoreniu susedského vzťahu.

Example 4-14 *Verifying ACLs Applied to Interfaces*

```
R1# show ip interface gig 1/0
GigabitEthernet1/0 is up, line protocol is up
  Internet address is 10.1.12.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound access list is 100
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
```

Example 4-15 *Verifying ACL Entries*

```
R1# show access-lists 100
Extended IP access list 100
  10 deny eigrp any any (62 matches)
  20 permit ip any any
```

Riešenie problémov s príslušnými susedmi protokolu EIGRP pre IPv4

Časovače

Hoci sa časovače EIGRP nemusia zhodovať, ak sú časovače dostatočne skreslené, adjacency bude klapať.

Je dôležité, aby smerovače posielali pakety hello rýchlosťou, ktorá je rýchlejšia ako časovač podržania. Nakonfigurované časovače overíte príkazom **show ip eigrp interfaces detail**, ako je uvedené v príklade 4-10.

Example 4-10 Verifying EIGRP Authentication on an Interface

```
R1# show run interface gig 1/0
Building configuration...

Current configuration : 178 bytes
!
interface GigabitEthernet1/0
 ip address 10.1.12.1 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 EIGRP_AUTH
 negotiation auto
end

R1# show ip eigrp interfaces detail gigabitEthernet 1/0
EIGRP-IPv4 Interfaces for AS(100)

      Xmit Queue  PeerQ      Mean Pacing Time  Multicast  Pending
Interface Peers Un/Reliable Un/Reliable SRTT  Un/Reliable  Flow Timer  Routes
Gig1/0      1      0/0        0/0         87    0/0         376         0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Packetized sent/expedited: 2/0
  Hello's sent/expedited: 17/2
  Un/reliable mcasts: 0/3 Un/reliable ucasts: 2/2
  Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
  Retransmissions sent: 1 Out-of-sequence rcvd: 1
  Topology-ids on interface - 0
  Authentication mode is md5, key-chain is "EIGRP_AUTH"
```

Riešenie problémov s EIGRP pre smery IPv4

- Po nadviazaní susedského vzťahu vykoná smerovač EIGRP úplnú výmenu smerovacích informácií s novovytvoreným susedom. Po úplnej výmene sa s týmto susedom vymieňajú len aktualizácie smerovacích informácií.
- Existujú rôzne dôvody, prečo trasy EIGRP môžu chýbať v topologickej alebo smerovacej tabuľke, a ak plánujete úspešne riešiť problémy súvisiace s trasami EIGRP, musíte o nich vedieť.
- Táto časť sa zaoberá dôvodmi, prečo trasy EIGRP môžu chýbať, a spôsobmi, ako zistiť, prečo chýbajú.

Riešenie problémov s EIGRP pre smery IPv4

Chýbajúce trasy EIGRP

Nižšie sú uvedené niektoré bežné dôvody, prečo môžu trasy EIGRP chýbať v topologickej alebo smerovacej tabuľke:

- **Zlý alebo chýbajúci príkaz siete** - Príkaz **siete** zapína proces EIGRP na rozhraní a vkladá prefix siete, ktorej je rozhranie súčasťou, do procesu EIGRP.
- **Lepší zdroj informácií** - Ak sa presne rovnaký sieťový prefix naučíte zo spoľahlivejšieho zdroja, použije sa namiesto informácií naučených v rámci EIGRP.
- **Filtrovanie smerov** - filter môže brániť inzerovaniu alebo naučeniu sieťovej prefixu.
- **Konfigurácia stub** - Ak sa počas konfigurácie stub smerovača vyberie nesprávne nastavenie alebo ak sa ako stub smerovač vyberie nesprávny smerovač, môže to zabrániť inzerovaniu sieťového prefixu.
- **Rozhranie je vypnuté** - Rozhranie s povoleným EIGRP musí byť zapnuté, aby sa sieť spojená s rozhraním mohla inzerovať.
- **Split horizont** - Split horizont je funkcia prevencie slučky, ktorá zabraňuje smerovaču inzerovať trasy na tom istom rozhraní, na ktorom boli naučené.

Riešenie problémov s EIGRP pre smery IPv4

Zlý alebo chýbajúci sieťový príkaz

- Keď použijete príkaz **network**, proces EIGRP sa povolí na rozhraniach, ktoré patria do rozsahu IP adries identifikovaných príkazom. EIGRP potom vezme sieť/podsieť, ktorej je rozhranie súčasťou, a vloží ju do topologickej tabuľky, aby mohla byť inzerovaná ostatným smerovačom v autonómnom systéme.
- Ak príkaz **siete** chýba alebo je nesprávne nakonfigurovaný, EIGRP nie je na rozhraní povolený a sieť, do ktorej rozhranie patrí, nie je nikdy inzerovaná, a preto je pre ostatné smerovače nedostupná.
- **Pomocou príkazu show ip eigrp interfaces** môžete potvrdiť, ktoré rozhrania sa zúčastňujú procesu EIGRP, ako je uvedené v príklade 4-4.

Example 4-4 *Verifying EIGRP Interfaces with show ip eigrp interfaces*

```
R2# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Gi0/0	0	0/0	0	0/0	0	0
Gi1/0	1	0/0	78	0/0	300	0

Riešenie problémov s EIGRP pre smery IPv4

Lepší zdroj informácií

- Aby sa trasa naučená v protokole EIGRP nainštalovala do smerovacej tabuľky, musí byť naj dôveryhodnejším zdrojom smerovania. Dôveryhodnosť je založená na administratívnej vzdialenosti (AD). AD EIGRP je 90 pre interne naučené trasy (siete vnútri autonómneho systému) a 170 pre externe naučené trasy (siete mimo autonómneho systému).
- Ak iný zdroj s lepším AD inzeruje presne tú istú sieť, tento zdroj vyhráva a jeho informácie sa nainštalujú do smerovacej tabuľky.
- Príklad 4-20, ktorý zobrazuje výstup príkazu **show ip route 172.16.33.16 255.255.255.252**, identifikuje, že táto sieť je priamo pripojená a má AD 0. Keďže priamo pripojená sieť má AD 0 a interná trasa EIGRP má AD 90, priamo pripojený zdroj je nainštalovaný v smerovacej tabuľke

Example 4-20 *Sample show ip route 172.16.33.16 255.255.255.252 Command Output*

```
Router# show ip route 172.16.33.16 255.255.255.252
Routing entry for 172.16.33.16/30
  Known via "connected", distance 0, metric 0 (connected, via interface)
  ...output omitted...
```

Riešenie problémov s EIGRP pre smery IPv4 Lepší zdroj informácií (pokračovanie)

- Používanie neoptimálneho zdroja smerovacích informácií môže spôsobiť neoptimálne smerovanie v sieti.
- Na obrázku 4-1 je znázornená sieť s dvoma rôznymi smerovacími protokolmi. Aj keď je rýchlejšie použiť cestu OSPF (Open Shortest Path First), EIGRP štandardne vyhráva, pretože má nižšiu hodnotu AD, a dochádza k neoptimálnemu smerovaniu. V tomto prípade by ste mohli zvážiť zvýšenie AD protokolu EIGRP alebo zníženie AD protokolu OSPF s

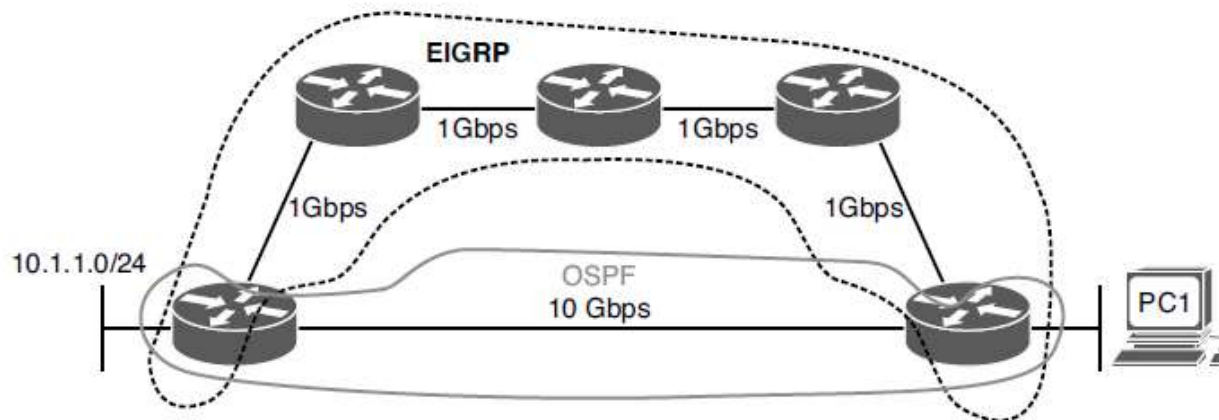


Figure 4-1 Using the Suboptimal EIGRP Path

Riešenie problémov s EIGRP pre smery IPv4

Filtrovanie smeroviek

- Distribučný zoznam aplikovaný na proces EIGRP riadi, ktoré trasy sa inzerujú susedom a ktoré trasy sa prijímajú od susedov. Distribučný zoznam sa aplikuje v konfiguračnom režime EIGRP buď na prichádzajúce alebo odchádzajúce trasy a odoslané alebo prijaté trasy sa riadia pomocou ACL, zoznamov prefixov alebo smerovacích máp.
- Pri riešení problémov s filtrovaním trás zvážte nasledujúce skutočnosti:
 - Je distribučný zoznam použitý v správnom smere?
 - Je distribučný zoznam použitý na správne rozhranie?
 - Ak distribučný zoznam používa ACL, je ACL správne?
 - Ak distribučný zoznam používa zoznam prefixov, je zoznam prefixov správny?
 - Ak zoznam distribúcie používa mapu trasy, je mapa trasy správna?

Riešenie problémov s EIGRP pre smery IPv4

Filtrovanie smeroviek (pokračovanie)

Príkaz **show ip protocols** identifikuje, či je distribučný zoznam aplikovaný na všetky rozhrania alebo na jednotlivé rozhranie, ako je uvedené v príklade 4-21. Tento príklad ukazuje, že neexistujú žiadne odchádzajúce filtre a že na Gig1/0 je použitý prichádzajúci filter.

- Príchodový filter v príklade 4-21 na Gig1/0 filtruje pomocou ACL 10. Ak chcete overiť položky v ACL, musíte vydať príkaz **show access-lists 10**. Ak bol použitý zoznam prefixov, vydáte príkaz **show ip prefix-list**. Ak bola použitá mapa trasy, vydáte príkaz **show route-map**.
- Ako je uvedené v príklade 4-22, príkaz, ktorý bol použitý na použitie distribučného zoznamu, overíte v bežiacom nastavení tak, že si prezriete časť konfigurácie EIGRP.

Example 4-21 Verifying Route Filters with show ip protocols

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  GigabitEthernet1/0 filtered by 10 (per-user), default is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 10.1.12.1
  ...output omitted...
```

Example 4-22 Verifying EIGRP distribute-list Command

```
R1# show run | section router eigrp
router eigrp 100
  distribute-list 10 in GigabitEthernet1/0
  network 10.1.1.1 0.0.0.0
  network 10.1.12.1 0.0.0.0
  passive-interface GigabitEthernet0/0
```

Riešenie problémov s EIGRP pre smery IPv4

Konfigurácia Stub

- Funkcia EIGRP stub umožňuje kontrolovať rozsah dotazov EIGRP v sieti.
- Obrázok 4-2 ukazuje normálny rozsah dopytu pre EIGRP, smerovač R3 prijme dopyt, hoci nikdy nebude mať alternatívne informácie o sieti 192.168.1.0/24.
- Ako je znázornené na obrázku 4-3, konfigurácia funkcie EIGRP stub na R3 pomocou príkazu **eigrp stub** zabezpečí, že R2 nikdy nepošle dotaz na R3.

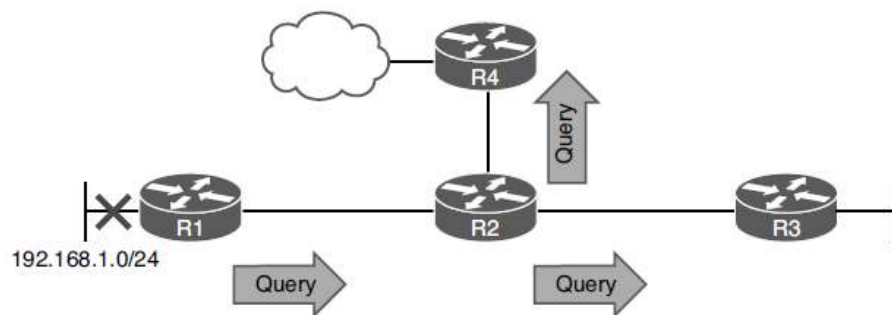


Figure 4-2 Query Scope Without the EIGRP Stub Feature

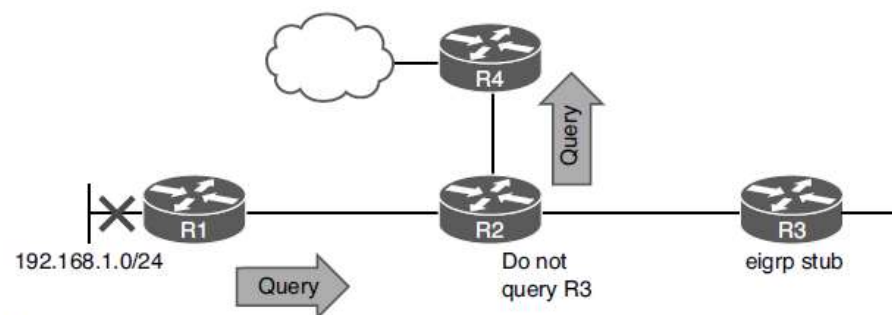


Figure 4-3 Query Scope with the EIGRP Stub Feature

Riešenie problémov s EIGRP pre smery IPv4

Stub konfigurácia (pokračovanie)

- Funkcia EIGRP stub je užitočná pri pomalých prepojeniach WAN typu hub-and-spoke, ako je znázornené na obrázku 4-4.
- Konfigurácia stub sietí znižuje množstvo prevádzky EIGRP odosielanej cez linky WAN. Okrem toho znižuje pravdepodobnosť, že trasa uviazne v aktívnom stave (SIA) z dôvodu preťaženia siete WAN.
- Smerovač EIGRP stub štandardne inzeruje pripojené a súhrnné trasy. Máte možnosť inzerovať pripojené, súhrnné, redistribuované alebo statické trasy - alebo ich kombináciu. Druhou možnosťou je neposielať žiadne trasy (nazýva sa len príjem). Ak sa vyberie nesprávna možnosť, stub smerovače neinzerujú správne trasy svojim susedom, čo má za následok chýbajúce trasy v uzle a ostatných smerovačoch v topológii.

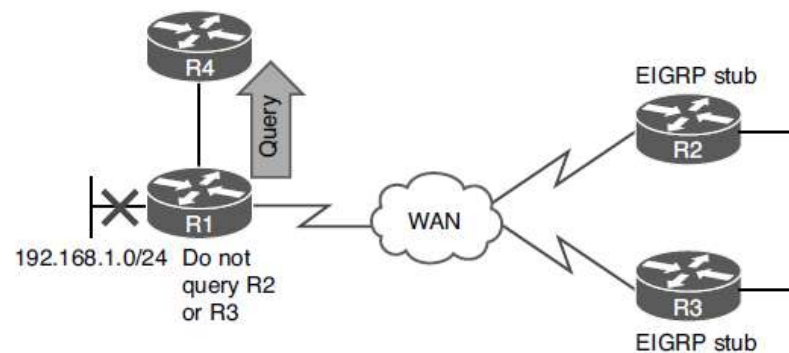


Figure 4-4 EIGRP Stub Feature over WAN Links

Riešenie problémov s EIGRP pre smery IPv4

Stub konfigurácia (pokračovanie)

- Ak chcete overiť, či je smerovač stub smerovačom, a určiť trasy, ktoré bude inzerovať, zadajte príkaz **show ip protocols**, ako je znázornené v príklade 4-23.
- Ak chcete zistiť, či je sused stub smerovačom a aké typy trás inzeruje, zadajte príkaz **show ip eigrp neighbors detail**. Príklad 4-24 ukazuje výstup príkazu **show ip eigrp neighbors detail** na R1, ktorý naznačuje, že sused je stub smerovač, ktorý inzeruje pripojené a súhrnné trasy a potláča dotazy.

Example 4-23 *show ip protocols Command Output on R2*

```
R2# show ip protocols
...output omitted...
EIGRP-IPv4 Protocol for AS(100)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 192.1.1.1
  Stub, connected, summary
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
...output omitted...
```

Example 4-24 *Verifying Whether an EIGRP Neighbor Is a Stub Router*

```
R1# show ip eigrp neighbors detail
EIGRP-IPv4 Neighbors for AS(100)
H   Address                Interface           Hold Uptime    SRTT   RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
0   10.1.13.1                Se1/0              14 00:00:18   99    594  0   11
Version 11.0/2.0, Retrans: 0, Retries: 0, Prefixes: 2
Topology-ids from peer - 0
Stub Peer Advertising (CONNECTED SUMMARY ) Routes
Suppressing queries
...output omitted...
```

Riešenie problémov s EIGRP pre smery IPv4

Rozhranie je vypnuté

- Príkaz **network** zapína proces smerovania na rozhraní.
- Keď je proces EIGRP na rozhraní povolený, sieť, ktorej súčasťou je IP adresa rozhrania, je vložená do procesu EIGRP.
- Ak je rozhranie vypnuté, v smerovacej tabuľke nie je žiadna priamo pripojená položka pre sieť.
- Rozhranie musí byť zapnuté, aby sa mohli inzerovať trasy alebo vytvárať susedské vzťahy.

Riešenie problémov s EIGRP pre smery IPv4

Rozdelený horizont

- Pravidlo rozdeleného horizontu EIGRP stanovuje, že žiadne trasy naučené na rozhraní nebudú inzerované von z toho istého rozhrania. Toto pravidlo je určené na zabránenie smerovacích slučiek. Toto pravidlo však predstavuje problém v určitých topológiách, napríklad v sieti DMVPN (Dynamic Multipoint Virtual Private Network) alebo v topológiách bez rozhlasového vysielania, s viacerými prístupmi Frame Relay hub-and-spoke. Na obrázku 4-5 je znázornená sieť využívajúca viacbodové rozhrania, v ktorej sa vyskytuje problém s rozdeleným horizontom.
- Viacbodové rozhranie poskytuje pripojenie k viacerým smerovačom v tej istej podsieti cez jedno rozhranie, podobne ako Ethernet.
- Ak chcete overiť, či je na rozhraní povolený split horizon, zadajte príkaz **show ip interface_type interface_number**, ako je znázornené v príklade 4-25.

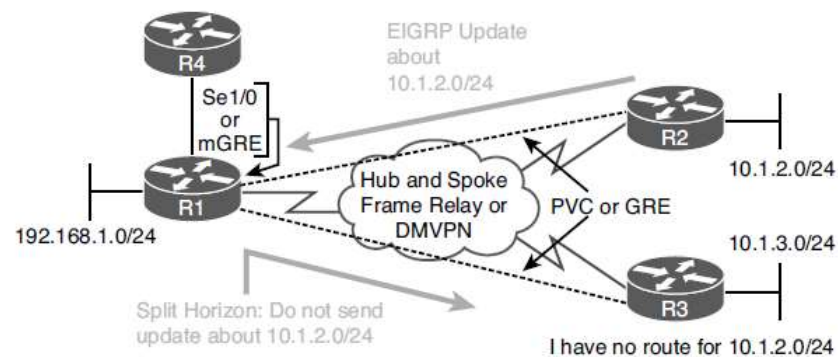


Figure 4-5 EIGRP Split Horizon Issue

Example 4-25 Verifying Whether Split Horizon Is Enabled on an Interface

```
R1# show ip interface tunnel 0
Tunnel0 is up, line protocol is up
 Internet address is 192.168.1.1/24
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1476 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are never sent
 ...output omitted...
```

Riešenie problémov s EIGRP pre smery IPv4 Split Horizon (pokračovanie)

- Ak chcete úplne zakázať rozdelený horizont na rozhraní, zadajte príkaz **no ip split-horizon** v režime konfigurácie rozhrania. Ak ho chcete zakázať len pre proces EIGRP spustený na rozhraní, zadajte príkaz **no ip split-horizon eigrp autonomous_system_number**.
- Ak zakážete split horizon pre proces EIGRP, vo výstupe príkazu **show ip interface** sa stále zobrazuje ako povolený (pozri príklad 4-25). Ak chcete overiť, či je split horizon pre proces EIGRP na rozhraní povolený alebo zakázaný, zadajte príkaz **show ip eigrp interfaces detail interface_type interface_number**. Príklad 4-26 ukazuje, že je zakázaný pre EIGRP na rozhraní tunel 0.

Example 4-26 Verifying Whether Split Horizon Is Enabled for EIGRP on an Interface

```
R1# show ip eigrp interfaces detail tunnel 0
EIGRP-IPv4 Interfaces for AS(100)

```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Tu0	0	0/0	0	6/6	0	0

```

Hello-interval is 5, Hold-time is 15
Split-horizon is disabled
Next xmit serial <none>
Packetized sent/expedited: 0/0
Hello's sent/expedited: 17/1
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Topology-ids on interface - 0
Authentication mode is not set
```

Riešenie rôznych problémov s EIGRP pre IPv4

- Táto časť sa zameriava na riešenie problémov súvisiacich s uskutočniteľnými následníkmi, nesúvislými sieťami a automatickou sumarizáciou, sumarizáciou trasy a vyrovnávaním záťaže s rovnakou a nerovnakou metrikou.

Riešenie rôznych problémov s EIGRP pre IPv4

Uskutočnitelní nástupcovia

- Najlepšia trasa (na základe metriky najnižšej uskutočniteľnej vzdialenosti [FD]) pre konkrétnu sieť v topologickej tabuľke EIGRP sa stáva kandidátom na zaradenie do smerovacej tabuľky smerovača.
- Termín kandidát sa používa preto, lebo aj keď ide o najlepšiu trasu EIGRP, môže sa použiť lepší zdroj rovnakých informácií.
- Ak je táto trasa skutočne vložená do smerovacej tabuľky, stane sa známou ako *následná* (najlepšia) trasa.
- Následná trasa sa potom inzeruje susedným smerovačom.

Riešenie rôznych problémov s EIGRP pre IPv4

Uskutočiteľní nástupcovia (pokračovanie)

- V príklade 4-27 je zobrazená vzorová tabuľka topológie EIGRP, ktorú môžete zobrazit' príkazom **show ip eigrp topology**.
- V zátvorkách za IP adresou nasledujúceho reťazca je FD, za ktorou nasleduje nahlásená vzdialenosť (RD):
 - **Dosiahnuteľná vzdialenosť** - RD plus metrika na dosiahnutie suseda na adrese ďalšieho kroku, ktorý inzeruje RD.
 - **Nahlásená vzdialenosť** - vzdialenosť od suseda na adrese ďalšieho kroku do cieľovej siete.
- Nástupca je cesta s najnižším FD, avšak EIGRP tiež vopred vypočíta cesty, ktoré by sa mohli použiť, ak by nástupca zmizol. Tieto trasy sú známe ako *uskutočiteľní následníci*.
- Aby sa cesta stala uskutočiteľným následníkom, musí byť RD cesty, ktorá sa má stať uskutočiteľným následníkom, menšia ako FD následníka.

Example 4-27 Sample show ip eigrp topology Command Output

```
R4# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

...output omitted...
P 10.1.13.0/24, 1 successors, FD is 3072
   via 10.1.34.3 (3072/2816), GigabitEthernet2/0
P 0.0.0.0/0, 1 successors, FD is 28160
   via Rstatic (28160/0)
P 192.1.1.1/32, 1 successors, FD is 131072
   via 10.1.34.3 (131072/130816), GigabitEthernet2/0
P 172.16.32.192/29, 1 successors, FD is 2174976
   via 172.16.33.5 (2174976/30720), Serial1/0
   via 172.16.33.6 (2684416/2172416), Serial1/0
   via 172.16.33.18 (2684416/2172416), Serial1/2
P 198.51.100.0/30, 1 successors, FD is 28416
   via 10.1.34.3 (28416/28160), GigabitEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 2172416
   via 172.16.33.5 (2172416/28160), Serial1/0
...output omitted...
```

Riešenie rôznych problémov s EIGRP pre IPv4

Uskutočnitelní nástupcovia (pokračova

- Pri riešení problémov je dôležité poznamenať, že výstup príkazu **show ip eigrp topology** zobrazuje iba následníkov a realizovateľných následníkov. Ak potrebujete overiť FD alebo RD iných ciest k tomu istému cieľu, ktoré nie sú uskutočniteľnými následníkmi, môžete použiť príkaz **show ip eigrp topology all-links**.
- Príklad 4-28 zobrazuje výstup príkazov **show ip eigrp topology** a **show ip eigrp topology all-links**.
- Vo výstupe príkazu **show ip eigrp topology** si všimnite, že je uvedená len jedna cesta. Vo výstupe príkazu **show ip eigrp topology all-links** si všimnite, že sú uvedené dve cesty. Je to preto, že ďalší skok 172.16.33.13 má RD väčší ako FD následníka, a preto nemôže byť uskutočniteľným následníkom.

Example 4-28 Sample show ip eigrp topology Comparison

```
Router# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.16.33.14)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.33.8/30, 1 successors, FD is 2169856
   via Connected, Serial1/0
P 10.1.34.0/24, 1 successors, FD is 2682112
   via 172.16.33.9 (2682112/2170112), Serial1/0
P 203.0.113.0/30, 1 successors, FD is 2684416
   via 172.16.33.9 (2684416/2172416), Serial1/0
P 172.16.32.192/29, 1 successors, FD is 28160
   via Connected, FastEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 5511936
   via Connected, Serial1/1
P 172.16.33.0/29, 1 successors, FD is 2681856
   via 172.16.33.9 (2681856/2169856), Serial1/0

Router# show ip eigrp topology all-links
EIGRP-IPv4 Topology Table for AS(100)/ID(172.16.33.14)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.33.8/30, 1 successors, FD is 2169856, serno 1
   via Connected, Serial1/0
P 10.1.34.0/24, 1 successors, FD is 2682112, serno 8
   via 172.16.33.9 (2682112/2170112), Serial1/0
   via 172.16.33.13 (6024192/3072256), Serial1/1
P 203.0.113.0/30, 1 successors, FD is 2684416, serno 9
   via 172.16.33.9 (2684416/2172416), Serial1/0
   via 172.16.33.13 (6026496/3074560), Serial1/1
P 172.16.32.192/29, 1 successors, FD is 28160, serno 3
   via Connected, FastEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 5511936, serno 2
   via Connected, Serial1/1
P 172.16.33.0/29, 1 successors, FD is 2681856, serno 5
   via 172.16.33.9 (2681856/2169856), Serial1/0
   via 172.16.33.13 (6023936/3072000), Serial1/1
```


Riešenie rôznych problémov s EIGRP pre IPv4

Uskutočnitelní nástupcovia (pokračovanie)

- Topologická tabuľka EIGRP obsahuje nielen trasy naučené z iných smerovačov, ale aj trasy, ktoré boli redistribuované do procesu EIGRP, a lokálne pripojené siete, ktorých rozhrania sa zúčastňujú procesu EIGRP, ako je zvýraznené v príklade 4-29.

Example 4-29 Verifying Connected and Redistributed Entries in the Topology Table

```
R4# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

...output omitted...
P 192.2.2.2/32, 1 successors, FD is 131072
   via 10.1.34.3 (131072/130816), GigabitEthernet2/0
P 10.1.13.0/24, 1 successors, FD is 3072
   via 10.1.34.3 (3072/2816), GigabitEthernet2/0
P 0.0.0.0/0, 1 successors, FD is 28160
   via Rstatic (28160/0)
P 192.1.1.1/32, 1 successors, FD is 131072
   via 10.1.34.3 (131072/130816), GigabitEthernet2/0
P 172.16.32.192/29, 1 successors, FD is 2174976
   via 172.16.33.5 (2174976/30720), Serial1/0
   via 172.16.33.6 (2684416/2172416), Serial1/0
   via 172.16.33.18 (2684416/2172416), Serial1/2
P 198.51.100.0/30, 1 successors, FD is 28416
   via 10.1.34.3 (28416/28160), GigabitEthernet2/0
P 172.16.33.12/30, 1 successors, FD is 2172416
   via 172.16.33.5 (2172416/28160), Serial1/0
P 192.6.6.6/32, 2 successors, FD is 2297856
   via 172.16.33.6 (2297856/128256), Serial1/0
   via 172.16.33.18 (2297856/128256), Serial1/2
P 172.16.33.0/29, 1 successors, FD is 2169856
   via Connected, Serial1/0
...output omitted...
```

Nesúvislé siete a automatická sumarizácia

- EIGRP podporuje maskovanie podsiete s premenlivou dĺžkou (VLSM). Vo verziách systému Cisco IOS pred verziou 15.0 EIGRP automaticky vykonával sumarizáciu trasy na hraniciach siete s celou triedou.
- V systéme Cisco IOS verzie 15.0 a novších je automatická sumarizácia predvolene vypnutá. **Príkaz no auto-summary** už nie je potrebné konfigurovať.
- Hoci je tento príkaz v predvolenom nastavení vypnutý, je možné ho manuálne zapnúť a môže spôsobiť problémy so smerovaním, ak sieť obsahuje nesúvislé siete. Na obrázku 4-6 je uvedený príklad nesúvislých podsietí siete triedy B 172.16.0.0/16.

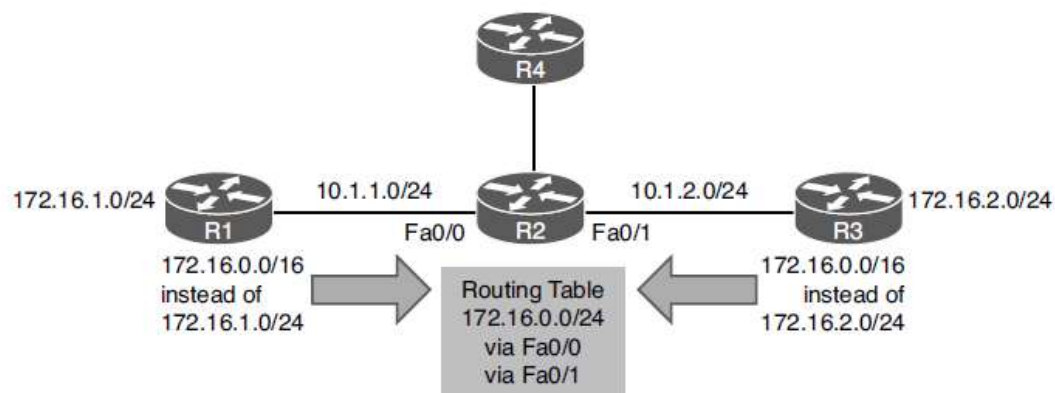


Figure 4-6 Discontiguous Network Example

Riešenie rôznych problémov s EIGRP pre IPv4

Nesúvislé siete a automatická sumarizácia

- Ak máte nesúvislú sieť, automatické sumarizovanie musí byť vypnuté a pri manuálnom sumarizovaní musíte byť opatrní.
- Ak chcete overiť, či je automatická sumarizácia povolená alebo zakázaná, použite príkaz **show ip protocols**, ako je uvedené v príklade 4-30.

Example 4-30 *Verifying Route Summarization with show ip protocols*

```
Router# show ip protocols
...output omitted...
EIGRP-IPv4 Protocol for AS(100)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 10.1.13.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1

Automatic Summarization: disabled
Address Summarization:
  10.1.0.0/20 for Gi2/0
    Summarizing 2 components with metric 2816
  Maximum path: 4
  Routing for Networks:
...output omitted...
```

Riešenie rôznych problémov s EIGRP pre IPv4

Sumarizácia trasy

- V predvolenom nastavení systému IOS 15.0 a novších verzií je funkcia autosummary vypnutá. Preto ju môžete buď zapnúť (čo sa neodporúča), alebo vykonať manuálnu sumarizáciu trasy (čo sa odporúča).
- V systéme EIGRP je manuálna sumarizácia trasy povolená na základe jednotlivých rozhraní.
- Je dôležité, aby ste vytvorili presné súhrnné trasy, aby ste zabezpečili, že váš smerovač nebude v súhrnnej trase propagovať siete, ktoré skutočne nevie dosiahnuť.
- Pri riešení problémov so sumarizáciou trasy EIGRP majte na pamäti nasledujúce informácie:
 - Povolili ste sumarizáciu trasy na správnom rozhraní?
 - Priradili ste súhrnnú trasu k správnej autonómnej systéme EIGRP?
 - Vytvorili ste príslušnú súhrnnú trasu?
- Odpovede na tieto otázky zistíte pomocou príkazu `show ip protocols`, ako je uvedené v príklade 4-30.

Riešenie rôznych problémov s EIGRP pre IPv4

Sumarizácia trasy (pokračovanie)

- Keď sa na smerovači vytvorí súhrnná trasa, vytvorí sa aj súhrnná trasa do nuly 0, ako je znázornené v nasledujúcom úryvku:

```
Router# show ip route | include Null  
D 10.1.0.0/20 je súhrn, 00:12:03, Null0
```

- Táto trasa do nuly 0 je vytvorená na zabránenie smerovacích slučiek. Je nevyhnutné, aby táto trasa existovala v tabuľke. Zabezpečuje, že keď smerovač prijme paket s neznámou cieľovou sieťovou adresou, ktorá spadá do súhrnu, paket bude zahodený. Ak by trasa na null 0 neexistovala a na smerovači by bola predvolená trasa, smerovač by paket preposlal pomocou predvolenej trasy. Smerovač nasledujúceho cieľa by potom skončil s presmerovaním paketu späť na tento smerovač, pretože používa súhrnnú trasu, a proces by sa opakoval. Toto je smerovacia slučka.
- Trasa do nuly 0 má hodnotu AD 5, aby sa zabezpečilo, že je dôveryhodnejšia ako väčšina ostatných zdrojov smerovacích informácií. Jediný spôsob, ako by táto trasa nebola v smerovacej tabuľke, je, ak by ste mali zdroj s nižším AD (napríklad ak by niekto vytvoril statickú trasu pre tú istú súhrnnú sieť a nasmeroval ju na IP adresu ďalšieho cieľa namiesto null 0).

Riešenie rôznych problémov s EIGRP pre IPv4

Vyrovnávanie záťaže

- V predvolenom nastavení EIGRP vyvažuje záťaž na štyroch rovnomerných cestách. Túto hodnotu môžete zmeniť pomocou príkazu **maximum-paths** v režime konfigurácie smerovača EIGRP.
- EIGRP podporuje aj vyrovnávanie záťaže na nerovnako metrických cestách pomocou funkcie *variácie*. V predvolenom nastavení je hodnota variácie pre smerovací proces EIGRP 1, čo znamená, že vyrovnávanie záťaže sa uskutoční len cez rovnomerné metrické cesty. Zvýšením násobiteľa sa zväčší rozsah metrík, nad ktorými bude prebiehať vyvažovanie záťaže.
- Aj pri nerovnomernom vyrovnávaní záťaže sa stále riadite príkazom **maximum-paths**. Preto ak máte päť nerovnomerných ciest, ktoré chcete použiť, a nakonfigurujete správny násobiteľ odchýlky, ale maximum-paths je nastavené na 2, použijete len dve z piatich ciest.
- Ak cesta nie je uskutočniteľným následníkom, nemožno ju použiť na nerovnomerné vyrovnávanie zaťaženia. Z tohto pravidla neexistuje žiadna výnimka.

Riešenie rôznych problémov s EIGRP pre IPv4

Vyrovnávanie záťaže (pokračovanie)

Ak chcete overiť nakonfigurované maximálne cesty a odchýlky, použite príkaz **show ip protocols**, ako je uvedené v príklade 4-31.

Example 4-31 Verifying Variance and Maximum Paths

```
Router# show ip protocols
Routing Protocol is "eigrp 100"

  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
EIGRP-IPv4 Protocol for AS(100)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  NSF-aware route hold timer is 240
  Router-ID: 10.1.12.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    0.0.0.0
  Routing Information Sources:
    Gateway         Distance    Last Update
    10.1.12.2         90         10:26:36
  Distance: internal 90 external 170
```