

FlexVPN HA Dual Hub نيوكت لاثم

تايوت حمل

[عمدقم](#)

[سيساس الابل طتم](#)

[ابل طتم](#)

[عمدختسم ال تانوكم](#)

[سيساس ا تامولعم](#)

[نيوكت](#)

[كبش ليل طي طخت ال مسر](#)

[يداع ال تاي لمع ال ويراني](#)

[\(راضخ\) ملك - ليل شحت](#)

[يداع ال ليغش ال ويراني سل هيوت ال تاجر مولاو](#)

[HUB1 لش ف ويراني](#)

[تانيوكت](#)

[R1-HUB نيوكت](#)

[R2-HUB2 نيوكت](#)

[R3-TALK1 نيوكت](#)

[R4-Talk2 نيوكت](#)

[R5-AGGR1 نيوكت](#)

[R6-AGGR2 نيوكت](#)

[\(كبش ليل كليت ف فيضم ال اكم\) R7 فيضم نيوكت](#)

[قماه نيوكت تاظالم](#)

[حص ال تم ققحت](#)

[اهال الصاوا طخ ال فاشكتسا](#)

[قلص تاذا تامولعم](#)

عمدقم

لصت تي ال اديع ال ب تاكم لل لماك راركت ميمصت نيوكت افيك دنتسم ال اذه حضوي لثم، نم آريغ اكبش طيسو ربع IPSec ال ا دنتسم ال VPN اكبش ربع تانايب زكرمب تانرتن ال.

سيساس الابل طتم

ابل طتم

دنتسم ال اذهل عصاخ اابل طتم دجوت ال

عمدختسم ال تانوكم

الالات الينقت ال تانوكم ال دنتسم ال اذه في ا دراو ال تامولعم ال دنتست

- مداوخلال نيپوتانايبال زكرم لخاد هيچوت لوكوتوربك (BGP) [في دودخل اربعل لوكوتورب](#) VPN. ككبش عيشغت يف زكارملالو.
- [تاطابتالال فاشتكاب موقت فيلاك \(BFD\)](#) [هاجتالال يئانث هيچوتال اداعا فاشتك](#) قافنال ربع سيلو) طقف تانايبال زكرم لخاد لمعت يتال (لفسالال هجومال) لفسال (ةلخادتمال).
- [تاناكلم نيكمت عم](#)، [في عرفال ماسقالاو عيزوتال تاحول نيپ Cisco IOS® FlexVPN](#) [جمانرب](#) يدمل ريصق ليوت ربع ثدحتال.
- [ةثداحمال ربع لاصتال نيكمتل نيروحم نيپ](#) [يقفنال \(GRE\)](#) [ماعال هيچوتال ني مضت](#)، [ةفلتخم زكارمب ةلصتم تاددحمال نوكت امدنع ىت](#).
- [ةبقعتمال تانئالكالب ةطبترممال ةتباتال تاراسمالو](#) [نسحمال نئالكالب قعت](#).

ةصاخ ةيلمعم ةئيپ يف ةدوجومال ةزهجال نم دنتسمال اذه يف دراوال تامولعملال عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمال اذه يف ةمدختسُمال ةزهجال عيمج تادب رماي ال لمحتمال ريثأتلل كمهف نم دكأتف، ةرشابم كتكبش.

ةيساسأ تامولعم

يلالعال رفاوتال نوكي ام ابلاغ، تانايبال زكرم لدعب نع لوصولال لولح ميمصتب موقت امدنع مامملل ةيويحل مدختسمال تاقيبطتل ةيساسال تابلطتمال دحأ (HA).

تاهوي رانيس نم دادر تسالال او عيرسال فاشتكالال ةيناكلم دنتسمال اذه يف دراوال لجال حيتي اداعا يف لكاشم ببسب VPN تاكبش اهان زكارم دحأ لطعت اهيف متي يتال لاطعال كلذ دعب (ةيعرفال) ةديعبال بتاكمال تاهجوم عيمج مدختست. ةقاولا و ةيقرتال و ا ليحتال لشفال اذه لثم فاشتكال دنع ةرشابم رخال ليغشتال زكرم.

ميمصتال اذه تازيم يلي اميف:

- VPN ككبش معد وي رانيس نم ةقئاف ةعرسب ككبشال دادر تسإ
- نامأ نارثقاو، (SAs) IPSec نامأ تانارثقا لثم) ةدقعم ةلاح نالعا ةنمازم تايلمع دجوتال (ريفشتال هيچوتو)، (ISAKMP) حيتافمال ةرادا لوكوتوربل نامال تاكبشو، تانرتنالال VPN تاكبش زكارم نيپ
- مقرر ةنمازم يف ريخأتلل ببسب ليغشتال اداعا مدعب ةقلعتم لكاشم دجوتال IPSec ةلاحال يذ HA عم (ESP) ني مضتال نامأ ةلومح لسلسلست
- و ةزهجا (VPN) ةيره اظال ةصاخال ككبشالال ةصاخال عيزوتال تاحول مدختست نأ نكمي Cisco IOS/IOS-XE الى دنتست ةفلتخم جمارب
- هليغشت متي يذل هيچوتال لوكوتوربك BGP عم ةنرمال لامحال ةنزاوم ذيفنت تاراخي (VPN) ةيره اظال ةصاخال ككبشال عيشغت يف
- لمعت ةيفخم تايلالىل عيوتحتال يتال ةزهجال عيمج يلع هتءارق نكمي و حضاو هيچوت

ةيفلخلاف

- فتاهال ربع رشابم لالاصتالال ةيناكم!
- ةدوجو (AAA) ةبساحمل او ضيوفتال او ةقداصلم لالماكت نيمضت ل [FlexVPN](#) تازيم عي مج (QoS) قفن لكال ةمدخلال

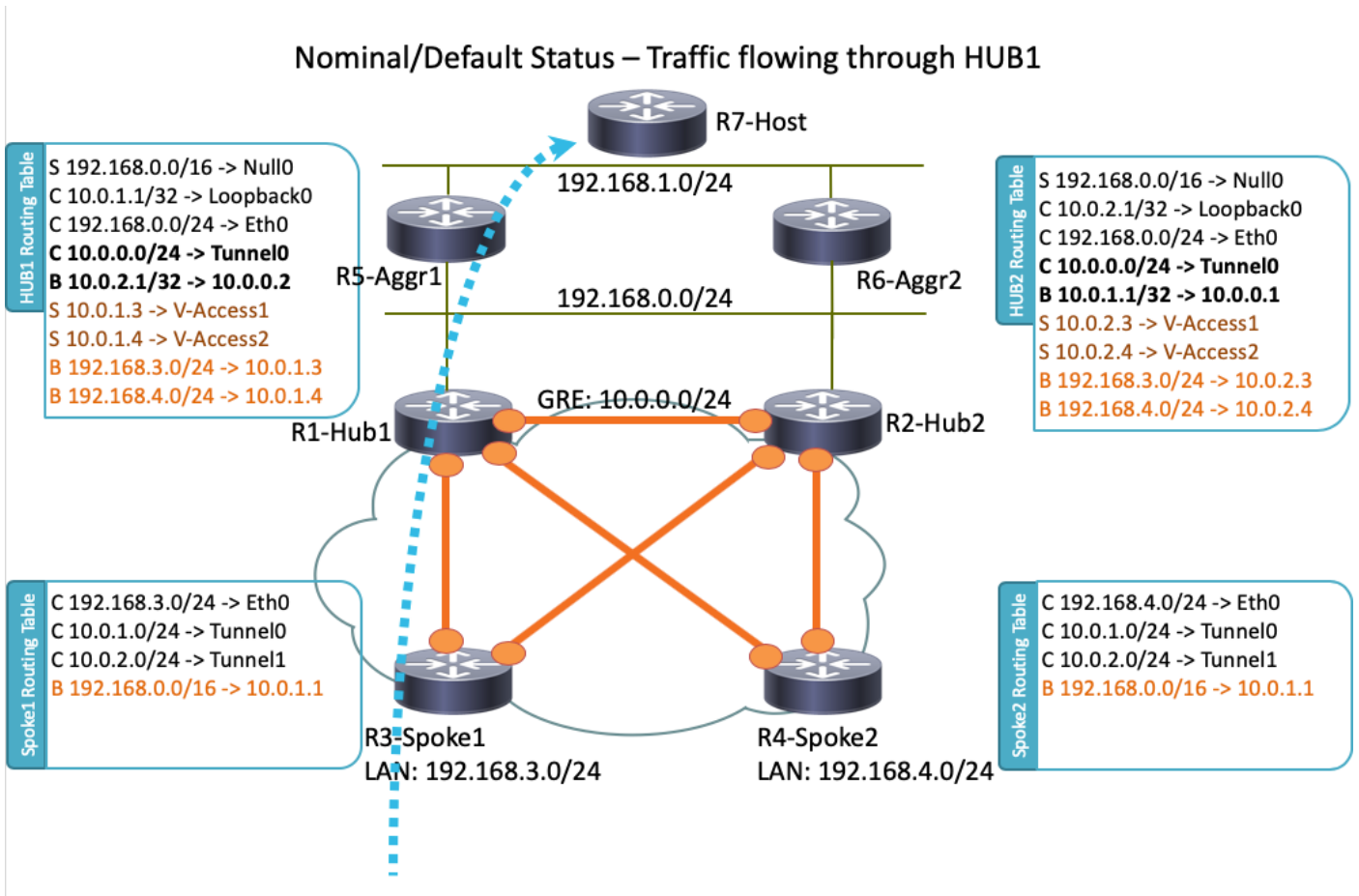
نيوكتالا

بتاكمل ل لماك راركت مي مصت ني وكت ةي فيك فص يو تا هوي رانيس ةلثمأ مسقلا اذه مدقي ةمئاقلا (VPN) ةيره اظلا ةصاخلا ةكبشلا لال خ نم تانايا بلا زكرمب لصتت يتلا ةديعبلا .نم آريغ ةكبش طسو ربع IPSec لو كوت ورب ىلع

نم ڊي زملع لوصحلل (طقف نيلچسملال عالعملل) رملوالا شحب ءاڊا مڊختسا :عظحال م
مسلال اڏه ي ف ءمڊختسملال رملوالا لوح تامولعملال

ةكبشلل يطي طختلا مسرلا

دنتسمل اذه يف مدختسمل اةكبشلا ططخم وه اذه



رإدصل إلل لئ غشش ب ططخ م اذ ه ل ف ا ه م ادخس إ م ت ل ل ا ت ا ه و م ل ع ل م ج م و ق ت : ط ط ح ا ل م
172.16.0.0/24 ن ا و ن ع م ا ط ن ت ن ر ت ن إ ل ا ع ب ا ح س م د خ ت س ت و ، Cisco IOS ن م 15.2(4)M1

ةيداعال تاي لمعال ويراني س

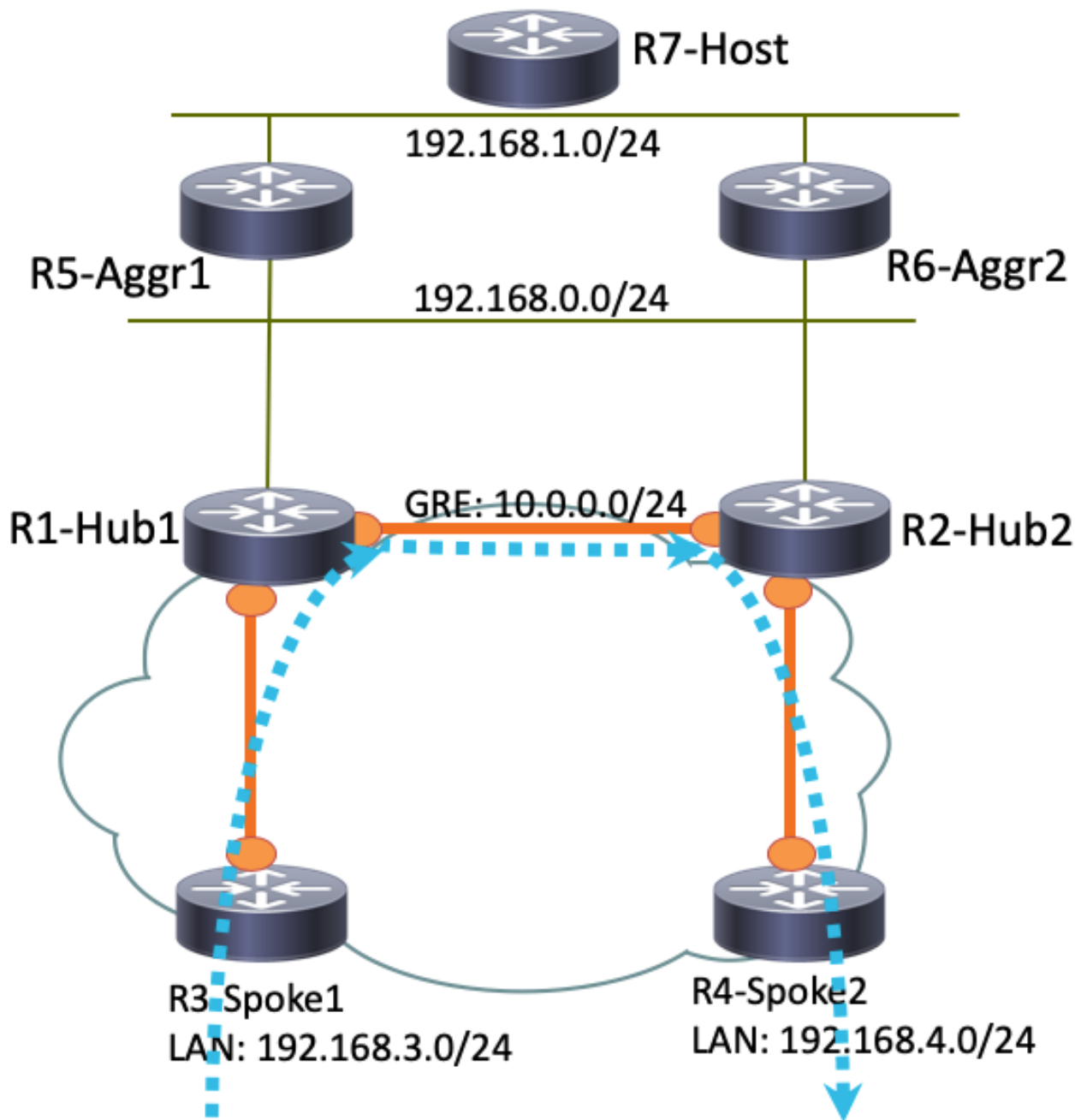
موقت ،لي غشتالاولي غشتالديق تاهجومال عي مج نوكت ام دنع ،يدياع لي غشت ويراني س يف ققحتي و. (R1-HUB1) يضارثفالا عزومال ربع رورمال ةكرح هي جوتب ةي كحمال تاهجومال عي مج BGP لوكوتوربل يضارثفالا يل حمال ليضفتال ني عت متي ام دنع اذه هي جوتال ليضفت رمال اذه طبض نكمي .(لي صافات يل عل لوصحلل عبتت يتال ماسقأال يل عجرا) 200 يل عل رورمال ةكرح لمح ةنزاوم لثم ،رشنال تابلطتم يل اذانتسا

(راصتخا) ملك -يل اذحت

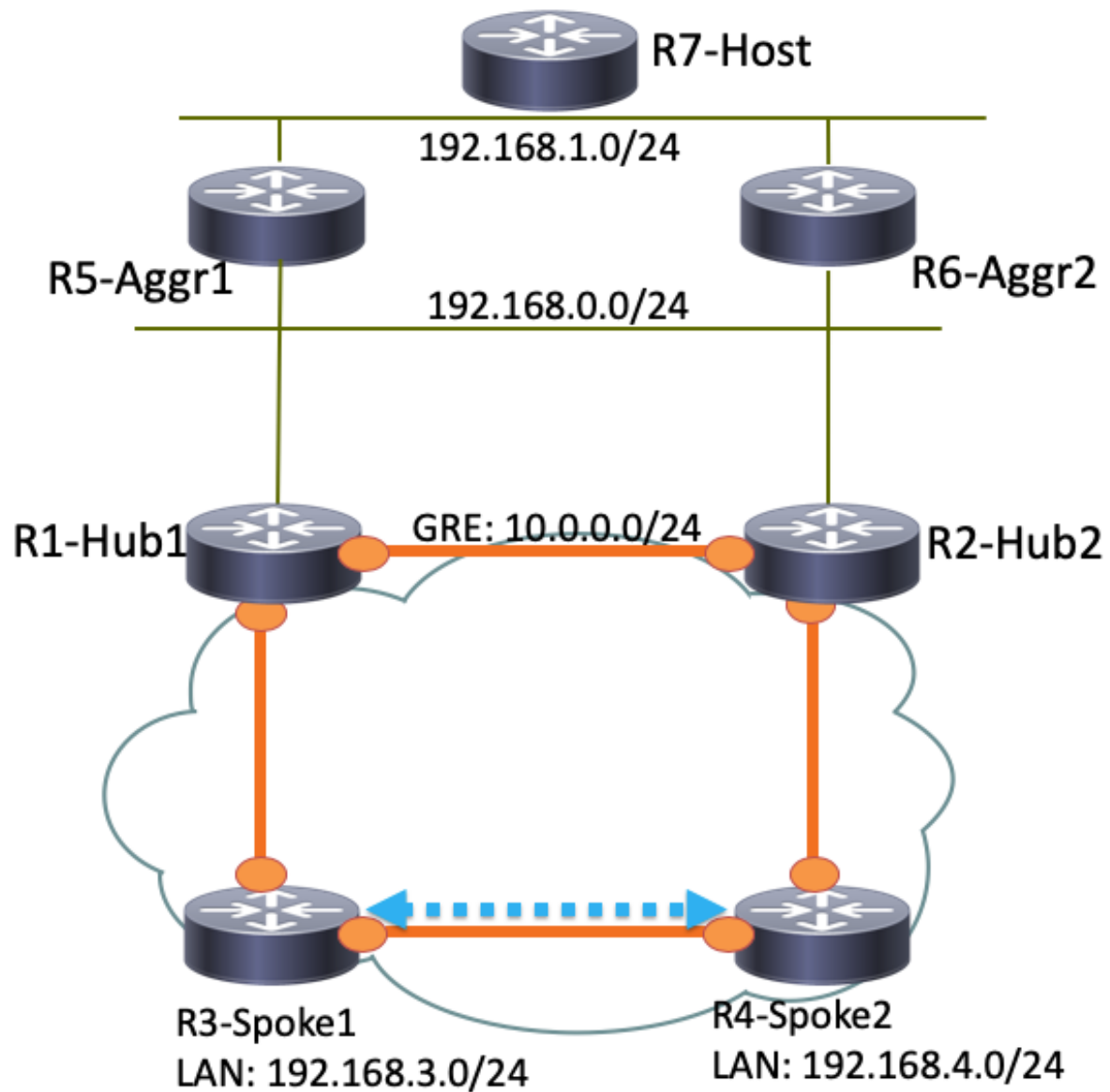
مادختساب Dynamic Talk-Speaker قفن عاشنإ متي ،R4-Talk2 ب لاصتا ادبب R3-Talk1 ماق اذإ يدمل ري صق لي وحتال ني وكت

 [ةطساوب هنع اذحتلا](#) متي [يذل](#) ني وكتال [ليلد](#) يل عجرا ،لي صافاتال نم ديزمل :حيملت [FlexVPN](#).

نكمي ،R2-HUB2 ب طقف ال صتم R4-TALK2 ناك و ،R1-HUB1 ب طقف ال صتم R3-Talk1 ناك اذإ يف .رواحمال ني ب دتم يذل ةطقن يل ةطقن نم GRE قفن عم ةرشابم اذحت لاصتا ققحت اذهل اهباشم R4-Talk2 و R3-Talk1 ني ب ةيلوال رورمال ةكرح راسم رهظي ،ةلاحال هذه



سفن ىلع يوتحت يتلاو، برهاظلا لوصولا ةهجاو ىلع ةمزحلا لبقتسي R1-Hub1 نأل ارظنو
 هناف GRE قفن يف لالحا وه امك يلاتلا (NHRP) ةوطخلا ليلحت لوكتورب ةكبش فرعم
 ىلإ ثدحتي يكيمايد قفناشن ىلإ يدؤي اذهو. R3-Talk1 ىلإ رورملا ةكرح قرأش لاسرا متي:



ي داعال لي غشتال ويراني سل هي جوتال تاجرم و لواج

مظنم لي غشت ويراني س في R1-HUB1 هي جوت لودج لي امي ف

<#root>

R1-HUB1# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 a - application route

+ - replicated route, % - next hop override

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
S    10.0.0.0/8 is directly connected, Null0
C    10.0.0.0/24 is directly connected, Tunnel0
L    10.0.0.1/32 is directly connected, Tunnel0
C    10.0.1.1/32 is directly connected, Loopback0
S    10.0.1.2/32 is directly connected, Virtual-Access1
S    10.0.1.3/32 is directly connected, Virtual-Access2
B    10.0.2.1/32 [200/0] via 10.0.0.2, 00:05:40
B    10.0.2.3/32 [200/0] via 10.0.0.2, 00:05:40
B    10.0.2.4/32 [200/0] via 10.0.0.2, 00:05:40
B    10.0.5.1/32 [200/0] via 192.168.0.5, 00:05:40
B    10.0.6.1/32 [200/0] via 192.168.0.6, 00:05:40
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.0.0/24 is directly connected, Ethernet0/0
L    172.16.0.1/32 is directly connected, Ethernet0/0
S    192.168.0.0/16 is directly connected, Null0
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.0.0/24 is directly connected, Ethernet0/2
L    192.168.0.1/32 is directly connected, Ethernet0/2
B    192.168.1.0/24 [200/0] via 192.168.0.5, 00:05:40
B    192.168.3.0/24 [200/0] via 10.0.1.4, 00:05:24
B    192.168.4.0/24 [200/0] via 10.0.1.5, 00:05:33
```

يذلل قف نللا ءاشنل دعب مظتنم يتايل لمع ويراني س ي ف R3-TALK1 هيجوت لودج يلي امي ف
R4-TALK2: عم هيلل ثدحتي

<#root>

R3-SPOKE1# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
B    10.0.0.0/8 [200/0] via 10.0.1.1, 00:06:27
H    10.0.0.1/32 is directly connected, 00:06:38, Tunnel1
S    %    10.0.1.1/32 is directly connected, Tunnel0
C    10.0.1.3/32 is directly connected, Tunnel0
H    10.0.1.4/32 is directly connected, 00:01:30, Virtual-Access1
S    10.0.2.1/32 is directly connected, Tunnel1
C    10.0.2.3/32 is directly connected, Tunnel1
H    10.0.2.4/32 [250/1] via 10.0.2.3, 00:01:30, Virtual-Access1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.0.0/24 is directly connected, Ethernet0/0
```

```

L      172.16.0.3/32 is directly connected, Ethernet0/0
B      192.168.0.0/16 [200/0] via 10.0.1.1, 00:06:27

      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.3.0/24 is directly connected, Ethernet0/1
L      192.168.3.3/32 is directly connected, Ethernet0/1
      192.168.4.0/32 is subnetted, 1 subnets
H      192.168.4.4 [250/1] via 10.0.1.3, 00:01:30, Virtual-Access1

```

ةيلحم تاليفتفب 192.168.0.0/16 ةكبشل نيلالخدإ ىلع BGP لودج يوتحي، R3-Talk1 في
 (R1-Hub1 لصف في) ةفلتخم:

<#root>

R3-SPOKE1#show ip bgp 192.168.0.0/16

```

BGP routing table entry for 192.168.0.0/16, version 8
Paths: (2 available, best #2, table default)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    10.0.2.1 from 10.0.2.1 (10.0.2.1)
      Origin incomplete, metric 0, localpref 100, valid, internal
      rx pathid: 0, tx pathid: 0
    Refresh Epoch 1
  Local

    10.0.1.1 from 10.0.1.1 (10.0.1.1)

      Origin incomplete, metric 0, localpref 200, valid, internal, best
      rx pathid: 0, tx pathid: 0x0

```

مظتنم يليغشت ويراني في R5-AGGR1 هيجوت لودج يلي امي:

<#root>

R5-LAN1#show ip route

```

      10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B      10.0.0.0/8 [200/0] via 192.168.0.1, 00:07:22
B      10.0.0.0/24 [200/0] via 192.168.0.1, 00:07:22
B      10.0.1.1/32 [200/0] via 192.168.0.1, 00:07:22
B      10.0.1.3/32 [200/0] via 192.168.0.1, 00:07:17
B      10.0.1.4/32 [200/0] via 192.168.0.1, 00:07:16
B      10.0.2.1/32 [200/0] via 192.168.0.2, 15:44:13
B      10.0.2.3/32 [200/0] via 192.168.0.2, 15:44:13
B      10.0.2.4/32 [200/0] via 192.168.0.2, 15:44:13
C      10.0.5.1/32 is directly connected, Loopback0

```



```

B      10.0.6.1/32 [200/0] via 192.168.0.6, 00:07:22
      172.16.0.0/24 is subnetted, 1 subnets
B      172.16.0.0 [200/0] via 192.168.0.1, 00:07:22
B      192.168.0.0/16 [200/0] via 192.168.0.1, 00:07:22
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.0.0/24 is directly connected, Ethernet0/0
L      192.168.0.5/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, Ethernet0/1
L      192.168.1.5/32 is directly connected, Ethernet0/1
B      192.168.3.0/24 [200/0] via 10.0.1.3, 00:07:06
B      192.168.4.0/24 [200/0] via 10.0.1.4, 00:07:15

```

مظتنم يلىغشت ويرانىس في R7-Host هيجوت لودج يلى امي ف

<#root>

R7-HOST#show ip route

```

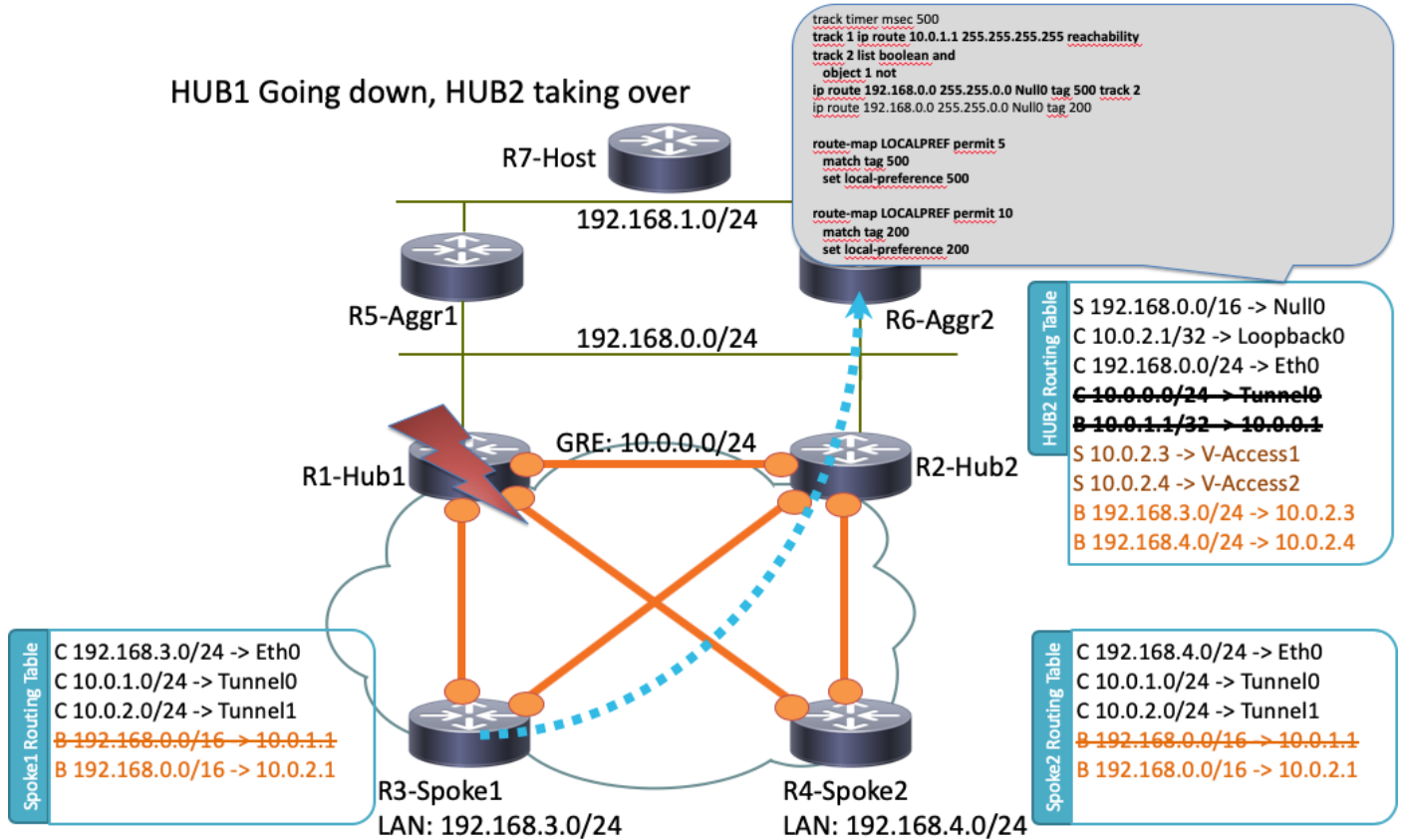
S*    0.0.0.0/0 [1/0] via 192.168.1.254
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, Ethernet0/0
L      192.168.1.7/32 is directly connected, Ethernet0/0

```

HUB1 لشف ويرانىس

وأيئابرهكلال رايتال عاطقنا لثم تاءارجإ ببسب) R1-HUB1 لفسأ ويرانىس يلى امي ف
 (ةيقرتل:

HUB1 Going down, HUB2 taking over



ثادألل لسلسلت ال اذه ثدحي ،ويراني س ال اذه في

1. R5-AGGR1 و R6-AGGR2 (LAN) ةلحمل ال ةبش ال عيمجت تاهجوم و R2-HUB2 لى لى BFD موقى . روفل بى بى بى راج ةقطنم راهنت ،كلذل ةجيتنو . R1-HUB1 طوبه ةلاى فاشتكا ب R1-HUB1 .
2. R1-HUB1 عاىرت س ال دوى فشتكى يذل R2-HUB2 ل راسم ال نئاك فاشتكا لى طعتى . (نىوكتل لاثم فى 1 راسم ال).
3. راسم ال لاقتنال رآ راسم لى غشتب هطوقس عبتت مت يذل نئال اذه موقى . (NOT). 1. راسم ال ضفخنا ام لك لى عأل 2 راسم ال بهذى ،لاىم ال اذه فى .
4. ةمى ق ب ب س ب هى جوتل لودى لى لى فاضال تباث IP هى جوت لاى لى غشت لى لى اذه يدوى . بسانم ال نىوكتل انه . ةىضارت فال ةىرادال ةفاسم ال نم لى ق :

<#root>

```

! Routes added when second HUB is down
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
  
```

```

ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
  
```

! Default static routes are with Tag 200 and admin distance of 150

```
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
```

```
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
```

5. ليحلّم BGP ليضفت مادختساب ةتباثل تاراسملا هذه عيزوت ةداعاب R2-HUB2 موقّي. ليحلّم ليضفت مادختساب متّي، لاثملا اذه في R1-HUB1 ل ةني عمل ةميقلا نم ربكأ R1-HUB1: ةطساوب اهنّي عت متّي ل 200 نم الدب، لشفل ويرانيس في 500 هراقم

```
<#root>
```

```
route-map LOCALPREF permit 5  
match tag 500
```

```
set local-preference 500
```

```
!
```

```
route-map LOCALPREF permit 10  
match tag 200
```

```
set local-preference 200
```

```
!
```

لاخداناً طحال (BGP) دودحل ةباوب لوكوتورب تاجرخم في كلذ ةيؤركنكمي، R3-talk1 في مدختسم ريغ هنكلو، ادوجوم لازي ال R1

```
<#root>
```

```
R3-SPOKE1#show ip bgp 192.168.0.0/16
```

```
BGP routing table entry for 192.168.0.0/16, version 10  
Paths: (2 available, best #1, table default)  
Not advertised to any peer  
Refresh Epoch 1  
Local
```

```
10.0.2.1 from 10.0.2.1 (10.0.2.1)
```

```
Origin incomplete, metric 0, localpref 500, valid, internal, best
```

```
rx pathid: 0, tx pathid: 0x0
```

```
Refresh Epoch 1  
Local
```

```
10.0.1.1 from 10.0.1.1 (10.0.1.1)
Origin incomplete, metric 0, localpref 200, valid, internal
rx pathid: 0, tx pathid: 0
```

6. إلى رورملا ةكرح لاسرا في (R3-Talk1 و R4-Talk2) نيفرطالال ك أدبي، ةطقنللا هذه دنع
هيجوتلل لودج يلي امي في ةدحاو ةيناث في تاوطخللا هذه عيجم شحت نأ بجي R2-HUB2.
في Talk 3:

<#root>

R3-SPOKE1#show ip route

```
10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B    10.0.0.0/8 [200/0] via 10.0.2.1, 00:00:01
S    10.0.1.1/32 is directly connected, Tunnel0
C    10.0.1.3/32 is directly connected, Tunnel0
S    10.0.2.1/32 is directly connected, Tunnel1
C    10.0.2.3/32 is directly connected, Tunnel1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.0.0/24 is directly connected, Ethernet0/0
L    172.16.0.3/32 is directly connected, Ethernet0/0

B    192.168.0.0/16 [200/0] via 10.0.2.1, 00:00:01

192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.3.0/24 is directly connected, Ethernet0/1
L    192.168.3.3/32 is directly connected, Ethernet0/1
```

7. ريظنللا فاشتكلا ليزي و R1-HUB1 و عورفللا نيب BGP لمع تاسلج لزنت دعب امي في
ىلع اذه رثؤي ال، كلذ عم و R1-HUB1 ىلعا هؤاهن متي يتي IPsec قافن (DPD) تيملا
ءاهن ةباوبك لعفللاب مدختسم R2-HUB2 نأل ارظن، تانايبلا رورم ةكرح هيجوت ةداع
ةيسيئرلل قفنللا:

<#root>

R3-SPOKE1#show ip bgp 192.168.0.0/16

```
BGP routing table entry for 192.168.0.0/16, version 10
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
Local
10.0.2.1 from 10.0.2.1 (10.0.2.1)
Origin incomplete, metric 0, localpref 500, valid, internal, best
rx pathid: 0, tx pathid: 0x0
```

تانيوكتلا

اذه ي ف اهم ادخ تس ا م تي ي ت ل ا ت ا و ن ق ل ا و ع ي ز و ت ل ا ت ا ح و ل ت ا ن ي و ك ت ل ا ج ذ و م ن م س ق ل ا ا ذ ه ر ف و ي ط ط خ م ل .

R1-HUB ن ي و ك ت

<#root>

```
version 15.4
!
hostname R1-HUB1
!
aaa new-model
!
aaa authorization network default local
!
aaa session-id common
!
! setting track timers to the lowest possible (the lower this value is
! the faster router will react

track timer ip route msec 500

!
! Monitoring of HUB2's loopback present in routing table
! If it is present it will mean that HUB2 is alive
track 1 ip route 10.0.2.1 255.255.255.255 reachability
!
! Monitoring of loopback of R5-AGGR-1
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
! Monitoring of loopback of R6-AGGR-2
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
! Track 2 should be UP only when HUB2 is not available and both AGGRE routers are up
!
track 2 list boolean and
  object 1 not
  object 3
  object 4
!

! IKEv2 Config Exchange configuration (IP addresses for spokes are assigned from pool)
crypto ikev2 authorization policy default
  pool SPOKES
  route set interface
  route accept any tag 20
!
!
! IKEv2 profile for Spokes - Smart Defaults used
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  aaa authorization group psk list default default
  virtual-template 1
!
interface Loopback0
  ip address 10.0.1.1 255.255.255.255
```

```
!  
! GRE Tunnel configured to second HUB. It is required for spoke-to-spoke connectivity  
! to work in all possible circumstances  
!
```

no BFD echo

```
configuration is required to avoid Traffic Indication sent by remote HUB  
! (BFD echo is having the same source and destination IP address)
```

```
!  
interface Tunnel0  
ip address 10.0.0.1 255.255.255.0  
ip nhrp network-id 1  
ip nhrp redirect  
  
bfd interval 50 min_rx 50 multiplier 3
```

no bfd echo

```
tunnel source Ethernet0/2  
tunnel destination 192.168.0.2  
!  
interface Ethernet0/0  
ip address 172.16.0.1 255.255.255.0  
!  
interface Ethernet0/2  
ip address 192.168.0.1 255.255.255.0  
bfd interval 50 min_rx 50 multiplier 5  
!  
interface Virtual-Template1 type tunnel  
ip unnumbered Loopback0  
ip nhrp network-id 1  
ip nhrp redirect  
tunnel protection ipsec profile default  
!  
! BGP Configuration  
router bgp 1  
bgp log-neighbor-changes  
! dynamic peer-groups are used for AGGR routers and SPOKES  
bgp listen range 192.168.0.0/24 peer-group DC  
bgp listen range 10.0.1.0/24 peer-group SPOKES  
! BGP timers configured  
timers bgp 15 30  
neighbor SPOKES peer-group  
neighbor SPOKES remote-as 1  
neighbor DC peer-group  
neighbor DC remote-as 1  
! Within DC BFD is used to determine neighbour status  
neighbor DC fall-over bfd  
neighbor 10.0.0.2 remote-as 1  
! BFD is used to detect HUB2 status  
neighbor 10.0.0.2 fall-over bfd  
!  
address-family ipv4  
redistribute connected  
! route-map which determines what should be the local-pref  
redistribute static route-map LOCALPREF  
neighbor SPOKES activate  
! to spokes only Aggregate/Summary routes are sent  
neighbor SPOKES route-map AGGR out  
neighbor DC activate
```

```

neighbor DC route-reflector-client
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 route-reflector-client
exit-address-family
!
ip local pool SPOKES 10.0.1.2 10.0.1.254
!

```

! When HUB2 goes down Static Routes with Tag 500 are added and admin distance of 1

```
ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2
```

```
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2
```

! Default static routes are with Tag 200 and admin distance of 150

```
ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200
```

```
ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200
```

```

!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
 match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
 match tag 500
 set local-preference 500
!
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 200
!
route-map LOCALPREF permit 15
 match tag 20

```

نېوكت R2-HUB2

<#root>

```

hostname R2-HUB2
!
aaa new-model
!
aaa authorization network default local
!
track timer ip route msec 500

```

```

!
track 1 ip route 10.0.1.1 255.255.255.255 reachability
!
track 2 list boolean and
    object 1 not
    object 3
    object 4
!
track 3 ip route 10.0.5.1 255.255.255.255 reachability
!
track 4 ip route 10.0.6.1 255.255.255.255 reachability
!
!
crypto ikev2 authorization policy default
    pool SPOKES
    route set interface
    route accept any tag 20
!
!
crypto ikev2 profile default
    match identity remote any
    authentication remote pre-share key cisco
    authentication local pre-share key cisco
    aaa authorization group psk list default default
    virtual-template 1
!
!
interface Loopback0
    ip address 10.0.2.1 255.255.255.255
!
interface Tunnel0
    ip address 10.0.0.2 255.255.255.0
    ip nhrp network-id 1
    ip nhrp redirect
    bfd interval 50 min_rx 50 multiplier 3
    no bfd echo
    tunnel source Ethernet0/2
    tunnel destination 192.168.0.1
!
interface Ethernet0/0
    ip address 172.16.0.2 255.255.255.0
!
interface Ethernet0/2
    ip address 192.168.0.2 255.255.255.0
    bfd interval 50 min_rx 50 multiplier 5
!
interface Virtual-Template1 type tunnel
    ip unnumbered Loopback0
    ip nhrp network-id 1
    ip nhrp redirect
    tunnel protection ipsec profile default
!
router bgp 1
    bgp log-neighbor-changes
    bgp listen range 192.168.0.0/24 peer-group DC
    bgp listen range 10.0.2.0/24 peer-group SPOKES
    timers bgp 15 30
    neighbor SPOKES peer-group
    neighbor SPOKES remote-as 1
    neighbor DC peer-group
    neighbor DC remote-as 1
    neighbor DC fall-over bfd

```



```

neighbor 10.0.0.1 remote-as 1
neighbor 10.0.0.1 fall-over bfd
!
address-family ipv4
 redistribute connected
 redistribute static route-map LOCALPREF
 neighbor SPOKES activate
 neighbor SPOKES route-map AGGR out
 neighbor DC activate
 neighbor DC route-reflector-client
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 route-reflector-client
exit-address-family
!
ip local pool SPOKES 10.0.2.2 10.0.2.254
ip forward-protocol nd
!
!
ip route 192.168.0.0 255.255.0.0 Null0 tag 500 track 2

```

```

ip route 10.0.0.0 255.0.0.0 Null0 tag 500 track 2

```

```

ip route 10.0.0.0 255.0.0.0 Null0 150 tag 200

```

```

ip route 192.168.0.0 255.255.0.0 Null0 150 tag 200

```

```

!
!
ip prefix-list AGGR seq 5 permit 192.168.0.0/16
ip prefix-list AGGR seq 10 permit 10.0.0.0/8
!
route-map AGGR permit 10
 match ip address prefix-list AGGR
!
route-map LOCALPREF permit 5
 match tag 500
 set local-preference 500
!
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 100
!
route-map LOCALPREF permit 15
 match tag 20

```

R3-TALK1 نڧوكت

```

hostname R3-SPOKE1
!
aaa new-model
!

```

```

aaa authorization network default local
!
!
crypto ikev2 authorization policy default
    route set interface
!
!
crypto ikev2 profile default
    match identity remote any
    authentication remote pre-share key cisco
    authentication local pre-share key cisco
    dpd 10 2 on-demand
    aaa authorization group psk list default default
!
! Tunnel to the HUB1
!
interface Tunnel0
    ip address negotiated
    ip nhrp network-id 1
    ip nhrp shortcut virtual-template 2
    tunnel source Ethernet0/0
    tunnel destination 172.16.0.1
    tunnel protection ipsec profile default
!
! Tunnel to the HUB2
!
interface Tunnel1
    ip address negotiated
    ip nhrp network-id 1
    ip nhrp shortcut virtual-template 2
    tunnel source Ethernet0/0
    tunnel destination 172.16.0.2
    tunnel protection ipsec profile default
!
interface Ethernet0/0
    description INTERNET-CLOUD
    ip address 172.16.0.3 255.255.255.0
!
interface Ethernet0/1
    description LAN
    ip address 192.168.3.3 255.255.255.0
!
interface Virtual-Template2 type tunnel
    ip unnumbered Ethernet0/1
    ip nhrp network-id 1
    ip nhrp shortcut virtual-template 2
    tunnel protection ipsec profile default
!
router bgp 1
    bgp log-neighbor-changes
    timers bgp 15 30
    neighbor 10.0.1.1 remote-as 1
    neighbor 10.0.2.1 remote-as 1
    !
    address-family ipv4
        network 192.168.3.0
        neighbor 10.0.1.1 activate
        neighbor 10.0.2.1 activate
    exit-address-family

```

R4-Talk2 نيوكت

```
hostname R4-SPOKE2
!
aaa new-model
!
aaa authorization network default local
!
!
crypto ikev2 authorization policy default
  route set interface
!
crypto ikev2 profile default
  match identity remote any
  authentication remote pre-share key cisco
  authentication local pre-share key cisco
  dpd 10 2 on-demand
  aaa authorization group psk list default default
!
interface Tunnel0
  ip address negotiated
  ip nhrp network-id 1
  ip nhrp shortcut virtual-template 2
  tunnel source Ethernet0/0
  tunnel destination 172.16.0.1
  tunnel protection ipsec profile default
!
interface Tunnel1
  ip address negotiated
  ip nhrp network-id 1
  ip nhrp shortcut virtual-template 2
  tunnel source Ethernet0/0
  tunnel destination 172.16.0.2
  tunnel protection ipsec profile default
!
interface Ethernet0/0
  ip address 172.16.0.4 255.255.255.0
!
interface Ethernet0/1
  ip address 192.168.4.4 255.255.255.0
!
interface Virtual-Template2 type tunnel
  ip unnumbered Ethernet0/1
  ip nhrp network-id 1
  ip nhrp shortcut virtual-template 2
  tunnel protection ipsec profile default
!
router bgp 1
  bgp log-neighbor-changes
  timers bgp 15 30
  neighbor 10.0.1.1 remote-as 1
  neighbor 10.0.2.1 remote-as 1
  !
  address-family ipv4
    network 192.168.4.0
    neighbor 10.0.1.1 activate
    neighbor 10.0.2.1 activate
  exit-address-family
!
```

R5-AGGR1 نى وىكت

```
hostname R5-LAN1
!
no aaa new-model
!
!
interface Loopback0
 ip address 10.0.5.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.5 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
! HSRP configuration on the LAN side
!
interface Ethernet0/1
 ip address 192.168.1.5 255.255.255.0
 standby 1 ip 192.168.1.254
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 1
 neighbor 192.168.0.1 fall-over bfd
 neighbor 192.168.0.2 remote-as 1
 neighbor 192.168.0.2 fall-over bfd
!
 address-family ipv4
  redistribute connected
  redistribute static
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.2 activate
 exit-address-family
```

R6-AGGR2 نى وىكت

```
hostname R6-LAN2
!
interface Loopback0
 ip address 10.0.6.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.6 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 5
!
interface Ethernet0/1
 ip address 192.168.1.6 255.255.255.0
 standby 1 ip 192.168.1.254
 standby 1 priority 200
!
router bgp 1
 bgp log-neighbor-changes
```

```

neighbor 192.168.0.1 remote-as 1
neighbor 192.168.0.1 fall-over bfd
neighbor 192.168.0.2 remote-as 1
neighbor 192.168.0.2 fall-over bfd
!
address-family ipv4
 redistribute connected
 redistribute static
 neighbor 192.168.0.1 activate
 neighbor 192.168.0.2 activate
exit-address-family
!

```

(ةكبشلا كلت ي ف فيضملا ةكاحم) R7 فيضم نيوكت

```

hostname R7-HOST
!
no aaa new-model
!
interface Ethernet0/0
 ip address 192.168.1.7 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254

```

ةماه نيوكت تاظالم

ةقباسلا ماسقألا في ةحضملا تانيوكتلا لوح ةمهمل تاظالملا ضعب يلي امي:

- لال خ نم لاصتالا ريفوتل نيوكترملا ني ب ةطقن لىا ةطقن نم GRE قفن دوجو مزلي و ، تاهوي راني سلا عي مج في لمعلل رشابملا لاصتالا لال خ نم لاصتالا لال خ نم لاصتالا دحأب الا عورفلا ضعب اهي ف لصتت ال يتلا تاهوي راني سلا ني مضا دي دحتلا هجو لىعو . رخآ زكرم ب لىا لصتت امن ب نيوكترملا
- رورملا ةكرح ةراشإ بنجتل نيوكترملا ني ب GRE قفن ةهجاو في no bfd echo نيوكت مزلي ، ةهجو لاو ردصملا IP ناو نع سفن لىا BFD لىا دص يوتحي . رخآ عزوم نم اهلا سلا متي يتلا هي جوت متي هنأ ارظنو . BFD لىا دص لسري يذلا هجوملا ب صاخلا IP ناو نع يواسي يذلاو . NHRP رورم ةكرح تارشؤم عاشنإ متي ، بيجتسي يذلا هجوملا ةطساوب لىا رخأ ةرم مزحلا هذه
- وحن تاكبشلا نع نلعت يتلا راسملا ةطي رخ ةيفصت نوكت ال ، BGP نيوكت في نع نالعالا متي هنأ ارظن ةيلالام رثكأ تانيوكتلا لعجت اهنكلو ، ةبولطم مداوخل طقف زجوملا/ عي مجتلا تاهجوم

<#root>

neighbor SPOKES route-map AGGR out

- دادعإ لجأ نم راسم المة طيرخ لة لة حم المة اءاءعإل نة وكة مزلے، عة زوتل اءاول ىل ع
ءاعم المة ءءبائل اءاسم المة ءة فصءب موقے امك، بس انم المة لة حم المة BGP لة لة صفء
طقف IKEv2 و صءلم المة نة وكة عءو اءاسم ىل اءاع زوت
- طبار عطقنا اءا. (مككء) Remote Office عءاوم ف راركءل مة م صءل اءه لوانءة ال
طابءر اءافاضاب مق. لمعء ال اضة VPN ءكبش ناف، ءوصل ربكم ىل ع WAN ءكبش
لءاء هب ءءءل مءة ناء هءوم ءافاضا و اءب ءءءل مءة لة هءوم ال هءوم ال ىل ناء
ءل ءشم المة هءه ءل اعم لجأ نم عءوم ال سفن

هـ حاصل انم ققحتلا

اهـ حال صـ او ءاطـ خـ الـ فـ اشـ كـ تـ سـ اـ

قلص تاذا تامل و علم

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا