FlexVPN HA雙集線器配置示例

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

- 網路圖表
- 常規操作方案
- 輻條到輻條（快捷方式）
- 常規運行方案的路由表和輸出
- HUB1故障場景
- 組態
  - R1-HUB配置
  - R2-HUB2配置
  - R3分支配置1
  - R4-SPOKE2配置
  - R5-AGGR1配置
  - R6-AGGR2配置
  - R7-HOST配置（模擬該網路中的主機）
- 重要配置說明

驗證

疑難排解

相關資訊

簡介

本文檔介紹如何為通過基於IPSec的VPN通過不安全網路介質（如Internet）連線到資料中心的遠端辦公室配置完全冗餘設計。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下技術元件而建立：

- 邊界閘道通訊協定(BGP)，作為資料中心內以及VPN重疊中輻條與集線器之間的路由通訊協定。
- 雙向轉發檢測(BFD)是一種機制，可檢測僅運行在資料中心內部（而不是通過重疊隧道）的下行鏈路（路由器關閉）。
- 在集線器和輻條之間的Cisco IOS® FlexVPN，通過快捷交換啟用分支到分支功能。
- 兩個集線器之間的通用路由封裝(GRE)通道化，啟用輻射到輻射通信，即使輻射連線到不同的集線器。
- 增強的對象跟蹤和與被跟蹤對象關聯的靜態路由。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

在為資料中心設計遠端訪問解決方案時，高可用性(HA)通常是任務關鍵型使用者應用程式的關鍵要求。

本文檔中提供的解決方案允許快速檢測和從故障情形中恢復，在這些故障情形中，一個VPN終端集線器因重新載入、升級或電源問題而關閉。然後，所有遠端辦公室路由器（分支）在檢測到此類故障後立即使用另一個運行中心。

此設計的優點如下：

- 從VPN集線器關閉情形中快速恢復網路
- VPN集線器之間沒有複雜的狀態同步(例如IPSec安全關聯(SA)、Internet安全關聯和金鑰管理協定(ISAKMP)SA以及加密路由)
- 由於IPSec有狀態HA的封裝安全負載(ESP)序列號同步存在延遲，因此沒有反重播問題
- VPN集線器可以使用不同的基於Cisco IOS/IOS-XE的硬體或軟體
- 靈活的負載均衡實施選擇，BGP作為VPN重疊中運行的路由協定
- 清除所有裝置上可讀的路由，且沒有後台運行的隱藏機制
- 直接輻條到輻條連線
- FlexVPN的所有優勢，包括驗證、授權和記帳(AAA)整合以及每通道服務品質(QoS)

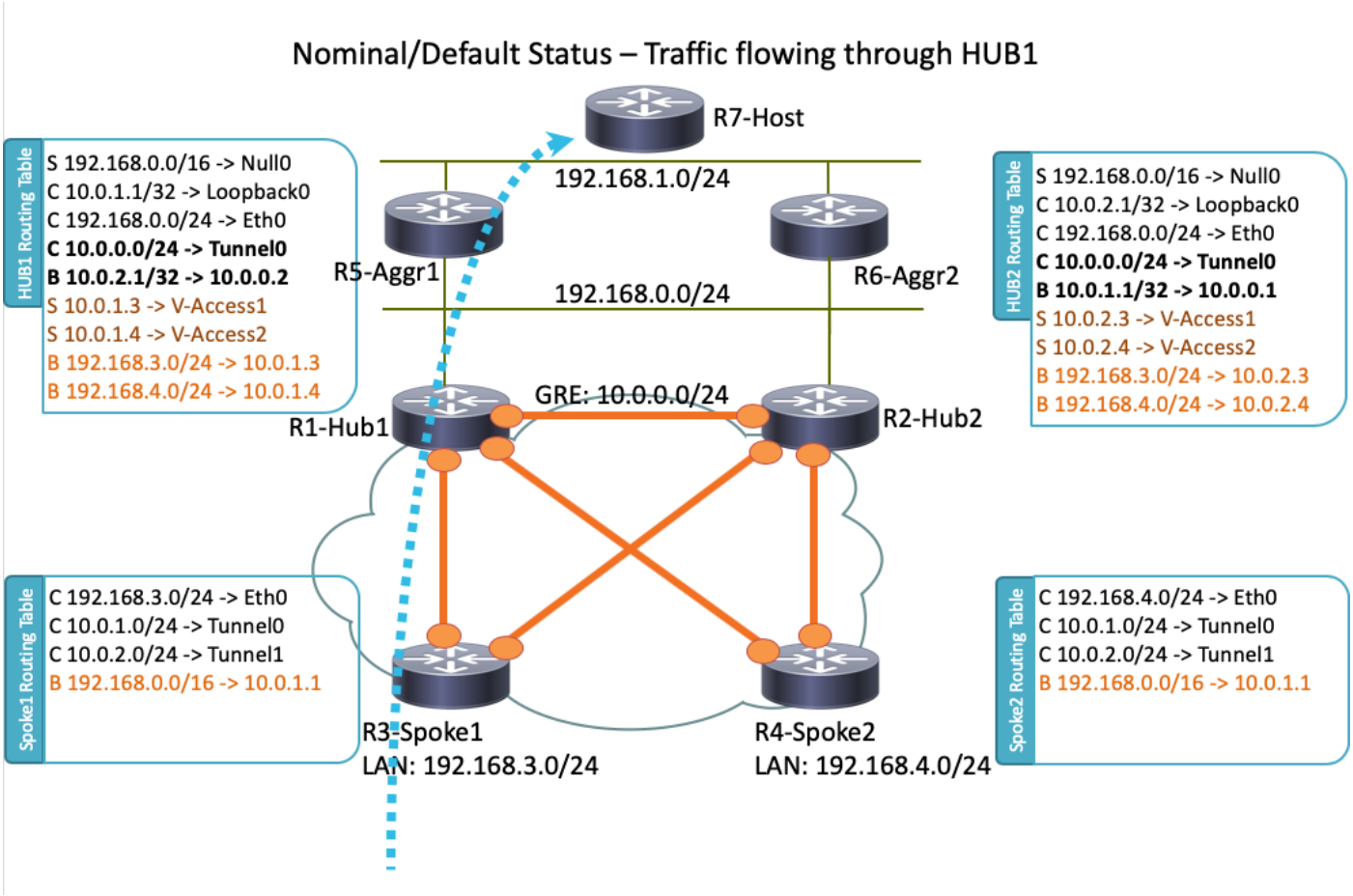
設定

本節提供示例場景，並說明如何為通過不安全網路介質上基於IPSec的VPN連線到資料中心的遠端辦公室配置完全冗餘設計。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表

本檔案使用的網路拓撲如下：



附註：此拓撲中使用的所有路由器都運行Cisco IOS版本15.2(4)M1，而Internet Cloud使用的地址方案為172.16.0.0/24。

常規操作方案

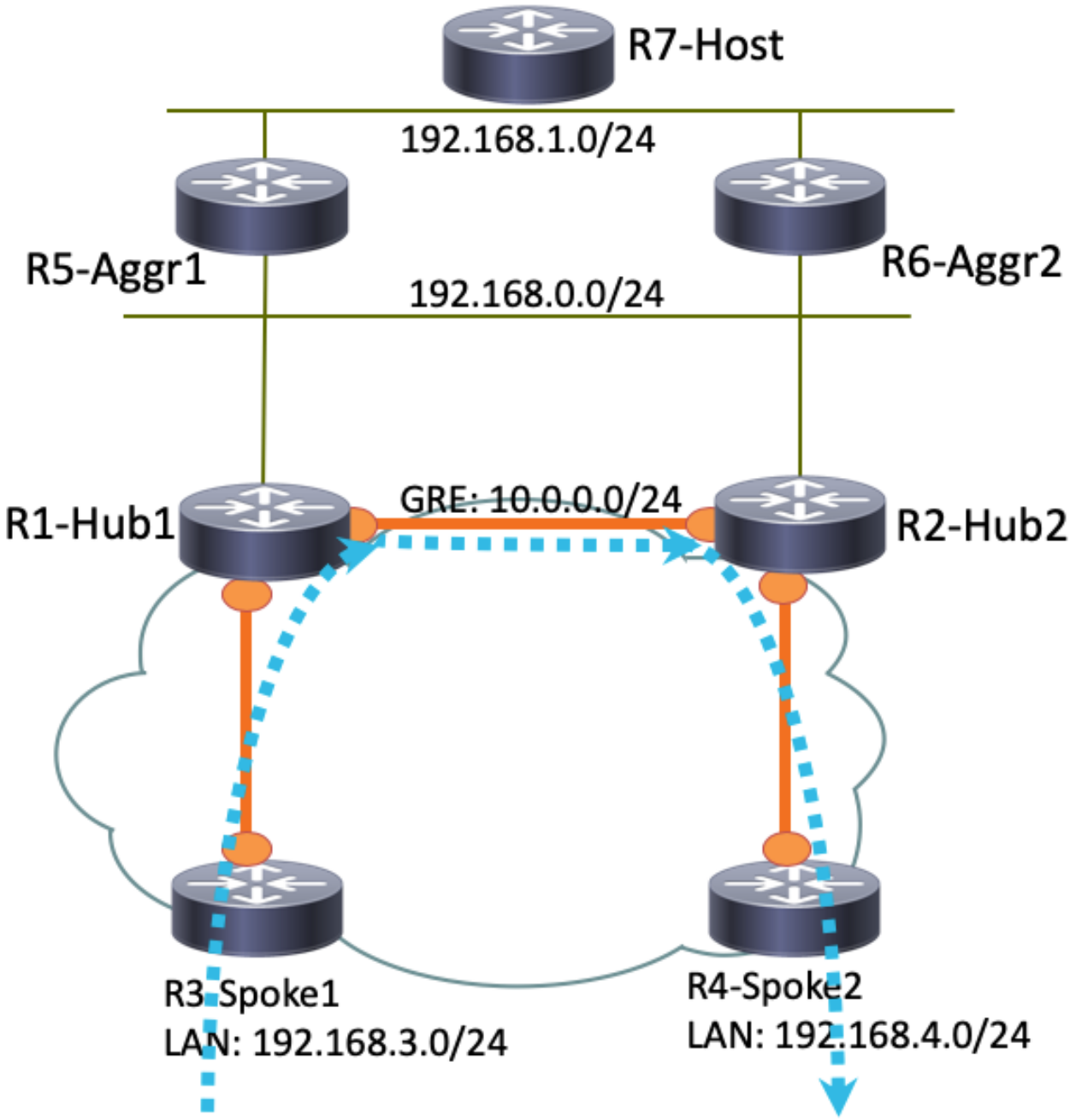
在正常運行情況下，當所有路由器都啟動並正常運行時，所有分支路由器都會通過預設集線器(R1-HUB1)路由所有流量。 當預設BGP本地首選項設定為200時（請參閱後面的章節瞭解詳細資訊），就會獲得此路由首選項。它可以根據部署要求（如流量負載平衡）進行調整。

輻條到輻條（快捷方式）

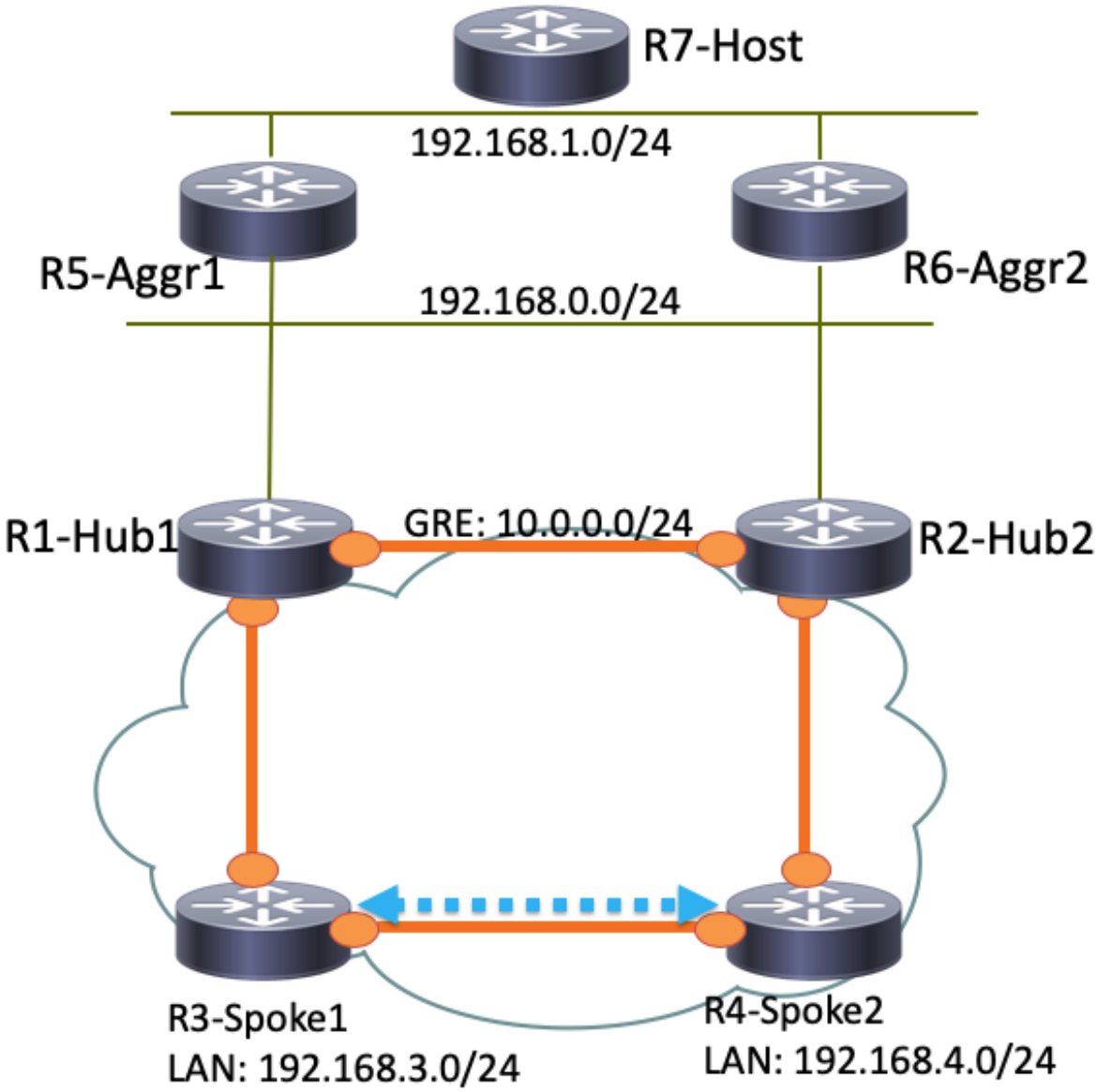
如果R3-Spoke1發起到R4-Spoke2的連線，則會使用短路徑交換配置建立動態輻條到輻條隧道。

提示：有關詳細資訊，請參閱配置FlexVPN分支到分支配置指南。

如果R3-Spoke1僅連線到R1-HUB1，而R4-Spoke2僅連線到R2-HUB2，則仍然可以通過在集線器之間運行的點對點GRE隧道實現直接輻條到輻條連線。在這種情況下，R3-Spoke1和R4-Spoke2之間的初始流量路徑看起來與以下類似：



由於R1-Hub1在虛擬接入介面上收到資料包，該介面與GRE隧道上的下一跳解析協定(NHRP)網路ID相同，因此將向R3-Spoke1傳送流量指示。這將觸發建立分支到分支的動態隧道：



常規運行方案的路由表和輸出

以下是正常運行場景中的R1-HUB1路由表：

<#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
```

以下是使用R4-SPOKE2的輻條到輻條隧道建立後常規運行方案中的R3-SPOKE1路由表：

<#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
```

在R3-Spoke1上，BGP表有兩個用於192.168.0.0/16網路的條目，它們的本地首選項不同（首選R1-Hub1）：

<#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
```

以下是正常運行場景中的R5-AGGR1路由表：

<#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
```

以下是正常運行方案中的R7-HOST路由表：

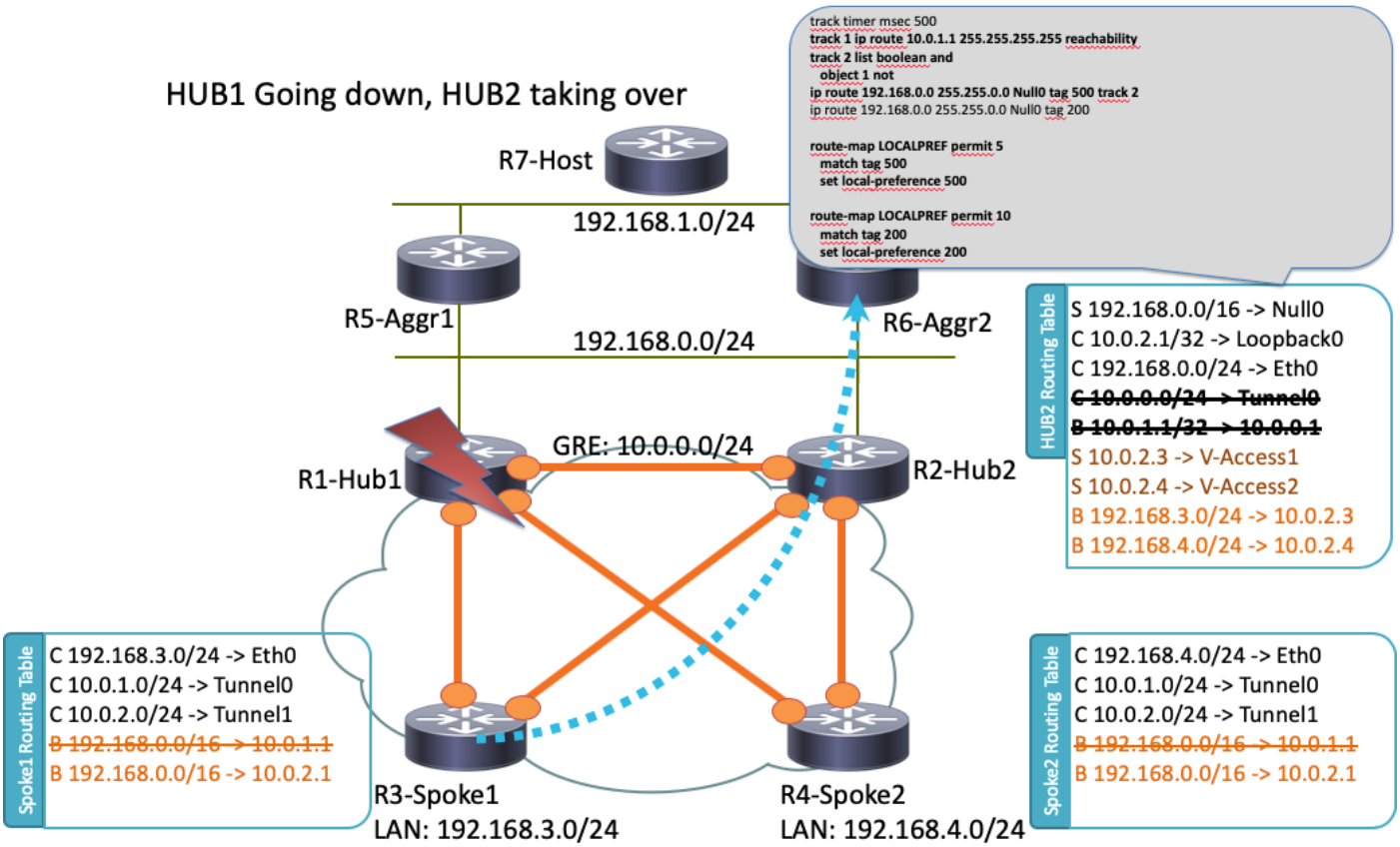
<#root>

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故障場景

以下是R1-HUB1故障情況（由於停電或升級等操作）：



在此案例中，發生以下系列事件：

1. R2-HUB2和LAN上的BFD聚合路由器R5-AGGR1和R6-AGGR2檢測到R1-HUB1的關閉狀態。因此，BGP鄰居關係立即關閉。

2. 檢測R1-HUB1環回是否存在的R2-HUB2的跟蹤對象檢測會關閉（示例配置中的跟蹤1）。

3. 此已下載的跟蹤對象將觸發另一個跟蹤啟動（邏輯NOT）。 在本例中，軌道2在軌道1關閉時啟動。

4. 這會觸發靜態IP路由條目，由於該條目值小於預設管理距離，因此該條目將被新增到路由表中。以下是相關組態：

<#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. R2-HUB2使用大於為R1-HUB1設定的值的BGP local-preference來重新分發這些靜態路由。在此示例中，本地優先順序500用於故障方案，而不是由R1-HUB1設定的200:

<#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


!
```

在R3-Spoke1上，您可以在BGP輸出中看到這一點。請注意，R1的條目仍然存在，但未使用：

<#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. 此時，兩個分支（R3-Spoke1和R4-Spoke2）開始向R2-HUB2傳送流量。所有這些步驟都應在一秒鐘內完成。分支3上的路由表如下：

<#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. 分支和R1-HUB1之間的較後BGP會話關閉，而失效對等項檢測(DPD)將刪除在R1-HUB1上終止的IPSec隧道。但是，這不會影響流量轉發，因為R2-HUB2已用作主隧道終止網關：

<#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
```

組態

本節提供此拓撲中使用的集線器和輻條的配置示例。

R1-HUB配置

<#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
```

R2-HUB2配置

<#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分支配置1

```
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-SPOKE2配置

```
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配置

```
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配置

```
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
!
```

R7-HOST配置（模擬該網路中的主機）

```
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
```

重要配置說明

以下是前面幾節中介紹的有關配置的一些重要說明：

- 兩個集線器之間的點對點GRE隧道是輻射點到輻射點連線在所有場景下正常工作的必要條件，特別是要包括某些輻射點僅連線到其中一個集線器，而另一些輻射點連線到另一個集線器的場景。

- 兩個集線器之間的GRE通道介面中需要no bfd echo組態，才能避免從另一個集線器傳送的流量指示。BFD Echo具有相同的源IP地址和目的IP地址，該地址等於傳送BFD Echo的路由器的IP地址。由於這些資料包由作出響應的路由器傳回，因此會生成NHRP流量指示。

- 在BGP配置中，不需要將網路通告到分支的路由對映過濾，但是它使配置更最佳化，因為僅通告聚合/彙總路由：

  <#root>

  neighbor SPOKES route-map AGGR out

- 在集線器上，需要route-map LOCALPREF配置才能設定正確的BGP本地首選項，並且它會將重分發的靜態路由篩選為僅彙總路由和IKEv2配置模式路由。

- 此設計不能解決遠端辦公室位置（分支）的冗餘問題。 如果分支上的WAN鏈路斷開，VPN也無法工作。將第二個鏈路新增到分支路由器或在同一位置新增第二個分支路由器以解決此問題。

總而言之，文中呈現的備援設計可視為有狀態切換(SSO)/有狀態功能的現代替代方案。它非常靈活，可進行微調，以滿足您的特定部署要求。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco IOS FlexVPN產品手冊
- 配置FlexVPN分支到分支
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。