

FlexVPN HA双重集线器上配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[正常可操作的方案](#)

[spoke-to-spoke \(快捷方式\)](#)

[路由表和输出正常可操作的方案的](#)

[HUB1故障情景](#)

[配置](#)

[R1-HUB配置](#)

[R2-HUB2配置](#)

[R3-SPOKE1配置](#)

[R4-SPOKE2配置](#)

[R5-AGGR1配置](#)

[R6-AGGR2配置](#)

[R7-HOST配置\(主机的模拟在该网络的\)](#)

[必需的配置附注](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何配置连接到数据中心通过非安全网络媒体的基于IPSec的VPN的远程办公室的一个全面冗余设计，例如互联网。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文的信息根据这些技术组件：

- [边界网关协议\(BGP\)](#)作为路由协议在数据中心内和在spoke和集线器之间在VPN重叠。

- [双向转发检测](#)(BFD)作为发现在链路的机制(下来路由器下)该运行在仅数据中心里面(不在重叠隧道)。
-
- [建立隧道](#)在两集线器为了enable (event) spoke-to-spoke通信之间的[通用路由封装\(GRE\)](#)，既使当spoke被连接到另外集线器。
- [改进的对象跟踪](#)和静态路由附加对被跟踪的对象。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

当您设计数据中心的时远程访问解决方案，高可用性(HA)经常是目标关键用户应用的一个关键需求。

在本文被提交的解决方案允许快速的检测和恢复从故障情景在哪个VPN终止的集线器沿着走由于重新加载、升级或者电源问题。所有远程办公室路由器(spoke)立即然后使用另一台可操作的集线器当查出这样故障时。

这是此设计的优点：

- 从VPN HUB下来方案的快速的网络恢复
- 没有复杂有状态的同步(例如IPSec安全关联(SA)、互联网安全协会和密钥管理协议(ISAKMP) SAS和Crypto路由)在VPN集线器之间
- 没有反重放问题由于封装安全有效载荷(ESP)序号同步的延迟与IPSec有状态的HA
- VPN集线器能使用另外Cisco IOS/IOS-XE基于硬件或软件
- 与BGP的灵活的负载平衡实施选择作为在VPN重叠运行的路由协议
- 在所有设备的清楚和可读的路由没有在背景中运行的隐藏的机制
- 直接spoke-to-spoke连接
- 所有[FlexVPN](#)优点，包括验证、授权和统计(AAA)集成和每隧道服务质量(QoS)

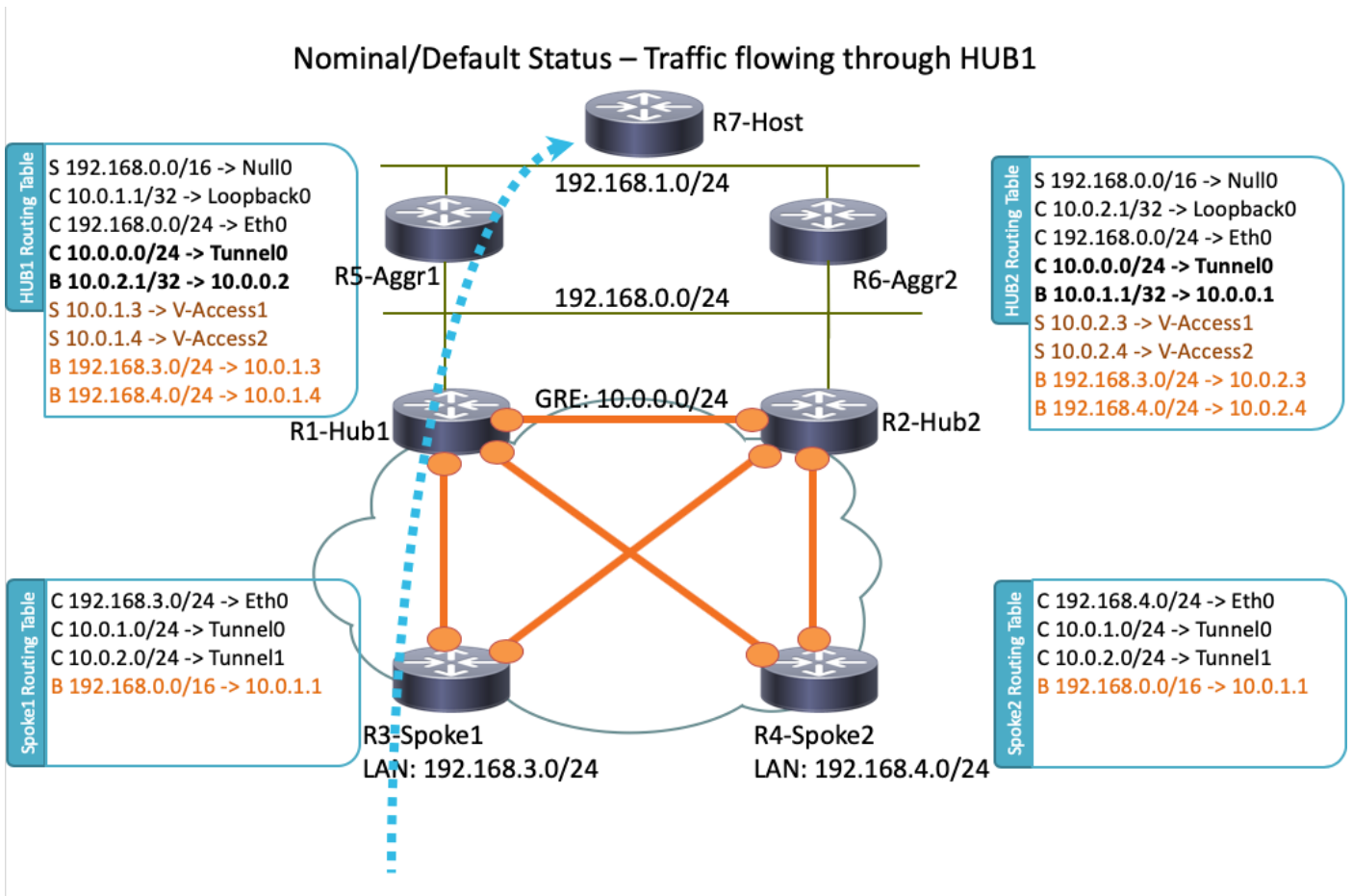
配置

此部分提供示例情景并且描述如何配置连接到数据中心通过非安全网络媒体的基于IPSec的VPN的远程办公室的一个全面冗余设计。

Note:使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

网络图

这是在本文使用的网络拓扑：



Note: 在此拓扑方面使用的所有路由器运行Cisco IOS版本15.2(4)M1和互联网Cloud使用地址方案172.16.0.0/24。

正常可操作的方案

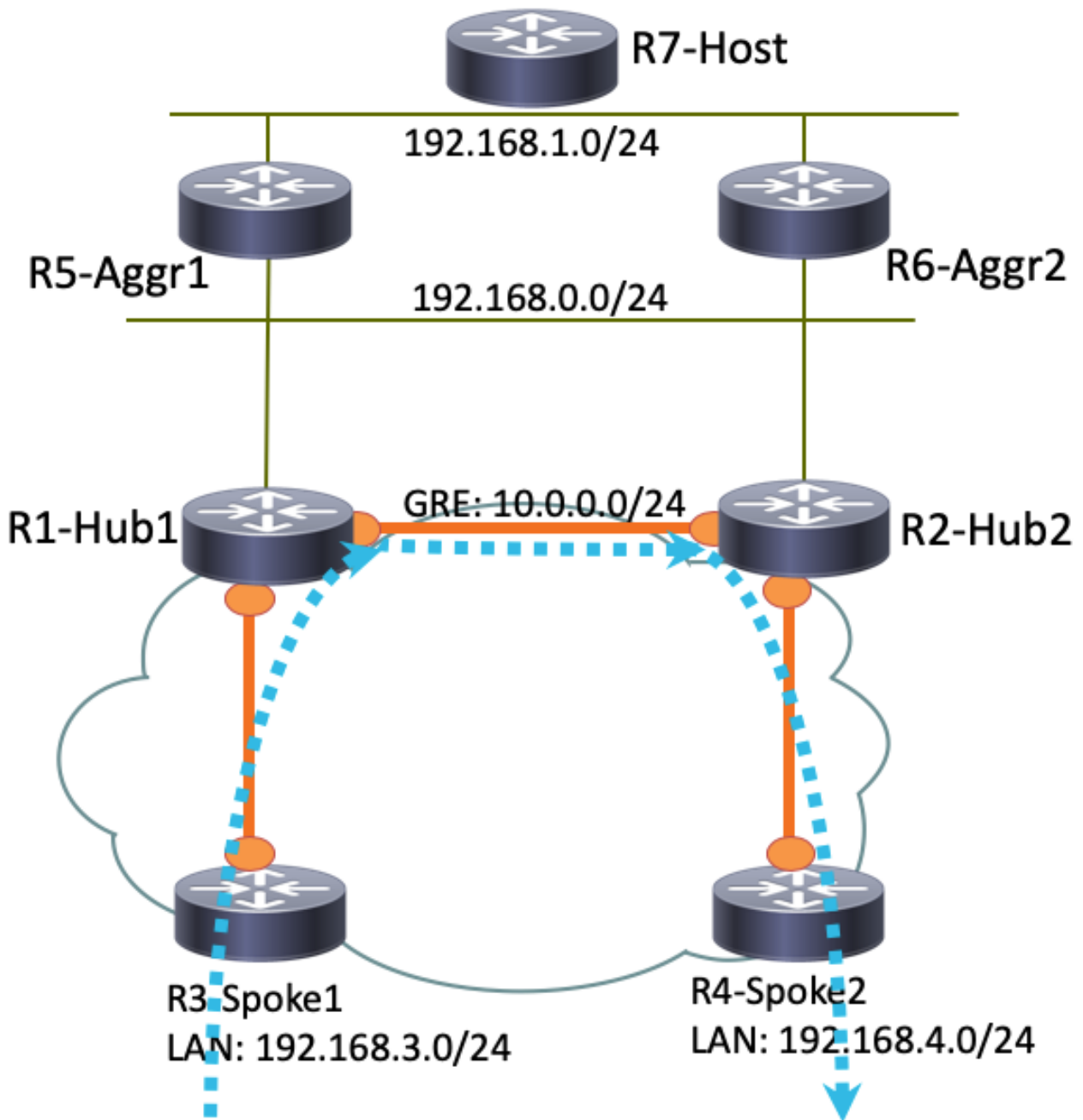
在一个正常可操作的方案中，当所有路由器是上和可操作的时，所有分支路由器通过默认集线器 (R1-HUB1)发送所有数据流。此路由首选达到，当默认BGP本地首选设置到200时(请参见跟随关于详细资料)的部分。这可以根据配置需求被调整，例如数据流负载平衡。

spoke-to-spoke (快捷方式)

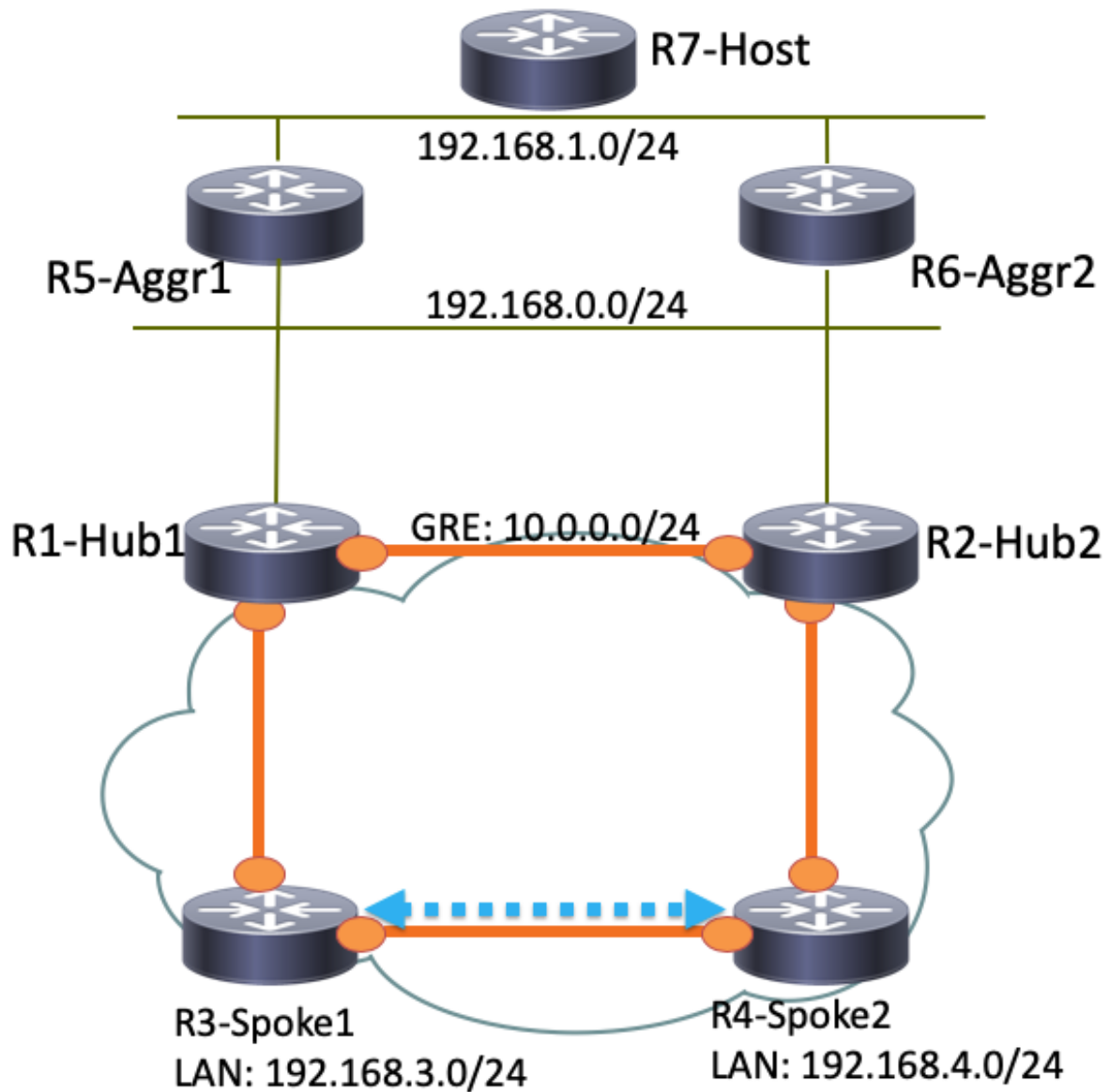
如果R3-Spoke1首次与R4-Spoke2的连接，一条动态spoke-to-spoke隧道用快捷方式交换配置创建。

提示： 欲了解更详细的信息，请参见[配置的FlexVPN分支对分支配置指南](#)。

如果R3-Spoke1仅被连接到R1-HUB1，并且R4-Spoke2仅被连接到R2-HUB2，直接spoke-to-spoke连接可能仍然达到与运行在集线器之间的点到点GRE封装隧道。在这种情况下，R3-Spoke1之间的最初的数据流路径和R4-Spoke2看起来与此相似：



因为R1-Hub1收到在虚拟访问接口的信息包，有下一跳解析协议(NHRP)网络ID和那一样在GRE封装隧道，流量指示被发送往R3-Spoke1。这触发spoke-to-spoke动态隧道创建：



路由表和输出正常可操作的方案的

这是在正常可操作的方案的R1-HUB1路由表：

```
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

```

这是在一个正常可操作的方案的R3-SPOKE1路由表，在有R4-SPOKE2的spoke-to-spoke隧道被创建后：

```
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，BGP表有192.168.0.0/16网络的两个条目用不同的本地首选(R1-Hub1更喜欢)：

```
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

```

这是在一个正常可操作的方案的R5-AGGR1路由表：

```

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

```

这是在一个正常可操作的方案的R7-HOST路由表：

```

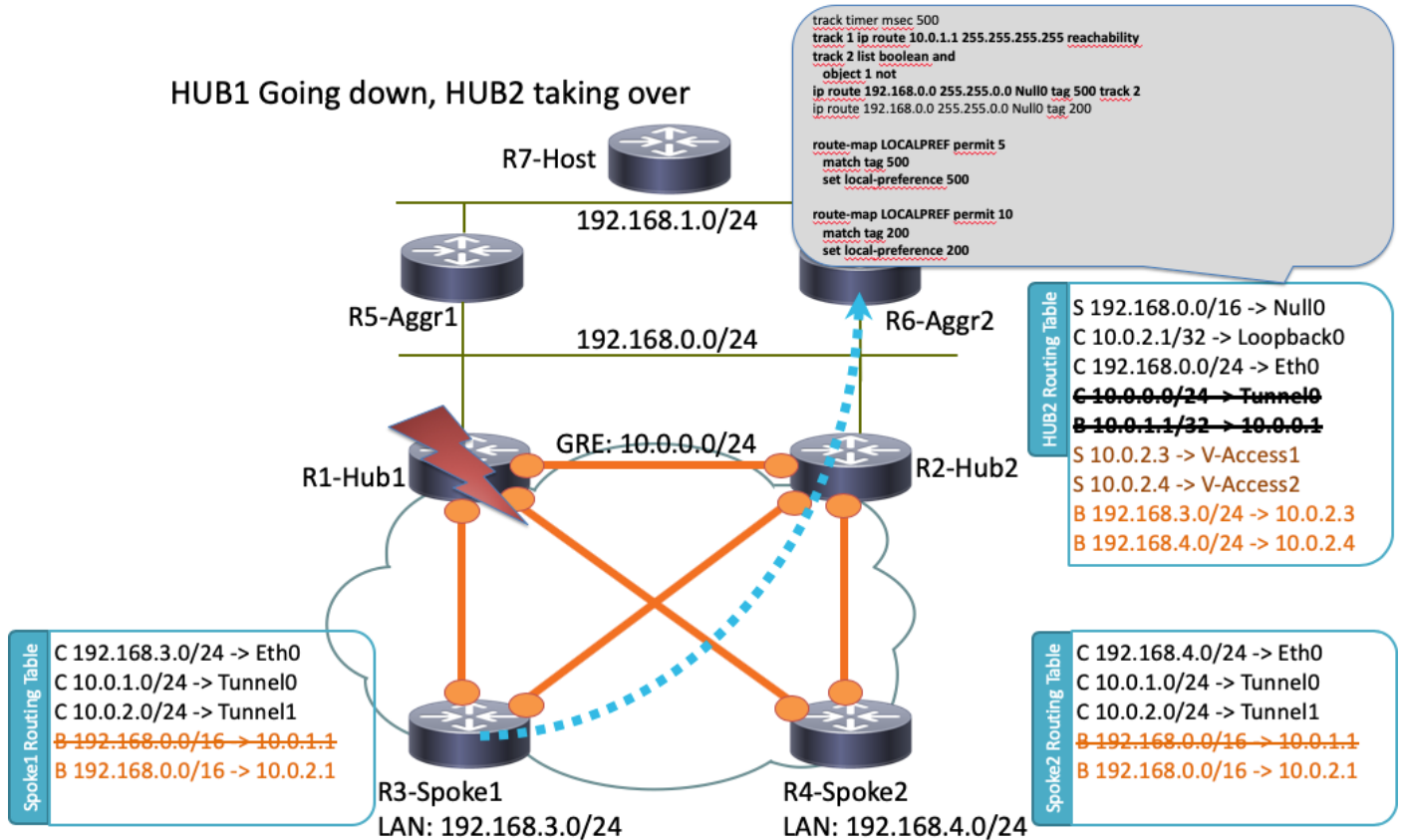
R7-HOST#show ip route
S*   0.0.0.0/0 [1/0] via 192.168.1.254
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, Ethernet0/0
L    192.168.1.7/32 is directly connected, Ethernet0/0

```

HUB1故障情景

这是R1-HUB1下来方案(由于动作例如停电或升级)：

HUB1 Going down, HUB2 taking over



在此方案中，此事件顺序出现：

1. BFD在R2-HUB2和在LAN聚合路由器R5-AGGR1和R6-AGGR2发现R1-HUB1的中断状态。结果，BGP邻居立即断开。
2. 发现R1-HUB1环回的出现的R2-HUB2的跟踪对象检测断开(在示例配置的跟踪1)。
3. 向下的这跟踪了对象触发另一跟踪上升(逻辑没有)。在本例中，跟踪2上升，每当跟踪1断开。
4. 这触发将被添加的静态IP路由条目到路由表由于比默认管理距离低的值。这是相关配置：

```

! 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. 大于值为R1-HUB1设置的R2-HUB2再分布有BGP local-preference的这些静态路由。在本例中，local-preference 500用于R1-HUB1设置的故障情景，而不是200：

```

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，您在BGP输出中能看到此。注意对R1的条目仍然存在，但是没有使用：

```
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. 这时，两个spoke (R3-Spoke1和R4-Spoke2)开始发送数据流到R2-HUB2。所有这些步骤应该发生在一秒钟以内。这是在Spoke3的路由表：

```
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. 在spoke和R1-HUB1之间的最新BGP会话断开，并且对端死机检测(DPD)去除在R1-HUB1被终止的IPSec隧道。然而，因为R2-HUB2已经使用作为主要隧道终止的网关，这不影响数据流转发：

```
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
```

配置

在此拓扑方面使用的此部分为集线器提供配置示例和spoke。

R1-HUB配置

```
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

```
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-Templatel 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-SPOKE1配置

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

```

R4-SPOKE2配置

```

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-Templatel 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

```

R5-AGGR1配置

```

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
```

R6-AGGR2配置

```
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
```

R7-HOST配置(主机的模拟在该网络的)

```
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

```

必需的配置附注

这是关于在前面的部分描述的配置的一些注意事项：

- 在两集线器之间的点到点GRE封装隧道对于spoke-to-spoke连接在所有情形是必需的工作，特别包括某些spoke仅被连接到其中一集线器和其他对另一台集线器的那些方案。
- 两集线器之间没有要求在从另一台集线器被派出的GRE隧道接口的bfd echo配置为了避免流量指示。Bfd echo有同样源和目的地IP地址，与路由器的IP地址是相等的发送Bfd echo。因为这些信息包由回应的路由器发送，NHRP数据流征兆生成。

- 在BGP配置中，通告往spoke的网络没有需要的路由映射过滤，但是它做配置更加最佳，因为聚合/仅汇总路由做通告：

```
neighbor SPOKES route-map AGGR out
```

- 在集线器上，**路由映射LOCALPREF** configurationis要求为了设置适当的BGP本地首选，并且过滤再分布的静态路由到仅汇总和IKEv2配置模式路由。

- 此设计不在远程办公室位置(分支)寻址冗余。如果在分支的广域网链路断开，VPN也不运作。

添加分支路由器的第二条链路或添加在同一个位置内的第二分支路由器为了解决此问题。

总之，在本文展示的冗余设计可以对待对Stateful Switchover (SSO) /Stateful功能的一个现代选择。它是高度灵活的，并且可以优化为了符合您的特定配置要求。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [Cisco IOS FlexVPN数据表或宣传单页](#)
- [配置对分支的FlexVPN分支](#)
- [技术支持和文档 - Cisco Systems](#)