FlexVPN HA デュアル ハブの設定例

内容

概要

このドキュメントでは、インターネットなどの安全でないネットワーク媒体上で IPsec ベースの VPN を介してデータセンターに接続する、リモート オフィス向けの完全な冗長性設計を設定する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のテクノロジー コンポーネントに基づいています。

- データセンター内および VPN オーバーレイのスポークとハブの間のルーティング プロトコルとしての Border Gateway Protocol（BGP）。
- データセンター内でのみ実行する（オーバーレイ トンネルでは実行しない）ダウン リンク（ルータ ダウン）を検出するメカニズムとしての双方向フォワーディング検出（BFD）。
- ショートカット スイッチングを使用してスポーク間機能が有効にされたハブとスポーク間の Cisco IOS® FlexVPN。
- スポークが異なるハブに接続されている場合でもスポーク間の通信を可能にするための 2 つのハブ間での Generic Routing Encapsulation（GRE）トンネリング。
- 拡張オブジェクト トラッキングおよび追跡されるオブジェクトに結び付けられたスタティック ルート。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

データセンター用のリモート アクセス ソリューションを設計する際、多くの場合、ミッション クリティカルなユーザ アプリケーションにとって、ハイ アベイラビリティ（HA）は重要な要件となります。

このドキュメントで説明するソリューションは、リロード、アップグレード、または電源の問題が原因で VPN 終端ハブの 1 つがダウンするという障害シナリオの早期検出と回復を可能にします。すべてのリモート オフィス ルータ（スポーク）は、このような障害が検出されるとすぐに、もう一方の稼働しているハブを使用します。

この設計の利点は次のとおりです。

- VPN ハブのダウン シナリオから迅速にネットワークを回復します。
- VPN ハブ間の複雑なステートフル同期（IPSec セキュリティ アソシエーション（SA）、Internet Security Association and Key Management Protocol（ISAKMP）SA、暗号ルーティングなど）がありません。
- IPSec ステートフル HA を使用した Encapsulating Security Payload（ESP）シーケンス番号の同期における遅延が原因となってアンチリプレイの問題が発生することはありません。
- VPN ハブで異なる IOS/IOS-XE ベースのハードウェアまたはソフトウェアを使用できます。
- VPN オーバーレイで実行するルーティング プロトコルとして BGP を使用する、柔軟なロード バランシングの実装を選択できます。
- バックグラウンドで実行する隠されたメカニズムがない、すべてのデバイスで読み取り可能な明確なルーティング。

- スポーク間の直接接続。
- 認証、許可、アカウンティング（AAA）統合やトンネルごとの Quality of Service（QoS）を含むすべての FlexVPN の利点を活用できます。

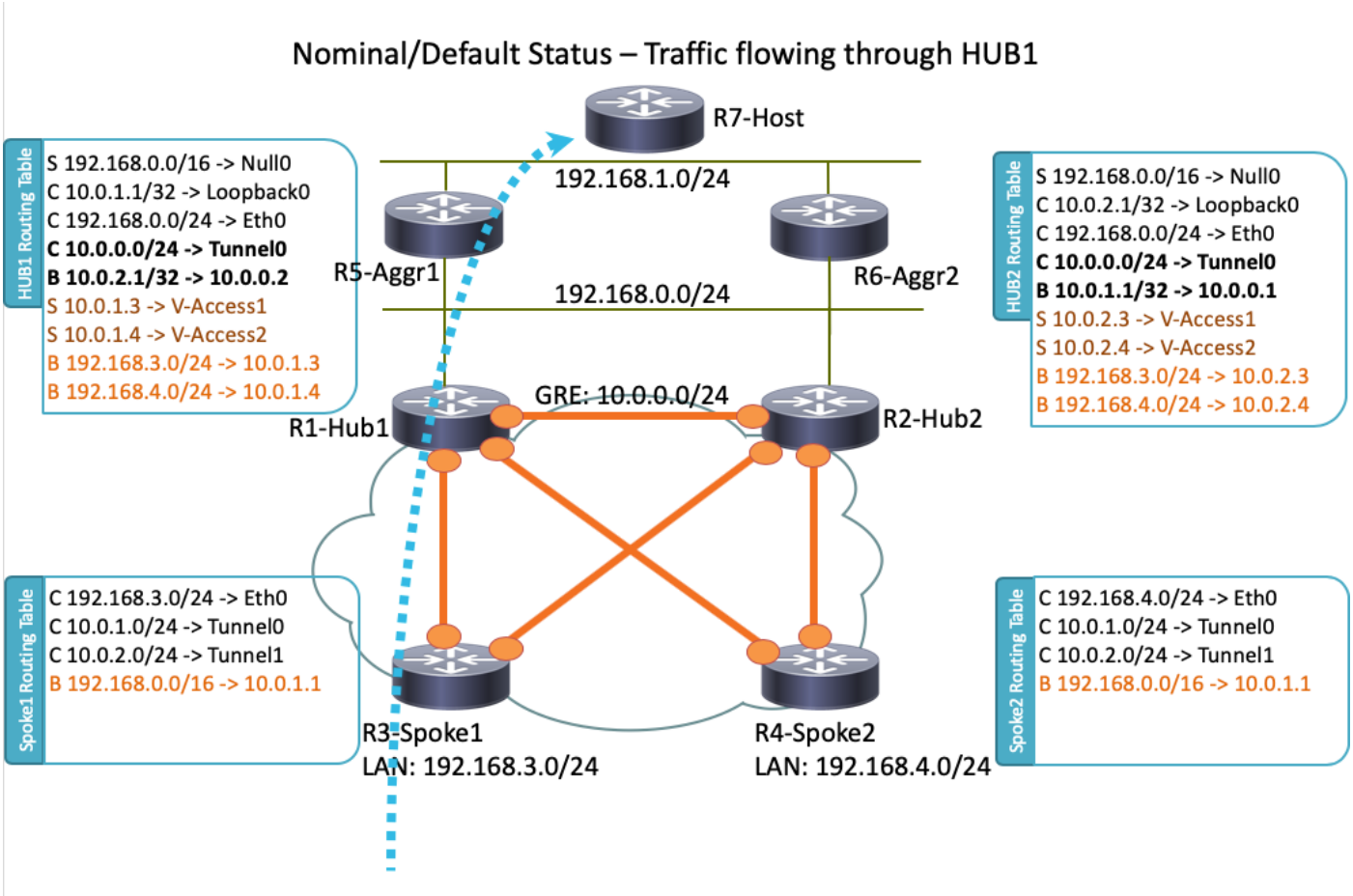
設定

このセクションでは、サンプルのシナリオを提供し、安全でないネットワーク媒体上で IPsec ベースの VPN を介してデータセンターに接続する、リモート オフィス向けの完全な冗長性設計を設定する方法について説明します。

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

以下は、このドキュメントで使用されるネットワーク図です。



> **注**：このトポロジで使用されているすべてのルータは、Cisco IOS バージョン 15.2(4)M1 で、インターネット クラウドは 172.16.0.0/24 のアドレス方式を使用します。

通常の運用シナリオ

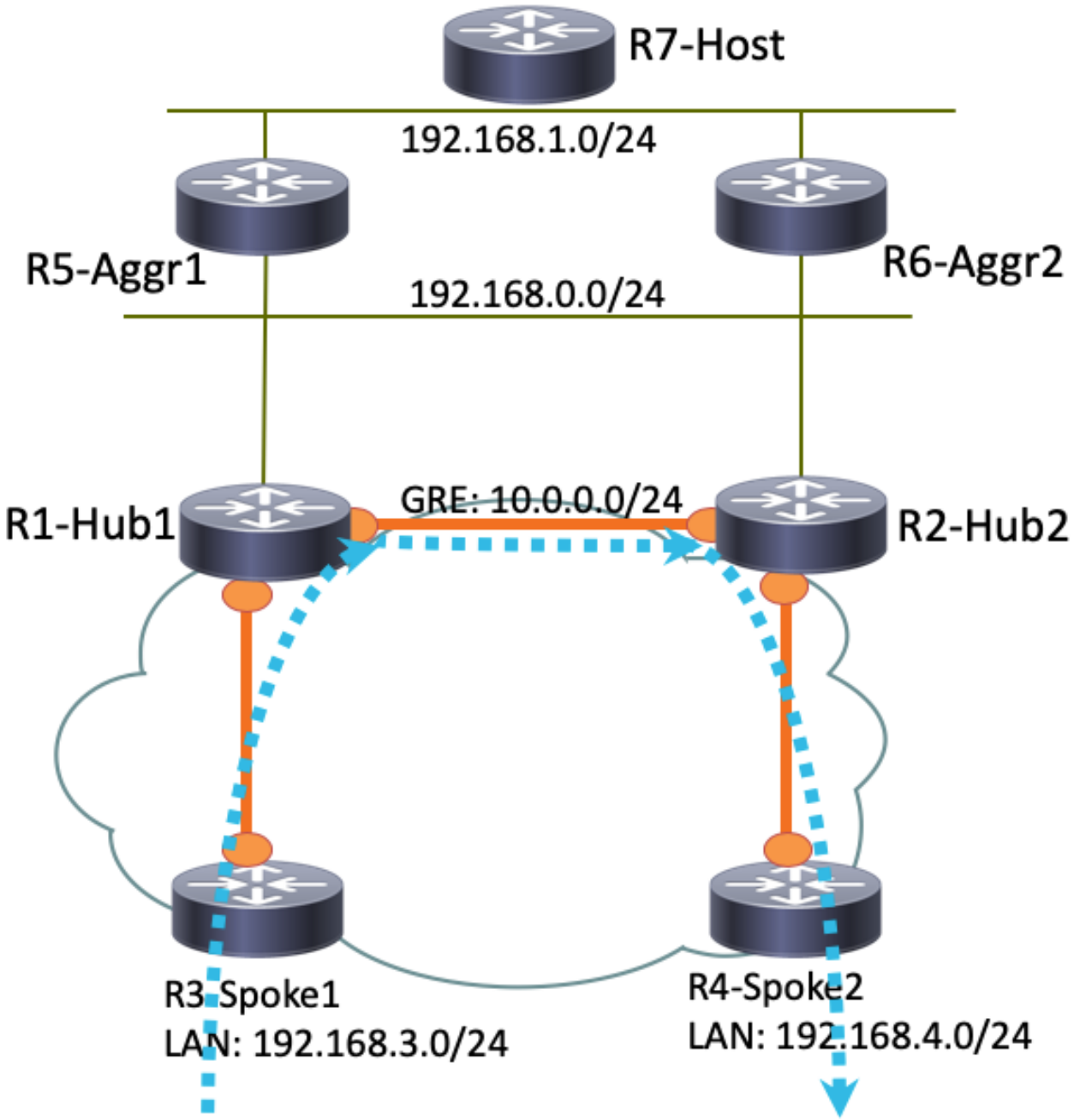
通常の運用シナリオでは、すべてのルータが稼働しているとき、すべてのスポーク ルータはデフォルトのハブ（R1-HUB1）を介してすべてのトラフィックをルーティングします。 このルーティング設定は、デフォルトのBGPローカルプリファレンスが200に設定されている場合に行われます（詳細については、以降のセクションを参照）。これは、トラフィックのロードバランシングなどの展開要件に基づいて調整できます。

スポーク間（ショートカット）

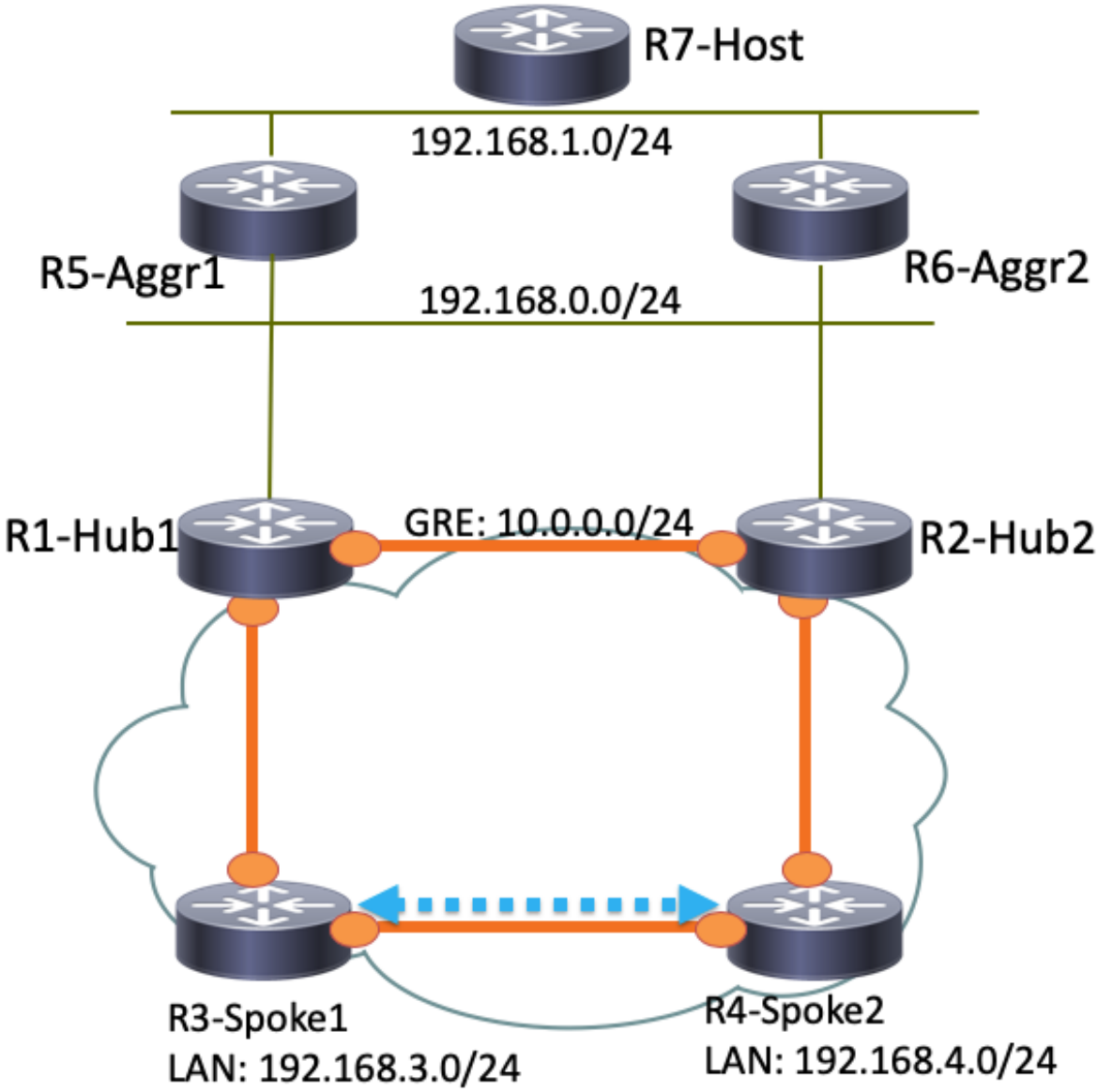
R3-Spoke1 が R4-Spoke2 への接続を開始すると、動的なスポーク間トンネルがショートカット スイッチング設定を使用して作成されます。

> **ヒント**：詳細については、「FlexVPN スポーク間の設定」設定ガイドを参照してください。

R3-Spoke1 を R1-HUB1 にのみ接続し、R4-Spoke2 を R2-HUB2 にのみ接続する場合、ハブ間で実行するポイントツーポイント GRE トンネルを使用したスポーク間の直接接続を実現できます。この場合、R3-Spoke1 と R4-Spoke2 の間の最初のトラフィック パスは次のようになります。



R1-Hub1は、GREトンネル上のものと同じNext Hop Resolution Protocol(NHRP)ネットワークIDを持つ仮想アクセスインターフェイス上のパケットを受信するため、Traffic IndicationがR3-Spoke1に送信されます。これにより、スポーク間ダイナミックトンネルの作成がされます。



通常の運用シナリオのルーティング テーブルと出力

通常の運用シナリオにおける R1-HUB1 ルーティング テーブルを次に示します。

```
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
```

R4-SPOKE2 を使用したスポーク間トンネルが作成された後の、通常の運用シナリオにおける R3-SPOKE1 ルーティング テーブルを次に示します。

```
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
```

R3-Spoke1 で、BGP テーブルに、異なるローカル設定を持つ 192.168.0.0/16 の 2 つのエントリが存在します（R1-Hub1 が優先）。

```
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
```

通常の運用シナリオにおける R5-AGGR1 ルーティング テーブルを次に示します。

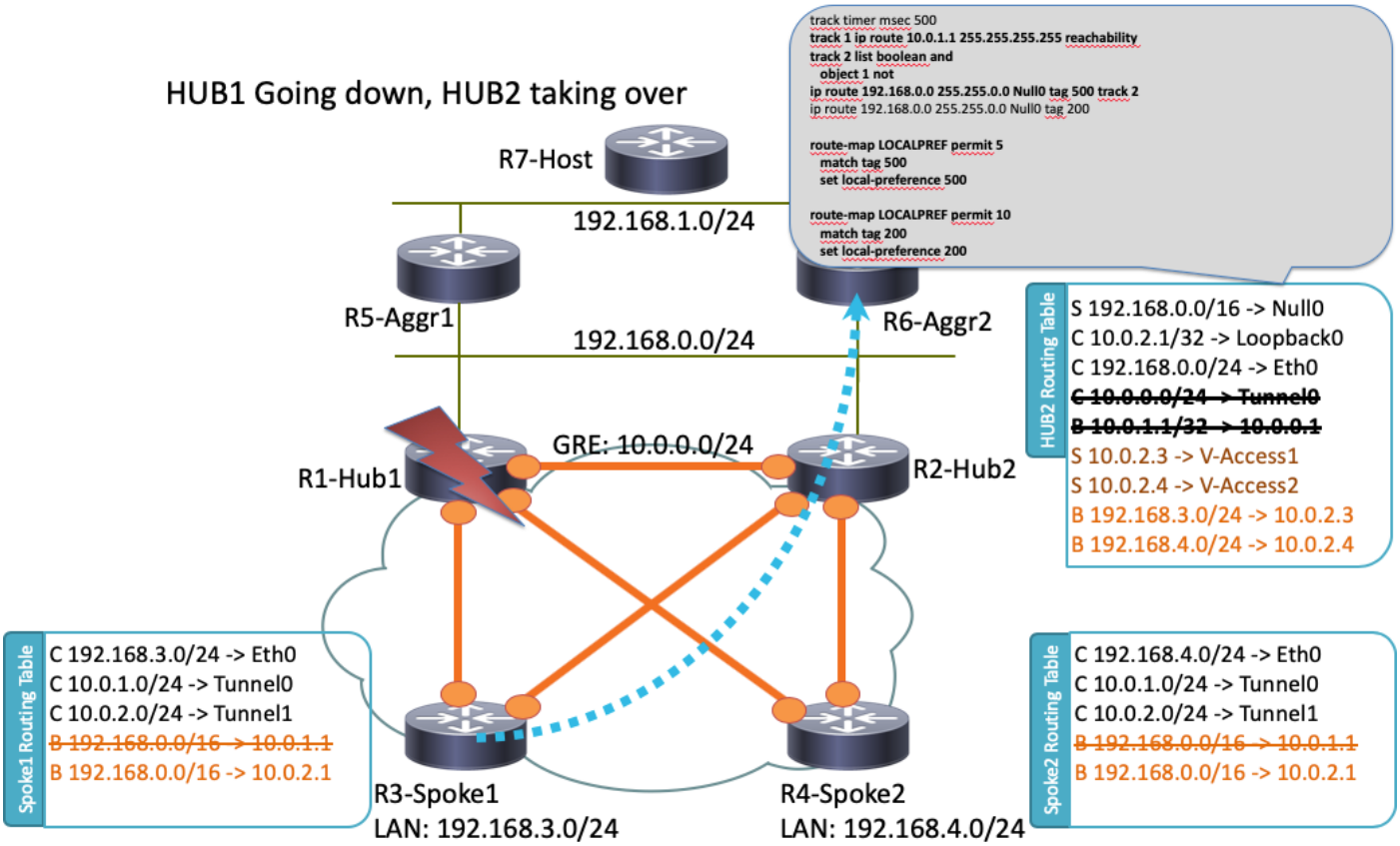
```
R5-LAN1#show ip route
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 192.168.0.1, 00:07:22
B        10.0.0.0/24 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.1/32 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.3/32 [200/0] via 192.168.0.1, 00:07:17
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
```

通常の運用シナリオにおける R7-HOST ルーティング テーブルを次に示します。

```
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 障害シナリオ

R1-HUB1 ダウン シナリオ (停電またはアップグレードなどの操作が原因) を次に示します。



このシナリオでは、次の一連のイベントが発生します。

1. R2-HUB2およびLAN集約ルータR5-AGGR1およびR6-AGGR2のBFDは、R1-HUB1のダウンステータスを検出します。その結果、BGPネイバーシップは即座にダウンします。

2. R1-HUB1 ループバックのプレゼンスを検出する R2-HUB2 の追跡対象検出がダウンします（設定例の Track 1）。

3. このダウンした追跡対象によって別の追跡がトリガーされます（論理 NOT）。 この例では、Track 1 がダウンすると、Track 2 が起動します。

4. これにより、デフォルトのアドミニストレーティブ ディスタンスよりも低い値であるため、スタティック IP ルーティング エントリのルーティング テーブルへの追加がトリガーされます。関連する設定を次に示します。

```
! 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は、R1-HUB1に設定された値よりも大きいBGPローカルプリファレンスを使用してこれらのスタティックルートを再配布します。この例では、R1-HUB1によって設定された**200ではなく、ローカルプリファレンス**500が障害シナリオで使用されます。

```
route-map LOCALPREF permit 5
```

```
 match tag 500
 set local-preference 500
!
route-map LOCALPREF permit 10
 match tag 200
 set local-preference 200
!
```

R3-Spoke1 では、BGP 出力でこれを確認できます。R1 へのエントリが存在しますが、使用されていないことに注意してください。

```
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. この時点で、両方のスポーク（R3-Spoke1とR4-Spoke2）がR2-HUB2へのトラフィックの送信を開始します。これらの手順はすべて1秒以内に実行される必要があります。Spoke 3 のルーティング テーブルを次に示します。

```
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. スポークとR1-HUB1間の後のBGPセッションがダウンし、Dead Peer Detection(DPD)によってR1-HUB1で終端されるIPSecトンネルが削除されます。ただし、R2-TERMINATING2はメイントンネルゲートウェイとして既使用されているため、トラフィック転送には影響しません。

```
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
```

設定

このセクションでは、このトポロジで使用されているハブとスポークの設定例を示します。

R1-HUB 設定

```
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 設定

```
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-SPOKE1 設定

```
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 設定

```
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 設定

```
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 設定

```
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 設定（そのネットワークでのホストのシミュレーション）

```
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
```

重要な設定に関する注意事項

前のセクションで説明した設定に関する重要な注意事項を次に示します。

- 2 つのハブの間のポイントツーポイント GRE トンネルは、スポーク間の接続をすべてのシナリオで機能させるために必要です。特に、あるスポークがハブの 1 つと接続され、別のスポークがもう 1 つのハブと接続されるシナリオでは重要となります。

- 2 つのハブの間の GRE トンネル インターフェイスにおける no bfd echo 設定が、別のハブから送信される Traffic Indication を回避するために必要となります。BFD エコーには、同じ送信元と宛先の IP アドレスがあります。これは、BFD エコーを送信するルータの IP アドレスと同じになります。これらのパケットが応答するルータによってルーティングされるため、NHRP Traffic Indication が生成されます。

- BGP 設定ではスポークにネットワークをアドバタイズするルート マップ フィルタリングは必須ではありませんが、集約/サマリー ルートのみがアドバタイズされるため、設定がより最適化されます。

  neighbor SPOKES route-map AGGR out
- ハブでは、適切なBGPローカルプリファレンスを設定するためにroute-map LOCALPREF設定が必要で、再配布されたスタティックルートを集約およびIKEv2コンフィギュレーションモードルートだけにフィルタします。

- この設計は、リモート オフィス ロケーション（スポーク）での冗長性は考慮されていません。 スポークの WAN リンクがダウンすると、VPN も機能しません。この問題に対処するには、2 番目のリンクをスポーク ルータに追加するか、同じロケーション内に 2 番目のスポーク ルータを追加します。

つまり、このドキュメントに記載されている冗長性の設計は、ステートフル スイッチオーバー（SSO）/ステートフル機能に対する最新の代替手段として扱うことができます。これは非常に柔軟で、特定の導入要件に合わせて微調整することができます。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco IOS FlexVPN データ シート
- FlexVPN スポーク間の設定
- テクニカル サポートとドキュメント – Cisco Systems