目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[ネットワーク図](#)
[規則的な操作上シナリオ](#)
[スポーク間（ショートカット）](#)
[規則的な操作上シナリオのためのルーティング テーブルおよび出力](#)
[HUB1 障害シナリオ](#)
[設定](#)
[R1-HUB 設定](#)
[R2-HUB2 設定](#)
[R3-SPOKE1 設定](#)
[R4-SPOKE2 設定](#)
[R5-AGGR1 設定](#)
[R6-AGGR2 設定](#)
[R7-HOST 設定（そのネットワークのホストのシミュレーション）](#)
[重要な設定に関する注記](#)
[確認](#)
[トラブルシューティング](#)
[関連情報](#)

概要

この資料に不確かなネットワークメディア上の IPSec ベース VPN によってデータセンタに接続するインターネットのようなリモートオフィスのための完全 な 冗長性 設計を設定する方法を記述されています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報はこれらの技術コンポーネントに基づいています:

- データセンタ内のおよび VPN オーバーレイのスポークとハブ間のルーティング プロトコルとして Border Gateway Protocol （ BGP ）。
- リンク（ルータ）の下でデータセンタだけのの中のその実行を検出する メカニズムとして双方向フォワーディング検出（ BFD ）（ないオーバーレイ トンネルに ）。
- ショートカット切り替えによって有効に されて スポーク間機能が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る時でさえスポーク間通信を有効に するために 2 つのハブの間でトンネル伝送する総称ルーティング カプセル化（ GRE ）。
- トラッキングされたオブジェクトに結ばれる拡張 な オブジェクト トラッキングおよびスタティック· 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

データセンタのためのリモートアクセス ソリューションを設計するとき、ハイ アベイラビリティ（ HA ）は頻繁にミッションクリティカル な ユーザアプリケ– ションのための重要 な 要件です。

ソリューションたどって行く VPN 終端 ハブのどれがリロード、アップグレード、または電力の問題が原因でをこので障害シナリオからの資料割り当てファースト検出およびリカバリ示される。 リモートオフィス ルータ（スポーク）全員はそのような失敗を検出次第他の操作上ハブをすぐに使用します。

この設計の長所はここにあります:

- VPN ハブ シナリオからのファースト ネットワーク リカバリ
- 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結合（ SA ）、Internet Security Association and Key Management Protocol（ ISAKMP ） SA、および暗号ルーティングのような ）
- IPSec ステートフル HA の Encapsulating Security Payload （ ESP ） シーケンス番号 同期の遅延による再生防止問題無し
- VPN ハブは別の Cisco IOS/IOS-XE によって基づくハードウェアかソフトウェアを使用できます
- VPN オーバーレイで動作するルーティング プロトコルとして BGP の適用範囲が広いロードバランシング 実装選択

- バックグラウンドで動作する非表示 メカニズム無しのすべてのデバイスのクリアおよび読解可能なルーティング
- 直接スポーク間 接続
- FlexVPN 長所すべて、認証、許可、アカウンティング（AAA）統合およびトンネルごとのQuality of Service（QoS）が含まれるため

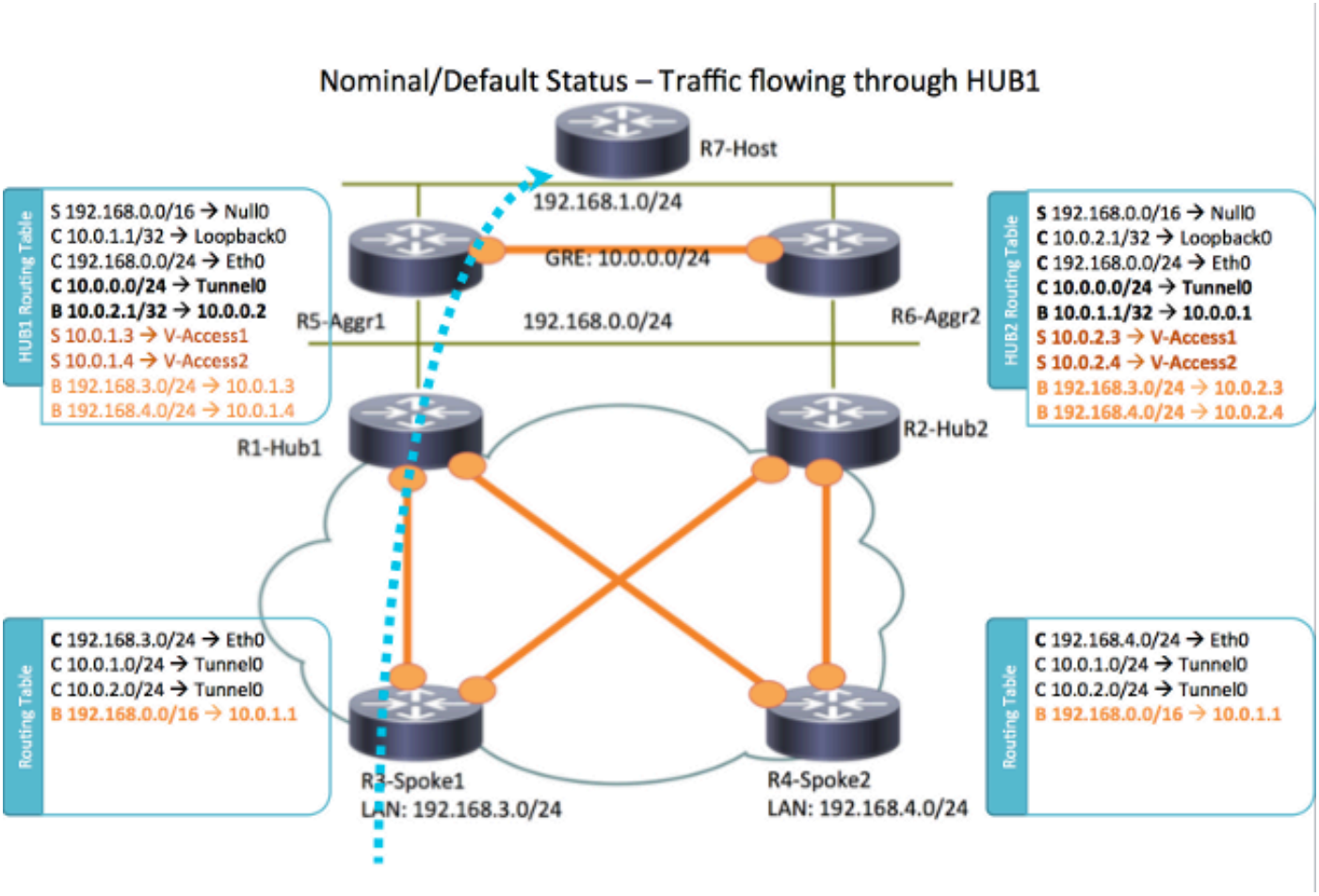
設定

このセクションはシナリオ例を提供し、不確かなネットワークメディア上の IPSec ベース VPN によってデータセンタに接続するリモートオフィスのための完全 な 冗長性 設計を設定する方法を記述します。

> **注** このセクションで使用されているコマンドの詳細を調べるには、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

これはこの資料で使用するネットワーク トポロジです:



> **注** このトポロジーで使用するルータ全員は Cisco IOSバージョン 15.2(4)M1、およびインタ

ーネット クラウドを使用します 172.16.0.0/24 のアドレス方式を実行します。

規則的な操作上シナリオ

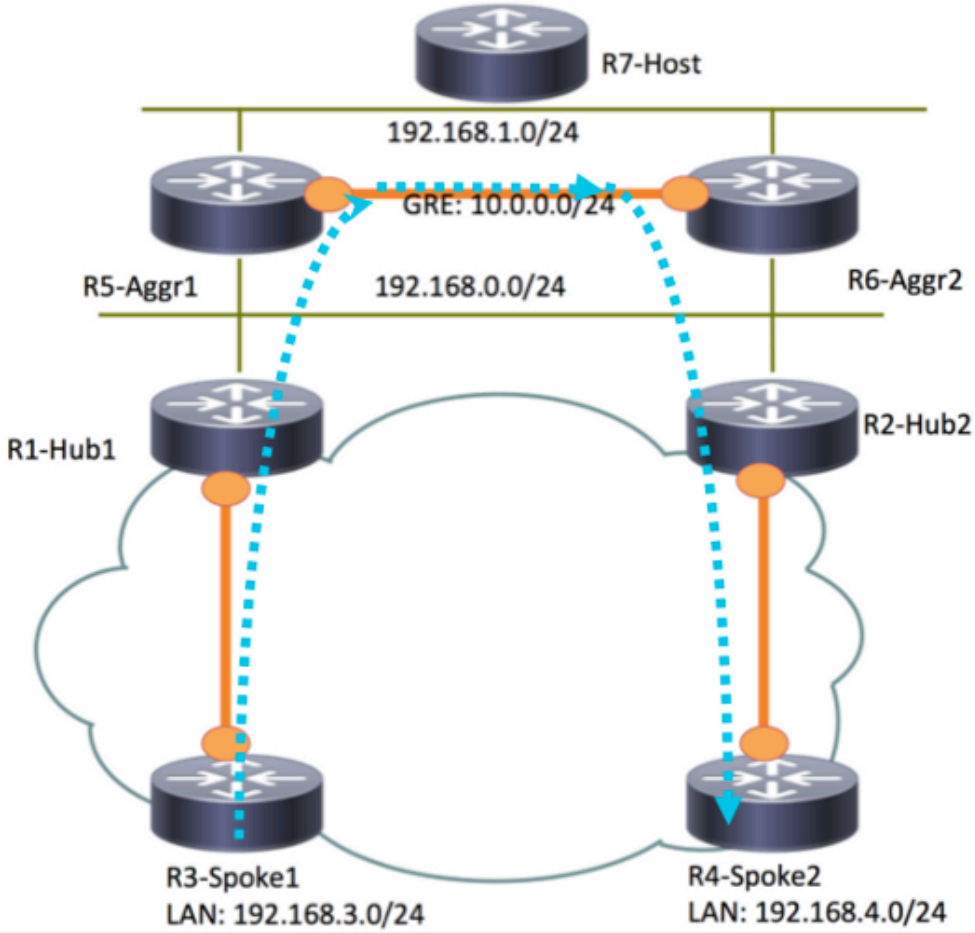
正常な操作上シナリオでは、ルータ全員がアップし、正常に動作しているとき、すべてのスポークルータはデフォルト ハブ（R1-HUB1）を通してトラフィックすべてをルーティングします。このルーティング プリファレンスはデフォルト BGP ローカルプリファレンスが 200 に設定 されるとき実現します（詳細については続く）セクションを参照して下さい。 これはトラフィック のロードバランシングのような配置の要件に基づいて、調節することができます。

スポーク間（ショートカット）

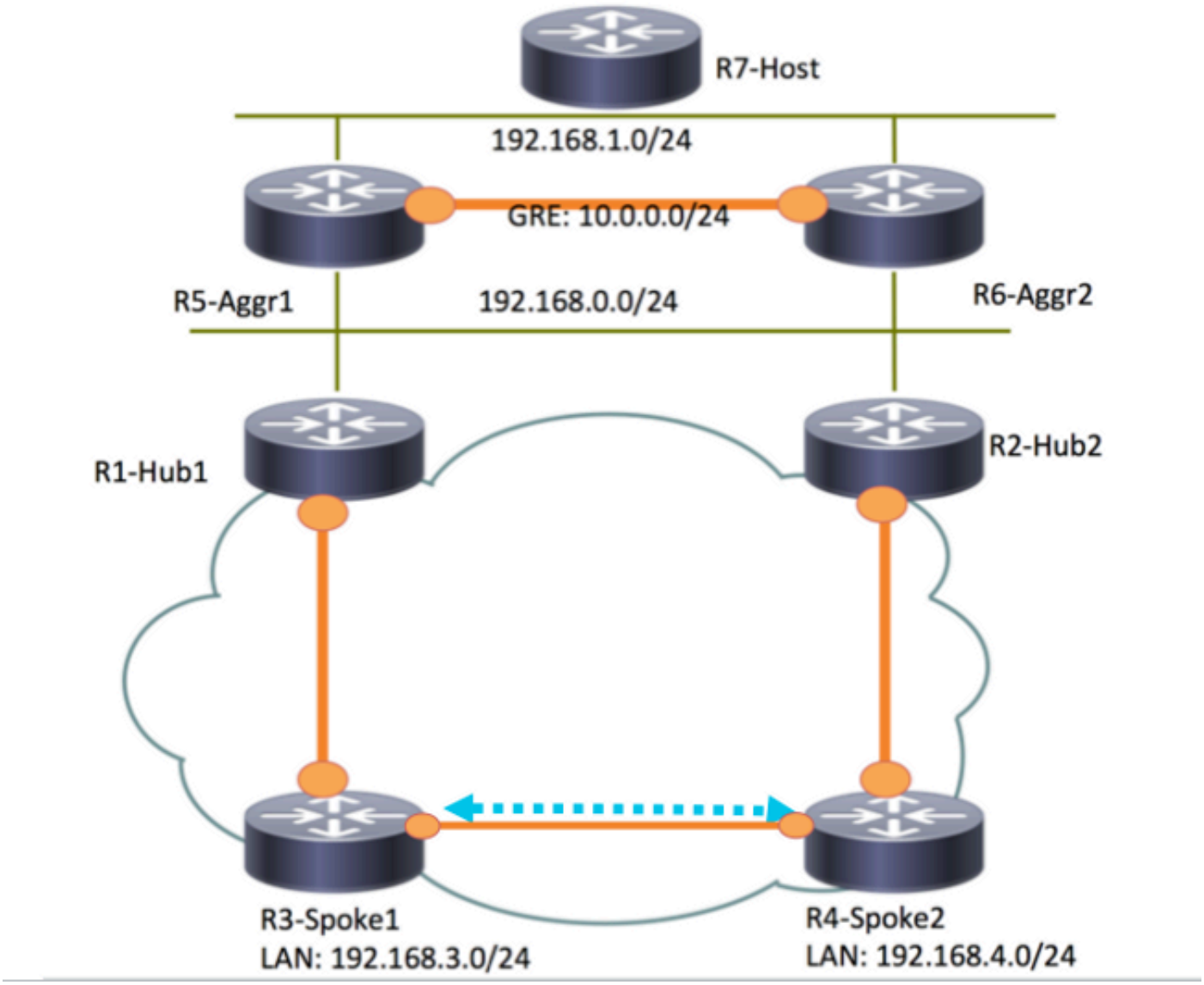
R3-Spoke1 が R4-Spoke2 への接続を開始する場合、ダイナミック スポーク間 トンネルはショートカット スイッチングの設定で作成されます。

> **ヒント**： 詳細については、設定 FlexVPN を話しましたスポーク設定 ガイドに参照して下さい。

R3-Spoke1 が R1-HUB1 にだけ接続され、R4-Spoke2 が R2-HUB2 にだけ接続されれば場合、ハブの間で動作するポイントツーポイント GREトンネルが付いている直接スポーク間接続を達成するまだことができます。 この場合、R3-Spoke1 間の最初のトラフィックパスおよび R4-Spoke2 はこれに類似したのようです:



R1-Hub1 がそれと GREトンネルの同じ Next Hop Resolution Protocol（NHRP） ネットワーク ID がある仮想アクセスインターフェイスのパケットを受信するので、トラフィック示す値は R3-Spoke1 の方に送信 されます。 これはスポーク間 ダイナミック トンネル作成を引き起こします:



規則的な操作上シナリオのためのルーティング テーブルおよび出力

規則的な操作上シナリオの R1-HUB1 ルーティング テーブルはここにあります:

```
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 のスポーク間 トンネルが作成された後規則的な操作上シナリオの R3-SPOKE1 ルーティング テーブルはここにあります:

```
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プリファレンスの 192.168.0.0/16 ネットワークのための 2 つのエントリがあります (R1-Hub1 は好まれます) :

```
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
```

規則的な操作上シナリオの R5-AGGR1 ルーティング テーブルはここにあります:

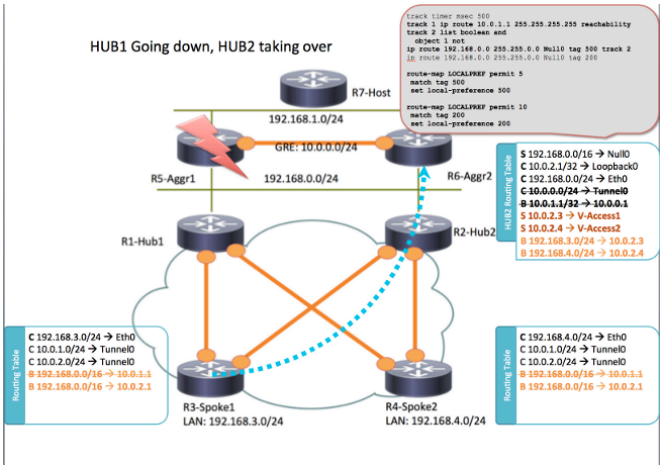
```
R5-LAN1#show ip route
     10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks
B        10.0.0.0/8 [200/0] via 192.168.0.1, 00:07:22
B        10.0.0.0/24 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.1/32 [200/0] via 192.168.0.1, 00:07:22
B        10.0.1.3/32 [200/0] via 192.168.0.1, 00:07:17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

規則的な操作上シナリオの R7-HOST ルーティング テーブルはここにあります:

```
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 シナリオはここにダウンしています (停電またはアップグレードのような操作による) :



このシナリオでは、この出来事の順序は実行されます:

1. R2-HUB2 と LAN 集約 ルータ R5-AGGR1 および R6-AGGR2 の BFD は R1-HUB1 のダウン ステータスを検出する。 その結果、BGP 隣接性はすぐにダウン状態になります。

2. R1-HUB1 ループバックの存在を検出する R2-HUB2 のためのトラック オブジェクト 検出は ダウン状態になります (設定例のトラック 1) 。

3. これは上がるためにダウンされたトラッキングされたオブジェクト別のトラックを引き起こします (論理的ない) 。 この例では、トラック 1 がダウン状態になる時はいつでもトラック 2 は上がります。

4. これはデフォルトの管理者距離より下部のである値によるルーティング テーブルに追加されるべき静的な IP ルーティングエントリを引き起こします。 関係のある構成はここにあります:
```
! 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 のために設定 される値より大きい BGP ローカルプリファレンスの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、500 のローカルプリファレンスは 200 の代りに R1-HUB1 によって設定 される 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、BGP 出力でこれを表示できます。 まだ存在 する R1 へのエントリ使用されないがことに注目して下さい:
```
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、スポークは両方とも (R3-Spoke1 および R4-Spoke2) R2-HUB2 にトラフィックを送信 し始めます。 これらのステップすべては 1秒以内に行われるはずです。 スポーク 3 のルーティング テーブルはここにあります:
```
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 間のより遅い BGPセッションはダウン状態になり、Dead Peer Detection （ DPD ）は R1-HUB1 で終わる IPSecトンネルを取除きます。 ただし、これは R2-HUB2 が主要なトンネル終端 ゲートウェイとして既に使用されているので、トラフィック転送に影響を与えません:

```
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

このトポロジーで使用するスポーク ハブにおよびこのセクションは設定 例を提供します。

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 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 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
```

R5-AGGR1 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
```

R6-AGGR2 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
```

R7-HOST 設定（そのネットワークのホストのシミュレーション）

```
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
```

重要な設定に関する注記

前のセクションに説明があるコンフィギュレーションについてのいくつかの注記はここにあります:

- スポーク間 接続がすべて の シナリオではたらくことができる、とりわけいくつかのスポークが別のハブへのハブの 1 つおよび他にだけ接続されるそれらのシナリオが含まれるためにように 2 つのハブ間のポイントツーポイント GREトンネルが必要となります。

- 2 つのハブ間の GREトンネル インターフェイスの **bfd エコー** 設定が別のハブから送信されるトラフィック示す値を避けるために必要となりません。 BFD エコーに同じ送信元 および宛先 IPアドレスがあります、BFD エコーを送信 する ルータの IP アドレスと等しい。 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ので、NHRP トラフィック示す値は生成されます。

- スポークの方のネットワークをアドバタイズする BGP設定では、集約/サマリールートだけアドバタイズされるのでルート マップ フィルタリングが、それ作成しますコンフィギュレーションを最適に必要となりませんが:
  neighbor SPOKES route-map AGGR out
- ハブで適切な BGP ローカルプリファレンスを設定するために、**ルート マップ LOCALPREF** 設定が必要となり概略だけおよび IKEv2 コンフィギュレーションモード ルーティングに再配布されたスタティック· ルートをフィルタリングします。

- この設計によってはリモートオフィス場所（スポーク）で冗長性が当たりません。 スポークの WAN リンクがダウン状態になる場合、VPN はまたはたらきません。 第 2 リンクをスポークルータに追加するか、またはこの問題に対処するために同じ位置内の第 2 スポークルータを追加して下さい。

要約すると、冗長性 設計は Stateful Switchover （SSO）/Stateful 機能への現代代替としてこの資料で示される扱うことができます。 それは非常に適用範囲が広く、特定の配置の要件を満たすために最適化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。

トラブルシューティング

現在のところ、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
- スポークへの FlexVPN スポークの設定
- テクニカルサポートとドキュメント - Cisco Systems