Configure and Troubleshoot FlexVPN Spoke to Spoke via EIGRP

Contents

Introduction

This document describes deploying and troubleshooting Cisco FlexVPN spoke-to-spoke using IKEv2 and NHRP for direct client crypto tunnels.

Prerequisites

- Flex VPN hub and Flex VPN client configuration

Requirements

Cisco recommends that you have knowledge of these topics:

- IKEv2
- Route-based VPN
- Virtual Tunnel Interfaces (VTI)
- NHRP
- IPSec
- EIGRP
- VRF-Lite

Components Used

The information in this document is based on:

- Cisco IOS XE 17.9.4a

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Scalability

FlexVPN can easily expand from small offices to large business networks. It can manage many VPN connections without needing a lot of extra work, which is great for organizations that are growing or have many remote users.

Key Features

- Dynamic Configuration and On-Demand Tunnels:
  - Virtual Tunnel Interfaces (VTI): FlexVPN uses VTIs that can be created and removed as needed. This means VPN tunnels are set up only when there is traffic and removed when not needed, saving resources and improving scalability.
  - Dynamic Routing Protocols: It works with routing protocols like OSPF, EIGRP, and BGP over VPN tunnels. This keeps routing information updated automatically, which is important for large and dynamic networks.
- Flexibility in Deployment:
  - Hub-and-Spoke Model: A central hub connects to multiple branch offices. FlexVPN simplifies setting up these connections with a single framework, making it ideal for large networks.
  - Full Mesh and Partial Mesh Topologies: All sites can communicate directly without going through a central hub, reducing delay and improving performance.
- High Availability and Redundancy:
  - Redundant Hubs: Supports multiple hubs for backup. If one hub fails, branches can connect to another hub, ensuring continuous connectivity.
  - Load Balancing: Distributes VPN connections across multiple devices to avoid any single device becoming overloaded, which is crucial for maintaining performance in large deployments.
- Scalable Authentication and Authorization:
  - AAA Integration: Works with AAA servers like Cisco ISE or RADIUS for centralized management of user credentials and policies, essential for large-scale use.
  - PKI and Certificates: Supports Public Key Infrastructure (PKI) and digital certificates for secure authentication, which is more scalable than using pre-shared keys, especially in large environments.

Background Information

FlexVPN and NHRP

The FlexVPN server provides the server-side functionality of FlexVPN. The FlexVPN client establishes a secure IPsec VPN tunnel between a FlexVPN client and another FlexVPN server.

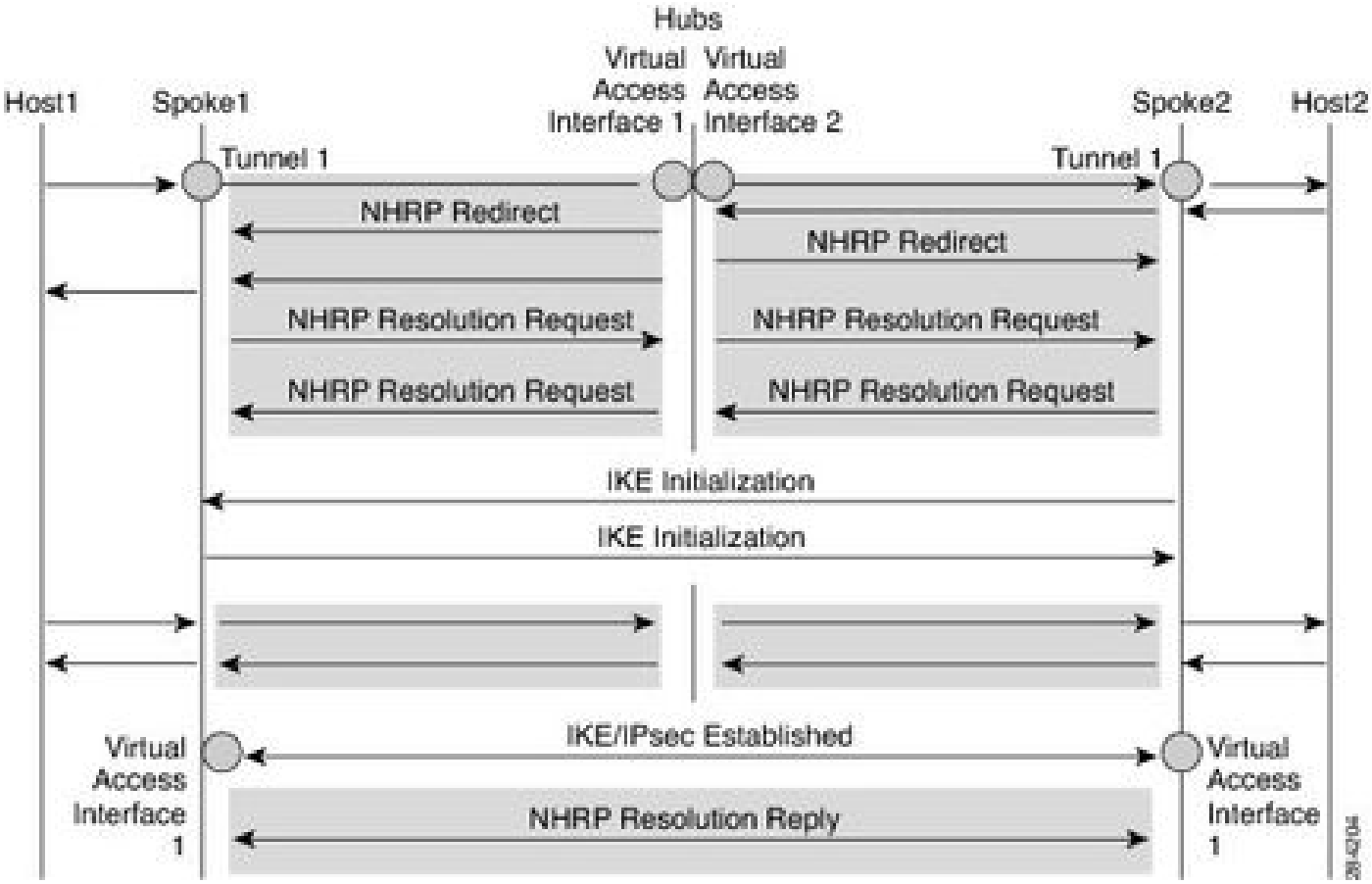
NHRP is an Address Resolution Protocol (ARP)-like protocol that alleviates nonbroadcast multiaccess (NBMA) network problems. With NHRP, NHRP entities attached to an NBMA network dynamically learn the NBMA address of the other entities that are part of that network, allowing these entities to directly communicate without requiring traffic to use an intermediate hop.

The FlexVPN Spoke to Spoke feature integrates NHRP and FlexVPN client (spoke) to establish a direct crypto channel with another client in an existing FlexVPN network. The connections are built using virtual tunnel interfaces (VTI), IKEv2, and NHRP, where NHRP is used for resolving the FlexVPN clients in the network.

Cisco recommends ensurig that:

- Routing entries are not exchanged between spokes. One key consideration, explained later as we progress to troubleshoot EIGRP-based topology.
- Different profiles are used for the spokes and the config-exchange command is not configured for the spokes.

NHRP Process

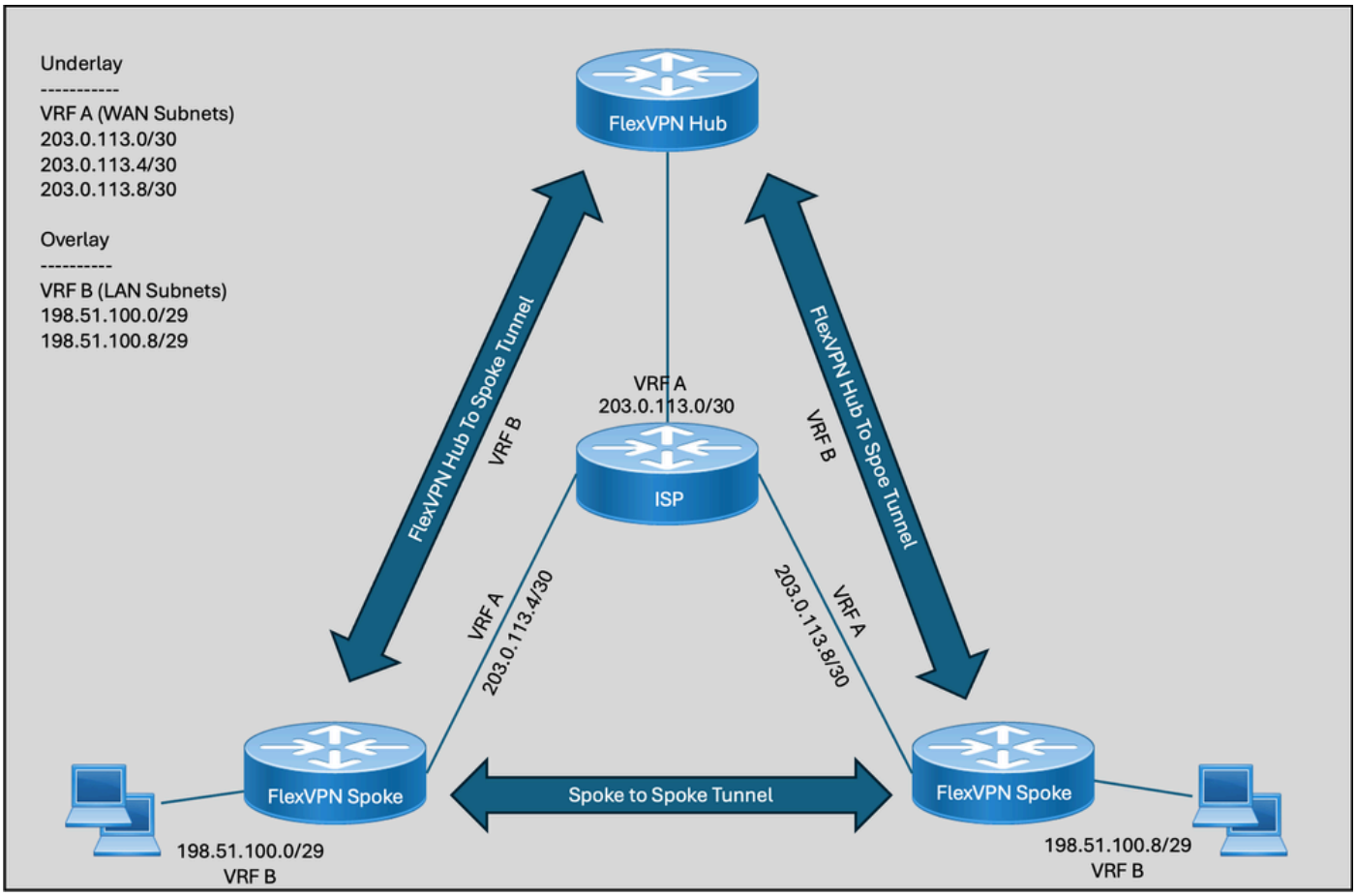


The illustration demonstrates the traffic flow between Spoke 1 and Spoke 2, with networks 198.51.100.0/29/24 and 198.51.100.8/29, both advertised through EIGRP peering directly to the spokes via the hub. Here is how the traffic flow looks like when communication is established between Spoke 1(198.51.100.0/29/24) and Spoke 2 (198.51.100.8/29).

1. Host1 sends traffic destined to Host2. Route-lookup at host 1 results in forwarding it to the hub tunnel interface because the hub is advertising that network via EIGRP.
2. When traffic reaches the hub, hub end route-lookup confirms that spoke 2 network 198.51.100.8/29 is learned via spoke 2 virtual-access.
3. Hub initiates NHRP redirect since both virtual-access interfaces (spoke 1 and spoke 2) are part of the same NHRP network having the same NHRP network ID.
4. On receiving the redirect, Spoke1 initiates a resolution request for the spoke 2 network over the tunnel interface (the same interface over which it received the redirect). Spoke 2 repeats the same process for the resolution request of the spoke 1 network.
5. Spoke2 receives the resolution request on the tunnel interface and retrieves the virtual template number as defined in the configuration. The virtual template number is used to create the virtual access interface to establish a crypto session between two spokes. Once the crypto SAs between the two spokes are up, both spokes install routes of next-hop IP address learned via IPSEC post establishment of virtual-access interfaces.
6. Both spokes then proceed to verify next-hop reachability before sending the resolution reply out via the newly created interface virtual-access for spoke-to-spoke connectivity.
7. Once the next hop is reachable, both spokes send a resolution reply to each other.
8. Both spokes can now override each of their network next-hop IP address for virtual-access via NHO.
9. Spoke1 installs the necessary cache entries for Spoke2's next-hop IP and its network. Spoke1 also deletes the temporary cache entry pointing to the hub to resolve the network under tunnel interface1.
10. The same step is repeated by spoke 2, it also installs cache entries for spoke 1 next-hop IP and its network moving forward in deleting the old hub entry via the tunnel.
11. NHRP adds shortcut routes as the next-hop override (NHO) or H (NHRP) route.

Configure FlexVPN Spoke to Spoke Using EIGRP

Topology Diagram



Key Considerations for EIGRP-Based Topology

Before proceeding towards configuration, there are some key concepts that we must understand:

- For any EIGRP deployment, if spokes are receiving a full routing table of other spokes or just summary routes, a prefix list needs to be installed on the hub side for outbound routing updates to filter tunnel IP addresses of spokes to be advertised into each other.

- The split horizon in EIGRP works differently than in IBGP. EIGRP only stops advertising networks out of an interface where they were learned from. For example, hub has two spokes one connected via virtual-access 1 and the other via virtual-access 2 interfaces. Routes learned by hub via VA 1 from Spoke 1 are advertised back to spoke 2 via VA 2 and vice versa since VA 1 and VA 2 are different interfaces. In the case of IBGP, it does not advertise any networks learned from its peer back to another peer. In a similar example, a hub configured with IBGP does not advertise back networks it learned from VA 1 to VA 2 and vice versa.

- This behavior in EIGRP creates a conflict in the CEF adjacency for the next hop IP address (an IP address of virtual-access interface for a spoke-to-spoke tunnel) since it is first learned via EIGRP using a hub tunnel interface and then via IPsec using a virtual-access interface. That causes asymmetric routing for NHRP traffic and also results in a duplicate NHRP entry in the NHRP table and duplicate NHO entries in the routing table as well for both next hop interfaces (tunnel via hub) and (virtual-access via spoke).

- Hub side virtual-template needs to have IP from a different pool than spokes tunnel interfaces since we want to filter outgoing EIGRP updates to make sure hub and spoke EIGRP peering is not affected.

Here are two examples showing how to configure FlexVPN spoke to spoke using EIGRP on the FlexVPN server and the FlexVPN client. We have followed best practices for segregating underlay and overlay traffic

by putting them both in specific VRFs. VRF A is for underlay while B is used for overlay.

Example 1 - Utilize NHO (Next-Hop-Override) For Spoke To Spoke Communication

FlexVPN Server

```
ip local pool FLEXPOOL 192.0.2.129 192.0.2.254

crypto ikev2 authorization policy CISCO_FLEX
 pool FLEXPOOL
 def-domain cisco.com
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Loopback0
 ip vrf forwarding B
 ip address 192.0.2.1 255.255.255.255

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.2 255.255.255.252

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

ip prefix-list CISCO_PREFIX seq 5 deny 192.0.2.128/25 le 32
ip prefix-list CISCO_PREFIX seq 6 permit 0.0.0.0/0 le 32

router eigrp B
```

```
!
address-family ipv4 unicast vrf B autonomous-system 1
!
af-interface default
hello-interval 2
hold-time 10
exit-af-interface
!
topology base
distribute-list prefix CISCO_PREFIX out
exit-af-topology
network 192.0.2.128 0.0.0.127
network 192.0.2.1 0.0.0.0
exit-address-family
```

FlexVPN Client 1

```
ip host vrf A hub.cisco.com 203.0.113.2

crypto ikev2 authorization policy CISCO_FLEX
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 client flexvpn CISCO_CLIENT
 peer 1 fqdn hub.cisco.com dynamic
 client connect Tunnel1

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Tunnel1
 ip vrf forwarding B
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
```

```
 tunnel destination dynamic
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF
end

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.6 255.255.255.252

interface Loopback1
 ip vrf forwarding B
 ip address 198.51.100.1 255.255.255.248

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Tunnel1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

router eigrp B
 address-family ipv4 unicast vrf B autonomous-system 1

 af-interface default
  hello-interval 2
  hold-time 10
  passive-interface
 exit-af-interface

 af-interface Tunnel1
  no passive-interface
 exit-af-interface

  topology base
  exit-af-topology
  network 198.51.100.0 0.0.0.7
  network 192.0.2.128 0.0.0.127
 exit-address-family
```

FlexVPN Client 2

```
ip host vrf A hub.cisco.com 203.0.113.2

crypto ikev2 authorization policy CISCO_FLEX
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 client flexvpn CISCO_CLIENT
 peer 1 fqdn hub.cisco.com dynamic
```

```
 client connect Tunnel1

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Tunnel1
 ip vrf forwarding B
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination dynamic
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF
end

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.10 255.255.255.252

interface Loopback1
 ip vrf forwarding B
 ip address 198.51.100.9 255.255.255.248

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Tunnel1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

router eigrp B
 address-family ipv4 unicast vrf B autonomous-system 1

 af-interface default
  hello-interval 2
  hold-time 10
  passive-interface
 exit-af-interface

 af-interface Tunnel1
  no passive-interface
 exit-af-interface

  topology base
  exit-af-topology
  network 198.51.100.8 0.0.0.7
```

```
  network 192.0.2.128 0.0.0.127
 exit-address-family
```

Example 2 - Utilize NHRP Installed Routes For Spoke To Spoke Communication

FlexVPN Server

The only change in the EIGRP configuration is to introduce summary routes instead of full routing table on spokes. Please make sure to bring virtual-template down to push the summary configuration into the EIGRP topology. Please refer to Cisco bug ID CSCwn84303.

```
router eigrp B
!
address-family ipv4 unicast vrf B autonomous-system 1
!
af-interface default
hello-interval 2
hold-time 10
exit-af-interface
!
af-interface Virtual-Template1
summary-address 198.51.100.0 255.255.255.0 <<<<<<<<<<< Summary address
exit-af-interface
!
topology base
distribute-list prefix CISCO_PREFIX out
exit-af-topology
network 192.0.2.128 0.0.0.127
network 192.0.2.1 0.0.0.0
exit-address-family
```

Verification and Troubleshooting

Example 1 - Utilize NHO (Next-Hop-Override) For Spoke To Spoke Communication

Spoke 1 (Before Spoke to Spoke NHRP Resolution & Tunnel Establishment)

```
Spoke1#show ip route vrf B

Routing Table: B
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 2 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.130 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
D        198.51.100.8/29 [90/102451840] via 192.0.2.1, 00:01:46
```

Spoke 2 (Before Spoke to Spoke NHRP Resolution & Tunnel Establishment)

```
Spoke2#show ip route vrf B

Routing Table: B
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 2 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.129 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
D        198.51.100.0/29 [90/102451840] via 192.0.2.1, 00:04:01
C        198.51.100.8/29 is directly connected, Loopback1
L        198.51.100.9/32 is directly connected, Loopback1
Spoke2#
```

Spoke 1 (After Spoke to Spoke NHRP Resolution & Tunnel Establishment)

Initiate ICMP to trigger spoke-to-spoke tunnel:

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 111/111/111 ms
```

Verify NHRP shortcut:

```
Spoke1#show ip nhrp vrf B detail
192.0.2.129/32 via 192.0.2.129
   Virtual-Access1 created 00:00:18, expire 00:09:41
   Type: dynamic, Flags: router nhop rib nho
   NBMA address: 203.0.113.10
   Preference: 255
198.51.100.8/29 via 192.0.2.129
   Virtual-Access1 created 00:00:17, expire 00:09:41
   Type: dynamic, Flags: router rib nho
   NBMA address: 203.0.113.10
   Preference: 255
```

Verify NHO routes post shortcut creation:

```
Spoke1#show ip route vrf B next-hop-override

Routing Table: B
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
S   %    192.0.2.129 is directly connected, Virtual-Access1
                     [NHO][1/255] via 192.0.2.129, Virtual-Access1
C        192.0.2.130 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
D   %    198.51.100.8/29 [90/102451840] via 192.0.2.1, 00:07:13
                         [NHO][90/255] via 192.0.2.129, 00:00:45, Virtual-Access1
```

Verify NHRP counters:

```
Spoke1#show ip nhrp traffic
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 2
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 3
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  1 Traffic Indication  0 Redirect Suppress
Virtual-Access1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 3
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         2 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 1
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
Virtual-Template1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

Spoke 2 (After Spoke to Spoke NHRP Resolution & Tunnel Establishment)

Verify NHRP shortcut:

```
Spoke2#show ip nhrp vrf B detail
192.0.2.130/32 via 192.0.2.130
   Virtual-Access1 created 00:04:42, expire 00:05:18
   Type: dynamic, Flags: router nhop rib nho
   NBMA address: 203.0.113.6
   Preference: 255
198.51.100.0/29 via 192.0.2.130
   Virtual-Access1 created 00:04:40, expire 00:05:18
   Type: dynamic, Flags: router rib nho
   NBMA address: 203.0.113.6
   Preference: 255
```

Verify NHO routes post shortcut creation:

```
Spoke2# show ip route vrf B next-hop-override

Routing Table: B
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.129 is directly connected, Tunnel1
S   %    192.0.2.130 is directly connected, Virtual-Access1
                     [NHO][1/255] via 192.0.2.130, Virtual-Access1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
D   %    198.51.100.0/29 [90/102451840] via 192.0.2.1, 00:11:20
                         [NHO][90/255] via 192.0.2.130, 00:04:52, Virtual-Access1
C        198.51.100.8/29 is directly connected, Loopback1
L        198.51.100.9/32 is directly connected, Loopback1
```

Verify NHRP counters:

```
Spoke2#show ip nhrp traffic
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 2
         2 Resolution Request   0 Resolution Reply   0 Registration Request
         0 Registration Reply   0 Purge Request   0 Purge Reply
         0 Error Indication   0 Traffic Indication   0 Redirect Suppress
   Rcvd: Total 3
         2 Resolution Request   0 Resolution Reply   0 Registration Request
         0 Registration Reply   0 Purge Request   0 Purge Reply
         0 Error Indication   1 Traffic Indication   0 Redirect Suppress
Virtual-Access1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 3
         0 Resolution Request   1 Resolution Reply   0 Registration Request
         0 Registration Reply   0 Purge Request   0 Purge Reply
         2 Error Indication   0 Traffic Indication   0 Redirect Suppress
   Rcvd: Total 1
         0 Resolution Request   1 Resolution Reply   0 Registration Request
         0 Registration Reply   0 Purge Request   0 Purge Reply
         0 Error Indication   0 Traffic Indication   0 Redirect Suppress
Virtual-Template1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request   0 Resolution Reply   0 Registration Request
         0 Registration Reply   0 Purge Request   0 Purge Reply
         0 Error Indication   0 Traffic Indication   0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request   0 Resolution Reply   0 Registration Request
         0 Registration Reply   0 Purge Request   0 Purge Reply
         0 Error Indication   0 Traffic Indication   0 Redirect Suppress
```

Here is a step-by-step explanation of how a direct spoke-to-spoke tunnel is established with the help of debugs from one of the spokes.

- Spoke 1 initiated ICMP:

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 111/111/111 ms
```

- Hub received ICMP and initiated redirect (Traffic indication) to both spokes:

```
*Feb 3 16:15:35.280: NHRP: Receive Traffic Indication via Tunnel1 vrf: B(0x4), packet size: 104
.
*Feb 3 16:15:35.280: (M) traffic code: redirect(0)
*Feb 3 16:15:35.280: src NBMA: 203.0.113.2
*Feb 3 16:15:35.280: src protocol: 192.0.2.1, dst protocol: 198.51.100.1
.
*Feb 3 16:15:35.281: NHRP-DETAIL: NHRP traffic indication for afn 1 received on interface Tunnel1 , for
```

- Both spokes triggered a resolution request which went through tunnel1:

```
*Feb 3 16:15:35.295: NHRP: Sending NHRP Resolution Request for dest: 198.51.100.9 to nexthop: 198.51.10
*Feb 3 16:15:35.295: NHRP: Attempting to send packet through interface Tunnel1 via DEST dst 198.51.100.
*Feb 3 16:15:35.295: NHRP-DETAIL: First hop route lookup for 198.51.100.9 yielded 192.0.2.1, Tunnel1
*Feb 3 16:15:35.295: NHRP: Send Resolution Request via Tunnel1 vrf: B(0x4), packet size: 72
*Feb 3 16:15:35.295: src: 192.0.2.130, dst: 198.51.100.9
.
*Feb 3 16:15:35.296: src NBMA: 203.0.113.6
*Feb 3 16:15:35.296: src protocol: 192.0.2.130, dst protocol: 198.51.100.9
```

- Both spokes received a resolution request via Tunnel1:

```
*Feb 3 16:15:35.392: NHRP: Receive Resolution Request via Tunnel1 vrf: B(0x4), packet size: 92
.
*Feb 3 16:15:35.392: src NBMA: 203.0.113.10
*Feb 3 16:15:35.392: src protocol: 192.0.2.129, dst protocol: 198.51.100.1
*Feb 3 16:15:35.392: (C-1) code: no error(0), flags: none
.
*Feb 3 16:15:35.392: NHRP-DETAIL: Resolution request for afn 1 received on interface Tunnel1 , for vrf:
```

- Both spokes performed route-lookup for their local networks 198.51.100.0/29/24 and 198.51.100.8/29:

```
*Feb 3 16:15:35.392: NHRP-DETAIL: Multipath IP route lookup for 198.51.100.1 in vrf: B(0x4) yielded Loo
*Feb 3 16:15:35.392: NHRP: Route lookup for destination 198.51.100.1 in vrf: B(0x4) yielded interface L
.
*Feb 3 16:15:35.392: NHRP: We are egress router. Process the NHRP Resolution Request.
.
*Feb 3 16:15:35.393: NHRP-DETAIL: Multipath IP route lookup for 198.51.100.1 in vrf: B(0x4) yielded Loo
*Feb 3 16:15:35.393: NHRP: nhrp_rtlookup for 198.51.100.1 in vrf: B(0x4) yielded interface Loopback1, p
*Feb 3 16:15:35.393: NHRP-DETAIL: netid_out 0, netid_in 1
*Feb 3 16:15:35.393: NHRP: We are egress router for target 198.51.100.1, recevied via Tunnel1 vrf: B(0x
```

- Resolution reply got enqueued and IPsec establishment got started since both spokes are now aware of each others NBMA addresses:

```
*Feb 3 16:15:35.393: NHRP: Checking for delayed event 192.0.2.129/198.51.100.1 on list (Tunnel1 vrf: B(
*Feb 3 16:15:35.393: NHRP: No delayed event node found.
*Feb 3 16:15:35.394: NHRP-DETAIL: Updated delayed event with ep src:203.0.113.6 dst:203.0.113.10 ivrf:B
*Feb 3 16:15:35.394: NHRP: Enqueued Delaying resolution request nbma src:203.0.113.6 nbma dst:203.0.113
*Feb 3 16:15:35.394: NHRP: Interface: Tunnel1 configured with FlexVPN. Deferring cache creation for nho
*Feb 3 16:15:35.406: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
*Feb 3 16:15:35.456: NHRP: Virtual-Access1: Tunnel mode changed from
'Uninitialized tunnel mode' to 'GRE over point to point IPV4 tunnel mode'
*Feb 3 16:15:35.456: NHRP: Virtual-Access1: NHRP not enabled in delay_if_up
*Feb 3 16:15:35.511: NHRP: Registration with Tunnels Decap Module succeeded
```

```
*Feb 3 16:15:35.511: NHRP: Rejecting addr type 1
*Feb 3 16:15:35.511: NHRP: Adding all static maps to cache
*Feb 3 16:15:35.511: NHRP-DETAIL: Adding summary-prefix entry: nhrp router block not configured
*Feb 3 16:15:35.512: NHRP:
*Feb 3 16:15:35.512: Instructing NHRP to create Virtual-Access from Virtual template 1 for interface Vi
*Feb 3 16:15:35.537: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
*Feb 3 16:15:35.539: NHRP-CACHE: Virtual-Access1: Cache add for target 192.0.2.130/32 vrf: B(0x4) label
*Feb 3 16:15:35.540: 203.0.113.6 (flags:0x20)
.
*Feb 3 16:15:35.548: NHRP: Updating delayed event with destination 203.0.113.10 on interfaceTunnel1 wit
*Feb 3 16:15:35.788: NHRP:
*Feb 3 16:15:35.788: Fetched address from underlying IKEv2 for interfaceVirtual-Access1. Pre-NATed = 20
*Feb 3 16:15:35.788: %DMVPN-5-CRYPTO_SS: Virtual-Access1: local address : 203.0.113.6 remote address :
```

- During IPSEC establishment and NHRP shortcut creation process, both spokes learnt and installed each others tunnel ip addresses in their routing table as IPSEC route and probed next hop reachability:

```
*Feb 3 16:15:35.788: NHRP: Processing delayed event on interface Tunnel1 with NBMA 203.0.113.10
.
*Feb 3 16:15:35.789: NHRP-CACHE: Virtual-Access1: Cache add for target 192.0.2.129/32 vrf: B(0x4) label
*Feb 3 16:15:35.789: 203.0.113.10 (flags:0x2080)
*Feb 3 16:15:35.789: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.791: NHRP-RT: Route addition to RIB Successful
*Feb 3 16:15:35.791: NHRP-EVE: NHP-UP: 192.0.2.129, NBMA: 203.0.113.10
*Feb 3 16:15:35.791: %DMVPN-5-NHRP_NHP_UP: Virtual-Access1: Next Hop NHP : (Tunnel: 192.0.2.129 NBMA: 2
*Feb 3 16:15:35.791: NHRP-CACHE:
*Feb 3 16:15:35.791: Next-hop not reachable for 192.0.2.129
*Feb 3 16:15:35.791: %NHRP-5-NHOP_UNREACHABLE: Nexthop address 192.0.2.129 for 192.0.2.129/32 is not ro
```

- Until completion of shortcut installation and NHO, spoke A performed the next hop lookup of virtual-access IP addresses of spoke B and vice versa but the next hope lookup returned "yielded N/A" due to which spoke A sent an error indication to spoke B confirming next hop is unreachable. The particular lookup can be referred to as a multi-path lookup:

```
*Feb 3 16:15:35.791: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:15:35.791: NHRP: Sending error indication. Reason: 'Cache pak failure' LINE: 13798
*Feb 3 16:15:35.791: NHRP: Attempting to send packet through interface Virtual-Access1 via DEST dst 192
*Feb 3 16:15:35.791: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:15:35.791: NHRP: Send Error Indication via Virtual-Access1 vrf: B(0x4), packet size: 132
*Feb 3 16:15:35.791: src: 192.0.2.130, dst: 192.0.2.129
.
*Feb 3 16:15:35.791: (M) error code: protocol address unreachable(6), offset: 0
*Feb 3 16:15:35.791: src NBMA: 203.0.113.6
*Feb 3 16:15:35.791: src protocol: 192.0.2.130, dst protocol: 192.0.2.129
```

- Once NHO kicked in for the next hop and the shortcut was created, both spokes sent out resolution requests for each of their networks again:

```
*Feb 3 16:15:35.813: NHRP: No need to delay processing of resolution event nbma src:203.0.113.6 nbma ds
*Feb 3 16:15:35.813: NHRP-CACHE: Virtual-Access1: Cache update for target 192.0.2.129/32 vrf: B(0x4) la
```

```
*Feb 3 16:15:35.813: 203.0.113.10 (flags:0x2280)
*Feb 3 16:15:35.813: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.814: NHRP-RT: Route addition to RIB Successful
.
*Feb 3 16:15:35.841: NHRP-RT: Route entry 192.0.2.129/32 via 192.0.2.129 (Vi1) clobbered by distance
*Feb 3 16:15:35.847: NHRP-RT: Unable to stop route watch for 192.0.2.129/32 interface Virtual-Access1 .
*Feb 3 16:15:35.847: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.847: NHRP-RT: Route addition failed (admin-distance)
*Feb 3 16:15:35.847: NHRP-RT: nexthop-override added to RIB
.
*Feb 3 16:15:37.167: NHRP: Sending NHRP Resolution Request for dest: 198.51.100.9 to nexthop: 198.51.10
*Feb 3 16:15:37.167: NHRP: Attempting to send packet through interface Tunnel1 via DEST dst 198.51.100.
*Feb 3 16:15:37.167: NHRP-DETAIL: First hop route lookup for 198.51.100.9 yielded 192.0.2.1, Tunnel1
*Feb 3 16:15:37.167: NHRP: Send Resolution Request via Tunnel1 vrf: B(0x4), packet size: 72
*Feb 3 16:15:37.167: src: 192.0.2.130, dst: 198.51.100.9
.
*Feb 3 16:15:37.167: src NBMA: 203.0.113.6
*Feb 3 16:15:37.167: src protocol: 192.0.2.130, dst protocol: 198.51.100.9
```

- Once both spokes received resolution requests for each of their networks, NHO replaced the EIGRP route via Tunnel (HUB) with virtual-access:

```
*Feb 3 16:30:57.768: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) labe
*Feb 3 16:30:57.768: 203.0.113.10 (flags:0x1000)
*Feb 3 16:30:57.768: NHRP-RT: Adding route entry for 198.51.100.8/29 via 192.0.2.129, Virtual-Access1 v
*Feb 3 16:30:57.769: NHRP-RT: Route addition failed (admin-distance)
*Feb 3 16:30:57.769: NHRP-RT: nexthop-override added to RIB
*Feb 3 16:30:57.769: NHRP-EVE: NHP-UP: 192.0.2.129, NBMA: 203.0.113.10
*Feb 3 16:30:57.769: %DMVPN-5-NHRP_NHP_UP: Virtual-Access1: Next Hop NHP : (Tunnel: 192.0.2.129 NBMA: 2
*Feb 3 16:30:57.769: NHRP-CACHE: Deleting incomplete entry for 198.51.100.9/32 interface Tunnel1 vrf: B
*Feb 3 16:30:57.769: NHRP-EVE: NHP-DOWN: 198.51.100.9, NBMA: 198.51.100.9
```

- Afterward, both spokes send a resolution reply out via the virtual-access interface:

```
*Feb 3 16:30:57.436: NHRP-CACHE: Virtual-Access1: Internal Cache add for target 198.51.100.0/29 vrf: B(
*Feb 3 16:30:57.436: 203.0.113.6 (flags:0x20)
*Feb 3 16:30:57.436: NHRP: Attempting to send packet through interface Virtual-Access1 via DEST dst 192
*Feb 3 16:30:57.436: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:30:57.436: NHRP: Send Resolution Reply via Virtual-Access1 vrf: B(0x4), packet size: 120
*Feb 3 16:30:57.436: src: 192.0.2.130, dst: 192.0.2.129
.
*Feb 3 16:30:57.437: src NBMA: 203.0.113.10
*Feb 3 16:30:57.437: src protocol: 192.0.2.129, dst protocol: 198.51.100.1
.
*Feb 3 16:30:57.437: client NBMA: 203.0.113.6
*Feb 3 16:30:57.437: client protocol: 192.0.2.130
*Feb 3 16:30:57.437: NHRP: 144 bytes out Virtual-Access1
```

Example 2 - Utilize NHRP Installed Routes For Spoke To Spoke Communication

FlexVPN Server

Verify EIGRP topology for summary route introduced:

```
FLEX-HUB#show ip eigrp vrf B topology 198.51.100.0
EIGRP-IPv4 VR(B) Topology Entry for AS(1)/ID(192.0.0.1)
          Topology(base) TID(0) VRF(B)
EIGRP-IPv4(1): Topology base(0) entry for 198.51.100.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 9837035520, RIB is 76851840
  Descriptor Blocks:
  0.0.0.0 (Null0), from 0.0.0.0, Send flag is 0x0
      Composite metric is (9837035520/0), route is Internal
      Vector metric:
        Minimum bandwidth is 100 Kbit
        Total delay is 50101250000 picoseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1476
        Hop count is 0
        Originating router is 192.0.0.1
```

FlexVPN Clients

Verify the presence of summary route:

```
Spoke1#show ip route vrf B eigrp

Routing Table: B
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      198.51.100.0/24 is variably subnetted, 4 subnets, 3 masks
D        198.51.100.0/24 [90/102451840] via 192.0.2.1, 00:00:04
```

Try establishing spoke-to-spoke tunnel by initiating traffic:

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 13/13/13 ms
```

Verify again:

```
Spoke1#show ip route vrf B next-hop-override

Routing Table: B
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, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       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
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
H        192.0.2.129 is directly connected, 00:02:18, Virtual-Access1
C        192.0.2.132 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 4 subnets, 3 masks
D        198.51.100.0/24 [90/102451840] via 192.0.2.1, 00:02:13
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
H        198.51.100.8/29 [250/255] via 192.0.2.129, 00:02:18, Virtual-Access1
```

There is a very minor change in the debugs output for spokes network installation where it shows route-installation successful instead of RIB failure and adding NHO:

```
*Feb 3 16:43:38.957: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) labe
*Feb 3 16:43:38.957: 203.0.113.10 (flags:0x1000)
*Feb 3 16:43:38.957: NHRP-RT: Adding route entry for 198.51.100.8/29 via 192.0.2.131, Virtual-Access1 v
*Feb 3 16:43:38.957: NHRP-RT: Route addition to RIB Successful
*Feb 3 16:43:38.957: NHRP-EVE: NHP-UP: 192.0.2.131, NBMA: 203.0.113.10
```

Related Information

- Configuring FlexVPN Spoke to Spoke
- FlexVPN Spoke in Redundant Hub Design with FlexVPN Client Block Configuration Example