Advanced Concepts of DMVPN
(Dynamic Multipoint VPN)

Mike Sullenberger – Distinguished Engineer

BRKSEC-4054
Agenda

• DMVPN Design Overview
  • DMVPN general and IWAN Specific
• NHRP Details
  • NHRP Overview
  • NHRP Registrations/Resolutions/Redirects
• Interaction with IWAN
  • VRFs, RIB and PfR
• Recent and New Features
DMVPN Design Overview
Agenda

- DMVPN Design Overview
  - DMVPN General
  - IWAN Specific
- NHRP Details
  - NHRP Overview
  - NHRP Registrations/Resolutions/Redirects
- Interaction with IWAN
  - VRFs
  - NHRP the RIB and PfR
- Recent and New Features
What is Dynamic Multipoint VPN?

DMVPN is a Cisco IOS software solution for building IPsec+GRE VPNs in an easy, dynamic and scalable manner

• Uses two proven technologies
  • Next Hop Resolution Protocol (NHRP)
    • Creates a distributed mapping database of VPN (tunnel int.) to real (public int.) addresses
  • Multipoint GRE Tunnel Interface
    • Single GRE interface to support multiple GRE/IPsec tunnels and endpoints
    • Simplifies size and complexity of configuration
    • Supports dynamic tunnel creation
DMVPN Major Features

• Configuration reduction and no-touch deployment
• Supports:
  • Passenger protocols (IP(v4/v6) unicast, multicast and dynamic Routing Protocols)
  • Transport protocols (NBMA) (IPv4 and IPv6)
  • Remote peers with dynamically assigned transport addresses.
  • Spoke routers behind dynamic NAT; Hub routers behind static NAT.
• Dynamic spoke-spoke tunnels for partial/full mesh scaling.
• Can be used without IPsec Encryption
• Works with MPLS; GRE tunnels and/or data packets in VRFs and MPLS switching over the tunnels
• Wide variety of network designs and options.
# DMVPN Phases

<table>
<thead>
<tr>
<th>Phase 1 – 12.2(13)T</th>
<th>Phase 2 – 12.3(4)T (Phase 1 +)</th>
<th>IWAN 1.0</th>
<th>Phase 3 – 12.4.(6)T (Phase 2 +)</th>
<th>IWAN 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub and spoke functionality</td>
<td>Spoke to spoke functionality</td>
<td>mGRE interface on spokes</td>
<td>More network designs and greater scaling</td>
<td></td>
</tr>
<tr>
<td>p-pGRE interface on spokes, mGRE on hubs</td>
<td>mGRE interface on spokes</td>
<td>Direct spoke to spoke data traffic reduces load on hubs</td>
<td>Same Spoke to Hub ratio</td>
<td></td>
</tr>
<tr>
<td>Simplified and smaller configuration on hubs</td>
<td>Direct spoke to spoke data traffic reduces load on hubs</td>
<td>Hubs must interconnect in daisy-chain</td>
<td>No hub daisy-chain</td>
<td></td>
</tr>
<tr>
<td>Support dynamically addressed CPEs (NAT)</td>
<td>Hubs must interconnect in daisy-chain</td>
<td>Spoke must have full routing table – no summarization</td>
<td>Spokes don’t need full routing table – can summarize</td>
<td></td>
</tr>
<tr>
<td>Support for routing protocols and multicast</td>
<td>Spoke must have full routing table – no summarization</td>
<td>Spoke-spoke tunnel triggered by spoke itself</td>
<td>Spoke-spoke tunnel triggered by hubs</td>
<td></td>
</tr>
<tr>
<td>Spokes don’t need full routing table – can summarize on hubs</td>
<td>Spoke-spoke tunnel triggered by spoke itself</td>
<td>Routing protocol limitations</td>
<td>Remove routing protocol limitations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NHRP routes/next-hops in RIB (15.2(1)T)</td>
</tr>
</tbody>
</table>
DMVPN How it works

• Spokes build a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes. They register as clients of the NHRP server (hub).

• When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries via NHRP for the real (outside) address of the destination spoke.

• Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address).

• The dynamic spoke-to-spoke tunnel is built over the mGRE interface.

• When traffic ceases then the spoke-to-spoke tunnel is removed.
DMVPN Example

Static Spoke-to-hub tunnels
Dynamic Spoke-to-spoke tunnels

Static known IP address
Dynamic unknown IP addresses

LANs can have private addressing

192.168.0.0/24
192.168.1.0/24
192.168.2.0/24

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

Physical: dynamic
Tunnel0: 10.0.0.12

Physical: 172.17.0.1
Tunnel0: 10.0.0.11

Spoke A

Spoke B

Static known
IP address
Dynamic unknown
IP addresses
DMVPN and IPsec

- IPsec integrated with DMVPN, but not required
- Packets Encapsulated in GRE, then Encrypted with IPsec
  - Both IKEv1 (ISAKMP) and IKEv2 supported
- NHRP controls the tunnels, IPsec does encryption
- Bringing up a tunnel
  - NHRP signals IPsec to setup encryption
  - ISAKMP/IKEv2 authenticates peer, generates SAs
  - IPsec responds to NHRP and the tunnel is activated
  - All NHRP and data traffic is Encrypted
- Bringing down a tunnel
  - NHRP signals IPsec to tear down tunnel
  - IPsec can signal NHRP if encryption is cleared or lost
- ISAKMP/IKEv2 Keepalives monitor state of spoke-spoke and spoke-hub tunnels
DMVPN Encryption Scaling

SLB Design
Throughput depends on number and types of hub platforms

- ASR1006+/RP2/ESP100
- ASR1006+/RP2/ESP40
- ASR1004+/RP2/ESP20
- ASR100(1/2)-X/Integrated
- ASR1004+/RP2/ESP10
- 4451-X
- 4351
- 3945E

IMIX Encryption Throughput at 70% Max CPU

Throughput depends on number and types of hub platforms.
Routing over DMVPN

- Supports all routing protocols, except ISIS
- Best routing protocols are EIGRP and BGP
- Hubs are routing neighbors with spokes
  - Receive spoke network routes from spokes
  - Advertise spoke and local networks to **all** spokes
    - Phase 1 & 3: Can Summarize (except OSPF)
    - Phase 2: Cannot summarize (OSPF limited to 2 hubs)
- Hubs are routing neighbors with other hubs
  - Phase 1: Can use different interface and routing protocol than hub-spoke tunnels
  - Phase 2: Must use same tunnel interface and routing protocol as hub-spoke tunnels
  - Phase 3: Can use different tunnel interface and routing protocol than hub-spoke tunnels
- Spokes are only routing neighbors with hubs, **not** with other spokes
  - Phase 3: Spoke-spoke NHRP “routes” are added directly to routing table (15.2(1)T)
Routing Table Example (Spoke)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phase 1 &amp; 3</strong></td>
<td>(with summarization)</td>
<td>C 172.16.1.0/30 is directly connected, Serial1/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 10.0.0.0/24 is directly connected, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 192.168.1.0/24 is directly connected, Ethernet0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S* 0.0.0.0/0 is directly connected, Serial1/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.0.0/16 [90/2841600] via 10.0.0.1, 00:00:08, Tunnel0</td>
</tr>
<tr>
<td><strong>Phase 1 &amp; 3</strong></td>
<td>(without summarization, next-hop <strong>not</strong> preserved)</td>
<td>C 172.16.1.0/30 is directly connected, Serial1/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 10.0.0.0/24 is directly connected, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.0.0/24 [90/297372416] via 10.0.0.1, 00:02:36, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 192.168.1.0/24 is directly connected, Ethernet0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.2.0/24 [90/297321216] via 10.0.0.1, 00:02:36, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.3.0/24 [90/297321216] via 10.0.0.1, 00:02:36, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S* 0.0.0.0/0 [1/0] via 172.16.1.1</td>
</tr>
<tr>
<td><strong>Phase 2</strong></td>
<td>(no summarization, next-hop preserved)</td>
<td>C 172.16.1.0/30 is directly connected, Serial1/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 10.0.0.0/24 is directly connected, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.0.0/24 [90/297372416] via 10.0.0.1, 00:42:34, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C 192.168.1.0/24 is directly connected, Ethernet0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.2.0/24 [90/297321216] via 10.0.0.1, 00:02:36, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D 192.168.3.0/24 [90/297321216] via 10.0.0.1, 00:42:34, Tunnel0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S* 0.0.0.0/0 [1/0] via 172.16.1.1</td>
</tr>
</tbody>
</table>
Routing Protocols over DMVPN

EIGRP

• Distance Vector style matches with DMVPN NBMA network style
  • Feasible successor for quick spoke-to-hub convergence
• Good scaling with reasonably fast convergence (hello 5, hold 15)
• Good metric control
  • Change metrics, route tagging, filtering or summarization at hub and/or spoke
  • Can be used to control load-balancing of spoke $\leftrightarrow$ hub(s) traffic
  • Automatic metric increase per DMVPN hop
• New code changes (Phase 2)
  • Equal Cost MultiPath (15.2(3)T, 15.2(1)S)
  • Add-path (15.3(1)S)
Routing Protocols over DMVPN

BGP

- Base Distance Vector style matches with DMVPN NBMA network style
  - iBGP (recommended)
    - Allows use of MED to control/compare routes
    - Dynamic Neighbors
    - May need to use “local-as” for iBGP (15.2(2)T, 15.1(3)S)
  - eBGP (okay)
    - AS-Path length is only thing to control/compare routes
- Good scaling but with slower convergence (hello 10+, hold 30+)
- Good metric control
  - Change metrics, route tagging, filtering or summarization at hub and/or spoke*
  - Can be used to control load-balancing of spoke ↔ hub(s) traffic
  - Only manual metric increase per DMVPN hop
- Some issues with Equal Cost multi-path (ECMP) route selection
  - Between multiple DMVPNs and preserving correct next-hop
  - Spoke-spoke tunnel load-balancing for spoke sites with multiple spoke routers
Routing Protocols over DMVPN

OSPF

• Link-state style doesn’t match as well with DMVPN NBMA network style
• Area issues – DMVPN requires single Area
  • Area 0 over DMVPN
    • Spoke sites can be in different areas
    • Area 0 extended over WAN – possible stability issues for Area 0
  • Non-Area 0 over DMVPN
    • All spokes sites in same area
  • Multi-subnet DMVPN can be used to have multiple OSPF areas
    • Increase in complexity of DMVPN and OSPF design
• More difficult metric control
  • Can only change metrics, filter or summarize at area boundaries
  • Automatic metric increase per DMVPN hop
  • Slight metric issue for failover path between multiple DMVPNs
• No issues with Equal Cost multi-path (ECMP) route selection
Routing Protocol?

• Which routing protocol should I use?
   • In general you would use the same routing protocol over DMVPN that you use in the rest of your network, or over other WAN networks (like MPLS).
   
• BUT...
   • EIGRP being an advanced distance vector protocol matches really well with DMVPN network topologies
   • BGP, specifically iBGP, runs well over DMVPN, but is more complicated to setup to have it act more like an IGP than an EGP.
   • OSPF can run over DMVPN, BUT lower scaling and Area 0 issues can complicate the network.
   • RIP can be used, but has longer hold time and limited metric values
   • IS-IS cannot be used since it doesn’t run over IP
Routing Protocol Scaling

SLB design using BGP or EIGRP

OSPF
- 3945E
- 4451-X

EIGRP
- 3945E
- 4451-X

BGP
- 3945E
- 4451-X

ASR1004+/RP2 (ASR100x-X)

Estimate: More testing is needed for OSPF

4000 spoke routes total: 4000 spokes with 1 route/spoke*

Test up to 10,000 spokes (ESP100)

Number of Branches

1000 2000 3000 4000
Redundancy

- Active-active redundancy model – two or more hubs per spoke
  - All configured hubs are active and are routing neighbors with spokes
    - Can use Backup NHS feature to activate a subset of configured hubs
  - Routing protocol routes are used to determine traffic forwarding
    - Single route: one tunnel (hub) at a time – primary/backup mode
    - Multiple routes: multiple tunnels (hubs) – load-balancing mode (CEF, PfR)

- ISAKMP/IPsec
  - Cannot use IPsec Stateful failover (NHRP isn’t supported)
  - ISAKMP invalid SPI recovery is not useful with DMVPN
    - no crypto isakmp invalid-spi-recovery
  - ISAKMP keepalives on spokes for timely hub recovery
    - crypto isakmp keepalives initial retry [periodic]
    - crypto isakmp nat keepalive interval
Redundancy (cont)

• Can use single or multiple DMVPNs for redundancy
  • Each mGRE interface is a separate DMVPN network using
    • Same: Tunnel source (optional).
    • Different: NHRP network-id and IP subnet, (or no) Tunnel key
  • If using same tunnel source with different tunnel key
    • tunnel protection ipsec profile name shared
  • Can “glue” mGRE interfaces into same DMVPN network (Phase 3 only)
    • Same: NHRP network-id and authentication, (or no) Tunnel key
    • Different: Tunnel source and IP subnet

• Spokes – at least two hubs (NHSs)
  • Phase 1: (Hub-and-spoke)
    • p-pGRE interfaces → two DMVPN networks, one hub on each
  • Phase 1, 2 or 3: (Hub-and-spoke or Dynamic Mesh)
    • mGRE interface → one DMVPN network, two or more hubs
Redundancy (cont)

- Hubs – interconnect and routing
  - Phase 1: (Hub and spoke only)
    - Interconnect hubs directly over physical link, p-pGRE or mGRE
    - Hubs can exchange routing through any of these paths
    - Same or different routing protocol as with spokes
  - Phase 2: (Dynamic Mesh)
    - Interconnect hubs over same mGRE, daisy-chain as NHSs
    - Hubs must exchange routing over DMVPN network
    - Must use same routing protocol as with spokes
  - Phase 3: (Dynamic Mesh)
    - Interconnect hubs over same or different mGRE (same NHRP Network-id)
    - Hubs must exchange routing over a DMVPN network
    - Same or different routing protocol as with spokes
Spoke-Spoke Tunnels – Considerations

• Resiliency
  • No direct monitoring of spoke-spoke tunnel* (use ISAKMP keepalives)
    • crypto isakmp keepalives [periodic] initial retry

• Path Selection*
  • NHRP will always build spoke-spoke tunnel
  • No bandwidth/latency measurement of spoke-spoke vs. spoke-hub-spoke paths
  • Can do interesting things with Smart-spoke feature

• Overloading spoke routers
  • CPU or memory → IKE Call Admission Control (CAC)
    • crypto call admission limit ike {sa | in-negotiation } max-SAs
    • call admission limit percent
    • show crypto call admission statistics
  • Bandwidth → Design for expected traffic
    • Hub-spoke versus Spoke-spoke; Spoke-spoke availability is best effort
Best Practices

• mGRE Tunnel configuration
  • Both Hubs and Spokes
    • tunnel source <interface>
    • bandwidth <WAN-interface> (as starting point, may adjust)
    • ip mtu 1400; ip tcp adjust-mss 1360

• NHRP
  • Spokes
    • ip nhrp shortcut
    • ip nhrp nhs <hub-tunnel> nbma <hub-nbma-ip|hub-fqdn> multicast (12.4(20)T)
  • Hubs
    • ip nhrp redirect
    • ip nhrp map multicast dynamic
    • ip nhrp server-only*
Best Practices (cont)

• Crypto
  • crypto isakmp [nat] keepalive initial [retrans]… – Spokes only
    • Initial = 30 (> RP hello); retrans = 5 → 55 seconds for neighbor down

• Routing
  • Phase 2 – Check that RP advertises routes with remote spoke as the next-hop
    • EIGRP: (hubs) no ip [next-hop-self | split-horizon] eigrp <as>, (all) use delay to adjust metric
    • OSPF: (all) ip ospf network broadcast; (spokes only) ip ospf priority 0
    • BGP: iBGP (hubs) route-reflectors; (spokes) neighbor <hub> next-hop-self
  • Phase 3 – Check that RP advertises routes with the hub as the next-hop
    • EIGRP: (hubs) no ip split-horizon eigrp <as>
    • OSPF: (all) ip ospf network point-multipoint; prefix-suppression (suppress /32 routes)
    • BGP: iBGP (hubs) route-reflectors; (all)* neighbor <hub|spoke> next-hop-self
  • To manipulate path selection through DMVPN use:
    • EIGRP: delay not bandwidth; OSPF: cost; iBGP: MED
Cisco IOS Code and Platform Support

- 3900 (E), 2900, 1900, 890, 880
  - 12.4(24)T8 (880 only);
  - 15.2(4)M8, 15.3(3)M5*, 15.4(3)M2*;
  - 15.4(2)T3, 15.5(2)T

- ASR1000(RP2), ASR1000-X, 4451-X, 4431, 4300
  - (3.10.5S)15.3(3)S5**, (3.12.3S)15.4(2)S3*, (3.13.2S) 15.4(3)S2*, (3.15.0S) 15.5(2)S

- CSR1000V
  - (3.12.3S)15.4(2)S3, (3.13.3S) 15.4(3)S3, (3.14.1S) 15.5(1)S1*, (3.15.0S) 15.5(2)S

* Recommended
+ N/A for 4431,4300
Basic DMVPN Designs

• Hub-and-spoke – Order(n)
  • Spoke-to-spoke traffic via hub
    • Phase 1: Hub bandwidth and CPU limit VPN
    • SLB: Many “identical” hubs; increases CPU and bandwidth limits
  • Spoke-to-spoke – Order(n) « Order(n^2)
  • Control traffic; Hub and spoke; Hub to hub
    • Phase 2: (single)
    • Phase 3: (hierarchical)
  • Unicast Data traffic; Dynamic mesh
    • Spoke routers support spoke-hub and spoke-spoke tunnels currently in use.
    • Hub supports spoke-hub traffic and overflow from spoke-spoke traffic.

• Network Virtualization
  • VRF-lite; Multiple DMVPNs (one per VRF)
  • MPLS over DMVPN (2547oDMVPN); Single DMVPN (many VRFs)
Basic DMVPN Designs

**Dual DMVPN Single Hub**
Single mGRE tunnel on Hub, two p-pGRE tunnels on Spokes

**Single DMVPN Dual Hub**
Single mGRE tunnel on all nodes

- **Spoke A**
  - Physical: 172.17.0.5
  - Tunnel0: 10.0.1.1
- **Spoke B**
  - Physical: (dynamic)
  - Tunnel0: 10.0.0.11
  - Tunnel1: 10.0.1.11

- **Hub**
  - Physical: 172.17.0.1
  - Tunnel0: 10.0.0.1
  - Tunnel0: 10.0.0.12
  - Tunnel1: 10.0.1.12

- **IP Addresses**
  - 192.168.0.0/24
  - 192.168.1.0/24
  - 192.168.2.0/24
  - 192.168.0.0/24
  - 192.168.1.0/24
  - 192.168.2.0/24

- **Physical**
  - 192.168.0.1
  - 192.168.0.1
  - (dynamic)
  - (dynamic)

- **Tunnel**
  - 10.0.0.1
  - 10.0.1.1
  - 10.0.1.1
  - (dynamic)
  - (dynamic)

- **Spoke-to-Spoke**
  - Green line = Dynamic Spoke-to-spoke

Diagram:
- Dual DMVPN Single Hub
- Single DMVPN Dual Hub
Multiple DMVPNs versus Single DMVPN

- **Multiple DMVPNs**
  - Best for Hub-and-spoke only
    - Easier to manipulate RP metrics between DMVPNs for Load-sharing
      - EIGRP – Route tags, Delay; iBGP – Communities, MED; OSPF – Cost
    - Performance Routing (PfR) selects between interfaces
  - Load-balancing over multiple ISPs (physical paths)
    - Load-balance data flows over tunnels → Better statistical load-balancing

- **Single DMVPN**
  - Best for spoke-spoke DMVPN
    - Can only build spoke-spoke within a DMVPN not between DMVPNs*
    - Slightly more difficult to manipulate RP metrics within DMVPN for Load-sharing
      - EIGRP – Route tags, delay; iBGP – Communities, MED; OSPF – Can’t do
  - Load-balancing over multiple ISPs (physical paths)
    - Load-balance tunnel destinations over physical paths → Worse statistical load-balancing
DMVPN Combination Designs

Retail/Franchise

Spoke-to-hub tunnels
Spoke-to-spoke tunnels

Dual ISP

ISP 1
ISP 2

Spoke-to-hub tunnels
Spoke-to-spoke tunnels
Spoke-hub-hub-spoke tunnel
DMVPN Combination Designs (cont)

Hierarchical

Server Load Balancing

- Spoke-to-hub tunnels
- Spoke-to-spoke tunnels
- Hub-to-hub tunnel
Network Virtualization
Separate DMVPN mGRE tunnel per VRF (VRF-lite)

- Hub routers handle all DMVPNs
  - Multiple Hub routers for redundancy and load
- IGP used for routing protocol over DMVPNs on Spokes and Hubs
  - Address family per VRF
  - Routing neighbor per spoke per VRF
- BGP used only on the hub
  - Redistribute between IGP and BGP for import/export of routes between VRFs
  - “Internet” VRF for Internet access and routing between VRFs
- Global routing table used for routing DMVPN tunnel packets
Network Virtualization
MPLS over DMVPN – 2547oDMVPN

- MPLS VPN over DMVPN
  - Single DMVPN/mGRE tunnel on all routers
  - Multiple Hub routers for redundancy and load
- MPLS configuration – routers are PEs
  - Spoke to spoke via hub and direct shortcut
  - MPLS labels via NHRP, ‘mpls nhrp’ (15.4(1)S, 15.4(2)T)
    - Replaces ‘mpls ip’; No LDP
- Routing
  - Global for routing DMVPN tunnel packets
  - IGP for routing outside of DMVPN
  - MP-BGP for routing over DMVPN
    - Redistribute between IGP and BGP for over DMVPN
    - Import/export routes between VRFs and Global (or Internet VRF)
    - One routing neighbor per spoke
Agenda

• DMVPN Design Overview
  • DMVPN General
  • IWAN Specific
• NHRP Details
  • NHRP Overview
  • NHRP Registrations/Resolutions/Redirects
• Interaction with IWAN
  • VRFs
  • NHRP the RIB and PfR
• Recent and New Features
Intelligent WAN Solution Components

- **Transport Independent**
  - Consistent operational model
  - Simple provider migrations
  - Scalable and modular design
  - DMVPN IPsec overlay design

- **Intelligent Path Control**
  - Application best path based on delay, loss, jitter, path preference
  - Load balancing for full utilization of all bandwidth
  - Improved network availability
  - Performance Routing (PfR)

- **Application Optimization**
  - Application monitoring with Application Visibility and Control (AVC)
  - Application Acceleration and bandwidth savings with WAAS

- **Secure Connectivity**
  - Certified strong encryption
  - Comprehensive threat defense with ASA and IOS firewall/IPS
  - Cloud Web Security (CWS) for scalable secure direct Internet access
Flexible Secure WAN Design Over Any Transport
Dynamic Multipoint VPN

Transport-Independent

Simplifies WAN Design

- Easy multi-homing over any carrier service offering
- Single routing control plane with minimal peering to the provider

Flexible

Dynamic Full-Meshed Connectivity

- Consistent design over all transports
- Automatic site-to-site IPsec tunnels
- Zero-touch hub configuration for new spokes

Secure

Proven Robust Security

- Certified crypto and firewall for compliance
- Scalable design with high-performance cryptography in hardware
DMVPN design with IWAN

- Multiple DMVPNs
  - One per physical transport network
  - Path diversity
  - Separate failure domains

- Each Phase 3 DMVPN
  - Single layer hub-and-spoke; hierarchical not currently supported
  - Physical WAN interface in f-VRF
  - Single Hub; Multi-Hub
    - PfRv3 Multi-NH and Multi-DC feature (15.5(3)S, 15.5(3)M)
  - Spoke-Spoke dynamic tunnels
  - Per-Tunnel QOS

- PfRv3 interoperability
  - Dynamic path selection
    - Per application
    - Load Balancing
    - Brownout circumvention
  - Communicates with NHRP via RIB
    - Triggers secondary spoke-spoke tunnels

- Single Overlay Routing Domain
  - Simplified operations and support
  - Simple ECMP load-balancing and primary path provisioning
  - EIGRP or BGP
    - PfRv3 gets secondary path directly from RP
Basic DMVPN Design for IWAN

Dual DMVPN Dual Hub

Internet DMVPN
MPLS DMVPN
Dynamic Spoke-to-spoke

Physical: 172.16.0.1
Tunnel0: 10.0.0.1
Loop0: 172.18.0.1

Physical: 172.17.0.5
Tunnel0: 10.0.0.2
Loop0: 172.18.1.1

Physical: 172.16.0.5
Tunnel0: 10.0.0.1
Loop0: 172.18.1.1

Physical: 172.17.0.1
Tunnel0: 10.0.0.13
Tunnel1: 10.0.0.11
Loop0: 172.18.0.1

Physical: 192.168.10.0/24
Physical: 192.168.3.0/24
Physical: 192.168.20.0/24

Spoke A
Spoke B1
Spoke B2
Spoke C

192.168.1.0 /24
192.168.10.0/24
192.168.20.0/24
192.168.3.0/24
192.168.100.0/24

192.168.10.0/24
192.168.100.0/24
192.168.20.0/24
192.168.3.0/24

Internet
MPLS
# VPN Selection

<table>
<thead>
<tr>
<th>Use Case/Solution</th>
<th>DMVPN</th>
<th>GETVPN</th>
<th>FlexVPN (dVTI)</th>
<th>SSLVPN</th>
<th>Easy VPN</th>
<th>IPsec VPN (sVTI, p-pGRE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access</td>
<td>No</td>
<td>No</td>
<td>Yes (IKEv2)</td>
<td>Yes (TLS)</td>
<td>Yes (IKEv1)</td>
<td>No</td>
</tr>
<tr>
<td>Static Site to Site</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic Site to Site</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IoT</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IWAN</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
NHRP Details
Agenda

- DMVPN Design Overview
  - DMVPN General
  - IWAN Specific
- NHRP Details
  - NHRP Overview
  - NHRP Registrations/Resolutions/Redirects
- Interaction with IWAN
  - VRFs
  - NHRP the RIB and PfR
- Recent and New Features
NHRP Message Types

• Registration
  • Build base hub-and-spoke network for control and data traffic
    (Phase 1 and 2 – single layer, Phase 3 – hierarchical)

• Resolution – Phase 2 and 3
  • Get mapping to build dynamic spoke-spoke tunnels

• Traffic Indication (Redirect) – Phase 3
  • Trigger resolution requests at previous GRE tunnel hop

• Purge
  • Clear out stale dynamic NHRP mappings

• Error
  • Signal error conditions
NHRP Main Functionality

• NHRP Registrations
  • Static NHRP mappings on spokes for Hub (NHS)
  • Spoke (NHC) dynamically registers its VPN to NBMA address mapping with hub (NHS)

• NHRP Resolutions – Phase 2 and 3
  • Dynamically resolve spoke to spoke VPN to NBMA mapping for spoke-spoke tunnels
    • Phase 2 – NHC self triggers to send NHRP Resolution request
    • Phase 3 – NHC triggered by first hop NHS to send NHRP Resolution request
  • NHRP Resolution requests sent via hub-and-spoke or direct spoke-spoke path
  • NHRP Resolution replies sent via direct spoke-spoke path

• NHRP Redirects (Traffic Indication) – Phase 3
  • Data packets forwarded via NHS, which “hairpins” data packets back onto DMVPN
  • NHS sends redirect message to “trigger” NHC to resolve direct spoke-spoke path
NHRP Message Extension Types

- Responder Address Extension:
  - Address mapping for Responding node (Reply messages)

- Forward Transit NHS Record Extension:
  - List of NHSs that NHRP request message traversed – copied to reply message

- Reverse Transit NHS Record Extension:
  - List of NHSs that NHRP reply message traversed

- Authentication Extension:
  - NHRP Authentication (clear-text*)

- NAT Address Extension:
  - Address mapping: For peer (Registration request/reply); For self (Resolution request/reply)

- Cisco Vendor Extension
  - NHRP Group name
  - Smart-spoke attributes (name; value)
NHRP Mapping Entries

- **Static**
  - Both host (/32, /128) and network (/<x>) mappings

- **Dynamic**
  - Registered (/32, /128)
    - From NHRP Registration
    - NAT – record both inside and outside address
  - Learned (/32, /128 or /<x>)
    - From NHRP Resolution
    - NAT – record both inside and outside address

- **Incomplete (/32, /128)**
  - Rate-limit NHRP Resolution Requests
  - Data packets process-switched via NHS while building spoke-spoke tunnels. (Phase 2)

- **Local (/32, /128 or /<x>)**
  - Mapping for local network sent in an NHRP Resolution Reply
  - Record which nodes were sent this mapping

- **Temporary (/32) (12.4(22)T)**
  - Same as “Incomplete” mapping except that NBMA is set to Hub
  - Data packets CEF-switched via NHS while building spoke-spoke tunnels. (Phase 2)

- **(no socket)**
  - Not used to forward data packets
  - Do not trigger IPsec encryption
  - Set on Local entries
NHRP Mapping Entries

Static

10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:20:10, never expire
Type: static, Flags: used
NBMA address: 172.17.0.9

Registered

10.0.0.19/32 via 10.0.0.19, Tunnel0 created 01:20:08, expire 00:05:51
Type: dynamic, Flags: unique registered used
NBMA address: 172.16.3.1

10.0.0.18/32 via 10.0.0.18, Tunnel0 created 00:16:09, expire 00:05:50
Type: dynamic, Flags: unique registered used
NBMA address: 172.18.0.2
( Claimed NBMA address: 172.16.2.1 )

10.0.0.18/32 via 10.0.0.18, Tunnel0 created 00:09:04, expire 00:00:22
Type: dynamic, Flags: router implicit
NBMA address: 172.18.0.2
( Claimed NBMA address: 172.16.2.1 )

192.168.23.0/24 via 10.0.0.19, Tunnel0 created 00:00:11, expire 00:05:48
Type: dynamic, Flags: router used
NBMA address: 172.16.3.1

NAT

192.168.15.0/24 via 10.0.0.11, Tunnel0 created 00:05:39, expire 00:05:50
Type: dynamic, Flags: router unique local
NBMA address: 172.16.1.1
(no-socket)

Incomplete

10.0.0.45/32, Tunnel0 created 00:00:21, expire 00:02:43
Type: incomplete, Flags: negative
Cache hits: 2

Temporary

10.0.0.17/32 via 10.0.2.17, Tunnel0 created 00:00:09, expire 00:02:55
Type: dynamic, Flags: used temporary
NBMA address: 172.17.0.9

Local (no-socket)
### NHRP Mapping Flags

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unique</td>
<td>Mapping entry is unique, don’t allow overwrite with new NBMA</td>
</tr>
<tr>
<td>registered</td>
<td>Mapping entry from an NHRP registration</td>
</tr>
<tr>
<td>authoritative</td>
<td>Mapping entry can be used to answer NHRP resolution requests</td>
</tr>
<tr>
<td>used</td>
<td>Mapping entry was used in last 60 seconds to forward data traffic</td>
</tr>
<tr>
<td>router</td>
<td>Mapping entry for remote router</td>
</tr>
<tr>
<td>implicit</td>
<td>Mapping entry from source information in NHRP resolution request packet</td>
</tr>
<tr>
<td>local</td>
<td>Mapping entry for a local network, record remote requester</td>
</tr>
<tr>
<td>nat</td>
<td>Remote peer supports the NHRP NAT extension</td>
</tr>
<tr>
<td>rib</td>
<td>Routing Table entry created</td>
</tr>
<tr>
<td>nho</td>
<td>Next-Hop-Override Routing Table entry created</td>
</tr>
<tr>
<td>nhop</td>
<td>Explicit Next-Hop route out tunnel interface added to RIB/FIB</td>
</tr>
</tbody>
</table>
Agenda

- DMVPN Design Overview
  - DMVPN General
  - IWAN Specific
- NHRP Details
  - NHRP Overview
  - NHRP Registrations / Resolutions/Redirects
- Interaction with IWAN
  - VRFs
  - NHRP the RIB and PfR
- Recent and New Features
Hub-and-Spoke – Features

- GRE, NHRP and IPsec configuration
  - p-pGRE or mGRE on spokes; mGRE on hubs
- ISAKMP/IKEv2 Authentication
  - Certificate (PKI), (Pairwise/Wildcard) Pre-shared Key (PSK)

- NHRP Registration
  - Spoke has static NHRP mapping for Hubs
  - Hub dynamically learns Spoke’s NHRP mapping
    - Handles dynamically addressed spokes (DHCP, NAT, …)
  - NAT detection support
NHRP Registration

- Builds base hub-and-spoke network
  - Hub-and-spoke data traffic
  - Control traffic; NHRP, Routing protocol, IP multicast
- Phase 2 – Single layer hub-and-spoke
- Phase 3 – Hierarchical hub-and-spoke (tree).

- Next Hop Client (NHC) has static mapping for Next Hop Servers (NHSs)
- NHC dynamically registers own mapping with NHS
  - Supports spokes with dynamic NBMA addresses or NAT
  - Reports outside address of Hub (Hub behind NAT?)
  - NHRP-group for per-Tunnel QoS (12.4(22)T)
  - IPv6: Includes both Unicast-Global and Link-local spoke mappings
- NHS registration reply gives liveliness of NHS
  - Supplies outside NAT address of spoke (Spoke behind NAT?)
  - IPv6: Includes link-local address hub mapping (needed by EIGRP; OSPF)
NHRP Registration
Building Spoke-Hub Tunnels

**NHRP Registration**

1. **Spoke A**
   - **Physical**: 172.17.0.1
   - **Tunnel 0**: 10.0.0.1
   - IP addresses:
     - 192.168.1.1/24
     - 192.168.2.1/24

2. **Spoke B**
   - **Physical**: (dynamic)
   - **Tunnel 0**: 10.0.0.11
   - IP addresses:
     - 10.0.0.11 → 172.16.1.1
     - 10.0.0.12 → 172.16.2.1

**Routing Table**

1. 172.16.1.1
2. 172.16.2.1

**NHRP Mapping**

1. 192.168.0.0/24
2. 192.168.1.0/24
3. 192.168.2.0/24

**Dynamic permanent IPsec tunnels**

- 10.0.0.1 → 172.17.0.1
- 10.0.0.11 → 172.16.1.1
- 10.0.0.12 → 172.16.2.1
- 192.168.1.0/24 → Conn.
- 192.168.2.0/24 → Conn.

---

**Cisco Live!**

BRKSEC_4054

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public 51
NHRP Registration
Routing Adjacency

- Spoke A
  - Physical: 172.17.0.1
  - Tunnel0: 10.0.0.1
  - Route: 192.168.1.0/24, 192.168.2.0/24

- Spoke B
  - Physical: 172.16.1.1
  - Tunnel0: 10.0.0.11
  - Tunnel1: 10.0.0.12
  - Route: 192.168.0.0/16, 192.168.0.0/24

- Dynamic permanent IPsec tunnels:
  - 192.168.0.0/16 → 10.0.0.1
  - 192.168.0.0/16 → Conn. (10.0.0.11, 10.0.0.12)
  - 192.168.0.0/24 → Conn.

- NHRP mapping:
  - 192.168.0.1/24

- Routing Table:
  - 192.168.0.0/16
  - 192.168.0.0/24

- NHRP packet:
  - 10.0.0.1 → 172.17.0.1
  - 192.168.0.0/16 → 10.0.0.1
  - 192.168.0.0/24 → Conn.
Hub-and-Spoke

Data Packet Forwarding

- Process-switching
  - Routing table selects outgoing interface and IP next-hop
  - NHRP looks up packet IP destination to select IP next-hop, overriding IP next-hop from routing table.
    - Could attempt to trigger spoke-spoke tunnel
      - ‘tunnel destination …’ → Can only send to hub
      - ‘ip nhrp server-only’ → Don’t send NHRP resolution request*
  - If no matching NHRP mapping then send to NHS (hub)

- CEF switching
  - IP Next-hop from FIB table (Routing table)
    - IP Next-hop → Hub → data packets send to Hub
  - Adjacency will be complete so CEF switch packet to hub
    - NHRP not involved
Agenda

• DMVPN Design Overview
  • DMVPN General
  • IWAN Specific
• NHRP Details
  • NHRP Overview
  • NHRP Registrations/Resolutions/Redirects
• Interaction with IWAN
  • VRFs
  • NHRP the RIB and PfR
• Recent and New Features
Phase 2 – Features

• Single mGRE interface with ‘tunnel protection …’
  • On Hubs and Spokes
  • Hubs must be inter-connected in a “Daisy chain” over same mGRE tunnel
  • IKE authentication information (Certificates, Wildcard Pre-shared Keys)

• Spoke-spoke data traffic direct
  • Reduced load on hub
  • Reduced latency
    • Single IPsec encrypt/decrypt

• Routing Protocol
  • Still hub-and-spoke
  • Cannot summarize spoke routes on hub
  • Routes on spokes must have IP next-hop of remote spoke (preserve next-hop)
Phase 2 – Process switching

- IP Data packet is forwarded out tunnel interface to IP next-hop from routing table
- NHRP looks in mapping table for IP destination
  - If Entry Found
    - Forward to NBMA from mapping table – overriding IP next-hop
  - If No Entry Found
    - Forward to IP next-hop (if in NHRP table) otherwise to NHS
    - If arriving interface was not tunnel interface
      - Initiate NHRP Resolution Request for IP next-hop and send via NHS path (first up NHS)
  - If (no socket) Entry Found
    - If arriving interface is not tunnel interface – convert entry to (socket)
    - Trigger IPsec to bring up crypto socket
    - Forward to IP next-hop (if in NHRP table) otherwise to NHS
Phase 2 – CEF Switching

- IP Data packet is forwarded out tunnel interface to IP next-hop from FIB table

  - If adjacency is of type Valid
    - Packet is encapsulated and forwarded by CEF out tunnel interface
    - NHRP is not involved

  - If adjacency is of type Glean or Incomplete
    - Punt packet to process switching
    - If original arriving interface was not this tunnel interface
    - Initiate NHRP Resolution Request for IP next-hop
      - Send resolution request for IP next-hop (tunnel IP address) of remote Spoke
      - Resolution request forwarded via NHS path (first up NHS)
      - Resolution reply is used to create NHRP mapping and to complete the Adjacency
Phase 2 – NHRP Resolution Request

Data packet
NHRP Resolution

NHRP mapping
CEF FIB Table
CEF Adjacency

192.168.0.1/24

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

192.168.0.1/24

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

192.168.0.1/24

Physical: 172.16.2.1
Tunnel0: 10.0.0.12

CEF FIB Table

NHRP mapping

CEF Adjacency

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

192.168.0.0/24 172.16.0.1 10.0.0.1 10.0.0.12 incomplete

192.168.0.0/24 172.16.0.1 (*) 172.16.1.1

192.168.0.1/24 172.16.0.1 (*) 172.16.1.1

192.168.0.0/24 Conn. 192.168.1.0/24 10.0.0.11

192.168.2.0/24 10.0.0.12

10.0.0.11 172.16.1.1
10.0.0.12 172.16.2.1

192.168.0.0/24 172.16.0.1 10.0.0.1

192.168.1.0/24 10.0.0.11

192.168.2.0/24 Conn.

10.0.0.11 172.16.2.1
10.0.0.12 172.16.2.1

10.0.0.1 172.17.0.1 (*)
10.0.0.12 ???

192.168.0.0/24 172.16.0.1 (*)
10.0.0.11 172.16.1.1

192.168.0.0/24 10.0.0.1

192.168.1.0/24 Conn.

192.168.2.0/24 Conn.

10.0.0.1 172.17.0.1 (*)
10.0.0.11 172.16.1.1

10.0.0.1 172.17.0.1
10.0.0.12 incomplete

10.0.0.1 172.17.0.1
10.0.0.12 incomplete

10.0.0.1 172.17.0.1
10.0.0.12 incomplete

10.0.0.1 172.16.0.1 (*)
10.0.0.11 172.16.1.1

10.0.0.1 172.17.0.1
10.0.0.12 incomplete

10.0.0.1 172.17.0.1
10.0.0.12 incomplete

10.0.0.1 172.17.0.1
10.0.0.12 incomplete
Phase 2 – NHRP Resolution Reply

**Data packet**
- NHRP Resolution

**NHRP mapping**

**CEF FIB Table**

**CEF Adjacency**

---

**Spoke A**

- Physical: 172.16.1.1
- Tunnel0: 10.0.0.1

- 192.168.1.1/24
- 10.0.0.1 172.16.0.1 (*)
- 10.0.0.11 172.16.1.1 (l)
- 10.0.0.12 172.16.2.1

- 192.168.0.0/24 10.0.0.1
- 192.168.1.0/24 Conn.
- 192.168.2.0/24 10.0.0.12

- 10.0.0.1 172.16.0.1 (*)
- 10.0.0.11 172.16.1.1 (l)
- 10.0.0.12 172.16.2.1

---

**Spoke B**

- Physical: 172.16.2.1
- Tunnel0: 10.0.0.12

- 192.168.2.1/24
- 10.0.0.1 172.16.0.1 (*)
- 10.0.0.11 172.16.1.1 (l)
- 10.0.0.12 172.16.2.1

- 192.168.0.0/24 10.0.0.1
- 192.168.1.0/24 10.0.0.11
- 192.168.2.0/24 Conn.

- 10.0.0.1 172.16.0.1 (*)
- 10.0.0.11 172.16.1.1 (l)
- 10.0.0.12 172.16.1.1

---

**Physical:** 172.17.0.1

**Tunnel0:** 10.0.0.1

- 192.168.0.1/24
- 10.0.0.11 172.16.1.1
- 10.0.0.12 172.16.2.1

- 192.168.0.0/24 Conn.
- 192.168.1.0/24 10.0.0.11
- 192.168.2.0/24 10.0.0.12

---

**CEF FIB Table**

- NHRP mapping

- CEF Adjacency
Phase 2 – NHRP Resolution Response Processing

• Receive NHRP Resolution reply
  • If using IPsec (tunnel protection …) then
    • Trigger IPsec to setup ISAKMP and IPsec SAs for tunnel
    • Data packets still forwarded via spoke-hub-…-hub-spoke path
    • IPsec triggers back to NHRP when done

• Install new mapping in NHRP mapping table

• Send trigger to CEF to complete corresponding CEF adjacency
  • Data packets now forwarded via direct spoke-spoke tunnel by CEF
  • NHRP no longer involved
Phase 2 – Refresh or Remove Dynamic mappings

- Dynamic NHRP mapping entries have finite lifetime
  - Controlled by ‘ip nhrp holdtime …’ on source of mapping (spoke)

- Background process checks mapping entry every 60 seconds
  - Process-switching
    - Used flag set each time mapping entry is used
    - If used flag is set and expire time < 120 seconds then refresh entry, otherwise clear used flag
  - CEF-switching
    - If expire time < 120 seconds, CEF Adjacency entry marked “stale”
    - If “stale” CEF Adjacency entry is then used, signal to NHRP to refresh entry

- Another resolution request is sent to refresh entry
  - Resolution request via NHS path; reply via direct tunnel

- If entry expires it is removed
  - If using IPsec → Trigger IPsec to remove IPsec/ISAKMP SAs
Agenda

- DMVPN Design Overview
  - DMVPN General
  - IWAN Specific
- NHRP Details
  - NHRP Overview
  - NHRP Registrations/Resolutions/Redirects
- Interaction with IWAN
  - VRFs
  - NHRP the RIB and PfR
- Recent and New Features
Phase 3 – Features

- Increase scale
  - Increase number of spokes, with same spoke/hub ratio
  - Distribution hubs off load central hub
    - Manage local spoke-spoke tunnels
    - IP multicast and routing protocol
- No hub daisy-chain
  - Use RIB to forward NHRP packets through NHSs
  - Reduces complexity and load for routing protocol
- OSPF not limited to 2 hubs
  - Network point-multipoint mode
  - Single OSPF area; No summarization

- Spokes don’t need full routing tables
  - Can summarize routes at the hub
  - Reduce space and load on spokes
  - Reduce routing protocol load on hub
    - 1000 spokes, 1 route per spoke;
    - hub advertises 1 route to 1000 spokes → 1000 advertisements
- Don’t recommend mixing Phase 2 and 3 on same DMVPN
  - Build separate Phase 3 DMVPN
  - Migrate spokes from Phase 2 DMVPN to Phase 3 DMVPN
  - Remove Phase 2 DMVPN
Phase 3 – Building Spoke-spoke Tunnels

- Originating spoke
  - IP Data packet is forwarded out tunnel interface to destination via Hub (NHS)
- Hub (NHS)
  - Receives and forwards data packet on tunnel interfaces with same NHRP Network-id.
  - Sends NHRP Redirect message to originating spoke.
- Originating spoke
  - Receives NHRP redirect message
  - Sends NHRP Resolution Request for Data IP packet destination
- Destination spoke
  - Receives NHRP Resolution Request
  - Builds spoke-spoke tunnel
  - Sends NHRP Resolution Reply over spoke-spoke tunnel
Phase 3 – NHRP Redirects

Data packet
NHRP Redirect
NHRP Resolution

NHRP mapping
CEF FIB Table
CEF Adjacency

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

192.168.1.1/24

10.0.0.1 → 172.16.0.1
192.168.2.1 → ???
192.168.1.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1
10.0.0.1 → 172.17.0.1

192.168.0.1/24

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1
192.168.0.0/24 → Conn.
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → 10.0.0.12

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

192.168.2.1/24

10.0.0.1 → 172.17.0.1

192.168.2.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1
10.0.0.1 → 172.17.0.1

192.168.1.0/24

Spoke A

Spoke B
Phase 3 – NHRP Redirect Processing

• Sender
  • Insert (GRE IP header source, packet destination IP address) in NHRP redirect table – used to rate-limit NHRP redirect messages ‘show ip nhrp redirect’
  • Send NHRP redirect to GRE/IP header source (previous tunnel hop)
  • Time out rate-limit entries from the NHRP redirect table

• Receiver
  • Check data IP source address from data IP header in redirect
  • If routing to the IP source is out:
    • A GRE tunnel interface with the same NHRP Network-id
      • then drop redirect
    • Another interface, ‘ip nhrp shortcut’ is configured and the IP destination is permitted by ‘ip nhrp interest ACL’ (if configured)
      • then trigger an NHRP resolution request to data IP destination from data IP header in redirect
      • otherwise drop redirect
Phase 3 – NHRP Resolution Request

Data packet
NHRP Redirect
NHRP Resolution

NHRP mapping
CEF FIB Table
CEF Adjacency

Physical: 172.17.0.1
Tunnel0: 10.0.0.1

192.168.0.1/24

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.2.1

CEF FIB Table
192.168.0.0/24 \rightarrow Conn.
192.168.1.0/24 \rightarrow 10.0.0.11
192.168.2.0/24 \rightarrow 10.0.0.12

CEF Adjacency
10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.2.1

CEF Adjacency
480x54
10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.2.1

CEF Adjacency

10.0.0.1 \rightarrow 172.16.1.1
10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.1.1

CEF Adjacency

10.0.0.1 \rightarrow 172.16.1.1
10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.1.1

CEF Adjacency

10.0.0.1 \rightarrow 172.16.1.1
10.0.0.11 \rightarrow 172.16.1.1
10.0.0.12 \rightarrow 172.16.1.1

CEF Adjacency
Phase 3 – NHRP Resolution Processing

- Spoke (NHC) routing table has Hub (NHS) as IP next-hop for networks behind remote Spoke
  - If routing table has IP next-hop of remote spoke then process as in Phase 2
- Data packets are forwarded (CEF-switched) via routed path
  - Redirect message sent by every tunnel hop on routed path
  - Redirect for data packet triggers resolution request only on source spoke
- Send resolution request for IP destination from data packet header in redirect
- Resolution requests forwarded via routed path
- Resolution replies forwarded over direct tunnel
  - Direct tunnel initiated from remote → local spoke
- Forward data packets over direct tunnel after receipt of resolution reply.
Phase 3 – NHRP Resolution Reply

(Prior to 15.2(1)T – ISR, 7200)

Data packet
NHRP Redirect
NHRP Resolution

NHRP mapping
CEF FIB Table
CEF Adjacency

Physical: 172.16.1.1
Tunnel0: 10.0.0.11

192.168.1.0/24

192.168.0.1/24

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

10.0.0.11 → 172.16.1.1
10.0.0.12 → 172.16.2.1

192.168.0.0/24 → Conn.
192.168.1.0/24 → 10.0.0.11
192.168.2.0/24 → 10.0.0.12

192.168.2.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1

192.168.2.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1

10.0.0.1 → 172.16.2.1

192.168.1.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1

10.0.0.1 → 172.17.0.1
10.0.0.12 → 172.16.2.1

10.0.0.1 → 172.17.0.1
10.0.0.12 → 172.16.2.1

192.168.1.0/24 → Conn.
192.168.0.0/16 → 10.0.0.1

10.0.0.1 → 172.17.0.1
10.0.0.11 → 172.16.1.1
Phase 3 – CEF Switching

Data Packet Forwarding

• IP Data packet is forwarded out tunnel interface
  1. IP next-hop from CEF FIB mapped to Adjacency
     If adjacency is:
     • Glean or Incomplete → Punt to process switching
     • Valid → Select adjacency for the packet
  2. NHRP in Outbound CEF Feature path
     Look up packet IP destination in NHRP mapping table
     • Matching entry: Reselect adjacency → use direct spoke-spoke tunnel
     • No matching entry: Leave CEF adjacency → packet goes to hub

• If packet arrived on and is forwarded out the same tunnel interface
  • Forward data packet
  • If ‘ip nhrp redirect’ is on inbound tunnel then send NHRP redirect
• Packet is encapsulated, encrypted and forwarded
Phase 3 – NHRP and Routing Table

Data Packet Forwarding

- When NHRP resolution is received
  - Insert mapping information in mapping table replacing Incomplete/Temporary mapping
  - Insert NHRP routing entry in Routing Table (RT)
    - NHRP NET/Mask is more specific than RT Net/Mask
      - Add new route owned by NHRP (Type = H)
      - Monitor parent route
      - If parent route changes outbound interface then remove NHRP route.
    - NHRP Net/Mask is equal to RT Net/Mask
      - Add Override Alternate Next-hop (% flag)
      - Route still owned by original owner
    - NHRP Net/Mask is less specific than RT Net/Mask
      - Reduce NHRP mask to = RT Mask
      - Add Override Alternate Next-hop (% flag)
      - Route still owned by original owner
  - Insert connected route for tunnel next-hop of NHRP parent mapping (nhop flag)
Phase 3 – NHRP and RT
Routing Table

#show ip route
H  192.168.11.0/24 [250/1] via 10.0.1.11, 00:01:02
D  %  192.168.128.0/24 [90/3200000] via 10.0.2.16, 00:50:56, Tunnel0

#show ip route next-hop-override | section H%  
H  192.168.11.0/24 [250/1] via 10.0.1.11, 00:01:02
D  %  192.168.128.0/24 [90/3200000] via 10.0.2.16, 00:50:56, Tunnel0

Routing entry for 192.168.11.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.0.1.11 00:05:29 ago
Routing Descriptor Blocks:
*  10.0.1.11, from 10.0.1.11, 00:05:29 ago
  Route metric is 1, traffic share count is 1

Routing entry for 192.168.128.0/24
Known via "eigrp 1", distance 90, metric 3200000, type internal
Redistributing via eigrp 1
Last update from 10.0.2.16 on Tunnel0, 00:43:44 ago
Routing Descriptor Blocks:
*  10.0.2.16, from 10.0.2.16, 00:43:44 ago, via Tunnel0
  Route metric is 3200000, traffic share count is 1

... [NHO]10.0.0.1, from 10.0.0.1, 00:05:57 ago, via Tunnel0
  Route metric is 1, traffic share count is 1
...
Phase 3 – Refresh or Remove Dynamic Mappings

- Dynamic NHRP mapping entries have finite lifetime
  - Controlled by ‘ip nhrp holdtime …’ on source of mapping (remote spoke)
  - Two types of mapping entries
    - Master entry – Remote Spoke Tunnel IP address
    - Child entries – Remote Network address(es) behind remote-spoke
- Background process checks mapping entries every 60 seconds
  - Master entry: Timing out* → mark CEF adjacency stale
    - If CEF adjacency is then used
      - Refresh Master entry and for each child entry that is also timing out* → queue for immediate refresh
- Refreshing entries
  - Send another Resolution request and reply
    - Resolution request/reply sent over direct tunnel
- If entry expires it is removed
  - If using IPsec and last entry using this NBMA address
    - Trigger IPsec to remove IPsec and ISAKMP/IKEv2 SAs

* Expire timer < 120 seconds
NHRP Purge Messages

• Used to clear invalid NHRP mapping information from the network
• NHRP “local”, “(no socket)” mapping entries
  • Created when sending an NHRP resolution reply
  • Copy of mapping information sent in reply
  • Entry tied to corresponding entry in routing table
  • Keeps list of nodes where resolution reply was sent – ‘show ip nhrp detail’
• If routing table changes so that local mapping entry is no longer valid
  • Purge message is sent to each NHRP node in list
  • NHRP nodes clear that mapping from their table
  • Purge messages forwarded over direct tunnel if available, otherwise sent via routed path
Interaction with IWAN
Agenda

- DMVPN Design Overview
  - General and IWAN Specific
- NHRP Details
  - NHRP Overview
  - NHRP Registrations/Resolutions/Redirects
- Interaction with IWAN
  - f-VRFs
  - NHRP the RIB and PfR
- Recent and New Features
DMVPN with IWAN f-VRFs
DMVPN with IWAN f-VRFs

• Create VRF for each transport WAN interface (Ex: INTERNET, MPLS)
  • vrf definition <fvrf-name>

• “Outside” of tunnel is in front-door VRF (f-VRF)
  • interface tunnel<x>; tunnel vrf <fvrf-name>

• WAN (transport) interface is in f-VRF
  • interface <wan-interface>; vrf forwarding <fvrf-name>

• Crypto – ISAKMP/IKEv2 are also in f-VRFs
  • ISAKMP – need keyring for each f-VRF
  • IKEv2 – need keyring, IKEv2 profile and IPsec profile
    • Separate one for each f-VRF
    Or
    • Single one for all fVRFs by using ‘match fvrf any’ in IKEv2 profile
**DMVPN with IWAN f-VRFs**

**f-VRF Configuration**

```plaintext
vrf definition INTERNET
    ...
vrf definition MPLS
    ...
! crypto ikev2 keyring DMVPN
    peer ANY
    address 0.0.0.0 0.0.0.0
    pre-shared-key cisco123
! crypto ikev2 profile DMVPN
    match fvrf any
    match identity remote address 0.0.0.0
    authentication remote pre-share
    authentication local pre-share
    keyring local DMVPN
    dpd 20 5 on-demand
! crypto ipsec transform-set DMVPN esp-aes 256 esp-sha256-hmac
    mode tunnel
! crypto ipsec profile DMVPN
    set transform-set DMVPN
    set ikev2-profile DMVPN
```

```plaintext
interface Tunnel0
    ip address 10.0.0.11 255.255.255.0
    tunnel source FastEthernet0
    tunnel key 100000
    tunnel vrf INTERNET
    tunnel protection ipsec profile DMVPN
interface Tunnel1
    ip address 10.0.1.11 255.255.255.0
    tunnel source FastEthernet1
    tunnel key 100001
    tunnel vrf MPLS
    tunnel protection ipsec profile DMVPN
! interface FastEthernet0
    vrf forwarding INTERNET
    ip address 172.16.1.1 255.255.255.240
! interface FastEthernet1
    vrf forwarding MPLS
    ip address 172.17.1.1 255.255.255.240
! ip route vrf MPLS 0.0.0.0 0.0.0.0 172.17.1.2
ip route vrf INTERNET 0.0.0.0 0.0.0.0 172.16.1.2
```
DMVPN with IWAN f-VRFs

Routing

Spoke1#show ip route vrf *

D*EX 0.0.0.0/0 [170/2918400] via 10.0.1.2, 00:00:04, Tunnel1
  10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C  10.0.0.0/24 is directly connected, Tunnel0
C  10.0.1.0/24 is directly connected, Tunnel1
D  192.168.0.0/24 [90/2892800] via 10.0.1.2, 00:20:27, Tunnel1
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C  192.168.1.0/24 is directly connected, Ethernet0/0
D  192.168.10.0/24 [90/2918400] via 10.0.1.2, 00:32:39, Tunnel1

Routing Table: INTERNET
Gateway of last resort is 172.16.1.2 to network 0.0.0.0
S*  0.0.0.0/0 [1/0] via 172.16.1.2
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C  172.16.1.0/28 is directly connected, FastEthernet0

Routing Table: MPLS
Gateway of last resort is 172.17.1.2 to network 0.0.0.0
S*  0.0.0.0/0 [1/0] via 172.17.1.2
    172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C  172.17.1.0/28 is directly connected, FastEthernet1

Crypto

Spoke1#show crypto ikev2 session

Session-id:1845, Status:UP-ACTIVE, IKE count:1, CHILD count:1

<table>
<thead>
<tr>
<th>T-id</th>
<th>Local</th>
<th>Remote</th>
<th>fvrf/ivrf</th>
<th>CHILD count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>172.16.1.1/500</td>
<td>172.16.0.1/500</td>
<td>INTERNET/none</td>
<td>READY</td>
</tr>
</tbody>
</table>

Life/Active Time: 86400/1263 sec
Child sa: local selector 172.16.1.1/0 - 172.16.1.1/65535
remote selector 172.16.0.1/0 - 172.16.0.1/65535
ESP spi in/out: 0x86D2651B/0x1B72FEB6

Session-id:1844, Status:UP-ACTIVE, IKE count:1, CHILD count:1

<table>
<thead>
<tr>
<th>T-id</th>
<th>Local</th>
<th>Remote</th>
<th>fvrf/ivrf</th>
<th>CHILD count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.17.1.1/500</td>
<td>172.17.0.5/500</td>
<td>MPLS/none</td>
<td>READY</td>
</tr>
</tbody>
</table>

Life/Active Time: 86400/1290 sec
Child sa: local selector 172.17.1.1/0 - 172.17.1.1/65535
remote selector 172.17.0.5/0 - 172.17.0.5/65535
ESP spi in/out: 0xF8C63D42/0x66DEA87D
DMVPN with IWAN DIA

DIA packets “route” between Global and f-VRF
DMVPN with IWAN DIA

• Outbound
  • Block learning default through tunnel
    • Access-list: deny default; match everything else
    • Route-map: if match “learn” route
  • Apply route-map in Routing Protocol
    • EIGRP: use “distribute-list ... in <tunnel-interface>
    • BGP: use “neighbor ... in”
  • Static default route in global table forwarding out Internet WAN interface
    • ip route 0.0.0.0 0.0.0.0 <Internet-WAN> <next-hop>|dhcp <admin-distance>

• Inbound
  • Policy-based routing (PBR)
    • access-list: match internal networks
    • route-map: if match use global routing table
DMVPN with IWAN DIA

Inbound

interface FastEthernet0
  description INTERNET
  vrf forwarding INTERNET
  ip address 172.16.1.1 255.255.255.240
  ip policy route-map INET-INTERNAL
!
  ip access-list extended INTERNAL-NETS
    permit ip any 10.0.0.0 0.0.1.255
    permit ip any 192.168.0.0 0.0.255.255
    permit ip any 172.20.0.0 0.0.255.255

route-map INET-INTERNAL permit 10
  match ip address INTERNAL-NETS
  set global
!

Outbound

router eigrp 1
  distribute-list route-map BLOCK-DEFAULT in Tunnel0
  [distribute-list route-map BLOCK-DEFAULT in Tunnel1]
  network 10.0.0.0 0.0.1.255
  network 192.168.1.0
!
  ip access-list standard ALL-EXCEPT-DEFAULT
    deny 0.0.0.0
    permit any
!
  route-map BLOCK-DEFAULT permit 10
    match ip address ALL-EXCEPT-DEFAULT
!
  ip route 0.0.0.0 0.0.0.0 FastEthernet0 172.16.1.2 10
DMVPN with IWAN DIA

Before

Spoke1#show ip eigrp topology
P 192.168.10.0/24, 1 successors, FD is 2918400
  via 10.0.1.2 (2918400/332800), Tunnel1
  via 10.0.0.1 (3020800/332800), Tunnel0
P 172.20.1.0/24, 1 successors, FD is 409600
  via 192.168.1.2 (409600/128256), Ethernet0/0
P 192.168.0.0/21, 1 successors, FD is 2892800
  via 10.0.1.2 (2892800/307200), Tunnel1
  via 10.0.0.1 (2995200/307200), Tunnel0
P 192.168.1.0/24, 1 successors, FD is 281600
  via Connected, Ethernet0/0
P 0.0.0.0/0, 1 successors, FD is 2918400
  via 10.0.1.2 (2918400/2636800), Tunnel1
  via 10.0.0.1 (3020800/2636800), Tunnel0

Spoke1#show ip route
D*EX 0.0.0.0/0 [170/2918400] via 10.0.1.2, 00:00:04, Tunnel1
D 172.20.1.0 [90/409600] via 192.168.1.2, 01:47:00, Ethernet0/0
D 192.168.0.0/21 [90/2892800] via 10.0.1.2, 00:20:27, Tunnel1
C 192.168.1.0/24 is directly connected, Ethernet0/0
D 192.168.10.0/24 [90/2918400] via 10.0.1.2, 00:32:39, Tunnel1

After

Spoke1#sho ip eigrp topology
P 192.168.10.0/24, 1 successors, FD is 2918400
  via 10.0.1.2 (2918400/332800), Tunnel1
  via 10.0.0.1 (3020800/332800), Tunnel0
P 172.20.1.0/24, 1 successors, FD is 409600
  via 192.168.1.2 (409600/128256), Ethernet0/0
P 192.168.0.0/21, 1 successors, FD is 2892800
  via 10.0.1.2 (2892800/307200), Tunnel1
  via 10.0.0.1 (2995200/307200), Tunnel0
P 192.168.1.0/24, 1 successors, FD is 281600
  via Connected, Ethernet0/0
P 0.0.0.0/0, 0 successors, FD is Infinity
  via 10.0.1.2 (2918400/2636800), Tunnel1

Spoke1#show ip route
S* 0.0.0.0/0 [10/0] via 172.16.1.2, Fastethernet0
D 172.20.1.0 [90/409600] via 192.168.1.2, 01:47:00, Ethernet0/0
D 192.168.0.0/21 [90/2892800] via 10.0.1.2, 01:46:28, Tunnel1
C 192.168.1.0/24 is directly connected, Ethernet0/0
D 192.168.10.0/24 [90/2918400] via 10.0.1.2, 01:46:28, Tunnel1
Agenda

• DMVPN Design Overview
  • General and IWAN Specific
• NHRP Details
  • NHRP Overview
  • NHRP Registrations/Resolutions/Redirects
• Interaction with IWAN
  • f-VRFs
    • NHRP the RIB and PfRv3
• Recent and New Features
Routing Protocol (RP), NHRP and PfRv3

- Routing protocol (RP) – destinations outside of the DMVPN
  - Advertises reachability of these destinations over any/all DMVPNs
  - Sets base forwarding within DMVPNs via the RIB

- PfRv3 – optimize forwarding of flows over different DMVPN paths
  - PfR RIB used to control forwarding of flows
  - Lookup alternate paths directly in RP database (except OSPF)
  - Bring up alternate paths, with probe traffic

- NHRP – optimizes forwarding within a single DMVPN
  - Shortcut (spoke-spoke) tunnels
    - Triggered by data traffic, including PfRv3 probe traffic
    - Changes forwarding by making changes in the RIB
    - Tracks RIB RP entries to control adding/removing shortcut tunnel
Basic DMVPN Design for IWAN

**Dual DMVPN**

**Hub1**
- Physical: 172.16.0.1
- Tunnel0: 10.0.0.1
- Loop0: 172.18.0.1

**Hub2**
- Physical: 172.17.0.5
- Tunnel1: 10.0.1.1
- Loop0: 172.18.0.2

**Internet DMVPN**
- Physical: 172.18.0.11
- Tunnel0: 10.0.0.11
- Tunnel1: 10.0.1.11
- Loop0: 172.18.0.11

**MPLS**
- Physical: 172.16.0.1
- Tunnel0: 10.0.0.1
- Loop0: 172.18.0.1

**Spoke A**
- Physical: 172.16.8.0/24
- Tunnel0: 10.0.0.12
- Loop0: 172.16.8.12

**Spoke B**
- Physical: 172.16.8.2
- Tunnel0: 10.0.0.12
- Tunnel1: 10.0.1.12

**Spoke C**
- Physical: 192.168.13.0/14
DMVPN with Routing Protocol

Routing Protocol – Both paths

```
SpokeA# show ip eigrp topology
```

- **Default over MPLS**
  - P 0.0.0.0/0, 0 successors, FD is Infinity via 10.0.1.2 (1769472000/1048576000), Tunnel1
  - P 10.0.1.0/24, 1 successors, FD is 1376256000 via Connected, Tunnel1
  - P 10.0.0.0/24, 1 successors, FD is 1638400000 via Connected, Tunnel0
  - P 192.168.0.0/24, 1 successors, FD is 1703936000 via 10.0.1.2 (1703936000/393216000), Tunnel1
  - P 192.168.1.0/24, 1 successors, FD is 131072000 via Connected, Ethernet0/0
  - P 192.168.10.0/24, 1 successors, FD is 1769472000 via 10.0.1.2 (1769472000/458752000), Tunnel1
  - P 192.168.11.0/24, 1 successors, FD is 196608000 via 192.168.1.2 (196608000/131072000), Ethernet0/0
  - P 192.168.13.0/24, 1 successors, FD is 2228224000 via 10.0.1.2 (2228224000/1507328000), Tunnel1
  - P 192.168.14.0/24, 1 successors, FD is 2752512000 via 10.0.1.2 (2752512000/1769472000), Tunnel0

- **Tunnel subnets**
- **Data Summary Route**
- **Local Subnet**
- **Data Specific Routes**
- **Not including MC/BR Loopback Routes**

```
In RIB
Not in RIB
MPLS
INET
```
DMVPN with Routing Protocol

RIB – Path via MPLS

SpokeA# show ip route

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [10/0] via 172.16.1.2, Serial1/0

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C  10.0.0.0/24 is directly connected, Tunnel0
C  10.0.1.0/24 is directly connected, Tunnel1

172.18.0.0/32 is subnetted, 8 subnets
D    172.18.0.1 [90/12800640] via 10.0.0.1, 01:10:55, Tunnel0
D    172.18.0.2 [90/10752640] via 10.0.1.2, 01:10:55, Tunnel1
D    172.18.0.10 [90/13312640] via 10.0.1.2, 01:10:55, Tunnel1
C    172.18.0.11 is directly connected, Loopback0
D    172.18.0.13 [90/16384640] via 10.0.1.2, 01:10:55, Tunnel1
D    192.168.0.0/21 [90/13312000] via 10.0.1.2, 01:10:55, Tunnel1
C    192.168.1.0/24 is directly connected, Ethernet0/0
D    192.168.1.10/24 [90/13824000] via 10.0.1.2, 01:10:55, Tunnel1
D    192.168.11.0/24 [90/15360000] via 192.168.1.2, 01:10:55, Ethernet0/0
D    192.168.13.0/24 [90/17408000] via 10.0.1.2, 01:10:55, Tunnel1
Building spoke-spoke tunnels with NHRP

NHRP inserts Mapping Entries into RIB

- Insert NHRP routing entry in Routing Table (RIB)
  - NHRP follows the rules outlined above for inserting RIB routes
  - BUT
    - NHRP also makes sure to not contradict routing protocol routes

- Check for “parent” route
  - Parent – next route with mask prefix less than or equal to NHRP route
  - If Parent route via:
    - same tunnel interface → add NHRP route
    - another interface → do not add NHRP route

- After adding NHRP route → Watch Parent route
  - If Parent route changed or removed (attach to next parent route)
  - If Parent route now via:
    - same tunnel interface → leave NHRP route
    - another interface → remove NHRP route

- Override with ‘no nhrp route-watch’ – can misroute or black-hole traffic
Forwarding over Primary DMVPN

Dual DMVPN

Physical: 172.16.0.1
Tunnel0: 10.0.0.11
Tunnel1: 10.0.1.11
Loop0: 172.18.0.11

Hub1

Physical: 172.17.0.5
Tunnel0: 10.0.0.13
Loop0: 172.18.0.13

Hub2

Physical: (dynamic)
Tunnel0: 10.0.0.13
Tunnel1: 10.0.1.13
Loop0: 172.18.0.13

Physical: 192.168.10.3
Loop0: 172.18.0.10

MPLS

Spoke A

192.168.1.0/24
192.168.11.0/24

Internet

MC

192.168.3.0/24
192.168.13.0/14

Spoke C

192.168.16.0/24

Physical: (dynamic)
Tunnel0: 10.0.0.11
Tunnel1: 10.0.1.11
Loop0: 172.18.0.11

Hub1

Physical: 172.16.0.1
Tunnel0: 10.0.0.1
Loop0: 172.18.0.1

Hub2

Physical: 172.17.0.5
Tunnel1: 10.0.1.1
Loop0: 172.18.0.2

Internet DMVPN
MPLS DMVPN
Primary path
nhrp route-watch
no nhrp route-watch
## Forwarding over Primary DMVPN

### NHRP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpokeA# show ip nhrp</td>
<td></td>
</tr>
<tr>
<td>10.0.1.13/32 via 10.0.1.13</td>
<td>Tunnel1 created 00:04:23, expire 00:04:19</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router nhop rib NBMA address: 172.17.3.1</td>
<td></td>
</tr>
<tr>
<td>192.168.1.0/24 via 10.0.1.11</td>
<td>Tunnel1 created 00:04:25, expire 00:01:36</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router unique local NBMA address: 172.17.1.1 (no-socket)</td>
<td></td>
</tr>
<tr>
<td>192.168.3.0/24 via 10.0.1.13</td>
<td>Tunnel1 created 00:01:40, expire 00:04:19</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router rib NBMA address: 172.17.3.1</td>
<td></td>
</tr>
<tr>
<td>192.168.11.0/24 via 10.0.1.11</td>
<td>Tunnel1 created 00:04:02, expire 00:01:57</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router unique local NBMA address: 172.17.1.1 (no-socket)</td>
<td></td>
</tr>
<tr>
<td>192.168.13.0/24 via 10.0.1.13</td>
<td>Tunnel1 created 00:04:02, expire 00:01:57</td>
</tr>
<tr>
<td>Type: dynamic, Flags: router rib nho NBMA address: 172.17.3.1</td>
<td></td>
</tr>
</tbody>
</table>

### RIB

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpokeA# show ip route</td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks</td>
<td></td>
</tr>
<tr>
<td>C 10.0.0.0/24 is directly connected, Tunnel0</td>
<td></td>
</tr>
<tr>
<td>L 10.0.0.1/32 is directly connected, Tunnel0</td>
<td></td>
</tr>
<tr>
<td>C 10.0.1.0/24 is directly connected, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>L 10.0.1.1/32 is directly connected, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>H 10.0.1.13/32 is directly connected, 00:05:28, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>D 192.168.0.0/21 [90/13312000] via 10.0.1.2, 00:11:02, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks</td>
<td></td>
</tr>
<tr>
<td>C 192.168.1.0/24 is directly connected, Ethernet0/0</td>
<td></td>
</tr>
<tr>
<td>L 192.168.1.1/32 is directly connected, Ethernet0/0</td>
<td></td>
</tr>
<tr>
<td>H 192.168.3.0/24 [250/1] via 10.0.1.13, 00:03:06, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>D 192.168.10.0/24 [90/13824000] via 10.0.1.2, 00:11:02, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>D 192.168.11.0/24 [90/1536000] via 192.168.1.2, 00:11:02, Ethernet0/0</td>
<td></td>
</tr>
<tr>
<td>D 192.168.13.0/24 [90/17408000] via 10.0.1.2, 00:11:02, Tunnel1</td>
<td></td>
</tr>
<tr>
<td>[NHO][90/1] via 10.0.1.13, 00:05:28, Tunnel1</td>
<td></td>
</tr>
</tbody>
</table>
Forwarding over Secondary DMVPN

Dual DMVPN

Hub1
- Physical: 172.16.0.1
- Tunnel0: 10.0.0.1
- Loop0: 172.18.0.1

Hub2
- Physical: 172.17.0.5
- Tunnel1: 10.0.1.1
- Loop0: 172.18.0.2

MC
- Physical: 192.168.10.3
- Loop0: 172.18.0.10

Internet DMVPN

MPLS

Physical:
- 172.16.0.1
- Tunnel0: 10.0.0.11
- Tunnel1: 10.0.1.11
- Loop0: 172.18.0.11

Spoke A
- 192.168.1.0/24
- 192.168.11.0/24

Spoke C
- 192.168.3.0/24
- 192.168.13.0/14

Hub1
- Physical: (dynamic)
- Tunnel0: 10.0.0.11
- Tunnel1: 10.0.1.11
- Loop0: 172.18.0.11

Hub2
- Physical: (dynamic)
- Tunnel0: 10.0.0.13
- Tunnel1: 10.0.1.13
- Loop0: 172.18.0.13

Spoke A
- 192.168.1.0/24
- 192.168.11.0/24
## Forwarding over Secondary DMVPN

### NHRP

**SpokeA# show ip nhrp**

<table>
<thead>
<tr>
<th>Route</th>
<th>Tunnel</th>
<th>Created/Expires</th>
<th>Type</th>
<th>Flags</th>
<th>NBMA Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.13/32</td>
<td>Tunnel0</td>
<td>00:01:01/05:07</td>
<td>dynamic</td>
<td>router nhop</td>
<td>172.16.3.1</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>Tunnel0</td>
<td>00:01:01/04:58</td>
<td>dynamic</td>
<td>router unique</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(no-socket)</td>
<td></td>
<td>local</td>
<td></td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>Tunnel0</td>
<td>00:01:00/04:59</td>
<td>dynamic</td>
<td>router</td>
<td>172.16.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(no-socket)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.11.0/24</td>
<td>Tunnel0</td>
<td>00:00:52/05:07</td>
<td>dynamic</td>
<td>router unique</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(no-socket)</td>
<td></td>
<td>local</td>
<td></td>
</tr>
<tr>
<td>192.168.13.0/24</td>
<td>Tunnel0</td>
<td>00:00:52/05:07</td>
<td>dynamic</td>
<td>router</td>
<td>172.16.3.1</td>
</tr>
</tbody>
</table>

**NHRP mapping entries not in RIB**

No matching Parent Route

### RIB

**SpokeA# show ip route**

<table>
<thead>
<tr>
<th>Route</th>
<th>Tunnel</th>
<th>Created/Expires</th>
<th>Type</th>
<th>Flags</th>
<th>NBMA Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>Tunnel0</td>
<td>00:04:38</td>
<td>is variably</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnetted,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 subnets,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 masks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.24</td>
<td>Tunnel0</td>
<td>00:04:38</td>
<td>is directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connected,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tunnel0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.32</td>
<td>Tunnel0</td>
<td>00:04:38</td>
<td>is directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connected,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tunnel0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.0/24</td>
<td>Tunnel1</td>
<td>00:04:38/05:07</td>
<td>is variably</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnetted,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 subnets,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 masks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.24</td>
<td>Tunnel1</td>
<td>00:04:38/05:07</td>
<td>is directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connected,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tunnel1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.32</td>
<td>Tunnel0</td>
<td>00:04:38/05:07</td>
<td>is variably</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnetted,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 subnets,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 masks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.40</td>
<td>Tunnel1</td>
<td>00:04:38/05:07</td>
<td>is directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connected,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tunnel1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.48</td>
<td>Tunnel0</td>
<td>00:04:38/05:07</td>
<td>is variably</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnetted,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 subnets,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 masks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.56</td>
<td>Tunnel1</td>
<td>00:04:38/05:07</td>
<td>is directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connected,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tunnel1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.64</td>
<td>Tunnel0</td>
<td>00:04:38/05:07</td>
<td>is variably</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>subnetted,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 subnets,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 masks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.1.72</td>
<td>Tunnel1</td>
<td>00:04:38/05:07</td>
<td>is directly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connected,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tunnel1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Forwarding over Secondary DMVPN  
(no nhrp route-watch)

- **Internet DMVPN**: Green
- **MPLS DMVPN**: Blue
- **Primary path**: Dashed line
- **nhrp route-watch**: Red
- **no nhrp route-watch**: Black

### Dual DMVPN

- **Hub1**
  - Physical: 172.16.0.1
  - Tunnel0: 10.0.0.1
  - Tunnel1: 10.0.1.1
  - Loop0: 172.18.0.11

- **Hub2**
  - Physical: 172.17.0.5
  - Tunnel0: 10.0.1.1
  - Tunnel1: 10.0.1.13
  - Loop0: 172.18.0.13

- **MC**
  - Physical: 192.168.10.3
  - Loop0: 172.18.0.10

### Physical Interfaces

- **Spoke A**
  - 192.168.1.0/24
  - 192.168.11.0/24

- **Spoke C**
  - 192.168.3.0/24
  - 192.168.13.0/14

### Internet MPLS

- **Hub1**
  - Physical: 172.16.0.1
  - Tunnel0: 10.0.0.1
  - Tunnel1: 10.0.1.1
  - Loop0: 172.18.0.11

- **Hub2**
  - Physical: 172.17.0.5
  - Tunnel0: 10.0.1.1
  - Tunnel1: 10.0.1.13
  - Loop0: 172.18.0.13

### Hub1 Physical Interfaces

- **Tunnel0**: 10.0.0.11
- **Loop0**: 172.18.0.11

### Hub2 Physical Interfaces

- **Tunnel1**: 10.0.1.13
- **Loop0**: 172.18.0.13

### Hub1 Tunnel Interfaces

- **Tunnel0**: 10.0.0.11
- **Loop0**: 172.18.0.11

### Hub2 Tunnel Interfaces

- **Tunnel1**: 10.0.1.13
- **Loop0**: 172.18.0.13
Forwarding over Secondary DMVPN

**NHRP**

SpokeA# show ip nhrp

10.0.0.13/32 via 10.0.0.13
   Tunnel0 created 00:00:36, expire 00:05:25
   Type: dynamic, Flags: router nhop rib
   NBMA address: 172.16.3.1

192.168.1.0/24 via 10.0.0.11
   Tunnel0 created 00:00:35, expire 00:05:24
   Type: dynamic, Flags: router unique local
   NBMA address: 172.16.1.1
   (no-socket)

192.168.3.0/24 via 10.0.0.13
   Tunnel0 created 00:00:34, expire 00:05:25
   Type: dynamic, Flags: router unique local
   NBMA address: 172.16.1.1

192.168.11.0/24 via 10.0.0.11
   Tunnel0 created 00:00:24, expire 00:05:35
   Type: dynamic, Flags: router unique local
   NBMA address: 172.16.1.1
   (no-socket)

192.168.13.0/24 via 10.0.0.13
   Tunnel0 created 00:00:24, expire 00:05:35
   Type: dynamic, Flags: router nhop
   NBMA address: 172.16.3.1

**RIB**

SpokeA# show ip route

- 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
- C 10.0.0.0/24 is directly connected, Tunnel0
- L 10.0.0.11/32 is directly connected, Tunnel0
- H 10.0.0.11/32 is directly connected, 00:00:34, Tunnel0
- C 10.0.1.0/24 is directly connected, Tunnel1
- L 10.0.1.11/32 is directly connected, Tunnel1
- D 192.168.0.0/21 [90/13312000] via 10.0.1.2, 00:11:02, Tunnel1
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
  - C 192.168.1.0/24 is directly connected, Ethernet0/0
  - L 192.168.1.1/32 is directly connected, Ethernet0/0
- H 192.168.3.0/24 [250/1] via 10.0.0.13, 00:00:34, Tunnel0
- D 192.168.10.0/24 [90/13824000] via 10.0.1.2, 00:11:02, Tunnel1
- D 192.168.11.0/24 [90/1536000] via 192.168.1.2, 00:11:02, Ethernet0/0
- D 192.168.13.0/24 [90/17408000] via 10.0.1.2, 00:11:02, Tunnel1

- [NHO][90/1] via 10.0.0.13, 00:00:28, Tunnel0

**No Check for Parent Routes**
Building spoke-spoke tunnels with NHRP and PfRv3

• PfRv3 Controlled Data flows
  • Forwards data flows over both primary and secondary DMVPN
    • PfR controls any load-balancing
  • Uses PfR Loopback as next-hop (Ex: 172.18.0.x)
    • NHRP triggered to build spoke-spoke tunnel over both DMVPNs
      • NHRP mapping entries to Loopback (Ex: 172.18.0.x)
      • NHRP modifies RIB for Loopback next-hop
      • If routing changes → PfR controlled flows quickly rerouted

• PfRv3 Uncontrolled Data flows
  • Data flows forwarded via the RIB
  • Uses primary DMVPN
  • Need ECMP routes to load-balancing over both DMVPNs
Building spoke-spoke tunnels with NHRP and PfRv3
Forwarding over Primary and Secondary DMVPN

### NHRP

**SpokeA# show ip nhrp brief**

<table>
<thead>
<tr>
<th>Target</th>
<th>Via</th>
<th>NBMA</th>
<th>Mode</th>
<th>Intfc</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1/32</td>
<td>10.0.0.1</td>
<td>172.16.0.1</td>
<td>static</td>
<td>Tu0</td>
</tr>
<tr>
<td>10.0.0.11/32</td>
<td>10.0.0.11</td>
<td>172.16.1.1</td>
<td>dyn,loc</td>
<td>Tu0</td>
</tr>
<tr>
<td>10.0.0.13/32</td>
<td>10.0.0.13</td>
<td>172.16.3.1</td>
<td>dyn,rib</td>
<td>Tu0</td>
</tr>
<tr>
<td>172.18.0.11/32</td>
<td>10.0.0.11</td>
<td>172.16.1.1</td>
<td>dyn,loc</td>
<td>Tu0</td>
</tr>
<tr>
<td>172.18.0.13/32</td>
<td>10.0.0.13</td>
<td>172.16.3.1</td>
<td>dyn,nho</td>
<td>Tu0</td>
</tr>
<tr>
<td>10.0.1.1/32</td>
<td>10.0.1.1</td>
<td>172.17.0.5</td>
<td>static</td>
<td>Tu1</td>
</tr>
<tr>
<td>10.0.1.11/32</td>
<td>10.0.1.11</td>
<td>172.17.1.1</td>
<td>dyn,loc</td>
<td>Tu1</td>
</tr>
<tr>
<td>10.0.1.13/32</td>
<td>10.0.1.13</td>
<td>172.17.3.1</td>
<td>dyn,rib</td>
<td>Tu1</td>
</tr>
<tr>
<td>172.18.0.11/32</td>
<td>10.0.1.11</td>
<td>172.17.1.1</td>
<td>dyn,loc</td>
<td>Tu1</td>
</tr>
<tr>
<td>172.18.0.13/32</td>
<td>10.0.1.13</td>
<td>172.17.3.1</td>
<td>dyn,nho</td>
<td>Tu1</td>
</tr>
<tr>
<td>192.168.1.0/24</td>
<td>10.0.1.11</td>
<td>172.17.1.1</td>
<td>dyn,loc</td>
<td>Tu1</td>
</tr>
<tr>
<td>192.168.3.0/24</td>
<td>10.0.1.13</td>
<td>172.17.3.1</td>
<td>dyn,rib</td>
<td>Tu1</td>
</tr>
<tr>
<td>192.168.11.0/24</td>
<td>10.0.1.11</td>
<td>172.17.1.1</td>
<td>dyn,loc</td>
<td>Tu1</td>
</tr>
<tr>
<td>192.168.13.0/24</td>
<td>10.0.1.13</td>
<td>172.17.3.1</td>
<td>dyn,nho</td>
<td>Tu1</td>
</tr>
</tbody>
</table>

### RIB

**SpokeA# show ip route next-hop-override**

- 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
  - C 10.0.0.0/24 is directly connected, **Tunnel0**
  - L 10.0.0.11/32 is directly connected, **Tunnel0**
  - H 10.0.0.13/32 is directly connected, 00:08:40, **Tunnel0**
  - C 10.0.1.0/24 is directly connected, **Tunnel1**
  - L 10.0.1.11/32 is directly connected, **Tunnel1**
  - H 10.0.1.13/32 is directly connected, 00:09:05, **Tunnel1**

172.18.0.0/32 is subnetted, 8 subnets
- D 172.18.0.1 [90/12800640] via 10.0.0.1, 02:07:25, **Tunnel0**
- D 172.18.0.2 [90/10752640] via 10.0.0.1, 02:07:25, **Tunnel1**
- D 172.18.0.10 [90/13312640] via 10.0.1.2, 02:07:25, **Tunnel1**
- C 172.18.0.11 is directly connected, Loopback0
- D % 172.18.0.13 [90/16384640] via 10.0.1.2, 02:04:46, **Tunnel1**
  - [NHO][90/1] via 10.0.0.13, 00:02:19, **Tunnel0**
  - [NHO][90/1] via 10.0.1.13, 00:08:40, **Tunnel1**
- D 192.168.0.0/21 [90/13312000] via 10.0.1.2, 02:07:25, **Tunnel1**
- 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
- C 192.168.1.0/24 is directly connected, Ethernet0/0
- L 192.168.1.1/32 is directly connected, Ethernet0/0
- H 192.168.3.0/24 [250/1] via 10.0.1.13, 00:09:05, **Tunnel1**
- D 192.168.10.0/24 [90/13824000] via 10.0.1.2, 02:04:46, **Tunnel1**
- D 192.168.11.0/24 [90/1536000] via 192.168.1.2, 02:07:25, Ethernet0/0
- D % 192.168.13.0/24 [90/17408000] via 10.0.1.2, 02:04:46, **Tunnel1**
  - [NHO][90/1] via 10.0.1.13, 00:08:59, **Tunnel1**
Summary
Routing Protocol (RP), NHRP and PfRv3

- Routing protocol (RP) – destinations outside of the DMVPN
  - Sets base forwarding for IWAN
  - Set preference for one DMVPN or can setup up ECMP routes
- PfRv3 – optimize forwarding of flows over different DMVPN paths
  - Find paths directly in RP database (except OSPF)
  - PfR RIB forwards flows over paths to MC/BR Loopback next-hop
  - Probe traffic over alternate paths
- NHRP – optimizes forwarding within a single DMVPN
  - Shortcut (spoke-spoke) tunnels
    - Triggered by data traffic and/or PfRv3 probe traffic
    - Use ‘no nhrp route-watch’ to enable shortcut tunnels over alternate paths
    - NHRP mapping/routes to MC/BR Loopback addresses
DMVPN Recent and Future Features
DMVPN Recent and Future Features

• Recently Available
  • 2547oDMVPN spoke-spoke support (mpls nhrp)
  • TrustSec (SGT) over DMVPN (CMD, NSH)
  • Per-tunnel QoS with 2547oDMVPN
  • DMVPN (Adaptive) Per-tunnel QoS (H→S, S→H, S→S)

• Coming next
  • Monitoring, Diagnostics for DMVPN
  • NHRP Summary-maps (ip nhrp summary-map <network> <mask>)
  • BFD for mGRE tunnels

• Coming next (cont)
  • GRE tunnel grouped interfaces
    • EVN WAN using DMVPN
    • Dynamic Tunnel Key on spoke
  • IWAN
    • DMVPN with Akamai optimized transport

• On the Radar
  • Hub down fast convergence
  • Native Multicast over DMVPN
  • Scaling to 8000+ on ASR/ESP100
  • Centralized VPN Policy Server
Thank you
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

• Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions
TOMORROW starts here.
Extras
Extras

• Recent and New Features
  • MPLS over DMVPN – 2547oDMVPN with DMVPN Phase 3
  • IKEv2 with DMVPN
  • DMVPN IPv6 Transport
  • Routing protocol
  • Per-tunnel QoS for hub to spoke tunnels
MPLS over DMVPN – 2547oDMVPN

- Single DMVPN to support network virtualization
  - Single mGRE tunnel on all routers

- Simplified MPLS configuration
  - Still adds complexity for managing and troubleshooting

- Routing:
  - EIGRP is used for routing outside the DMVPN
  - MP-BGP used for routing protocol over DMVPN
    - Redistribute EIGRP to/from BGP for transport over DMVPN, and Import/export of VRF routes

- Support:
  - DMVPN Phase 1 – hub-and-spoke only
  - DMVPN Phase 2 – spoke-spoke only after shortcut tunnel is up
  - DMVPN Phase 3 – full spoke-spoke support (15.4(1)S, 15.4(2)T)
MPLS over DMVPN Phase 3

- New support in NHRP to
  - keep track of NHRP mapping table entries per VRF
  - transport MPLS forwarding labels
    - MPLS LDP not used over DMVPN
    - MP-BGP still propagates VPN labels
- New CLI
  - `mpls nhrp` replaces `mpls ip` on the tunnel interface.
    - Provides
      - Tag switching over the Tunnel interface
      - Tag switching of the NHRP packets
      - Installs NHRP redirect feature; if “ip nhrp redirect” is configured.
  - Rest of configuration stays the same.

```sh
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 360
  ip nhrp redirect
  ip tcp adjust-mss 1360
  mpls nhrp
  tunnel source Serial2/0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
```
# show ip nhrp

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Next Hop</th>
<th>Mask</th>
<th>Tunnel Status</th>
<th>Type</th>
<th>Flags</th>
<th>NBMA Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>10.0.0.1</td>
<td>/32</td>
<td>Tunnel0 created 1d22h, never expire</td>
<td>static</td>
<td>used</td>
<td>172.17.0.1</td>
</tr>
<tr>
<td>10.0.0.13</td>
<td>10.0.0.13</td>
<td>/32</td>
<td>Tunnel0 created 00:00:08, expire 00:03:51</td>
<td>dynamic</td>
<td>router nhop rib</td>
<td>172.16.3.1</td>
</tr>
<tr>
<td>192.168.11.0/24 (CompA)</td>
<td>10.0.0.13</td>
<td></td>
<td>Tunnel0 created 00:00:07, expire 00:03:51</td>
<td>dynamic</td>
<td>router unique local</td>
<td>172.16.1.1</td>
</tr>
<tr>
<td>192.168.13.0/24 (CompA)</td>
<td>10.0.0.13</td>
<td></td>
<td>Tunnel0 created 00:00:07, expire 00:03:51</td>
<td>dynamic</td>
<td>router nhp rib nho</td>
<td>172.16.3.1</td>
</tr>
</tbody>
</table>

# show ip route vrf CompA next-hop-over

Routing Table: CompA

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Mask</th>
<th>Distance</th>
<th>Cost</th>
<th>Next Hop</th>
<th>Interface</th>
<th>Security</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.0/24</td>
<td></td>
<td></td>
<td></td>
<td>direct connected, Ethernet0/0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.11.0/24</td>
<td>[200/0]</td>
<td></td>
<td></td>
<td>192.168.1.2</td>
<td>Ethernet0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.13.0/24</td>
<td>[90/307200]</td>
<td></td>
<td></td>
<td>10.0.0.1</td>
<td>Tu0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>192.168.101.0/24</td>
<td>[200/409600]</td>
<td></td>
<td></td>
<td>10.0.0.1</td>
<td>Tu0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

# show mpls forwarding

<table>
<thead>
<tr>
<th>Label</th>
<th>IP Address</th>
<th>Mask</th>
<th>Cost</th>
<th>Next Hop</th>
<th>Interface</th>
<th>Security</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>192.168.1.0/24</td>
<td>[V]</td>
<td>0</td>
<td>aggregate/CompA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>192.168.11.0/24</td>
<td>[V]</td>
<td>2850</td>
<td>Et0/0</td>
<td>192.168.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>192.168.13.0/24</td>
<td>[V]</td>
<td>0</td>
<td>Tu0</td>
<td>10.0.0.13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>192.168.101.0/24</td>
<td>[V]</td>
<td>0</td>
<td>Tu0</td>
<td>10.0.0.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...
IKEv2 with DMVPN

- DMVPN works with ISAKMP (IKEv1) and/or IKEv2
  - Transparent to DMVPN
  - Node can be responder for both ISAKMP and IKEv2
    - Both ISAKMP and IKEv2 are configured.
  - Node can be Initiator for either ISAKMP or IKEv2 not both
    - Configure under the ‘crypto ipsec profile …’

```
crypto isakmp policy 2
encri aes
authentication pre-share
group 2

crypto ikev2 keyring DMVPN
peer DMVPN
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123

crypto ikev2 profile DMVPN
match identity remote address 0.0.0.0
authentication local pre-share
authentication remote pre-share
keyring DMVPN

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set DMVPN esp-aes esp-sha-hmac
mode transport [require]

crypto ipsec profile DMVPN
set transform-set DMVPN
set ikev2-profile DMVPN

interface Tunnel0
...
tunnel protection ipsec profile DMVPN
```
DMVPN over IPv6 Transport – 15.2(1)T

- IPv6 and IPv4 packets over DMVPN IPv6 tunnels
  - Introduced in IOS 15.2(1)T, 15.3(1)S
  - IPv6 infrastructure network
  - IPv6 and/or IPv4 data packets over same IPv6 GRE tunnel
  - NHRP modifies Routing Table
- Can run both DMVPN IPv4 and IPv6
  - Separate DMVPNs (mGRE tunnel)
  - DMVPN IPv4 ↔ IPv6
    spoke to spoke via hub

- Configuration
  - Standard IPv6 configuration on Outside (WAN) interface
  - Small change on mGRE tunnel
  - Must use IKEv2 for IPsec encryption

- Split-tunneling
  - Enterprise versus ISP assigned IPv6 addresses at spoke
  - No NAT66
DMVPN over IPv6 Transport – Configuration

**Hub**

```plaintext```
crypto ikev2 keyring DMVPN
peer DMVPNv6
address ::/0
pre-shared-key cisco123v6

crypto ikev2 profile DMVPN
match identity remote address ::/0
authentication local pre-share
authentication remote pre-share
keyring DMVPN

crypto ipsec profile DMVPN
set transform-set DMVPN
set ikev2-profile DMVPN

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ipv6 address 2001:DB8:0:100::1/64
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 100006
tunnel source Serial2/0
tunnel mode gre multipoint ipv6
tunnel protection ipsec profile DMVPN
```

**Spoke**

```plaintext```
crypto ikev2 keyring DMVPN
peer DMVPNv6
address ::/0
pre-shared-key cisco123v6

crypto ikev2 profile DMVPN
match identity remote address ::/0
authentication local pre-share
authentication remote pre-share
keyring DMVPN
dpd keepalive 30 5 on-demand

crypto ipsec profile DMVPN
set transform-set DMVPN
set ikev2-profile DMVPN

interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ipv6 address 2001:DB8:0:100::1/64
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 100006
tunnel source Serial2/0
tunnel mode gre multipoint ipv6
tunnel protection ipsec profile DMVPN

interface Serial2/0
ip address 172.17.0.1 255.255.255.252
ipv6 address 2001:DB8:0::FFFF:1::1/126
ipv6 route ::/0 Serial2/0
```

---

**Spoke**

```plaintext```
crypto ikev2 keyring DMVPN
peer DMVPNv6
address ::/0
pre-shared-key cisco123v6

crypto ikev2 profile DMVPN
match identity remote address ::/0
authentication local pre-share
authentication remote pre-share
keyring DMVPN
dpd keepalive 30 5 on-demand

crypto ipsec profile DMVPN
set transform-set DMVPN
set ikev2-profile DMVPN

interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ipv6 address 2001:DB8:0:100::1/64
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 100006
tunnel source Serial1/0
tunnel mode gre multipoint ipv6
tunnel protection ipsec profile DMVPN

interface Serial1/0
ip address 172.16.1.1 255.255.255.252
ipv6 address 2001:DB8:0::FFFF:0:1::1/126
ipv6 route ::/0 Serial1/0
```

---

**Spoke**

```plaintext```
crypto ikev2 keyring DMVPN
peer DMVPNv6
address ::/0
pre-shared-key cisco123v6

crypto ikev2 profile DMVPN
match identity remote address ::/0
authentication local pre-share
authentication remote pre-share
keyring DMVPN
dpd keepalive 30 5 on-demand

crypto ipsec profile DMVPN
set transform-set DMVPN
set ikev2-profile DMVPN

interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ipv6 address 2001:DB8:0:100::1/64
ipv6 nhrp map multicast dynamic
ipv6 nhrp network-id 100006
tunnel source Serial1/0
tunnel mode gre multipoint ipv6
tunnel protection ipsec profile DMVPN

interface Serial1/0
ip address 172.16.1.1 255.255.255.252
ipv6 address 2001:DB8:0::FFFF:0:1::1/126
ipv6 route ::/0 Serial1/0
DMVPN over IPv6 Transport – Data Structures

Hub1# show ipv6 nhrp
10.0.0.11/32 via 10.0.0.11
Tunnel0 created 22:26:55, expire 00:03:37
Type: dynamic, Flags: unique registered used
NBMA address: 2001:DB8:0:FFFF:0:1:0:1

Hub1# show ipv6 nhrp
2001:DB8:0:100::B/128 via 2001:DB8:0:100::B
Tunnel0 created 22:27:52, expire 00:03:39
Type: dynamic, Flags: unique registered
NBMA address: 2001:DB8:0:FFFF:0:1:0:1
FE80::A8BB:CCFF:FE00:C800/128 via 2001:DB8:0:100::B
Tunnel0 created 22:27:52, expire 00:03:39
Type: dynamic, Flags: unique registered
NBMA address: 2001:DB8:0:FFFF:0:1:0:1

Hub1# show crypto session
Interface: Tunnel0; Session status: UP-ACTIVE
Peer: 2001:DB8:0:FFFF:0:1:0:1 port 500
IKEv2 SA: local 2001:DB8:0:FFFF:1::1/500
remote 2001:DB8:0:FFFF:0:1:0:1/500 Active
IPSEC FLOW: permit 47 host 2001:DB8:0:FFFF:1::1 host 2001:DB8:0:FFFF:0:1:0:1
Active SAs: 2, origin: crypto map
Routing Protocol Features – BGP

- **iBGP Local-AS** (15.2(2)T, 15.1(3)S (CSCtj48063))
  - Run iBGP over DMVPN
    - Tunnel end-point routers may have different native BGP ASs
    - Allows ‘neighbor ... local-as #’ and ‘neighbor ... remote-as #’ to be the same (iBGP)
    - ‘neighbor ... local-as #’ is different from local native BGP AS, ‘router bgp #’
      - Almost like eBGP within the router between the native AS and the AS over DMVPN
    - Also use BGP Dynamic Neighbors to reduce configuration on hub

```
router bgp 65000
  bgp listen range 10.0.0.0/24 peer-group spokes
  neighbor spokes peer-group
  neighbor spokes remote-as 65001
  neighbor spokes local-as 65001
```

- **BGP Dynamic Neighbors**
- **iBGP Local-AS**
Routing Protocol Features – EIGRP

- **Equal Cost MultiPath** (15.2(3)T, 15.2(1)S (CSCsj31328))
  - Destination network is reachable via more than one DMVPN (mGRE tunnel) and the ip next-hop needs to be preserved (Phase 2).

  ```
  no ip next-hop-self eigrp <as> [no-ecmp-mode]
  ```

- **Add-path** (15.3(1)S (CSCtw86791))
  - Spoke site has multiple DMVPN spoke routers and want to be able to load-balance spoke-spoke tunnels (Phase 2).
  - Requires new “named” EIGRP router configuration

  ```
  router eigrp <name>
  address-family ipv4 unicast autonomous-system 1
  af-interface Tunnel0
  no next-hop-self
  add-path <paths> (<paths> = number of extra paths)
  no split-horizon
  ```
Per-tunnel QoS – 12.4(22)T

- QoS per tunnel (spoke) on hub
  - Dynamically selected Hierarchical (parent/child) QoS Policy
    - **Spoke:** Configure NHRP group name
    - **Hub:** NHRP group name mapped to QoS template policy
  - Spokes with same NHRP group name are mapped to individual instances of the same QoS template policy
- QoS policy applied at outbound physical interface
  - Classification done before GRE encapsulation by tunnel
  - ACL matches against Data IP packet
  - Don’t configure ‘qos pre-classify’ on tunnel interface
  - Shaping/policing done on physical after IPsec encryption
  - Can’t have separate aggregate QoS policy on physical
- CPU intensive; reduces hub scaling by about 50%
Per-tunnel QoS – Configurations

**Hub**

```
class-map match-all typeA_voice
  match access-group 100
class-map match-all typeB_voice
  match access-group 100
class-map match-all typeA_Routing
  match ip precedence 6
class-map match-all typeB_Routing
  match ip precedence 6

policy-map typeA
  class typeA_voice
    priority 1000
  class typeA_Routing
    bandwidth percent 20

policy-map typeB
  class typeB_voice
    priority percent 20
  class typeB_Routing
    bandwidth percent 10

policy-map typeA_parent
  class class-default
    shape average 3000000
    service-policy typeA

policy-map typeB_parent
  class class-default
    shape average 2000000
    service-policy typeB
```

**Hub (cont)**

```
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  ip nhrp map group typeA service-policy output typeA_parent
  ip nhrp map group typeB service-policy output typeB_parent
  ip nhrp redirect
  ip nhrp multicast 172.17.0.1
  ip nhrp map multicast 172.17.0.1
  ip nhrp nhs 10.0.0.1

interface Tunnel0
  ip address 10.0.0.11 255.255.255.0
  ip nhrp map group typeB service-policy output typeB_parent

interface Tunnel0
  ip address 10.0.0.12 255.255.255.0
  ip nhrp map group typeA service-policy output typeA_parent

interface Tunnel0
  ip address 10.0.0.13 255.255.255.0
  ip nhrp map group typeB service-policy output typeB_parent
```

**Spoke1**

```
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  ip nhrp map group typeA service-policy output typeA_parent
```

**Spoke2**

```
interface Tunnel0
  ip address 10.0.0.11 255.255.255.0
  ip nhrp group typeB
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
```

**Spoke3**

```
interface Tunnel0
  ip address 10.0.0.12 255.255.255.0
  ip nhrp group typeA
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
```

Spoke1

Spoke2

Spoke3
### Per-tunnel QoS – QoS Output

**Hub#show ip nhrp**

<table>
<thead>
<tr>
<th>Tunnel0 created</th>
<th>Type: dynamic, Flags: unique registered</th>
<th>NBMA address: 172.16.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.11/32 via 10.0.0.11</td>
<td>Flag: typeA</td>
<td></td>
</tr>
<tr>
<td>10.0.0.12/32 via 10.0.0.12</td>
<td>Flag: typeB</td>
<td></td>
</tr>
<tr>
<td>10.0.0.13/32 via 10.0.0.13</td>
<td>Flag: typeA</td>
<td></td>
</tr>
</tbody>
</table>

**Hub#show ip nhrp group-map**

<table>
<thead>
<tr>
<th>Interface: Tunnel0</th>
<th>NHRP group: typeA</th>
<th>QoS policy: typeA_parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel destination overlay/transport address</td>
<td>10.0.0.11/172.16.1.1</td>
<td></td>
</tr>
<tr>
<td>10.0.0.12/172.16.2.1</td>
<td>Flag: typeB</td>
<td></td>
</tr>
</tbody>
</table>

**Hub#show policy-map multipoint tunnel 0 <spoke> output**

<table>
<thead>
<tr>
<th>Interface Tunnel0</th>
<th>Service-policy output: typeA_parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-map: class-default (match-any)</td>
<td>19734 packets, 6667163 bytes</td>
</tr>
<tr>
<td>shape (average) cir 3000000, bc 12000, be 12000</td>
<td></td>
</tr>
</tbody>
</table>

**Service-policy : typeA**

| Class-map: typeA_voice (match-all) | 3737 packets, 4274636 bytes |
| Class-map: typeA_Routing (match-all) | 14424 packets, 1269312 bytes |
| Class-map: class-default (match-any) | 1573 packets, 1123215 bytes |

**Interface Tunnel0 | 172.16.2.1**

<table>
<thead>
<tr>
<th>Service-policy output: typeB_parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-map: class-default (match-any)</td>
</tr>
<tr>
<td>shape (average) cir 2000000, bc 8000, be 8000</td>
</tr>
</tbody>
</table>

**Service-policy : typeB**

| Class-map: typeB_voice (match-all) | 1005 packets, 128640 bytes |
| Class-map: typeB_Routing (match-all) | 10001 packets, 880088 bytes |
| Class-map: class-default (match-any) | 414 packets, 68170 bytes |

**Interface Tunnel0 | 172.16.3.1**

<table>
<thead>
<tr>
<th>Service-policy output: typeA_parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-map: class-default (match-any)</td>
</tr>
<tr>
<td>shape (average) cir 3000000, bc 12000, be 12000</td>
</tr>
</tbody>
</table>

**Service-policy : typeA**

| Class-map: typeA_voice (match-all) | 4914 packets, 4734392 bytes |
| Class-map: typeA_Routing (match-all) | 523 packets, 46004 bytes |
| Class-map: class-default (match-any) | 21 packets, 14995 bytes |