12. DMVPN mit mGRE und NHRP

In diesem Kapitel erfahren Sie

- wie mulltiple VPN Verbindungen dynamisch verwaltet werden können
- warum eine virtuelle Hub & Spoke Topologie für die virtuelle Topologie verwendet werden muss
- wie mGRE für multipoint Verbindungen eingesetzt wird und welche Aufgaben NHRP dabei übernimmt
- wie DMVPN Funktionalität in Phasen unterteilt wird
- wie DMVPN für IPv4 und IPv6 konfiguriert und verifiziert wird

DMVPN Überblick

In einer fully-meshed VPN Topologie kann der Konfigurationsaufwand für VPN Verbindungen – jeder mit jedem - sehr komplex werden .. und damit schwer zu adminstrieren und zu überwachen.

In einer Hub & Spoke (partial-meshed) VPN Topology, in der alle Standorte (Spokes) eine Verbindung zur Zentrale (Hub) haben – aber nicht untereinander – muss Datenverkehr zwischen den Standorten immer über die Zentrale weitergeleitet werden:

1. Tunnel vom "Sender"-Spoke zum Hub und
2. Tunnel vom Hub zum "Empfänger"-Spoke

DMVPN kann in Hub & Spoke VPN Topologien direkte, dynamische L3 Tunnelverbindungen zwischen Standorten (spoke-to-spoke IPSec Tunnel) aufbauen, wenn diese benötigt werden .. d.h. wenn remote sites miteinander kommunizieren möchten.

DMVPN verwendet dazu folgende Funktionalitäten

- **mGRE** – multipoint GRE (notwendig)
  → multiple Tunnelverbindungen über ein einzelnes Tunnel Interface

- **NHRP** – Next-Hop Resolution Protocol (notwendig)
  → dynamische Ermittlung der realen "outside" IP Adressen aller beteiligten Router

- **IPSec** – IP Security (optional)
  → Verschlüsselung und Authentication

- **Dynamisches Routing** (optional)
  → NUR EIGRP (best choice), OSPF und BGP nutzbar – nicht RIP, nicht IS-IS
  → ACHTUNG OSPF: network type non-broadcast auf tunnel IF verwenden (und neighbor Konfiguration durchführen) .. sonst keine Aufbau der dynamischen Tunnel.

Klassische DMVPN Arbeitsweise

- Jeder Spoke hat einen permanenten IPSec Tunnel zum Hub Router.

- Jeder Spoke registriert sich als Client des NHRP Server (der Hub Router)

- Wenn ein Spoke Datenverkehr an einen anderen Spoke weiterleiten muss (über ein Tunnel Interface routen muss), erfragt er die reale "outside" IP Adresse des Spokes beim NHRP Server (NHRP query).

- Nach Erhalt der Antwort vom NHRP Server, kann der Spoke einen dyamischen IPSec Tunnel zum remote Spoke aufbauen – er kennt jetzt die Tunnel DST IP.

- Der Spoke-to-Spoke Tunnel wird über das mGRE Interface aufgebaut, immer wenn Datenverkehr zwischen den Spokes übertragen werden muss.

- Nach Aufbau des Spoke-to-Spoke Tunnels werden die Pakete nicht mehr über den Hub weitergeleitet, sondern über den direkten Tunnel übertragen.
  ACHTUNG: Die Lebensdauer des Tunnels (default 300 Sekunden) kann mit folgendem Kommando – identisch auf allen VTIs aller Router - verändert werden:
  (config-if)# **ip nhrp holdtime** <1-65535>

mGRE – multipoint GRE

Eigenschaften
- Erlaubt multiple GRE Tunnel auf einem einzelnen GRE Tunnel Interface
- Stellt die gleichen Funktionen wie GRE zur Verfügung
- Kann dynamisch Tunnel aufbauen
  → unter Verwendung von NHRP, um die IP Adresse(n) des/der Tunnelendpunktes/ten zu ermitteln (tunnel destination)
- Reduziert administrativen Aufwand

mGRE kann wie folgt verwendet werden:
- **hub-and-spoke topology** (DMVPN Phase 1)
  NUR der Hub Router verwendet ein mGRE Interface – die Spokes ein GRE Interface
  → die Spoke Router können nicht direkt miteinander kommunizieren

- **spoke-to-spoke topology** (DMVPN Phase 2 und 3)
  ALLE beteiligten Router verwenden ein mGRE Interface (dynamischer Aufbau von Tunneln zwischen den spokes)
  → die Spoke Router können direkt miteinander kommunizieren

NHRP – Next Hop Resolution Protocol

Auf allen beteiligten Routen muss NHRP aktiv sein.
NHRP verwendet ein Client/Server Modell
- Hub Router → Server
- Spoke Router (remote) → Clients.

Spoke Router kennen die IP Adresse des Hub (durch Konfiguration).

Ist der Hub erreichbar, senden Spokes folgende Informationen an den Hub:
- die physikalische IP (tunnel source) .. kann natürlich auch ein virtuelles (dialer, loopback) oder logisches Interface (SubIF) sein .. der Router muss über diese IP via WAN erreichbar sein.
- die virtuelle IP (tunnel IP address) auf dem virtuellen Tunnel Interface

Diese Informationen verwaltet der Hub Router (NHRP Server) innerhalb seiner NHRP Database.

Ablauf
1. Will ein Spoke mit einem anderen Spoke kommunizieren (via dynamischem Tunnel) erfragt er die physikalische IP Adresse des anderen Spoke beim Hub Router – NHRP query.
2. Der Hub Router überprüft seine NHRP Database, die alle physikalischen und virtuellen Tunnel IP Adressen beinhaltet, und sendet die physikalische IP des "anderen" Spoke an den Fragesteller-Spoke zurück.
3. Jetzt kann der Spoke einen dynamischen Tunnel zum andern Spoke aufbauen.

Troubleshooting

    # **show ip nhrp**

    Zeigt Tunnel SRC IP (NBMA Adress) der Tunnelendpunkte, Tunnel IP Adressen, Tunnelbezeichnung und Zeiten (wie lange existiert der Tunnel schon).
    Das authoritative Flag innerhalb der Ausgabe verweist auf den NHRP Server.

DMVPN Phasen, Konfiguration und Troubleshooting

Konfiguration und Funktionalität von DMVPN werden in 3 Phasen beschrieben.

Generelle Voraussetzung: **CEF** ist aktiv auf dem Router (ip cef, ipv6 cef).

Phase 1 (kann bei der Konfiguration ausgelassen werden)
→ in dieser Phase können Spoke Router nicht direkt miteinander kommunizieren,
→ sämtlicher Datenverkehr wird ausschliesslich über den Hub Router geroutet

- Hub Router → mGRE
- Spoke Router → GRE P2p

Phase 2
→ in dieser Phase können Spoke Router direkt miteinander kommunizieren

- Hub Router → mGRE
- Spoke Router → mGRE

→ Spoke-to-spoke Tunnel sind – nach erstmaligem dynamischem Aufbau - permanent aktiv
→ Datenverkehr zwischen Spokes wird direkt geroutet (Route aus dem Routing Prozess)

ACHTUNG OSPF: funktional mit folgenden Einstellungen
→ Hub wird DR (priority 100), Spokes nehmen an der Wahl nicht teil (priority 0)

- **ip ospf network broadcast**
- **ip ospf network non-broadcast** mit **neighbor** Konfiguration

ACHTUNG EIGRP: split-horizon und next-hop-self – NUR auf Hub - abschalten

- **no ip split-horizon eigrp** *as-nr*
- **no ip next-hop-self eigrp** *as-nr*

  EIGRP default → Routen werden mit der Next-Hop-IP auf dem lokalen, ausgehenden Interface propagiert. Durch Abschalten des default-Verhaltens wird EIGRP angewiesen, die empfangene Next-HOP-IP für eine Route zu verwenden.

Phase 3 (Erweiterung der Phase 2)
→ in dieser Phase werden die Spoke-to-Spoke Routen im Bedarfsfall dynamisch via NHRP an die Spokes verteilt
→ Datenverkehr zwischen Spokes wird – im Bedarfsfall – direkt geroutet
.. dann Darstellung in der Routing Tabelle: **%** (Next-Hop-Override Route)
show ip route next-hop-override

ACHTUNG OSPF: Mögliche Network Types

- **ip ospf network broadcast**
- **ip ospf network non-broadcast** mit **neighbor** Konfiguration,
- **ip ospf network point-to-multipoint**

ACHTUNG EIGRP: split-horizon und next-hop-self – NUR auf Hub - abschalten

- **no ip split-horizon eigrp** *as-nr*
- **no ip next-hop-self eigrp** *as-nr*

Generelle zusätzliche Konfiguration: Aktivierung der **IPSec** Protection für den Tunnel

Konfigurationsablauf: VTI Konfiguration für DMVPN PHASE 2/3

IM BEISPIEL verwendet IP Adressen:

- HUB Router:
  - IP auf physikalischer Verbindung → 42.42.42.42 (äusserer Header)
  - Tunnel IP → 172.16.1.42 (innerer Header)
- SPOKE Router 1:
  - IP auf physikalischer Verbindung → 1.1.1.1 (äusserer Header)
  - Tunnel IP → 172.16.1.1 (innerer Header)

HUB	**Spoke1**
VTI: Anlegen eines virtuellen Tunnel IF mit Tunnel IP (innerer Header) für NBMA	
interface tunnel 0 ip address 172.16.1.42 255.255.255.0	interface tunnel 0 ip address 172.16.1.1 255.255.255.0
NHRP Einstellungen (Phase 2) • Network ID • Mapping HUB: nur dynamisches Mapping • Mapping Spokes: statisches Mapping (zum Hub) auch für Multicast (Tunnel DST IP) .. .. und Angabe des NRRP Next-Hop-Server (nhs – auch der Hub: Tunnel IP) • Authentication: immer sinnvoll, aber optional HINWEiS zur Vollständigkeit: optionales "ip nhrp holdtime *sec*" macht manchmal Probleme ..	
ip nhrp network-id 42 ip nhrp map multicast dynamic ip nhrp authentication cisco	ip nhrp network-id 42 ip nhrp map 172.16.1.42 42.42.42.42 ip nhrp map multicast 42.42.42.42 ip nhrp nhs 172.16.1.42 ip nhrp authentication cisco
NHRP Einstellungen (Phase 3) Obligatorisch für dynamisches Routing zwischen Spokes via NHRP	
ip nhrp redirect	ip nhrp shortcut
Tunneleinstellungen (Phase2/Phase3) Phase 2/3: Tunnel Source (äusserer Header) und Tunnel Mode (mGRE für Hub und Spoke) .. ACHTUNG: keine Tunnel DST – diese wird über NHRP jeweils automatisch ermittelt Hinweis f. Phase 1: Spokes (GRE P2p) → tunnel destination (42.42.42.42) , tunnel mode gre	
tunnel source 1.1.1.1 tunnel mode gre multipoint	tunnel source 42.42.42.42 tunnel mode gre multipoint
Optional: **IPSec Absicherung** der Tunnel → die erforderliche IPSec Konfiguration (ISAKMP Policy und PSK, IPSec Transform-set und Profile) ist hier nicht dargestellt .. siehe Beispielkonfiguration DMVPN auf den nächsten Seiten	
tunnel protection ipsec profile IPSECPROFILE end	tunnel protection ipsec profile IPSECPROFILE end

Troubleshooting DMVPN

Informationen zu den DMVPN Verbindungen

show dmvpn [**detail**]

show dmvpn | **begin** Interface
show dmvpn | **include** IKE

debug dmvpn all all
debug dmvpn ?

Informationen zu NHRP

show ip nhrp
show ip nhrp traffic

debug nhrp
debug nhrp routing
debug nhrp condition { **interface** | **peer** | **vrf** } *params*

Logmeldungen bei NHRP Ereignissen aktivieren

(config)# **logging dmvpn**

IPSec Informationen

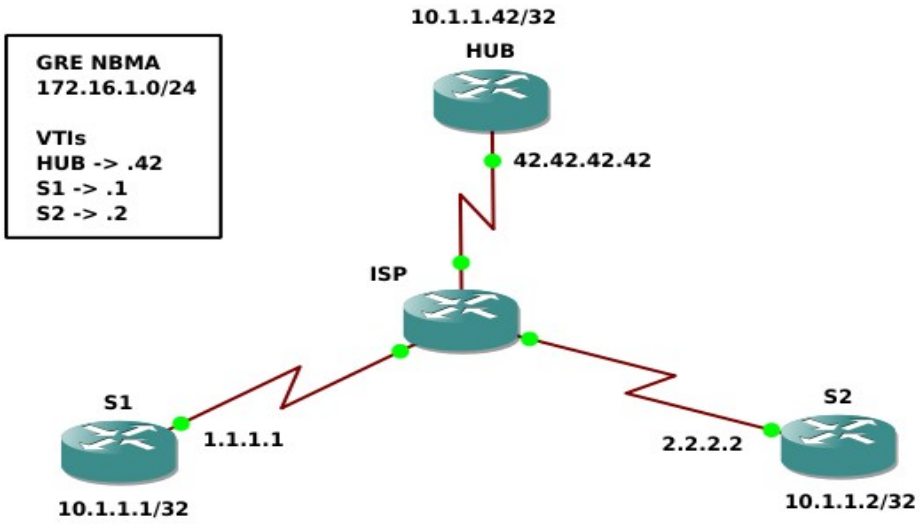
show crypto ipsec sa
show crypto isakmp sa

Routing Tabellen

show ip route *prefix* **longer-prefixes**
show ip route next-hop-override

DMVPN Beispielkonfiguration

DMVPN Phase 3 .. mit IPSec Protection



Konfigurationsanforderungen (chronologisch)

- VORAUSSETZUNGEN SCHAFFEN
  Schnittstellen für Tunnelendpunkte – und lokale Schnittstellen – einrichten
  .. und Erreichbarkeit der Tunnelendpunkt IP Adressen durch **statisches Routing** garantieren

- DMVPN Konfiguration
  - **IPSec** Parameter definieren
    - ISAKMP Policy
    - ISAKMP Key
    - IPSec Transform Set .. mit IPSec Mode Transport
    - IPSec Profile
  - **VTIs** einrichten
    - IP Adresse → IP Adresse für die virtuelle Tunnelverbindung
    - MTU, adjust-mss → Fragmentierungen vermeiden
    - NHRP Einstellungen
      - Net-ID → identisch auf allen Routern notwendig
      - Mapping → Hub: nur dynamisch, Spokes: statisch zum Hub + Angabe NHS
      - Authentication → optional aber empfehlenswert
      - Holdtime → optional
      - redirect/shortcut → notwendig für DMVPN Phase 3
    - Tunnel Einstellungen
      - Source → Angabe des Tunnelendpunkt IFs oder der Tunnelendpunkt IP
      - Mode (mGRE) → auf Hub .. und Spokes (notwendig für Phase 2)
      - PMTUD → Fragmentierungsprobleme auf Tunnelverbindung vermeiden
      - IPSec Protection → Authentication/Encryption für die Tunnelverbindung
    - Einstellungen für das verwendete Routing Protokoll

- **Routing Protokoll** auf VTI aktivieren

Hub	S1
Interfaces und Tunnelendpunkt Routing	
! int lo 0 ip address 10.1.1.42 255.255.255.255 ! int ser 3/0 desc ISP bandwidth 8064 enc ppp ip address 42.42.42.42 255.255.255.252 no shut ! ip route 0.0.0.0 0.0.0.0 42.42.42.41 !	! int lo 0 ip address 10.1.1.1 255.255.255.255 ! int ser 3/0 desc ISP bandwidth 8064 enc ppp ip address 1.1.1.1 255.255.255.252 no shut ! ip route 0.0.0.0 0.0.0.0 1.1.1.2 !
IPSec	
! crypto isakmp policy 1 authentication pre-share enc aes 256 hash sha256 group 5 ! crypto isakmp key cisco address 0.0.0.0 ! crypto ipsec transform-set TS ah-md5-hmac esp-aes 256 mode transport ! crypto ipsec profile DMVPN set transform-set TS !	! crypto isakmp policy 1 authentication pre-share enc aes 256 hash sha256 group 5 ! crypto isakmp key cisco address 0.0.0.0 ! crypto ipsec transform-set TS ah-md5-hmac esp-aes 256 mode transport ! crypto ipsec profile DMVPN set transform-set TS !
VTI	
int tunnel 0 ip address 172.16.1.42 255.255.255.0 ip mtu 1400 ip tcp adjust-mss 1360 ip nhrp network-id 42 ip nhrp map multicast dynamic ip nhrp authentication cisco ip nhrp redirect tunnel source serial 3/0 tunnel mode gre multipoint tunnel path-mtu-discovery tunnel protection ipsec profile DMVPN ip ospf network point-to-multipoint no ip split-horizon eigrp 1 no ip next-hop-self eigrp 1 !	! int tunnel 0 ip address 172.16.1.1 255.255.255.0 ip mtu 1400 ip tcp adjust-mss 1360 ip nhrp network-id 42 ip nhrp map 172.16.1.42 42.42.42.42 ip nhrp map multicast 42.42.42.42 ip nhrp nhs 172.16.1.42 ip nhrp authentication cisco ip nhrp shortcut tunnel source serial 3/0 tunnel mode gre multipoint tunnel path-mtu-discovery tunnel protection ipsec profile DMVPN ip ospf network point-to-multipoint !
DMVPN Routing → nur OSPF oder EIGRP möglich (nachfolgend OSPF) → OSPF ist aktiv auf Tunnel IF und Loopback – NICHT auf dem Tunnelendpunkt Interface	
! router ospf 1 ! interface loopback 0 ip ospf 1 area 0 ! interface tunnel 0 ip ospf 1 area 0 !	! router ospf 1 ! interface loopback 0 ip ospf 1 area 0 ! interface tunnel 0 ip ospf 1 area 0 !

DMVPN und IPv6

DMVPN kann auch mit IPv6 verwendet werden.

HINWEISE:
- Die Konfiguration ist nahezu identisch mit der IPv4 DMVPN Konfiguration.
- Es muss nur genau 1 dual-stack VTI konfiguriert werden
- Als interne Routing Protokolle sind OSPFv3 und EIGRP verwendbar (das externe Routing Protokoll BGP wird auch unterstützt).

Voraussetzung
IPv6 Routing und IPv6 CEF sind aktiv

```
!
ipv6 unicast-routing
ipv6 cef
!
```

IPv6 Tunnel Einstellungen: IPv6 MTU, IPv6 Adressing, IPv6 NHRP, OSPFv3
→ HINWEIS: bei Problemen mgl. zusätzlichen einen identischen tunnel key konfigurieren.

HUB	SPOKE
interface tunnel *IF-ID* **ipv6 mtu** 1400 → IPv6 Adressierung **ipv6 address** *IPv6 link-local* **ipv6 address** *IPv6/prefix-length* → NHRP Network ID (obligatorisch) **ipv6 nhrp network-id** *ID* → NHRP Authentication (sinnvolll) **ipv6 nhrp authentication** *password* → NHRP Mapping (HUB nur dynamic) **ipv6 nhrp map multicast dynamic** → NHRP Phase 3 **ipv6 nhrp redirect** → OSPFv3 **ipv6 ospf network broadcast** **ipv6 ospf** *process-ID* **area** *area-ID*	**interface tunnel** *IF-ID* **ipv6 mtu** 1400 → IPv6 Adressierung **ipv6 address** *IPv6 link-local* **ipv6 address** *IPv6/prefix-length* → NHRP Network ID (obligatorisch) **ipv6 nhrp network-id** *ID* → NHRP Authentication (sinnvoll) **ipv6 nhrp authentication** *password* → NHRP Mapping (statisch zum HUB) **ipv6 nhrp map** *IPv6 IPv4* **ipv6 nhrp map multicast** *IPv4* **ipv6 nhrp nhs** *IPv6* → NHRP Phase 3 **ipv6 nhrp shortcut** → OSPFv3 **ipv6 ospf network broadcast** **ipv6 ospf** *process-ID* **area** *area-ID*

Troubleshooting IPv6 DMVPN .. eine Auswahl

```
# show dmvpn [ ipv4 | ipv6 ]
# show ipv6 nhrp
# show ipv6 route
# show ipv6 route shortcut
```

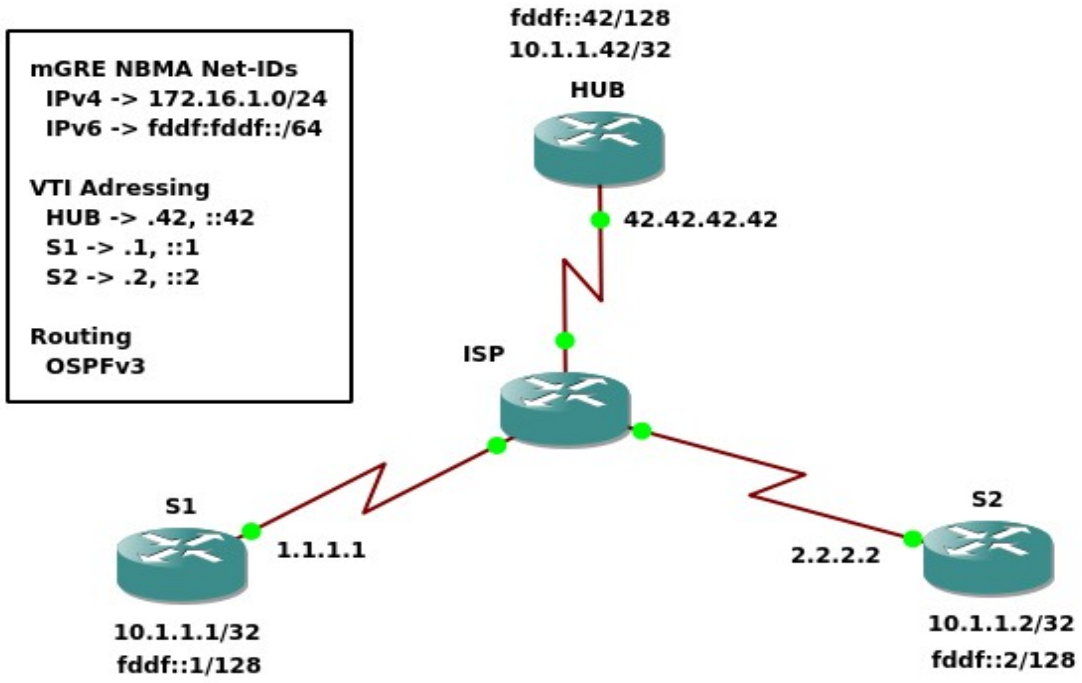
Dual-Stack DMVPN Beispielkonfiguration

Erweiterung des vorangegangenen Beispiels mit IPv6

HINWEISE zur Konfiguration (siehe nächste Seite)

- Dual-Stack IP Adressierung
- Manuelle Vergabe der IPv6 Link Local Adressen (immer sinnvoll, bessere Übersicht beim Troubleshooting) – identisch auf allen Interfaces
  - HUB → fe80::42
  - S1 → fe80::1
  - S2 → fe80::2
- Routing
  - IPv4 → OSPFv2
  - IPv6 → (traditional) OSPFv3
- Dual Stack DMVPN Phase 3 mit IPSec Protection

Topologie



Cisco Router 4

HUB	**S1**
!	!
ipv6 unicast-routing	ipv6 unicast-routing
ipv6 cef	ipv6 cef
!	!
crypto isakmp policy 1	crypto isakmp policy 1
encr aes 256	encr aes 256
hash sha256	hash sha256
authentication pre-share	authentication pre-share
group 5	group 5
!	!
crypto isakmp key cisco address 0.0.0.0	crypto isakmp key cisco address 0.0.0.0
!	!
crypto ipsec transform-set TS ah-md5-hmac esp-aes 256	crypto ipsec transform-set TS ah-md5-hmac esp-aes 256
mode transport	mode transport
!	!
crypto ipsec profile DMVPN	crypto ipsec profile DMVPN
set transform-set TS	set transform-set TS
!	!
interface Loopback0	interface Loopback0
ip address 10.1.1.42 255.255.255.255	ip address 10.1.1.1 255.255.255.255
ipv6 address FDDF::42/128	ipv6 address FDDF::1/128
ip ospf 1 area 0	ip ospf 1 area 0
ipv6 ospf 1 area 0	ipv6 ospf 1 area 0
!	!
interface Serial3/0	interface Serial3/0
description ISP	description ISP
ip address 42.42.42.42 255.255.255.252	ip address 1.1.1.1 255.255.255.252
encapsulation ppp	encapsulation ppp
!	!
interface Tunnel0	interface Tunnel0
ip address 172.16.1.42 255.255.255.0	ip address 172.16.1.1 255.255.255.0
no ip redirects	no ip redirects
ip mtu 1400	ip mtu 1400
ip nhrp authentication cisco	ip nhrp authentication cisco
ip nhrp map multicast dynamic	ip nhrp map 172.16.1.42 42.42.42.42
ip nhrp network-id 42	ip nhrp map multicast 42.42.42.42
ip nhrp redirect	ip nhrp network-id 42
ip tcp adjust-mss 1360	ip nhrp nhs 172.16.1.42
ip ospf network point-to-multipoint	ip nhrp shortcut
ip ospf 1 area 0	ip tcp adjust-mss 1360
ipv6 address FE80::42 link-local	ip ospf network point-to-multipoint
ipv6 address FDDF:FDDF::42/64	ip ospf 1 area 0
ipv6 nhrp authentication cisco	ipv6 address FE80::1 link-local
ipv6 nhrp map multicast dynamic	ipv6 address FDDF:FDDF::1/64
ipv6 nhrp network-id 642	ipv6 nhrp authentication cisco
ipv6 nhrp redirect	ipv6 nhrp map FDDF:FDDF::42/64 42.42.42.42
ipv6 ospf 1 area 0	ipv6 nhrp map multicast 42.42.42.42
ipv6 ospf network broadcast	ipv6 nhrp network-id 642
tunnel source Serial3/0	ipv6 nhrp nhs FDDF:FDDF::42
tunnel mode gre multipoint	ipv6 nhrp shortcut
tunnel path-mtu-discovery	ipv6 ospf 1 area 0
tunnel protection ipsec profile DMVPN	ipv6 ospf network broadcast
!	tunnel source Serial3/0
!	tunnel mode gre multipoint
!	tunnel path-mtu-discovery
!	tunnel protection ipsec profile DMVPN
!	!
ip route 0.0.0.0 0.0.0.0 42.42.42.41	ip route 0.0.0.0 0.0.0.0 1.1.1.2
!	!
router ospf 1	router ospf 1
!	!
ipv6 router ospf 1	ipv6 router ospf 1
!	!

Selbstkontrolle – Aufgaben und Übungen

1. Welche virtuelle WAN Topologie wird als grundlegende Topologie in DMVPN Netzen verwendet?

- ○ Fully meshed NBMA
- ○ Partial meshed NBMA
- ○ Partial meshed Hub & Spoke NBMA
- ○ Partial meshed Hub & Spoke P2p

2. Welche der folgenden Aussagen trifft zu?

- ☐ In DMVPN Phase 1 können Spoke Router permanent direkt miteinander kommunizieren
- ☐ In DMVPN Phase 2 können Spoke Router im Bedarfsfall (dynamisch) direkt miteinander kommunizieren
- ☐ In DMVPN Phase 2 können Spoke Router nicht direkt miteinander kommunizieren.
- ☐ In DMVPN Phase 1 können Spoke Router nicht direkt miteinander kommunizieren.
- ☐ In DMVPN Phase 3 können Spoke Router permanent direkt miteinander kommunizieren
- ☐ In DMVPN Phase 3 können Spoke Router im Bedarfsfall (dynamisch) direkt miteinander kommunizieren
- ☐ In DMVPN Phase 2 können Spoke Router permanent direkt miteinander kommunizieren

3. Welche Cisco Funktion muss auf einem Cisco Router aktiviert sein, damit DMVPN verwendet werden kann?

- ○ CEF
- ○ DTP
- ○ VNR
- ○ VRF

4. Welche Protokolle bzw. Funktionen müssen auf einem DMVPN Hub Router immer verwendet werden?

- ☐ GRE
- ☐ mGRE
- ☐ NHRP
- ☐ IPSec

5. Welche Information wird mittels NHRP ermittelt?

- ○ Tunnel NBMA IP
- ○ Tunnel Key ID
- ○ IPSec SA
- ○ mGRE Mode

6. Welcher Tunnel Mode muss für DMVPN Phase 3 Verbindungen auf allen beteiligten Dual Stack Routern verwendet werden?

- O gre ipv4 ipv6
- O mgre dual-stack
- O gre multipoint
- O mgre multipoint

7. Welche EIGRP Funktion auf einem Hub Router kann unvollständige Routing Tabellen auf Spoke Routern zur Folge haben und sollte deaktiviert werden?

- O variance
- O split horizon
- O dual
- O nssa

8. Welcher OSPF Network Type kann sowohl für IPv4 als auch für IPv6 Routing über DMVPN Strukturen verwendet werden? Notieren Sie das/die notwendige/n Kommando/s um den ensprechen OSPF network type auf dem VTI für IPv4 und IPv6 einzustellen.

9. Welche der folgenden Einstellungen auf einem VTI sind optional für eine Phase 3 Verbindung.

- ☐ NHRP Redirect Funkton für HUB aktivieren
- ☐ Aktivierung der NHRP Authentication auf Hub und Spokes
- ☐ Festlegung einer identischen NHRP Netzwerk ID auf Hub und Spokes
- ☐ Statisches NHRP Mapping zum HUB auf Spokes einrichten
- ☐ NHRP Shortcut Funktion für Spokes aktivieren
- ☐ Dynamische NHRP Mapping zu den Spokes auf HUB einrichten
- ☐ IPSec Protection auf Hub und Spokes aktivieren
- ☐ Routing Protokoll auf Hub und Spokes aktivieren

10. Notieren Sie das notwendige Kommando, um sich via NHRP ermittelte NBMA Adressen am Bildschirm anzeigen zu lassen.

11. Mit welchem Kommando können detaillierte Informationen zu DMVPN Verbindungen am Bildschirm angezeigt werden. Notieren Sie das Kommando.

Selbstkontrolle – Lösungen

1. Welche virtuelle WAN Topologie wird als grundlegende Topologie in DMVPN Netzen verwendet?

O Fully meshed NBMA
O Partial meshed NBMA
xO Partial meshed Hub & Spoke NBMA
O Partial meshed Hub & Spoke P2p

2. Welche der folgenden Aussagen trifft zu?

☐ In DMVPN Phase 1 können Spoke Router permanent direkt miteinander kommunizieren
☐ In DMVPN Phase 2 können Spoke Router im Bedarfsfall (dynamisch) direkt miteinander kommunizieren
☐ In DMVPN Phase 2 können Spoke Router nicht direkt miteinander kommunizieren.
x☐ In DMVPN Phase 1 können Spoke Router nicht direkt miteinander kommunizieren.
☐ In DMVPN Phase 3 können Spoke Router permanent direkt miteinander kommunizieren
x☐ In DMVPN Phase 3 können Spoke Router im Bedarfsfall (dynamisch) direkt miteinander kommunizieren
x☐ In DMVPN Phase 2 können Spoke Router permanent direkt miteinander kommunizieren

3. Welche Cisco Funktion muss auf einem Cisco Router aktiviert sein, damit DMVPN verwendet werden kann?

xO CEF
O DTP
O VNR
O VRF

4. Welche Protokolle bzw. Funktionen müssen auf einem DMVPN Hub Router immer verwendet werden?

☐ GRE
x☐ mGRE
x☐ NHRP
☐ IPSec

5. Welche Information wird mittels NHRP ermittelt?

xO Tunnel DST IP
O Tunnel Key ID
O IPSec SA
O mGRE Mode

6. Welcher Tunnel Mode muss für DMVPN Phase 3 Verbindungen auf allen beteiligten Dual Stack Routern verwendet werden?

- O gre ipv4 ipv6
- O mgre dual-stack
- xO gre multipoint
- O mgre multipoint

7. Welche EIGRP Funktion auf einem Hub Router kann unvollständige Routing Tabellen auf Spoke Routern zur Folge haben und sollte deaktiviert werden?

- O variance
- xO split horizon
- O dual
- O nssa

8. Welcher OSPF Network Type kann sowohl für IPv4 als auch für IPv6 Routing über DMVPN Strukturen verwendet werden? Notieren Sie das/die notwendige/n Kommando/s um den ensprechen OSPF network type auf dem VTI für IPv4 und IPv6 einzustellen.

ip ospf network broadcast
ipv6 ospf network broadcast

9. Welche der folgenden Einstellungen auf einem VTI sind optional für eine Phase 3 Verbindung.

- x☐ NHRP Redirect Funkton für HUB aktivieren
- ☐ Aktivierung der NHRP Authentication auf Hub und Spokes
- x☐ Festlegung einer identischen NHRP Netzwerk ID auf Hub und Spokes
- x☐ Statisches NHRP Mapping zum HUB auf Spokes einrichten
- x☐ NHRP Shortcut Funktion für Spokes aktivieren
- x☐ Dynamische NHRP Mapping zu den Spokes auf HUB einrichten
- ☐ IPSec Protection auf Hub und Spokes aktivieren
- ☐ Routing Protokoll auf Hub und Spokes aktivieren

10. Notieren Sie das notwendige Kommando, um sich via NHRP ermittelte NBMA Adressen am Bildschirm anzeigen zu lassen.

 # show ip nhrp

11. Mit welchem Kommando können detaillierte Informationen zu DMVPN Verbindungen am Bildschirm angezeigt werden. Notieren Sie das Kommando.

 # show dmvpn detail