# Настройка Dynamic Multipoint VPN (DMVPN) на маршрутизаторах Cisco

Наташа Самойленко

*Сетевые Дни*

# Типы VPN в Cisco

# Типы VPN в Cisco

**Site-to-Site VPN:**

- VPN с crypto-map
- Static VTI
- Dynamic VTI
- **DMVPN**
- FlexVPN

**Remote VPN:**

- EasyVPN*
- SSLVPN

# DMVPN. Технологии и протоколы

# Составляющие DMVPN

**В основе DMVPN лежат несколько технологий:**

- mGRE-туннели
- Протокол NHRP (Next Hop Resolution Protocol)
- Протоколы динамической маршрутизации
- IPsec

# Преимущества DMVPN

- Поддерживает передачу:
  - IPv4/IPv6 unicast, multicast
  - Динамические протоколы маршрутизации
- DMVPN позволяет использовать динамически назначенные IP-адреса на spoke-маршрутизаторах
- Если двум spoke-маршрутизаторам необходимо установить туннель напрямую, то он устанавливается динамически
- Может использоваться без IPsec
- При добавлении новых маршрутизаторов в существующую сеть DMVPN, необходимо настроить только новый маршрутизатор, изменений на уже существующих маршрутизаторах не требуется
- Поддерживает разные варианты дизайна

# Multipoint GRE

# Multipoint GRE

Multipoint GRE (mGRE) – туннель, который позволяет терминировать на себе несколько GRE-туннелей:

- mGRE-туннель позволяет одному GRE-интерфейсу поддерживать несколько туннелей и упрощает количество и сложность настроек, по сравнению с GRE-туннелями точка-точка

# Next Hop Resolution Protocol (NHRP)

# Next Hop Resolution Protocol (NHRP)

Next Hop Resolution Protocol (NHRP):

- клиент-серверный протокол преобразования адресов
- позволяет всем клиентам, которые находятся в NBMA(Non Broadcast Multiple Access)-сети, динамически выучить NBMA-адреса (физические адреса) друг друга обращаясь к next-hop-серверу (NHS)
- После этого клиенты могут обмениваться информацией друг с другом напрямую

# Next Hop Resolution Protocol (NHRP)

В сети DMVPN:

- Hub-маршрутизатор будет работать как NHS (Next-hop Server), а spoke-маршрутизаторы будут клиентами.
- Hub-маршрутизатор хранит и обслуживает базу данных NHRP, в которой хранятся соответствия между физическими адресами и адресами mGRE-туннелей spoke-маршрутизаторов.
- На каждом spoke-маршрутизаторе hub-маршрутизатор статически указан как NHS и задано соответствие между физическим адресом и адресом mGRE-туннеля hub-маршрутизатора.
- При включении каждый spoke-маршрутизатор регистрируется на NHS и, при необходимости, запрашивает у сервера информацию об адресах других spoke-маршрутизаторов для построения spoke-to-spoke туннелей.

# Сообщения NHRP

- **Registration**
  - С помощью этих сообщений заполняется база на NHS и строится базовая топология Hub-and-Spoke
- **Resolution**
  - Получение соответствия адресов, для построения динамических туннелей spoke-spoke
- **Traffic Indication (Redirect)**
  - Пересылает запрос о получении соответствия
- **Purge**
  - Удаляет истекшие динамические записи NHRP
- **Error**
  - Сигнализирует об ошибках

# Протоколы маршрутизации

# Протоколы маршрутизации

Рекомендуемые протоколы маршрутизации для использования с DMVPN:

- EIGRP
- BGP

Могут использоваться также:

- OSPF (есть ограничения)
- RIP

IS-IS не может использоваться в DMVPN

# Протоколы маршрутизации

- С точки зрения протоколов маршрутизации, Hub сосед spoke
- Spoke анонсируют свои локальные сети Hub
- Hub анонсирует свои локальные сети и сети Spoke другим Spoke
- Особенности по фазам:
  - Phase 1 и Phase 3:
    - Hub может суммировать сети
  - Phase 2:
    - На Hub нельзя выполнять суммирование
    - OSPF поддерживает только 2 Hub
- Связь Hub – Hub
  - Phase 1, 3:
    - Хабы могут использовать другой интерфейс и протокол маршрутизации для связи между собой
  - Phase 2:
    - Хабы должны использовать между собой  тот же интерфейс и протокол маршрутизации, что и для связи со spoke

# Дистанционно-векторные протоколы

EIGRP

- Как дистационно-векторный протокол подходит лучше под схему DMVPN
- Функционал EIGRP Stub
- Масштабируется до большого количества Spokes
- Легкое управление метрикой

BGP

- Как дистационно-векторный протокол подходит лучше под схему DMVPN
- Рекомендуется iBGP
- MED используется для управления маршрутами
- По умолчанию медленная сходимость

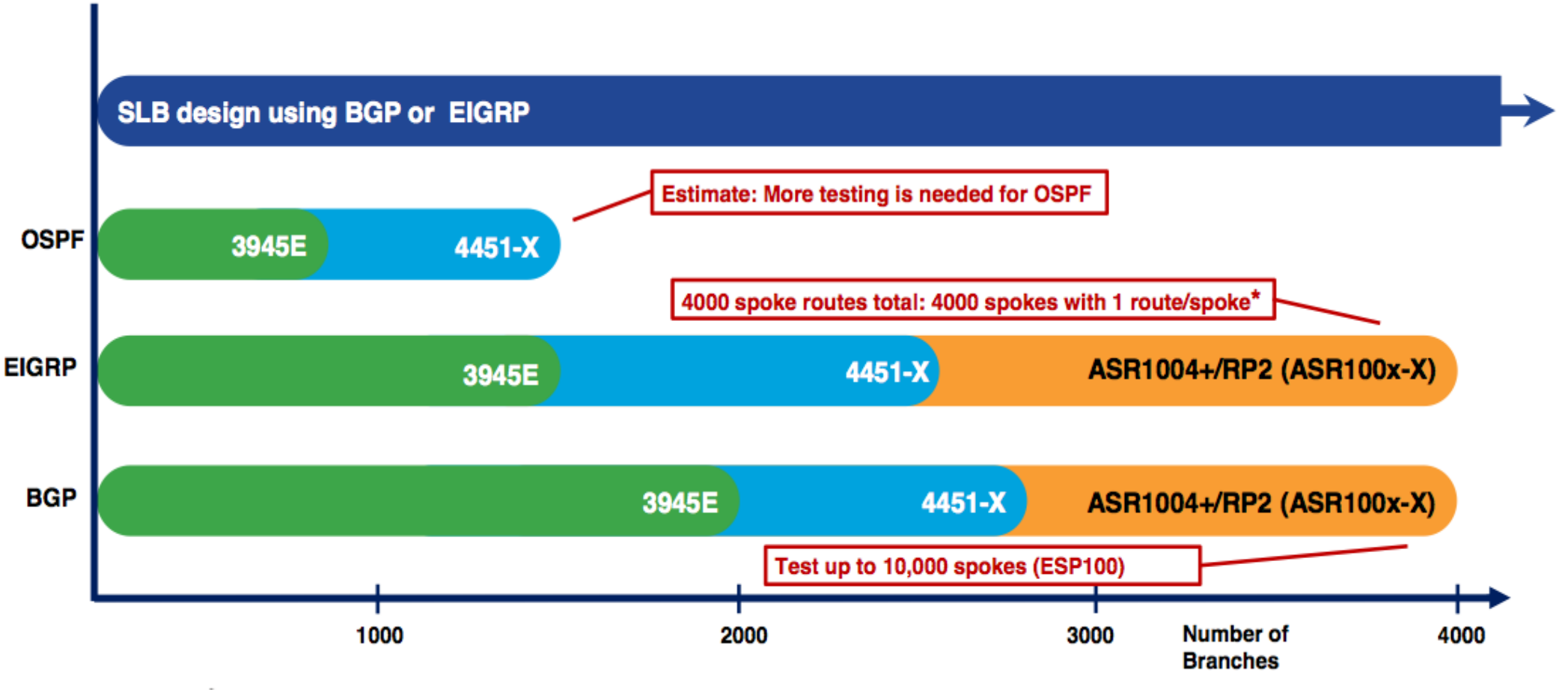
# OSPF

- Link-state хуже подходит под структуру сети DMVPN
- Сеть DMVPN должна быть в одной зоне (Area)
- При большом количестве Spoke лучше выбрать другой протокол

Дизайн OSPF:

- Area 0 в DMVPN
  - Spoke могут быть в других зонах
  - Если Spoke в зоне 0, то возможны проблемы со стабильностью работы зоны 0
- Ненулевая зона в DMVPN
  - Все Spoke в одной и той же зоне
- Можно разделить облако DMVPN на несколько подсетей
  - Усложняет дизайн OSPF и DMVPN

# Routing Protocol Scaling




Источник: BRKSEC-4054 Advanced Concepts of DMVPN

# IPsec

# IP Security (IPsec)

IPsec – это набор протоколов использующийся для обеспечения сервисов приватности и аутентификации на сетевом уровне.

Протоколы можно разделить на два класса:

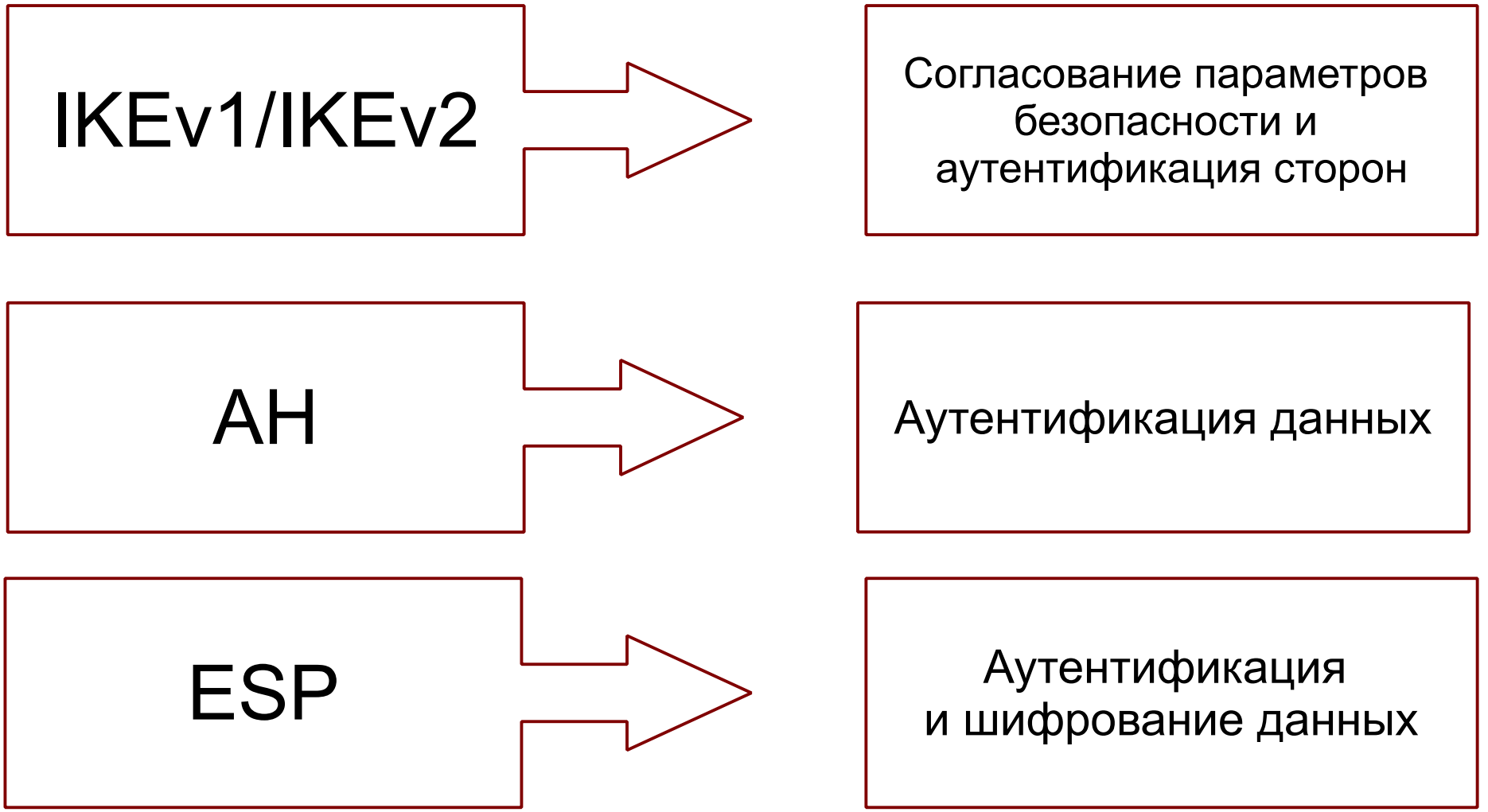
- протоколы защиты передаваемых данных
  - AH
  - ESP
- протоколы обмена ключами*
  - IKEv1
  - IKEv2

# IP Security (IPsec)

Для работы DMVPN настройка IPsec опциональна, но, как правило, DMVPN используется с IPsec:

- Поддерживаются IKEv1 и IKEv2
- Пакеты инкапсулируются в GRE, а потом шифруются IPsec
- Поднятие туннеля:
  - NHRP сигнализирует IPsec о необходимости поднять туннель
  - IKEv1/IKEv2 аутентифицируют маршрутизаторы, генерируются SA
  - Поднимается туннель IPsec
  - Пакеты NHRP и данные шифруются
- Удаление туннеля
  - NHRP сигнализирует IPsec о необходимости удалить туннель
  - DPD может также сигнализировать о потере связи с маршрутизатором
  - Туннель очищен вручную

# IP Security (IPsec)



# Фазы DMVPN

# Фазы DMVPN

DMVPN развивался постепенно, поэтому, в зависимости от версии IOS, его функционал и поведение могут отличаться. Этапы развития DMVPN называются фазами:

- **Phase 1**
  - Hub mGRE
  - Spoke P2P GRE
- **Phase 2**
  - Hub & Spoke mGRE
- **Phase 3**
  - Hub & Spoke mGRE
  - Иерархический DMVPN, NHRP redirect и shortcut

# Настройка DMVPN Phase 1

# DMVPN Phase 1

DMVPN Phase 1:

- Только на хабе настраивается mGRE, а на spoke p2p GRE
- Трафик между spoke ходит через Hub
- Возможности строить туннели spoke-to-spoke нет
- На spoke можно отправлять только маршрут по умолчанию или суммарный маршрут

# Настройка DMVPN Phase 1 без IPsec

# DMVPN Phase 1 без IPsec

DMVPN можно настраивать и использовать без включения IPsec. Это позволяет проверить работу:

- протоколов маршрутизации
- NHRP
- mGRE, p2p GRE

Исключение IPsec из списка “подозреваемых” очень упрощает процесс поиска неисправностей.

Для туннеля настройки IPsec сосредоточены в IPsec profile:

- Так как к тунельным интерфейсам ipsec profile применяется одной командой, его легко отменить и проверить работу DMVPN без IPsec

# Настройка DMVPN Hub Phase 1

# DMVPN Hub Phase 1 (R1)

```
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

# DMVPN Hub Phase 1 (R1)

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0

 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5

 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 ip nhrp authentication cisco100

 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

# Настройка DMVPN Spoke Phase 1

# DMVPN Spoke Phase 1 (R3)

```
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
 eigrp stub connected
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

# DMVPN Spoke Phase 1 (R3)

```
interface Tunnel3
 ip address 10.0.0.3 255.255.255.0

 ip nhrp nhs 10.0.0.1
 ip nhrp map 10.0.0.1 16.0.0.1
 ip nhrp map multicast 16.0.0.1
 ip nhrp network-id 100
 ip nhrp authentication cisco100

 tunnel source FastEthernet0/0
 tunnel destination 16.0.0.1
 tunnel key 100

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

# DMVPN Spoke Phase 1 (R4)

```
interface FastEthernet0/0
 ip address 48.0.0.4 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.4.4.4 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
 eigrp stub connected
!
ip route 0.0.0.0 0.0.0.0 48.0.0.8
```

# DMVPN Spoke Phase 1 (R4)

```
interface Tunnel4
 ip address 10.0.0.4 255.255.255.0

 ip nhrp nhs 10.0.0.1
 ip nhrp map 10.0.0.1 16.0.0.1
 ip nhrp map multicast 16.0.0.1
 ip nhrp network-id 100
 ip nhrp authentication cisco100

 tunnel source FastEthernet0/0
 tunnel destination 16.0.0.1
 tunnel key 100

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

# Проверка DMVPN Phase 1 (без IPsec)

# DMVPN Hub mGRE Tunnel (R1)

```
r1#sh int tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.0.1/24
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 16.0.0.1 (FastEthernet0/0)
   Tunnel Subblocks:
      src-track:
       Tunnel1 source tracking subblock associated with Fa0/0
           Set of tunnels with source Fa0/0, 1 member
(includes iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key 0x64, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
```

# DMVPN Spoke P2P GRE Tunnel (R3)

```
r3#sh int tunnel 3
Tunnel3 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.0.3/24
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 38.0.0.3 (FastEthernet0/0), destination
16.0.0.1
   Tunnel Subblocks:
     src-track:
       Tunnel3 source tracking subblock associated with Fa0/0
          Set of tunnels with source Fa0/0, 1 member
(includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key 0x64, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1472 bytes
```

# DMVPN routing

**r1#sh ip route eigrp**

```
Gateway of last resort is 16.0.0.6 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D        10.3.3.0/24 [90/1561600] via 10.0.0.3, 00:01:10, Tunnel1
D        10.4.4.0/24 [90/1561600] via 10.0.0.4, 00:33:02, Tunnel1
D        10.5.5.0/24 [90/1561600] via 10.0.0.5, 00:33:02, Tunnel1
```

**r3#sh ip route eigrp**

```
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D        10.1.1.0/24 [90/1561600] via 10.0.0.1, 00:00:09, Tunnel3
D        10.4.4.0/24 [90/2841600] via 10.0.0.1, 00:00:09, Tunnel3
D        10.5.5.0/24 [90/2841600] via 10.0.0.1, 00:00:09, Tunnel3
```

# DMVPN Hub NHRP (R1)

```
r1#sh ip nhrp
10.0.0.3/32 via 10.0.0.3
   Tunnel1 created 17:03:28, expire 01:38:05
   Type: dynamic, Flags: unique registered used
   NBMA address: 38.0.0.3
10.0.0.4/32 via 10.0.0.4
   Tunnel1 created 16:51:30, expire 01:48:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 48.0.0.4
10.0.0.5/32 via 10.0.0.5
   Tunnel1 created 00:00:24, expire 01:59:35
   Type: dynamic, Flags: unique registered used
   NBMA address: 58.0.0.5
```

```
r1#sh ip nhrp brief
   Target     Via         NBMA        Mode   Intfc  Claimed
10.0.0.3/32   10.0.0.3    38.0.0.3    dynamic  Tu1     <   >
10.0.0.4/32   10.0.0.4    48.0.0.4    dynamic  Tu1     <   >
10.0.0.5/32   10.0.0.5    58.0.0.5    dynamic  Tu1     <   >
```

# DMVPN Spoke NHRP (R3)

```
r3#sh ip nhrp
10.0.0.1/32 via 10.0.0.1
   Tunnel3 created 17:06:40, never expire
   Type: static, Flags:
   NBMA address: 16.0.0.1
```

```
r3#sh ip nhrp brief
   Target     Via        NBMA       Mode   Intfc   Claimed
10.0.0.1/32   10.0.0.1   16.0.0.1   static   Tu3      <   >
```

# DMVPN Hub DMVPN (R1)

```
r1#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R -->
Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1          38.0.0.3         10.0.0.3    UP 17:26:09     D
     1          48.0.0.4         10.0.0.4    UP 17:15:27     D
     1          58.0.0.5         10.0.0.5    UP 00:24:39     D
```

# DMVPN Hub DMVPN (R1)

```
r1#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.1, VRF ""
   Tunnel Src./Dest. addr: 16.0.0.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect ""
   Interface State Control: Disabled
   nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb  Target Network
----- --------------- --------------- ----- -------- ----- ---------------
    1       38.0.0.3        10.0.0.3    UP 17:28:16    D      10.0.0.3/32
    1       48.0.0.4        10.0.0.4    UP 17:17:35    D      10.0.0.4/32
    1       58.0.0.5        10.0.0.5    UP 00:26:47    D      10.0.0.5/32

Crypto Session Details:
--------------------------------------------------------------------------
Pending DMVPN Sessions:
```

# DMVPN Spoke DMVPN (R3)

```
r3#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R -->
Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================

Interface: Tunnel3, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1         16.0.0.1         10.0.0.1    UP 17:31:10     S
```

# DMVPN Spoke DMVPN (R3)

```
r3#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel3 is up/up, Addr. is 10.0.0.3, VRF ""
   Tunnel Src./Dest. addr: 38.0.0.3/16.0.0.1, Tunnel VRF ""
   Protocol/Transport: "GRE/IP", Protect ""
   Interface State Control: Disabled
   nhrp event-publisher : Disabled

IPv4 NHS:
10.0.0.1  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1       16.0.0.1        10.0.0.1    UP 17:31:59    S        10.0.0.1/32

Crypto Session Details:
--------------------------------------------------------------------------
Pending DMVPN Sessions:
```

# Настройка IPsec

# Настройка IPsec profile

# Hub, spokes IPsec profile

**Hub (R1):**

```
crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac
 mode transport

crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN

interface Tunnel1
 ...
 tunnel protection ipsec profile DMVPN_Profile
```

**Spoke (R3):**

```
crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac
 mode transport

crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN

interface Tunnel3
 ...
 tunnel protection ipsec profile DMVPN_Profile
```

# Настройка IKEv1 (ISAKMP)

# Hub, spokes IKEv1 (ISAKMP)

```
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 15

crypto isakmp key cisco12345 address 0.0.0.0 0.0.0.0
```

# Проверка DMVPN Phase 1 (IPsec + IKEv1)

# Hub (show dmvpn)

```
r1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R -->
Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1          38.0.0.3          10.0.0.3    UP 00:05:08     D
     1          48.0.0.4          10.0.0.4    UP 00:04:31     D
     1          58.0.0.5          10.0.0.5    UP 00:04:26     D
```

# Hub (show dmvpn detail)

```
r1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.1, VRF ""
   Tunnel Src./Dest. addr: 16.0.0.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_Profile"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1       38.0.0.3        10.0.0.3    UP 00:07:00    D        10.0.0.3/32

    1       48.0.0.4        10.0.0.4    UP 00:06:24    D        10.0.0.4/32

    1       58.0.0.5        10.0.0.5    UP 00:06:18    D        10.0.0.5/32
```

# Hub (show dmvpn detail) (продолжение)

```
Crypto Session Details:
-----------------------------------------------------------------------
Interface: Tunnel1
Session: [0xF251BA80]
  IKEv1 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:1001 lifetime:23:52:58
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 38.0.0.3
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 104 drop 0 life (KB/Sec) 4275379/3178
        Outbound: #pkts enc'ed 198 drop 0 life (KB/Sec) 4275366/3178
   Outbound SPI : 0x3279D993, transform : esp-aes esp-sha256-hmac
    Socket State: Open

Interface: Tunnel1
Session: [0xF251B890]
  IKEv1 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:1002 lifetime:23:53:34
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 48.0.0.4
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 92 drop 0 life (KB/Sec) 4306129/3214
        Outbound: #pkts enc'ed 92 drop 0 life (KB/Sec) 4306129/3214
   Outbound SPI : 0x54F95C20, transform : esp-aes esp-sha256-hmac
    Socket State: Open
```

# Hub (show crypto session)

```
r1#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv1 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 58.0.0.5 port 500
  IKEv1 SA: local 16.0.0.1/500 remote 58.0.0.5/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 58.0.0.5
        Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKEv1 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 2, origin: crypto map
```

# Hub (show crypto isakmp sa)

**r1#sh crypto isakmp sa**

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
16.0.0.1        58.0.0.5        QM_IDLE           1003 ACTIVE
16.0.0.1        38.0.0.3        QM_IDLE           1001 ACTIVE
16.0.0.1        48.0.0.4        QM_IDLE           1002 ACTIVE
```

**r1#sh crypto isakmp sa detail**

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local      Remote     I-VRF  Status Encr Hash   Auth DH Lifetime Cap.
1003  16.0.0.1   58.0.0.5          ACTIVE aes  sha256 psk  15 23:59:28
       Engine-id:Conn-id =  SW:3

1001  16.0.0.1   38.0.0.3          ACTIVE aes  sha256 psk  15 23:59:26
       Engine-id:Conn-id =  SW:1

1002  16.0.0.1   48.0.0.4          ACTIVE aes  sha256 psk  15 23:59:28
       Engine-id:Conn-id =  SW:2
```

# Настройка IKEv2

# Hub, spokes IKEv2

```
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco12345

crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring DMVPN

crypto ipsec profile DMVPN_Profile
 set ikev2-profile DMVPN_IKEv2*
```

* Если эта команда дана, то использоваться будет IKEv2, если же ее нет, то использоваться будет IKEv1 (ISAKMP)

# Проверка DMVPN Phase 1 (IPsec + IKEv2)

# Hub (show dmvpn)

```
r1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R -->
Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================
Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1          38.0.0.3          10.0.0.3    UP 00:05:08     D
     1          48.0.0.4          10.0.0.4    UP 00:04:31     D
     1          58.0.0.5          10.0.0.5    UP 00:04:26     D
```

# Hub (show dmvpn detail)

```
r1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.1, VRF ""
   Tunnel Src./Dest. addr: 16.0.0.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_Profile"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1       38.0.0.3        10.0.0.3    UP 00:07:00    D        10.0.0.3/32

    1       48.0.0.4        10.0.0.4    UP 00:06:24    D        10.0.0.4/32

    1       58.0.0.5        10.0.0.5    UP 00:06:18    D        10.0.0.5/32
```

# Hub (show dmvpn detail) (продолжение)

```
Crypto Session Details:
-----------------------------------------------------------------
Interface: Tunnel1
Session: [0xF26EA730]
  IKEv2 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
          Capabilities:(none) connid:1 lifetime:23:59:01
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 38.0.0.3
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 22 drop 0 life (KB/Sec) 4204612/4294967238
        Outbound: #pkts enc'ed 23 drop 0 life (KB/Sec) 4204612/4294967238
   Outbound SPI : 0xF6DEFD6E, transform : esp-aes esp-sha256-hmac
    Socket State: Open

Interface: Tunnel1
Session: [0xF26EA638]
  IKEv2 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:3 lifetime:23:59:00
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 48.0.0.4
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 22 drop 0 life (KB/Sec) 4303137/4294967237
        Outbound: #pkts enc'ed 25 drop 0 life (KB/Sec) 4303136/4294967237
   Outbound SPI : 0x143EA719, transform : esp-aes esp-sha256-hmac
    Socket State: Open
```

# Hub (show crypto session)

```
r1#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 48.0.0.4
        Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 58.0.0.5 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 58.0.0.5/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 58.0.0.5
        Active SAs: 4, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 38.0.0.3 port 500
  IKEv2 SA: local 16.0.0.1/500 remote 38.0.0.3/500 Active
  IPSEC FLOW: permit 47 host 16.0.0.1 host 38.0.0.3
        Active SAs: 4, origin: crypto map
```

# Hub (show crypto ikev2 session)

```
r1#sh crypto ikev2 session
 IPv4 Crypto IKEv2 Session

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:2

Tunnel-id Local           Remote          fvrf/ivrf    Status
1         16.0.0.1/500    38.0.0.3/500    none/none    READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/310 sec
Child sa: local selector  16.0.0.1/0 - 16.0.0.1/65535
          remote selector 38.0.0.3/0 - 38.0.0.3/65535
          ESP spi in/out: 0xC327B8CE/0xF6DEFD6E
Child sa: local selector  16.0.0.1/0 - 16.0.0.1/65535
          remote selector 38.0.0.3/0 - 38.0.0.3/65535
          ESP spi in/out: 0xD2B5B8C/0x89A661C0
```

# Настройка DMVPN Phase 2

# DMVPN Phase 2

DMVPN Phase 2:

- Hub и spoke используют mGRE
- Трафик между spoke ходит изначально через Hub
- При необходимости, поднимаются туннели spoke-to-spoke
- Для построения spoke-to-spoke туннелей, требуется чтобы:
  - hub не суммировал информацию о маршрутах
  - Маршруты приходили с next-hop spoke, а не hub

Недостатки Phase 2:

- Отсутствие суммирования может быть серьезной проблемой для масштабирования в крупных сетях, так как каждый spoke должен получать полную таблицу маршрутизации от других
- Первый пакет передается процессором, а не CEF
- Нельзя сделать иерархию хабов. Для крупных сетей это может быть существенным минусом

# Настройка DMVPN Hub Phase 2

# DMVPN Hub Phase 2 (R1)

```
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

# DMVPN Hub Phase 2 (R1)

```
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco12345

crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring DMVPN

crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac
 mode transport

crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
```

# DMVPN Hub Phase 2 (R1)

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0

 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1

 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 ip nhrp authentication cisco100

 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN_Profile

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

* нет команды ip summary-address eigrp

# Настройка DMVPN Spoke Phase 2

# DMVPN Spoke Phase 2 (R3)

```
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
 eigrp stub connected
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

# DMVPN Spoke Phase 2 (R3)

```
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco12345

crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring DMVPN

crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac
 mode transport

crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
```

# DMVPN Spoke Phase 2 (R3)

```
interface Tunnel3
 ip address 10.0.0.3 255.255.255.0

 ip nhrp nhs 10.0.0.1
 ip nhrp map 10.0.0.1 16.0.0.1
 ip nhrp map multicast 16.0.0.1
 ip nhrp network-id 100
 ip nhrp authentication cisco100

 tunnel source FastEthernet0/0
 tunnel key 100
 tunnel protection ipsec profile DMVPN_Profile
 tunnel mode gre multipoint

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

*нет команды tunnel destination

# Проверка DMVPN Phase 2

# DMVPN mGRE tunnel

**r1#sh interfaces tunnel 1**

```
 Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.0.1/24
  Tunnel source 16.0.0.1 (FastEthernet0/0)

  Tunnel protocol/transport multi-GRE/IP
```

**r3#sh interfaces tunnel 3**

```
 Tunnel3 is up, line protocol is up
  Internet address is 10.0.0.3/24
  Tunnel source 38.0.0.3 (FastEthernet0/0)

  Tunnel protocol/transport multi-GRE/IP
```

# DMVPN routing

**r1#sh ip route eigrp**

```
Gateway of last resort is 16.0.0.6 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D        10.3.3.0/24 [90/1561600] via 10.0.0.3, 00:01:10, Tunnel1
D        10.4.4.0/24 [90/1561600] via 10.0.0.4, 00:33:02, Tunnel1
D        10.5.5.0/24 [90/1561600] via 10.0.0.5, 00:33:02, Tunnel1
```

**r3#sh ip route eigrp**

```
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D        10.1.1.0/24 [90/1561600] via 10.0.0.1, 00:00:30, Tunnel3
D        10.4.4.0/24 [90/2841600] via 10.0.0.4, 00:00:30, Tunnel3
D        10.5.5.0/24 [90/2841600] via 10.0.0.5, 00:00:30, Tunnel3
```

# DMVPN Hub NHRP

```
r1#sh ip nhrp
10.0.0.3/32 via 10.0.0.3
   Tunnel1 created 00:28:52, expire 01:31:07
   Type: dynamic, Flags: unique registered
   NBMA address: 38.0.0.3
10.0.0.4/32 via 10.0.0.4
   Tunnel1 created 00:28:51, expire 01:31:08
   Type: dynamic, Flags: unique registered
   NBMA address: 48.0.0.4
10.0.0.5/32 via 10.0.0.5
   Tunnel1 created 00:28:50, expire 01:31:09
   Type: dynamic, Flags: unique registered
   NBMA address: 58.0.0.5
```

# DMVPN Spoke NHRP

```
r3#sh ip nhrp
10.0.0.1/32 via 10.0.0.1
   Tunnel3 created 00:30:31, never expire
   Type: static, Flags: used
   NBMA address: 16.0.0.1

r3#ping 10.4.4.13 source 10.3.3.3
r3#sh ip nhrp
10.0.0.1/32 via 10.0.0.1
   Tunnel3 created 00:00:39, never expire
   Type: static, Flags: used
   NBMA address: 16.0.0.1
10.0.0.3/32 via 10.0.0.3
   Tunnel3 created 00:00:05, expire 01:59:55
   Type: dynamic, Flags: router unique local
   NBMA address: 38.0.0.3
     (no-socket)
10.0.0.4/32 via 10.0.0.4
   Tunnel3 created 00:00:04, expire 01:59:55
   Type: dynamic, Flags: router implicit used
   NBMA address: 48.0.0.4
```

# DMVPN Spoke (sh dmvpn)

```
r3#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R -->
Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================

Interface: Tunnel3, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1         16.0.0.1         10.0.0.1    UP 00:03:08     S
     1         48.0.0.4         10.0.0.4    UP 00:02:33     D
```

# DMVPN Spoke (sh dmvpn detail)

```
r3#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel3 is up/up, Addr. is 10.0.0.3, VRF ""
   Tunnel Src./Dest. addr: 38.0.0.3/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_Profile"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled

IPv4 NHS:
10.0.0.1  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1       16.0.0.1        10.0.0.1    UP 00:04:49     S        10.0.0.1/32

    1       38.0.0.3        10.0.0.3    UP 00:04:15   DLX        10.0.0.3/32

    1       48.0.0.4        10.0.0.4    UP 00:04:15     D        10.0.0.4/32
```

# DMVPN Spoke (sh dmvpn detail) (продожение)

```
Crypto Session Details:
-----------------------------------------------------------------
Interface: Tunnel3
Session: [0xF2773D20]
  IKEv2 SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
          Capabilities:(none) connid:1 lifetime:23:55:10
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 16.0.0.1
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 151 drop 0 life (KB/Sec) 4316849/3310
        Outbound: #pkts enc'ed 146 drop 0 life (KB/Sec) 4316851/3310
   Outbound SPI : 0x66111539, transform : esp-aes esp-sha256-hmac
    Socket State: Open

Interface: Tunnel3
Session: [0xF2773E18]
  IKEv2 SA: local 38.0.0.3/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:2 lifetime:23:55:45
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 48.0.0.4
  IPSEC FLOW: permit 47 host 38.0.0.3 host 48.0.0.4
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 5 drop 0 life (KB/Sec) 4360198/3344
        Outbound: #pkts enc'ed 6 drop 0 life (KB/Sec) 4360198/3344
   Outbound SPI : 0xD4BDCED8, transform : esp-aes esp-sha256-hmac
    Socket State: Open
```

# DMVPN Spoke (sh crypto session)

```
r3#sh crypto session
Crypto session current status

Interface: Tunnel3
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 48.0.0.4
        Active SAs: 2, origin: crypto map

Interface: Tunnel3
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map
```

# DMVPN Spoke (sh crypto session)

```
r3#sh crypto ikev2 session
 IPv4 Crypto IKEv2 Session

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

Tunnel-id Local                 Remote                fvrf/ivrf     Status
1         38.0.0.3/500          16.0.0.1/500          none/none     READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/648 sec
Child sa: local selector  38.0.0.3/0 - 38.0.0.3/65535
          remote selector 16.0.0.1/0 - 16.0.0.1/65535
          ESP spi in/out: 0x80F86C62/0x66111539

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf     Status
2         38.0.0.3/500          48.0.0.4/500          none/none     READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/613 sec
Child sa: local selector  38.0.0.3/0 - 38.0.0.3/65535
          remote selector 48.0.0.4/0 - 48.0.0.4/65535
          ESP spi in/out: 0x8B2F7739/0xD4BDCED8
```

# DMVPN Phase 2 CEF

# До установки spoke-to-spoke tunnel

```
r3#sh ip cef 10.4.4.0/24 internal
10.4.4.0/24, epoch 0, RIB[I], refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00028000
  ifnums:
   Tunnel3(17): 10.0.0.4
  path F26D6160, path list F1985D3C, share 1/1, type attached nexthop, for IPv4
  nexthop 10.0.0.4 Tunnel3, adjacency IP adj out of Tunnel3, addr 10.0.0.4 (incomplete)
  output chain: IP adj out of Tunnel3, addr 10.0.0.4 (incomplete)

r3#sh ip cef 10.0.0.4 internal
10.0.0.0/24, epoch 0, flags attached, connected, cover dependents, need deagg, RIB[C],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x0003800C
  subblocks:
   Interest List:
     - ipv4fib connected receive
   gsb Connected chain head(11): 0xF212B448
   Covered dependent prefixes: 3
     need deagg: 2
     notify cover updated: 1
  ifnums:
   Tunnel3(17)
  path F0E38C48, path list F1985E7C, share 1/1, type connected prefix, for IPv4
  connected to Tunnel3, adjacency punt
  output chain: punt
```

# После установки spoke-to-spoke tunnel

```
r3#sh ip cef 10.4.4.0/24 internal
10.4.4.0/24, epoch 0, RIB[I], refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00028000
  ifnums:
   Tunnel3(17): 10.0.0.4
  path F26D6160, path list F1985D3C, share 1/1, type attached nexthop, for IPv4
  nexthop 10.0.0.4 Tunnel3, adjacency IP midchain out of Tunnel3, addr 10.0.0.4
F26A1E98
  output chain: IP midchain out of Tunnel3, addr 10.0.0.4 F26A1E98 IP adj out of
FastEthernet0/0, addr 38.0.0.8 F198DE10

r3#sh ip cef 10.0.0.4 internal
10.0.0.4/32, epoch 0, flags attached, refcount 5, per-destination sharing
  sources: Adj
  subblocks:
   Adj source: IP midchain out of Tunnel3, addr 10.0.0.4 F26A1E98
    Dependent covered prefix type adjfib cover 10.0.0.0/24
  ifnums:
   Tunnel3(17): 10.0.0.4
  path F26D6010, path list F273A5AC, share 1/1, type adjacency prefix, for IPv4
  attached to Tunnel3, adjacency IP midchain out of Tunnel3, addr 10.0.0.4 F26A1E98
  output chain: IP midchain out of Tunnel3, addr 10.0.0.4 F26A1E98 IP adj out of
FastEthernet0/0, addr 38.0.0.8 F198DE10
```

# DMVPN Spoke (sh adjacency)

```
r3#sh adjacency 10.0.0.4 detail
Protocol Interface                 Address
IP       Tunnel3                   10.0.0.4(11)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 28
                                   450000000000000FF2F65C826000003
                                   3000000420000800000000064
                                   Tun endpt
                                   Next chain element:
                                    IP adj out of FastEthernet0/0, addr
38.0.0.8
```

# Настройка DMVPN Phase 3

# DMVPN Phase 3

DMVPN Phase 3:

- Hub и spoke используют mGRE
- Трафик между spoke ходит изначально через Hub (но передаются CEF)
- При необходимости, поднимаются туннели spoke-to-spoke

Улучшения по сравнению с Phase 2:

- Для построения spoke-to-spoke туннелей, НЕ требуется чтобы:
  - hub суммировал информацию о маршрутах
  - Маршруты приходили с next-hop IP spoke
- Первый пакет передается CEF
- Можно сделать иерархию хабов. Для крупных сетей это может быть существенным плюсом
- На хабе используется **NHRP redirect**
- На spoke используется **NHRP shortcut**

# Настройка DMVPN Hub Phase 3

# DMVPN Hub Phase 3 (R1)

```
interface FastEthernet0/0
 ip address 16.0.0.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
!
ip route 0.0.0.0 0.0.0.0 16.0.0.6
```

# DMVPN Hub Phase 3 (R1)

```
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco12345

crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring DMVPN

crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac
 mode transport

crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
```

# DMVPN Hub Phase 3 (R1)

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0

 no ip split-horizon eigrp 1

 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 ip nhrp authentication cisco100
 ip nhrp redirect

 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile DMVPN_Profile

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

# Настройка DMVPN Spoke Phase 3

# DMVPN Spoke Phase 3 (R3)

```
interface FastEthernet0/0
 ip address 38.0.0.3 255.255.255.0
!
interface FastEthernet0/1
 ip address 10.3.3.3 255.255.255.0
!
router eigrp 1
 network 10.0.0.0
 eigrp stub connected
!
ip route 0.0.0.0 0.0.0.0 38.0.0.8
```

# DMVPN Spoke Phase 3 (R3)

```
crypto ikev2 keyring DMVPN
 peer DMVPN
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco12345

crypto ikev2 profile DMVPN_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring DMVPN

crypto ipsec transform-set DMVPN esp-aes esp-sha256-hmac
 mode transport

crypto ipsec profile DMVPN_Profile
 set transform-set DMVPN
 set ikev2-profile DMVPN_IKEv2
```

# DMVPN Spoke Phase 3 (R3)

```
interface Tunnel3
 ip address 10.0.0.3 255.255.255.0

 ip nhrp nhs 10.0.0.1
 ip nhrp map 10.0.0.1 16.0.0.1
 ip nhrp map multicast 16.0.0.1
 ip nhrp network-id 100
 ip nhrp authentication cisco100
 ip nhrp shortcut

 tunnel source FastEthernet0/0
 tunnel key 100
 tunnel protection ipsec profile DMVPN_Profile
 tunnel mode gre multipoint

 bandwidth 100000
 ip mtu 1400
 ip tcp adjust-mss 1360
```

# Проверка DMVPN Phase 3

# DMVPN mGRE tunnel

**r1#sh interfaces tunnel 1**

```
 Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.0.0.1/24
  Tunnel source 16.0.0.1 (FastEthernet0/0)

  Tunnel protocol/transport multi-GRE/IP
```

**r3#sh interfaces tunnel 3**

```
 Tunnel3 is up, line protocol is up
  Internet address is 10.0.0.3/24
  Tunnel source 38.0.0.3 (FastEthernet0/0)

  Tunnel protocol/transport multi-GRE/IP
```

# DMVPN routing

**r1#sh ip route eigrp**

```
Gateway of last resort is 16.0.0.6 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D        10.3.3.0/24 [90/1561600] via 10.0.0.3, 00:01:10, Tunnel1
D        10.4.4.0/24 [90/1561600] via 10.0.0.4, 00:33:02, Tunnel1
D        10.5.5.0/24 [90/1561600] via 10.0.0.5, 00:33:02, Tunnel1
```

**r3#sh ip route eigrp**

```
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D        10.1.1.0/24 [90/1561600] via 10.0.0.1, 00:00:30, Tunnel3
D        10.4.4.0/24 [90/2841600] via 10.0.0.1, 00:00:30, Tunnel3
D        10.5.5.0/24 [90/2841600] via 10.0.0.1, 00:00:30, Tunnel3
```

# DMVPN Hub NHRP

```
r1#sh ip nhrp
10.0.0.3/32 via 10.0.0.3
   Tunnel1 created 00:07:48, expire 01:52:11
   Type: dynamic, Flags: unique registered
   NBMA address: 38.0.0.3
10.0.0.4/32 via 10.0.0.4
   Tunnel1 created 00:07:47, expire 01:52:12
   Type: dynamic, Flags: unique registered
   NBMA address: 48.0.0.4
10.0.0.5/32 via 10.0.0.5
   Tunnel1 created 00:07:46, expire 01:52:13
   Type: dynamic, Flags: unique registered
   NBMA address: 58.0.0.5
```

# DMVPN Spoke NHRP

```
r3#sh ip nhrp
10.0.0.1/32 via 10.0.0.1
   Tunnel3 created 00:30:31, never expire
   Type: static, Flags: used
   NBMA address: 16.0.0.1

r3#ping 10.4.4.4 source 10.3.3.3
r3#sh ip nhrp
10.0.0.1/32 via 10.0.0.1
   Tunnel3 created 00:15:34, never expire
   Type: static, Flags: used
   NBMA address: 16.0.0.1
10.0.0.4/32 via 10.0.0.4
   Tunnel3 created 00:00:21, expire 01:59:38
   Type: dynamic, Flags: router implicit used
   NBMA address: 48.0.0.4
10.3.3.0/24 via 10.0.0.3
   Tunnel3 created 00:00:21, expire 01:59:38
   Type: dynamic, Flags: router unique local
   NBMA address: 38.0.0.3
    (no-socket)
10.4.4.0/24 via 10.0.0.4
   Tunnel3 created 00:00:19, expire 01:59:40
   Type: dynamic, Flags: router rib nho
   NBMA address: 48.0.0.4
```

# DMVPN Spoke NHRP shortcut

```
r3#sh ip nhrp shortcut
10.4.4.0/24 via 10.0.0.4
   Tunnel3 created 00:07:41, expire 01:52:18
   Type: dynamic, Flags: router rib nho
   NBMA address: 48.0.0.4
```

# DMVPN Spoke next-hop-override

**r3#sh ip route eigrp**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       ......
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 38.0.0.8 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
D       10.1.1.0/24 [90/1561600] via 10.0.0.1, 18:41:49, Tunnel3
D   %   10.4.4.0/24 [90/2841600] via 10.0.0.1, 18:41:49, Tunnel3
D       10.5.5.0/24 [90/2841600] via 10.0.0.1, 18:41:47, Tunnel3
```

**r3#sh ip route next-hop-override**

```
Gateway of last resort is 38.0.0.8 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 38.0.0.8
      10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Tunnel3
L       10.0.0.3/32 is directly connected, Tunnel3
D       10.1.1.0/24 [90/1561600] via 10.0.0.1, 18:42:51, Tunnel3
C       10.3.3.0/24 is directly connected, FastEthernet0/1
L       10.3.3.3/32 is directly connected, FastEthernet0/1
D   %   10.4.4.0/24 [90/2841600] via 10.0.0.1, 18:42:51, Tunnel3
                    [NHO][90/1] via 10.0.0.4, 00:05:43, Tunnel3
D       10.5.5.0/24 [90/2841600] via 10.0.0.1, 18:42:49, Tunnel3
```

# DMVPN Spoke (sh dmvpn)

```
r3#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R -->
Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================

Interface: Tunnel3, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1          16.0.0.1          10.0.0.1    UP 00:23:58     S
     2          48.0.0.4          10.0.0.4    UP 00:08:44     D
                                  10.0.0.4    UP 00:08:44   DT2
```

# DMVPN Spoke (sh dmvpn detail)

```
r3#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel3 is up/up, Addr. is 10.0.0.3, VRF ""
   Tunnel Src./Dest. addr: 38.0.0.3/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_Profile"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled

IPv4 NHS:
10.0.0.1  RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- ----------------
    1       16.0.0.1        10.0.0.1    UP 00:25:37    S        10.0.0.1/32

    2       48.0.0.4        10.0.0.4    UP 00:10:24    D        10.0.0.4/32
    0       48.0.0.4        10.0.0.4    UP 00:10:24  DT2        10.4.4.0/24

    1       38.0.0.3        10.0.0.3    UP 00:10:24  DLX        10.3.3.0/24
```

# DMVPN Spoke (sh dmvpn detail) (продожение)

```
Crypto Session Details:
-----------------------------------------------------------------------
Interface: Tunnel3
Session: [0xF27694D0]
  IKEv2 SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
          Capabilities:(none) connid:1 lifetime:23:34:23
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 16.0.0.1
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 696 drop 0 life (KB/Sec) 4285295/2062
        Outbound: #pkts enc'ed 693 drop 0 life (KB/Sec) 4285295/2062
   Outbound SPI : 0x76599119, transform : esp-aes esp-sha256-hmac
    Socket State: Open

Interface: Tunnel3
Session: [0xF27695C8]
  IKEv2 SA: local 38.0.0.3/500 remote 48.0.0.4/500 Active
          Capabilities:(none) connid:2 lifetime:23:49:36
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 48.0.0.4
  IPSEC FLOW: permit 47 host 38.0.0.3 host 48.0.0.4
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 7 drop 0 life (KB/Sec) 4338286/2975
        Outbound: #pkts enc'ed 6 drop 0 life (KB/Sec) 4338286/2975
   Outbound SPI : 0xC84725E2, transform : esp-aes esp-sha256-hmac
    Socket State: Open
```

# DMVPN Spoke (sh crypto session)

```
r3#sh crypto session
Crypto session current status

Interface: Tunnel3
Session status: UP-ACTIVE
Peer: 48.0.0.4 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 48.0.0.4/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 48.0.0.4
        Active SAs: 2, origin: crypto map

Interface: Tunnel3
Session status: UP-ACTIVE
Peer: 16.0.0.1 port 500
  IKEv2 SA: local 38.0.0.3/500 remote 16.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 38.0.0.3 host 16.0.0.1
        Active SAs: 2, origin: crypto map
```

# DMVPN Spoke (sh crypto session)

```
r3#sh crypto ikev2 session
 IPv4 Crypto IKEv2 Session

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

Tunnel-id Local          Remote          fvrf/ivrf     Status
1         38.0.0.3/500   16.0.0.1/500    none/none     READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1721 sec
Child sa: local selector  38.0.0.3/0 - 38.0.0.3/65535
          remote selector 16.0.0.1/0 - 16.0.0.1/65535
          ESP spi in/out: 0x3563FD6C/0x76599119

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local          Remote          fvrf/ivrf     Status
2         38.0.0.3/500   48.0.0.4/500    none/none     READY
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth
sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/808 sec
Child sa: local selector  38.0.0.3/0 - 38.0.0.3/65535
          remote selector 48.0.0.4/0 - 48.0.0.4/65535
          ESP spi in/out: 0x649D278B/0xC84725E2
```

# DMVPN Phase 3 CEF и NHRP shortcut

# До установки spoke-to-spoke tunnel

```
r3#sh ip cef 10.4.4.0/24 internal
10.4.4.0/24, epoch 0, RIB[I], refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00028000
  ifnums:
   Tunnel3(17): 10.0.0.1
  path F2717B88, path list F19C764C, share 1/1, type attached nexthop, for IPv4
  nexthop 10.0.0.1 Tunnel3, adjacency IP midchain out of Tunnel3, addr 10.0.0.1
F0A29F40
  output chain: IP midchain out of Tunnel3, addr 10.0.0.1 F0A29F40 IP adj out of
FastEthernet0/0, addr 38.0.0.8 F19CF3D0

r3#sh ip cef 10.0.0.4 internal
10.0.0.0/24, epoch 0, flags attached, connected, cover dependents, need deagg, RIB[C],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x0003800C
  subblocks:
   Interest List:
     - ipv4fib connected receive
   gsb Connected chain head(11): 0xF2701AE8
   Covered dependent prefixes: 3
     need deagg: 2
     notify cover updated: 1
  ifnums:
   Tunnel3(17)
  path F221AA28, path list F19C773C, share 1/1, type connected prefix, for IPv4
  connected to Tunnel3, adjacency punt
  output chain: punt
```

# После установки spoke-to-spoke tunnel

```
r3#sh ip cef 10.4.4.0/24 internal
10.4.4.0/24, epoch 0, RIB[I], refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00028000
  ifnums:
   Tunnel3(17): 10.0.0.4
  path F27179C8, path list F19C750C, share 1/1, type attached nexthop, for IPv4
  nexthop 10.0.0.4 Tunnel3, adjacency IP midchain out of Tunnel3, addr 10.0.0.4
F0A29E10
  output chain: IP midchain out of Tunnel3, addr 10.0.0.4 F0A29E10 IP adj out of
FastEthernet0/0, addr 38.0.0.8 F19CF3D0

r3#sh ip cef 10.0.0.4 internal
10.0.0.4/32, epoch 0, flags attached, refcount 5, per-destination sharing
  sources: Adj
  subblocks:
   Adj source: IP midchain out of Tunnel3, addr 10.0.0.4 F0A29E10
    Dependent covered prefix type adjfib cover 10.0.0.0/24
  ifnums:
   Tunnel3(17): 10.0.0.4
  path F2717A38, path list F19C755C, share 1/1, type adjacency prefix, for IPv4
  attached to Tunnel3, adjacency IP midchain out of Tunnel3, addr 10.0.0.4 F0A29E10
  output chain: IP midchain out of Tunnel3, addr 10.0.0.4 F0A29E10 IP adj out of
FastEthernet0/0, addr 38.0.0.8 F19CF3D0
```

# DMVPN Spoke (sh adjacency)

```
r3#sh adjacency tun3 detail
Protocol Interface                 Address
IP       Tunnel3                   10.0.0.1(13)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 28
                                   4500000000000000FF2F85CB26000003
                                   1000000120000800000000064
                                   Tun endpt
                                   Next chain element:
                                    IP adj out of FastEthernet0/0, addr
38.0.0.8
```

# DMVPN Spoke (sh adjacency)

```
r3#sh adjacency tun3 detail
Protocol Interface                 Address
IP       Tunnel3                   10.0.0.1(12)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 28
                                   4500000000000000FF2F85CB26000003
                                   1000000120000800000000064
                                   Tun endpt
                                   Next chain element:
                                    IP adj out of FastEthernet0/0, addr
38.0.0.8
IP       Tunnel3                   10.0.0.4(11)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 28
                                   4500000000000000FF2F65C826000003
                                   3000000420000800000000064
                                   Tun endpt
                                   Next chain element:
                                    IP adj out of FastEthernet0/0, addr
38.0.0.8
```

# Полезные crypto команды

# DMVPN Spoke (sh adjacency)

```
r3#sh crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
    1  IPsec   AES+SHA256             1130        0        0 38.0.0.3
    2  IPsec   AES+SHA256                0     1133     1133 38.0.0.3
    5  IPsec   AES+SHA256              449        0        0 38.0.0.3
    6  IPsec   AES+SHA256                0      450      451 38.0.0.3
 1001  IKEv2   SHA512+AES256             0        0        0 38.0.0.3
 1003  IKEv2   SHA512+AES256             0        0        0 38.0.0.3


r3#sh crypto ikev2 proposal
 IKEv2 proposal: default
     Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
     Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
     PRF        : SHA512 SHA384 SHA256 SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

# DMVPN Spoke (sh adjacency)

```
r3#sh crypto ikev2 profile

IKEv2 profile: DMVPN_IKEv2
 Ref Count: 5
 Match criteria:
  Fvrf: global
  Local address/interface: none
  Identities:
   address 0.0.0.0
  Certificate maps: none
 Local identity: none
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 EAP options: none
 Keyring: DMVPN
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: none
 Virtual-template: none
 AAA EAP authentication mlist: none
 AAA Accounting: none
 AAA group authorization: none
 AAA user authorization: none
```

# Per-tunnel QoS

# DMVPN Hub QoS

**Hub R1:**

```
policy-map LVV
 class class-default
  shape average 5000000
policy-map KIEV
 class class-default
  shape average 10000000

interface Tunnel1
 ip nhrp map group lvv service-policy output LVV
 ip nhrp map group kiev service-policy output KIEV
```

**Spoke R3:**

```
interface Tunnel3
 ip nhrp group lvv
```

**Spoke R4:**

```
interface Tunnel4
 ip nhrp group kiev
```

**Spoke R5:**

```
interface Tunnel5
 ip nhrp group kiev
```

# DMVPN Hub QoS

```
r1#sh ip nhrp
10.0.0.3/32 via 10.0.0.3
   Tunnel1 created 00:09:38, expire 01:50:21
   Type: dynamic, Flags: unique registered
   NBMA address: 38.0.0.3
   Group: lvv
10.0.0.4/32 via 10.0.0.4
   Tunnel1 created 00:09:37, expire 01:50:22
   Type: dynamic, Flags: unique registered
   NBMA address: 48.0.0.4
   Group: kiev
10.0.0.5/32 via 10.0.0.5
   Tunnel1 created 00:09:36, expire 01:50:23
   Type: dynamic, Flags: unique registered
   NBMA address: 58.0.0.5
   Group: kiev
```

# DMVPN Hub QoS

```
r1#sh ip nhrp group-map
Interface: Tunnel1
 NHRP group: lvv
  QoS policy: LVV
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  10.0.0.3/38.0.0.3

 NHRP group: kiev
  QoS policy: KIEV
  Tunnels using the QoS policy:
  Tunnel destination overlay/transport address
  10.0.0.4/48.0.0.4
  10.0.0.5/58.0.0.5
```

# DMVPN Hub QoS

```
r1#sh dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface Tunnel1 is up/up, Addr. is 10.0.0.1, VRF ""
   Tunnel Src./Dest. addr: 16.0.0.1/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "DMVPN_Profile"
   Interface State Control: Disabled
   nhrp event-publisher : Disabled
Type:Hub, Total NBMA Peers (v4/v6): 3

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- ----------------
    1       38.0.0.3        10.0.0.3    UP 00:07:44    D        10.0.0.3/32
NHRP group: lvv
 Output QoS service-policy applied: LVV

    1       48.0.0.4        10.0.0.4    UP 00:07:43    D        10.0.0.4/32
NHRP group: kiev
 Output QoS service-policy applied: KIEV

    1       58.0.0.5        10.0.0.5    UP 00:07:43    D        10.0.0.5/32
NHRP group: kiev
 Output QoS service-policy applied: KIEV
```

# DMVPN Hub QoS

```
r1#sh policy-map multipoint

Interface Tunnel1 <--> 38.0.0.3

Interface Tunnel1 <--> 48.0.0.4

Interface Tunnel1 <--> 58.0.0.5
```

# DMVPN Hub QoS

```
r1#sh policy-map target multipoint

Interface Tunnel1 <--> 38.0.0.3

  Service-policy output: LVV

    Class-map: class-default (match-any)
      394 packets, 34876 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 1250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 394/61364
      shape (average) cir 5000000, bc 20000, be 20000
      target shape rate 5000000

Interface Tunnel1 <--> 48.0.0.4

  Service-policy output: KIEV

    Class-map: class-default (match-any)
      198 packets, 17425 bytes
      ...
```

# DMVPN Hub QoS

**r1#sh policy-map target multipoint tunnel 1 58.0.0.5**

```
Interface Tunnel1 <--> 58.0.0.5

  Service-policy output: KIEV

    Class-map: class-default (match-any)
      213 packets, 18726 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 2500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 213/33090
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
```

# Полезные ресурсы

# Дополнительная информация

NHRP
http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html

Cisco Live:

- BRKSEC-4054 Advanced Concepts of DMVPN
- BRKSEC-3052  Advanced DMVPN Designs

# Настройка DMVPN на маршрутизаторах Cisco

**Автор курса: Наташа Самойленко**
**nataliya.samoylenko@gmail.com**

***Сетевые Дни***