GDOI Encryption for IPv6 Data Traffic Using IPv6 Tunnels

Currently Group Domain of Interpretation (GDOI) encryption is not supported for direct IPv6 data traffic. However, you can use GDOI encryption on IPv6 packets by applying the cryptography map on the physical interface with an IPv4 address and using IPv6 tunnels between the group members. IPv6 tunnels can be either 6to4 tunnels or multipoint generic routing encapsulation (mGRE) dynamic multipoint VPN (DMVPN) tunnels.

You can deploy a 6to4 tunnel with simple configuration; it is highly scalable to secure IPv6 traffic over an IPv4 network when compared with mGRE tunnels. 6to4 tunnels are not dependent on other protocols, so a 6to4 tunnel is the preferred solution.

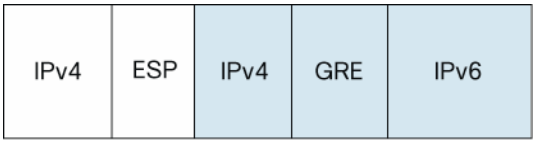
GDOI Encryption on IPv6 Traffic Using mGRE DMVPN Tunnels

Basic hub-and-spoke topology with DMVPN for tunneling IPv6 packets in IPv4 GRE tunnels is used for GDOI encryption. Group Encrypted Transport VPN is used for securing all the IPv4 data, including the tunneled IPv6 packets, by applying the cryptography map on the physical interface.

DMVPN tunnels are dynamically created and a new spoke could be added in the future with no changes on the hub. When native IPv6 is supported by Group Encrypted Transport VPN, you can remove the DMVPN tunnel to make the migration easier.

Figure 1 shows the final packet under this solution. The blue portion gets encrypted by Group Encrypted Transport VPN.

Figure 1. Packet Encapsulation Using IPv6 mGRE DMVPN Tunnels



DMVPN Solution Test Setup Topology

Solution test setup consists of two DMVPN spoke routers, demo-gm1 and demo-gm2, located in branch offices and one DMVPN hub router, demo-gm3, located at headquarters. Demonstration setup also includes one key server, demo-ks1. The multicast rekey method is used. For the testing, “demo-dmvpn” simulates the IP VPN network. Cisco® 3845 Integrated Services Router platforms running the Cisco IOS® Software 12.4(22)T IOS image are used.

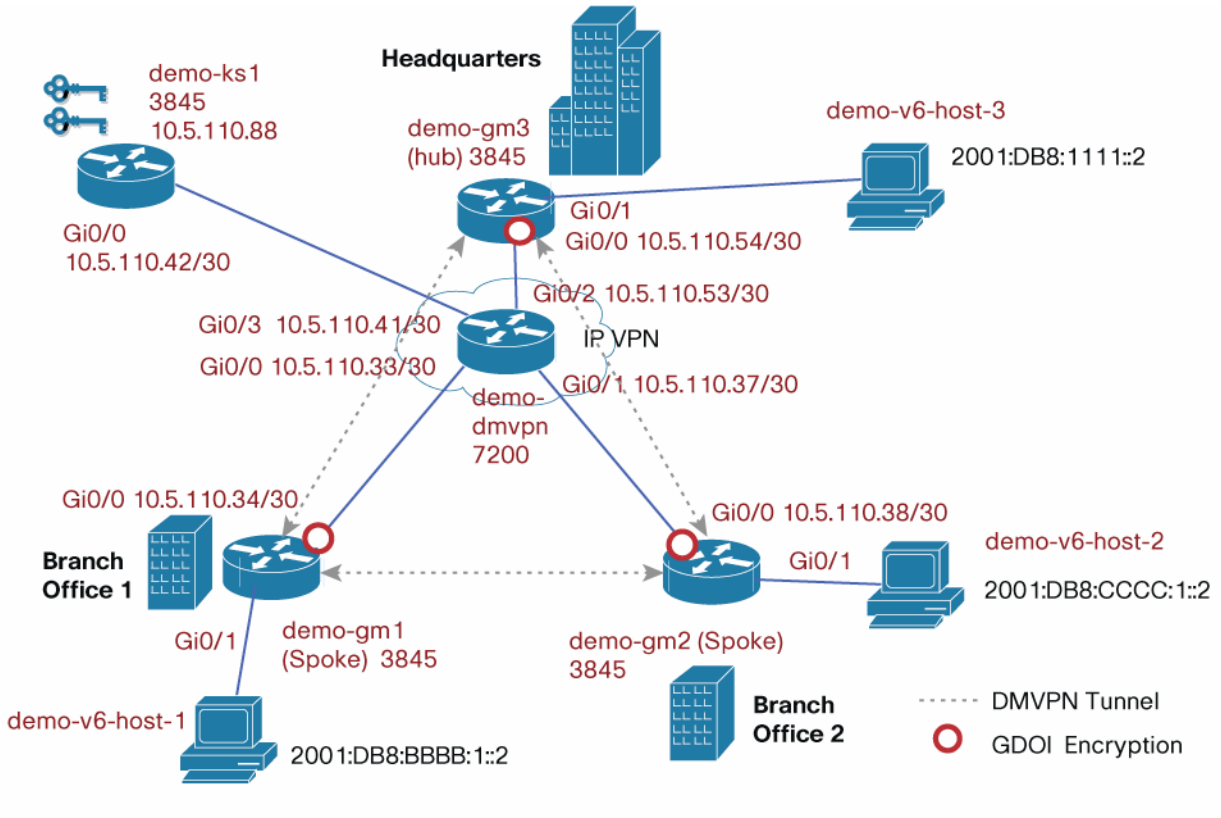
The Enhanced IGRP (EIGRP) routing protocol is used for DMVPN. Provider equipment uses the Border Gateway Protocol (BGP) routing protocol.

Configuring DMVPN for IPv6

The following explains how to configure DMVPN hub-and-spoke routers for IPv6. It covers only the necessary configuration for enabling DMVPN and IPv6. This configuration is a sample configuration; you should customize it to your correct corporate subnets and servers. Figure 2 shows the topology for testing. Corporate LAN v6 prefix: 2001:db8:1111::/64

- **Spoke-side LAN v6 prefixes**: 2001:db8:BBBB::/48 and 2001:db8:CCCC::/48
- **DMVPN v6 tunnel prefix**: 2001:db8:AAAA::/64

Figure 2. Topology Diagram for Using mGRE 6to4 Tunnels



Hub Router demo-gm3 Configuration

The configuration used in **demo-gm3** follows:

```
hostname demo-gm3
!
ip dhcp pool demo
  network 10.5.110.216 255.255.255.248
  default-router 10.5.110.217
!
ip multicast-routing
ip igmp ssm-map enable
!!! Enable IPv6 unicast routing !!!
ipv6 unicast-routing
!
! IKE policy used for GETVPN
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
```

```
!!! Preshared Key (PSK) for the KS !!!
crypto isakmp key dGvPnPsK address 10.5.110.88
!
! GDOI group configuration
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
!
! Crypto map for GDOI
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
!
interface GigabitEthernet0/0
 description connected to demo_dmvpn
 ip address 10.5.110.54 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi
!
!!! Enable IPv6 on upstream IF (connecting to corporate network) & IPv6 Host-3 !!!
interface GigabitEthernet0/1
 no ip address
 ip pim sparse-mode
 no autostate
 !!! Configure IPv6 address
 ipv6 address 2001:DB8:1111::1/64
 !!! Auto-generate a link-local address !!!
 ipv6 enable
 !!! Enable EIGRP on the interface !!!
 ipv6 eigrp 6
!
! DMVPN mGRE tunnel configuration
interface Tunnel5
 bandwidth 2000
 ip address 64.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
```

```
 ip pim sparse-dense-mode
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 44
 delay 2000
 ipv6 address 2001:DB8:AAAA::1/64
 ipv6 enable
 ipv6 mtu 1400
 ipv6 eigrp 6
 !!! Summary address used in DMVPN Phase 3 !!!
 no ipv6 split-horizon eigrp 6
 ipv6 summary-address eigrp 6 2001:DB8:BBBB::/48 5
 ipv6 summary-address eigrp 6 2001:DB8:CCCC::/48 5
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 6000
 ipv6 nhrp redirect
 qos pre-classify
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
!
interface Vlan10
 ip address 10.5.110.217 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 no autostate
!
ipv6 router eigrp 6
 no shutdown
!
router eigrp 44
 redistribute static
 network 10.5.110.216 0.0.0.7
 network 64.0.0.0 0.0.0.255
 no auto-summary
```

```
!
router bgp 400
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.5.110.53 remote-as 900
 no auto-summary
! overlay routing
ip route 10.5.110.32 255.255.255.252 10.5.110.53
ip route 10.5.110.36 255.255.255.252 10.5.110.53
!
! SSM configuration needed for receiving rekeys via multicast
! 1 is the ACL number
ip pim ssm range 1
!
access-list 1 permit 239.192.0.0 0.0.255.255
```

Spoke Router demo-gm1 Configuration

The configuration used in **demo-gm1** follows:

```
!
hostname demo-gm1
!
ip dhcp pool demo
  network 10.5.110.200 255.255.255.248
  default-router 10.5.110.201
!
ip multicast-routing
ip igmp ssm-map enable
!!! Enable IPv6 unicast routing !!!
ipv6 unicast-routing
! IKE policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 10.5.110.88  ! Pre-shared key
!
! GDOI group config
crypto gdoi group GETVPN-DEMO
```

```
 identity number 1357924756
 server address ipv4 10.5.110.88
!
! crypto map for GDOI
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
!
! DMVPN mGRE configuration
interface Tunnel10
 bandwidth 2000
 ip address 64.0.0.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip flow ingress
 ip pim sparse-dense-mode
 ip nhrp map multicast 10.5.110.54
 ip nhrp map 64.0.0.1 10.5.110.54
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 64.0.0.1
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 2000
 !!! Tunnel IPv6 unicast address !!!
 ipv6 address 2001:DB8:AAAA::2/64
 ipv6 enable
 ipv6 mtu 1400
 ipv6 eigrp 6
 !!! The NBMA address is IPv4 only !!!
 ipv6 nhrp map multicast 10.5.110.54
 ipv6 nhrp map 2001:DB8:AAAA::1/64 10.5.110.54
 ipv6 nhrp network-id 6000
 ipv6 nhrp nhs 2001:DB8:AAAA::1
 ipv6 nhrp shortcut
 ipv6 nhrp redirect
 qos pre-classify
```

```
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
!
interface GigabitEthernet0/0
 description connected to demo_dmvpn
 ip address 10.5.110.34 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi
!
interface GigabitEthernet0/1
 description Connected to Host-1
 no ip address
 ip flow ingress
 ip pim sparse-mode
 ipv6 address 2001:DB8:BBBB:1::1/64
 ipv6 enable
 ipv6 eigrp 6
!
interface Vlan10
 ip address 10.5.110.201 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 no autostate
!
ipv6 router eigrp 6
 no shutdown
!
router eigrp 44
 network 10.5.110.200 0.0.0.7
 network 64.0.0.0 0.0.0.255
 auto-summary
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.5.110.33 remote-as 900
```

```
 no auto-summary
!
! overlay routing for DMVPN tunnel
ip route 0.0.0.0 0.0.0.0 10.5.110.33
!
! SSM configuration to receive multicast rekeys
ip pim ssm range 1 ! 1 is ACL number
access-list 1 permit 239.192.0.0 0.0.255.255
```

Spoke Router demo-gm2 Configuration

The configuration used in **demo-gm2** follows:

```
!
hostname demo-gm2
!
ip dhcp pool demo
  network 10.5.110.208 255.255.255.248
  default-router 10.5.110.209
!
ip multicast-routing
ip igmp ssm-map enable
!!! Enable IPv6 unicast routing !!!
ipv6 unicast-routing
! IKE policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key dGvPnPsK address 10.5.110.88  ! Pre-shared key
!
! GDOI group config
crypto gdoi group GETVPN-DEMO
 identity number 1357924756
 server address ipv4 10.5.110.88
!
! crypto map for GDOI
crypto map demo-gdoi 1 gdoi
 set group GETVPN-DEMO
!
```

```
interface Tunnel10
 bandwidth 2000
 ip address 64.0.0.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-dense-mode
 ip nhrp map multicast 10.5.110.54
 ip nhrp map 64.0.0.1 10.5.110.54
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 64.0.0.1
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 2000
 !!! Tunnel IPv6 unicast address !!!
 ipv6 address 2001:DB8:AAAA::3/64
 ipv6 enable
 ipv6 mtu 1400
 ipv6 eigrp 6
 !!! The NBMA address is IPv4 only !!!
 ipv6 nhrp map multicast 10.5.110.54
 ipv6 nhrp map 2001:DB8:AAAA::1/64 10.5.110.54
 ipv6 nhrp network-id 6000
 ipv6 nhrp nhs 2001:DB8:AAAA::1
 ipv6 nhrp shortcut
 ipv6 nhrp redirect
 qos pre-classify
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
!
interface GigabitEthernet0/0
 description connected to demo_dmvpn
 ip address 10.5.110.38 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi
```

```
!
interface GigabitEthernet0/1
 description Connected to Host-2
 no ip address
 ip flow ingress
 ip pim sparse-mode
 ipv6 address 2001:DB8:CCCC:1::1/64
 ipv6 enable
 ipv6 eigrp 6
!
interface Vlan10
 ip address 10.5.110.209 255.255.255.248
 ip pim sparse-mode
 ip igmp join-group 239.192.1.190 source 10.5.110.88
 no autostate
!
ipv6 router eigrp 6
 no shutdown
!
router eigrp 44
 network 10.5.110.208 0.0.0.7
 network 64.0.0.0 0.0.0.255
 auto-summary
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.5.110.37 remote-as 900
 no auto-summary
!
! overlay routing for DMVPN tunnel
ip route 0.0.0.0 0.0.0.0 10.5.110.37
!
! SSM configuration to receive multicast rekeys
ip pim ssm range 1 ! 1 is ACL number
access-list 1 permit 239.192.0.0 0.0.255.255
```

Key Server demo-ks1 Configuration

The configuration used in **demo-ks1** follows:

```
!
hostname demo-ks1
! IKE Policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
! Preshared keys
crypto isakmp key dGvPnPsK address 10.5.110.34
crypto isakmp key dGvPnPsK address 10.5.110.54
crypto isakmp key dGvPnPsK address 10.5.110.38
!  Crypto GDOI attributes
crypto ipsec profile getvpn-profile
 set security-association lifetime seconds 900    ! TEK lifetime
 set transform-set aes128
!
crypto gdoi group GETVPN-DEMO
 identity number 1357924756                     ! group id
 server local                                   ! Key server
 rekey algorithm aes 128                        ! rekey algorithm
 rekey lifetime seconds 28800                   ! KEK lifetime
 rekey authentication mypubkey rsa rekeyrsa     ! rekey Authentication
 rekey transport unicast                        ! unicast rekey method
 sa ipsec 1                                     ! security association
  profile getvpn-profile                        ! Crypto attribute selection
  match address ipv4 sa-acl                     ! Encryption Policy
  replay time window-size 5                     ! Replay time window size
 address ipv4 10.5.110.88                       ! KS address
! KS address used for sending rekeys
interface Loopback0
 ip address 10.5.110.88 255.255.255.255
!
interface GigabitEthernet0/0
 description Connected to demo-dmvpn
 ip address 10.5.110.42 255.255.255.252
```

```
!
router bgp 800
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.40 mask 255.255.255.252
 network 10.5.110.88 mask 255.255.255.255
 neighbor 10.5.110.41 remote-as 900
 no auto-summary
! GDOI Encryption policy
ip access-list extended sa-acl
 deny  udp any eq 848 any eq 848       ! GDOI in clear
 deny  tcp any any eq ssh              ! Secure Shell control traffic in clear
 deny  tcp any eq ssh any              ! Secure Shell control traffic in clear
 deny  esp any any                     ! Exclude ESP traffic (GRE+IPSec)
 deny  tcp any eq bgp any              ! Exclude BGP
 deny  tcp any any eq bgp              ! Exclude BGP
 deny  udp any eq isakmp any eq isakmp ! Exclude IKE control traffic
 deny  eigrp any any                   ! Exclude EIGRP control traffic
 deny  igmp any any                    ! Exclude IGMP
 deny  pim any 224.0.0.13              ! Exclude PIM control
 deny  ip any 224.0.0.0 0.0.255.255    ! Exclude link-layer control protocols
 deny  udp any any eq ntp              ! Exclude NTP
 deny  udp any any eq snmp             ! Exclude SNMP
 deny  udp any any eq syslog           ! Exclude syslog
 permit ip any any                     ! Encrypt everything else
!
ip pim ssm range 1                     ! need for multicast rekey. 1 is ACL number.
!
ip access-list extended dgvpn-rekey-multicast-group
 permit ip any host 239.192.1.190
!
access-list 1 permit 239.192.0.0 0.0.255.255
```

Network Router demo-dmvpn Configuration

The configuration used in **demo-dmvpn** follows:

```
hostname demo_dmvpn
!
ip multicast-routing
```

```
ip igmp ssm-map enable
!
interface GigabitEthernet0/0
 description connected to GM1
 ip address 10.5.110.33 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/1
 description connected to GM2
 ip address 10.5.110.37 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/2
 description connected to GM3
 ip address 10.5.110.53 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernet0/3
 description connected to KS1
 ip address 10.5.110.41 255.255.255.252
 ip pim sparse-mode
!
router bgp 900
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.32 mask 255.255.255.252
 network 10.5.110.36 mask 255.255.255.252
 network 10.5.110.40 mask 255.255.255.252
 network 10.5.110.52 mask 255.255.255.252
 neighbor 10.5.110.34 remote-as 200
 neighbor 10.5.110.38 remote-as 300
 neighbor 10.5.110.42 remote-as 800
 neighbor 10.5.110.54 remote-as 400
 no auto-summary
```

IPv6 Host demo-v6-host-1 Configuration

This host is connected behind the group member in branch-office 1. The configuration used in **demo-v6-host-1** follows:

```
hostname demo-v6-host-1
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:BBBB:1::2/64
 ipv6 enable
 ipv6 eigrp 6
!
ipv6 router eigrp 6
 no shutdown
```

IPv6 Host demo-v6-host-2 Configuration

This host is connected behind the group member in branch-office 2. The configuration used in **demo-v6-host-2** follows:

```
hostname demo-v6-host-2
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:CCCC:1::2/64
 ipv6 enable
 ipv6 eigrp 6
!
ipv6 router eigrp 6
 no shutdown
```

IPv6 Host demo-v6-host-3 Configuration

This host is connected behind the group member at headquarters. The configuration used in **demo-v6-host-3** follows:

```
hostname demo-v6-host-3
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:1111::2/64
 ipv6 enable
 ipv6 eigrp 6
!
ipv6 router eigrp 6
 no shutdown
```

Verification of GDOI Encryption on IPv6 Traffic Using mGRE DMVPN Tunnels

Use the following configuration to verify mGRE DMVPN tunnel operation in the branch-office 1 router demo-gm1:

```
demo-gm1# 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
    UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel10, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
   1   10.5.110.54    64.0.0.1  UP  4d21h   S
Interface: Tunnel10, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 2
  1.Peer NBMA Address: 10.5.110.54
    Tunnel IPv6 Address: 2001:DB8:AAAA::1
    IPv6 Target Network: 2001:DB8:AAAA::/64
    # Ent: 1, Status: NHRP, UpDn Time: never, Cache Attrib: S
```

```
  2.Peer NBMA Address: 10.5.110.38
    Tunnel IPv6 Address: 2001:DB8:AAAA::3
    IPv6 Target Network: 2001:DB8:AAAA::3/128
    # Ent: 2, Status: UP, UpDn Time: 00:05:36, Cache Attrib: D
  3.Peer NBMA Address: 10.5.110.38
    Tunnel IPv6 Address: 2001:DB8:AAAA::3
    IPv6 Target Network: 2001:DB8:CCCC:1::/64
    # Ent: 0, Status: UP, UpDn Time: 00:05:36, Cache Attrib: D
```

Use the following configuration to verify mGRE DMVPN tunnel operation in the headquarters router demo-gm3:

```
demo-gm3# 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
    UpDn Time --> Up or Down Time for a Tunnel
==========================================================================
Interface: Tunnel5, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
   1   10.5.110.34    64.0.0.2  UP  4d21h   D
   1   10.5.110.38    64.0.0.3  UP   1w0d   D

Interface: Tunnel5, IPv6 NHRP Details
Type:Hub, Total NBMA Peers (v4/v6): 2
  1.Peer NBMA Address: 10.5.110.34
    Tunnel IPv6 Address: 2001:DB8:AAAA::2
    IPv6 Target Network: 2001:DB8:AAAA::2/128
    # Ent: 1, Status: UP, UpDn Time: 1w0d, Cache Attrib: D
  2.Peer NBMA Address: 10.5.110.38
    Tunnel IPv6 Address: 2001:DB8:AAAA::3
    IPv6 Target Network: 2001:DB8:AAAA::3/128
    # Ent: 1, Status: UP, UpDn Time: 2w3d, Cache Attrib: D
```

Use the following configuration to verify Internet Key Exchange (IKE) connection between the group member and the key system for receive rekeys:

```
demo-gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst       src       state     conn-id status
239.192.1.190  10.5.110.88   GDOI_REKEY    1071 ACTIVE
10.5.110.88   10.5.110.34   GDOI_IDLE     1070 ACTIVE
```

Verify whether the group member is participating in Group Encrypted Transport VPN encryption by executing the following command-line interface (CLI) command:

```
demo-gm1#show crypto gdoi
GROUP INFORMATION
  Group Name               : GETVPN-DEMO
  Group Identity           : 1357924756
  Rekeys received          : 1602
  IPSec SA Direction       : Both
  Active Group Server      : 10.5.110.88
  Group Server list        : 10.5.110.88
  Rekey Received(hh:mm:ss) : 00:00:54
  Rekeys received
     Cumulative     : 1602
     After registration : 1602
 ACL Downloaded From KS 10.5.110.88:
  access-list deny udp any port = 848 any port = 848
  access-list deny tcp any any port = 23
  access-list deny tcp any port = 23 any
  access-list deny esp any any
  access-list deny tcp any port = 179 any
  access-list deny tcp any any port = 179
  access-list deny udp any port = 500 any port = 500
  access-list deny ospf any any
  access-list deny eigrp any any
  access-list deny igmp any any
  access-list deny pim any any
  access-list deny ip any 224.0.0.0 0.0.255.255
  access-list deny udp any any port = 123
  access-list deny udp any any port = 161
```

```
  access-list deny udp any any port = 514
  access-list permit ip any any
KEK POLICY:
  Rekey Transport Type   : Multicast
  Lifetime (secs)     : 27129
  Encrypt Algorithm    : AES
  Key Size         : 128
  Sig Hash Algorithm    : HMAC_AUTH_SHA
  Sig Key Length (bits)  : 1024
TEK POLICY for the current KS-Policy ACEs Downloaded:
 GigabitEthernet0/0:
  IPsec SA:
    spi: 0x94095CF2(2483641586)
    transform: esp-aes esp-sha-hmac
    sa timing:remaining key lifetime (sec): (34)
    Anti-Replay(Time Based) : 5 sec interval
  IPsec SA:
    spi: 0x1F07791F(520583455)
    transform: esp-aes esp-sha-hmac
    sa timing:remaining key lifetime (sec): (824)
    Anti-Replay(Time Based) : 5 sec interval
```

Verify whether the group member is receiving rekeys from the key system after its registration using the following CLI command:

```
demo-gm1#show crypto gdoi gm rekey
Group GETVPN-DEMO (Multicast)
  Number of Rekeys received (cumulative)    : 3
  Number of Rekeys received after registration : 3
  Multicast destination address        : 239.192.1.190
Rekey (KEK) SA information :
     dst       src       conn-id my-cookie his-cookie
New   : 239.192.1.190  10.5.110.89    1071  E7917829  C9BAD494
Current : 239.192.1.190  10.5.110.89    1071  E7917829  C9BAD494
```

Verify whether the IPv6 traffic between the host at branch-office 1 and the host at headquarters gets encrypted by Group Encrypted Transport VPN by using the following CLIs:

Check the number of packets encrypted in demo1-gm as follows:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 3329, #pkts encrypt: 3329, #pkts digest: 3329
```

From demo-v6-host-1 in branch-office 1, ping demo-v6-host-3 in headquarters:

```
demo-v6-host-1# ping ipv6 2001:DB8:1111::2 rep 1000
```

Check whether all the packets are encrypted in demo1-gm in branch-office 1:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 4329, #pkts encrypt: 4329, #pkts digest: 4329
```

Verify whether the IPv6 traffic between the host in branch-office 1 and the host in branch-office 2 gets encrypted by Group Encrypted Transport VPN by using the following CLIs:

Check the number of packets encrypted in demo1-gm as follows:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 10220, #pkts encrypt: 10220, #pkts digest: 10220
```

From demo-v6-host-1 in branch-office 1, ping demo-v6-host-2 in branch-office 2

```
demo-v6-host-1# ping ipv6 2001:DB8:CCCC:1::2 rep 1000
```

Check whether all the packets are encrypted in demo1-gm in branch-office 1:

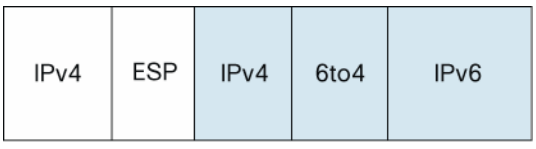
```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 11220, #pkts encrypt: 11220, #pkts digest: 11220
```

GDOI Encryption on IPv6 Traffic Using 6to4 Tunnels

IP 6to4 tunneling encapsulates IPv6 packets in IPv4 tunnels where a portion of the IPv4 address represents a portion of the IPv6 address. Group Encrypted Transport VPN is used for securing all the IPv4 data, including the tunneled IPv6 packets, by applying the cryptography map on the physical interface. The IP 6to4 tunnel uses only the IP protocol. IP 6to4 tunnels are efficient and simple to configure.

Figure 3 shows the final packet under this solution. The blue portion gets encrypted by Group Encrypted Transport VPN.

Figure 3. Packet Encapsulation Using 6to4 Tunnels



Solution Test Setup Topology

Solution test setup consists of two group-member routers, demo-gm1 and demo-gm2, located in branch offices and another group-member router, demo-gm3, located at headquarters. Demonstration setup also includes one key server, demo-ks1. A multicast rekey method is used. For the testing, “demo-getvpn” simulates the network. Cisco 3845 platform routers running the Cisco IOS Software 12.4(22)T IOS image are used.

Benefits of 6to4 Tunnels

The benefits to the enterprise of using 6to4 tunnels follow:

- The end-user host configuration is simple—it requires minimal management overhead.
- The tunnel is automatic; no enterprise-specific configuration is required at the 6to4 relay site. 6to4 tunnels scale well.
- This solution accommodates dynamic IP addresses at the enterprise.
- The tunnel exists only for the duration of the session.
- A 6to4 tunnel requires only a one-time configuration at the Internet service provider (ISP), making the 6to4 relay service available simultaneously to many enterprises.
- 6to4 tunnels are simple and efficient. They use only the IP protocol, and are not dependent on other protocols such as Hot Standby Router Protocol (HSRP) and EIGRP, whereas mGRE tunnels for IPv6 depend on other protocols.
- IP 6to4 uses an inferred /48 prefix for a site, allowing the operator to allocate subnets with the next 16 bits. It in effect provides 64,000 subnets to a given site while providing 64 bits for the host within each subnet.

Limitations of 6to4 Tunnels

6to4 tunnel usage has the following limitations:

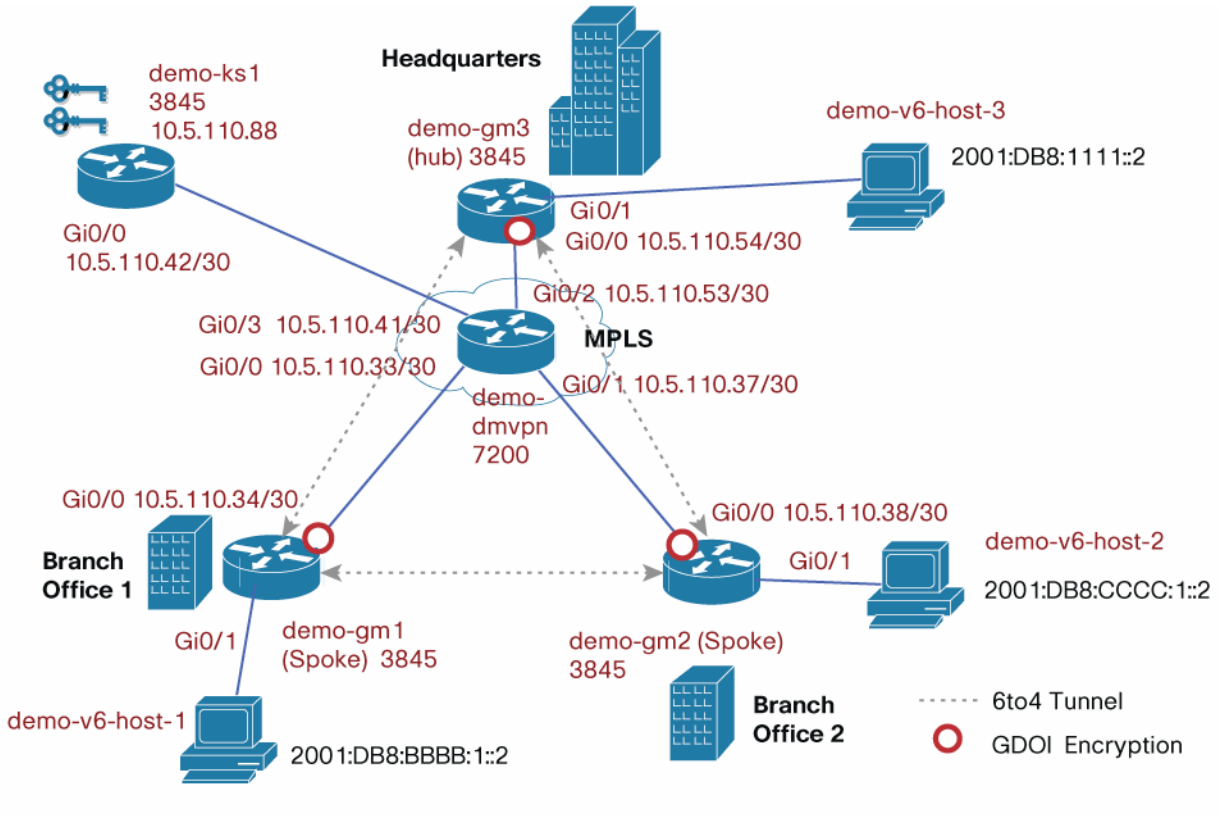
- Independently managed Network Address Translation (NAT) is not allowed along the path of the tunnel.
- You cannot easily implement multihoming.
- The 6to4 tunnel mechanism provides a /48 address block; no more addresses are available. All 6to4 tunnels prepend IPv4 addresses with the 2002: prefix.
- Because 6to4 tunnels are configured many-to-one and tunnel traffic can originate from multiple endpoints, 6to4 tunnels can provide only overall traffic information to the ISP.
- The underlying IPv4 address determines the enterprise 6to4 IPv6 address prefix, so the migration to native IPv6 requires renumbering the network.
- This solution is limited to static or BGP4+ routing.

Configuration of 6to4 Tunnels

The following explains how to configure 6to4 tunnels. Figure 4 shows the topology.

- **Corporate LAN v6 prefix**: 2001:db8:1111::/64
- **Spoke-side LAN v6 prefixes**: 2001:db8:BBBB::/48 and 2001:db8:CCCC::/48
- **6to4 tunnel prefix**: 2002:XXXX:XXXX::/64, where XXXX:XXXX is the IPv4 IP address of the tunnel source in hex. For example, demo-gm1 uses 10.5.110.34 as the tunnel source; the address can be represented in hex as 0a.05.6e.22. This hex address is embedded as a prefix in the v6 address on the VPN gateway. In our example, the v6 address would be 2002:A05:6E22::1/64, where the protected v6 hosts are assigned addresses in the space provided by XXXX:XXXX::Z. The destination to a remote v6 host is inferred from the target host assigned address.

Figure 4. Topology Diagram for Using IP 6to4 Tunnels



The routing of v6 packets is quite simple. The packets are encapsulated in 6to4 headers and routed out of the platform. If the 6to4 packet encounters a Group Encrypted Transport VPN cryptography map on the egress interface, the platform encrypts the v4 packet where the v6 frame is simply payload.

Group Encrypted Transport VPN configuration used in group members and key systems are the same as the configuration given in the section ”GDOI Encryption on IPv6 Traffic Using mGRE DMVPN Tunnels”. The following example uses 6to4 tunnels instead of a mGRE tunnel. Unlike mGRE tunnels, EIGRP configuration is not needed for 6to4 tunnels.

The following configurations show [[correct?]] an example 6to4 tunnel interface and routing statements.

Headquarters Group Member Router (demo-gm3) Configuration

IP 6to4 tunnel configuration used in headquarters group-member **demo-gm3** follows:

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo_getvpn
 ip address 10.5.110.54 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi
!
interface GigabitEthernet0/1
```

```
 description connected to the host
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:1111::1/64
 ipv6 enable
!
interface Tunnel100
 no ip address
 no ip redirects
 ipv6 address 2002:A05:6E36::1/16
 tunnel source GigabitEthernet0/0
 tunnel mode ipv6ip 6to4
!
router bgp 400
 network 10.5.110.52 mask 255.255.255.252
 neighbor 10.5.110.53 remote-as 900
 no synchronization
 bgp log-neighbor-changes
 no auto-summary
!
 address-family ipv6
 neighbor 2001:DB8:1111::2 remote-as 1000
 neighbor 2001:DB8:1111::2 activate
 neighbor 2002:A05:6E22::1 remote-as 200
 neighbor 2002:A05:6E22::1 activate
 neighbor 2002:A05:6E26::1 remote-as 300
 neighbor 2002:A05:6E26::1 activate
 network 2001:DB8:1111::/64
 exit-address-family
!
```

Branch-Office 1 Group-Member Router demo-gm1 Configuration

IP 6to4 tunnel configuration used in **demo-gm1** follows:

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo_dmvpn
 ip address 10.5.110.34 255.255.255.252
```

```
 ip pim sparse-mode
 crypto map demo-gdoi
!
interface GigabitEthernet0/1
 description connected to the host
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:BBBB:1::1/64
 ipv6 enable
!
interface Tunnel100
 no ip address
 no ip redirects
 ipv6 address 2002:A05:6E22::1/16
 tunnel source GigabitEthernet0/0
 tunnel mode ipv6ip 6to4
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.32 mask 255.255.255.252
 neighbor 10.5.110.33 remote-as 900
 no auto-summary
!
 address-family ipv6
 neighbor 2001:DB8:BBBB:1::2 remote-as 100
 neighbor 2001:DB8:BBBB:1::2 activate
 neighbor 2002:A05:6E36::1 remote-as 400
 neighbor 2002:A05:6E36::1 activate
 network 2001:DB8:BBBB:1::/64
 exit-address-family
!
```

Branch-Office 2 Group-Member Router demo-gm2 Configuration

IP 6to4 tunnel configuration used in **demo-gm2** follows:

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
```

```
 description connected to demo_dmvpn
 ip address 10.5.110.38 255.255.255.252
 ip pim sparse-mode
 crypto map demo-gdoi
!
interface GigabitEthernet0/1
 description connected to the host
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:CCCC:1::1/64
 ipv6 enable
!
interface Tunnel100
 no ip address
 no ip redirects
 ipv6 address 2002:A05:6E26::1/16
 tunnel source GigabitEthernet0/0
 tunnel mode ipv6ip 6to4
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 network 10.5.110.36 mask 255.255.255.252
 neighbor 10.5.110.37 remote-as 900
 no auto-summary
 !
 address-family ipv6
 neighbor 2001:DB8:CCCC:1::2 remote-as 2000
 neighbor 2001:DB8:CCCC:1::2 activate
 neighbor 2002:A05:6E36::1 remote-as 400
 neighbor 2002:A05:6E36::1 activate
 network 2001:DB8:CCCC:1::/64
 exit-address-family
```

IPv6 Host demo-v6-host-1 Configuration

This host is connected behind the group member in branch-office 1. The configuration used in **demo-v6-host-1** follows:

```
hostname demo-v6-host-1
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:BBBB:1::2/64
 ipv6 enable
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 no auto-summary
!
 address-family ipv6
 neighbor 2001:DB8:BBBB:1::1 remote-as 200
 neighbor 2001:DB8:BBBB:1::1 activate
 network 2001:DB8:BBBB:1::/64
 exit-address-family
! Default IPV6 route for return path
 ipv6 route ::/0 2001:DB8:BBBB:1::1
```

IPv6 Host demo-v6-host-2 Configuration

This host is connected behind the group member in branch-office 2. The configuration used in **demo-v6-host-2** follows:

```
hostname demo-v6-host-2
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip address
 ip pim sparse-mode
```

```
 ipv6 address 2001:DB8:CCCC:1::2/64
 ipv6 enable
!
router bgp 2000
 no synchronization
 bgp log-neighbor-changes
 no auto-summary
 !
 address-family ipv6
 neighbor 2001:DB8:CCCC:1::1 remote-as 300
 neighbor 2001:DB8:CCCC:1::1 activate
 network 2001:DB8:CCCC:1::/64
 exit-address-family
! Default IPV6 route for return path
ipv6 route ::/0 2001:DB8:CCCC:1::1
```

IPv6 Host demo-v6-host-3 Configuration

This host is connected behind the group member at headquarters. The configuration used in **demo-v6-host-3** follows:

```
hostname demo-v6-host-3
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 description connected to demo-gm1
 no ip address
 ip pim sparse-mode
 ipv6 address 2001:DB8:1111::2/64
 ipv6 enable
!
router bgp 1000
 bgp log-neighbor-changes
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv6
 neighbor 2001:DB8:1111::1 remote-as 400
```

```
 neighbor 2001:DB8:1111::1 activate
 network 2001:DB8:1111::/64
 exit-address-family
! Default IPV6 route for return path
ipv6 route ::/0 2001:DB8:1111::1
```

Verification of GDOI Encryption on IPv6 Traffic Using IP 6to4 Tunnels

Verify IP 6to4 tunnel operation in branch-office 1 router demo-gm1 by checking the tunnel interface information:

```
demo-gm1#show int Tunnel 100
Tunnel100 is up, line protocol is up
 Hardware is Tunnel
 MTU 17920 bytes, BW 100 Kbit/sec, DLY 50000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation TUNNEL, loopback not set
 Keepalive not set
 Tunnel source 10.5.110.34 (FastEthernet1/1)
 Tunnel protocol/transport IPv6 6to4
 Tunnel TTL 255
 Tunnel transport MTU 1480 bytes
 Tunnel transmit bandwidth 8000 (kbps)
 Tunnel receive bandwidth 8000 (kbps)
 Last input 2d23h, output 2d23h, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue: 0/0 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
   20663 packets input, 2745425 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   20993 packets output, 2172467 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
```

Verify IP 6to4 tunnel operation in branch-office 1 router demo-gm1 by checking connectivity:

```
demo-gm1#ping ipv6 2001:A05:6E36::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:A05:6E36::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
demo-gm1#ping ipv6 2001:A05:6E26::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:A05:6E26::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
```

Verify IP 6to4 tunnel operation in branch-office 1 router demo-gm1 by checking the route to hosts located in other branch offices:

```
demo-gm1#show ipv6 route 2001:DB8:1111::2
Routing entry for 2001:DB8:1111::/64
 Known via "static", distance 1, metric 0
 Route count is 1/1, share count 0
 Routing paths:
  2001:A05:6E36::1
   Last updated 3d00h ago

demo-gm1#show ipv6 route 2001:DB8:CCCC:1::2
Routing entry for 2001:DB8:CCCC:1::/64
 Known via "static", distance 1, metric 0
 Route count is 1/1, share count 0
 Routing paths:
  2001:A05:6E26::1
   Last updated 3d00h ago
```

Verify whether the IPv6 traffic between the host in branch-office 1 and the host at headquarters gets encrypted by Group Encrypted Transport VPN by using the following CLIs:

Check the number of packets encrypted in demo1-gm as follows:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 49862, #pkts encrypt: 49862, #pkts digest: 49862
```

From demo-v6-host-1 in branch-office 1, ping demo-v6-host-3 at headquarters:

```
demo-v6-host-1# ping ipv6 2001:DB8:1111::2 rep 1000
```

Check whether all the packets are encrypted in demo1-gm in branch-office 1:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 50862, #pkts encrypt: 50862, #pkts digest: 50862
```

Verify whether the IPv6 traffic between the host in branch-office 1 and the host in branch-office 2 gets encrypted by Group Encrypted Transport VPN by using the following CLIs:

Check the number of packets encrypted in demo1-gm as follows:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 53068, #pkts encrypt: 53068, #pkts digest: 53068
```

From demo-v6-host-1 in branch-office 1, ping demo-v6-host-2 in branch-office 2:

```
demo-v6-host-1# ping ipv6 2001:DB8:CCCC:1::2 rep 1000
```

Check whether all the packets are encrypted in demo1-gm in branch-office 1:

```
demo-gm1#show crypto ipsec sa | incl encaps
  #pkts encaps: 54068, #pkts encrypt: 54068, #pkts digest: 54068
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-598805-00 04/10