The need for mobility and flexibility in corporate networks can be achieved through the use of dynamic routing in DMVPN. However, this solution has created a new challenge, securing data exchange. Knowing that, IPsec cannot secure or encrypt the multicast packets used in dynamic routing. DMVPN solutions use a combination of several standard technologies together which are briefly explained below.

DMVPN Components

Dynamic multipoint VPN is based on the client / server model, it is a mechanism to establish IPsec/GRE (Generic Routing Encapsulation) tunnels directly between routers who want to interact with each other in a simplistic and totally dynamic way. GRE is an encapsulating protocol which can encapsulate multicast and broadcast packets in a unicast packet. Hence, it would be possible to encrypt it using IPsec. Basically, the solution is to implement multicast packets using GRE tunnels, and since GRE is not secure then IPsec is used for data encryption. Hence DMVPN components are as follows.

Next Hop Routing Protocol

In DMVPN two types of addresses are distinguished: Underlay and Overlay IP addresses. The underlay address is a public IP address used as the source or the destination address of the tunnel and the overlay address is a private IP address given to a GRE tunnel. Thus, the mapping between these addresses is done through the Next Hop Routing Protocol (NHRP). NHRP is based on the client-server standard ; the spokes (NHRP Clients) send periodic updates containing public and tunnel addresses to the hub (NHRP Server) of the network. Therefore, when a spoke router comes online, it automatically registers relational information with the hub router according to the external network public IP address of hub router and NHRP protocol.

Multipoint Generic Routing Encapsulation Multipoint Generic Routing Encapsulation (mGRE)

is responsible for the dynamic creation of tunnels. The use of mGRE is dependent on IPsec; since GRE tunnels can encapsulate multicast/broadcast packets into GRE packets, and GRE packets are unicast packets, so they can be encrypted by IPSec. That’s the multi and broadcast packet are transferred with mGRE and encrypted with IPSec. Basically, a GRE header is added to each packet which changes either the broadcast or multicast packet into a unicast. Since GRE uses the same link as IPsec, the IPsec header is applied to encrypt all the GRE data (Fig.1). Nevertheless, it is incapable of changing the physical IP address since the IPsec needs a fixed IP

address to create the IPSEC tunnel. Therefore, the GRE tunnel IP address is invariable.

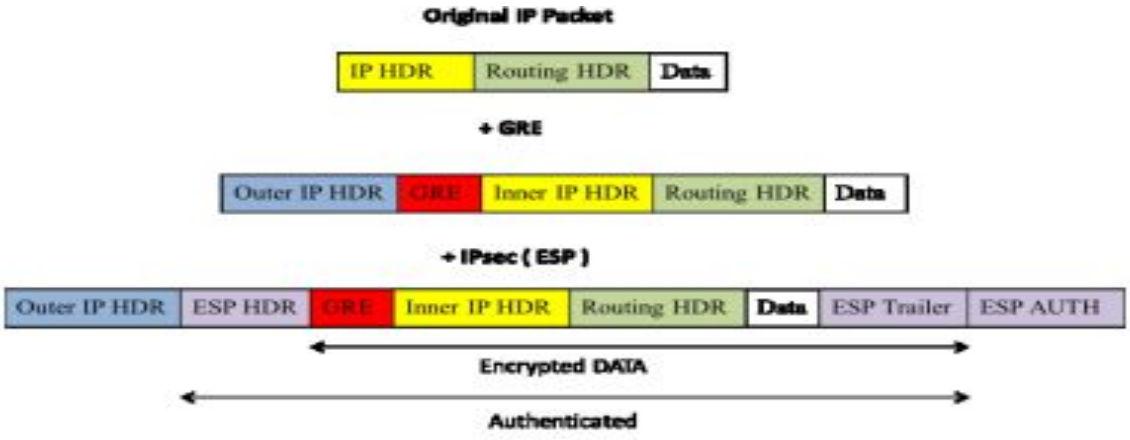

Fig 5.1: GRE/IPsec Encapsulation of an IP packet

Internet Protocol Security

The Internet protocol security (IPsec) itself is a set of protocols and mechanisms that provide end-to-end security in terms of encryption, authentication and integrity for all IP-enabled networks. IPsec is a flexible method to protect network traffic, it has relatively fewer vulnerabilities discovered and reported, and thus has become one of the most widely used VPN implementations. Despite that the use of IPsec in DMVPN is optional; it has a great importance to ensure the security of communicated data since GRE tunnels are not secured at all. Conventionally, IPSec uses an access control list (ACL) to define what data is to be encrypted. That is, when a data packet matches the defining entry of an ACL, the IPSec encryption tunnel will be set up immediately. However, when using IPSec/mGRE tunnels, the mGRE tunnel configuration includes the mGRE tunnel peer address already, which is also the IPSec peer address.

Routing Protocol

Beside all technologies mentioned previously, a dynamic routing protocol is mandatory for DMVPN. Indeed, routing protocols present a main part of the DMVPN solution, they ensure the smooth establishment of tunnels and have a major impact on network's behavior and transported applications. Hence, several works have been conducted assessing the network performances in order to determine the most convenient routing protocol for DMVPN . Among the routing protocols used for DMVPN we cite:

- Enhanced Interior Gateway Routing Protocol (EIGRP): a distance-vector routing protocol which is only available on cisco routers. EIGRP is used on a router to share routes with other routers within the same autonomous system.
- Routing Information Protocol ('RIP'): a distance-vector routing protocol which employs the hop count as a routing metric. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.
- Open Shortest Path First (OSPF): an IP based routing protocol which uses a link state routing algorithm and falls into the group of interior gateway protocols, operating within a single autonomous system.

DMVPN Phases

When there is a data exchange between two Spokes, the first spoke contacts the Hub, in order to obtain the information required on the other end, in order to be able to create a dynamic IPsec VPN tunnel directly between them. If the spoke uses a dynamic IP address, it must register with the headquarters router (Hub) while it joins the network every time. Then after passing the confirmation step, both routers can implement direct communication between them. The communication between spokes is done according to one of the three phases of DMVPN.

Phase 1:

Hub to Spoke In this phase, each spoke is configured with the IP address of the hub as the network server. Hence, each spoke has a static tunnel with a fixed destination IP which represents the Hub's physical address. Consequently, spokes can only get to each other across the hub. The key advantage of DMVPN Phase 1 is the simplified Hub configuration. Additionally, the choice of routing protocol is much easier since almost any dynamic routing protocol would help with attaining reachability. The hub just needs to advertise a default route to spokes, while spokes should advertise their subnets dynamically to the hub. However, the main drawback is inability to establish spoke-to-spoke shortcut tunnels. NHRP Phase 2 resolves this issue and allows for spoke-to-spoke tunnels

Phase 2:

Spoke to Spoke This mode requires all the spokes to have complete routing information with the next-hop preserved. Since not all spokes may accept full load of routing updates, this requirement may limit the scalability especially in large networks. The second phase limitation occurs in case of a network with 1000 spokes for example, where the routing table on each spoke will have too many entries, which essentially isn't needed. Hence it becomes difficult for the routers to have such a huge routing table.

Phase 3:

Spoke to Spoke with Scalable Infrastructure Basically, this phase accomplishes the same things as phase 2, but it improves on some of its limitations. Phase 3 fixed this problem in the most effective way. Because all spokes see the entire network being learned from the hub. The solution is to summarize the network on the hub. Hence DMVPN phase 3 can be used for very large deployments and it is a lot more scalable than DMVPN phase 2 and has a better hierarchy.

Simulation will be conducted with 9 scenarios. The scenario consists of DMVPN phase 1, phase 2 and phase 3 combined routing protocol RIP, OSPF, EIGRP. Each scenario will be simulated using GNS3 and parameters measured at each simulation is throughput, jitter, and packet loss.

The simulation uses the network simulation application Graphical Network Simulator 3 (GNS3) version 2.1.16,
VMware Workstation running on the operating system used is Windows 10. Cisco IOSv 15.6 series is used as a router with IOS operating system that runs on GNS3 and the Linux operating system inside Virtualbox as a PC. To determine the performance of the network, the author uses the Iperf3 tool application that runs on the PC.

The DMVPN solution introduces the following new commands:

crypto ipsec profile <name>
<ipsec parameters>

tunnel protection ipsec profile <name>

ip nhrp map multicast dynamic

With the DMVPN solution, IPsec is triggered immediately for both point-to-point and multipoint GRE tunnels.
Also, it is not necessary to configure any crypto ACLs, since these will be automatically derived from the GRE tunnel source and destination addresses. Notice that there is no set peer ... or match address ... commands required because this information is derived directly from the associated GRE tunnel or NHRP mappings.

crypto ipsec profile <profile-name>
set transform-set <transform-name>

The **crypto ipsec profile <name>** command is used like a dynamic crypto map, and it is designed specifically for tunnel interfaces. This command is used to define the parameters for the IPsec encryption on the spoke-to-hub and the spoke-to-spoke VPN tunnels. The only parameter that is required under the profile is the transform set.

The following command associates a tunnel interface with the IPsec profile.

interface tunnel<number>

...

tunnel protection ipsec profile <profile-name>

ip nhrp map multicast dynamic, allows NHRP to automatically add spoke routers to the multicast NHRP mappings when these spoke routers initiate the mGRE+IPsec tunnel and register their unicast NHRP mappings. This is needed to enable dynamic routing protocols to work over the mGRE+IPsec tunnels between the hub and spokes. If this command was not available, then the hub router would need to have a separate configuration line for a multicast mapping to each spoke.

The **ip nhrp authentication ...**, **ip nhrp network-id ...** and **tunnel key ...** commands are used to map the tunnel packets and the NHRP packets to the correct multipoint GRE tunnel interface and NHRP network when they are received on the hub. The **ip nhrp map ...** and **ip nhrp nhs ...** commands are used by NHRP on the spoke to advertise the spokes NHRP mapping (Spoke's Tunnel IP → Spoke's NBMA IP) to the hub. The NBMA IP address is retrieved from the ip address ... command on the tunnel interface and the tunnel IP address is retrieved from the tunnel destination ... command on the tunnel interface.

Supporting Dynamic Addresses on Spokes : Tunnel End-Point Discovery (TED) allows one IPsec peer to find another IPsec peer by sending a special Internet Security Association and Key Management Protocol (ISAKMP) packet to the IP destination address of the original data packet that needed to be encrypted. The assumption is that this packet will traverse the intervening network along the same path as taken by the IPsec tunnel packet. This packet will be picked up by the other-end IPsec peer, which will respond to the first peer. The two routers will then negotiate ISAKMP and IPsec Security Associations (SAs) and bring up the IPsec tunnel.

Once the IPsec tunnel is set up, an NHRP registration packet goes from the spoke router to the configured Next Hop Server (NHS). The NHS is the hub router of this hub-and-spoke network. The NHRP registration packet provides the information for the hub router to create an NHRP mapping for this spoke router. With this mapping, the hub router can then forward unicast IP data packets to this spoke router over the mGRE+IPsec tunnel. Also, the hub adds the spoke router to its NHRP multicast mapping list. The hub will then start sending dynamic IP routing

multicast packets to the spoke (if a dynamic routing protocol is configured). The spoke will then become a routing protocol neighbor of the hub, and they will exchange routing updates.

The concepts and configuration in this section show the full capabilities of DMVPN. NHRP provides the capability for the spoke routers to dynamically learn the exterior physical interface address of the other spoke routers in the VPN network. This means that a spoke router will have enough information to dynamically build an IPsec+mGRE tunnel directly to other spoke routers. This is advantageous since, if this spoke-to-spoke data traffic was sent via the hub router, then it must be encrypted/decrypted, twice increasing the delay and the load on the hub router. In order to use this feature, the spoke routers need to be switched from point-to-point GRE (p-pGRE) to multipoint GRE (mGRE) tunnel interfaces. They also need to learn the (sub)networks that are available behind the other spokes with an IP next-hop of the tunnel IP address of the other spoke router. The spoke routers learn these (sub)networks via the dynamic IP routing protocol running over the IPsec+mGRE tunnel with the hub.

The dynamic IP routing protocol running on the hub router can be configured to reflect the routes learned from one spoke back out the same interface to all of the other spokes, but the IP next-hop on these routes will usually be the hub router, not the spoke router from which the hub learned this route. The dynamic routing protocols (RIP, OSPF and EIGRP) need to be configured on the hub router to advertise the routes back out the mGRE tunnel interface and to set the IP next-hop to the originating spoke router for routes learned from one spoke when the route is advertised back out to the other spokes.

The following are requirements for the routing protocol configurations.

RIP

You need to turn off split horizon on the mGRE tunnel interface on the hub, otherwise RIP will not advertise routes learned via the mGRE interface back out that same interface.

no ip split-horizon

EIGRP

You need to turn off split horizon on the mGRE tunnel interface on the hub, otherwise EIGRP will not advertise routes learned via the mGRE interface back out that same interface.

no ip split-horizon eigrp <as>

EIGRP will, by default, set the IP next-hop to be the hub router for routes that it is advertising, even when advertising those routes back out the same interface where it learned them. So in this case, you need the following configuration command to instruct EIGRP to use the original IP next-hop when advertising these routes to create spoke-spoke tunnels.

no ip next-hop-self eigrp <as>

OSPF

Since OSPF is a link-state routing protocol, there are not any split horizon issues. Normally for multipoint interfaces you configure the OSPF network type to be point-to-multipoint, but this would cause OSPF to add host routes to the routing table on the spoke routers. These hosts routes would cause packets destined to networks behind other spoke routers to be forwarded via the hub, rather than forwarded directly to the other spoke. To get around this problem, configure the OSPF network type to be broadcast using the command.

ip ospf network broadcast

The hub router will be the Designated Router (DR) for the IPsec+mGRE network. This is done by setting the OSPF priority to be greater than 1 on the hub and 0 on the spokes.

- Hub: **ip ospf priority 2**
- Spoke: **ip ospf priority 0**

There are NHRP unicast and multicast mappings configured for the hub router.

ip nhrp map 172.16.4.1 10.1.1.1

ip nhrp map multicast 10.1.1.1

This command is now needed because the spokes GRE tunnel has changed to multipoint and there is more than one possible destination.

When the spoke router comes up, it must initiate the tunnel connection with the hub, since the hub router is not configured with any information about the spoke routers, and the spoke routers may have dynamically assigned IP addresses. The spoke routers are also configured with the hub as their NHRP NHS.

ip nhrp nhs 172.16.4.1

With the above command, the spoke router will send NHRP Registration packets through the mGRE+IPsec tunnel to the hub router at regular intervals. These registration packets provide the spoke NHRP mapping information that is needed by the hub router to tunnel packets back to the spoke routers.