# Cisco Dynamic Multipoint VPN (DMVPN) Configuration

Dynamic Multipoint VPN (DMVPN) is a Cisco IOS Software solution for building scalable IPsec Virtual Private Networks (VPNs).

Cisco DMVPN allows branch locations to communicate directly with each other over the public WAN (internet) without requiring a permanent VPN tunnel between sites. It enables zero-touch deployment of IPsec VPNs and improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization.

# Benefits

**Lowers capital and operational expenses** — Reduces costs in integrating voice, video with VPN security

**Simplifies branch communications** — Enables direct branch-to-branch connectivity for business applications like voice

**Reduces deployment complexity** — Offers a zero-touch configuration, dramatically reducing the deployment complexity in VPNs

**Improves business resiliency** — Prevents disruption of business-critical applications and services by incorporating routing with standards-based IPsec technology

# Network Diagram

The following diagram represents our DMVPN network. Our goal is to enable the communication of 2 LANs that are behind routers R2 and R3 with company’s head office LAN which is behind HUB router. The head office router (HUB) is the central Hub router which will act as NHRP server containing information about all spoke routers (R1 & R2), their public IP addresses and LANs connected to them.

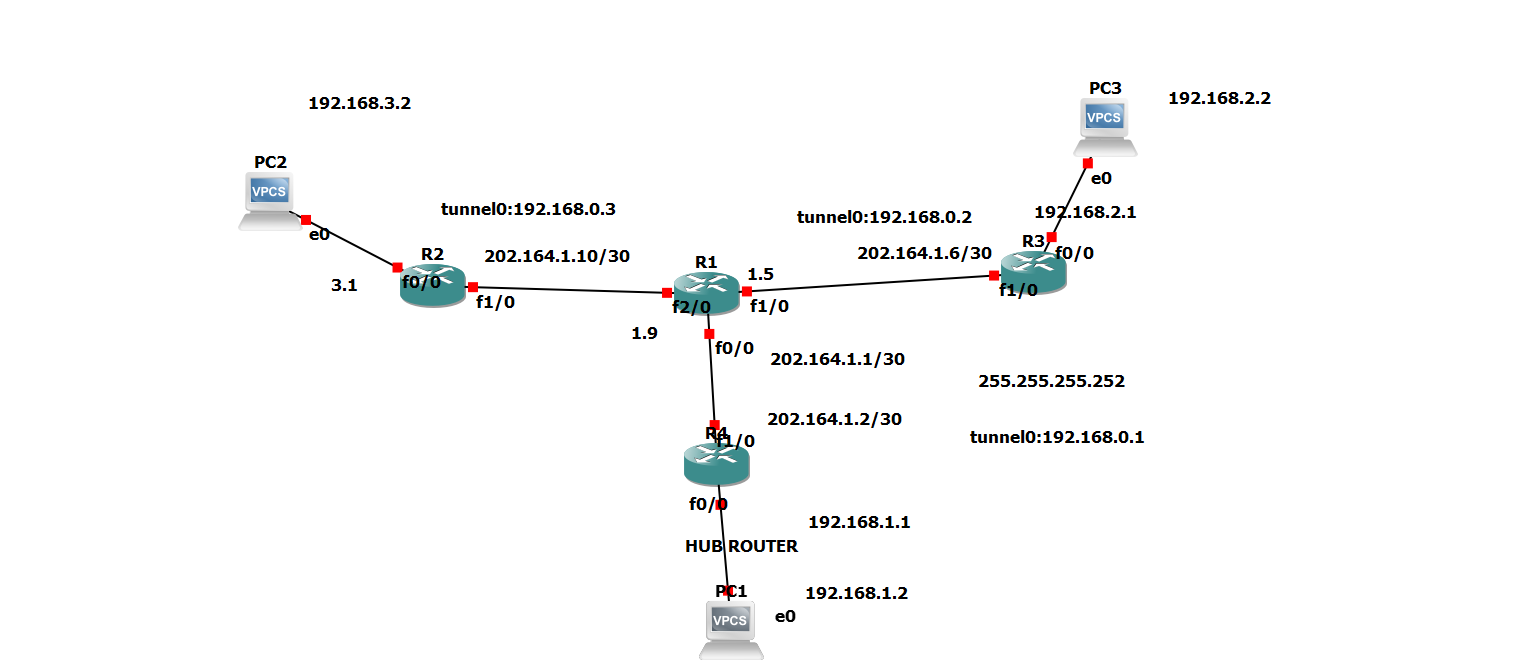


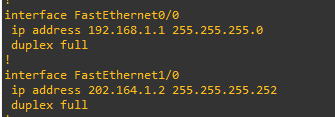
Fig: Network Diagram 1

# Configuration Steps

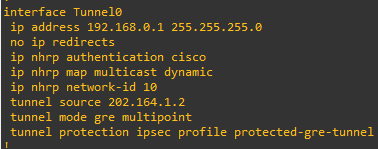
The whole DMVPN configuration contains following steps:

* Configuring the Hub router
* Configuring the Spoke routers
* Configuring the routing between GRE Tunnels
* Protecting the tunnels with IPSec

Following is the configuration of Outside and Inside interfaces of Hub router:



Following is the configuration of tunnel interface (Tunnel 0):



### Explanation of above configuration commands:

**ip address *192.168.0.1 255.255.255.0*:**This command configures the IP address on tunnel interface.

**no ip redirects:** This disables icmp redirect messages. Redirects happen when a router recognizes a packet arriving on an interface and the best route is out that same interface. This command is highly recommended from a security point of view because ICMP redirect messages can be used by an attacker to generate network topology and perform network diagnosis.

**ip nhrp authentication *cisco*:** This command allows you to specify a password for your DMVPN network so not just any GRE tunnel can join your DMVPN cloud. In our example ***cisco***is the password.

**ip nhrp map multicast dynamic:** This command allows NHRP to automatically map multicast traffic from other devices, without the need to statically configure each device.

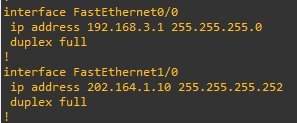
**ip nhrp network-id *10*:** The NHRP network-id number ensures this DMVPN interface only participates within it’s own DMVPN network. Just in case you have more the one tunnel interface on the same router connected to two separate DMVPN clouds/networks. All routers participating in DMVPN cloud must have the same network-id configured in order for tunnels formation. We used ***10*** in our example.

**tunnel source *202.164.1.2*:** This command specifies the tunnel source. The static IP of Outside interface must be used for Hub router. in our example the IP is ***202.164.1.2***.

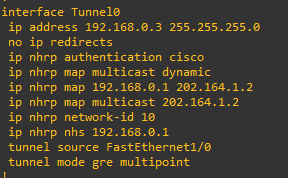
**tunnel mode gre multipoint**: This command specifies that the tunnel interface is GRE multipoint, means this will be acting as single interface connected to multiple spokes.

## Configuring the Spoke router (R2)

Following is the configuration of Inside and Outside interfaces of R2:

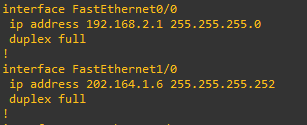


Following is the configuration of tunnel interface (Tunnel 0) on branch router R2:

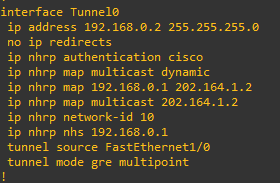


## Configuring the Spoke router (R3)

Configuration of all the spokes is almost same. Following is the configuration of R3 spoke router:



Following is the configuration of tunnel 0 interface:

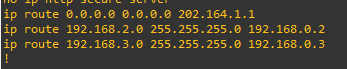


## Configuring the Routing Between GRE Tunnels

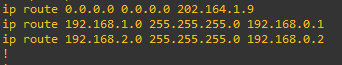
Next step is to enable the routing in our DMVPN network. This is required so that the hub and spoke routers are aware which packets need to be sent via the VPN tunnel.

We will configure the static routes on all routers so that routers could route the traffic between LANs connected behind each router. You can also use routing protocols such as EIGRP or OSPF but we will only configure static route in our topology.

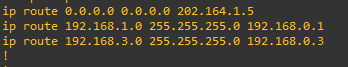
Static Route on Hub Router



Static Route on Spoke Router R2



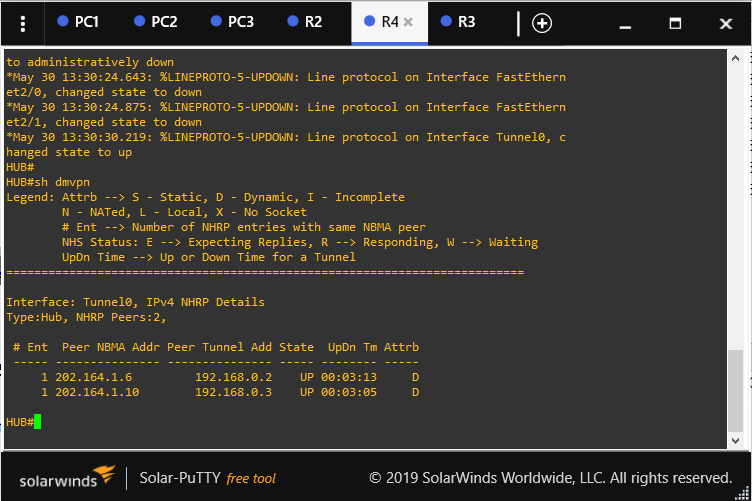
Static Route on Spoke Router R3



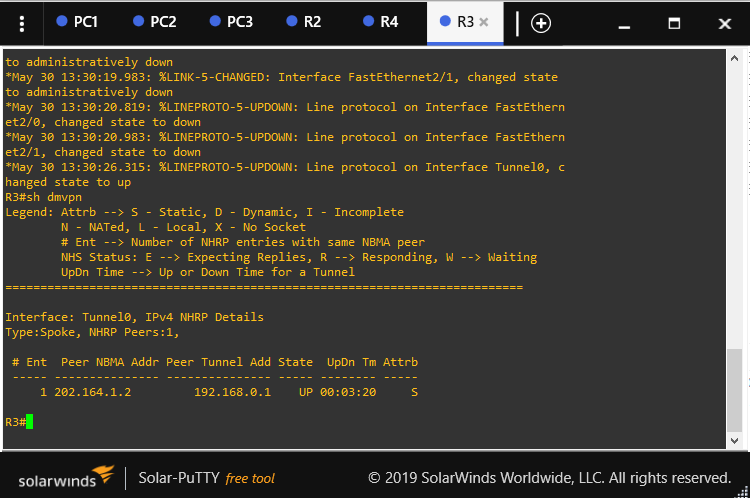
# Checking The Progress

At this point, our DMVPN network is ready. All networks are connected to each other and dynamic VPN tunnels between spokes can be established.

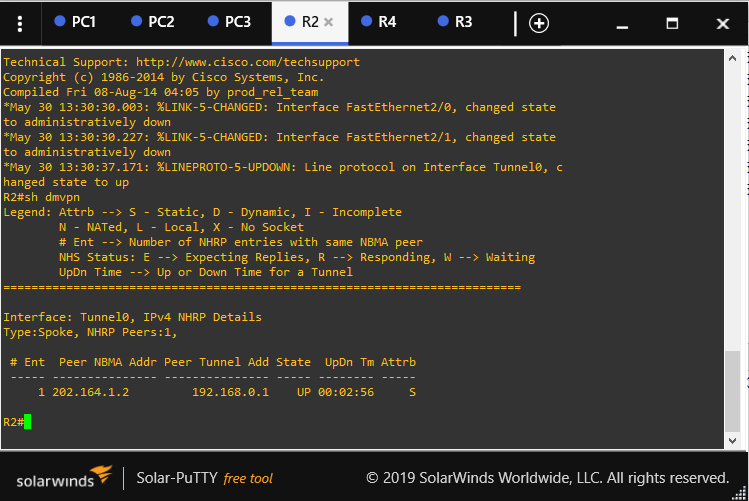
To view the status of DMVPN, you can use ***show dmvpn*** command on router. Below are the screenshots of ***show dmvpn*** command on all of our routers:











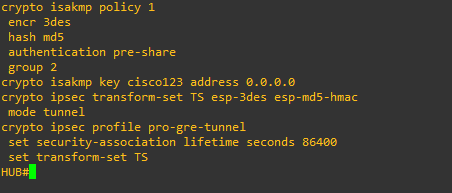


# Encrypting the DMVPN mGRE tunnels with IPSec

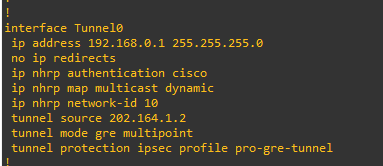
Since our mGRE tunnels are running in vulnerability, we need to encrypt them using IPSec to ensure that if anybody manage to capture our traffic, he will still not be able to read it.

We will create the IPSec policy on our routers and apply the policy on tunnel interface (Tunnel 0).

## IPSec Configuration on Hub router



Now apply the IPsec profile on Tunnel interface and final configuration of Tunnel 0 interface will look like below:

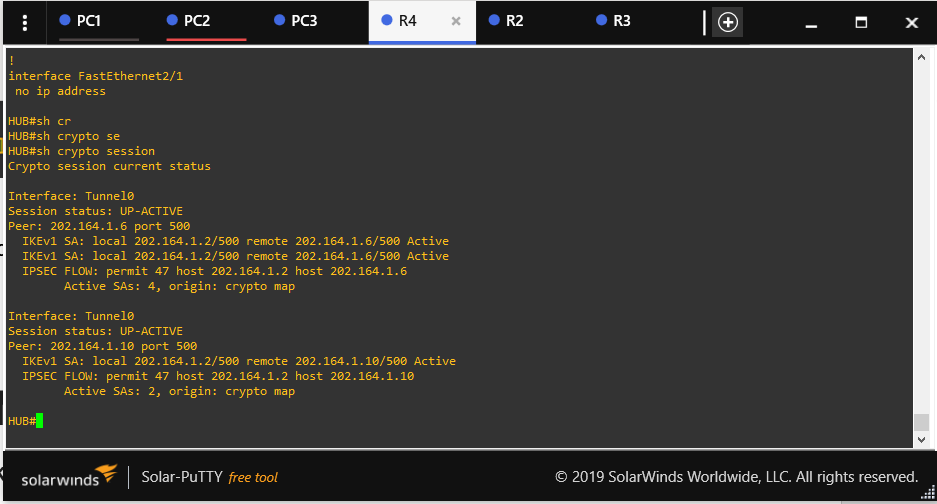




Same above two configurations are done on R2 and R3. Now that our tunnels are protected with IPSec

# Verifying the DMVPN Network

At this point our DMVPN network is fully configured and protected with IPSec. To verify the tunnels, you can use ***show crypto session*** command. The output of command is shown below:













# Conclusion

This is how we configure a DMVPN network using Cisco routers.

# References

https://www.techtutsonline.com/cisco-dynamic-multipoint-vpn-dmvpn-configuration/#Benefits