Mitigate Network Design Difficulties DMVPN

Abstract/Introduction

Many variables exist whenever an engineer, or engineers, architects a network enterprise. Over time, the variables magnify as the needs of the enterprise change. Engineers must consider key components, such as available subnet space, addressed optimized routing (either static or dynamic), enterprise expansion, and security, as the enterprise, and the technology, holistically evolves and grows. Though the endeavor seems challenging, engineers know that there are a variety of ways expansion difficulties and secure communications between various new branch locations—or even existing locations—can be mitigated and simplified.

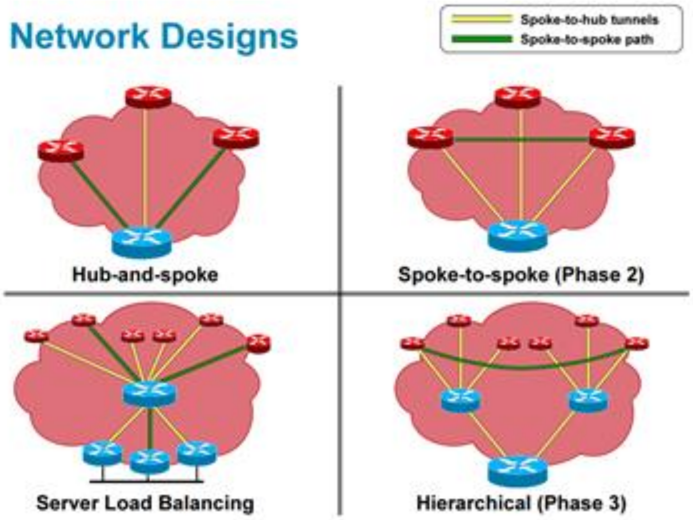
One such way leverages a widely known and incredibly useful technology known as DMVPN, or Dynamic Multipoint VPN. Readers may or may not have familiarity with the term or concept. This paper will explain DMVPN and definite its importance in use-case scenarios such as the aforementioned.

DMVPN, in its most basic function, allows remote branch locations to securely communicate with each other instead of directly needing to go back through the primary location, or "headquarters." It uses what is referred to as a hub-and-spoke architecture, which is another way of referring to a headquarter (the hub) and remote branch locations (the spokes). The general layout is essentially a dynamic-mesh VPN network that is encrypted using key cogs, including: IPSec, mGRE (Multipoint GRE), dynamic routing (such as BGP, OSPF, etc.) and NHRP (Next Hop Resolution Protocol) technologies. DMVPN essentially uses these GRE and mGRE tunnels as an overlay on the physical infrastructure.

Below is a brief overview from Cisco on various design methods involving DMVPN:

ABOUT THE AUTHOR

Michael Keller is a solutions-driven network architect, engineering professional and consultation expert. For more than two decades, he has supported a wide array of enterprise clients that have expressed the need to upgrade their existing wireless architecture from both a hardware and software perspective. He has validated and overseen countless architectural optimization efforts through surveys, calibrations, configuration, and installations. His experience includes developing, monitoring, and managing enterprise networking equipment for commercial companies and the United States Military.



What are “phases” as it pertains to DMVPN? In condensed terms, think of the “phases” in this way: Phase one is essentially a hub-to-spoke topology, phase two involves spoke-to-spoke, and phase three (the most scalable) is essentially a hierarchal topology reaping the benefits of both phase one and two involving summarization (P1) and spoke-spoke-spoke traffic flow (P2).

The phases work well because DMVPN is essentially a routing method that eliminates the need to statically configure devices and allows branch locations to communicate safely and securely with each other using the same resources – without the overhead required for a centralized VPN router, server, etc.

The phases yield benefits, which include reducing costs by leveraging VPN with communication between branches and allowing for better reliability and performance with encryption-security, in general. More importantly, DMVPN simplifies communication, reduces configuration, and adds a breadth of reliability between branch locations.

In short, DMVPN is a variety of protocols working together to achieve WAN encryption between branches.

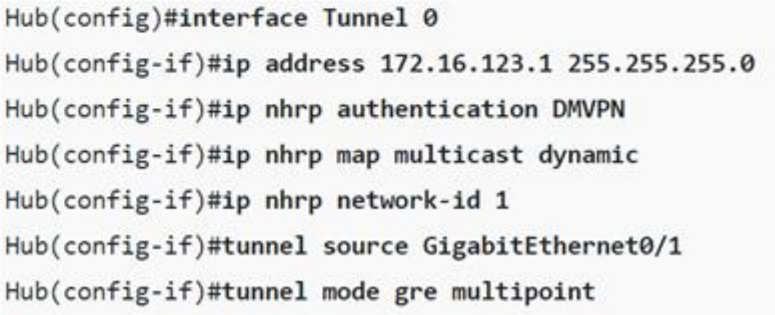
Problem Statement

A situation might arise in which enterprise senior management plans to establish simple spoke-to-spoke communication that leverages DPVPN technology between two branches. This scenario harkens back to DMVPN phase two (spoke-to-spoke). In this situation, the routing table is key. A spoke route will look at its routing table to determine the next-hop IP address. In DMVPN phase two, all spoke routers use multipoint GRE (with encrypted tunnels using IPSec). Loopback addresses and tunnel interfaces are an important co-factor as well.

How might one accomplish this?

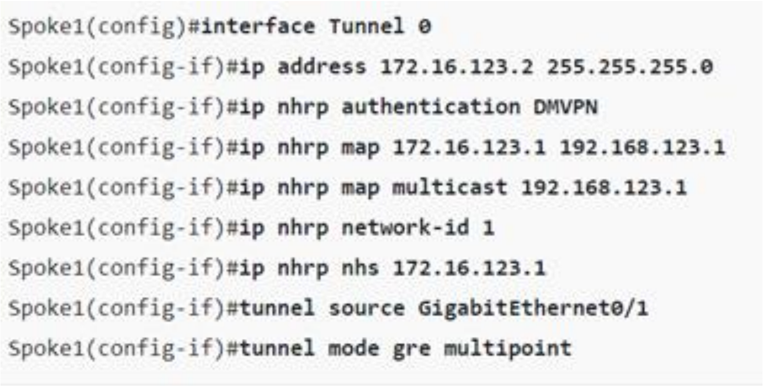
Phase two is close to phase one from a configuration standpoint (albeit working differently), though phase one lacks “direct” spoke-to-spoke communication. Phase two contains a mGRE tunnel interface on the spoke, which means that phase two has spoke-to-spoke tunneling. If a spoke router opts to communicate with another spoke, it will then send out an NHRP resolution request to the hub in search of the NBMA address of that other spoke.

The following example is of DMVPN phase two configuration on a hub router using a generic private IP addressing/subnet range (to keep things streamlined, please note that the last octet in the IP addressing of each tunnel indicates hub equaling .1, spoke one is .2 and spoke two is .3.):

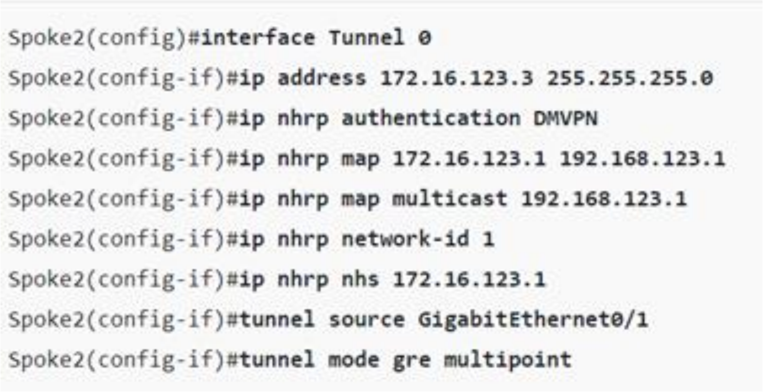


```
Hub(config)#interface Tunnel 0
Hub(config-if)#ip address 172.16.123.1 255.255.255.0
Hub(config-if)#ip nhrp authentication DMVPN
Hub(config-if)#ip nhrp map multicast dynamic
Hub(config-if)#ip nhrp network-id 1
Hub(config-if)#tunnel source GigabitEthernet0/1
Hub(config-if)#tunnel mode gre multipoint
```

And the spokes' configuration:



```
Spoke1(config)#interface Tunnel 0
Spoke1(config-if)#ip address 172.16.123.2 255.255.255.0
Spoke1(config-if)#ip nhrp authentication DMVPN
Spoke1(config-if)#ip nhrp map 172.16.123.1 192.168.123.1
Spoke1(config-if)#ip nhrp map multicast 192.168.123.1
Spoke1(config-if)#ip nhrp network-id 1
Spoke1(config-if)#ip nhrp nhs 172.16.123.1
Spoke1(config-if)#tunnel source GigabitEthernet0/1
Spoke1(config-if)#tunnel mode gre multipoint
```



```
Spoke2(config)#interface Tunnel 0
Spoke2(config-if)#ip address 172.16.123.3 255.255.255.0
Spoke2(config-if)#ip nhrp authentication DMVPN
Spoke2(config-if)#ip nhrp map 172.16.123.1 192.168.123.1
Spoke2(config-if)#ip nhrp map multicast 192.168.123.1
Spoke2(config-if)#ip nhrp network-id 1
Spoke2(config-if)#ip nhrp nhs 172.16.123.1
Spoke2(config-if)#tunnel source GigabitEthernet0/1
Spoke2(config-if)#tunnel mode gre multipoint
```

The DMVPN phase 2 deployment configuration setup is fairly simple. Engineers can advertise these interfaces into a dynamic routing protocol, such as EIGRP, but they must disable *split-horizon* on the hub to enable routes from one spoke to another. Disabling *split-horizon* on the hub will allow the hub to advertise the networks back out to the spoke routers; however, the spokes will drop the advertisements, because, otherwise, they would receive an advertisement from a neighbor with its own IP address as the next-hop (!).

Finally, IPSec encryption ensures tunnel protection. Configuring IPSec encryption involves creating and configuring an ISAKMP policy across all routers on the topology. Engineers will use either PKI or PSK to ensure tunnel security. After that, engineers will define a NBMA address (public address) because NHRP messages must resolve the NBMA address with the VPN address. Once implemented, the engineer can verify the topology by issuing a traceroute that verifies spoke-to-spoke traffic, in addition to *show dmvpn*. A simple, successful ping to the loopback interface of a neighboring spoke will point engineers towards correct configuration.

Background

Michael Keller is a Senior Consulting Engineer that has designed, architected, and configured intricate, complex routing and switching topologies for a variety of customers with many years of experience. With a seasoned background in more involved routing and switching deployments, his real-world experience in deploying DMVPN provides a strong knowledge base to help others successfully transition or upgrade their enterprise to state-of-the-art, optimal industry standards.

Solution

Successful network design includes an engineer’s plan for what will succeed and what might not during the network journey. In this case, the solution for deploying DMVPN – in any phase – is to properly configure it using a suite of protocols that work collectively and establish inter-spoke connectivity both securely and properly. The solution above outlines a simple spoke-to-spoke topology utilizing DMVPN phase two technology.

Conclusion

DMVPN can be incredibly useful when implemented under the circumstances, as outlined. Hub and spoke endpoints can be efficiently managed with a level of flexibility and security needed to ensure the optimal communication needs of the enterprise are met. However, it is key to understand that deploying DMVPN requires context and what you as the engineer are ultimately trying to achieve. It can be an incredibly useful protocol

While DMVPN can be a complex and granular topic to discuss, this brief overview offered a glimpse into its usefulness and the appropriate situations in which to use it.

References

https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn

https://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network

https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/prod_presentation0900aecd80313c9d.pdf

https://www.fieldengineer.com/blogs/dynamic-multipoint-vpn

https://hainc.com/dmvpn-what-is-it-when-should-i-use-it/

https://learningnetwork.cisco.com/s/article/dmvpn-concepts-amp-configuration

https://learningnetwork.cisco.com/s/question/0D53i00000Z7vDRCAZ/disabling-splithorizon-for-eigrp-using-dmvpn-ii

About Aspire Technology Partners

Aspire is a professional technology services firm specializing in the delivery of digital infrastructure solutions and managed services designed specifically to achieve our clients' business goals. We believe technology sits at the heart of every enterprise strategy. Our team takes time to understand your business initiatives and align technology solutions to drive the organization forward. Aspire's outcome-driven approach accelerates your journey by combining secure digital infrastructure, world-class design and implementation expertise, and managed services – all centered around transforming today's multi-cloud architectures into enablers of business value. Headquartered in Eatontown, New Jersey, Aspire is focused on serving the tri-state, mid-Atlantic, and New England regions with local operations in Mount Laurel, NJ; Albany and White Plains, NY; and Cambridge, MA. For more information, visit www.aspiretransforms.com.