EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

To Design a Network That Delivers Reliable Performance 24 Hours a Day 7 Days a Week for Higher Education in Uganda

Yakubu Ajiji Makeri[1,*]

[1]Kampala International University Uganda, School of Computing and Information Technology

Abstract

It aims at existing defects of traditional VPN (Virtual Private Network) in constructing enterprise network, analyses problems which must be considered in designing secure enterprise network, puts forward solution of DMVPN (Dynamic Multipoint VPN) technique to solve the problems that traditional VPN has not solved by now. At the same time, it expatiates on the implementation mechanism of DMVPN, puts forward a concrete case that to adopts the DMVPN technique constructs secure enterprise network of some universities and business chain organization, and network performance indexes are tested. From the results of the test, the DMVPN network entirely satisfies the actual requirements that an enterprise uses a network. It offers a mode that is a convenient and economical investment to an enterprise for building a secure network.

Keywords: Virtual Private Network, designing secure enterprise network, secure enterprise network.

Received on 26 May 2020, accepted on 15 July 2020, published on 16 July 2020

doi: 10.4108/eai.5-6-2020.165914

*Corresponding author. Email: yakubu.makeri@kiu.ac.ug

1. Introduction

The fast-moving of digital communications, companies are tending increasingly to use these new technologies for the storage of their data and archiving their activities with a quick, secure and distributed manner over several sites, with the use of VPN technologies, companies can communicate with each other securely through a public shared infrastructure “Internet” with a low cost compared to traditional solutions such as Frame Relay, ATM , etc. Wireless sensor networks are collections of autonomous devices (sensor nodes) endowed with computational, sensing and wireless communication capabilities Most universities extend their departments, which constitute a scalability problem, a reconfiguration of all equipment and a reservation of new static public IP address must be done. Dynamic Multipoint Virtual Private Network solution “DMVPN” proposed by Cisco corporation guarantees a full meshed connection between multiple sites with a dynamic, quick and automatic manner, DMVPN offers scalability, i.e. involves no extra configuration on already configured equipment. DMVPN architecture consists mainly of a Hub and a Spoke routers, Hub router called head office router, play a main role on dynamic creation of tunnels between multiple spokes, the letters are called Branch office routers, from the deployment perspective spokes builds a dynamic permanent tunnel to the HUB but not to other spokes, tunnels between spokes are temporarily created on-demand and deleted when exchanges are finished. DMVPN solution is based on the standard protocols; Multipoint Generic Routing Encapsulation « mGRE », Next-Hop Resolution Protocol « NHRP », Internet Protocol Security « IPsec » and routing protocols, the settings of these protocols vary from one architecture to another, the method “Policy-Based Management of a Secure Dynamic and Multipoint Virtual Private Network” enables centralized management of multiple DMVPN equipments, through a single graphical interface as follow

GRE: Generic routing protocol is a tunneling protocol that can encapsulate a variety of network layer protocols inside IP protocol , GRE tunnels forward Unicast, Multicast and broadcast traffic but they are static it means that a specification of combination of source and destination of each tunnel is required, mGRE allows to establish multiple tunnels across a single physical interface with multiple dynamic destinations.

2. Background Study

The challenges placed on IT daily grow more demanding. As well as the business user demands for access to new applications and services with minimal time to plan and make these operational, user expectations reflect the desire to access systems from wherever they are, using any device they want, at whatever time they wish. Enterprise in Uganda is becoming more dependent on the use of online applications and services to operate. This is forcing the IT department in the enterprise in Uganda to consider how to efficiently and securely enterprise can carry out its operations. One factor common to most application performance and security challenges can be found in enterprise networks, which connect users and business operations to the IT systems on which they depend. A recent study by Freeform Dynamics examined whether network infrastructures deployed in organizations today are capable of supporting changing work patterns and evolving to address existing as well as emerging threats. Yes, most networks are designed to support scalability that is, the network designed can grow to include new user groups, remote sites and can support new applications without impacting the level of service delivered to existing users. Security is always in the thoughts of IT and network managers. Enterprise in Lagos, design network in blocks sometimes to prevent a security bridge on one portion of the network from affecting another portion of the network. For example, a security bridge in a particular LAN portion should not affect the Datacenter if the network is designed in the block. sThis paper will be basically on designing a network that scalable, manageable, secure and highly available to meet organizational needs 24 hours 7 days a week.

3. Problem Statement

When network devices communicate with many other devices, the workload required of the CPUs on the devices can be burdensome. For example, in a large flat (switched) network, broadcast packets are burdensome. A broadcast packet interrupts the CPU on each device within the broadcast domain, and demands processing time on every device for which a protocol understanding for that broadcast is installed. This includes routers, workstations, and servers. Another potential problem with nonhierarchical networks, besides broadcast packets, is the CPU workload required for routers to communicate with many other routers and process numerous route advertisements. A hierarchical network design methodology lets you design a modular topology that limits the number of communicating routers. Using a hierarchical model can help you minimize costs. You can purchase the appropriate internetworking devices for each layer of the hierarchy, thus avoiding spending money on unnecessary features for a layer. Also, the modular nature of the hierarchical design model enables accurate capacity planning within each layer of the hierarchy, thus reducing wasted bandwidth. Network management responsibility and network management systems can be distributed to the different layers of a modular network architecture to control management costs.

Modularity lets you keep each design element simple and easy to understand. Simplicity minimizes the need for extensive training for network operations personnel and expedites the implementation of a design. Testing a network design is made easy because there is clear functionality at each layer. Fault isolation is improved because network technicians can easily recognize the transition points in the network to help them isolate possible failure points.

The hierarchical design facilitates changes. As elements in a network requirements change, the cost of making an upgrade is contained to a small subset of the overall network. In large flat or meshed network architectures, changes tend to impact a large number of systems. Replacing one device can affect numerous networks because of the complex interconnections.

4. Aims and Objectives

To design a network that delivers consistent, reliable performance, 24 hours a day, 7 days a week. In addition, the failure of a single link or piece of equipment should not significantly impact network performance.

Security must be considered when designing a network. Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.

5. Literature Review

5.1 Introduction

The enterprise campus network is usually understood as that portion of the computing infrastructure that provides access to network communication services and resources to end-users and devices spread over a single geographic location. It might span a single floor, building or even a large group of buildings spread over an extended geographic area. When building an enterprise network it

is necessary to have good knowledge of some of the networking models that are used in modern enterprise network designs. Networks are designed in hierarchy or modules with high availability. The hierarchical network model was one of the first models that divided the network into the core, distribution, and access layers. The Enterprise Architecture model provides a functional modular approach to network design. In addition to a hierarchy, modules are used to organize server farms, network management, campus networks, WANs, and the Internet. But since this project is restricted to just the LAN section of an enterprise network, it will only contain an overview of the enterprise architecture model. A modular approach to network design allows for higher scalability, better resiliency, and easier fault isolation of the network. Computers and information networks are critical to the success of businesses, both large and small. They connect people, support applications and services, and provide access to the resources that keep the businesses running. To meet the daily requirements of businesses, networks themselves are becoming quite complex.

5.2 Building a Good Network

Good networks do not happen by accident. They are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business.

The steps required to design a good network are as follows:

- Step 1. Verify the business goals and technical requirements.
- Step 2. Determine the features and functions required to meet the needs identified in Step 1.
- Step 3. Perform a network-readiness assessment.
- Step 4. Create a solution and site acceptance test plan.
- Step 5. Create a project plan.

After the network requirements have been identified, the steps to designing a good network are followed as the project implementation moves forward. Network users generally do not think in terms of the complexity of the underlying network. They think of the network as a way to access the applications they need, when they need them. NHRP: Next Hop Resolution Protocol is a resolution protocol like ARP and RARP on frame relay network, NHRP is used by a Spoke connected to Non-Broadcast Multi-Access “NBMA” to determine the IP address of the NBMA Next-Hop physical address (Public address), that could be of the HUB or another Spoke on the same cloud. All Spokes called Next-Hop Clients (NHC) register their physical addresses mapped to logical addresses (Tunnel address) with the HUB called Next-Hop Server (NHS), to ensure success of these registrations, NHS and NHC must be connected to the same Cloud and uses identical network ID and Network Password, the addresses of NHS must be pre-configured on each branch router. NHS Stores all registered mappings and replies to NHRP requests from Clients. NHRP allows mGRE tunnel endpoint to discover each other’s physical IP addresses.

- Dynamic routing protocols (detailed on the next section) are responsible for the creation, maintenance and updating dynamically routing tables, in order to ensure the optimal exchange of data between various sites.
- Many research studies have been conducted assessing the performances of DMVPN network , the first article evaluates the performances of DMVPN network varying both, dynamic routing protocols and the size of intermediaries routers, as DMVPN is a client solution, this was a good motivation to complete and to enhance the work by assessing DMVPN performances by varying the number of client-side routers, others works deal with the best practices for deploying dynamic routing protocols on DMVPN networks but without showing the improvement to the network. This project firstly explains about VPN theory (types of VPN), secondly studies the Design of DMVPN network using EIGRP as Routing Protocol, and Implementation of DMVPN between HQ and three Branches and finally the verifications.

Numerous universities factors are contributing to the rise of the departments and the need to empower the many and varied employees who work there are:

5.3 Globalization of the world's markets:

Businesses are reaching out to customers around the world, and many have opened offices in major cities to gain a worldwide presence.

5.4 The trend toward mergers and acquisitions:

Newly combined companies often leave offices in their original, disparate geographic locations.
With the heightened status of branch offices within organizations, it is more important than ever to equip distributed workers with the same productivity tools as their headquarters' counterparts. Historically, most branch offices have been afterthoughts and have received less-sophisticated and lower-performance network technology and IT services than headquarters. One reason is that branch-office networks are tethered to a WAN, which-until recently-has been inherently slower and more latency-prone than local networks. Another is that branch offices have evolved incrementally to contain inconsistent equipment and service sets across sites. This situation makes it complex to add new services, particularly in organizations without local IT staff. However, business conditions make it necessary to elevate remote workers'

network experience to be equivalent to that of employees connected directly to the corporate LAN.

Integrated security facilitates basic and advanced security services in the branch office and on the WAN to improve overall network security and extend the trusted domain of the enterprise to include the branch office. Dynamic Multipoint Virtual Private Network (DMVPN) is a solution that enables the data to transfer from one site to another, without having the verification process of traffic. That use to be held at the main VPN server of the concerned organization. This process helps the data to move from one end to another in the establishment of a secured network. It is integrated with a unique software that constructs IPsec and GRE VPNs in an unchallenged way. DMVPN Software solution is also involved in creating new and more secure communication routes in order to maintain network security while having entire integration with all the relevant departments.

5.5. Problem Statement

The goal of this research is to design a corporate computer communication network with a branched network of the affiliate departments of universities. The requirements we have on our solution are that the branched network of affiliates could be regionally extended, international-extended or worldwide-extended with a focus on the remote branch network implementation and avoid traditionally VPN to connect each remote site to the headquarters.

6. Aim and Objectives

There are various advantages of Dynamic Multipoint Virtual Private Network, a large amount of capital is not required, operational expenses are reduced. In VPN Security, the cost of integrating multimedia can be experienced with huge decrements. It shows great improvement in business flexibility, Business can easily complete their targets and if they are facing any sort of loss, they can easily recover it very soon and reaching their break-even level is not difficult anymore. The entire business flexibility enhances rapidly. By using IPsec technology disruption in business also reduced rapidly. Communication routes get easier and cheaper as Connectivity in the department of the university to level establishes a strong connection, particularly for voice and video sort of application and hence quick decision making. Huge decrements in deployment complexity occur. Zero-touch configurations are incorporated.

7. Significance of the Study

DMVPN is a secure network that exchanges data between sites without needing to pass traffic through an organization's headquarter virtual private network (VPN) server or router. VPNs traditionally connect each remote site to the headquarters; the DMVPN essentially creates a mesh VPN topology. This means that each site (spoke) can connect directly with all other sites, no matter where they are located. The use DMVPN to connect remote sites to a larger corporate network across the public Internet using a standard router configuration that's hands-off once completed and eliminates the need to know remote IP addresses, allowing for dynamically assigned IPs to connect to the infrastructure securely, registering their IP address with the DMVPN NHRP hub router.

8. Scope of the Research

This research will focus on developing a Design and Implementation of Secure Enterprise Network Based on Dynamic Multipoint Private Network of any university with departments. With Cisco systems as a long-time leadership in router and WAN technologies allow us to meet the specialized needs of the department while also optimizing the entire corporate network. Within an integrated network, the branch office can combine multiple components to make the whole better than the sum of its parts. Cisco combines software, hardware, routers, switches, mobility, security, and unified communications to provide consistent, secure service delivery across the WAN, simplifying operations of the entire networked system. Cisco integrated services routers also combine many of the functions of standalone appliances, giving customers an elegant service platform that offers flexibility to meet the specific needs of each remote branch on a consistent platform. Finally, whether integrated or standalone, the Cisco platform delivers innovation and depth of features for routing, switching, security, unified communications, mobility, and application intelligence. Therefore Due to resource availability and time constraint this project is limited to design and implement DMVPN using Cisco Technologies, based on GNS3 Simulation.

9. Implementation and Result

9.1 Introduction

For those enterprise networks that are seeking to reduce dependence on spanning tree and a common control plane, are familiar with standard IP troubleshooting tools and techniques, and desire optimal convergence, a routed access design (Layer 3 switching in the access) using EIGRP or OSPF as the campus routing protocol is a viable option. To achieve the optimal convergence for the routed access design, it is necessary to follow basic hierarchical design best practices and to use advanced EIGRP and OSPF functionality, including stub routing, route summarization, and route filtering for EIGRP, and LSA and SPF throttle tuning, totally stubby areas, and route summarization for OSPF as defined in this

document. This chapter basically on how we configure LAN network with EIGRP for optimization on a layer 3 switch command line interface.

9.2 1VPN Protocols

PPTP (Point-to-Point Tunneling Protocol)

Point-to-Point Tunneling Protocol (PPTP) is a Layer 2 tunneling protocol that allows a remote client to use a public IP network in order to communicate securely with a private network. Remote users can access a private network via PPTP by first dialing into their local ISP. PPTP connects to the target network by creating a virtual network for each remote client.

L2TP (Layer 2 Tunneling Protocol)

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support VPNs. It does not provide any encryption or confidentiality by itself. Rather it relies on an encryption protocol that it passes within the tunnel to provide privacy.

10. GRE (Generic Routing Encapsulation)

10.1. Tunneling Overview

Tunnels provide a way to transport protocols that the underlying network does not support. There are several reasons why this may be:

- The network infrastructure doesn't support the protocol being used
- The network infrastructure cannot route the packets due to lack of routing information or addressing types (public addressing vs. private addressing)
- The network infrastructure doesn't support the traffic type (multicast or broadcast)

The most common use case for tunnels is to connect remote, geographically separated. sites over an existing network, most notably routing over a public infrastructure (such as the Internet). When used in this manner, tunnels create VPN overlay networks between remote sites. Packets destined to remote private networks are encapsulated within a new IP header that is used to traverse the public internet.

10.2. GRE Tunnel

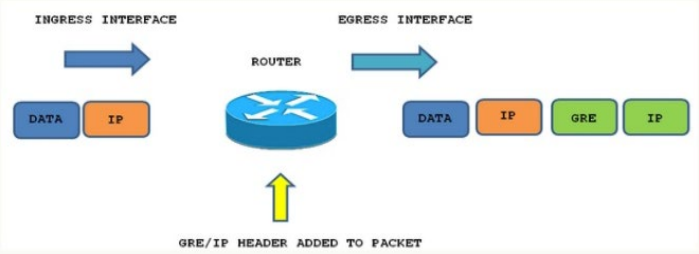
GRE tunnels provide an interface the device can use to forward data. The "data" in this sense is the passenger protocol itself, such as IPv6 or IPv4. These tunnels are comprised of three main components:
1. Delivery Header (Transport Protocol)
2. GRE Header (Carrier Protocol)
3. Payload Packet (Passenger Protocol)

GRE can be used with many different combinations of passenger and transport protocols. However, IPv4 and IPv6 are the most common transport protocols for GRE.

For example:

- GRE can use IPv4 as the transport protocol to tunnel an IPv4 packet across the underlying network infrastructure.
- GRE can use IPv4 as the transport protocol to tunnel an IPv6 packet across the underlying network infrastructure.
- GRE can use IPv6 as the transport protocol to tunnel an IPv4 packet across the underlying network infrastructure.
- GRE can use IPv6 as the transport protocol to tunnel an IPv6 packet across the underlying network infrastructure.

11. CISCO VPN Configuration



12. Why Use GRE Tunnels?

GRE's support for multiple protocols and packet types makes it ideal for solving many of the problems faced when trying to form VPNs across the Internet. The most obvious issue is that private addressing used in the enterprise cannot be routed across the public Internet. GRE solves this by encapsulating the IP header with private addressing using an outer IP header that uses public addressing.

GRE can be used to solve both of these problems:

1. GRE supports multicast traffic allowing hello messages generated by an IGP to be transported through the GRE tunnel across the underlying infrastructure as a unicast packet. IPsec can then be used to encrypt all traffic flowing through the GRE tunnel.

2. GRE configuration creates a logical direct connection between two sites over the underlying infrastructure. This means the control plane of the IGP believes it is directly connected to the neighbor with which it is exchanging hellos and therefore can form the adjacency.

12.1 Internet Protocol security (IPsec)

Internet Protocol security (IPsec) is a security framework contain protocols for cryptographically securing communications over the IP Layer.

It has two main protocols:
-Authentication Header (AH)
-Encapsulation Security Payload (ESP)

In addition to one protocol used for Key Management – Internet Key Exchange (IKE) Protocol.

13. Site to Site VPN

- Site-to-site VPNs are a popular way to provide secure communication between sites
- Used instead of private WAN connections or to improve the security of WAN connections
- There is a lot of configuration needed on both sites when creating VPN Site to Sites such as (ISAKMP Policy, IPsec Policy, Crypto map, ACLs and interfaces

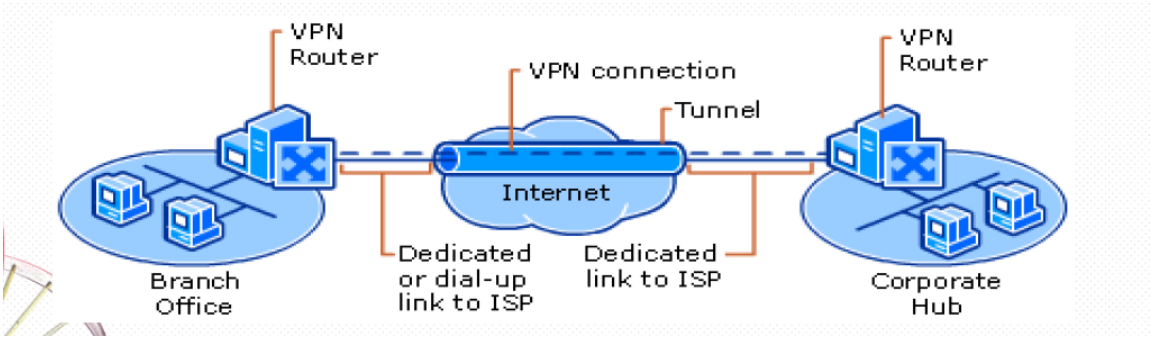


Figure 2.1. Site to the Site VPN router

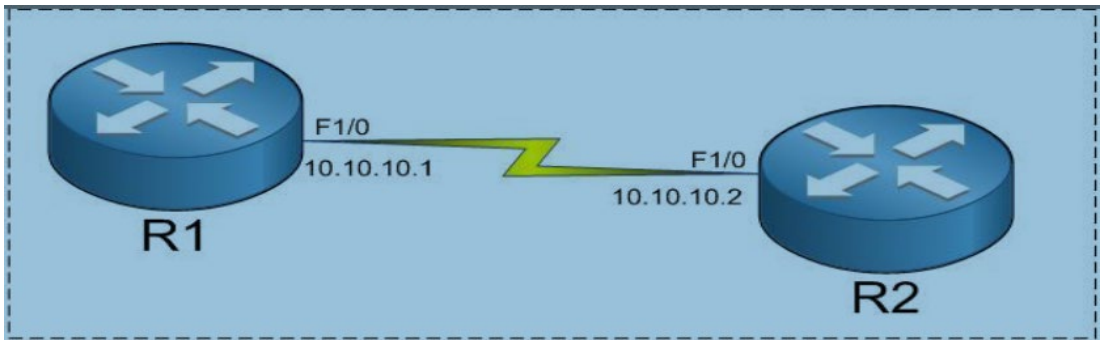


Figure 2.2. Site to Site VPN Configuration

Site to Site VPN

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 123 address 10.10.10.2

crypto ipsec transform-set MENOG esp-3des esp-sha

ip access-list extended 101
permit ip host 10.10.10.1 host 10.10.10.2

crypto map R1 10 ipsec-isakmp
set peer 10.10.10.2
match address 101
set transform-set MENOG

int F1/0
crypto map R1
```

```
crypto isakmp policy 1
authentication pre-share
hash md5
encryption des
group 1

crypto isakmp key 123 address 10.10.10.1

crypto ipsec transform-set MENOG esp-3des esp-sha

ip access-list extended 101
permit ip host 10.10.10.2 host 10.10.10.1

crypto map R1 10 ipsec-isakmp
set peer 10.10.10.1
match address 101
set transform-set MENOG

int F1/0
crypto map R1
```

14. VTI Site to Site VPN

- IPsec VTIs make it much easier to provide protection between site-to-site VPN tunnel. Using a virtual tunnel interface .
- there is no longer a requirement to statically map an IPsec crypto map to a physical interface on the router/Firewall.
- IPsec VTIs has many benefits:
    a. Simplify configuration Flexible interface.
    b. Support for multicast.
    c. Better scalability.

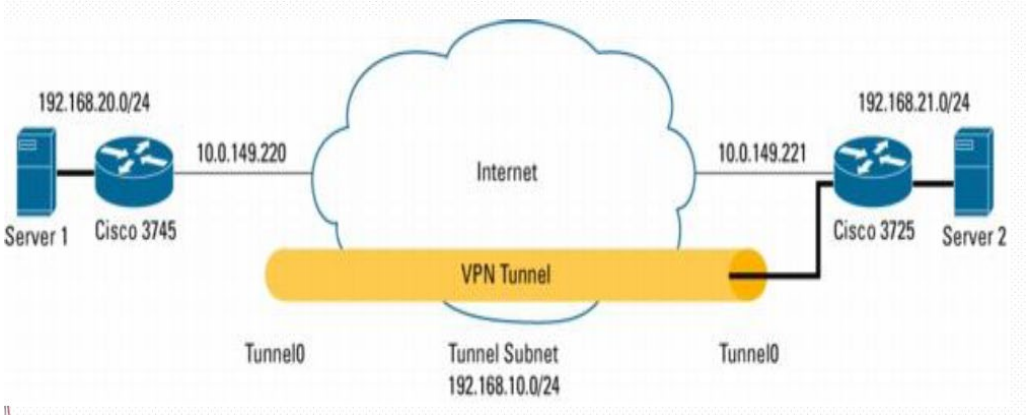


Figure 2.3. VTI Site to Site VPN

14.1. VTI Site to Site VPN Types

Static Point-to-Point IPsec VTI Tunnels

- Static VTI VPN tunnels provide secure connectivity between two sites.
- Deploying static VTI tunnels involves configuring a tunnel interface on both VPN peers.
- Static VTI tunnels are permanently established immediately after being configured.

Dynamic Point-to-Point VTI Tunnels

- It works with Hub-and-Spoke topology
- There is no requirement to statically map IPsec sessions to physical interfaces. Instead, VTIs on the

hub is created dynamically as tunnels to the hub are established.
- When a spoke peer initiates a tunnel, the tunnel and dynamic VTI are created. On the spoke peer, use a static VTI to establish a tunnel with the hub peer.

15. Tunnel Protection Mode

Tunnel protection is used to secure (encrypt) the data transfer inside the GRE tunnel. This is done by applying an IPsec profile to the mGRE tunnel interface. Crypto maps are unnecessary in IOS Release 12.2(13)T or later. IPsec profiles are used to accomplish the same result and share most of the same commands with the crypto map configuration. However, only a subset of the commands is needed in an IPsec profile. Only commands that pertain to an IPsec policy can be used under an IPsec profile. There is no need to specify the IPsec peer address or the ACL to match the packets that are to be encrypted. If a packet is routed through the tunnel, it is encrypted.

To associate either a p2p GRE or an mGRE tunnel with an IPsec profile on the same router, tunnel protection must be configured. Tunnel protection specifies that IPsec encryption is performed after the GRE headers are added to the tunnel packet. In p2p GRE tunnels, the tunnel destination IP address is used as the IPsec peer address. In mGRE tunnels, multiple IPsec peers are possible; the corresponding NHRP-mapped NBMA destination addresses are used as the IPsec peer address.

If more than one mGRE tunnel interface or an mGRE and p2pGRE tunnel interface is configured on a router, and they use the same tunnel source address, the **shared** keyword must be configured on the tunnel protection command. Each mGRE tunnel interface still requires a unique tunnel key, NHRP network-ID, and IP subnet address. This is common on a branch router when a dual DMVPN cloud topology is deployed. If a tunnel key is not configured, all mGRE tunnel interfaces must have unique tunnel source addresses. In this same case, p2p GRE tunnel interfaces can have the same tunnel source address as long as the interfaces have different tunnel destination addresses.

15.2 Configuration and Implementation

In this section, we look at common basic configurations recommended for all of the designs presented in the research. These configurations should be considered best practices for any DMVPN network design.

15.3. ISAKMP Policy Configuration

There must be at least one matching ISAKMP policy between two potential crypto peers for IKE Phase 1 to work. The following configuration shows a policy using Public Key Infrastructure (PKI) Rivest, Shamir, and Adelman (RSA) certificates (also known as digital certificates) for the ISAKMP authentication. The policy does not show up in the ISAKMP policy because it is the default, but we have shown it for completeness. It is also possible to use preshared keys (PSKs), but this is not very scalable, and is not recommended for large scale DMVPN designs.

To use PKI for ISAKMP, you must first create the crypto keys, which should be generated with a specified modulus size (the default is 512-bits). It is best to use 2048-bit or larger keys for most High-performance routers, but this may not be appropriate for lower performance platforms. After the keys are created, you must authenticate and enroll with the Certificate Authority (CA).

It is recommended to use a *strong* encryption algorithm, such as Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES). In the sample configuration, the encryption algorithm used for the ISAKMP SA is Triple-DES (3DES), and the Diffe-Helman group is 2. These are recommended, although other values may be used.

```
ip domain-name cisco.com
!
crypto pki trustpoint DMVPN-CA
 enrollment url http://10.1.1.254:80
 serial-number none
 ip-address 10.21.1.2
 password
 subject-name CN=DMVPN HUB, ou=CISCO
 revocation-check none
 rsakeypair dmvpnkey
 auto-enroll
!
crypto pki certificate chain DMVPN-CA
 certificate 3607
 <certs omitted>
 certificate ca 01
!
crypto isakmp policy 2
 encr 3des
 authentication rsa-sig
```

```
 group 2
!
```

15.4. mGRE Tunnel Interface Configuration

mGRE configuration enables a tunnel to have multiple tunnel destinations. The mGRE configuration on one side of a tunnel does not have any relation to the tunnel properties that might exist on the other side of the tunnel. This means that an mGRE tunnel on the hub can connect to a p2p tunnel on the branch. The tunnel destination distinguishes an mGRE interface and a p2p GRE interface. An mGRE interface has no configured destination. Instead, the GRE tunnel is configured with the tunnel mode gre multipoint command. This command is used instead of the tunnel destination x.x.x.x used with p2p GRE tunnels. Enabling multiple destinations for an mGRE tunnel requires NHRP to resolve the tunnel endpoints. mGRE is required on the hub device and recommended on the spoke router. It is required on the spoke router if spoke-to-spoke tunnels are desired.

```
interface Tunnel1
 bandwidth 1536
 ip address 10.81.1.1 255.255.0.0
 ip mtu 1440
 tunnel source 10.70.101.2
 tunnel mode gre multipoint
!
```

IP multicast/broadcast packets are supported only on tunnels with static mappings (the spoke-hub tunnels). Hubs are configured to enable NHRP to automatically add routers to multicast NHRP mappings. This is necessary to run routing protocols over the DMVPN mGRE tunnel. NHRP can only add a peer to the multicast mapping list when it receives an NHRP registration packet (only on NHRP NHSs).

NHRP hold time is used to determine how long receiving routers should consider the cached entry information to be valid. The configured value on the sender of the information is passed to the receiver in the NHRP registration request or resolution reply packet. When the remote node adds this information to its mapping database, the remote node starts a countdown timer. When this timer expires, the node removes cached entry information. If traffic is still flowing when the timer is about to expire, the node must request the mapping again to refresh it.

16. Recommendation

First off I'd recommend that enterprise in Uganda leverage the hierarchical campus approach because it can help in saving cost, its ease to understand, it supports Modular network growth and it improve fault isolation in the overall network. Secondly since in this project we are not recommending the use of layer 2 features such as spanning tree in our network the recommendations on this project will basically be on whether to use EIGRP or OSPF. So if we look at EIGRP with default settings and OSPF with default settings and there are multiple loop free paths to a destination then EIGRP will converge much faster because it keeps what are called feasible successors in its topology database. These are basically loop free alternatives to the best path. EIGRP also has summarization at any point in the network. It also has stub feature which is useful when you don't want to use a router for transit. Commonly deployed in DMVPNS. EIGRP is also less confusing than OSPF because it does not have different network types and EIGRP is easier to deploy in hub and spoke scenarios. EIGRP uses a flat network without areas, this can both be an advantage and disadvantage. OSPF is obviously an open standard so it's the logical choice if you have multiple vendors. It can perform well but it requires that you tweak SPF timers because by default in IOS there is a 5 second wait before running the SPF algorithm. OSPF uses areas which means you can segment the network more logically. OSPF can only summarize between areas. OSPF is link state so it has a better view of the entire network than EIGRP before it runs the SPF algorithm. Network administrators will usually be more comfortable with OSPF because it's more commonly deployed. Both protocols have advantages and disadvantages. So the question on whether to use OSPF or EIGRP depends on the network admin. But my personal choice will be EIGRP.

17. Conclusion

As a talent, innovation, and decision making become dispersed across highly distributed enterprises, it is critical that network experiences of branch-office users improve to match those of headquarters users. Making this happen requires transforming isolated and disparate branch-office network designs into replicable branch-office architectures to which new services can easily be added. To accomplish this scenario in a way that also curbs overall branch-office total cost of ownership (TCO), IT departments need to build a branch-office strategy that standardizes each type of site, rather than attempting to add services here and there as afterthoughts. The strategy should account for network application types in use now and in the future, where they are hosted, traffic flow patterns, and security.Standardized, integrated branch-office architecture elevates branch-office users to the productivity status of those employees at headquarters using the corporate LAN. Integration at a physical level reduces CapEx by requiring less equipment and real estate, and OpEx by providing a common management interface to manage all integrated functions. Integration at the services level allows all services to be provisioned, managed, and secured centrally by IT staff. Service-level integration also supports the application intelligence needed for one service not to interfere with another, as happens frequently with nonintegrated solutions. Rather, the correlation among a variety of security, QoS, and WAN-optimization services makes the power of the branch office greater than the sum of its parts.

References

[1] Bhaskaran, S., Desai, S., Jou, L., & Matthews, A. R. (2007). U.S. Patent No. 7, Washington, DC: U.S. Patent and Trademark Office.

[2] Chase, C. J., Holmgren, S. L., Medamana, J. B., & Saksena, V. R. (2001). U.S. Patent No. 6,188,671. Washington, DC: U.S. Patent and Trademark Office.

[3] Dynamic Multipoint VPN (DMVPN) Design Guide, Corporate Headquarters Cisco Systems, Inc. 2006,

[4] Bahnasse, A., & El Kamoun, N. (2014). Policy-based Management of a Secure Dynamic and Multipoint Virtual Private Network. Global Journal of Computer Science and Technology,

[5] Hanks, Stan, David Meyer, Dino Farinacci, and Paul Traina. RFC 2784-Generic routing encapsulation (GRE). (2000).

[6] P. Christian. RFC 3147 - Generic Routing Encapsulation over CLNS Networks. Nortel Networks, July 2001

[7] Luciani, J., D. Katz, D. Piscitello, B. Cole, and N. Doraswamy. Next hop resolution protocol (NHRP).RFC2332 (2001).

[8] Huttunen, Ari, Brian Swander, Victor Volpe, Larry DiBurro, and Markus Stenberg. UDP encapsulation of IPsec ESP packets. RFC 3948, January, 2005.P.

[9] Kent, Stephen. IP authentication header. RFC 4302, December, 2005

[10] Adoba, B., & Dixon, W. (2004). RFC 3715–IPSec-network address translation (NAT) compatibility requirements.

[11] Jankuniene, R., & Jankunaite, I. (2009, June). Route creation influence on DMVPN QoS. In Information Technology Interfaces, 2009. ITI'09. Proceedings of the ITI 2009 31st International Conference IEEE.

[12] Asati, R., Khalid, M., Retana, A. E., Van Savage, D., & Sethi, P. P. (2013). U.S. Patent No. 8,346,961. Washington, DC: U.S. Patent and Trademark Office.

[13] Chen, H. (2011, May). Design and implementation of secure enterprise network based on DMVPN. In Business Management and Electronic Information (BMEI), 2011 International Conference on IET.

[14] Savage, D., Slice, D., Ng, J., Moore, S., & White, R. (2013). Enhanced Interior Gateway Routing Protocol. Internet Engineering Task Force.

[15] Yang, Q. F., Shi, H. H., & Zhu, S. (2013). Analysis the Advantages and Packet Format of EIGRP. Applied Mechanics and Materials,.

[16] Sullenberger, M. L., & Vilhuber, J. (2008). U.S. Patent No. 7,447,901. Washington, DC: U.S. PatentC: U.S. Patent and Trademark Office.

[17] Nguyen, L. H., Van Savage, D., Slice Jr, D. E., Van Tran, T., & Yang, Y. (2011). U.S. Patent No. 7,898,981. Washington, DC: U.S. Patent and Trademark Office
[18] Cisco Systems, Dynamic Multipoint VPN (DMVPN) Design Guide (Version 1.1), 2008
[19] Berkowitz, Howard (1999), OSPF Goodies for ISPs, North American Network Operators Group NANOG 17, Montreal
[20] Aggarwal, A., & Khera, S. (2012). Combat Resources Shortages by making Stub Areas and Route Summarization in OSPF. International Journal of Scientific and Research Publications, 2(8).
[21] Ayoub BAHNASSE and Najib EL KAMOUN, Policy-Based Automation of Dynamique and Multipoint Virtual Private Network Simulation on OPNET Modeler International Journal of Advanced Computer Science and Applications(IJACSA), 5(12), 2014.
[22] Mishra, Vinita, and Smita Jangle. Analysis and comparison of different network simulators.International Journal of Application or Innovation in Engineering & Management (2014)
[23] Schilling, Bjorn. Qualitative comparison of network simulation tools.Institute of Parallel and Distributed Systems (IPVS), University of Stuttgart (2005).
[24] Lucio, Gilberto Flores, Marcos Paredes-Farrera, Emmanuel Jammeh, Martin Fleury, and Martin J. Reed. Opnet modeler and ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed.WSEAS Transactions on Computers 2, no. 3 (2003):
[25] BAHNASSE, A., & ELKAMOUN, N. (2015). Study and evaluation of the high availability of a Dynamic Multipoint Virtual Private Network. Revue MéDiterranéEnne Des TéLéCommunications,).
[26] Park, J. H., Oliveira, R., Amante, S., McPherson, D., & Zhang, L. (2012). BGP route reflection revisited. Communications Magazine, IEEE,
[27] SCALABLE DMVPN DESIGN AND IMPLEMENTATION GUIDE, Network Systems Integration & Test Engineering (NSITE),Document Version Number: 1.1, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA
[28] IKEv2 IPsec Virtual Private Networks Understanding and Deploying IKEv2, IPsec VPNs and FlexVPN in Cisco IOS (Graham Bartlett, CCIE No. 26709 Amjad Inamdar, CISSP No. 460898) Copyright @ 2017 Cisco Systems, Inc. Cisco Press logo is a trademark of Cisco Systems, Inc.Published by:Cisco Press,800 East 96th Street,Indianapolis, IN 46240 USA
[29] Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network (Ayoub Bahnasse STIC Laboratory Department of physics, Faculty of Sciences Chouaïb Doukali University El Jadida Morocco) and (Najib El Kamoun STIC Laboratory Department of physics, Faculty of Sciences Chouaïb Doukali University El Jadida Morocco