REPUBLIC OF TURKEY

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

EVALUATION AND OPTIMIZATION OF DMVPN NETWORK PERFORMANCE USING DYNAMIC ROUTING AND ADVANCED ENCRYPTION ALGORITHMS

Hasan Mohamed Ali MARAH

Master's Thesis

Supervisor

Asst. Prof. Dr. Muhammad ILYAS

Istanbul, 2022

EVALUATION AND OPTIMIZATION OF DMVPN NETWORK PERFORMANCE USING DYNAMIC ROUTING AND ADVANCED ENCRYPTION ALGORITHMS

Hasan Mohamed Ali MARAH

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled EVALUATION AND OPTIMIZATION OF DMVPN NETWORK PERFORMANCE USING DYNAMIC ROUTING AND ADVANCED ENCRYPTION ALGORITHMS prepared by HASAN MOHAMED ALI MARAH and submitted on 20/05/2022 has been **accepted unanimously** for the degree of Master of Science in Information Technologies.

Asst. Prof. Dr. Muhammad ILYAS

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Muhammad ILYAS	Faculty of Engineering and Architecture, Altinbaş University	_____
Asst. Prof. Dr. Hasan ABDULKADER	Faculty of Engineering and Architecture, Altinbaş University	_____
Asst. Prof. Dr. Jawad RASHEED	Faculty of Computer Engineering, Istanbul Aydin University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work ..

Hasan Mohamed Ali MARAH

Signature

DEDICATION

First and foremost to almighty Allah for his guidance and help that let me reach my target in this crucial stage of my age, then to my parents who have been waiting to this moment to see me with this great achievement, to my wife and children who suffered and struggled with me to reach this great moment, to my great supervisor who was my inspiration by pushing me forward each time to make new improvements and achievements.

ABSTRACT

EVALUATION AND OPTIMIZATION OF DMVPN NETWORK PERFORMANCE USING DYNAMIC ROUTING AND ADVANCED ENCRYPTION ALGORITHMS

Marah, Hasan Mohamed Ali

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Muhammad ILYAS

Date: 05/2022

Pages: 70

The DMVPN technology is an enhanced Cisco technique that allows for flexible implementation and interconnection of remote sites. Three key components must be configured to run a DMVPN network: mGRE tunneling, NHRP protocol, and dynamic routing protocol. The packets in the GRE tunneling must be protected; for this reason, IPsec/mGRE is utilized to protect data. IPsec offers several properties that can provide varying security levels depending on the network design and purpose. Encryption algorithms are critical security attributes that provide higher protection to the DMVPN network. However, they impact network performance and quality, especially in large scalable networks, necessitating the implementation of an appropriate routing protocol to avoid poor network quality and performance. Many studies have been conducted to measure network performance. This research work focuses on evaluating and optimizing the DMVPN network performance by testing a combination of routing protocols and encryption algorithms, symmetric encryption algorithms such DES, AES, and 3DES were configured and tested with other dynamic routing protocols such as OSPF, RIP, and EIGRP. Many network key indicators such as Speed, Latency time, Jitter, Throughput rate, and the percentage of datagram lost were captured and analyzed by using the Iperf measurement tool. Many scenarios were conducted using different

input criteria, in each experiment, labs were configured with a combination of one routing protocol and one encryption algorithm, streamed with two different UDP data of 500KB and 256KB respectively, restricted with a fixed bandwidth limit of 500KB/S. Restricting bandwidth amount to 500KB/S with data input of 500KB reveals that the EIGRP protocol with the AES algorithm gained the greatest performance, followed by RIP/ 3DES, unlike all other protocols. However, using RIP/AES reveals noticeable good performance when data streamed by (256KB)**.**

Keywords: DMVPN, EIGRP, IPSEC, MGRE, NHRP.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATION

AI	:	Artificial Intelligence
FSK	:	Frequency Shift Keying
IoT	:	Internet of Things
PAN	:	Personal Area Network
OFDM	:	Orthogonal Frequency Division Multiplexing
TDMA	:	Time Division Multiple Access

1. NTRODUCTION

VPNs provide a private network within an insecure network, making them one of the most widely utilized methods of connecting remote locations. Despite the greater level of security provided by standard VPNs, there are significant limitations and practical implications for a scalable network. Static configurations require a distinct public IP address, tunnel, and physical interface for each site, and adding additional remote sites necessitates resetting all network equipment, resulting in network connectivity difficulties. The "DMVPN" network enables rapid deployment, minimizes implementation time, and optimizes bandwidth use while maintaining a high level of confidentiality, integrity, and availability.

Dynamic routing protocols run and route the traffic between different DMVPN sites, based on that, choosing the incorrect protocol can have unintended repercussions. Due to the vulnerability of DMVPN traffic to theft and fraud, data is protected using IPsec/mGRE to provide authentication, encryption, and integrity. Peer-to-peer data encryption utilizes a variety of encryption techniques. Encryption is classified into two types: symmetric which is include 3DES, AES, and DES, whereas RSA is asymmetric. On the other hand, adopting security algorithms degrades the speed of the DMVPN network, owing to the increased traffic created by the addition of new packet headers to the IPsec main header. Additionally, the characteristics of each encryption scheme, such as key and block sizes, affect the network's key performance indicators.

In maintaining and optimizing DMVPN networks, dynamic routing protocols and encryption mechanisms are critical. Dynamic routing technologies whether distance-vector such as RIP protocols or link-state such as OSPF or hybrid such as EIGRP are deployed and evaluated with most common encryption techniques such as DES, 3DES, or AES to analyze network characteristics such as speed, jitter, latency, and bandwidth.

1.1 VPN NETWORK

1.1.1 Introduction

A Virtual Private Network, or "VPN," is a private connection environment that secures communication between network devices and remote users over insecure networks such as public networks and teleworkers[1]. The traffic flowing inside the VPN is encrypted by various security

mechanisms, which provide different levels of data security in terms of confidentiality, integrity, and authentication[2]. The VPN private connection is based on the tunneling mechanism, a virtual logical connection established between remote peers that encapsulates the packets in a specific VPN protocol format with other bundles of security protocols to maintain data transmitted between VPN clients and servers privately secured. VPN is a tunneling solution that can be involved in many organizations and multiple applications across any public connection [3],[4],.

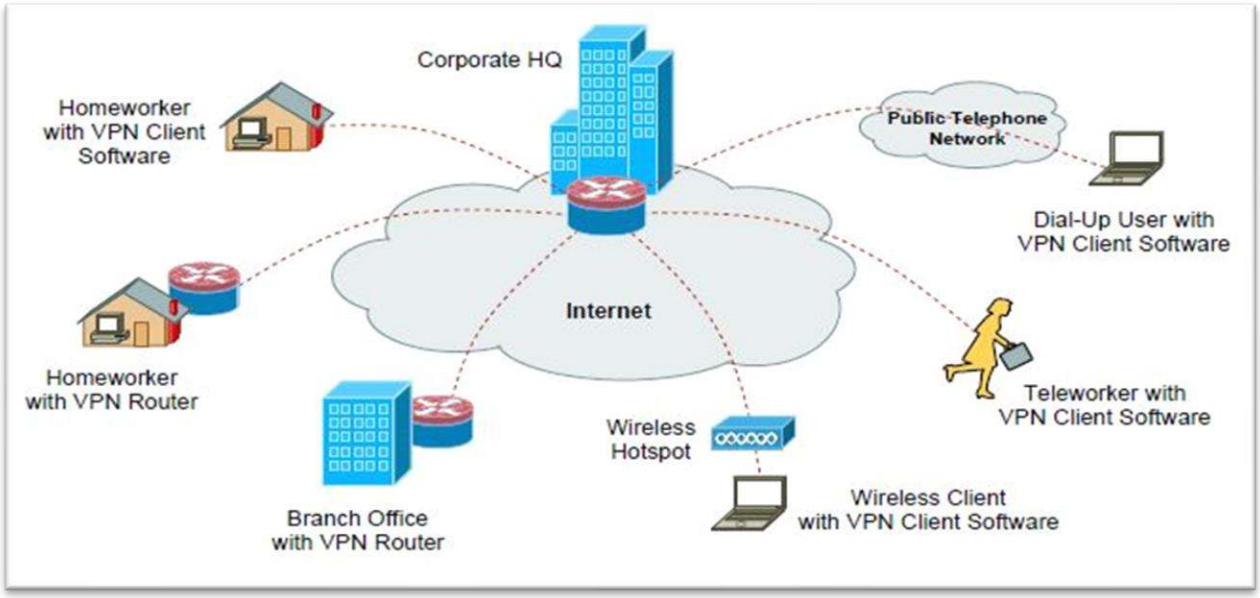

Figure 1.1: Virtual Private Network [5].

1.1.2 The Need for VPN

The secure private network was associated with and built with Frame Relay Networks (FRN). Many organizations used to layer two technologies and leased line connections such as Frame relay to keep and maintain their traffic safe and secured [1]. However, with the massive development of IP network technology, the demand for Layer 3 VPN technology has increased. All services start to migrate from layer 2 to layer three based on TCP/IP OSI Model. The main benefit of Layer 3 VPN network service is the cost reduction compared with layer two dedicated services, connections can be established to many remote distance sites and peers with flexible implementation and easy connectivity, moreover, the efficient utilization of network bandwidth, which means that network user can be obtained different level of network quality which enhances network performance [4]. In addition, network scalability permits the addition of more remote

devices and connections in a simple way. Based on TCP/IP OSI Model, VPN services are provided at different layers of the OSI model, Layer 3 such as IPsec, MPLS, or Layer 4 VPN protocol such as (TLS, SSL), which provide a secure connection in the transport layer [6],[7].

1.2 VPN CLASSIFICATION

VPN deployed based on topology or tunneling techniques.

i. Topology Based.

ii. Peer to Peer.

This type of topology is used to make a tunnel connection between two end devices or between two computers across a public network. Each tunnel interface has an assigned IP address which initiates two end devices to be connected privately after getting associated with physical media. This scenario is not widely used because of its limitation that no more than two computers can be connected to the tunnel connection [8], [9]. See the (Figure 1.2).

Figure 1.2: Peer to Peer [8].

1.2.1 Client To Server

The connection of the VPN client and server or a Client IPsec connection is a secured tunnel connection that establishes a secure VPN connection between a client and a remote site via a global network such as dial-up or DSL. A VPN client can connect all computer clients via a private IPsec tunnel, and keeps all data encrypted while connected with the VPN server, while the traffic from the VPN server to other computers is exposed to the public. This type of VPN connection is widely used by many remote users who need to access to their secured network with easy way and lower cost[8],[10],[9]. See the Figure (Figure 1.3).

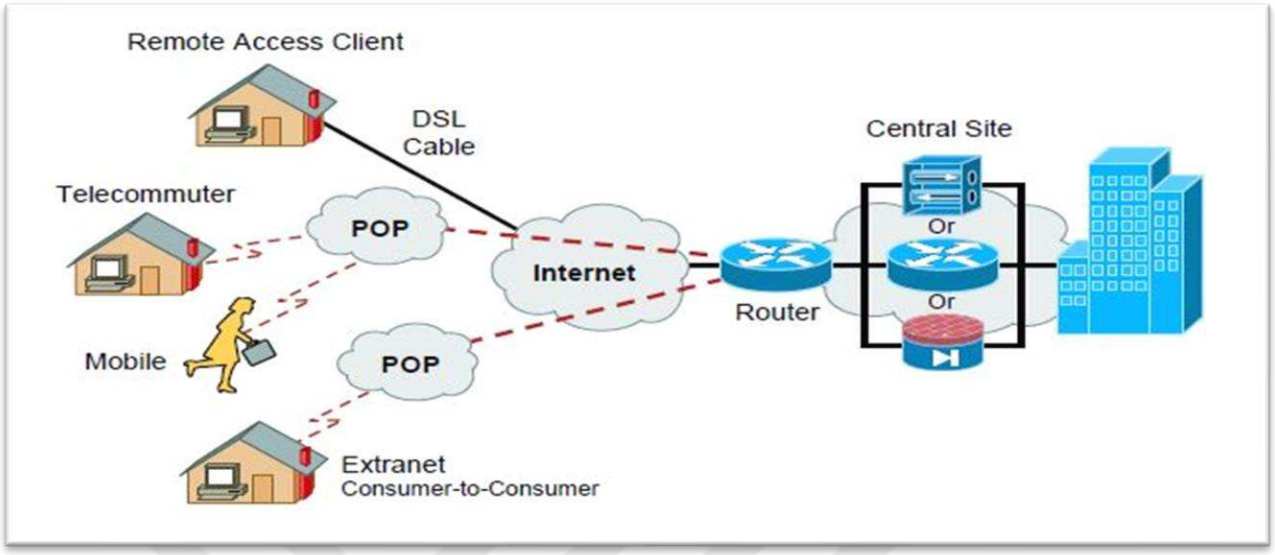

Figure 1.3: Client to Server [5].

1.2.2 Site To Site

Is an internet-based infrastructure that enables various offices and headquarters to establish a secure connection. In other words, site to site is a connection between LAN to LAN VPNs controlled and protected by IPsec tunneling protocol [8]. See the figure (Figure 1.4).

Site-to-site VPNs can be categorized into several categories.:

i. Intranet-based.

ii. Extranet-based.

When a company has many geographical locations and needs to merge all remote sites as one private network, in this case, an intranet net VPN is created.

When a company has many business partners and needs to connect to its network, an extranet network is created to communicate with a remote partner without accessing the intranet network.

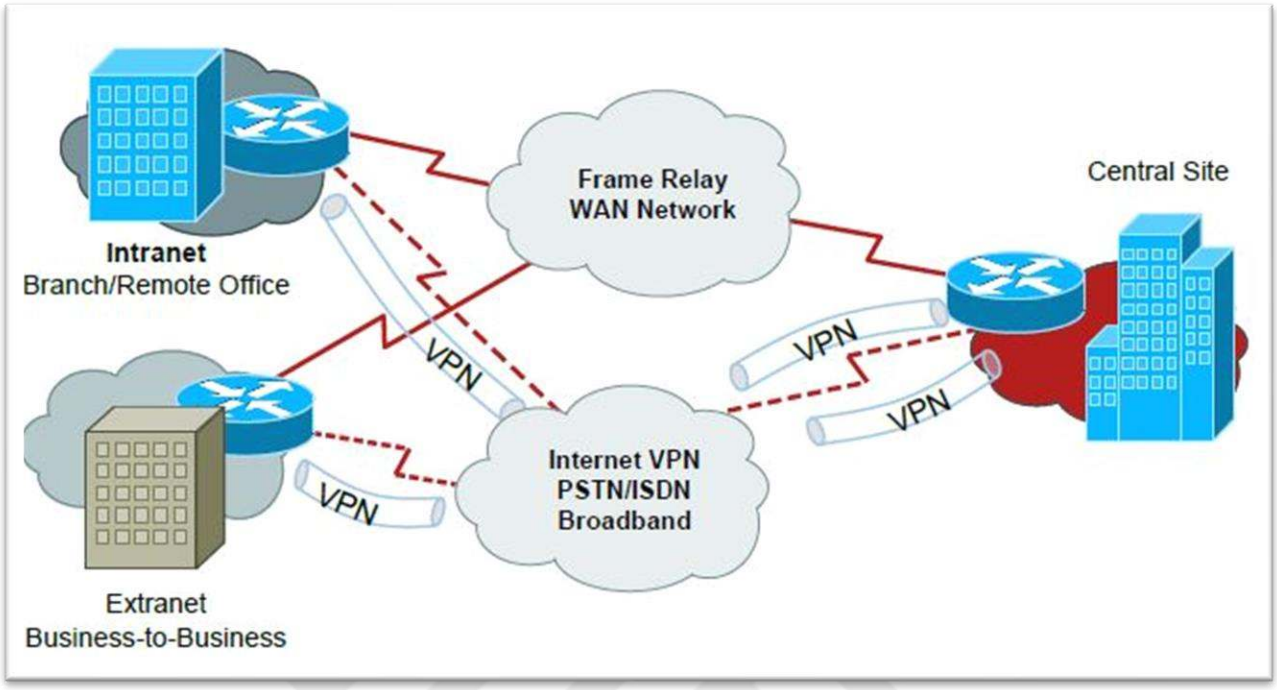

Figure 1.4: Site to Site [5].

1.2.3 Layer Protocol Based

Based on the type of traffic passing through the VPN tunnel, the selection of the VPN protocol is chosen. Based on the TCP/IP OSI model, three VPN protocols depend on the packet received from a specific OSI layer [11].

A. Layer 2 VPN

It encapsulates the whole link layer packet frame. Layer 2 VPNs employ industry-standard protocols such as L2TP, PPTP, and MPLS.

B. Layer 3 VPN

The Layer 3 VPN enables the encapsulation of the entire packet frame of the IP layer. Layer 3 VPN has standard protocols such as IPsec, MPLS, etc.

C. Layer 4 VPN

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are Layer 4 VPN protocols that encrypt the layer four traffic at the OSI model; the primary function of TLS is to secure web traffic

"HTTP" to form HTTPS traffic. Layer 4 VPN technologies can encrypt just layer four traffic; they cannot encrypt lower-layer traffic.

1.3 VPN COMPONENT

Three main components form an active VPN connection: authentication, tunneling, and encryption; whether Site-to-Site or Remote access VPN connection [11]. See the figure (Figure 1.5).

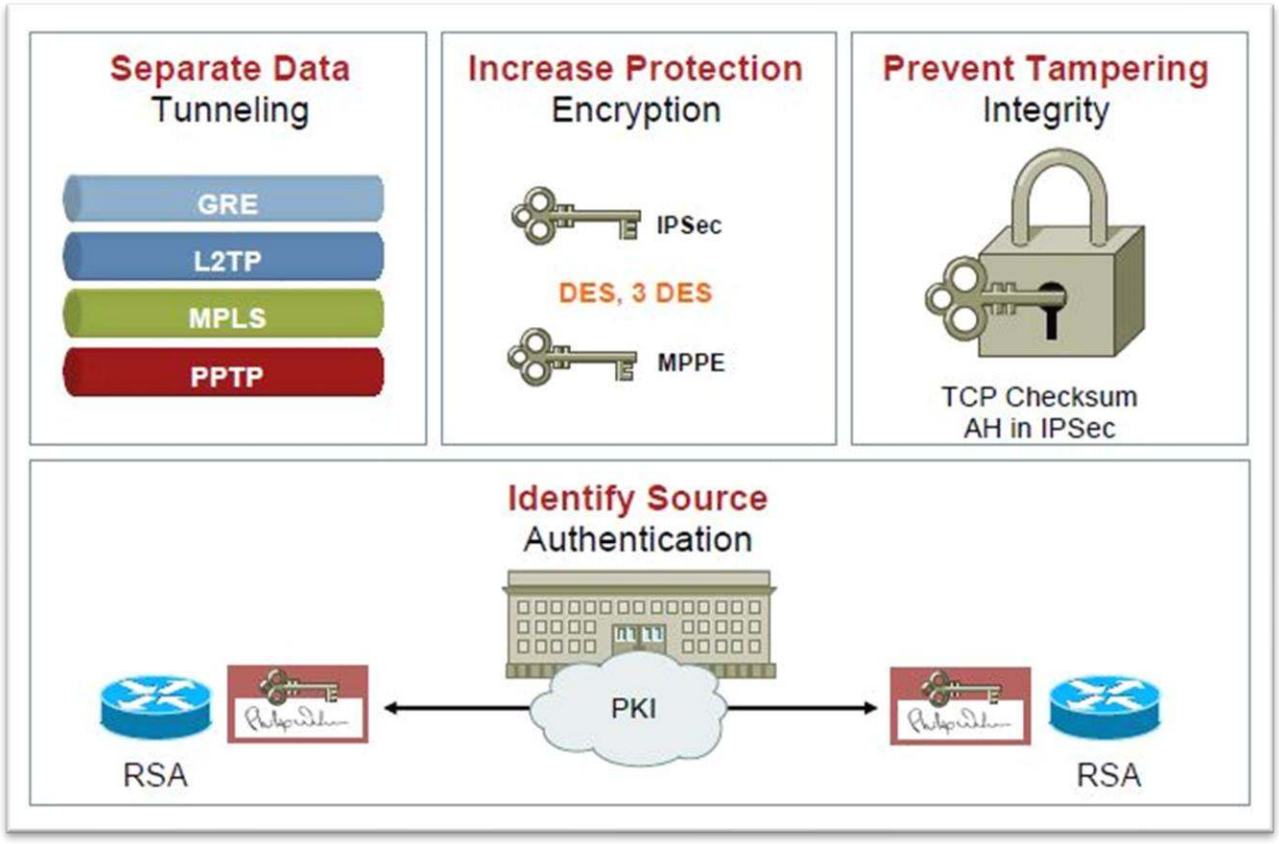

Figure 1.5: VPN Components [5].

1.3.1 Authentication

Authentication is a method used to guarantee user access or entity through a set of credentials and provides access control by verifying an electronic device or person's identity. Many algorithms are utilized to determine and authenticate peer's or remote sites identities. Digital signature and pre-shared key are one of the most common methods used for the authentication process. To get two

sites to communicate with each other, both sides must configure the same authentication key and attributes [12].

Pre-shared keys are not secure compared with a digital signature, the pre-shared key is a password consisting of complex and random numbers and symbols used to construct and establish a VPN tunnel between VPN nodes. Pre-shared keys are vulnerable to many types of cyberattacks. Moreover, this kind of authentication is not widely needed in scalable networks [13],[11],[14].

Digital certificates are a scalable solution, it is an authentication process used to identify the originality of the sending and receiving the message. DC is a type of public-key algorithm such as RSA. The sender is using a private key to generate a digital signature to encrypt the data sent, while the receiver must use the public key to decrypt the message. The digital signature is widely used in many organizations, it's a highly secure method used in the authentication process. [13].

1.3.2 Tunneling

Tunneling is the underlying technology behind virtual private network (VPN) technologies. VPN tunneling creates a logical connection to carry the payload data by utilizing a specific VPN protocol, all packets are encapsulated in a header and sent from source to destination, after receiving the packets by destination, all packets are decapsulated [1],[4],[15].

1.3.2.1 GRE

Cisco developed a tunneling technique called GRE, used to encapsulate packets to be sent while crossing a public network. The GRE premise is to construct a virtual tunnel between two routers and then send packets over that tunnel. In reality, GREs accept a wide range of protocols and packet types, making them ideal for resolving many of the issues that arise when attempting to construct VPNs over the internet [16], [17],[11].

1.3.2.2 L2TP

L2TP is considered a free and open-source tunneling protocol, it delivers UDP packets by encapsulating PPP frames. L2TP tunnel has two endpoint access called concentrator and network server. LAC encapsulates the PPP packets received from source nodes, while the LNS server decapsulates the packets to be received by destination users. L2TP involves IPsec protocols to ensure packet security as L2TP is not secured [8], [18].

1.3.2.3 MPLS

High-performance networks employ Multiprotocol Label Switching (MPLS), a system for transmitting data from one network node to another through a set of labels. The Labels are attached to the data packet and the packets will be sent based on the assigned labels. [19].

MPLS is a scalable protocol used to extend the capability of a wide range of network protocols. MPLS VPN is used to route traffic in OSI Layer 2. It is used to enhance access to the public internet and allow remotes sites and users to be connected easily. MPLS protocol is used to enhance network speed, for this reason, a provider edge router must be installed on the ISP side[20].

Each packet of data moving through the ISP network is encrypted using a Layer 2 MPLS VPN, protecting it from being accessed by other customers. Security is a primary concern when it comes to Layer 2 MPLS VPNs. On the ISP Network, sharing a Layer 2 medium, make it impossible to manage the packets delivered to that device, allowing packets from other customers to be easily intercepted and exploited against them. Due to the high cost of unique network devices, the likelihood of them being used on an ISP network is slim. To overcome this challenge, the ethernet connection can be established between physical ports. This means that before Layer 2 packets are delivered to their respective destination networks, they are encapsulated in 802.1Q Ethernet frames[20],[21].[8],[22],[23].

1.3.2.4 PPTP

PPTP is a Microsoft Tunneling protocol considered as an extension of PPP protocol. When establishing a VPN connection, PPTP uses two different packet kinds. The VPN payload data is wrapped by generic routing encapsulation (GRE). Using PPTP requires using encryption and authentication to ensure data confidentiality and integrity, as PPTP is not a secured tunnel[18].

The symmetric RC4 stream cipher encrypts the GRE payload to protect data privacy. The design of PPTP, it appears, is relatively straightforward, with only a VPN connection between ISP and remote clients, no additional VPN software is required. [24].

1.3.2.5 SSL/TLS

Netscape invented a secure Socket Layer (SSL). It is positioned above the TCP layer in the TCP/IP stacking model. So it might be used to enhance security protocols and keeps TCP applications

safer and more secured. SSL protocol is no longer used. Transport Layer Security (TLS) is considered a preferred protocol that provides a high level of security for remote users and securing access to external corporations and organizations. It protects sensitive data such as bank information or credit card passwords from being theft or hacking. TLS depends on two main steps to establish a secure connection, first, TLS record and handshake protocol, TLS provides a secured connection, while handshaking protocol initiates the server and the client to exchange security keys. [24],[25],[26],[27].

1.3.3 Encryption

Data encryption is a security approach to sending and receiving data between two users in a network without exposing the message. There are many security protocols used to secure data traffic, the most common protocols are MPPE and IPsec, they are used to encrypt data IP packets and create secured tunnels [1],[11],[18]. VPN is a tunneling protocol, that is not secured unless encryption techniques are used. Establishing a connection between the server and a client is not enough, IPsec must be implemented to secure the connection and provide end-to-end session protection.[28],[29]

1.3.3.1 IPsec

IPsec is a combination of security protocols and encryption procedures used to build secure connections between remote sites over a public network. VPN network is one of the most services that utilize IPsec protocol due to its high confidentiality. IP traffic naturally is insecure, packets transmitted between IP sources and destinations are exposed to attack and alteration, for this reason, IPsec IP packets need to be encrypted and authenticated. IPsec uses three main protocols, ESP, AH, and IKE, each protocol provides specific techniques and different levels of encapsulation depending on the tunneling method used by each protocol. [8],[30].

1.3.3.2 MPPE

Microsoft Point to Point Encryption (MPPE) encrypts PPP packets and transmits them to the destination in an encrypted state. MPPE ensures data confidentiality by utilizing the RSA RC4 algorithm. The length of the session key that will be used to initialize the encryption tables can be agreed upon. MPPE now supports session keys of 40, 56, and 128 bits in length. MPPE session keys are changed regularly; the negotiated options determine the exact frequency. It may, however,

occur once or twice per packet. The MPPE negotiation is contained in Option 18 of the Compression Control Protocol (CCP) [18],.

1.4 VPN SECURITY

1.4.1 Data Security Model

The security model is a multidimensional paradigm that focuses on implementing procedures that ensure data confidentiality, a high degree of integrity, and authority of essential information and relevant information systems. It is a strategic approach that focuses on policy deployment rather than infrastructure development[31]. See the figure (Figure 1.6).

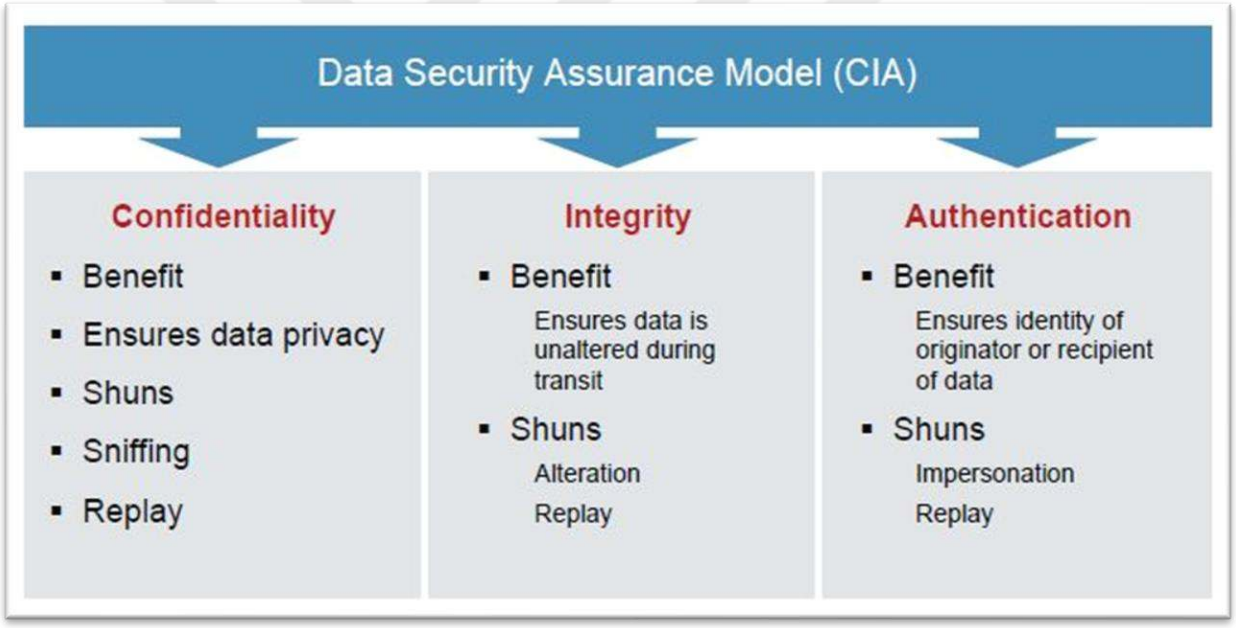

Figure 1.6: Data security model [5].

A. Confidentiality.

Allow authorized individuals to access sensitive data and prevent unauthorized users and people who have no legal writes from accessing private information. Encryption techniques, Access lists two-factor authentication are providing different aspects of security. Additionally, information is frequently classified according to its threat to those who obtain it. After that, the required security measures can be implemented.[31],[32].

B. Integrity

Guarantees that information is presented genuinely and adequately for its intended purpose. Only authorized individuals can alter the information, and while the information is not in use, it retains its original condition. Many security techniques are used to increase the consistency data level, such as hashing and data encryption. Non-human-caused events such as an electromagnetic or server crash might cause data alterations and data corruption, it is critical to have a backup strategy in place and redundant systems in place to protect against data loss [31],[32].

C. Authentication

It is a security service that aims to prove the legitimacy of message transmission by verifying the identification of the individual authorized to receive a specific category of information, such as a credit card number.

Various single-factor and multi-factor authentication methods ensure the multiple factors' availability. A single-factor authentication technique verifies the identification of users by using a single parameter, whereas a two-factor authentication approach verifies the identity of users by using several factors[31], [32],[33].

1.5 IPSEC VPN

1.5.1 Introduction

An IPsec network security protocol suite was created by the (Internet Engineering Task Force) in November 1998. It is an official standard for network security, and it was created with interoperability as a primary goal. It is compatible with both IPv4 and IPv6 networks[34],[35].

Information security protocol (IPsec) protects data integrity, and prevents unauthorized tries from viewing or altering the data, moreover, it provides encryption techniques that keep data fully encrypted by applying various methods of a mathematical algorithm that uses public and private keys for exchanging data. IKE, AH, and ESP are the main component of the IPsec protocol suite. [35],[36],[37]. See the figure (Figure 1.7).

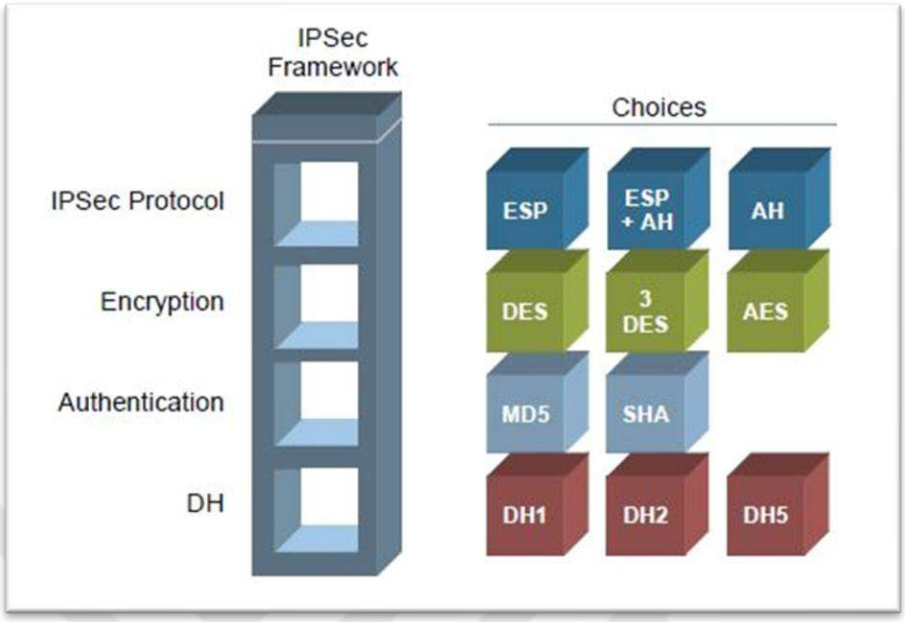

Figure 1.7: IPsec framework [5].

1.5.2 IPsec Modes

IPsec provides two alternative techniques for exchanging protected data over various types of virtual private networks (VPNs):

1.5.2.1 Tunnel mode

In this model, data security can be established between many remote sites, the entire IP packet encapsulated with the data payload, a new IP header is assigned to the IP packet, due to this encapsulation the entire IP packet is secured which give an advantage to IPsec gateway to establish a tunnel connection securely. Those gateways are represented by the outer IP header shown in the figure (Figure 1.8). This mode allows for the establishment of intranet and extranet virtual private networks [38],[37].

1.5.2.2 Transport mode

This option is solely relevant for the protection of hosts against one another. In this case, IP data payloads are protected and the IP data itself. The IP addresses of the outer header is specifying IPsec IP.[38],[37]. See the figure (Figure 1.8).

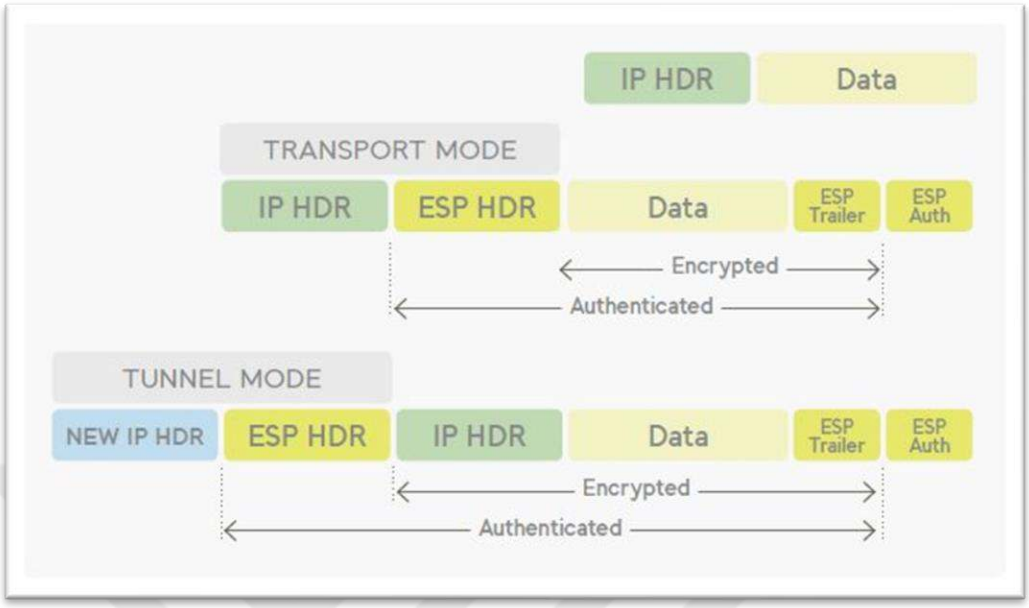

Figure 1.8: IPsec operation mode [38].

1.5.3 IPsec Protocols

IPsec standards have defined a key negotiation mechanism, IKE, and two data exchange protocols, ESP and AH. ESP is the most frequently encountered type used.

1.5.3.1 Authentication header

AH protects the entire IP datagram from spoofing and session hijacking threats by protecting the whole IP packet. AH, like ESP, computes the ICV over the IP header With payload using a secure hash method.

The ICV is a component of the AH header. While computing The ICV such as Checksum, TTL, and TOS, the AH protocol determines a group of IP header elements to be ignored to speed up the calculation process [6],[38],[39]. See the figure (Figure 1.9).

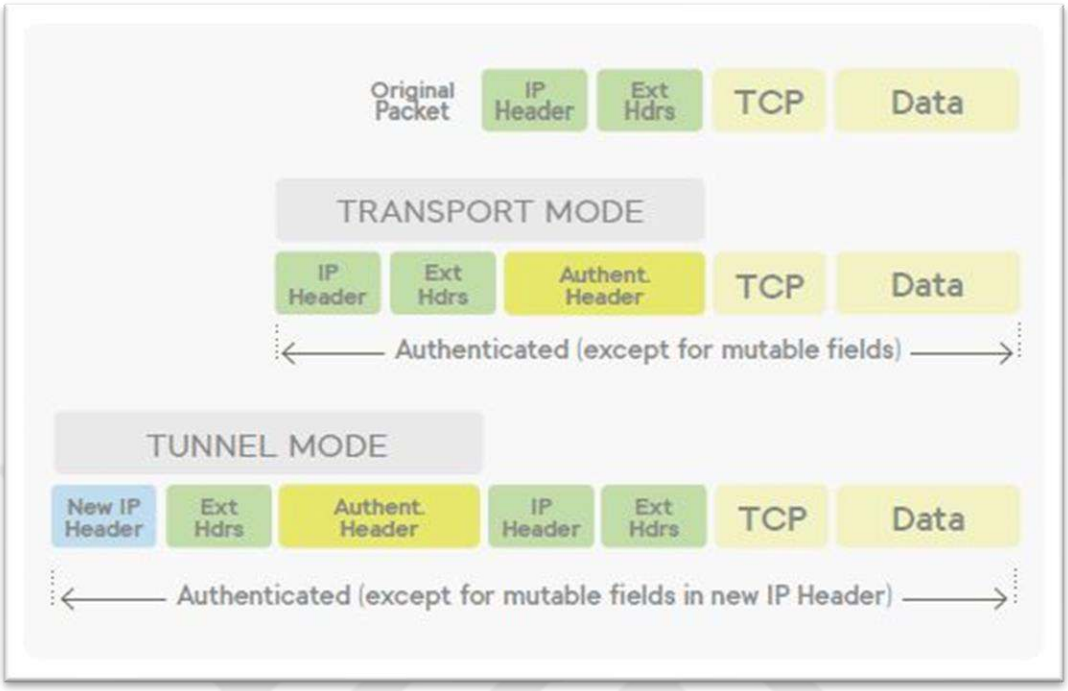

Figure 1.9: IPsec with AH mode [38].

1.5.3.2 Encapsulation security payload

The ESP protects the IP payload, ensuring data confidentiality, integrity, and replay protection. 3DES-CBC is a kind of encryption algorithm used to encrypt the payload. SHA1 or SHA2, are authentication protocols used to calculate the ICV of the payload which will be added on top of the payload in the header packet header, when the receiver gets the packet, it will decrypt the payload and calculate the ICV that must be matched ICV value. [38],[39].

Finally, if the calculation of ICVs value between the sender and receiver is not the same value, means data is altered and exposed to cyberattack. ESP algorithm requires protection unlike the AH algorithm. See the figure (Figure 1.10).

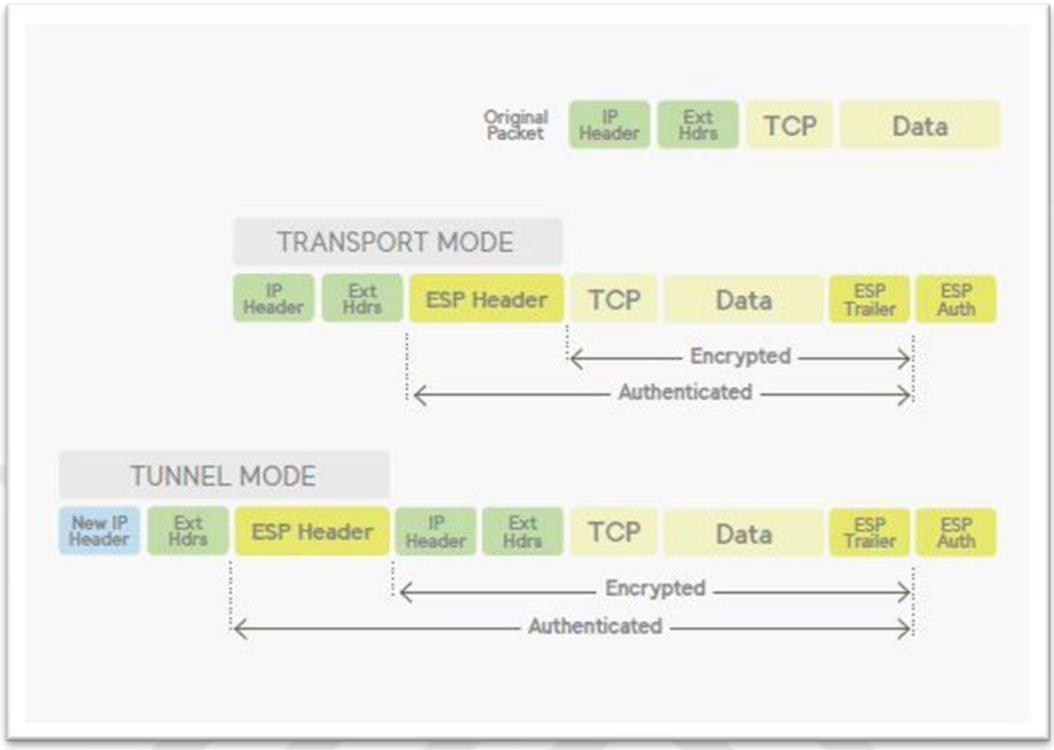

Figure 1.10: IPsec with ESP mode [38].

1.5.3.3 Security association

Security Associations (SAs), as they are referred to in IPsec nomenclature, serve as the foundation for IPsec operations. SA's are agreements between two parties that specify the IPsec protocols to be used for packet security, the transforms to be used, the keys to be used, and the duration of the keys to be used, among other things.

Secure associations (SAs) are a protocol used to establish a secure negotiation between two companies or organizations, IPsec is used to secure packets. To start interacting between two hosts, each client or node must have two SAs “in, out”. SA can specify security attributes such as encryption algorithm, encryption keys. SADB is the security association database to store all SAs for each node [9],[35].[6],[36],[38].

1.5.3.4 Internet key exchange

IKE defines the technique for establishing the security associations (SAs) required to secure packets between two IPsec peers. The transform specifics (the algorithm and the key) that will be

utilized to safeguard data are the essential components of security analysis. IKE specifies a method for automatically and securely negotiating these details between the two peers over the internet. There are two phases to the protocol's operation,[37][38],[40]:

A. Phase I (Authentication Phase):

Communicating over a public network is not secured, and the environment is exposed to cyber-attacks. Phase I to helps to start the negotiation and deploy and secure tunnel between communicated parties and produce security keys to protect the IKE protocol communications.

B. Phase II (Key Exchange):

When using the «Quick Mode», also known as Phase II, it is necessary to build the IPsec SA and generate fresh keying material.

1.6 DMVPN

1.6.1 Introduction

VPN is a sort of technology, which permits communication to the internet through a secured channel, it is becoming increasingly popular. This technology is frequently employed due to the low cost, wide availability, and high level of security provided by this technology. Conventional VPNs are set up statically and require a manual configuration to function correctly. As a result, consumers and enterprise companies have increasingly turned to DMVPN as an alternate solution to meet the demands of expanding organizational networks [41].

DMVPN is a solution used to build a wide network using some enhanced protocols called NHRP and mGRE, many advantages distinguish this network, configuring mGRE tunnel support remote uses to connect the network HUB with less time of configuration, once the remote router is attached to the network, dynamically il will assign with public IP by the feature of NHRP protocol, and start communicating with other remote sites. DMVPN works with different models, hub to spoke and spoke to spoke. GRE tunnel is combining public and private IP, without securing the packet, for this reason, IPsec protocol is applied to establish a secured GRE tunnel. [2],[37],[38][42]. See the figure (Figure 1.11).

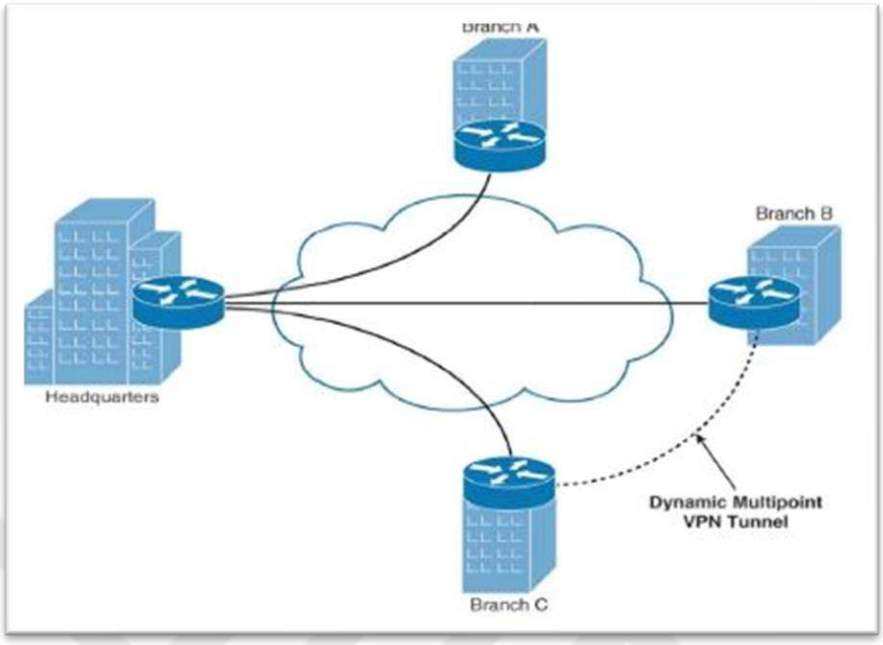

Figure 1.11: Dynamic Multipoint Virtual Private Network [43].

1.6.2 DMVPN Overview

By utilizing dynamic routing in DMVPN systems, it is feasible to meet corporate networks' mobility and flexibility requirements. However, due to this solution, a new difficulty has arisen: the security of data exchange which is that the multicast traffic in dynamic routing can not be encrypted by IPsec, for this reason, IPsec/mGRE tunneling is used to overcome encryption issue.. Various standard technologies are used in the DMVPN solution, which is briefly detailed in the following section[41].

GRE or mGRE is a tunneling protocol used to encapsulate IP packets to create the peer-to-peer tunnel, mGRE tunnel is not secured, to overcome this limitation, the IPsec protocol creates encryption by adding AH or ESP headers. NHRP maps between external and internal IP addresses. By using NHRP clients all spokes advertise their status and are assigned with IP addresses [44].

1.6.3 DMVPN Component

DMVPN is a hub/spoke model, it uses IPsec/mGRE protocol to tunnel and secure traffic between remote sites over the public internet. GRE is an encapsulation protocol used to aggregate many

types of traffic whether multicast or broadcast and combine them as unicast traffic. NHRP protocol is used to map between the private network and the public network in the DMVPN

1.6.3.1 Multipoint generic routing encapsulation

DMVPN introduces the mGRE interface, a "one-to-many" interface for creating many hubs and multiple spoke tunnels comparable to Frame Relay interfaces. V tunnel destinations are not configured, unlike p2p GRE tunnels. The headend is equipped with a mGRE interface in all DMVPN configurations to construct a dynamic tunnel for each linked branch. Compared to static p2p GRE topologies, the mGRE tunneling minimizes the configuration commands for each router tunnel interface, a benefit for large-scale designs. Individual tunnel instances exist for each linked distant spoke even with a mGRE interface, these tunnel instances have the advantage of being dynamically configured[45]. See the figure (Figure 1.12).

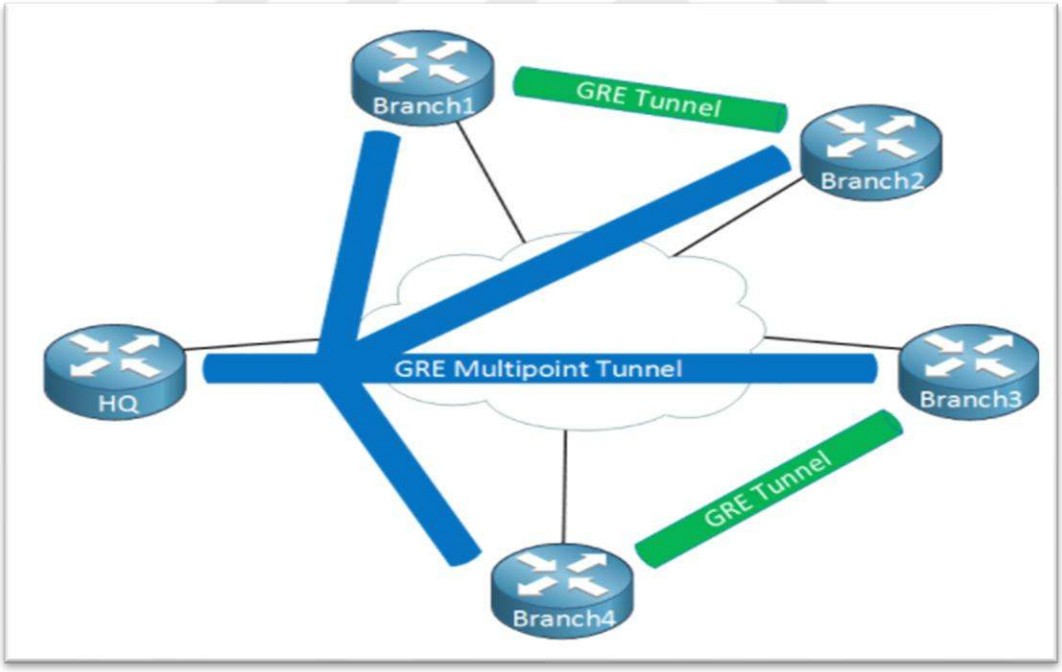

Figure 1.12: Multipoint Generic Routing Encapsulation [46].

It is necessary to use IPsec to encrypt mGRE, because that mGRE is unicast traffic, as seen in the Figure (Figure 1.13), IPsec header is on top of GRE data which encrypts all GRE data header, which means GRE packet has the same IP of IPsec, because in the same header and this assures that GRE IP is fixed.[41],[47],[48],[45]. See the figure (Figure 1.13).

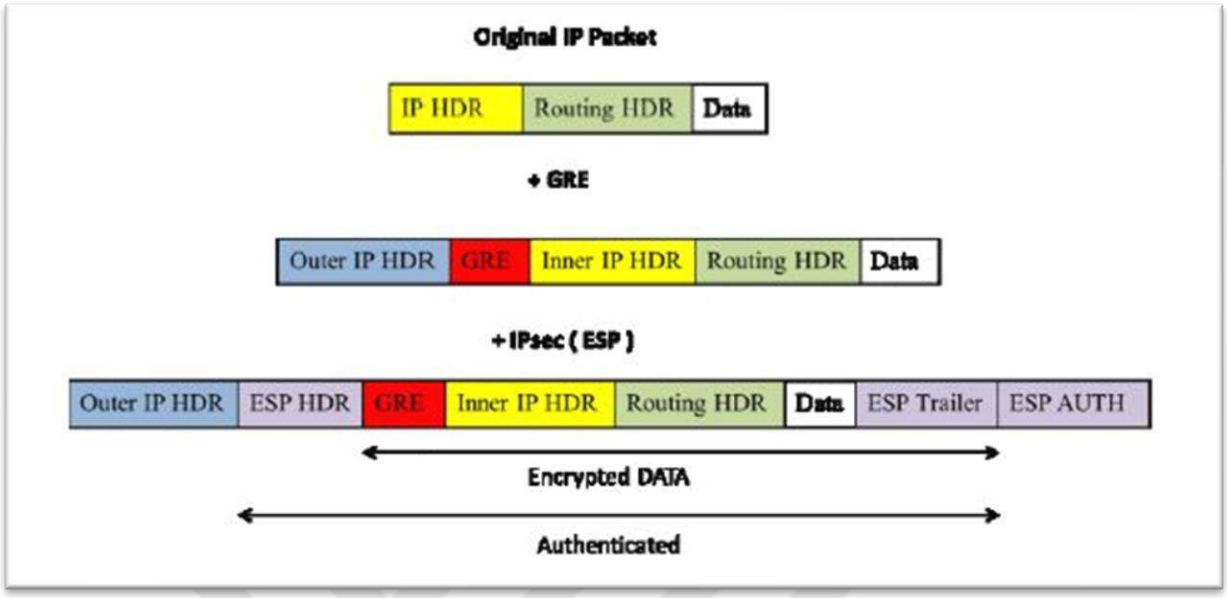

Figure 1.13: GRE/IPsec protocol encapsulation [41].

1.6.3.2 Next hop routing protocol

NHRP protocol used to map between two different IP network addresses in the DMVPN network, the GRE tunnel is assigned with a private IP address which is called an overlay network, while the public address is assigned to the source or destination of the tunnel address which is called underlay network. All spokes advertise updates periodically to the hub using the NHRP server, when a new spoke is connected, instantly, spoke information gets registered in the NHRP database in the HUB using NMBA address and NHRP protocol[45],[49].

1.6.3.3 Routing protocol

IGP as named (Interior Gateway Protocols) are dynamic routing protocols to route packets between different nodes and remote sites; furthermore Operating the DMVPN network in an optimized manner requires the selection of proper routing protocols to gain perfect performance and avoid network congestion and un stability[50].

1.6.4 DMVPN Phases

Three main phases operate in the DMVPN network, each phase has a specific topology and network attributes, the following section illustrates the main characteristics of each phase.

A. Phase 1: Hub to Spoke

The IP address of the Hub is used as the network server in this phase. As a result, each spoke has a static tunnel destination IP corresponding to the Hub's physical address. Hence, the Hub is the only way for spokes to communicate. The streamlined Hub configuration is a significant benefit of DMVPN Phase 1. Furthermore, choosing a routing system is simplified because practically any dynamic routing protocol will assist in achieving reachability. Spokes use the Hub advertises to determine its routes, and by using NHRP protocol, all spokes send periodic updates to the hub providing network subnets. In this phase, tunneling between spokes is not supported, the traffic between spokes must pass through the hub [51].

B. Phase 2: Spoke to Spoke

In Phase 2, all routed traffic passes between all spokes without crossing the hub, moreover, all the routing updates are sent by all spokes, due to this network may encounter scalability issues, such as expanding networks, moreover, due to high routing traffic generated by spokes, the network may encounter traffic congestion that issues poor network quality [51].

C. Phase 3: Spoke to Spoke with network infrastructure scalability

This phase is considered the most enhanced phase due to some improvement in network summary, It is a spoke-to-spoke model, when the hub broadcasts the routes, all local routes generated by the spoke can be summarized. [51].

Using DMVPN Phase 3, when the hub router returns the routing information to the remote spokes, then, summarizing the routes of the local spokes can be done, which is a helpful feature. Summarizing the local network does not affect the functionality, because in this case, knowing the networks behind the spokes will not make a difference. Phase 2 DMVPN necessitated that each spoke is well-versed in their specific network routing[45].

1.6.5 Dynamic Routing Protocol Over DMVPN Network

All scalable DMVPN systems use dynamic routing protocols to interconnect between different sites and locations.

When compared to traditional networks, routing protocols in a VPN provide the same functionality, which includes:

i. Network routing information
ii. Network change alerts
iii. Node status

Numerous DRP, including the following, can be employed to operate the DMVPN network:

i. Enhanced Interior Gateway Protocol (EIGRP)
ii. Open Shortest Path First (OSPF)
iii. Routing Information Protocol version 2 (RIP v2)
iv. On-Demand Routing (ODR)

DMVPN networks of enormous scale are devoid of any other means of exchanging routing information than through routing protocols. The disadvantage is that the CPU consumption on the network node will increase; for this reason, choosing dynamic protocol properly while developing the DMVPN network to avoid any network defects [45].

Typically, based on network topology and the number of network nodes, routing protocol represents the primary constraint, moreover, the throughput of the encryption must be considered when the router acts as a hub and calculating the average amount of throughput per spokes to keep sufficient traffic to handle between hub and spokes [45].

All routing protocols are algorithm-based. This algorithm must specify specific steps that ensure the routing protocols run correctly. These methods are as follows:

i. A process for receiving and transmitting network information
ii. Using a routing database for determining the optimal route to a destination.
iii. Finally, a mechanism for detecting, reacting to and informing other devices about network topology changes.

Distance Vector and Link State are the two protocols used based on The Bellman-Ford and Dijkstra algorithms.[52].

1.6.5.1 Link state routing protocol

LSRP is an intra-domain routing protocol that is used for networks that span multiple domains but are all under the same domain. When using link-state routing, the routers generate Link State Packets (LSP) regularly, usually every 1-2 hours. The LSP comprises information on the node's identity, a list of links, a sequence number, and the node's age. Following the creation of LSP, the routers distribute it to all other routers. The router uses the Dijkstra method to construct the shortest path tree.

1.6.5.2 Distance vector routing protocol

It is routing protocol uses database of routing table containing information about distances and directions.

The minimal distance for packet transferring is always included in the router table when using hop count as the metric; therefore, the minimum cost is the smallest number of hops or routers required to transmit the packets from source to destination and vice versa. Each node periodically distributes its routing table to the nodes near its vicinity. The table below (Table 1.1) shows the most important attributes of routing protocols.

Most of the time, routers generate and update their routing tables using some sort of algorithm. The bellman-ford algorithm is one of the most commonly used algorithms.

Table 1.1: Dynamic routing protocol specifications [53].

Protocol	Protocol type	Algorithm Type	Algorithm mechanism	Convergence	Scalability	CPU usage
EIGRP	IGP	Bellman-Ford	Distance Vector	Faster	Good	High
RIP	IGP	Bellman-Ford	Distance Vector	Slower	Medium	Low
OSP	IGP	Dijkstra	Link State	Faster	Good	High

1.6.5.3 Enhanced interior gateway routing protocol (EIGRP)

EIGRP is an improved version of IGRP, it supports IPv4, and it combines both features of Distance vector protocol, which is sending all routing table entries to the connected nodes, and gain the feature of link-state which provides routers with the information of directly connected links. EIGRP has a faster convergence due to recording and saving the entire network routes, changing only routing information that is not included in the neighboring table. EIGRP is used in scalable networks, because of its high capabilities when the topology changes. [54].

The metric is used to see if the chosen route is optimal. The bandwidth, delay, dependability, load, and MTU are all factors in the EIGRP statistic. Metric= BandWidth+Delay* 256 is the default EIGRP metric expression. EIGRP is made up of four basic components, which are as follows:

i. Neighbor Discovery/Recovery
ii. Protocol Dependent Module
iii. Reliable Transport Protocol
iv. DUAL Finite State Machine

1.6.5.4 Routing information protocol (RIP)

RIP is a standardized vector distance routing protocol that determines route selection using a type of distance metric called the hop count. A vector of distances denotes it. RIP avoids routing loops by limiting the number of hops permitted in paths connecting sources and destinations. The maximum number of hops permitted for RIP is 15, as per standard practice. However, to eliminate routing loops, the size of the supporting networks must be lowered. Additionally, because RIP permits a maximum of 15 hop counts, the route will be considered inaccessible if the number of hop counts exceeds 15 [54],[55].

1.6.5.5 Open shortest path first (OSPF)

OSPF is a protocol defined in RFC 2328, OSPF is the most widely used routing protocol in large industrial networks, and it dominates the three samples investigated. OSPF is based on the link-state protocol and determines the shortest path between two sites using the SPF algorithm" [54],[55].

Before attempting to complete the computation, all routers in the network must be aware of one another and the links that connect them. The next phase entails calculating the shortest path between each router. They share link-state information for all routers, which is stored in the link-state database. A router's database is updated with the information included in a link-state update, and the router that got the update propagates the amended information to all other routers [54],[55].

In the case of OSPF, the cost (metric) is the cost of transmitting packets in a specific interface. Cost= 10000 0000 /BW. Bandwidth cost would be lesser if the capacity were higher[54],[55].

1.7 CRYPTOGRAPHY

1.7.1 Introduction

The usage of virtual private networks (VPNs) allows company employees to share resources more conveniently and operate more efficiently, yet current VPN technology is still potentially susceptible. The architecture of the VPN's Cryptographical System, which includes various critical aspects such as encryption, authentication, and VPN tunneling, is responsible for the security of the VPN[56].

When data cryptography is used, it encrypts the content of data files (such as text or images), making them incoherent and unreadable throughout the transferring process (also known as encryption) to prevent data fraud or make them unintelligible and illegible. The act of converting original plain text into ciphertext is called the encryption process while the decryption process is the steps of retrieving the original text from the ciphertext [57].

Cryptography is mainly used to safeguard data from being compromised by hackers. It is required to have a large keyspace to raise the encryption's security level [3]. “The size of the key space affected the time required for an intruder to hack it; the more significant the key space, the greater the security level. A larger keyspace enables a greater variety of alternate keys, including those with typical key widths of 128, 192, or 256 bits. For instance, if the usual key size is 256, a keyspace with a key size of 2256 is available. The primary reasons for utilizing the encryption method throughout the data transfer procedure are to defend against data theft, data fraud, and data loss. Cryptography can be classified into symmetric (private) keys encryption and asymmetric (public) keys encryption. The most often used symmetric key algorithms are Advanced Encryption

Standard (AES), Triple DES (3DES), and Data Encryption Standard (DES). In contrast, the most widely used asymmetric key algorithms are Rivest-Shamir Adelman and RSA (RSA)" [57], [58],[59],[60].

1.7.2 Types of Cryptographic Algorithms

1.7.2.1 Secret key cryptography (SKC)

Symmetric encryption is a type of encryption that uses the same key for decryption. It is mainly employed for privacy and confidentiality[61]. The most commonly used algorithm are AES, DES, 3DES, and Blowfish[62],[63],[64].

1.7.2.2 Public key cryptography (PKC)

Asymmetric, which is encryption, uses a unique key for encryption and a unique key for decryption. Authentication, non-repudiation, and key exchange are the primary functions of this protocol[61]. The most known algorithms used are TLS, RSA, and Diffie-Hellman

1.7.2.3 Hash Functions

"It uses a mathematical calculation to "encrypt" information irreversible in order to produce a digital fingerprint. Message integrity is the main process to calculate ICV" [61]. Message digest (MD) and Secure Hash Algorithm (SHA) are commonly used. The figure below (Figure 1.14) shows the types of cryptography[65].

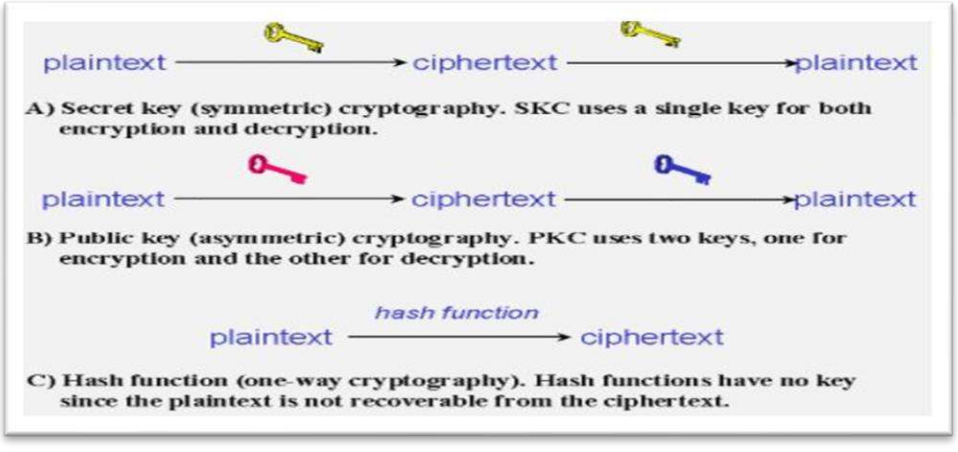

Figure 1.14: Type of cryptographic algorithms [61].

The table (Table 1.2) illustrates the significant attributes of the Secret Key Cryptography.

Table 1.2: Secret key cryptography attributes.

	Plain text Block bit size	**Ciphertext Bit size**	**Key bit size**	**Encryption level**	**vulnerability**
AES	128	128	128,192 or 256	High	Brute-force attack
3DES	64	64	112 or 168	Medium	Brute-force, Differential Crypt attack
DES	64	64	56	Low	Linear crypt differential Crypt analysis

The (Table 1.3) shows the comparison of the most known integrity protocols, MD5 and SHA.

Table 1.3: Differences between MD and SHA protocols [53].

	Message Length	**Attacks**	**Speed**	**Time required to break message**	**Security Level**
MD5	128 (Bit)	Some reports	Fast	2^128 bit	High
SHA	160 (Bit)	No reports	Slow	2^160	Super Higher

2. LITERATURE REVIEW

The VPN provides a safe network in a non-secure network, making it one of the most used methods for linking remote locations. Despite the better security level of traditional VPNs, several restrictions and implementation consequences exist for a scalable network. A static configuration requires a unique public IP, tunnel, and physical interface for each site, and adding more remote sites requires resetting all network equipment, causing network connectivity issues. The "DMVPN" network ensures smooth deployment, reduces implementation time, saves bandwidth while maintaining a high level of confidentiality, integrity, and availability.

The DMVPN network utilizes dynamic routing protocols to route network traffic. nevertheless, adopting the improper protocol can have undesired consequences. Because DMVPN traffic is vulnerable to theft and fraud, IPsec/mGRE security and tunneling protocols are utilized to secure network traffic. Peer-to-peer data encryption utilizes a variety of encryption techniques. Encryption is classified into two types: symmetric and asymmetric; most common symmetric algorithms include DES, 3DES, and AES, while, RSA encryption is considered asymmetric.

Dynamic routing protocols and encryption techniques play an essential role in managing and optimizing DMVPN networks. To improve and evaluate network performance, Dynamic routing technologies whether distance-vector such as RIP protocols or link-state such as OSPF or hybrid such as EIGRP are deployed and evaluated with most common encryption techniques such as DES, 3DES, or AES to analyze network characteristics such as speed, jitter, latency, and bandwidth.

Several pieces of research have been focused on and conducted to determine the optimum routing and encryption performance for DMVPN, which is critical in terms of performance. The proposed solutions are reviewed in chronological sequence.

As demonstrated in [45]; Large-scale DMVPN networks can only share routing information using routing protocols. The disadvantage is increased CPU usage on the network device, which must be factored into the DMVPN deployment. Typically, the number of spoke nodes that can communicate with the hub router is restricted by the routing protocol. Moreover, the encryption throughput of the hub router forms a limiting factor. This average per-spoke value is calculated by dividing it by the number of supported spoke routers. The assumed burden is caused by spoke

routers attempting to access resources behind the hub router. Because not all spokes stay active, there is frequently considerable oversubscription.

EIGRP is Cisco's recommended dynamic routing technology due to its low CPU usage and fast convergence. EIGRP additionally offers address summarization and default route propagation settings.

According to [42], the authors implemented DMVPN spoke-to-spoke network in OPNET MODELER 10.5 and examined the effect of Qos assurance when using different routing protocols (RIP, EIGRP). The authors investigated the impact of tunnel formation on multiple flow packs delay in spoke-to-spoke connection; the results showed that RIP protocols had the most negligible delay value when hops did not exceed 15; OSPF protocol was not recommended due to its scalability issues; Adding more than 50 routers in the same OSPF area cases undesirable results. Moreover, one router is restricted with only three areas. However, the EIGRP protocol is the best routing protocol with a scalable network.

In [66], the authors deployed a DMVPN network to evaluate network scalability by using different routing protocols (OSPF, EIGRP, BGP). Some critical parameters are tested to evaluate network performance, such as network convergence, delay, queuing, and throughput; authors used Opnet Modeler to establish the network; authors applied three different scenarios to study the performance of DMVPN scalability. Three different networks were implemented, 6 sites, 11 sites, and 20 sites as a single hub and multi spokes. The authors demonstrated that EIGRP outperforms OSPF in latency time, throughput rate, and queuing time delay, whereas BGP outperforms OSPF in terms of efficiency.

In [67], Siti Ummi Masruroh and et al, evaluated and compared different routing protocols performance in various phases of DMVPN, used GNS3 simulator to establish the network, tested many parameters such as jitter, latency, throughput, and packet loss. The authors used "Iperf" tools to send TCP and UDP traffic in different window sizes. The results demonstrate that the RIP protocol in Phase 2 shows a high throughput rate value, while the highest value of jitter is obtained by EIGRP. DMVPN phase 3 RIP shows the greatest percentage value of the dropped datagram. Finally, DMVPN phase 3 shows lower parameter values among other DMVPN phases.

In [57], Fenny Anak Daud and et al, tested several DMVPN performance parameters (Latency, Speed, Throughput, Packet loss) with different encryption types (AES, DES, 3DES). The findings confirm that when files transfer between source and destination while applying AES encryption takes more time and reduces the speed unlike when traffic is not encrypted. AES outperforms DES and 3DES algorithms and shows better performance in all other scenarios

In [68], Ayoub Bahnasse and et al evaluated the quality of videoconferencing technology in the DMVPN network; they tested the influence of site count, participant count, and the impact of routing protocol (EIGRP, OSPF); they used the Riverbed Modeler simulator to implement the DMVPN network. Moreover, they investigated some sensitive parameters such as packet loss, variance in delay, the volume of transmitted traffic, and protocol routing convergence. The results revealed that the number of sites has less of an impact on videoconferencing than the number of clients; Moreover, the EIGRP shows the best for videoconferencing traffic routing.

In [2], Hasan Mohamed Marah and et al, studied and analyzed the impact of dynamic routing protocol in DMVPN network phase 1 and phase 2; additionally, phase 2 is implemented using IPsec encryption to determine the effect of security protocols on DMVPN performance. Additionally, the authors examined and contrasted phase 1 and phase 2 performance in terms of latency, packet loss, jitter, and throughput. The results revealed that the Phase 2 design has significantly better values for all metrics than phase 1, indicating that it is more valuable than phase 1. With IPsec security tunneling, throughput dropped to 4.41 Mbits/sec in phase 2, which is requiring consideration of security protocols when building DMVPN networks.

In [53], the authors implemented the DMVPN phase 3 network using GNS3 simulator; they tested and compared the performance of the DMVPN network with consideration of three different dynamic interior gateway protocols such as (RIP, OSPF, EIGRP) and various encryption techniques (3DES, DES, AES). In addition, 18 different scenarios were implemented to find the optimum pair of protocols to operate and enhance the DMVPN network. The findings showed EIGRP/AES and RIP/3DES are the best protocol combinations when input streamed data = 500KB and BW = 500KB/S, when the data input is equal to (256KB) and below the bandwidth limit of 500 KB/S, RIP/AES is the best protocol combination.

In [41], the authors surveyed to examine several works on the DMVPN concept and demonstrated the limits of the existing methods designed to address DMVPN concerns. The authors addressed many issues based on the challenges that researchers encountered. The table (Table 2.1) shown below illustrates the findings of the most relevant works related to the DMVPN issues organized in chronological order.

Table 2.1: Comparison of routing protocol performance over DMVPN.

Author	Year	Objective	Contribution	Results	Drawbacks
Thorenoor, S. G	2010	Find the most effective protocol type of DMVPN	(EIGRP, RIP, OSPF) protocols tested	EIGRP shows better performance	Static scenarios
Nowosielski, et al	2015	Encryption algorithm impacts	Resolve data confidentiality Issues using different encryption protocols	DMVPN/IPsec offers considerable flexibility and security.	Only DMVPN phase1 is verified.
TIZAZU, et al	2017	Show the best Dual Hub DMVPN hub-to-spoke routing protocol.	Compare routing protocol performance (latency, delay time, convergence speed, and link usage)	EIGRP is the most suitable protocol	Hub-to-Spoke topology is tested.
AJANI, et al	2017	Show which routing protocol recovers fastest after a failure.	Compare RIP, OSPF in terms of failover recovery	OSPF for high-failure networks, RIP for low-failure networks	Only MAN is used in the study

3. METHODOLOGY

3.1 INTRODUCTION

Cisco's DMVPN (Dynamic Multipoint VPN) network is the greatest solution to the lack of industry-standard VPN approaches. To operate the DMVPN network, it is necessary to configure mGRE, NHRP, and the routing protocol. Due to the insecure nature of GRE, IPsec/mGRE protects network traffic and provides security and integrity to the network. Routing protocols and encryption mechanisms both help improve DMVPN performance. Encryption methods are a critical factor in determining IPsec network performance. Numerous scenarios and experimental laboratories were run, tested, and tweaked to provide the best outcomes. Numerous aspects of the DMVPN network are evaluated and studied to determine its performance. These characteristics include throughput, jitter, speed, packet loss, and latency. It examines the performance of EIGRP, RIP, and OSPF routing protocols and encryption methods (AES, 3DES, and DES) to determine the optimal routing protocol and crypto algorithm combination for boosting the performance of DMVPN networks.

3.2 DMVPN NETWORK CONSIDERATION

i. DMVPN has three main phases used to interconnect remote sites, phase three is developed to overcome limitations in phases one and two, phase three can handle fast routing than phases two and one due to its fast local routing summarization.

ii. Heavy traffic between nodes might affect router use, bandwidth consumption, and convergence time. Numerous dynamic routing protocols, such as EIGRP, RIP, OSPF, BGP, ISIS, and ODR, are used to route traffic between branch offices, even though not all routing methods are suitable for usage in scalable networks. For this reason, routing protocols have a significant impact and must be selected based on network scalability.

iii. The IPsec protocol supports two distinct encryption modes: transport mode and tunnel mode. Due to the encryption method used in DMVPN phase 3, the network must be set in transport mode. When transport mode is used, the payload of GRE/IP header is encrypted, and the processing time is significantly decreased compared to when tunnel mode is used.

3.3 ENVIRONMENT ASSUMPTION AND LAB SETUP

The specifications of the hardware utilized in the simulation significantly impact the findings obtained in the experiments, moreover, the IOS (RAM & CPU) running in the lab may occur unexpected results, for this reason, tuning of experimentation and taking data output several times will help to reduce data inconsistency and provide excellent and steady results. Nonetheless, it is advised that all studies be carried out on actual network gear to obtain realistic findings. The number of remote sites is niglicted in out research as it has been studied in several conducted research.

Main PC and simulation tools are used to implement the DMVPN network. The GNS3 simulator is the main simulator used to perform all experiments with the support of a virtual machine (Virtual Box). GNS3 has several advantages over other network simulators, such as a packet tracer; GNS3 can use real Cisco IOS images, which enables the creation of complex network designs. Additionally, "Iperf3" version 3 is GNS3 built-in tool that is extremely useful for measuring network parameters, which helps to generate different UDP, TCP streams in different server-client modes. The router IOS sources, system characteristics, and measurement performance tools are recommended in this lab are based on best practice experiments. See table (Table 3.1).

Table 3.1: Hardware and Software Specification.

Hardware Specification	
Machine	Main PC
Operating System	Windows 10 Professional
Status	Host OS
Software Specification	
Virtual Machine	Virtual Box version “6.1.4 r136177 (Qt5.6.2)”
RAM Size	8G
IOS and Router	C7200, Version ‘12.4(24)T5”
Simulator	GNS 2.2.7“GNS VM 2.2.7 ubuntu (64 bit)”
Client & Server OS	Ubuntu 18.04.1
Measurement Tool	Iperf version 2

3.4 NETWORK DESIGN AND IP PLAN

The figure (Figure 3.1) illustrates the primary DMVPN topology, demonstrating a single hub-multispoke topology consisting of a single hub (HUB) acting as a server and five spokes (SP 3, SP 4, SP 5, SP 6, SP7) acting as clients linked via ISP. Additionally, six personal computers (PC1,to PC6) which are running Ubuntu 8.04.1 OS and connected via a LAN network. Six tunnel interfaces are considered underlay networks (a private network) assigned with tunnel IP address 192.168.1.x, and 6 WAN interfaces are used as an overlay network (public network) configured with NMBA IP address x.0.0.1. Each PC includes a network measuring tool called "Iperf2" that consists of a variety of valuable capabilities for monitoring network KPIs such as Speed, packet loss, bandwidth, jitter, CPU usage, etc.). Iperf2 tools support many significant features which allow generating several sorts of network traffic streams such as UDP and TCP traffic, moreover, it sets different attributes; additionally, Iperf supports multi-client traffic mode allowing data input to be sent to multiple network clients concurrently, allowing for more precise measurement and calculation of output results. ICMP utility is used to test the reachability of hosts. The WAN connections are all gigabit, while the LAN ports are fast ethernet (100mbps). Refer to the table (Table 3.2).

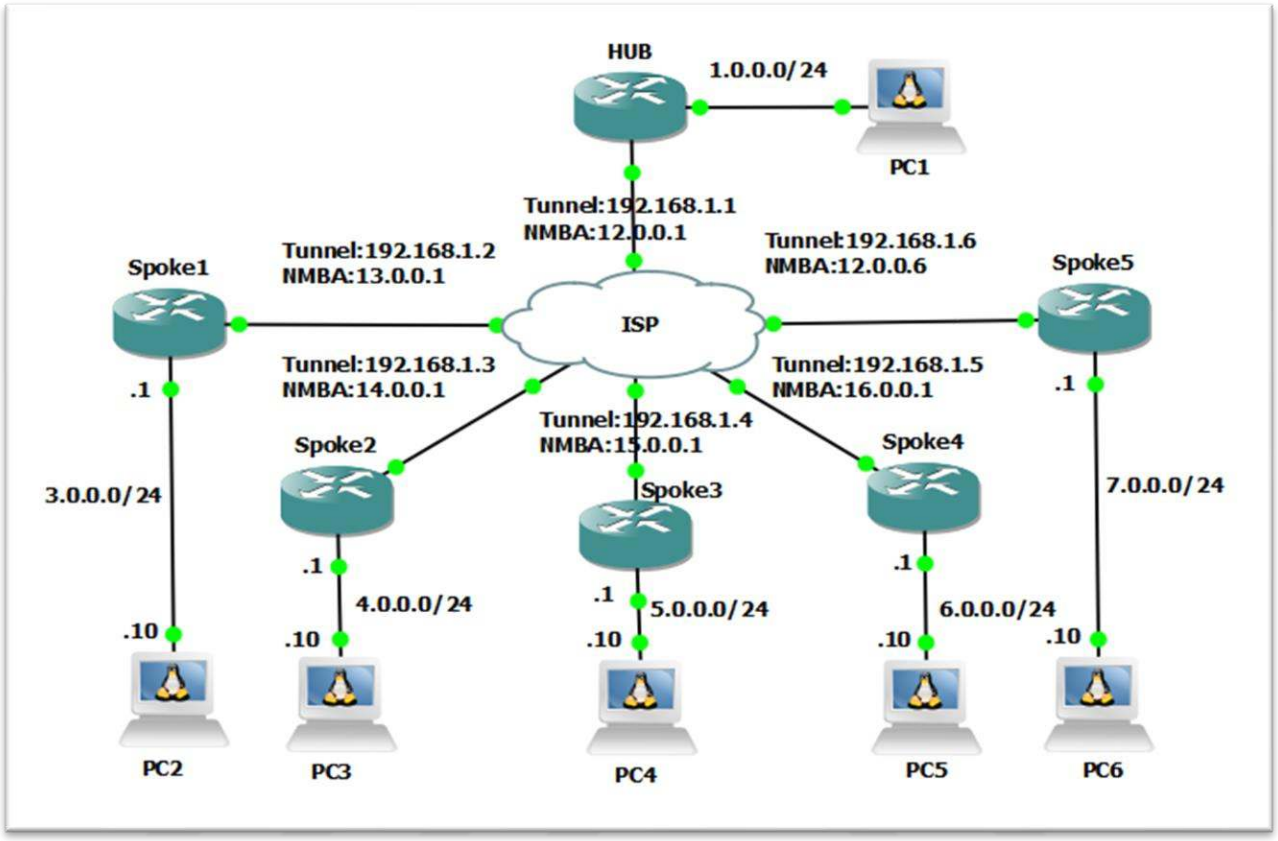

Figure 3.1: DMVPN Network Design and IP Plan.

Table 3.2: IP plan and Interface label.

Network Device	**IP & Interface Type**		
	Tunnel IP	**WAN Interface**	**LAN Interface**
Internet service provider (ISP)	No IP	g1/0 12.0.0.2	No IP
		g2/0 13.0.0.2	
		g3/0 14.0.0.2	
		g4/0 15.0.0.2	
		g5/0 16.0.0.2	
		g6/0 17.0.0.2	
Hub	192.168.1.1	g1/0 12.0.0.1	g2/0 1.0.0.1
Spoke 3	192.168.1.2	g1/0 13.0.0.1	g2/0 3.0.0.1

Spoke 4	192.168.1.3	g1/0 14.0.0.1	g2/0 4.0.0.1
Spoke 5	192.168.1.4	g1/0 15.0.0.1	g2/0 5.0.0.1
Spoke 6	192.168.1.5	g1/0 16.0.0.1	g2/0 6.0.0.1
Spoke 7	192.168.1.6	g1/0 17.0.0.1	g2/0 7.0.0.1
PC1	N/A	NA	Eth0 1.0.0.10
PC2			Eth0 3.0.0.10
PC3			Eth0 4.0.0.10
PC4			Eth0 5.0.0.10
PC5			Eth0 6.0.0.10
PC6			Eth0 7.0.0.10

3.5 NETWORK CONFIGURATION AND IMPLEMENTATION

Basic standards and recommended configurations based on best practices on Cisco devices used to implement DMVPN Phased 3 Network, Routing protocol configuration (EIGRP, OSPF, RIP), and all DMVPN components such mGRE, NHRP, and IPsec configured in best-optimized practice.

3.5.1 ISAKMP Policy Configuration

For IKE Phase 2 to succeed, both prospective crypto peers must have at least one matching ISAKMP policy. The following configuration demonstrates an ISAKMP authentication policy that uses secret-key pre-shared keys (PSKs) certificates (a.k.a. digital certificates). SHA 256 is configured as a hash function; although SHA is slower than MD5, it is more secure.

Diffie-Hellman (DH) is a public-key cryptography scheme used to encrypt the traffic between two peers over a public network. IKE employs Diffie-Hellman to generate keys that are used to encrypt both the Internet Key Exchange (IKE) and IPSec communication channels.

DH Group 2 is employed, which uses a 1024-bit key. Three distinct encryption algorithms, AES, DES, and 3DES, were utilized to encrypt DMVPN tunnel communication in each instance.

**Global IKE policy // Policy Configuration

**Protection suite of priority 1

**encryption algorithm: AES - Advanced Encryption Standard (128-bit keys).

**hash algorithm: Secure Hash Standard

**authentication method: Pre-Shared Key

**Diffie-Hellman group: #2 (1024 bit)

**lifetime: 86400 seconds, no volume limit

Figure 3.2: ISAKMP Policy Configuration.

3.5.2 IPsec Transform Configuration

IPsec is configured based on specifying authentication and encryption algorithms, to ensure the tunneling between the peers, all transforms must be the same to start peers negotiation, whether using any type of IPsec protocols such as ESP, AH, all attributes must be configured to match peers to start deploying IPsec session. [45]. ESP is utilized as the IPsec exchange protocol in our configuration.

**Transform set abc: { ah-sha-hmac } will negotiate = { Tunnel, },

**{ esp-aes } will negotiate = { Tunnel, }, // AES Encryption

**Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac }// Athentication

**will negotiate = { Transport, },

Figure 3.3: IPsec Transform Configuration.

3.5.3 Tunnel Protection and IPsec Profile

Setting the IPsec profile is configured by grouping tunnel settings and determining the transform-set of the DMVPN. To associate an IPsec profile with a tunnel interface, use the " *tunnel protection IPsec profile profile-name* command". [45].

```
**crypto ipsec profile dmvpn 10 // Tunnel protection

**set transform-set abc

**interface Tunnel1

**tunnel protection ipsec profile dmvpn 10
```

Figure 3.4: Tunnel Protection and IPsec Profile.

i. MGRE Tunnel Interface Configuration

Multiple tunnel destinations are possible with mGRE configuration. The mGRE arrangement on one side of a tunnel has no bearing on the tunnel properties on the opposite side. This provides the ability to mGRE tunnel on the Hub to establish a connection to a peer-to-peer tunnel on the opposite side. Multipoint GRE in unlike peer-to-peer GRE interface, the tunnel destination can distinguish the mGRE interface, moreover, mGRE can tunnel with any remote interface without determining a specific destination. To enable multiple destinations for a mGRE tunnel, the tunnel endpoints must be resolved using NHRP. mGRE setting is required in the Hub side, and optional in hub-to-spoke mode, but in spoke-to-spoke mode, mGRE is necessary on all spoke nodes[45].

```
**interface Tunnel1

**IP mtu 1436

**ip address 192.168.1.2 255.255.255.0

**tunnel source 13.0.0.1

**tunnel mode gre multipoint // Hub and Sopke
```

Figure 3.5: MGRE Tunnel Interface Configuration.

i. NHRP Configuration

NHRP is configured to map a connection between overlay network (public network) and underlay network (private network) addresses, NHS server locates tunnel endpoints and determines a map of network spokes. Each endpoint (spoke) configures its public and private mappings with the NHS. NHS mapping on a local level must remain static at all times. To connect NHRP mapping with the NHS server, NHRP static must be configured in the spoke router [45].

ii. Hub Configuration.

```
**interface Tunnel1
**ip address 192.168.1.1 255.255.255.0
**no ip redirects
**ip nhrp authentication DMVPN
**ip nhrp map multicast dynamic
**ip nhrp network-id 1
**ip nhrp shortcut
**ip nhrp redirect
**tunnel source 12.0.0.1
**tunnel mode gre multipoint
```

Figure 3.6: Hub Configuration.

iii. Spoke Configuration

```
" interface Tunnel1
** ip address 192.168.1.2 255.255.255.0
**no ip redirects
**ip nhrp authentication DMVPN
**ip nhrp map 192.168.1.1 12.0.0.1
**ip nhrp map multicast 12.0.0.1
**ip nhrp network-id 1
**ip nhrp nhs 192.168.1.1 // NHRP
**ip nhrp shortcut
**ip nhrp redirect
**tunnel source 13.0.0.1
**tunnel mode gre multipoint // MGRE
**tunnel protection ipsec profile dmvpn"
```

Figure 3.7: Spoke Configuration.

3.5.4 Routing Protocols

3.5.4.1 EIGRP

The DMVPN network functions smoothly and provides the most acceptable dynamic routing exchanges by implementing a proper configuration. Additionally, the HUB should disable the IP SPLIT HORIZON option to ensure that the HUB broadcasts route out of the interface tunnel via which they were received. Further, the IP NEXT-HOP-SELF option should be disabled; by default, the HUB configures the IP next-hop value for routes it advertises to be itself; when this option is

enabled, Spokes will constantly interact via the HUB. The STUB-linked option must be set at spokes, which allows spokes to re-advertise only directly related routes, optimizing resource consumption and assuring stability [47].

The following configurations detail the EIGRP setup that is suggested for DMVPN networks.

i. Hub Configuration

```
**router eigrp 100 //
**network 1.0.0.0
**network 192.168.1.0 // next hop
**auto-summary
,,,,,,,,,,,,,,,,,,,,,
**interface Tunnel1 // tunnel configuration
**no ip next-hop-self eigrp 100
**no ip split-horizon eigrp 100
```

Figure 3.8: Hub Configuration (EIGRP).

ii. Spoke Configuration

```
**router eigrp 100
**network 3.0.0.0
**network 192.168.1.0
**auto-summary
**eigrp stub connected
```

Figure 3.9: Spoke Configuration (EIGRP).

3.5.4.2 OSPF

OSPF in a DMVPN network should adhere to the same OSPF constraints as in other networks; no router should have more than three zones, and no area should have more than fifty zones. In a DMVPN network, OSPF consumes the selected router's CPO resources and IPsec encryption and NHRP trade over. As a result, the specified router must be connected to every spoke on the network [47].

To maintain scalability and stability, an OSPF router should not be set in more than three areas. Along with the OSPF algorithm's high CPU usage, the additional complexity associated with encryption and NHRP discussions must be incorporated into the network topology design..

i. Hub configuration

```
**router ospf 1**

**network 1.0.0.0 0.0.0.255 area 0

**network 192.168.1.0 0.0.0.255 area 1

**interface tunnel1

**ip ospf network broadcast
```

Figure 3.10: Hub Configuration (OSPF).

ii. Spoke Configuration

```
**router ospf 1

**network 3.0.0.0 0.0.0.255 area 1

 **network 192.168.1.0 0.0.0.255 area 1

**Interface tunnel1 // tunnel coniguration

**ip ospf network broadcast

**ip ospf priority 0
```

Figure 3.11: Spoke Configuration (OSPF).

3.5.4.3 RIP

RIP is a well-known and straightforward routing mechanism, it simply functionalizes the distance-vector algorithm, its routing criteria based on finding reachable hops and advertises them. It is a low overhead protocol, but it has a limitation and scalability issues. We disabled split-horizon on the Hub while using RIP as the routing protocol in DMVPN Phase 3 because, when split-horizon is enabled, the router is prevented from advertising the summary route, moreover, the routes between the hub and spoke will not be updated. The command of "auto-summary" is disabled to improve the efficiency of the routing process.

i. Hub Configuration

```
router rip   // router configuration
 *version 2
 *network 1.0.0.0
 *network 192.168.1.0
 *no auto-summary
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
*interface tunnel1
*no ip split-horizon
```

Figure 3.12: Hub Configuration (RIP).

ii. Spoke Configuration

```
**router rip

**version 2

**network 3.0.0.0

**network 192.168.1.0

**no auto-summary
```

Figure 3.13: Spoke Configuration (RIP).

3.6 TESTNG SCENARIOS

By running different routing protocols and applying several types of encryption techniques, eighteen different experiments were tested and conducted to evaluate the DMVPN network phase 3. Two main scenarios were applied using different data input (256 KB, 500KB) and a fixed bandwidth limit of 500 KB/S; in each experiment, all measurements of network parameters including jitter, packet loss, bandwidth, speed, and latency are collected and analyzed to determine the higher performance of encryption and routing protocol.

Table 3.3: Scenarios of experimentations.

	EIGRP	**OSPF**	**RIP**
AES	*	*	*
DES	*	*	*
3DES	*	*	*

3.7 EXPERIMENTS AND TESTING CRITERIA

Nine laboratories and eighteen tests were implemented and executed in the GNS3 simulator, with each lab utilizing the identical DMVPN architecture and exact environment setting. The Iperf2 utility sets and measures input parameters and output performance indicators.

3.7.1 Input Data

i. ICMP is an echo command utilized to determine latency time by sending and receiving data packets between two IP nodes.
ii. Bandwidth is the largest amount of network traffic that can be sent in a determined piece of time.
iii. Data traffic is the amount of TCP or UDP traffic in the network.

3.7.2 Output Data

i. The maximum amount of measured traffic in Mbit/s is known as throughput.
ii. Jitter: is the time difference between packet arrivals.
iii. The speed of data transmission is defined as the time required to transfer data traffic from one source to another destination.
iv. Latency is the time it takes for packets to travel from source to destination.
v. Packet loss is the percentage amount of dropped packets when moving from source to destination.

The below table (Table 3.4) shows the input and output parameters.

Table 3.4: Input and Output Parameter.

Input (UDP Traffic)	Output
Data amount (256 KB, 500 KB)	Throughput, Jitter, Packet loss, Speed
Bandwidth (500 KB/S)	
ICMP	Latency

3.8 DATA COLLECTION

As illustrated in the figure (Figure 3.1), PC2 is a server, while all other PCs are clients. Iperf tool is used to send commands to transfer data from servers to clients. All experiments employ the multiclient mode to assure output consistency. After preparing the DMVPN network and choosing

routing protocol with the targeted encryption algorithm, it started to run the Iperf tool on the server-side, by opening the Ubuntu terminal and executing the command "iperf -s -u -P 4". On the client-side, different attributes are used that contains the amount of data, the maximum throughput, and the server IP to start the connection with the server node. The following attributes: "iperf -c 3.0.0.10 -V -u -b 500k -n 500k" are sent to the server in each experiment. The server sends packets to the clients. All output data are calculated by taking the average from the server and spoke nodes, "Average amount = Data/number of SPs to determine the performance of the entire network." The MTR tool was used to determine the latency. Refer to the table (Table 3.5)

The average of thirty maximum round trip times was calculated using the formula "Average = sum of 30 maximum time/number of data packets".

Table 3.5: Input and Output Command.

Traffic Type	**Input Command**
UDP (Server)	iperf -s -u -P 4
UDP (Client)	iperf -c 3.0.0.10 -V -u -b 500k -n 500k iperf -c 3.0.0.10 -V -u -b 500k -n 256k
ICMP (Client)	Ping 3.0.0.1 or MTR 3.0.0.1

4. RESULTS AND DISCUSSION

output parameters, multiple encryption techniques, various protocols, and various data inputs were analyzed and discussed. Each output parameter has two charts; the charts represent various data input of (256KB, 500KB) and fixed bandwidth of (500KB/S). The first figure depicts data with a size of 500KB, while the second chart depicts data with a size of 256KB.

i. Throughput

Due to the packet encryption and decryption inherent in all encryption techniques, network throughput is severely degraded. As shown in figure (Figure 4.1(A)), the chart illustrates the various throughput outputs taken when three distinct encryption algorithms are implemented. Using the AES algorithm shows the lowest throughput performance of the RIP protocol; however, the EIGRP shows the highest throughput output when using both the AES and the DES encryption algorithms. EIGRP protocol also has the highest throughput value when using the 3DES encryption algorithm; however, the RIP protocol has the lowest average throughput value when using the 3DES encryption algorithm.

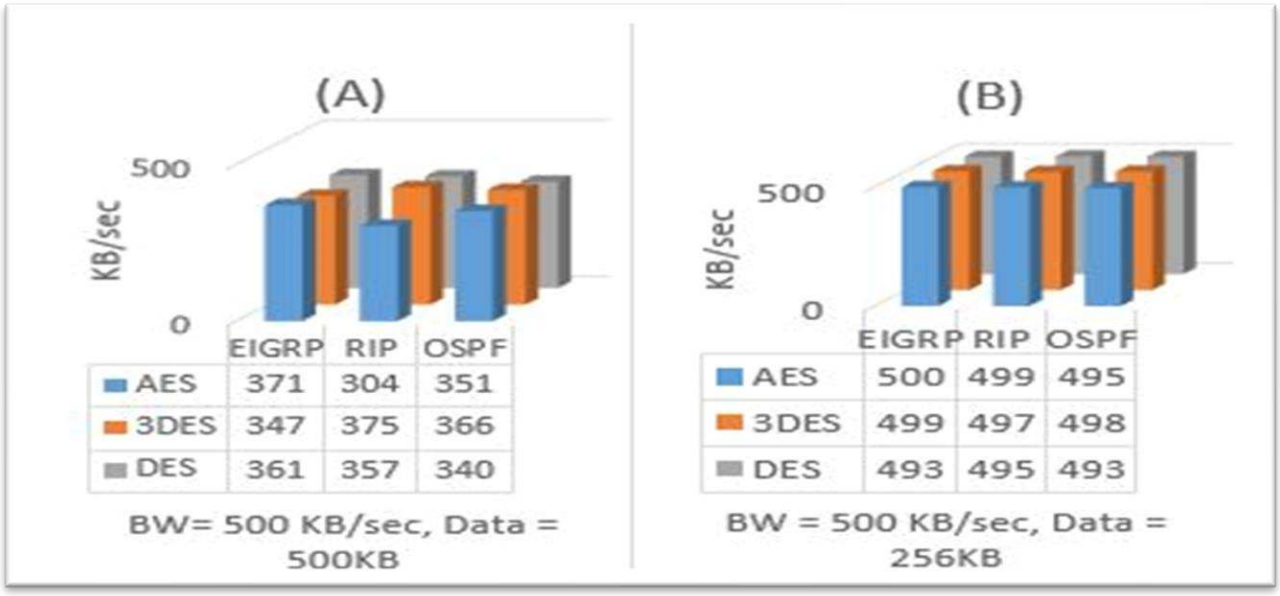

Figure 4.1: Throughput.

It can be seen in the figure (Figure 4.1(B)) that results of throughput values for all protocols with data amount of 256 KB shows higher performance than the input data of 500KB. By focusing on data input of 500KB, it can be seen that RIP/ 3DES and EIGRP/AES, both combinations of protocols reveal the greatest value among all other protocols. On the other hand, RIP/AES and OSPF/DES show the worst throughput values.

ii. Jitter

The figure (Figure 4.2(A)) illustrates that when data input streamed is higher the jitter values increase, but it can be seen that the DES algorithm had higher jitter values compared with other protocols, and the greatest jitter value is owned by RIP/AES which indicates a bad performance of RIP/AES protocols. On the other hand, the best jitter output is owned by EIGRP/AES by a value of 27.6 ms, which indicates good performance.

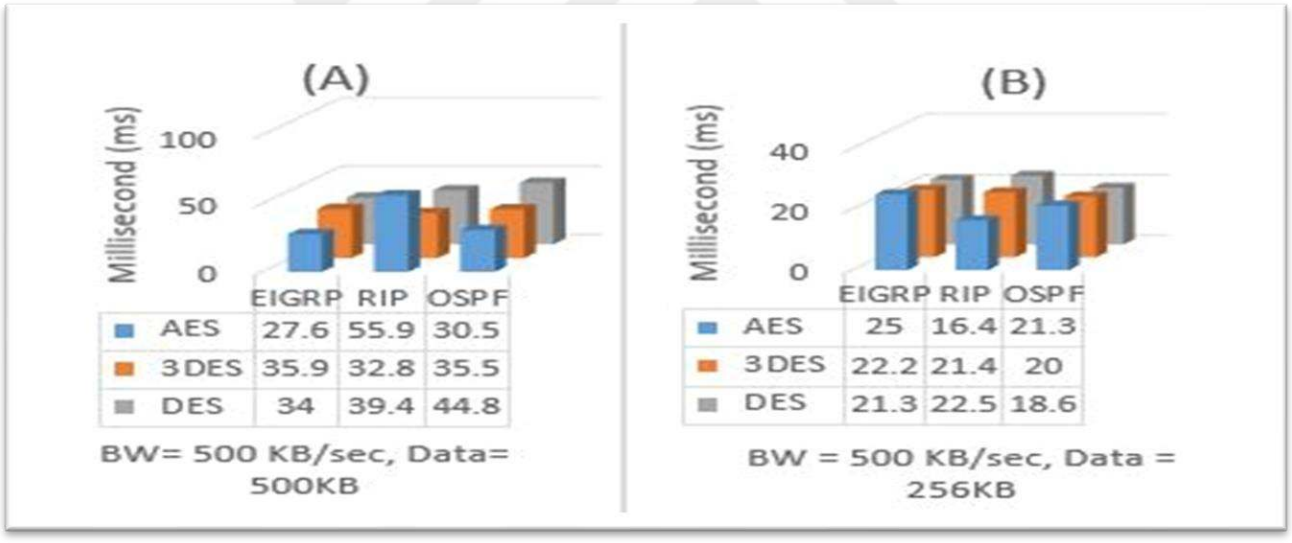

Figure 4.2: Jitter.

As shown in the figure (Figure 4.2(B)), all jitter values are relatively close, output values significantly decreased due to the reduced amount of input data, unlike Figure 4.2(A), the RIP/AES protocols reveals the best jitter values when data input is lesser.

iii. Packet Loss

In the figure (Figure 4.3(B)), the bars demonstrated that using input data of 256 KB and bandwidth limit of 500 KB/s can perform a good network performance, no datagram dropped, all protocols

with all encryption techniques are at the same level of output results. On the other hand, as illustrated in the figure (Figure 4.3(A)), data input is increased to double, more traffic is generated which caused packet loss, all datagram dropped are relatively close, but the worst value is owned by RIP/AES by a percentage of 38.3%, while the reasonable values are owned by EIGRP/AES followed by OSPF/RIP/3DES.

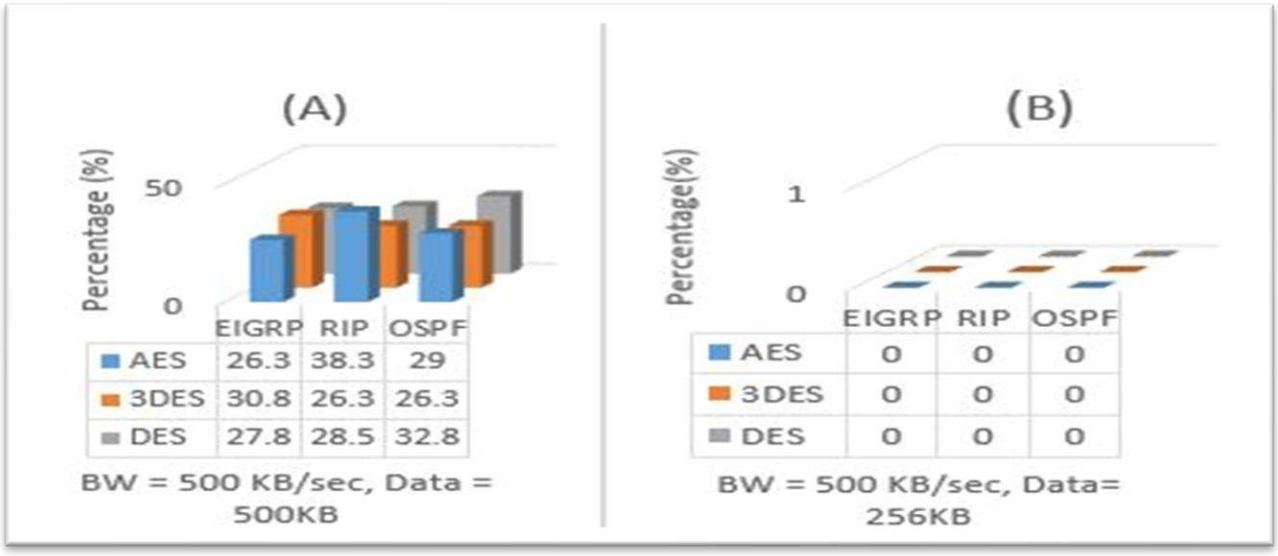

Figure 4.3: Packet loss**.**

iv. Speed

As shown in the figure (Figure 4.4(A)), the data transmission speed between the source and the destination was measured in seconds. The bandwidth is fixed to 500 KB/sec, while the amount of data streamed is 500 KB, it can be seen that combining RIP protocol with DES encryption leads to the slowest time to transfer data between two destinations, while with 3DES encryption spent shorter time. On the other hand, EIGRP and OSPF showed relative measurements with all encryption protocols except OSPF with DES, which revealed the most enhanced data transfer time.

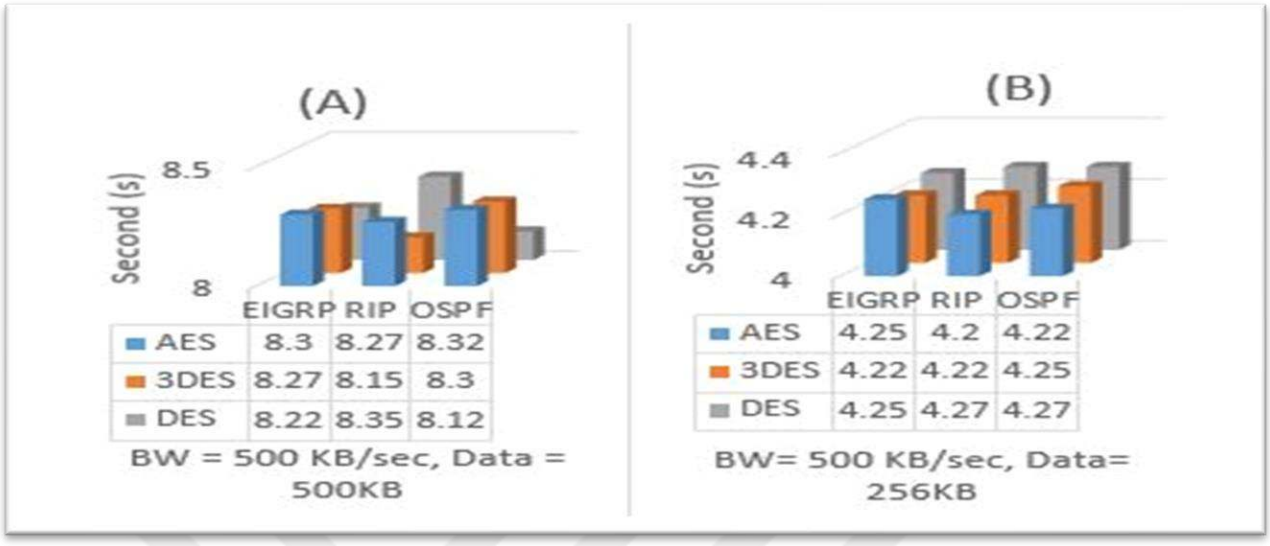

Figure 4.4: Speed.

As illustrated in figure (Figure 4.3) shows that the time taken to transmit data has decreased significantly and has reached nearly half of its previous level compared to the data provided in the figure (Figure 4.4), due to the amount of data decreased to the half. However, the figure revealed that all routing protocols showed very relative results; except OSPF/EIGRP, when configured with DES encryption, it is revealed that the speed scored the longest time between source and destination.

A. Latency

According to the figure (Figure 4.5), the different average values of time measured during ICMP testing are depicted in a bar chart format. The EIGRP and OSPF protocols, as shown in figure (Figure 4.5), have the best latency values when the AES algorithm is used, whereas all protocols have the worst latency values when the DES algorithm is used. On the other hand. OSPF/DES shows the worst value compared to all other protocols, while EIGRP/AES reveals the best latency time. It can be said that AES and 3DES show better latency performance than DES.

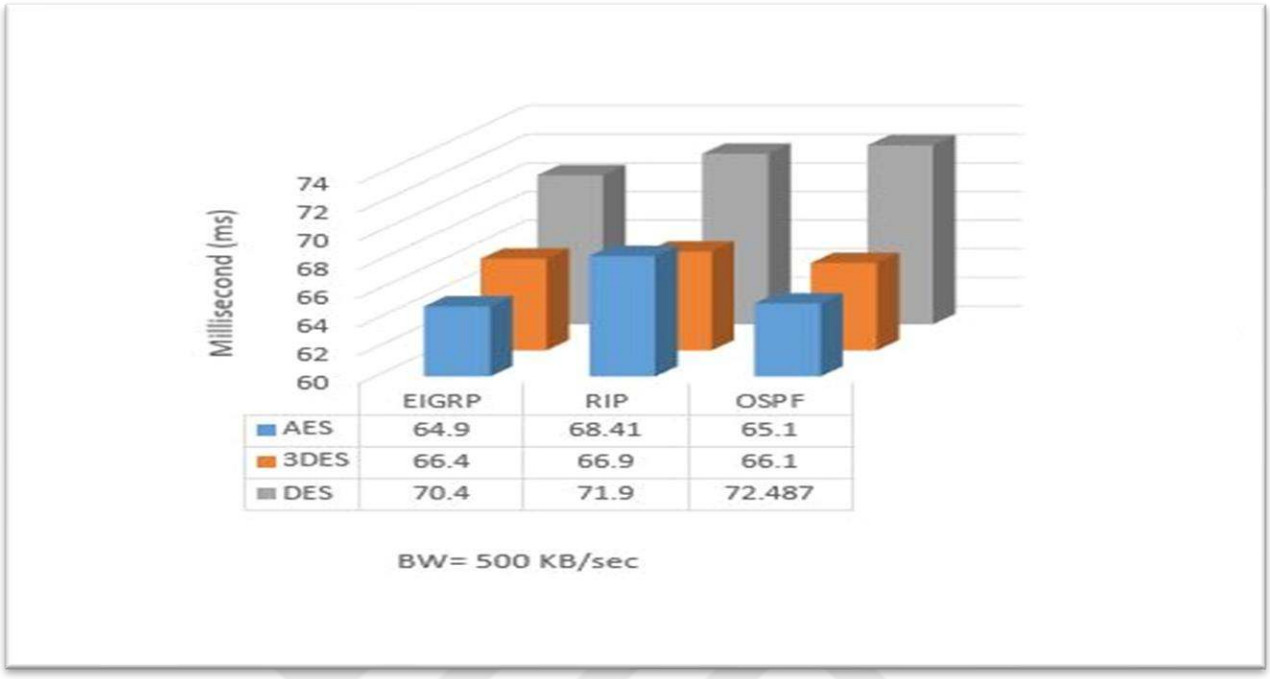

Figure 4.5: Latency.

5. CONCLUSION AND FUTURE WORK

DMVPN technology is one of Cisco's most popular and frequently used solutions, and it's used to connect remote sites and branches more securely and straightforwardly than old techniques. A number of routing algorithms and encryption mechanisms are used to keep the DMVPN network working at peak performance. Many studies were conducted to evaluate and optimize the influence of encryption algorithms and routing protocols on DMVPN performance. A variety of scenarios were tested and analyzed in order to establish the optimal couple of protocols that may improve and enhance the DMVPN's functionality. Many network KPIs are measured such as speed, throughput, latency, and packet loss to determine the behavior of encryption techniques and routing protocol that lead to higher DMVPN performance. Different amounts of UDP input data are streamed (256KB, 500KB) with a fixed amount of bandwidth (500KB/S) using the Iperf measurement tool. All captured data are analyzed and presented in bar charts. The following are the outcomes:

i. Streaming data input size of 256 KB has a significant effect on data transfer time, which is transferred more quickly between IP nodes, and the combination of RIP and AES provides the best performance.
ii. Increasing data input to 500 KB reveals different behavior of EIGRP/AES and RIP/3DES which achieve higher throughput values of 371 kbps and 375 kbps, respectively, compared to OSPF.
iii. EIGRP/AES owned the minimum jitter value of 27.6 ms among all other protocols.
iv. EIGRP/AES achieves the best packet loss performance of 26.3 %, indicating superior DMVPN network quality than other protocols and encryption schemes.
v. OSPF/DES has the fastest data transmission rate of 8.12 seconds, followed by RIP/3DES at 8.15 seconds.
vi. The output parameters reveal higher and undesirable values when the data input exceeds 500 KB.

Finally, It may be said that EIGRP/AES and RIP/3DES protocols perform better when data input is higher, whereas RIP/AES performs better when data input is lower. For further works, all the following can be investigated as further research:

i. Different IPsec attributes, such as integrity algorithms and IPsec modes, can be researched to determine how would a larger scaled DMVPN network performs.
ii. Dual hub redundancy network.
iii. Analysis of cyber-attacks and security exploits of the GRE tunneling.

REFERENCES

S. Bhattarai, “VPN research (Term Paper),” no. January, 2016, doi: 10.13140/RG.2.1.4215.8160.

H. M. Marah, J. R. Khalil, A. Elarabi, and M. Ilyas, “DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption,” *3rd Int. Conf. Electr. Commun. Comput. Eng. ICECCE 2021*, no. June, pp. 12–13, 2021, doi: 10.1109/ICECCE52056.2021.9514142.

J. Zhang, “Research on Key Technology of VPN Protocol Recognition,” *Proc. 2018 IEEE Int. Conf. Saf. Prod. Informatiz. IICSPI 2018*, pp. 161–164, 2019, doi: 10.1109/IICSPI.2018.8690472.

A. Alshalan, S. Pisharody, and D. Huang, “A Survey of Mobile VPN Technologies,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1177–1196, 2016, doi: 10.1109/COMST.2015.2496624.

E. Spengler, “Virtual Private Networks (VPNs) Simplified Agenda ƒ Demonstration ƒ Introduction to VPNs ƒ VPN Security (IPSec , PPTP , SSL) ƒ VPN Technology Comparison VPN Group Exercise,” pp. 1–37, 2008.

W. Meteorological and O. Wmo, *Guide to Virtual Private Networks via the Internet between WMO Information System Centres*, no. 1116. .

Z. Huachun, L. Ying, and G. Jianfeng, “The development research of IPSEC-VPN based on address-split-mapping mechanism,” *Proc. 2009 2nd IEEE Int. Conf. Broadband Netw. Multimed. Technol. IEEE IC-BNMT2009*, pp. 602–607, 2009, doi: 10.1109/ICBNMT.2009.5347846.

I. Journal, “Technical Overview of Virtual Private Networks (VPNs) Technical Overview of Virtual Private Networks (VPNs),” no. June, 2017, doi: 10.15373/22778179/JULY2013/32.

F. Hauser, M. Haberle, M. Schmidt, and M. Menth, “P4-IPsec: Site-to-Site and Host-to-Site VPN with IPsec in P4-Based SDN,” *IEEE Access*, vol. 8, pp. 139567–139586, 2020, doi: 10.1109/ACCESS.2020.3012738.

Z. Wu and M. Xiao, “Performance evaluation of VPN with different network topologies,” *2019 2nd Int. Conf. Electron. Technol. ICET 2019*, pp. 51–55, 2019, doi: 10.1109/ELTECH.2019.8839611.

S. Jahan, M. S. Rahman, and S. Saha, “Application specific tunneling protocol selection for Virtual Private Networks,” *Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017*, pp. 39–44, 2017, doi: 10.1109/NSysS.2017.7885799.

A. R. Alabbas, L. A. Hassnawi, M. Ilyas, H. Pervaiz, Q. H. Abbasi, and O. Bayat, “Performance enhancement of safety message communication via designing dynamic power control mechanisms in vehicular ad hoc networks,” *Comput. Intell.*, vol. 37, no. 3, pp. 1286–1308, 2021, doi: 10.1111/coin.12367.

“VPN authentication - IPSec tutorial guide, pre shared keys and digital signatures.” http://www.internet-computer-security.com/VPN-Guide/Authentication.html (accessed Nov. 11, 2021).

H. H. Al-Khshali, M. Ilyas, and O. N. Ucan, “Effect of PE File Header Features on Accuracy,” *2020 IEEE Symp. Ser. Comput. Intell. SSCI 2020*, pp. 1115–1120, 2020, doi: 10.1109/SSCI47803.2020.9308507.

I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, “Design and Implementation of UDP Tunneling-based on OpenSSH VPN,” *Proc. - IEEE 2018 Int. Conf. Adv. Comput. Commun. Control Networking, ICACCCN 2018*, no. 1, pp. 640–645, 2018, doi: 10.1109/ICACCCN.2018.8748849.

D. El Idrissi, N. Elkamoun, and R. Hilal, “Study of the impact of failure on GRE Tunnel,” *7th Mediterr. Congr. Telecommun. 2019, C. 2019*, pp. 1–4, 2019, doi: 10.1109/CMT.2019.8931368.

M. S. Dayananda and A. Kumar, “Architecture for inter-cloud services using IPsec VPN,” *Proc. - 2012 2nd Int. Conf. Adv. Comput. Commun. Technol. ACCT 2012*, pp. 463–467, 2012, doi: 10.1109/ACCT.2012.32.

Y. Niu, J. Li, and L. Li, “Research on authentication security of wireless local area network based

on L2TP protocol," *Proc. - 2009 IITA Int. Conf. Serv. Sci. Manag. Eng. SSME 2009*, pp. 491–494, 2009, doi: 10.1109/SSME.2009.30.

V. Jain and A. S. Gandhi, "An architecture for implementation of IEEE1588v2 over MPLS/MPLS-TP networks," *Proc. - 2014 4th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2014*, pp. 222–227, 2014, doi: 10.1109/CSNT.2014.51.

R. Zheng and W. Yang, "H-MPLS: A lightweight NFV-based MPLS solution in access network," *2014 IEEE 11th Consum. Commun. Netw. Conf. CCNC 2014*, no. Ccnc, pp. 887–892, 2014, doi: 10.1109/ccnc.2014.6994428.

A. Bahnasse, M. Talea, A. Badri, and F. E. Louhab, "New smart platform for automating MPLS virtual private network simulation," *Proc. - 2018 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2018*, pp. 1–8, 2018, doi: 10.1109/COMMNET.2018.8360268.

E. M. Gales and V. Croitoru, "Traffic Engineering and QoS in a Proposed MPLS-VPN," *2020 14th Int. Symp. Electron. Telecommun. ISETC 2020 - Conf. Proc.*, pp. 3–6, 2020, doi: 10.1109/ISETC50328.2020.9301135.

T. Tamanna and T. Fatema, "MPLS VPN over mGRE design and implementation for a service provider's network using GNS3 simulator," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2339–2342, 2018, doi: 10.1109/WiSPNET.2017.8300178.

T. Berger, "Analysis of current VPN technologies," *Proc. - First Int. Conf. Availability, Reliab. Secur. ARES 2006*, vol. 2006, pp. 108–115, 2006, doi: 10.1109/ARES.2006.30.

Y. Song, H. Li, L. Cheng, M. Xiang, and J. Cai, "SSL VPN resources log optimization techniques based on bloom filter algorithm," *Proc. 2016 IEEE Inf. Technol. Networking, Electron. Autom. Control Conf. ITNEC 2016*, pp. 733–736, 2016, doi: 10.1109/ITNEC.2016.7560458.

H. Mao, L. Zhu, and H. Qin, "A comparative research on SSL VPN and IPSec VPN," *2012 Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2012*, vol. 2012, pp. 0–3, 2012, doi: 10.1109/WiCOM.2012.6478270.

D. Rybin, K. Piliugina, and P. Piliugin, “Investigation of the applicability of SSL/TLS protocol for VPN in APCS,” *Proc. 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2018*, vol. 2018-Janua, pp. 1318–1321, 2018, doi: 10.1109/EIConRus.2018.8317339.

M. Al-Qaraghuli, S. Ahmed, and M. Ilyas, “Encrypted Vehicular Communication Using Wireless Controller Area Network,” *Iraqi J. Electr. Electron. Eng.*, vol. sceeer, no. 3d, pp. 17–24, 2020, doi: 10.37917/ijeee.sceeer.3rd.3.

A. B. Abdulhussein, A. K. Hadi, and M. Ilyas, “Design a tracing system for a seed supply chain based on blockchain,” *2020 3rd Int. Conf. Eng. Technol. its Appl. IICETA 2020*, pp. 209–214, 2020, doi: 10.1109/IICETA50496.2020.9318792.

Y. Zhou and K. Zhang, “DoS Vulnerability Verification of IPSec VPN,” *Proc. 2020 IEEE Int. Conf. Artif. Intell. Comput. Appl. ICAICA 2020*, pp. 698–702, 2020, doi: 10.1109/ICAICA50127.2020.9182437.

P. Miguel and S. Moniz, “Confidentiality , Integrity and Non-Repudiation in Smartgrids Confidentiality , Integrity and Non-Repudiation in Smartgrids,” 2011.

Z. Jiang and Y. Xie, “Study and implement of VPN penetrating NAT based on IPSec protocol,” *Proc. 2011 Int. Conf. Transp. Mech. Electr. Eng. TMEE 2011*, pp. 404–407, 2011, doi: 10.1109/TMEE.2011.6199228.

A. K. A. Al-Mashadani and M. Ilyas, “Distributed Denial of Service Attack Alleviated and Detected by Using Mininet and Software Defined Network,” *Webology*, vol. 19, no. 1, pp. 4129–4144, 2022, doi: 10.14704/web/v19i1/web19272.

H. Niazi, N. Shah, B. Zhou, and V. Sethi, “Group Encrypted Transport VPN (Get VPN) Design and Implementation Guide,” no. February 2010, pp. 1–220, 2010.

G. Wang, Y. Sun, Q. He, G. Xin, and B. Wang, “A content auditing method of IPsec VPN,” *Proc. - 2018 IEEE 3rd Int. Conf. Data Sci. Cyberspace, DSC 2018*, pp. 634–639, 2018, doi: 10.1109/DSC.2018.00101.

K. K. V. V. Singh and H. Gupta, “A new approach for the securityof VPN,” *ACM Int. Conf.*

Proceeding Ser., vol. 04-05-Marc, no. March 2016, 2016, doi: 10.1145/2905055.2905219.

D. Fang, P. Zeng, and W. Yang, "Attacking the IPsec standards when applied to IPv6 in confidentiality-only ESP tunnel mode," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 401–405, 2014, doi: 10.1109/ICACT.2014.6778990.

"INTERNET PROTOCOL SECURITY (IPSEC) I NT RO DU C I N G I PSE C – NE T WO R K LAYE R."

B. K. Chawla, O. P. Gupta, and B. K. Sawhney, "A Review on IPsec and SSL VPN," *Int. J. Sci. Eng. Res.*, vol. 5, no. 11, pp. 21–24, 2014.

A. V. Uskov, "Information security of IPsec-based mobile VPN: Authentication and encryption algorithms performance," *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012*, pp. 1042–1048, 2012, doi: 10.1109/TrustCom.2012.187.

R. Khelf and N. Ghoualmi-Zine, "A survey on dynamic multipoint virtual private networks," *CEUR Workshop Proc.*, vol. 2379, no. June 2019, pp. 15–24, 2018.

R. Jankuniene and I. Jankunaite, "Route creation influence on DMVPN QoS," *Proc. Int. Conf. Inf. Technol. Interfaces, ITI*, pp. 609–614, 2009, doi: 10.1109/ITI.2009.5196156.

T. Alam *et al.*, "Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol," *2018 Int. Conf. Innov. Sci. Eng. Technol. ICISET 2018*, no. November, pp. 367–371, 2018, doi: 10.1109/ICISET.2018.8745601.

H. Chen, "Design and implementation of secure enterprise network based on DMVPN," *BMEI 2011 - Proc. 2011 Int. Conf. Bus. Manag. Electron. Inf.*, vol. 1, pp. 506–511, 2011, doi: 10.1109/ICBMEI.2011.5916984.

I. Cisco Systems, "SCALABLE DMVPN DESIGN AND IMPLEMENTATION GUIDE." p. 143, 2007, [Online]. Available: http://www.cisco.com.

"Introduction to DMVPN." https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn (accessed May 15, 2021).

A. Bahnasse and N. El, “Study and Analysis of a Dynamic Routing Protocols’ Scalability over a Dynamic Multi-point Virtual Private Network,” *Int. J. Comput. Appl.*, vol. 123, no. 2, pp. 26–31, 2015, doi: 10.5120/ijca2015905249.

M. Rizal and S. U. Masruroh, “Evaluasi Kinerja Jaringan Dmvpn Menggunakan,” vol. 2, no. 3, pp. 143–150, 2018.

“IP Addressing: NHRP Configuration Guide, Cisco IOS XE Release 3S - Configuring NHRP [Support] - Cisco.” https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-3s/nhrp-xe-3s-book/config-nhrp.html (accessed May 15, 2021).

M. M. A. Alkadhmi, O. N. Uçan, and M. Ilyas, “An Efficient and Reliable Routing Method for Hybrid Mobile Ad Hoc Networks Using Deep Reinforcement Learning,” *Appl. Bionics Biomech.*, vol. 2020, 2020, doi: 10.1155/2020/8888904.

R. Khelf and N. Ghoualmi-Zine, “A survey on dynamic multipoint virtual private networks,” *CEUR Workshop Proc.*, vol. 2379, no. 1, pp. 15–24, 2018.

G. A. Tizazu, K. H. Kim, and A. B. Berhe, “Dynamic routing influence on secure enterprise network based on DMVPN,” *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, pp. 756–759, 2017, doi: 10.1109/ICUFN.2017.7993894.

M. Ilyas, “The Influence of Encryption Techniques and Dynamic Routing Protocols on DMVPN Network Performance,” vol. 128, no. October, pp. 27–28, 2021.

J. Deng, S. Wu, and K. Sun, “Comparison of RIP, OSPF and EIGRP Routing Protocols based on OPNET,” *http://www.sfu.ca/~sihengw/ENSC427_Group9/*, no. 06, p. 23, 2014, [Online]. Available: http://www.sfu.ca/~sihengw/ENSC427_Group9/%0Ahttp://www.sfu.ca/~sihengw/ENSC427_Group9/Final Report .pdf.

J. Ferdaus and R. Salihi, “Routing: Internet Routing Protocols and Algorithms,” no. September, pp. 0–19, 2015, doi: 10.13140/RG.2.1.4341.1680.

Y. Li, G. Zhao, T. Liu, and L. Du, “The research on cryptographical system of IPSEC VPN based

on combined symmetric key," *Proc. 2009 IEEE Int. Conf. Netw. Infrastruct. Digit. Content, IEEE IC-NIDC2009*, pp. 999–1003, 2009, doi: 10.1109/ICNIDC.2009.5360958.

F. A. Daud, R. Ab Rahman, M. Kassim, and A. Idris, "Performance of encryption techniques using dynamic virtual protocol network technology," *ICSET 2018 - 2018 IEEE 8th Int. Conf. Syst. Eng. Technol. Proc.*, no. October, pp. 29–34, 2019, doi: 10.1109/ICSEngT.2018.8606381.

Y. Yuan, Y. Yang, L. Wu, and X. Zhang, "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," *2018 IEEE Int. Conf. Electron Devices Solid State Circuits, EDSSC 2018*, pp. 4–5, 2018, doi: 10.1109/EDSSC.2018.8487056.

N. Floissac and Y. L'Hyver, "From AES-128 to AES-192 and AES-256, how to adapt differential fault analysis attacks on key expansion," *Proc. - 2011 Work. Fault Diagnosis Toler. Cryptogr. FDTC 2011*, pp. 43–53, 2011, doi: 10.1109/FDTC.2011.15.

C. H. Kim, "Differential fault analysis against AES-192 and AES-256 with minimal faults," *Fault Diagnosis Toler. Cryptogr. - Proc. 7th Int. Work. FDTC 2010*, pp. 3–9, 2010, doi: 10.1109/FDTC.2010.10.

O. A. Claret, "Overview of Cryptography," no. December, 2017, doi: 10.2139/ssrn.2741776.

A. Shamir, "How to Share a Secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

Y. Zhu, H. Zhang, and Y. Bao, "Study of the AES realization method on the reconfigurable hardware," *Proc. - 2013 Int. Conf. Comput. Sci. Appl. CSA 2013*, pp. 72–76, 2013, doi: 10.1109/CSA.2013.23.

F. R. Nuradha, S. D. Putra, Y. Kurniawan, and M. A. Rizqulloh, "Attack on AES Encryption Microcontroller Devices with Correlation Power Analysis," *Proceeding - 2019 Int. Symp. Electron. Smart Devices, ISESD 2019*, pp. 1–4, 2019, doi: 10.1109/ISESD.2019.8909447.

M. Singh and D. Garg, "Choosing Best Hashing Strategies and Hash Functions," *2009 IEEE Int. Adv. Comput. Conf. IACC 2009*, no. Iacc, pp. 50–55, 2009, doi: 10.1109/IADCC.2009.4808979.

A. Bahnasse and N. El, “Study and Analysis of a Dynamic Routing Protocols’ Scalability over a Dynamic Multi-point Virtual Private Network,” *Int. J. Comput. Appl.*, vol. 123, no. 2, pp. 26–31, 2015, doi: 10.5120/ijca2015905249.

S. U. Masruroh, K. H. P. Widya, A. Fiade, and I. R. Julia, “Performance Evaluation DMVPN Using Routing Protocol RIP, OSPF, and EIGRP,” *2018 6th Int. Conf. Cyber IT Serv. Manag. CITSM 2018*, no. Citsm, pp. 1–6, 2019, doi: 10.1109/CITSM.2018.8674051.

A. Bahnasse, F. E. Louhab, A. Khiat, A. Badri, M. Talea, and A. Sahel, “Dynamic Multipoint Virtual Private Network influence on Video Conferencing Quality of Service,” *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769447.