Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

Analysis of IPSec Implementation on Dynamic Multipoint VPN Protocol Using Routing Border Gateway Protocol

Muhammad Ali Said*, Setyorini, Erwid M Jadied

Informatics, School of Computing, Telkom University, Bandung, Indonesia
Email: [1,*]muhammadalisaid@student.telkomuniversity.ac.id, [2]setyorini@telkomuniversity.ac.id,[3]jadied@telkomuniversity.ac.id
Correspondence Author Email: muhammadalisaid@student.telkomuniversity.ac.id
Submitted:**08/07/2022**; Accepted:**27/07/2022**; Published**: 30/09/2022**

Abstract−Dynamic Multipoint Virtual Private Network (DMVPN) technology is one of Cisco's solutions to overcome the limitations of VPN scalability. DMVPN has a combination of components: Next hop resolution protocol (NHRP), Multipoint Generic Routing Encapsulation (mGRE) and Routing protocol. This research implements a simple network consisting of Hub, Spoke1, Spoke2, Lan1, Lan2 and Lan3 using the GNS3 simulator. This study compares the performance of IPSec and without IPsec on DMVPN using the BGP Routing protocol on performance parameters namely delay, throughput, jitter and packet loss to evaluate the security impact of the DMVPN network. The results of this study indicate that IPSec DMVPN has an effect on sending UDP packets which have a throughput value without IPSec of 5082.18 kbit/s while IPSec's throughput is 5034.40 kbit/s. The value of packet loss without IPSec has a value of 7.54% while IPSec has a value of 4.79%. The results of the jitter value have the same value. The delay value without IPSec has a value of 0.183s while the IPSec delay value is 0.410s. TCP packet delivery has a throughput value without IPSec is 1139.16 kbit/s while the IPSec throughput value is 1105.20 kbit/s. The results of the packet loss value and the jitter value have the same value. The delay value without IPSec has a value of 0.185s while the IPSec delay value is 0.187s.

Keywords: DMVPN; VPN; BGP Routing; IPSec; Network Performance

1. INTRODUCTION

Virtual Private Network (VPN) technology using IPSec is a common solution applied to maintain confidentiality, integrity, and availability on the network. VPN technology has weaknesses in implementation configuration time and has high latency. The cause of the high latency is the increase in traffic load on the main Hub. VPN also has a reduction in packet routing overhead caused by high traffic from the client to the hub, resulting in higher network performance and even reduced network power consumption [1], [2].

To overcome the limitations of VPN, the company Cisco introduced the Dynamic Multipoint Virtual Private Network (DMVPN). DMVPN is a routing modeling technique that uses a mesh network topology on a hub (Server) that is connected between spoke (Client) routers that are connected and allows traffic between spoke routers to be sent without going through the hub. In addition, DMVPN does not need to reconfigure the location of the new client connected to the hub and has broad scalability compared to VPN [1][2][3][4].

DMVPN has a dynamic routing protocol that is used to manipulate routing packet updates on spokes and hubs. The types of dynamic routing used include RIP, OSPF, EIGRP, IS – IS, and BGP [1], [3]. In this study, the BGP routing protocol is used which can be used with a high scalability range and is suitable for use on the DMVPN protocol which has wide scalability [5]. Encryption of traffic between hubs is important to protect the system from cyber criminals. The use of the right encryption algorithm is important because it will be directly proportional to the performance of network communication. IPSec is an encapsulation method used to secure traffic between clients. To build and protect a DMVPN network, a basic IPsec configuration with mGRE and NHRP must be implemented at each node to ensure a basic level of confidentiality and integrity to establish protection on the DMVPN network[1], [6][7][8].

In a previous study by Hasan Mohamed Marah [1], the performance analysis of the DMVPN network on dynamic routing protocols and IPSec on OSPF routing was successfully carried out. The results of the study illustrate that phase 2 has better results than phase 1, in phase 2 OSPF routing without security implementation shows higher performance and has the best throughput value of 7.04 Mbits/sec, with the lowest jitter value of 18.243 ms and shows the lowest latency value is 100,983 ms. The implementation of IPsec in phase 2 reduces the throughput of OSPF up to 62.642%. In phase 2, EIGRP showed the highest jitter of 26,775 ms, and RIPv2 showed the highest latency of 120,741 ms .

In research by Siti Ummi Masruroh [3], an analysis of the performance of DMVPN on the RIP, OSPF, and EIGRP routing protocols has been carried out using the main phases of DMVPN. The results of this study were conducted to compare the performance of DMVPN from three routing protocols using RIP, OSPF, and EIGRP using GNS3. The parameters used in this study are throughput, jitter, and packet loss. The purpose of this paper is to show that DMVPN RIP phase 2 has the highest throughput value. Then DMVPN phase 2 EIGRP has the best jitter value. And the DMVPN 3 RIP phase has the highest packet loss value. And the DMVPN 3 phase total has the lowest value among other simulations.

The results of research from Nanda Iryani [10] regarding the Implementation of Dynamic Multipoint Virtual Private Network Dual Hub by applying the High Availability concept show that the test scenario using dual Hub gets the best value from all Quality of Service parameters using EIGRP routing with spoke to spoke communication design.

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

Communication design speaks superior to design models that use OSPF routing. The Quality of Service parameter has a very good value, such as the throughput value of 3,324.774 kbps, jitter 2.16 ms, and packet loss which is only 0.01% while the delay value is 255.02 ms is the standard category. The results of the second test scenario are using one hub using EIGRP and OSPF routing to get the same inhibiting results. The delay value has the best value, which is 408.64 ms when using EIGRP. This value belongs to the medium category, for the throughput value is 3,114,231 kbps, the jitter is 2.30 ms and the packet loss is 0.01% classified as a very good category.

Angelescu's research [2] conducted a DMVPN simulation on the GNS3 network simulation software, in this study a DMVPN simulation on GNS3 to compare VPN performance. The result of this study is that DMVPN has broad scalability compared to VPN.

The problem raised in this study is to determine the impact of IPSec on the DMVPN protocol on the Quality of service in BGP Routing with performance parameters of delay, throughput, jitter, and packet loss. The test parameters in this study consist of throughput to measure the bit rate per second (BPS) with the total number of packet arrivals observed within a certain destination time interval, delay (latency) to determine the time it takes data to travel a certain distance from sender to receiver, jitter the number of delay and packet loss variances to show the parameters of the number of packets lost in sending packets to the destination[11][12][13][14][15].In this study, we will compare the analysis of IPSec and without IPSec on DMVPN using the BGP Routing Protocol. The implementation of this study uses the GNS3 simulator application to perform network design, network configuration, and testing of network performance using D-ITG tools. The purpose of this study is to model IPSec on a special DMVPN using the BGP Routing protocol, and analyze the performance of IPSec and without IPsec on a DMVPN using the BGP protocol on performance parameters such as delay, throughput, jitter and packet loss.

2. RESEARCH METHODOLOGY

2.1 Research Stages.

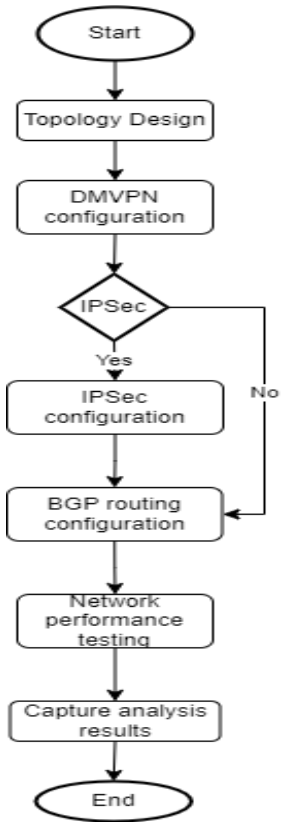

Figure 1. Modeling System

The network system design scheme to be built is to combine the DMVPN protocol with BGP and IPsec routing. In addition, in this design uses D-ITG software to determine network performance such as delay, throughput, jitter, and packet loss. In designing this system model using the GNS3 simulator with the features used in modeling this system, namely Cisco 7200, Ubuntu 20, and D-ITG Routers. The steps in modeling this system are first to design the topology which will be designed through the GNS3 simulator after doing the design then to configure NHRP and mGRE in each tunnel. Then after configuring NHRP and mGRE, the next step is to configure IPSec and BGP Routing on network devices (hub and spoke). Then after completing all the configurations, the next stage is to test network performance using D-ITG and the last stage is to capture the results from the D-ITG test. In Figure 1 is a modeling system that will be made in this study.

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

2.2 Software and Hardware Specifications

Some of the software used in this study uses the Windows 10 operating system, for the simulator application using GNS3, besides that it also uses a virtual box that functions to install the Ubuntu operating system for clients and uses Cisco routers for hubs, ISPs, and spokes. The hardware used in this research is Intel Core i7, 8GB Ram, and 250GB SSD. Software and hardware in using the GNS3 simulator have minimum requirements, namely the Windows 7 operating system, 2 64-bit logical core processors, 4GB of RAM, and 1GB of memory. In addition, the recommended specifications are Windows 7 and above, 4 logical core processors, 8GB RAM and memory using SSD.

2.3 Topology Design

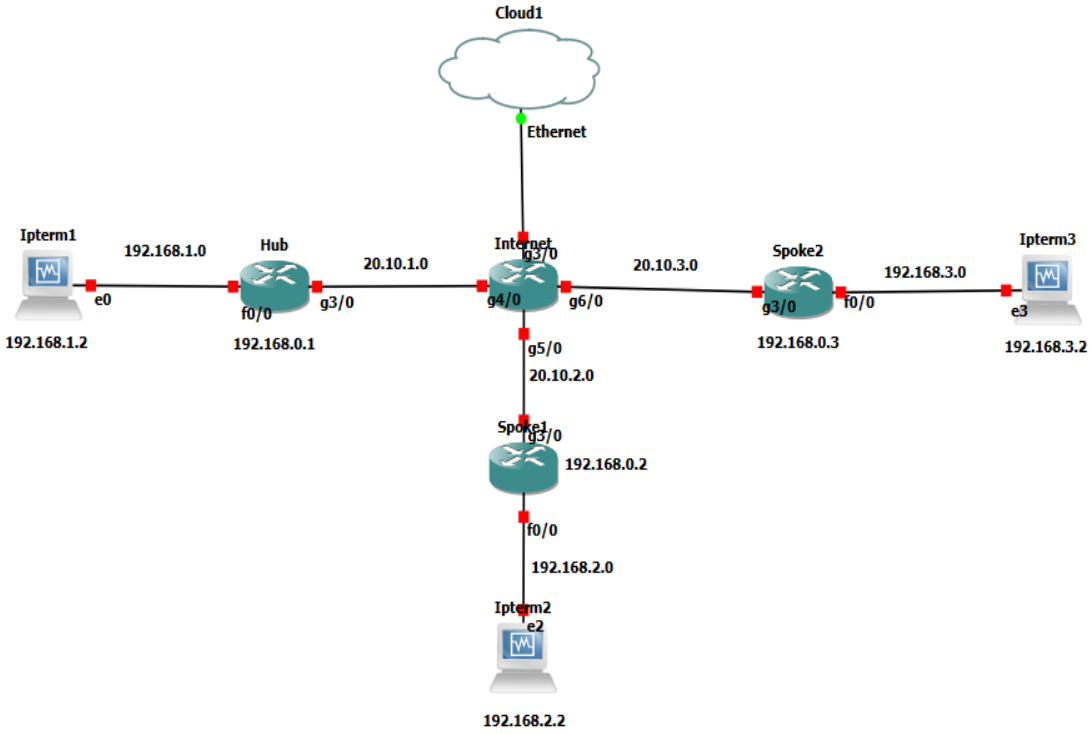

Figure 2. Topology Design

The justification for this topology design is using a mesh topology, which is a form of computer network that is connected. In this topology design, it is designed to use one hub (server) and two spokes (client) because it is a minimum requirement to test network performance on the DMVPN protocol, it must have one hub as a server and two spokes as a client.

Things that must be prepared in designing the topology in the GNS3 simulator are preparing a Cisco 7200 router image which can be downloaded on the GNS3 website, the Cisco 7200 router is used for Hub, ISP, and Spoke devices. In addition, it also prepares a virtual box that is used to install the Ubuntu operating system which functions as a network performance analysis (client). The implementation of IPSec in this topology design is found in hub devices and spoke1 and spoke2 devices. In Figure 2 is the topology design that will be made in this study.

2.4 IP Address Configuration

The IP address below consists of the ISP Interface, HUB, Spoke, and Ipterm. In the IP Address below, the hub uses AS 65001, and Spoke uses AS 65002 and 65003. The table 1 below describes the IP addresses used on each interface. Table 1 is the IP Address that will be used in this study.

Table 1. IP Address

Interface	Tunnel	NBMA	IP LAN
ISP	-	20.10.1.1	-
ISP	-	20.10.2.1	-
ISP	-	20.10.3.1	-
HUB AS 65001	192.168.0.1	20.10.1.2	192.168.1.1
HUB AS 65002	192.168.0.2	20.10.2.2	192.168.2.1
HUB AS	192.168.0.3	20.10.3.2	192.168.3.1

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

65003			
Ipterm1	-	-	192.168.1.2
Ipterm2	-	-	192.168.2.2
Ipterm3	-	-	192.168.3.2

2.5 Scenario

The test scenario consists of two main tests carried out in this final project, namely the results of the output delay, throughput, jitter, and packet loss of the BGP protocol on DMVPN without IPsec and the evaluation of BGP performance with IPSec tunnel on DMVPN.

3. RESULTS AND DISCUSSION

3.1 DMVPN Configuration

The steps in configuring a dynamic multipoint virtual private network are as follows:

a. The first step is setting the IP address on the hub, spoke1, spoke2, and internet router according to table 1. In figure 3 the results of the configuration of the IP address of the hub, figure 4 the results of the configuration of the IP address of the internet router, the figure 5 the results of the configuration of the IP address of spoke1, and the figure 6 the results of the configuration of the IP address of the spoke2.

```
Hub#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.1     YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/1            unassigned      YES NVRAM  administratively down down
FastEthernet2/0            unassigned      YES NVRAM  administratively down down
FastEthernet2/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         20.10.1.2       YES NVRAM  up                    up
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet5/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet6/0         unassigned      YES NVRAM  administratively down down
```

Figure 3. The result of configuring the hub's IP address

```
Internet#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/1            unassigned      YES NVRAM  administratively down down
FastEthernet2/0            unassigned      YES NVRAM  administratively down down
FastEthernet2/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         192.168.50.140  YES DHCP   up                    up
GigabitEthernet4/0         20.10.1.1       YES NVRAM  up                    up
GigabitEthernet5/0         20.10.2.1       YES NVRAM  up                    up
GigabitEthernet6/0         20.10.3.1       YES NVRAM  up                    up
```

Figure 4. The result of the internet router IP address configuration

```
Spoke1#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.2.1     YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/1            unassigned      YES NVRAM  administratively down down
FastEthernet2/0            unassigned      YES NVRAM  administratively down down
FastEthernet2/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         20.10.2.2       YES NVRAM  up                    up
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet5/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet6/0         unassigned      YES NVRAM  administratively down down
```

Figure 5. Result of IP address configuration spoke1

```
Spoke2#sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.3.1     YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
FastEthernet1/1            unassigned      YES NVRAM  administratively down down
FastEthernet2/0            unassigned      YES NVRAM  administratively down down
FastEthernet2/1            unassigned      YES NVRAM  administratively down down
GigabitEthernet3/0         20.10.3.2       YES NVRAM  up                    up
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet5/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet6/0         unassigned      YES NVRAM  administratively down down
```

Figure 6. Result of IP address configuration spoke2

b. The second step is to configure the tunnels on the hub, spoke1, and spoke2. The tunnel configuration consists of mGRE and NHRP configurations. in the figure 7 the results of the tunnel hub configuration, the figure 8 the results of the spoke1 tunnel configuration, and the figure 9 the results of the spoke2 tunnel configuration.

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

```
Hub#sh run int tunnel0
Building configuration...

Current configuration : 262 bytes
!
interface Tunnel0
 ip address 192.168.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication DMVPN
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet3/0
 tunnel mode gre multipoint
end
```

Figure 7. Results of the tunnel hub configuration

```
Spoke1#sh run int tunnel0
Building configuration...

Current configuration : 355 bytes
!
interface Tunnel0
 ip address 192.168.0.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication DMVPN
 ip nhrp map multicast dynamic
 ip nhrp map 192.168.0.1 20.10.1.2
 ip nhrp map multicast 20.10.1.2
 ip nhrp network-id 1
 ip nhrp nhs 192.168.0.1
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet3/0
 tunnel mode gre multipoint
end
```

Figure 8. Results of the spoke1 tunnel configuration

```
Spoke2#sh run int tunnel0
Building configuration...

Current configuration : 355 bytes
!
interface Tunnel0
 ip address 192.168.0.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication DMVPN
 ip nhrp map multicast dynamic
 ip nhrp map 192.168.0.1 20.10.1.2
 ip nhrp map multicast 20.10.1.2
 ip nhrp network-id 1
 ip nhrp nhs 192.168.0.1
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet3/0
 tunnel mode gre multipoint
end
```

Figure 9. Results of the spoke2 tunnel configuration

c. Next shows the DMVPN that is connected to each tunnel, as shown in Figure 10 shows the results of the IP NBMA and IP tunnel from the hub. Figure 11 shows the results of IP NBMA and IP tunnel from spoke1 and figure 12 shows the results of IP NBMA and IP tunnel from spoke2.

```
Hub#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
======================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 20.10.2.2           192.168.0.2    UP 00:07:27     D
     1 20.10.3.2           192.168.0.3    UP 00:07:30     D
```

Figure 10. The results of the IP NBMA and IP tunnel from the hub

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

```
Spoke1#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 20.10.1.2           192.168.0.1    UP 00:08:58     S
```

Figure 11. The results of IP NBMA and IP tunnel from spoke1

```
Spoke2#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 20.10.1.2           192.168.0.1    UP 00:08:33     S
```

Figure 12. The results of IP NBMA and IP tunnel from spoke2

d. It then displays the IP NHRP connected to each tunnel. Figure 13 shows the IP NHRP results from the hub, Figure 14 shows the IP NHRP results from spoke1, and Figure 15 shows the IP NHRP results from spoke2.

```
Hub#sh ip nhrp
192.168.0.2/32 via 192.168.0.2
   Tunnel0 created 00:10:00, expire 01:50:00
   Type: dynamic, Flags: unique registered nhop
   NBMA address: 20.10.2.2
192.168.0.3/32 via 192.168.0.3
   Tunnel0 created 00:10:03, expire 01:49:56
   Type: dynamic, Flags: unique registered nhop
   NBMA address: 20.10.3.2
```

Figure 13. The IP NHRP results from the hub

```
Spoke1#sh ip nhrp
192.168.0.1/32 via 192.168.0.1
   Tunnel0 created 00:11:49, never expire
   Type: static, Flags: used
   NBMA address: 20.10.1.2
```

Figure 14. The IP NHRP results from the spoke1

```
Spoke2#sh ip nhrp
192.168.0.1/32 via 192.168.0.1
   Tunnel0 created 00:11:01, never expire
   Type: static, Flags: used
   NBMA address: 20.10.1.2
```

Figure 15. The IP NHRP results from the spoke2

e. Add clients without having to configure from scratch on the hub, and it doesn't take long to configure. Figure 16 is the configuration result from the client (new spokes) to the hub and the configuration and results of adding clients (new spokes).

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

```
HUB#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 20.10.2.2           192.168.0.2    UP 00:01:09     D
     1 20.10.3.2           192.168.0.3    UP 00:01:08     D
     1 20.10.4.2           192.168.0.4    UP 00:01:09     D

HUB#sh nhrp
% Incomplete command.

HUB#sh ip nhrp
192.168.0.2/32 via 192.168.0.2
   Tunnel0 created 00:01:28, expire 01:58:31
   Type: dynamic, Flags: unique registered nhop
   NBMA address: 20.10.2.2
192.168.0.3/32 via 192.168.0.3
   Tunnel0 created 00:01:27, expire 01:58:32
   Type: dynamic, Flags: unique registered nhop
   NBMA address: 20.10.3.2
192.168.0.4/32 via 192.168.0.4
   Tunnel0 created 00:01:28, expire 01:58:31
   Type: dynamic, Flags: unique registered nhop
   NBMA address: 20.10.4.2
```

```
Spoke3#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 20.10.1.2           192.168.0.1    UP 00:00:52     S

Spoke3#sh run int tunnel0
Building configuration...

Current configuration : 355 bytes
!
interface Tunnel0
 ip address 192.168.0.4 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 192.168.0.1 20.10.1.2
 ip nhrp map multicast 20.10.1.2
 ip nhrp network-id 1
 ip nhrp nhs 192.168.0.1
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet3/0
 tunnel mode gre multipoint
end

Spoke3#sh ip nhrp
192.168.0.1/32 via 192.168.0.1
   Tunnel0 created 00:03:02, never expire
   Type: static, Flags: used
   NBMA address: 20.10.1.2
```

Figure 16. The result of the configuration of the addition of a new spoke

3.2 Routing BGP

The steps in configuring the border gateway protocol routing on a dynamic multipoint virtual private network are as follows:

a. The first step is to configure the IP address as in point 3.1 part a.
b. The second step is to configure a dynamic multipoint virtual private network like point 3.1.
c. Next, configure the BGP routing on the hub, spoke1, and spoke2. in the figure 17 is the BGP syntax of the hub, spoke1, and spoke2.

```
Hub
conf t
router bgp 65001
neighbor 20.10.1.1 remote-as 65001
network 20.10.1.0 mask 255.255.255.0
network 192.168.0.0 mask 255.255.255.0
network 192.168.1.0 mask 255.255.255.0
```

```
spoke1
conf t
router bgp 65002
neighbor 20.10.2.1 remote-as 65001
network 20.10.2.0 mask 255.255.255.0
network 192.168.0.0 mask 255.255.255.0
network 192.168.2.0 mask 255.255.255.0
```

```
spoke2
conf t
router bgp 65003
neighbor 20.10.3.1 remote-as 65001
network 20.10.3.0 mask 255.255.255.0
network 192.168.0.0 mask 255.255.255.0
network 192.168.3.0 mask 255.255.255.0
```

Figure 17. the BGP syntax of the hub, spoke1, and spoke2

Figure 17 explains that area 65001 is an autonomous system from the hub, for routing paths through the internet with IP 20.10.1.1 with autonomous system 65001, for the network address itself we register the network from the NHRP hub network, network tunnel hub, and connected network to perform testing. Figure 17 explains that area 65002 is an autonomous system from spoke1, for routing paths through the internet with IP 20.10.2.1 with autonomous system 65001, for the network address itself we register the network from the NHRP network spoke1, the tunnel network spoke1, and the connected network to perform the test. Figure 17 explains that area 65003 is an autonomous system from spoke1, for routing paths through the internet with IP 20.10.3.1 with autonomous system 65001, for the network address itself we register the network from the NHRP spoke2 network, the spoke2 tunnel network, and the connected network to perform the test.

d. In the figure 18 the results of routing BGP hub, spoke1 and spoke2.

```
      20.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B        20.10.2.0/24 [200/0] via 20.10.1.1, 00:16:24
B        20.10.3.0/24 [200/0] via 20.10.1.1, 00:16:24
B     192.168.2.0/24 [200/0] via 20.10.2.2, 00:15:59
B     192.168.3.0/24 [200/0] via 20.10.3.2, 00:15:59

      20.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B        20.10.1.0/24 [20/0] via 20.10.2.1, 00:17:17
B        20.10.3.0/24 [20/0] via 20.10.2.1, 00:17:17
B     192.168.1.0/24 [20/0] via 20.10.2.1, 00:17:17
B     192.168.3.0/24 [20/0] via 20.10.2.1, 00:16:46

      20.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B        20.10.1.0/24 [20/0] via 20.10.3.1, 00:16:33
B        20.10.2.0/24 [20/0] via 20.10.3.1, 00:16:33
B     192.168.1.0/24 [20/0] via 20.10.3.1, 00:16:33
B     192.168.2.0/24 [20/0] via 20.10.3.1, 00:16:02
```

Figure 18. Result of routing BGP hub, spoke1 and spoke2

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

3.3 IPSec configuration

The steps for IPSec configuration on a dynamic multipoint virtual private network are as follows:

a. The first step is to configure the IP address as in point 3.1 part a.
b. The second step is to configure a dynamic multipoint virtual private network like point 3.1.
c. The third step is to configure the border gateway protocol routing as in point 3.2.
d. Next, configure IPsec on the tunnel hub, spoke1, and spoke2. In the figure 19 is the IPSec syntax of the hub, spoke1, and spoke2.

```
crypto isakmp policy 1
encr aes
authentication pre-share
group 5
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac
crypto ipsec profile dmvpn-protect
set transform-set myset
```

Figure 19. The IPSec syntax of the hub, spoke1, and spoke2

Figure 19 describes the IPSec configuration, the first step that is configured for IPSec is to perform crypto ISAKMP (Internet Security Association and Key Management Protocol) policy 1 which is a security protocol, then perform AES encryption, which is an encryption algorithm to encode messages into a form that cannot be read. Then for pre-shared authentication, which functions as key authentication for third parties. The IPsec transform is to do a combination of esp, SHA, and HMAC, then configure IPsec on each tunnel profile.

e. Then displays the IPSec results on the hub, spoke 1, and spoke 2. Figure 20 IPSec hub results, 21 IPSec spoke1 results, and 22 IPSec spoke2 results.

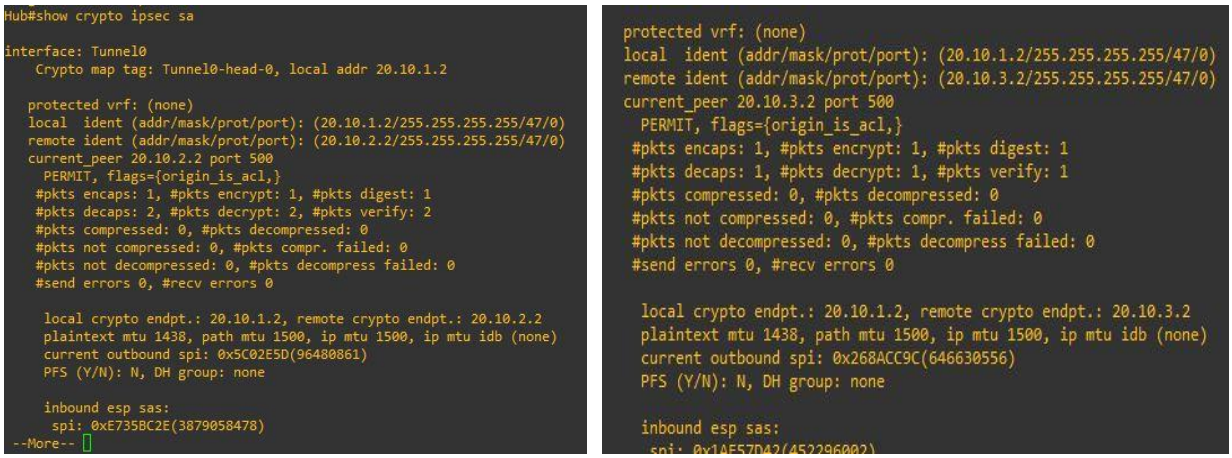

Figure 20. IPsec hub results

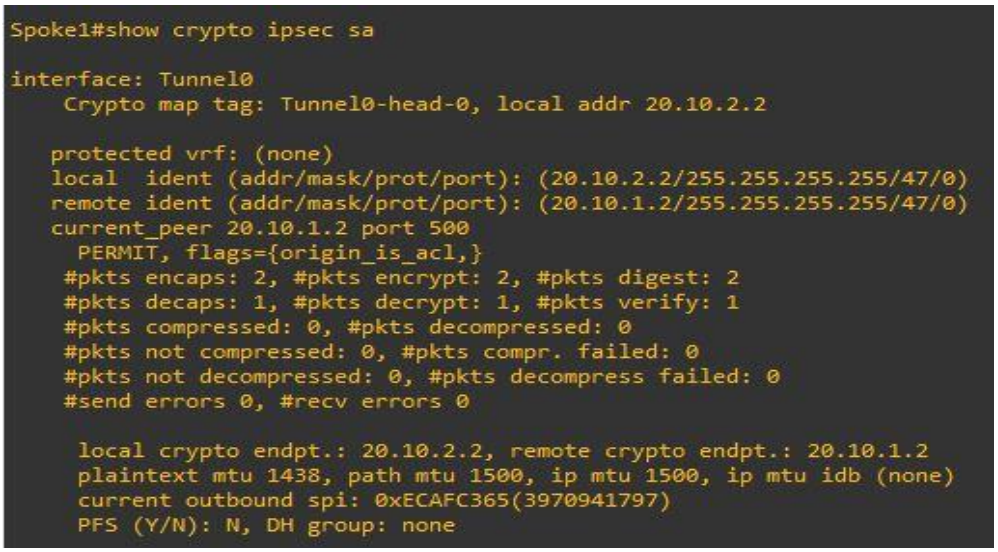

Figure 21. IPSec spoke1 results

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

```
Spoke2#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 20.10.3.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (20.10.3.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (20.10.1.2/255.255.255.255/47/0)
   current_peer 20.10.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
    #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 20.10.3.2, remote crypto endpt.: 20.10.1.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x1AF57D42(452296002)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x268ACC9C(646630556)
```

Figure 22. IPSec spoke2 results

3.4 Test Parameters

This study, in measuring network performance using measuring parameters, namely throughput, delay, jitter, and packet loss. In this measure, additional software is used, namely D-ITG (Distributed Internet Traffic Generator) which functions for network monitoring and testing. To measure network performance using Routing protocols BGP, DMVPN, and IPSec. The test parameter used is the network convergence time.

The scenario for this final project is that pc1, pc2, and pc3 perform different data exchanges at the transport layer such as sending TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) data. When sending data, the D-ITG software is run on both PCs that will carry out testing. In one example of this case, pc1 hub as sender and pc2 spoke1 as a receiver, and vice versa. The command for configuring D-ITG on both the sending and receiving sides is shown in Figure 23 the network performance will be observed during the data transmission time. The results of the measurements will be stored in a log file in PC2 spoke1.

```
PC Pengirim
./ITGSend (mengirim paket) -T (Paket yang dikirim) -a (IP tujuan) -C (Paket per second) -c (size paket) -t (waktu pengiriman per paket) -x file.log (file hasil monitoring)

PC Penerima
./ITGRecv (menerima paket)

./ITGDec (membuat file monitoring) file.log (nama file monitoring)
```

Figure 23. D-ITG command

In Figure 23, this test uses 2 sending packets, namely UDP and TCP, for packets per second using 250 packets per second, the packet size used is 3125 bits UDP, 625 bits TCP and packet delivery time is 10000 ms.

3.5 Scenario Analysis Test Results

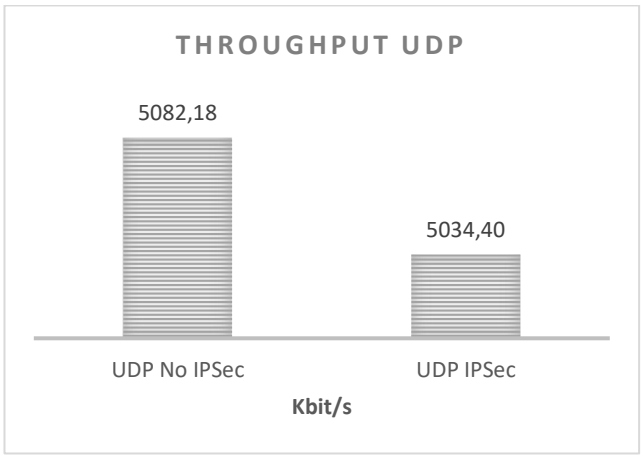

Figure 24. UDP Throughput Value Results

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

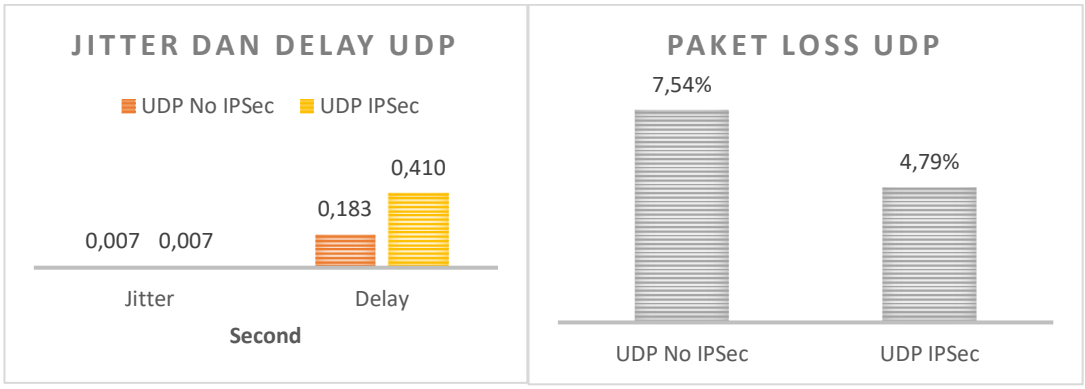

Figure 25. Results of Packet Loss, Delay, and Jitter UDP Values

Figure 24 and Figure 25 are the results of the trial of sending packets 30 times from UDP No IPSec DMVPN packets and IPSec DMVPN UDP packets. This test uses UDP packets and for packets per second in this test, it uses 250 packets per second, besides that the package size used in this test is 3125 bits in the calculation of the packet size used, with reference to the average throughput value of 5Mb with the calculation of 5,000,000 bits / 8 = 625,000 bits / 200ps = 3125 bits and with a packet delivery duration of 10000 milliseconds.

It can be seen from the graph in Figure 24 that the throughput value of UDP No IPSec DMVPN is greater than UDP IPSec DMVPN because in the Bit Per Second (BPS) measurement when transferring data using IPsec it is necessary to have encapsulation, encryption, and authentication methods on packet delivery to provide security protection when sending packets. sending, resulting in reduced IPSec UDP throughput value.

The jitter value can be seen in the graph in Figure 25 UDP IPSec DMVPN and UDP no IPSec DMVPN has the same value. The Delay value shown in Figure 25 UDP IPSec has a higher value than the UDP no IPSec value because the IPSec method in sending packets to provide security protection when sending makes delays in the delivery process to the destination causing a high delay value. And the value of packet loss UDP No IPSec DMVPN has a higher value than UDP IPSec DMVPN because IPSec avoids failure or loss of data sent to its destination by using the IPSec method, namely encapsulation, encryption, and authentication. Thus reducing the occurrence of data loss when sending to the destination.

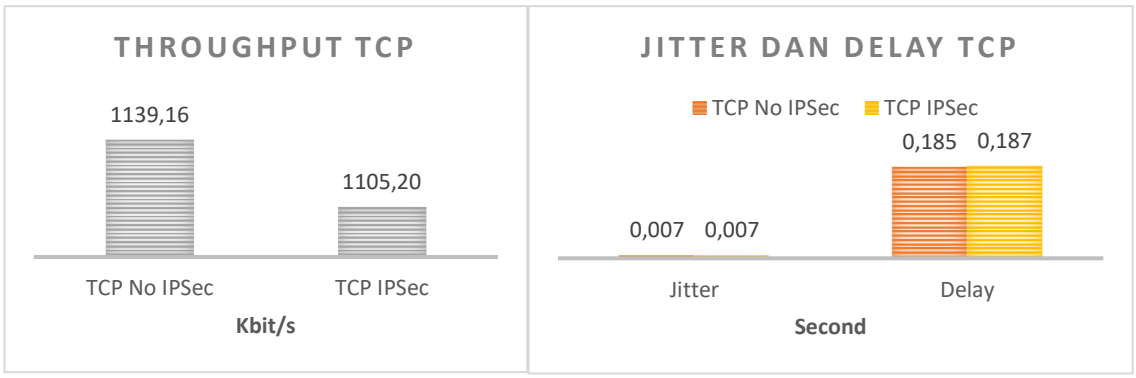

Figure 26. TCP Delay, Jitter, and Throughput Value Results

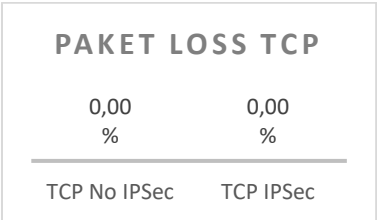

Figure 27. TCP Packet Loss Value Results

Figure 26 and Figure 27 are the results of the trial of sending packets 30 times from TCP No IPSec DMVPN packets and TCP IPSec DMVPN packets. This test uses TCP packets and for packets per second in this test, it uses 250 packets per second, besides that, the package size used in this test is 625 bits in the calculation of the packet size used concerning the average throughput value of 1Mb with the calculation of 1,000,000 bits / 8 = 125,000 bits / 200ps = 625 bits and with a packet delivery duration of 10000 milliseconds..

It can be seen from the graph in Figure 26 that the throughput value of TCP No IPSec DMVPN is greater than TCP IPSec DMVPN because in the Bit Per Second (BPS) measurement when transferring data using IPsec it is necessary to have encapsulation, encryption, and authentication methods on packet delivery in order to provide

Building of Informatics, Technology and Science (BITS)
Volume 4, No 2, September 2022 Page: 595−605
ISSN 2684-8910 (media cetak)
ISSN 2685-3310 (media online)
DOI 10.47065/bits.v4i2.1836

security protection when sending packets. make the delivery so that the impact of reducing the value of TCP IPSec DMVPN throughput.

The jitter value is shown in the graph in Figure 26 TCP IPSec DMVPN and TCP No IPSec DMVPN have the same value. The delay value shown in Figure 26 TCP IPSec DMVPN has a higher value than the TCP No IPSec value because the IPSec method in sending packets provides security protection when sending the delay in the delivery process to the destination causing a high delay value. And in the graph of Figure 27, the packet loss values for TCP No IPSec DMVPN and TCP IPSec DMVPN have the same value.

4. KESIMPULAN

Based on the results of this study, it shows that IPSec DMVPN has an effect on sending UDP packets which have a throughput value without IPSec of 5082.18 kbit/s while IPSec's throughput value is 5034.40 kbit/s. The value of packet loss No IPSec has a value of 7.54% while IPSec has a value of 4.79%. The jitter value of No IPSec and IPSec has the same value so it has no effect and the delay value of No IPSec has a value of 0.183s while the value of IPSec delay is 0.410s. Sending TCP DMVPN packets has a No IPSec throughput value of 1139.16 kbit/s while the IPSec throughput value of 1105.20 kbit/s. The value of packet loss No IPSec and IPSec have the same value so it has no effect. The jitter value of No IPSec and IPSec has the same value so it has no effect and the No IPSec delay value has a value of 0.185s while the IPSec delay value is 0.187s. IPsec security tunnel with BGP protocol causes decreased throughput and packet loss compared to without IPsec implementation we need to consider for security method when setting up DMVPN network for acceptable network performance.

REFERENCES

[1] H. M. Marah, J. R. Khalil, A. Elarabi, and M. Ilyas, “DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption,” Jun. 2021. doi: 10.1109/ICECCE52056.2021.9514142.
[2] N. Angelescu, D.C. Puchianu, G. Predusca, L.D. Circiumarescu, and G. Movila, “DMVPN simulation in GNS3 network simulation software,” ECAI 2017 - International Conference – 9th Edition, 2017.
[3] Ummi Masruroh, Khairul Hamdi Putra Widya, Andrew Fiade, Imelda Ristanti Julia, and Siti, “Performance Evaluation DMVPN Using Routing Protocol RIP, OSPF, And EIGRP,” The 6th International Conference on Cyber and IT Service Management, 2018.
[4] R. Khelf and N. Ghoualmi-Zine, “A Survey on Dynamic Multipoint Virtual Private Networks,” 2019.
[5] T. Ernawati and J. Endrawan, “Peningkatan Kinerja Jaringan Komputer dengan Border Gateway Protocol (BGP) dan Dynamic Routing (Studi Kasus PT Estiko Ramanda),” 2018.
[6] P. Hendradi and B. Santosa, “PENERAPAN METODE IPSEC UNTUK OPTIMALISASI KONEKSI JARINGAN di PT. OTO MULTIARTHA,” 2016.
[7] Citraweb, “Pemilihan Tipe VPN,” Dec. 09, 2013. https://citraweb.com/artikel_lihat.php?id=61 (accessed Feb. 28, 2022).
[8] yurmag, “DMVPN. Part 2. Routing and overhead optimization,” Jul. 06, 2016. https://yurmagccie.wordpress.com/2016/06/07/dmvpn-2/ (accessed Feb. 28, 2022).
[9] H. M. Marah, J. R. Khalil, A. Elarabi, and M. Ilyas, “DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption,” Jun. 2021. doi: 10.1109/ICECCE52056.2021.9514142.
[10] N. Iryani and D. D. Andika, “Implementasi Dynamic Multipoint Virtual Private Network Dual Hub,” Jurnal Telekomunikasi dan Komputer, vol. 11, no. 2, p. 118, Aug. 2021, doi: 10.22441/incomtech.v11i2.10839.
[11] Wahyu Patrya Sasmita, Novi Safriadi, and Azhar Irwansyah, “ANALISIS QUALITY OF SERVICE(QOS) PADA JARINGAN INTERNET (STUDI KASUS : FAKULTAS KEDOKTERAN UNIVERSITAS TANJUNGPURA),” 2013.
[12] P. R. Utami, “ANALISIS PERBANDINGAN QUALITY OF SERVICE JARINGAN INTERNET BERBASIS WIRELESS PADA LAYANAN INTERNET SERVICE PROVIDER (ISP) INDIHOME DAN FIRST MEDIA,” Jurnal Ilmiah Teknologi dan Rekayasa, vol. 25, no. 2, pp. 125–137, 2020, doi: 10.35760/tr.2020.v25i2.2723.
[13] Hasanul Fahmi, “ANALYSIS QOS (QUALITY OF SERVICE) MEASUREMENT OF DELAY , JITTER, PACKET LOST AND THROUGHPUT TO GET GOOD QUALITY OF RADIO STREAMING WORK,” vol. 7, no. 2, pp. 98–105, 2018.
[14] R. Wulandari, “ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON-LIPI),” Jurnal Teknik Informatika dan Sistem Informasi, vol. 2, pp. 2443–2229, 2016.
[15] A. Akmaludin, A. Mt, and S. U. Masruroh, “Evalusi Kinerja Hot Standby Router Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP) untuk Layanan Video Streaming,” vol. 2, no. 1, pp. 43–51, 2019.