Method And Implementation of MPLS Tunnel Selection On Nokia Metro-E Devices

R. Muhammad. Arifin[1)]
Politeknik Negeri Semarang[1)]

Abstract— Tunneling is an interconnection solution between local networks separated by remote over a public IP. The current issue does not have proper guidelines for using tunneling techniques. Tunneling selection is generally only based on the beliefs and experience of network management operators or following SOP. The brand of tunneling device is widely used by telecommunication operators in Indonesia (especially P. Java) is Nokia. In this study, implementation, testing and analysis of MPLS techniques on Nokia devices to produce recommendations when to use MPLS tunnels according to network topology appropriately. The software used in this study was FTP, Tfgen and Wireshark. FTP and Tfgen as network traffic generators and Wireshark to record throughput, delay and downtime. Analysis of MPLS on Nokia devices is conducted based on recording results for various traffic engineering scenarios including loadless conditions, and various other conditions in case of network disruption. MPLS research results when without load all went well with an average throughput of 1.08 Mbps and delay of 10 ms. When with load has a stability delay of 10 ms, when when network disruption using ICMP get 1 Request Time Out or 4s. MPLS techniques are used on established networks because it can provide alternative density lines.

Index Terms—IP, Tunneling, Nokia, MPLS

1. Introduction

Network technology is now a phenomenon used globally, so IP-based services have been growing and diverse, one of which is Tunneling. Tunneling is an techniques of establishing local communication lines between two or more routers using a public IP network.

The problems faced in the tunnel system currently have no guidelines to provide recommendations when to use the right techniques according to the network topology used. The use of tunneling is done based on the beliefs and experience of network management operators or follow sops. Brands of devices that can do tunneling are very diverse in Indonesia, but in particular P. Java the most use on telecommunication operators is Nokia in addition to Cisco, Huawei, Mikrotik, etc. Nokia devices have two techniques namely GRE and MPLS techniques. In this study, implementation, testing and analysis focus on MPLS techniques were conducted to produce recommendations on when to use the technique.

MPLS is tunneling on Nokia devices that is flexible in finding the best path for service. When tunneling MPLS use data to be encapsulated with two MPLS labels namely outer transport label and service inner label. Transport services are labeled Distribution Protocol (LDP/RSVP-TE) or Label Switched Paths (LSP).

Research related to MPLS has been done but only provides comparative information with other tunneling, here's the research: analysis of traffic engineering (TE) performance with Resource Reservation Protocol (RSVP) and ignition segment. The result of the study is that MPLS simplifies the performance of the labeling and in maintaining signaling protocols. Test results occur high traffic on the main line, with both the ignition segment and the RSVP having the same value. While on the backup path get a smaller value of the interrupt segment, so that in the ignition segment can send data faster than with RSVP. Test results of 100% packet delivery rate and 0% packet loss with detractor segment and RSVP on main and backup lines get the same value. The implementation of the interrupt segment has an actual bandwidth value greater than the RSVP implementation, so the interrupt segment can send data faster than RSVP. Then when the link condition is routed, both have a 1% packet loss, but the path shift is done faster on interrupt segment [1].

Subsequent research tested IPsec-protected MPLS, MPLS VPN and MPLS VPN technologies conducted by GNS3 simulations. The parameters used are jitter, latency, MOS score and missing package as well as cisco device. The results of the study were obtained from a technology scenario, the jitter increased from the MPLS VPN scenario when using IPsec which is 46875 bytes or lost 5% packet. But MPLS technology offers a loss rate of less than 1% and lower latency than the technology tested [2].

MPLS tunnel research has been conducted on BGP/MPLS networks using Linux-based Provider Edge (PE) and Customer Edge (CE) deterrence as proposed by the IETF. Network comparison scenarios are created with PE-PE and CE-PE detractor using MPLS, GRE tunnels and the offering is GRE tunnels with IP Security (IPSec) capabilities. IPsec is a protocol used to secure transmissions in maintaining packets. The research runs on purpose, but has the drawback that PE implementation is based on manual routing, as well providing input that CE-PE integration can be tried using different Interior Gateway Protocol (IGP)

Corresponding author. Tel.: Arifin
Email : rdnmuhammad.arifin@gmail.com

routing protocols because PE-PE distribution must be based on BGP routing [3].

Analysis of services in layer 3 using MPLS or GRE tunnels is performed, by splitting the departure and return lines of customer service, as well as testing using a wide range of deodorizers such as Cisco, Alcatel, ZTE, Red Back and Juniper. The shortcomings in this study do not show the finished results only to give the big picture of topology and configuration of each of the various deterrents [4].

There is research with GRE multiprotocol tunnels (mGRE) using GNS simulations in layer 3 where it permits the use of Label Switched Path (LSP), Carrier Supporting Carrier (CSC) or Label Distribution Protocol (LDP) and uses VPNv4/v6 encapsulation in CE inter-labeling. This study does not list the results of mGRE usage completely as there is a comparison of delay time with existing tunnels, as well as research using GNS3 simulations in its formation [5].

There is research related to security vulnerabilities on MPLS VPN networks with various improvement techniques that have been implemented. Security vulnerabilities such as malicious software policy flaws and hardware-fiber software vulnerabilities that need to be mitigated. The required requirements separate traffic from other users so only PE knows the IP address and route, in order to avoid man in the middle or DOS attacks. The idea of several security techniques such as Intrusion Detection System (IDS), Secure Socket Layer Encryption, Cryptographic Hashing Algorithm -- (Message Digest 5 (MD5) and Security Hash Algorithm), Advanced Encryption Standard, Rivest-Shamir-Adlehman (RSA), Diffie-Hellman and IP Security. The results obtained that the IDS technique is suitable for use in strengthening security in and out of cloud MPLS [6].

Subsequent research conducted QoS analysis on the MPLS VPN method applied to GNS3 simulations using MPLS and OSPF routing. This study says that MPLS is a core network technology that is usually called layer 2.5 network. A VPN provides a private path under the shared path with the internet. The results provided that MPLS with VPN is a solution to create a personal path at a cost that is not expensive and has flexibility in the creation of tunnels, as well as providing high data communication capabilities and able to maintain data security. The disadvantage of this study is that it does not provide information related to data values such as actual bandwidth, break-up time, but only talk about whether or not an MPLS VPN system [7].

Analysis ISP network renewal on devices using MPLS and BGP routing, for this research simulator using GNS3 and OPNET. The network requirements required today are reliability, availability, security and network management. The results stated that the merger of both MPLS and BGP routing creates a good relationship of data performance, speed and capacity as well as cost-effective management [8].

Research on QoS on MPLS networks, as traffic networks become increasingly complex there is a need to migrate from circuits to packet-based networks. The research analyzed QoS, on the quality of services on MPLS networks such as MPLS TE network implementation and its integration with IntServ and DiffServ, MPLS QoS applications on MPLS VPNs, as well as MPLS-TP integration with SDN. The shortcomings of this study do not mention quantitative results [9].

Performance analysis Multi Protocol Label Switching–Virtual Private Network (MPLS-VPN) with THE GRE tunnel method that uses FTP and in this study used various mesh and ring topologies in its testing and devices using Mikrotik. The results of the second topology study experienced a decrease in the actual bandwidth value, delay time and packet loss caused by the use of resources on the exchange of communication codes (interkey exchange) in the formation of GRE tunnels where the background traffic of 0 Mbps at the time of delay using ring topology get 183s when using net topology 176s. As well as missing packets using a ring topology of 0.010336368% when using a mesh topology get 0.010355744%. GRE tunnels cause a rise in missing packets, in the ring topology missing packets rise by 0.093101493% from 0.010262188% to 0.010336368% after the GRE tunnel is carried out and on the net topology the packet is up by 0.00085672% from 0.010270072% to 0.010355744% the decrease in performance is experienced due to the use of resources on the network in the form of communication code at the time of formation of the GRE [10].

Analysis involving real-time applications, MPLS-based Voice over IP (VoIP) was developed to combine data-link layer properties with datagram network layer flexibility and durability in efficient traffic transmission and QoS support. The Connection Admission Control (CAC) mechanism for RSVP-TE in MPLS networks divulges its availability to achieve high performance especially with the growing importance of real-time applications requiring high end-to-end QoS. So this study conducted a Connection Admission Control (CAC) mechanism with input parameters not only bandwidth but also end-to-end delays and jitters for decision making. Comparison simulations using OPNET simulators between the proposed algorithm and the most commonly used CAC are presented. Simulation results from the proposed algorithm compared to other algorithms showed that the proposed algorithm outperformed the others in terms of delay, jitter, and delay variation. Further research expects dynamic CAC to increase threshold values to dynamically modify its parameters based on network conditions to achieve optimal decision-making under different network conditions [11].

Therefore, this research was conducted to produce the right recommendations for operators in determining tunneling systems according to the network topology used. Research conducted analyzing: MPLS method data service by analyzing the quality of data communication services by sending file transfer protocol (FTP) and then forming ring and mesh topology and will be given traffic load on the network line. Furthermore, it also performs an analysis of the quality of data communication services when the path used is broken up until it moves another line connected to the destination. The testing method is done by pinging the computer and trace commands from the router as well as performing a service quality analysis performed based on throughput, delay, and downtime recorded using Wireshark.

2. Methods

The design of research methods is carried out with the following steps:

2.1. Observation

Conducted to obtain the data searched by reference and literature studies in the form of: books, journals, research, scientific works, articles about Nokia devices used such as VPN VPLS with optimal data security, as well as studying how the activation protocol performance MPLS, OSPF, LDP, RSVP as a support for research.

2.2. System Planning

System design is done using EVE-NG application with this software can perform the configuration as original. What is needed in the design is that there are Nokia routers, FTP Servers, and client computers:

- Nokia routers are tasked with routing between router interfaces to connect, by adjusting the configuration according to the design that has been made.
- Computer 1 is tasked to upload files on the FTP server. On the other hand, computer 2 and computer 4 serve as senders and receivers to perform various network engineering scenarios using tfgen software.
- FTP Server serves as a serving computer 1. By using wireshark software can be done data retrieval and traffic analysis on this server according to the network engineering scenario that has been created.

To test the quality of service and get recommendations when the right time using MPLS tunneling techniques, several network engineering scenarios are performed where using ring topology and mesh topology. The following research needs to be done:

- Establishing topology and protocol configuration according to design as in figure 1 and figure 2.

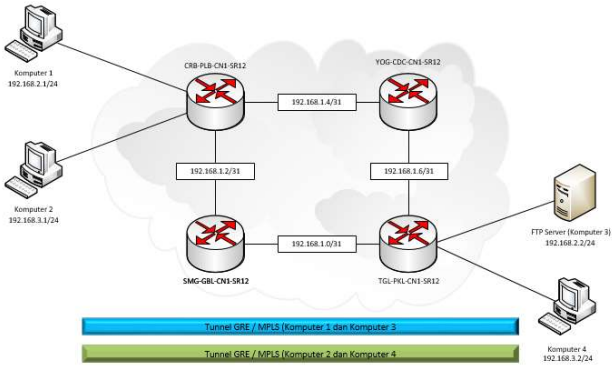

Fig. 1. Ring Implementation Topology.

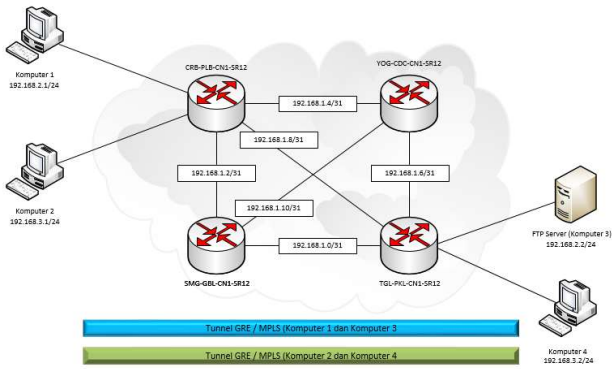

Fig. 2. Mesh Implementation Topology

- Set the throughput of each inter router communication given 1 Gigabits per second (Gbps).
- Create a VPLS VPN service on a CRB-PLB-CN1-SR12 router with TGL-PKL-CN1-SR12 to connect 1 computer with FTP server and 2 computers with 4 computers.
- Perform initial setup: computer 1 uploads 75 Megabytes (MB) of files to the FTP server, computer 2 and computer 4 run traffic engineering scenarios using tfgen software, and performs recording of incoming data traffic from computer 1 to FTP server using wireshark software.
- Perform router-side testing, which has VPLS VPN service installed, by sending ping and trace connection commands during file uploading and traffic engineering. The ping command is used to view the results of the runtime, while traces to see the path that the client computer passes through.
- Testing various network engineering scenarios, 10 times each, on MPLS tunneling for ring topology and mesh topology. The engineering is a)when without load, b)when with load engineering from the beginning of the upload runs, c)when with load engineering performed on FTP runs 50% and d)when there is interference on the main line.
- Make observations on collected data to be processed and analyzed. The results are used to assess the performance quality of MPLS services for ring topology network and mesh topology in different traffic conditions.

The following hardware and software needs, then continued from the stage of telecommunication device configuration until connected and conducted data service quality testing.

- Needs Hardware

Table 1. Hardware

No	Hardware	Specification	Total	Information
1	Laptop Server	AMD A10, Memory 12 GB DDR3L, Hardisk 1TB, Ethernet 10/100 Mbps, Win 10 x64	1	Used as an FTP Server

2	Laptop Client	Intel Core i5 Memory 12 GB Hardisk 500GB, Ethernet 10/100 Mbps, Win 10 x64	1	Used as an FTP Client & for virtual router
3	UTP Cable	Cat5e	1	

- Needs Software

Table 2. Software

No	Software	Total	Information
1	Wireshark	1	To traffic analysis
2	WinSCP	1	To file sharing computer
3	EVE-NG	1	To Virtual Router
4	Tfgen	1	To Traffic Generator
5	Vmware	1	To Instalation virtual computer komputer in EVE-NG

Table 3. IP Address Router

No	Name Hardware	To	Port	IP PTP
1	SMG-GBL-CN1-SR12	TGL-PKL-CN1-SR12	1/1/1	192.168.1.0/31
		CRB-PLB-CN1-SR12	1/1/4	192.168.1.3/31
		YOG-CDC-CN1-SR12	1/1/5	192.168.1.10/31
2	TGL-PKL-CN1-SR12	SMG-GBL-CN1-SR12	1/1/1	192.168.1.1/31
		CRB-PLB-CN1-SR12	1/1/5	192.168.1.9/31
		YOG-CDC-CN1-SR12	1/1/4	192.168.1.7/31
3	CRB-PLB-CN1-SR12	SMG-GBL-CN1-SR12	1/1/1	192.168.1.2/31
		TGL-PKL-CN1-SR12	1/1/3	192.168.1.8/31
		YOG-CDC-CN1-SR12	1/1/2	192.168.1.4/31
4	YOG-CDC-CN1-SR12	TGL-PKL-CN1-SR12	1/1/1	192.168.1.6/31
		CRB-PLB-CN1-SR12	1/1/2	192.168.1.5/31
		SMG-GBL-CN1-SR12	1/1/3	192.168.1.11/31

The EVE-NG settings on the Vmware software are made with a 9.0 GB memory specification, 50 GB of storage and a network adapter added into three wirelesss. On VMnet 2 it is used for local communication between Vmware and EVE-NG, while VMnet 0 is used to connect communication to computer 1 EVE-NG with the computer's FTP server, and VMnet 3 is redirected to loopback as computer communication 1. With the specifications of the device used, then can build MPLS tunneling using EVE-NG by installing Nokia type 7750 SR router as many as 4 pieces with IP System SMG-GBL-CN1-SR12 (10.10.10.1/32), TGL-PKL-CN1-SR12 (10.10.10.2/32), CRB-PLB-CN1-SR12 (10.10.10.3/32), YOG-CDC-CN1-SR12 (10.10.10.4/32) and 4 computers communicating with each other with the appropriate IP address allocation in tables 3 and 4.

Table 4. IP Address Computer.

No	Name Hardware	To	IP Port	Information
1	Computer 1	Computer 2	192.168.2.2/24	-
2	Computer 2	Computer 1	192.168.2.1/24	FTP Server
3	Computer 3	Computer 4	192.168.3.1/24	Traffic Generator

This research requires several stages such as in Figure 2, namely preparing hardware and software. Then provide the appropriate infrastructure scenario. After all can communicate with the configuration of MPLS activation protocol, RSVP, LDP, and OSPF on the router, then create a VPN path and tunneling by selecting MPLS

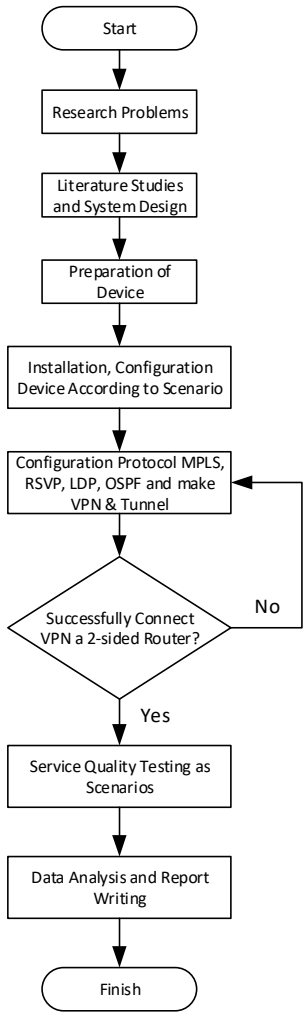

Fig. 2. Research flow chart

2.3. Data Collection

Collecting research data that has been implemented and tested for performance from network engineering scenarios.

2.4. Data Processing

It's a place where the collected data is processed using excel tables, then the test results are done on average to get accuracy in obtaining throughput, delay and downtime values.

2.5. Documentation

It's the final data collection then input in the report as evidence of documentation of the results of research that has been done.

3. Results And Discussion

This section contains a discussion about the results of the implementation and testing of tunneling MPLS using VPN VPLS. Performance comparison when sending files to FTP server with network traffic engineering from unburdened until there is a flow to full traffic.

3.1. Communication Testing

This test is done to find out that VPN performance has run smoothly according to the desired topology. nokia router as a medium of data communication between computer. The standard for communication testing is to use ping commands between computer. With the intention to know the data package sent to the destination IP address until getting a reply which means VPLS VPN that has been created successfully. If there is a Request Time Out (RTO) message on the computer, then there is an error in the creation of tunnel solutions that is to double-check the condition of tunneling that has been configured in an active or dead state as in Figure 3 and by performing ping commands to each tunneling in the router such as Figure 4:

```
A:TGL-PKL-CN1-SR12# show service sdp

===============================================================================
Services: Service Destination Points
===============================================================================
SdpId  AdmMTU  OprMTU  Far End          Adm  Opr         Del     LSP   Sig
-------------------------------------------------------------------------------
5      0       8914    10.10.10.3       Up   Up          MPLS    R     TLDP
7      0       8914    10.10.10.3       Up   Up          MPLS    R/L   TLDP
10     0       8894    10.10.10.3       Up   Up          GRE     n/a   TLDP
50     0       8894    10.10.10.3       Up   Up          GRE     n/a   TLDP
-------------------------------------------------------------------------------
Number of SDPs : 4
-------------------------------------------------------------------------------
Legend: R = RSVP, L = LDP, B = BGP, M = MPLS-TP, n/a = Not Applicable
===============================================================================
```

Fig. 3. Service SDP

```
A:CRB-PLB-CN1-SR12# oam sdp-ping 5 resp-sdp 5 count 10
Request      Response     RTT
-------------------------------------------------------------------
1            Success      10.6ms
2            Success      4.31ms
3            Success      3.27ms
4            Success      3.37ms
5            Success      4.11ms
6            Success      3.68ms
7            Success      5.82ms
8            Success      5.84ms
9            Success      3.38ms
10           Success      5.18ms

Sent: 10     Received: 10
Min: 3.27ms   Max: 10.6ms   Avg: 4.96ms
```

Fig. 4. Ping Tunnel

```
C:\Users\muhammad.arifin>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=6ms TTL=128
Reply from 192.168.2.2: bytes=32 time=5ms TTL=128
Reply from 192.168.2.2: bytes=32 time=5ms TTL=128
Reply from 192.168.2.2: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

Fig. 5. Ping Between Computers

From Figure 4 means SDP ID on CRB-PLB-CN1-SR12 and TGL-PKL-CN1-SR12 with sdp-ping reading 10 comes from source i.e. from CRB-PLB-CN1-SR12 after that resp-sdp 10 the destination SDP ID obtained from TGL-PKL-CN1-SR12. Figure 4 is the result of the SDP back and forth ping command on the router when using MPLS service but has not been given VPLS VPN connection. After the re-examination, it can be proven that the computer 1 client tested the VPN network with ping command 192.168.2.2, and has been responded from the owner of the IP address as in Figure 5, so that the VPN build worked successfully.

3.2. Loadless Testing

In this section, testing is performed on MPLS tunneling when uploading files from computer 1 to the FTP server as well as monitoring the condition of the router's network port and viewing the path that the file passes through to its destination. After ftp file flow on ring topology and mesh topology, take every test with ICMP protocol performed on computer 1 to FTP server. Figure 6 proves that when using MPLS with ftp traffic mesh topology will go to port 1/1/2 YOG-CDC-CN1-SR12 with the results of monitoring on Nokia devices obtained 0.11% of the delivery of 75 Mb files, it is due to the configuration of LSP lines by operators who choose the path to pass. From figure 7 can be interpreted all still look safe because the value of delay time is still below 150 ms according to TIPHON, if it gets more than that then there will be a slowdown in file delivery.

```
A:CRB-PLB-CN1-SR12# monitor port 1/1/1 1/1/2 1/1/3 interval 3 rate repeat 1 | matc
h .
Utilization (% of port capacity)                    ~0.00                   ~0.00
Utilization (% of port capacity)                    ~0.00                    0.11
Utilization (% of port capacity)                    ~0.00                   ~0.00
A:CRB-PLB-CN1-SR12# show router interface

===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm       Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                  PfxState
-------------------------------------------------------------------------------
system                           Up        Up/--       Network system
   10.10.10.3/32                                               n/a
to_SMG-GBL-CN1-SR12              Up        Up/--       Network 1/1/1
   192.168.1.2/31                                              n/a
to_TGL-PKL-CN1-SR12              Up        Up/--       Network 1/1/3
   192.168.1.8/31                                              n/a
to_YOG-CDC-CN1-SR12              Up        Up/--       Network 1/1/2
   192.168.1.4/31                                              n/a
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
```

Fig. 6. Monitoring Router

```
C:\Users\muhammad.arifin>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 9ms, Average = 8ms
```

Fig. 7. Ping Computer Without Load

3.3. Load Testing From Scratch

This test is still the same using FTP but different because there is tfgen as the basis of network traffic load with a configuration of 5 Mbps. The path that is missed is also still the same no change only different network traffic that goes in the ignition. As can be seen in the ring topology and mesh topology on the MPLS tunnel. MPLS is more favored in avoiding services so as not to pass through traffic-intensive lanes. Where in the condition of ring topology or mesh topology remains following the path that has been made. As in Figure 8 it appears that the flow from tfgen follows the LDP path, but for FTP files pass through different paths that go to port 1/1/2 to_YOG-CDC-CN1-SR12 and make traffic balanced with tfgen entering CRB-PLB-CN1-SR12 gets 0.16% through port 1/1/1 while 0.21% through port 1/1/2 with the result as well as doing ICMP testing with ping commands on the computer and getting results in Figure 9 does not occur latency.

```
A:CRB-PLB-CN1-SR12# show router interface

===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm       Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                  PfxState
-------------------------------------------------------------------------------
system                           Up        Up/--       Network system
   10.10.10.3/32                                               n/a
to_SMG-GBL-CN1-SR12              Up        Up/--       Network 1/1/1
   192.168.1.2/31                                              n/a
to_TGL-PKL-CN1-SR12              Up        Down/--     Network 1/1/3
   192.168.1.8/31                                              n/a
to_YOG-CDC-CN1-SR12              Up        Up/--       Network 1/1/2
   192.168.1.4/31                                              n/a
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
A:CRB-PLB-CN1-SR12# monitor port 1/1/1 1/1/2 interval 3 rate repeat 3 | match .
Utilization (% of port capacity)                    ~0.00                    0.16
Utilization (% of port capacity)                    ~0.00                    0.21
Utilization (% of port capacity)                    ~0.00                    0.17
Utilization (% of port capacity)                    ~0.00                    0.16
Utilization (% of port capacity)                    ~0.00                    0.17
Utilization (% of port capacity)                    ~0.00                    0.21
```

Fig. 8. Monitoring Router With Load

```
C:\Users\muhammad.arifin>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=10ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=7ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 10ms, Average = 8ms
```

Fig. 9. Ping Computer With Load

3.4. Testing With Sudden Loads

Testing here means that when ftp conditions are running low traffic suddenly get an abundance of traffic from other detractor using MPLS tunnels is still the same as previous tests do not pass through a dense path, but all depends on the form of topology tested. The scenario in this test is to send ftp files when the file is 50% sent, and then add the load using tfgen software on the tunnel. Then the ICMP protocol test with the ping command and get MPLS has no effect because the load condition follows the LDP path as in Figure 10.

```
C:\Users\muhammad.arifin>ping 192.168.2.2 -n 10

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=17ms TTL=128
Reply from 192.168.2.2: bytes=32 time=11ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128
Reply from 192.168.2.2: bytes=32 time=21ms TTL=128
Reply from 192.168.2.2: bytes=32 time=7ms TTL=128
Reply from 192.168.2.2: bytes=32 time=12ms TTL=128
Reply from 192.168.2.2: bytes=32 time=11ms TTL=128
Reply from 192.168.2.2: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 21ms, Average = 11ms
```

Fig. 10. Ping Computer With Sudden Load

3.5. Testing When The Main Link Is Down

This scenario tests the communication lines to the same backup line as the destination. Standardized testing scenarios continue to use the ICMP ping protocol from computer 1 to computer 2 with the test results visible in Figure 11.

```
C:\Users\muhammad.arifin>ping 192.168.2.2 -n 10

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=23ms TTL=128
Reply from 192.168.2.2: bytes=32 time=26ms TTL=128
Reply from 192.168.2.2: bytes=32 time=33ms TTL=128
Reply from 192.168.2.2: bytes=32 time=44ms TTL=128
Request timed out.
Reply from 192.168.2.2: bytes=32 time=10ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=8ms TTL=128
Reply from 192.168.2.2: bytes=32 time=22ms TTL=128
Reply from 192.168.2.2: bytes=32 time=26ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 44ms, Average = 22ms
```

Fig. 11. Ping Computer When Link Down

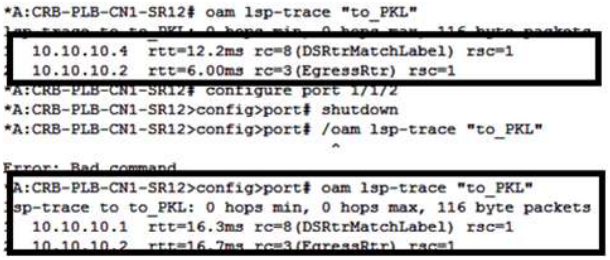

Fig. 12. Tracert MPLS

The test results in Figure 11 prove that data communication was replied to by the owner of IP 192.168.2.2 but when the main line is disconnected there is an RTO where the IP owner does not reply to the communication later because there are other lines that have the same neighbor interface as the destination then automatically move the path according to Figure 12. You can see the command on the Nokia deodorizer for LSP "oam lsp-trace" on router.

3.6. Analysis Throughput

Throughput testing is performed to test the capabilities of MPLS tunnels. Data plan results are subject to change according to conditions, the amount of data accessed, computer capabilities, and other supporting devices. The scenario in this analysis as in the previous testers is various conditions of network traffic. Can be seen the results of processed data and tunnel graphs in traffic load conditions 0 Mbps as follows:

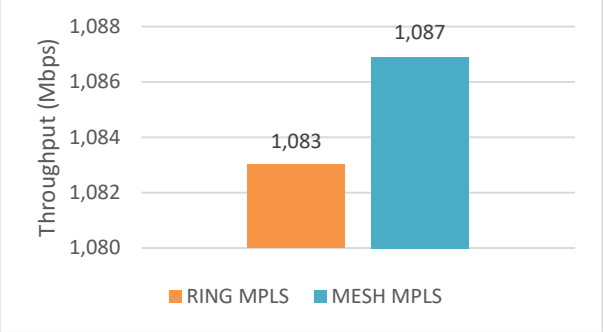

Fig. 13. Average Throughput Withoud Load

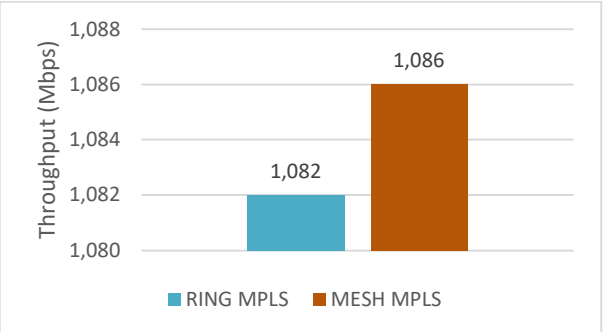

Fig. 14. Average Throughput With Load

Figure 13 using the MPLS tunnel mesh topology scored 1,087 Mbps, while the MPLS ring topology experienced a decrease in performance of 0.006 Mbps, but not so significant. This value is still considered normal because network traffic is still stretched. Then the next research was done by adding tfgen 5 Mbps software as a traffic loader which can be seen in the table and graph follows Figure 14.

MPLS tunnel results are still the same as when the ring topology has stability with a value of 10,603 ms and throughput worth 1,082 Mbps and in mesh topology has a value of 1,086 Mbps for actual throughput and 10,458 ms for delay, because in MPLS is able to avoid traffic that is likely to cause heavy traffic on certain lines. And then the next test with the scenario where FTP 50% of the file delivery is given traffic load from tfgen software of 5 Mbps can be seen in Figure 15 as follows:

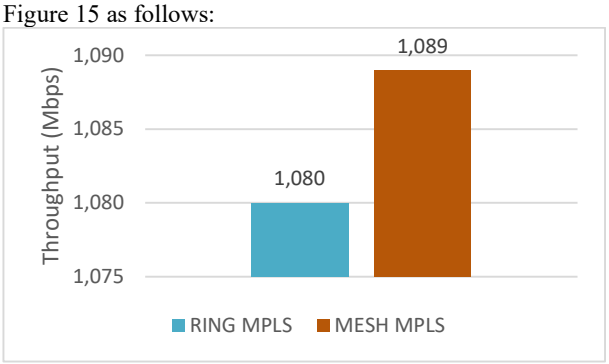

Fig. 15. Average Throughput With Load Suddenly

The result is MPLS when suddenly load with ring topology gets a value of 1,080 Mbps for throughput and 10,550 ms for delay, which means that the MPLS tunnel runs normally despite the traffic load. When the mesh topology has a value of 1,089 Mbps for throughput and 10,437 ms for delay, which means that the MPLS tunnel on the mesh topology also runs normally despite the traffic load, because MPLS can find a loose path with the help of the operator. With these results remain considered normal and the difference is not very significant.

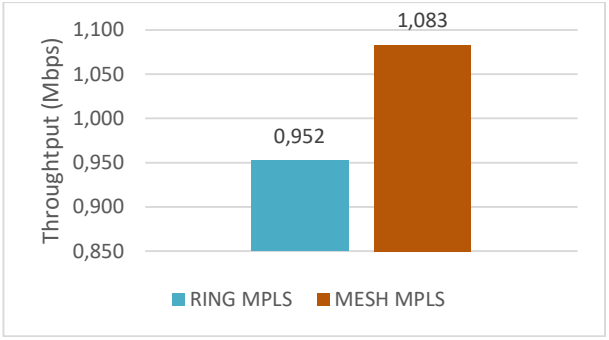

Fig. 16. Average Throughput With Link

The actual bandwidth result at the time of disconnection in the main line was also done by this study with the results obtained when there is interference in MPLS tunnels with ring topology that has a value of 0.952 Mbps for throughput and 12.127 ms for delay, there is a high value because in ring topology only has the remaining 1 neighbor

interface. Then when there is a disturbance in the MPLS tunnel with mesh topology that has a value of 1,083 Mbps for throughput and 10,447 ms delay, it is declared normal because in mesh topology has the remaining 2 neighbor interfaces that do not cause traffic density. Figure 16 can be interpreted MPLS in the form of ring topology because there is only one path left, it will experience traffic on that path and high ping on the client computer. In contrast to the mesh topology in CRB-PLB-CN1-SR12 has three neighbors or liaisons that are to SMG-GBL-CN1-SR12, YOG-CDC-CN1-SR12 and direct line TGL-PKL-CN1-SR12. When a breakup is still declared safe there is no other traffic disruption.

3.7. Analysis Delay

Delay testing is also performed to test the tunnel capabilities of MPLS. The result of the data package may vary according to the conditions. The scenario in this analysis is like previous tests, and it can be seen that the first thing to test is when it is without load. The results of the data process can be seen Figure 17 can be fickle due to the condition of the computer and its path, but from the results is still considered a normal and standard lag time.

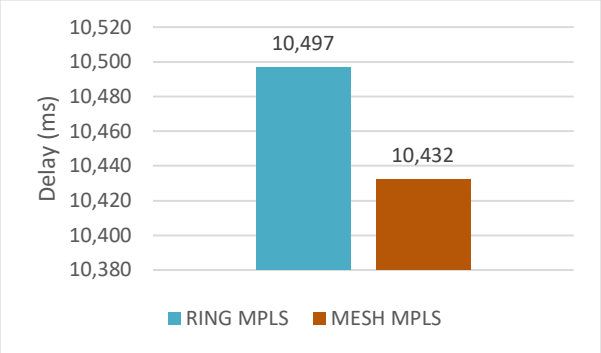

Fig. 17. Average Delay Without Load

Different when research with load, in Figure 18 get a delay result of around 10ms which is considered normal because it does not miss the traffic-intensive path.

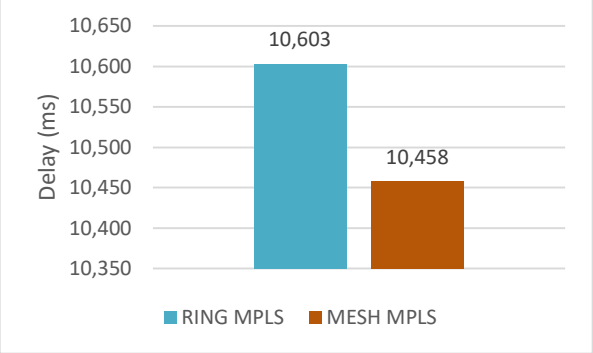

Fig. 18. Average Delay With Load

Figure 19 scenario when given load when FTP runs 50% obtained MPLS value is still the same as before.

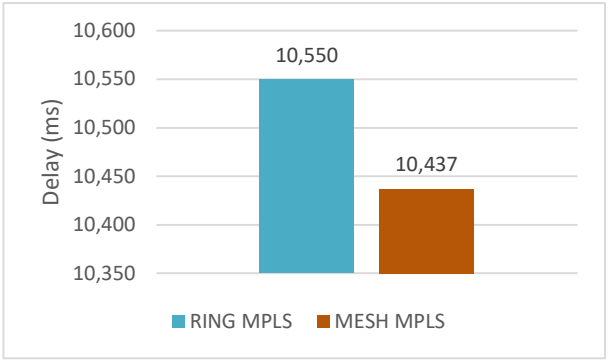

Fig. 19. Average Delay With Load Suddenly

The last research when the main line broke up was obtained for MPLS tunnel high delay ranged from 12 ms on ring topology because the ring only has 1 spare line, for mesh topology get a normal value of about 10 ms caused as explained earlier that did not miss the full traffic line.

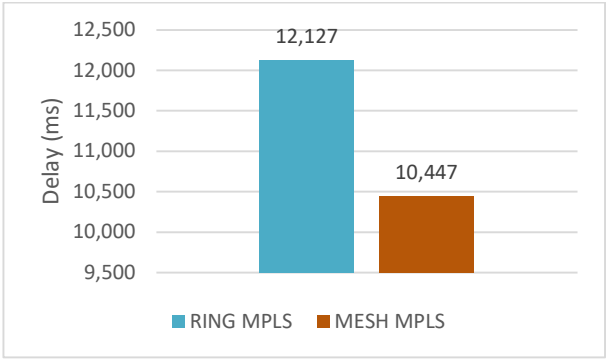

Fig. 20. Average Delay With Link Down

3.8. Analysis Downtime

This analysis is used to determine the quality of data communication when the main line is broken, the VPLS service moves to another line that is still one neighbor with the destination. And obtained testing from protocols that use icmp protocol with ping command. Testing was conducted to determine the quality of the MPLS tunnel. Where computer 1 performs ping commands to 2 computers with IP address 192.168.2.2, with a running time of 10 replies, then disconnected at the time of reply to 5 and get rto results, rto is a message that does not manage to get a reply from computer 2 because there is a disruption of tunnel communication but after finding another line delivery is done again until getting a reply. When the study took data, obtained a time lag of 1 RTO or by default 4s so that it can be concluded when breaking the TUNNEL MPLS get the result of a break time of 4s. In Figure 21 is the time of the breakup of the MPLS tunnel.

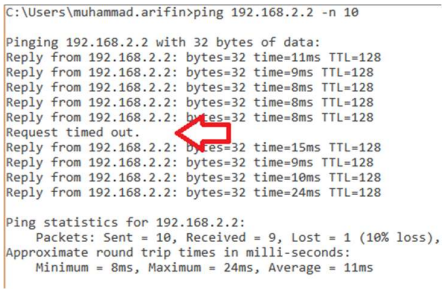

Fig. 21. Analysis Downtime

3.9. Analysis Network Scenario

Tests that have been conducted in various scenarios of network traffic engineering to obtain accuracy in choosing MPLS tunnels, the following table results are obtained:

Table 5. Research Results

	Scenerio MPLS	Ring	Mesh
1	Without Load Traffic	√	√
2	With Load Traffic (Beginning)	√	√
3	With Load Traffik (Suddenly)	√	√
4	With Link Down	-	√

Table 5 results get that tunneling MPLS in data communication can be reliable, and when interference occurs in the transfer of data paths very quickly only requires 4s can already re-occur communication. When there is a disturbance in the ring topology can not be reliable because when the line is broken only has a backup of 1 lane it was previously filled with traffic so it can make traffic density occur on the backup line. Table 6 is the advantages and disadvantages at the time after the research. Tunneling MPLS when given a direct traffic load can choose a path that does not need a deodorizer that does it, so it can directly select on empty traffic, so there is no up and down traffic, but it needs special expertise in the manufacture because it is so complicated.

Table 5. Results Advantages and Disadvantages

Advantages	Disadvantages
a) Can more certainly do traffic balancing, by combining strict and loose commands on the path created by LSP. b) It has commands that have no effect despite ospf metric configuration and LDP filtering. c) Can avoid traffic-heavy lanes.	a) The complexity of configuring, because it is necessary to create a path then performed binding on the LSP, then SDP and channels. b) The path selection configuration is done manually by the network operator.

5. Conclusion

After the research of MPLS tunnel on Nokia devices can be concluded, namely:

A. The use of MPLS tunneling has its role. 1) In terms of configuration of tunneling system MPLS is more complicated because it must make a simulation of the path first then perform binder LSP and channel. 2) In terms of the ability to overcome traffic density, MPLS is able to balance traffic because before making a simulated path, the operator finds a loose path first.

B. The use of tunneling in ring and mesh topology can be reliable, but MPLS tunneling is more suitable for use in mesh topology because it can provide an alternative solid path.

C. At the time of mpls traffic density has been set at the beginning so it is not possible to occur density.

D. Tunneling MPLS is more suitable for use on established networks because it can provide alternative routes.

References

[1] Ariyanti, Dwi, and Unan Yusmaniar Oktiawati. 2019. "Analisis Perbandingan Performa Traffic Engineering Dengan Resource Reservation Protocol (RSVP) Dan Segment Routing." *Teknika* 8(2): 86–91

[2] Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Scalability evaluation of VOIP over various MPLS tunneling under OPNET modeler. Indian Journal of Science and Technology, 10(29), 1-8.

[3] Fajardo, Jose Oscar, Jon Ander Picó, and Alejandro Muñoz. 2008. "New Tunneling Capabilities for BGP/MPLS IP VPN in GNU/Linux." In *Proceedings - 7th International Conference on Networking, ICN 2008*, Mexico: IEEE, 324–29.

[4] Dumka, Ankur, and Hardwari Lal Mandoria. 2014. "Layer 3 Services Implementation in Different Routers." In *2014 International Conference on Computing for Sustainable Global Development, INDIACom 2014*, India: IEEE, 716–18.

[5] Tamanna, Tasnim, and Tasmiah Fatema. 2018. "MPLS VPN over MGRE Design and Implementation for a Service Provider's Network Using GNS3 Simulator." In *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, IEEE, 2339–4.

[6] Eze, M. N., M. N. C. Ogbu, and S. N. Arinze. 2018. "Security Vulnerability on Multi-Protocol Label Switching in Virtual Private Network." International Journal of Engineering, Science and Mathematics (IJESM) Vol.7: 48-55.

[7] Maheshwarn, S., Lillypet, S., dan Vennila, C. 2016. QOS Capabilities for Building MPLS VPN. *International Journal of Science and Research (IJSR)*, 5(5): 2247-2251.

[8] Song, Z., Prasad, P. A. A. dan Pham, L. E. A. 2016. *Upgrading Internet Service Provider (ISP) Network in Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP) environment*. Putrajaya, Malaysia, IEEE.

[9] Turcanu, D., 2020. "Quality of Services in MPLS Networks." Electronics and Computer Science Computers and Information Technology Vol. XXVII(October): 102-110.

[10] Septarindra, A., Munadi, R., dan Negara, R. M. 2016. "Implementation And Analysis Multi Protocol Label Switching-Virtual Priaver Network (MPLS-VPN) Performance With Generic Routing Encapsulation (GRE) Method On File Transfer Protocol (FLP) Based Services" In *E-Proceeding of Engineering*, , 4504–11.

[11] Allah, A. S. G., El-Fishawy, N. A., & El-Shennawy, N. M. (2017). Admission control algorithm for MPLS-TE networks. International Journal of Computer Applications, 975, 8887.