

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam lingkungan Universitas Islam Sumatera Utara (UISU), Jaringan *Wide Area Network* (WAN) memegang peran yang sangat penting dalam mendukung operasional dan kolaborasi antara fakultas serta unit administratif. Saat ini, UISU masih mengandalkan *routing* statis sebagai metode utama untuk mengelola *rute* komunikasi di jaringannya. Namun, untuk meningkatkan efisiensi dan keandalan jaringan, penelitian ini bertujuan untuk beralih ke Protokol *Routing OSPF (Open Shortest Path First)* sebagai metode *routing* dinamis yang lebih adaptif.

Penggunaan OSPF diantisipasi akan memberikan solusi terhadap beberapa tantangan yang dihadapi dalam penggunaan *routing* statis saat ini. Salah satu masalah utama adalah keterbatasan *fleksibilitas* dan *responsivitas* saat terjadi perubahan dalam topologi jaringan atau penambahan perangkat. OSPF memungkinkan pengenalan otomatis terhadap perubahan ini, mengurangi kebutuhan akan pembaruan manual yang rumit pada setiap *router*. Menurut Nugroho et al., 2023, protokol *routing* OSPF lebih mudah diterapkan karena tidak perlu mendaftarkan atau mengkonfigurasi setiap router ke semua *network* yang menghubungkan *network* asal ke tujuan. Penggunaan topologi WAN juga memiliki kelebihan tersendiri sebagaimana yang ditunjukkan oleh penelitian Rengel et al., 2017, salah satu kelebihan WAN yaitu dapat menghubungkan semua orang dengan menggunakan data lalu lintas yang sama.

Selain itu, pengelolaan skala yang kompleks dalam jaringan UISU dapat diatasi dengan OSPF. Dalam konteks yang melibatkan banyak fakultas dan unit administratif, OSPF memberikan kemampuan untuk mengelola rute secara dinamis, mengurangi kompleksitas administrasi, dan meminimalkan risiko kesalahan konfigurasi.

Kemampuan OSPF dalam mengatasi kegagalan jaringan secara otomatis juga menjadi keunggulan penting. Dalam situasi di mana keandalan jaringan adalah suatu keharusan, OSPF dapat mendeteksi dan merespon kegagalan dengan cepat, meminimalkan waktu henti dan menjaga kelancaran layanan jaringan.

Melalui penelitian ini, diharapkan akan diperoleh pemahaman mendalam tentang kinerja OSPF termasuk pengukuran *delay*, *throughput* dan *packet loss* dalam jaringan UISU. Informasi yang diperoleh dari penelitian ini akan memberikan dasar yang kokoh untuk menerapkan OSPF sebagai metode *routing* dinamis, memastikan bahwa jaringan di UISU tidak hanya efisien dan andal, tetapi juga siap menghadapi tuntutan perubahan dinamis dalam lingkungan akademik dan administratif universitas.

1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini dapat dijelaskan antara lain sebagai berikut :

1. Bagaimana menganalisa kinerja protokol *routing* OSPF pada jaringan di lingkungan UISU?
2. Bagaimana mengukur *delay*, *throughput* dan *packet loss* pada jaringan UISU?

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini antara lain sebagai berikut :

1. Simulasi dilakukan dengan menggunakan perangkat lunak jaringan *Graphical Network Simulator 3*.
2. Simulasi dilakukan dengan menggunakan topologi yang terdapat di UISU dengan masing-masing fakultas mewakili *path* OSPF dinamis yang digunakan.

1.4 Tujuan Penelitian

Berikut beberapa tujuan dalam penelitian ini :

1. Untuk menganalisis kinerja protokol *routing* OSPF pada jaringan UISU dengan menggunakan *Graphical Network Simulator 3*.
2. Mengidentifikasi faktor-faktor yang mempengaruhi kinerja protocol *routing* OSPF dalam jaringan UISU.
3. Untuk mengukur dan menganalisis *delay*, *throughput* dan *packet loss* dalam jaringan UISU menggunakan alat bantu pengukuran yang disediakan oleh *Graphical Network Simulator 3*.

1.5 Manfaat Penelitian

Berikut merupakan manfaat dari penelitian ini :

1. Kontribusi dalam Bidang Penelitian: Penelitian ini akan memberikan kontribusi dalam bidang penelitian jaringan komputer, khususnya pada analisis kinerja protokol *routing* OSPF dalam konteks jaringan di UISU. Temuan dan rekomendasi dari penelitian ini dapat menjadi dasar untuk pengembangan penelitian lebih lanjut dalam bidang ini.
2. Pengoptimalan Konfigurasi Jaringan: Melalui pengukuran kinerja dan analisis yang dilakukan, penelitian ini akan memberikan pemahaman yang lebih baik tentang faktor-faktor yang mempengaruhi kinerja protokol *routing* OSPF

dalam jaringan UISU. Dengan demikian, penelitian ini dapat membantu para profesional jaringan dalam melakukan pengoptimalan konfigurasi jaringan mereka untuk mencapai kinerja yang lebih baik.

3. Peningkatan Kualitas Layanan Jaringan: Dengan pemahaman yang lebih baik tentang *delay*, *throughput* dan *packet loss* dalam jaringan UISU, penelitian ini akan memberikan wawasan yang berharga bagi penyedia layanan jaringan atau organisasi yang mengelola jaringan mereka sendiri. Rekomendasi yang dihasilkan dapat digunakan untuk meningkatkan kualitas layanan jaringan, mengurangi gangguan, dan meningkatkan kepuasan pengguna.
4. Pengembangan Strategi Redudansi: Penelitian ini juga akan membahas strategi redudansi sederhana dengan penambahan dan penonaktifan *router* dalam jaringan UISU. Hal ini akan memberikan pemahaman tentang efektivitas strategi redudansi dalam meningkatkan kinerja jaringan dan kehandalan layanan. Informasi ini dapat membantu organisasi dalam merancang dan mengimplementasikan strategi redudansi yang sesuai dengan kebutuhan mereka.
5. Penerapan Praktis dengan *Graphical Network Simulator 3*: Penelitian ini menggunakan *Graphical Network Simulator 3* sebagai alat simulasi. Dengan demikian, penelitian ini juga akan memberikan manfaat praktis bagi para praktisi jaringan yang menggunakan atau berencana menggunakan *Graphical Network Simulator 3* sebagai alat untuk menguji dan mengoptimalkan jaringan UISU.

1.6 Sistematika Penulisan

Skripsi ini disusun dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab pertama ini merupakan pendahuluan yang berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan ruang lingkup penelitian. Pendahuluan ini bertujuan untuk memberikan gambaran umum tentang topik penelitian, mengidentifikasi masalah yang akan dipecahkan, serta memberikan pemahaman tentang pentingnya penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab kedua ini berisi kajian teori yang relevan dengan penelitian ini. Pada bagian ini, akan diulas konsep-konsep dasar mengenai jaringan *Wide Area Network* (WAN), protokol *routing* OSPF, pengukuran kinerja jaringan, konfigurasi perangkat jaringan, verifikasi konektivitas, dan analisis redundansi.

BAB III METODE PENELITIAN

Bab ini berisi metodologi penelitian yang menjelaskan tentang metode yang digunakan dalam penelitian ini. Metodologi meliputi pendekatan penelitian, jenis data yang dikumpulkan serta teknik analisis data. Dalam bab ini, juga akan dijelaskan langkah-langkah yang dilakukan dalam melakukan pengujian, pengukuran kinerja, dan evaluasi redundansi.

BAB IV HASIL PENELITIAN

Bab ini merupakan hasil penelitian yang berisi presentasi dan analisis data yang telah dikumpulkan. Hasil penelitian ini akan meliputi pengukuran kinerja jaringan, verifikasi konektivitas, dan evaluasi redundansi. Data yang diperoleh akan dianalisis secara kuantitatif dan dijelaskan secara terperinci untuk menjawab rumusan masalah yang telah diajukan.

BAB V KESIMPULAN DAN SARAN

Bab kelima adalah kesimpulan dan rekomendasi. Pada bagian ini, akan disajikan rangkuman temuan-temuan penting dari penelitian, diikuti oleh kesimpulan yang dapat diambil berdasarkan analisis data. Selain itu, rekomendasi praktis juga akan diberikan sebagai panduan untuk meningkatkan kinerja protokol *routing* OSPF dalam jaringan berdasarkan temuan peneliti.

BAB II

TINJAUAN PUSTAKA

2.1 Jaringan Komputer

2.1.1 Pengertian Jaringan

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Jaringan komputer terdiri dari perangkat lunak, perangkat keras dan media penghubung yang ketiganya saling terintegrasi satu sama lainnya (Haries ,et al. 2022).

2.1.2 Sejarah Jaringan

Sejarah jaringan komputer dimulai pada tahun 1940-an di Amerika Serikat ketika sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan grup riset Universitas Harvard yang dipimpin oleh profesor Howard Aiken mulai mengembangkan konsep jaringan komputer. Pada awalnya, proyek tersebut hanya ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian (Arif, 2019).

Namun, jaringan komputer yang kita kenal saat ini baru berkembang pada tahun 1960-an ketika Departemen Pertahanan Amerika Serikat mengembangkan jaringan komputer yang disebut ARPANET (*Advanced Research Projects Agency Network*) untuk menghubungkan beberapa universitas dan lembaga penelitian. ARPANET kemudian menjadi cikal bakal internet yang kita kenal saat ini (Pamungkas et al., 2018).

Sejak itu, jaringan komputer terus berkembang dan semakin kompleks. Pada tahun 1980-an, jaringan komputer mulai digunakan secara luas di perusahaan dan institusi pemerintah. Pada tahun 1990-an, internet mulai populer di kalangan masyarakat umum dan menjadi salah satu teknologi yang paling berpengaruh di dunia saat ini (Wijayanti S., 2021).

2.1.3 Jenis-Jenis Jaringan

Menurut Purigawati (2020) jika dilihat dari cakupan areanya jaringan memiliki beberapa jenis yang terdiri dari :

a. *Local Area Network (LAN)*

Jaringan area lokal (LAN) dirancang untuk menghubungkan komputer pribadi dan perangkat digital lainnya dalam radius setengah mil atau 500 meter. LAN biasanya menghubungkan beberapa komputer di kantor kecil, semua komputer di satu gedung, atau semua komputer di beberapa bangunan di dekat tempat itu.

b. *Metropolitan Area Network (MAN)*

Jaringan area metropolitan (MAN) adalah jaringan yang membentang di wilayah metropolitan, biasanya kota dan pinggiran kota utamanya. Lingkup geografisnya berada di antara WAN dan LAN.

c. *Wide Area Network (WAN)*

Jaringan area luas (WAN) menjangkau jarak geografis yang luas-seluruh wilayah, negara bagian, benua, atau seluruh dunia. WAN yang paling universal dan bertenaga adalah Internet. Komputer terhubung ke WAN melalui jaringan publik, seperti sistem telepon atau sistem kabel pribadi, atau melalui jalur sewa atau satelit.

2.2 Topologi

2.2.1 Pengertian Topologi

Topologi merupakan suatu tatanan untuk menghubungkan beberapa komputer atau perangkat-perangkat jaringan yang digunakan menjadi suatu jaringan yang saling terhubung (Alvionita, 2019). Jaringan komputer dapat diatur dalam berbagai topologi, masing-masing dengan keunggulan dan kelemahan uniknya.

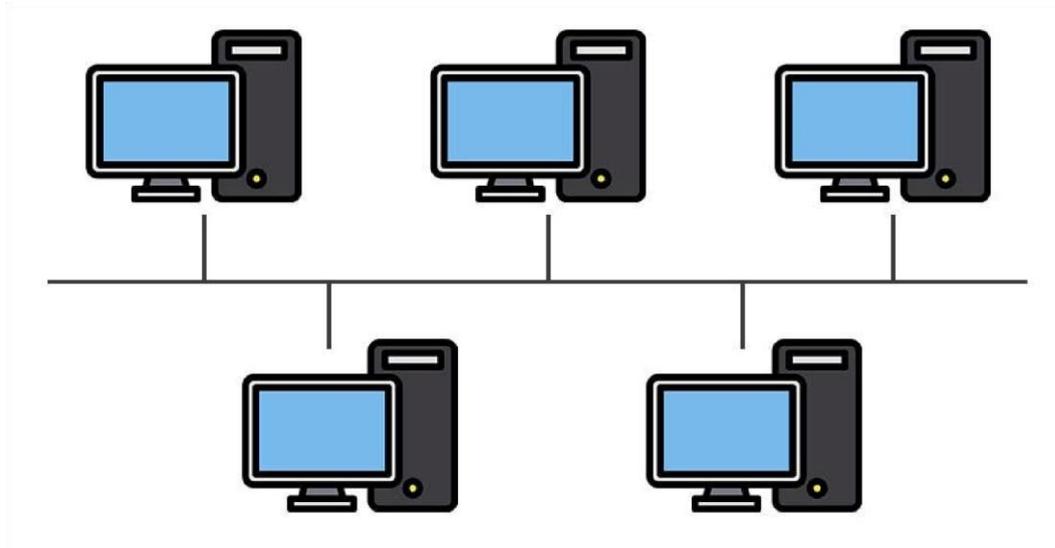
2.2.2 Jenis-Jenis Topologi

Menurut Artha et al (2023) topologi terbagi atas beberapa jenis yaitu Topologi *Point-to-Point* menghubungkan dua perangkat secara langsung, membentuk koneksi khusus antara keduanya seperti gambar 2.1 dibawah ini.



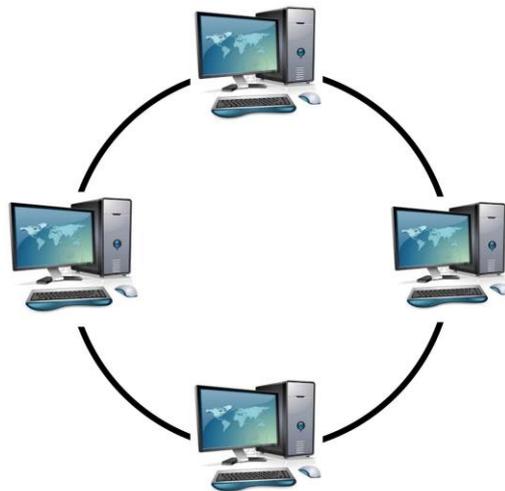
Gambar 2. 1 Topologi Point-to-point

Sementara itu, topologi Bus menghubungkan semua perangkat ke saluran komunikasi bersama, memungkinkan data yang dikirim oleh satu perangkat dapat mencapai semua perangkat lain seperti gambar 2.2 dibawah.



Gambar 2. 2 Topologi Bus Point-to-point

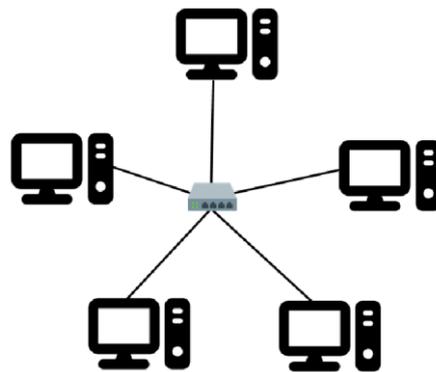
Walaupun efisien secara biaya, topologi *bus* rentan terhadap kegagalan jaringan karena satu kerusakan pada saluran komunikasi dapat mempengaruhi seluruh jaringan.



Gambar 2. 3 Topologi Ring

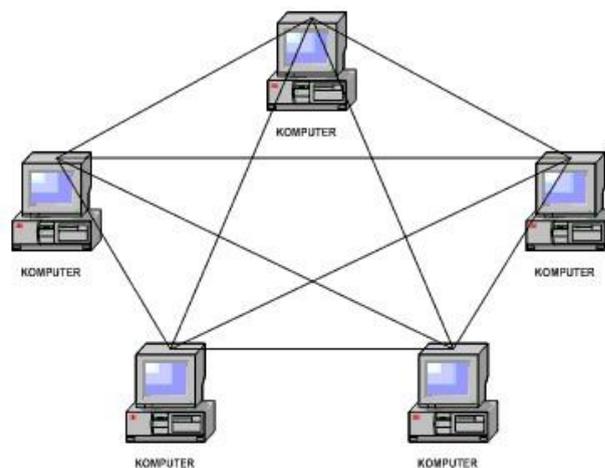
Sebaliknya, dalam topologi Ring seperti yang ditunjukkan oleh gambar 2.3 diatas, perangkat dihubungkan dalam pola melingkar, di mana data bergerak dalam satu arah, melewati setiap perangkat hingga mencapai penerima yang dituju. Meskipun memberikan transmisi data yang efisien, topologi Ring dapat terpengaruh oleh kegagalan satu tautan, mengakibatkan terputusnya jaringan.

Sementara itu, dalam topologi Star, semua perangkat terhubung ke satu pusat (*switch* atau *hub*), memastikan keandalan dan skalabilitas jaringan. Namun, jika pusat tersebut mengalami masalah, hanya perangkat yang terhubung padanya yang terpengaruh seperti yang terlihat pada gambar 2.4 dibawah.



Gambar 2. 4 Topologi Star

Disisi lain, topologi Mesh pada gambar 2.5 dibawah menghubungkan perangkat secara penuh, meningkatkan redundansi dan toleransi kesalahan, membuatnya cocok untuk jaringan berukuran besar.



Gambar 2. 5 Topologi Mesh

Terakhir, topologi *Hybrid* menggabungkan beberapa jenis topologi, menciptakan jaringan yang lebih fleksibel dan efisien dengan kemampuan toleransi kesalahan dan skalabilitas yang lebih baik. Pemilihan topologi harus mempertimbangkan kebutuhan khusus jaringan tersebut, memastikan bahwa

struktur jaringan mendukung kehandalan, biaya efisiensi, serta kemampuan untuk mengatasi kesalahan dan perkembangan jaringan yang masa depan (Artha et al., 2023).

2.3 Protokol Routing OSPF

2.3.1 Prinsip Kerja OSPF

OSPF (*Open Shortest Path First*) adalah protokol *routing* yang digunakan dalam jaringan komputer untuk menghitung dan memilih jalur terpendek antara dua node dalam jaringan. Berikut ini adalah prinsip kerja OSPF:

1. Algoritma Dijkstra : OSPF menggunakan algoritma Dijkstra untuk menghitung jalur terpendek antara dua *node* dalam jaringan (Retnani et al., 2022). Algoritma ini menghitung jalur dengan mempertimbangkan bobot atau metrik yang diatur pada setiap link jaringan. Metrik ini dapat berupa *bandwidth, delay, throughput*, atau kombinasi dari faktor-faktor tersebut.
2. *Routing Hierarchy*: OSPF menggunakan struktur hierarkis dalam penyebaran informasi routing (Retnani et al., 2022). Jaringan OSPF dibagi menjadi area-area yang saling terhubung. Setiap area memiliki satu atau lebih router yang bertindak sebagai *Area Border Router (ABR)* untuk menghubungkan area-area tersebut. ABR bertanggung jawab untuk mentransmisikan informasi routing antara area-area yang berbeda.
3. *Link State Database (LSDB)*: Dalam OSPF, router dan sistem yang berada dalam area yang sama mempertahankan *database link-state* yang serupa, yang memuat informasi topologi area tersebut. Setiap router di dalam area tersebut membentuk Database Status Tautan dari Pengumuman Status

Tautan (LSA) yang diterimanya dari semua router dalam area yang sama (Jannah et al., 2023)

4. *Shortest Path First (SPF) Calculation*: Setiap router OSPF menggunakan algoritma SPF (*Shortest Path First*) untuk menghitung jalur terpendek ke setiap tujuan dalam jaringan. Algoritma SPF menggunakan informasi dalam LSDB untuk menentukan jalur terpendek dengan mempertimbangkan metrik *link*.
5. *Sinkronisasi Database*: OSPF menggunakan proses sinkronisasi untuk memastikan bahwa *database* LSDB di setiap router dalam jaringan OSPF konsisten. Router secara periodik bertukar informasi *database* dengan router tetangganya dan memperbarui *database* mereka sesuai dengan perubahan topologi.

2.3.2 Pengaturan OSPF

Pengaturan OSPF melibatkan konfigurasi protokol OSPF pada perangkat jaringan yang terlibat dalam jaringan *Wide Area Network* (WAN). Berikut ini adalah beberapa pengaturan umum yang perlu dipertimbangkan saat mengkonfigurasi OSPF:

1. *Area OSPF*: Jaringan OSPF biasanya dibagi menjadi beberapa area untuk mempermudah manajemen dan skalabilitas. Konfigurasi OSPF menggunakan area *backbone* atau area 0 dengan wajib mendaftarkan area router yang berada di bawahnya berdasarkan alamat sesuai main router dan backup router (Mudhoep et al., 2021).

2. *Hello Packet* dan *Dead Interval*: OSPF menggunakan pesan Hello untuk menjaga konektivitas antara router dalam jaringan OSPF. Anda perlu mengatur
3. *Hello Interval*, yaitu interval waktu antara pengiriman pesan Hello, dan *Dead Interval*, yaitu interval waktu di mana *router* menganggap tetangganya tidak aktif jika tidak menerima pesan Hello. Pengaturan ini mempengaruhi deteksi kegagalan dan pemulihan link dalam jaringan (Karamela et al., 2023).
4. *Expense* : Dalam konteks OSPF, biaya dihitung berdasarkan *bandwidth* antarmuka. Semakin tinggi *bandwidth*, semakin rendah biaya, yang berarti jalur dengan *bandwidth* yang lebih tinggi memiliki biaya lebih rendah dan menjadi jalur yang diinginkan. Biaya adalah parameter yang diberikan kepada setiap antarmuka router dalam jaringan OSPF, dan OSPF akan memilih jalur dengan biaya terendah untuk mencapai tujuan (Karamela et al., 2023).

2.4 Pengukuran Kinerja Jaringan

Pengukuran kinerja jaringan adalah proses mengukur dan menganalisis parameter kinerja yang relevan dalam jaringan komputer. Hal ini dilakukan untuk memahami kualitas, efisiensi, dan keandalan jaringan. Beberapa parameter kinerja yang umum diukur dalam jaringan meliputi :

1. *Delay* adalah total waktu untuk mengirimkan satu paket data dari pengirim ke penerima. *Delay* yang sering dialami oleh *traffic* yang lewat adalah *delay* transmisi (Iryani et al., 2021). Persamaan untuk menghitung *delay* adalah sebagai berikut.

$$Delay(ms) = WaktuPaketDiterima - WaktuPaketDikirim$$

2. *Throughput* : *Throughput* adalah ukuran jumlah data yang berhasil ditransmisikan melalui jaringan dalam suatu periode waktu. Faktor-faktor seperti kepadatan jaringan dan overhead protokol mempengaruhi *throughput*. Ini diukur dalam unit yang sama dengan *bandwidth*, seperti kbps atau Mbps, dan mengindikasikan efisiensi sebenarnya dari transmisi data melalui jaringan. Pengelola jaringan menggunakan informasi *throughput* untuk mengoptimalkan kinerja jaringan dan memastikan transmisi data yang efisien (Artha et al., 2023). Persamaan untuk *throughput* adalah sebagai berikut.

$$Throughput(byte) = \frac{TotalDataYangDiterima}{LamaPengamatan}$$

3. *Packet Loss* (Kehilangan Paket): *Packet loss* adalah parameter yang mengindikasikan jumlah data yang hilang selama proses pengiriman data. Ini terjadi ketika paket-paket data yang dikirim melalui jaringan tidak sampai ke tujuan secara utuh atau hilang selama perjalanan. Jumlah *packet loss* mencerminkan seberapa efisien jaringan dalam mengirim data, dan tingkat yang rendah diinginkan untuk memastikan keandalan dan kualitas transmisi data (Alvionita, 2019). Persamaan yang digunakan untuk mencari *packet loss* adalah sebagai berikut.

$$PacketLoss(\%) = \frac{(PaketDataDikirim - PaketDataDiterima) * 100\%}{PaketDataDikirim}$$

Pengukuran kinerja jaringan dilakukan dengan menggunakan alat bantu pengukuran yang biasanya menyediakan informasi tentang *delay*, *throughput* dan

packet loss. Alat-alat ini dapat berupa perangkat lunak jaringan khusus, perangkat pemantau jaringan, atau fitur yang disediakan oleh perangkat jaringan itu sendiri.

2.5 Konfigurasi Perangkat Jaringan

2.5.1 Konfigurasi OSPF pada Router

Konfigurasi OSPF pada router melibatkan langkah-langkah untuk mengaktifkan protokol OSPF dan mengatur parameter OSPF yang diperlukan. OSPF *routing* membagi jaringan pada beberapa level dan setiap tingkatan dibagi menjadi beberapa kelompok (Diansyah et al., 2019). Berikut ini adalah langkah-langkah umum untuk melakukan konfigurasi OSPF pada router:

1. Mengaktifkan OSPF: Pertama, Anda perlu mengaktifkan protokol OSPF pada router. Hal ini dilakukan dengan menggunakan perintah konfigurasi di mode konfigurasi *router*. Misalnya, di Cisco IOS, perintah untuk mengaktifkan OSPF adalah sebagai berikut:

```
# router ospf <process-id>
```

Di sini, *<process-id>* adalah identifikasi unik untuk proses OSPF pada *router*. Anda dapat memilih nilai process ID sesuai kebutuhan Anda.

2. Mengkonfigurasi Area OSPF: Setelah mengaktifkan OSPF, Anda perlumenentukan area OSPF untuk *router*. Setiap *router* OSPF harus ditempatkan dalam area OSPF yang sesuai. Perintah untuk mengkonfigurasi area OSPF adalah sebagai berikut:

```
# network <network-address> <wildcard-mask> area <area-id>
```

Di sini, *<network-address>* adalah alamat jaringan yang terhubung ke *router*, *<wildcard-mask>* adalah masker *wildcard* yang sesuai, dan

<area-id> adalah ID area OSPF yang sesuai dengan konfigurasi jaringan Anda.

3. Mengatur *Authentication* (Opsional): Jika Anda ingin meningkatkan keamanan OSPF, Anda dapat mengatur autentikasi pada router. Ini memastikan bahwa hanya router dengan autentikasi yang benar yang dapat berpartisipasi dalam OSPF. Untuk mengatur autentikasi, Anda dapat menggunakan metode autentikasi seperti autentikasi *password* atau autentikasi menggunakan kunci kriptografis.
4. Mengkonfigurasi *Metric dan Cost*: Anda dapat mengatur *metric* atau *cost* pada antarmuka jaringan yang terhubung ke router OSPF. Metrik digunakan oleh OSPF untuk memilih jalur terpendek dalam jaringan. Anda dapat mengatur metrik dengan menggunakan perintah seperti:

```
# ip ospf cost <cost-value>
```

Di sini, *<cost-value>* adalah nilai *cost* yang Anda terapkan untuk antarmuka jaringan tertentu. Semakin rendah *cost*, semakin disukai jalur tersebut dalam pemilihan jalur OSPF.

5. Mengonfigurasi Redistribusi (Opsional): Jika Anda menggunakan protokol *routing* lain dalam jaringan Anda, seperti RIP dan EIGRP, Anda dapat mengkonfigurasi redistribusi untuk berbagi informasi *routing* antara protokol yang berbeda. Hal ini memungkinkan *router* OSPF untuk menerima *rute* dari protokol *routing* lain dan mengumumkannya dalam jaringan OSPF.

2.5.2 Pengaturan Antarmuka Jaringan

Pengaturan antarmuka jaringan pada *router* dalam konteks konfigurasi OSPF melibatkan langkah-langkah untuk mengkonfigurasi parameter OSPF pada antarmuka yang terhubung ke jaringan. Berikut ini adalah langkah-langkah umum untuk melakukan pengaturan antarmuka jaringan:

1. Identifikasi Antarmuka: Pertama, identifikasi antarmuka yang akan dikonfigurasi. Ini melibatkan mengetahui nomor atau nama antarmuka yang ingin Anda konfigurasi dalam konteks OSPF.
2. Aktifkan OSPF pada Antarmuka: Mengaktifkan OSPF pada antarmuka yang terhubung ke jaringan adalah langkah penting. Perintah untuk mengaktifkan OSPF pada antarmuka adalah sebagai berikut:

```
# interface <interface-name>
```

```
# ip ospf <process-id> area <area-id>
```

Di sini, *<interface-name>* adalah nama atau nomor antarmuka yang akan diaktifkan OSPF, *<process-id>* adalah identifikasi unik untuk proses OSPF yang sama dengan yang ditentukan pada konfigurasi OSPF pada router, dan *<area-id>* adalah ID area OSPF yang sesuai dengan konfigurasi area OSPF yang telah ditentukan.

3. Mengatur *Network Type*: Setiap antarmuka jaringan harus dikonfigurasi dengan tipe jaringan yang sesuai. Tipe jaringan menggambarkan karakteristik fisik dan protokol yang digunakan dalam antarmuka tersebut. Tipe jaringan umum untuk OSPF meliputi:
 - a) *Broadcast*: Untuk antarmuka yang terhubung ke jaringan yang mendukung pemancaran paket.

- b) *Point-to-Point*: Untuk antarmuka yang terhubung ke jaringan *point-to-point*.
- c) *Non Broadcast Multiaccess* (NBMA): Untuk antarmuka yang terhubung ke jaringan NBMA seperti Frame Relay atau ATM.
- d) *Point-to-Multipoint*: Untuk antarmuka yang terhubung ke jaringan *point-to-multipoint* seperti *hub and spoke*. Perintah untuk mengatur tipe jaringan pada antarmuka adalah sebagai berikut:

```
# interface <interface-name>
```

```
# ip ospf network <network-type>
```

Di sini, *<interface-name>* adalah nama atau nomor antarmuka yang akan dikonfigurasi, dan *<network-type>* adalah tipe jaringan yang sesuai dengan jenis antarmuka yang digunakan.

4. Menentukan *Hello* dan *Dead Intervals*: *Hello Interval* adalah interval waktu antara pengiriman pesan Hello oleh antarmuka OSPF, sementara *Dead Interval* adalah interval waktu di mana *router* menganggap tetangganya tidak aktif jika tidak menerima pesan Hello. Anda dapat mengatur nilai ini pada antarmuka yang terhubung ke jaringan menggunakan perintah:

```
# interface <interface-name>
```

```
# ip ospf hello-interval <interval-value>
```

```
# ip ospf dead-interval <interval-value>
```

Di sini, *<interface-name>* adalah nama atau nomor antarmuka yang akan dikonfigurasi, dan *<interval-value>* adalah nilai *interval* yang Anda tentukan dalam detik.

5. Autentikasi (Opsional): Jika Anda ingin menggunakan autentikasi OSPF pada antarmuka, Anda dapat mengatur autentikasi menggunakan perintah yang sesuai, seperti autentikasi *password* atau autentikasi menggunakan kunci *kriptografis*. Autentikasi dapat membantu meningkatkan keamanan OSPF di antarmuka tersebut. Konfigurasi untuk setiap perangkat dilakukan agar pertukaran *routing table* di dalamnya tidak menjadi kacau ketika terdapat salah satu *interface* yang *down* (Rahmawati & Mutiara Anjani, 2023).

2.5.3 Pemetaan Jaringan

Pemetaan jaringan (*network mapping*) adalah proses untuk mendapatkan pemahaman menyeluruh tentang struktur, topologi, dan elemen-elemen yang ada dalam jaringan komputer dan juga untuk mendukung konsep hirarki *routing* dengan membagi jaringan menjadi beberapa tingkatan yang diwujudkan dengan sistem pengelompokan wilayah (Retnani et al., 2022). Hal ini melibatkan identifikasi, dokumentasi, dan visualisasi komponen-komponen jaringan, termasuk perangkat keras (*hardware*), perangkat lunak (*software*), koneksi, dan sumber daya jaringan lainnya. Berikut adalah beberapa langkah yang umum dilakukan dalam pemetaan jaringan:

1. Identifikasi Komponen Jaringan : Identifikasi dan dokumentasikan semua perangkat keras dan perangkat lunak yang ada dalam jaringan. Ini mencakup *server*, *switch*, *router*, *firewall*, perangkat jaringan lainnya, serta sistem operasi, aplikasi, dan layanan yang dijalankan pada setiap perangkat.

2. Dokumentasikan Koneksi : Catat semua koneksi fisik antara perangkat jaringan, baik kabel fisik maupun koneksi nirkabel. Identifikasi jalur koneksi, tipe koneksi (*Ethernet, fiber optic, Wi-Fi*, dll.), dan perangkat yang terhubung pada setiap ujung koneksi.
3. Identifikasi Alamat IP dan *Subnet* : Catat semua alamat IP yang digunakan dalam jaringan beserta subnet *mask*-nya. Ini melibatkan identifikasi alamat IP yang diberikan kepada setiap perangkat dan subnet yang terbentuk dalam jaringan.
4. Identifikasi Layanan dan Aplikasi : Dokumentasikan semua layanan dan aplikasi yang dijalankan dalam jaringan, seperti *web server, email server, database server*, dan sebagainya. Catat juga port yang digunakan oleh setiap layanan atau aplikasi.
5. Visualisasi Topologi Jaringan : Gunakan perangkat lunak pemetaan jaringan atau alat bantu lainnya untuk membuat visualisasi topologi jaringan. Ini dapat berupa diagram yang menunjukkan hubungan antara perangkat dan koneksi dalam jaringan. Diagram ini membantu memahami hubungan fisik dan logis antara elemen-elemen jaringan.

2.6 Verifikasi Konektivitas

2.6.1 Pengujian *Ping*

Pengujian *Ping* adalah metode yang umum digunakan untuk menguji konektivitas dan mengukur *delay* dalam jaringan komputer. Pengujian ini menggunakan protokol ICMP (*Internet Control Message Protocol*) untuk mengirim paket pesan ke tujuan tertentu dan menerima responnya. Berikut adalah langkah-langkah umum untuk melakukan pengujian *Ping*:

1. Buka *command prompt* atau terminal pada perangkat Anda.
2. Ketik perintah "*ping*" diikuti dengan alamat IP atau nama host tujuan yang ingin Anda uji. Misalnya:

```
# ping 192.168.0.1
```

3. Tekan tombol *Enter* untuk menjalankan perintah *Ping*. Sistem akan mengirimkan serangkaian paket ICMP ke tujuan dan menunggu responnya.
4. Perangkat akan mulai menerima respons dari tujuan. Setiap respons akan menampilkan waktu yang diperlukan (dalam milidetik) untuk paket pergi dan kembali. Anda juga akan melihat jumlah paket yang hilang, jika ada.
5. Biarkan pengujian berjalan selama beberapa saat untuk mengumpulkan cukup sampel respons.
6. Setelah cukup waktu, Anda dapat mematikan pengujian dengan menekan tombol *Ctrl + C*. Setelah pengujian dihentikan, Anda akan melihat ringkasan statistik, termasuk persentase paket yang hilang, waktu rata-rata (avg), dan lainnya.

2.6.2 Pengujian *Traceroute*

Pengujian *Traceroute* adalah metode yang digunakan untuk memberi perintah untuk menunjukkan rute yang dilewati paket untuk mencapai tujuan dengan melakukan pengiriman pesan *Internet Control Message Protocol (ICMP) Echo Request* ke tujuan dengan nilai *Time to Live* yang semakin meningkat (Karamela et al., 2023). Metode ini membantu dalam mengetahui *hop-hops* atau titik-titik antara sumber dan tujuan, serta menunjukkan *delay* pada masing-masing *hop*.

Berikut ini adalah langkah-langkah umum untuk melakukan pengujian *traceroute*:

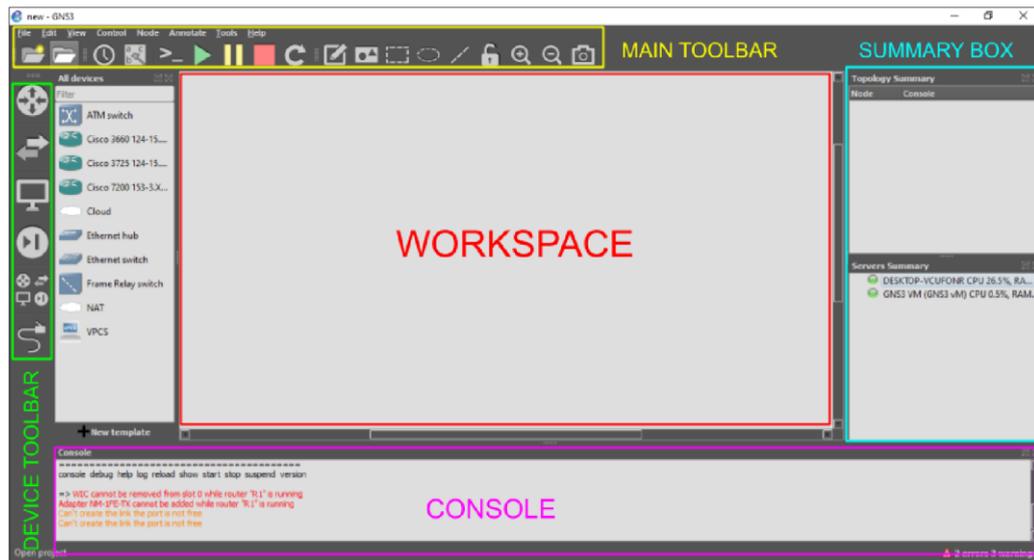
1. Buka *command prompt* atau terminal pada perangkat Anda.
2. Ketik perintah "*traceroute*" diikuti dengan alamat IP atau nama host tujuan yang ingin Anda lacak. Misalnya :

```
# traceroute 192.168.0.1
```

3. Tekan tombol Enter untuk menjalankan perintah *Traceroute*. Sistem akan mengirimkan serangkaian paket ICMP dengan TTL (*Time-to-Live*) yang berturut-turut meningkat.
4. Setiap *hop* atau titik antara sumber dan tujuan akan merespons dengan informasi tentang waktu yang diperlukan (dalam milidetik) untuk paket mencapai *hop* tersebut. Anda juga akan melihat alamat IP *hop* tersebut.
5. *Traceroute* akan melanjutkan langkah 3 dan 4 hingga mencapai tujuan atau hingga batas TTL tercapai.
6. Setelah *traceroute* selesai, Anda akan melihat daftar *hop* yang dilalui beserta waktu respons dan alamat IP masing-masing *hop*.

2.7 *Graphical Network Simulator 3*

GNS3 atau *Graphical Network Simulator-3*, adalah perangkat lunak simulasi jaringan yang memberikan pengguna kemampuan untuk membuat dan menguji topologi jaringan secara virtual. Dengan antarmuka *grafis* intuitif, pengguna dapat dengan mudah membuat simulasi perangkat keras jaringan seperti *router*, *switch*, dan *firewall*. Keunggulan GNS3 terletak pada interoperabilitasnya dengan perangkat keras jaringan nyata, memungkinkan integrasi yang mulus untuk pengujian yang lebih realistis.



Gambar 2. 6 Interface GNS3

Pada gambar diatas terdapat beberapa elemen penting yang membantu pengguna dalam merancang dan mengelola topologi jaringan virtual. Pertama adalah "*Device Toolbar*," yang berfungsi sebagai tempat untuk memilih dan menambahkan perangkat jaringan seperti *router*, *switch*, dan *firewall* ke dalam area kerja simulasi. Kemudian, "*Main Toolbar*" menyediakan akses cepat ke fungsi utama, seperti menyimpan dan membuka proyek, mengelola preferensi, serta mengontrol proses simulasi. Sementara itu, "*Summary Box*" memberikan gambaran singkat tentang konfigurasi dan status perangkat yang dipilih, termasuk informasi seperti *IP address* dan *MAC address*. Terakhir, "*Console*" adalah jendela konsol yang memungkinkan pengguna berinteraksi langsung dengan perangkat, membuka sesi konsol, dan mengkonfigurasi perangkat melalui antarmuka baris perintah. Elemen-elemen ini bekerja sama untuk memberikan pengalaman pengguna yang lebih baik dalam merancang, menguji, dan mengelola topologi jaringan virtual menggunakan GNS3.

2.8 Gambaran Umum Universitas Islam Sumatera Utara (UISU)

2.8.1 Profil Universitas Islam Sumatera Utara

Universitas Islam Sumatera Utara disingkat UISU didirikan pada tanggal 7 Januari 1951, merupakan perguruan tinggi pertama yang berdiri di luar pulau Jawa, yang dipelopori oleh tokoh pemuda pemudi islam saat itu, yaitu Bahrum Djamil, Adnan Benawi, Sariani AS, Rivai Abdul Manaf Nasution, dan Sabaruddin Ahmad. UISU pada mulanya membuka kelas persiapan Akademi Islam Indonesia (setara dengan kelas III SMA bagian A) dan selanjutnya dengan dukungan Bapak Abd. Hakim (Gubernur Sumatera Utara saat itu) dan Bapak K.H. A. Wahid Hasyim (Menteri Agama saat itu) Akademi Islam Indonesia diubah menjadi Perguruan Tinggi Islam Indonesia (PTII) dan dimulailah peresmian kegiatan perkuliahan pertama pada 7 Januari 1952 pada Fakultas Hukum dan Ilmu Kemasyarakatan. Selanjutnya tanggal 7 Januari 1952 Miladiah bertepatan 9 Rabiul Awal 1371 Hijriah dijadikan sebagai hari jadi PTII yang selanjutnya berubah menjadi Universitas Islam Sumatera Utara dan mendapatkan pengesahan dari Mendikbud RI No. 0677/U/1977 tanggal 31 Desember 1977.

Dengan perjuangan dan tekad yang kuat dari seluruh sivitas akademika UISU dan dukungan dari pemerintah, ulama dan masyarakat, saat ini UISU mengelola 9 Fakultas dan 26 Program Studi S-1, 3 Program Studi S-2, dan 1 Program Studi S-3 Ilmu Ekonomi dan Kebijakan kerjasama UISU dengan UII Yogyakarta.

Fakultas dan Program Studi yang dibina antara lain Hukum, Agama Islam, Ekonomi, Sastra Inggris, Keguruan dan Ilmu Pendidikan, Ilmu Sosial dan Ilmu Politik, Pertanian, Kedokteran, Teknik dan Pascasarjana.

2.8.2 Profil Universitas Islam Sumatera Utara

Fakultas Teknik Universitas Islam Sumatera Utara (FT-UISU) didirikan pada tahun 1981 adalah salah satu fakultas dari 9 (sembilan) fakultas yang ada di Universitas Islam Sumatera Utara. Fakultas Teknik merupakan fakultas yang terakhir dibuka pada saat UISU didirikan. Pada perkembangannya, Program Studi pertama di FT adalah Jurusan Teknik Mesin, Teknik Elektro dan Teknik Sipil. Kemudian pada tahun 1983 berdiri Program Studi baru yaitu Program Studi Teknik Industri. Dilanjutkan pada tahun 2003 berdiri Program Studi Teknik Informatika.

2.8.3 Visi, Misi Dan Tujuan UISU

Visi : Menjadi UISU yang islami, Andal, Teruji, dan Bermartabat Mulia, dicintai oleh Masyarakat dan diridhai Allah SWT

Misi : 1. Melaksanakan proses pembelajaran sesuai dengan standar Nasional Perguruan Tinggi berorientasi pada kebutuhan masyarakat dalam bidang Ilmu Pengetahuan dan Teknologi,serta melaksanakan Penelitian dan Pengabdian Masyarakat serta 27 Dakwah Islamiah secara profesional guna meningkatkan taraf hidup masyarakat, Bangsa dan umat manusia.

2. Membentuk Sarjana Teknik yang Islami Nasionalis, berkualitas ber Iman dan ber Taqwa, berakhlak mulia, berilmu dan beramal saleh, turut berperan dalam pembangunan umat Islam, agama Bangsa dan Negara Republik Indonesia demi kemaslahatan dan kesejahteraan umat manusia.

3. Membentuk Sarjana Teknik yang Islami Nasionalis, berkualitas ber Iman dan ber Taqwa, berahlak mulia, berilmu dan beramal saleh, turut berperan dalam pembangunan umat Islam, agama Bangsa dan Negara Republik Indonesia demi kemaslahatan dan kesejahteraan umat manusia.

Tujuan : 1. Menghasilkan Sarjana Teknik di bidang Ilmu Pengetahuan dan Teknologi yang unggul, andal, teruji dan kompetitif yang berkarakter Islami.

2. Menghasilkan karya yang inovatif untuk meningkatkan mutu pendidikan demi kemaslahatan umat.

3. Menghasilkan Sarjana Teknik yang dapat mengabdikan Ilmu Pengetahuan dan Teknologi untuk kemaslahatan masyarakat.

4. Meningkatkan Kompetensi dan Profesionalisme Dosen serta tenaga kependidikan.

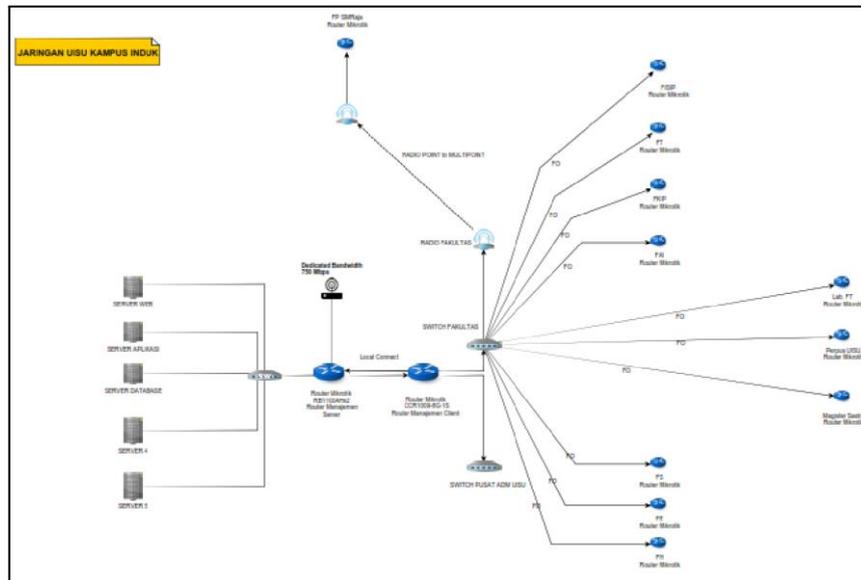
5. Meningkatkan peran aktif alumni dalam membantu pemerintah, masyarakat dan *stakeholder* melalui Pengabdian Kepada Masyarakat (PKM) dengan cara menciptakan metode dan teknik yang maju.

6. Dapat menjadi panutan dalam penerapan nilai nilai Islami di tengah masyarakat melalui Dakwah Islamiyah.

2.8.4 Topologi Jaringan UISU

Topologi jaringan menjadi salah satu aspek kritis dalam merancang suatu sistem komunikasi dan pertukaran data. Pemilihan topologi yang tepat dapat memastikan kelancaran aliran informasi, ketersediaan layanan, serta keamanan data di seluruh lingkungan kampus. Topologi jaringan juga harus mampu

menyesuaikan diri dengan kompleksitas kebutuhan pengguna, mulai dari mahasiswa, dosen, hingga staf administrasi. Berikut topologi yang digunakan pada Universitas Islam Sumatera Utara.



Gambar 2. 7 Topologi Jaringan UISU

Pada gambar diatas dapat diketahui bahwa Universitas Islam Sumatera Utara memiliki 5 buah *server* yang terdiri dari *Server Web*, *Server Aplikasi*, *Server Database*, *Server 4* dan *5*. Kemudian terdapat 12 buah *router* berjenis mikrotik yang terdiri dari 2 *router managemen server* dan *client* serta 10 *router* untuk masing-masing fakultas UISU dan laboratorium yang dihubungkan melalui sebuah switch fakultas.

2.9 Beberapa Penelitian Terkait Dengan Laporan Skripsi

1. Haries Anom Susetyo Aji Nugroho, Sri Hartati, , Sonhaji 2022

Judul : Analisis Perbandingan Protokol *Routing* OSPF Dan *Static* Untuk Optimalisasi Jaringan Komputer SMA XYZ

Pembahasan : Protokol *Routing* OSPF dapat diterapkan pada jaringan computer SMA XYZ dikarenakan dalam proses konfigurasi atau *routing* lebih mudah karena tidak perlu mendaftarkan

atau mengkonfigurasi semua *network* ke setiap *router* karena dengan *routing* OSPF.

2. Sindy Alvionita¹, Heru Nurwasito 2019

Judul : Analisis Kinerja Protokol *Routing* OSPF, RIP dan EIGRP Pada Topologi Jaringan Mesh

Pembahasan : Rata-rata *packet loss* pada topology mesh yang dikonfigurasi menggunakan protokol routing OSPF, RIP dan EIGRP yaitu 0% atau tidak terjadi *packet loss* karena pada topology mesh memiliki 4 link yang bisa menjadi backup jika ada 2 link yang down sesuai skenario pengujian yang dilakukan.

3. Debbi Irfan Mudhoep, Linawati, Oka Saputra 2021

Judul : Protokol *Routing* OSPF dan BGP dengan VRRP, HSRP, GLBP

Pembahasan : *Routing* OSPF dengan metode kinerja VRRP lebih direkomendasikan untuk mengatasi permasalahan jaringan di sekolah karena memiliki waktu tunggu yang lebih pendek didukung protokol routing menggunakan mekanisme link yang stabil dan menggunakan media yang lebih stabil.