

Analisis Routing Loop dalam Open Shortest Path First (OSPF) Routing Menggunakan Teknik Spanning Tree di Jaringan Multi Area

Rachmat Aulia, Risiko Liza, Haida Dafitri

Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia

INFORMASI ARTIKEL

Diterima Redaksi: 10 Desember 2023

Revisi Akhir: 08 Januari 2024

Diterbitkan Online: 12 Februari 2024

KATA KUNCI

Jaringan OSPF; *Spanning Tree Protocol*;
Looping Routing GNS3;

KORESPONDENSI

Phone: +62 813-1507-3770

E-mail: jackm4t@gmail.com

A B S T R A K

Konektivitas jaringan merupakan hal mendasar yang harus diterapkan dalam suatu instansi atau perusahaan, dengan tujuan untuk memudahkan pertukaran dan pengumpulan data. Pembahasan yang disajikan dalam penelitian ini adalah implementasi jaringan *Open Shortest Path First* (OSPF) dengan metode *Spanning Tree Protocol* untuk memelihara loop routing menggunakan *Graphical Network Simulator 3* (GNS3). Definisi dari OSPF adalah protokol *routing* dinamis yang menggunakan algoritma *link-state* untuk membuat dan menghitung jalur terpendek ke semua tujuan yang diketahui. Penggunaan *Routing* mempunyai pengaruh dalam menentukan rute yang diambil oleh paket yang masuk dari node sumber ke node tujuan dalam jaringan. *Spanning Tree Protocol* (STP) berfungsi sebagai protokol untuk pengaturan koneksi dengan menggunakan algoritma *spanning tree*. Tujuan dari artikel ini adalah mempermudah pelaksanaan pekerjaan khususnya dalam hal pengumpulan data yang terdapat dalam sistem komunikasi yang diperlukan bagi instansi atau perusahaan.

PENDAHULUAN

Teknologi Internet adalah media yang terdiri dari berbagai infrastruktur, protokol, dan sistem yang memungkinkan transmisi dan pertukaran data melalui jaringan komputer di seluruh dunia. Dengan cara ini, penyebaran data dapat dilakukan secara besar-besaran dan dalam waktu singkat karena dapat menghubungkan banyak pengguna di seluruh dunia. Mereka yang terhubung satu sama lain di seluruh dunia pasti menggunakan teknologi jaringan komputer. Dengan demikian, komunikasi global terjalin di lokasi yang berbeda-beda sehingga aktivitas pengiriman dan pertukaran data dapat berlangsung tanpa terpengaruh oleh jarak dan waktu [1].

Di era revolusi industri 4.0 saat ini, semua bisnis harus menggunakan teknologi informasi dan komunikasi yang mana salah satu contohnya adalah jaringan komputer. Jaringan komputer adalah kumpulan interkoneksi komputer autonomous yang terkoneksi dengan media transmisi kabel atau tanpa kabel (*wireless*). Dalam penerapannya terdapat suatu teknik yang dikenal dengan *routing*. Teknik tersebut merupakan suatu mekanisme untuk menentukan rute yang dilalui oleh suatu paket yang berasal dari sumber *node* ke *node* tujuan dalam jaringan. Ada banyak protokol yang digunakan dalam jaringan komputer. Pada penelitian ini protokol yang dibahas adalah *Open Short Path First* (OSPF) dan *Spanning Tree Protocol* (STP). OSPF adalah protokol *routing* dinamis yang menggunakan algoritma *link-state* untuk membuat dan menghitung jalur terpendek ke semua tujuan yang diketahui. Protokol ini berfokus pada kinerja prosesor, kebutuhan memori, dan konsumsi *bandwidth* [2]. Tujuannya adalah untuk fokus mempelajari *routing* dan waktu pemrosesan (*time*) yang dicapai pada saat pengiriman paket data dari sumber sampai diterima berdasarkan tujuannya [3]. Sedangkan STP merupakan protokol jaringan komputer yang dapat menghindari operasi berulang saat menghubungkan *LAN Ethernet* [4]. Koneksi yang telah terjadi pada protokol ini menggunakan algoritma *spanning tree* [5].

Permasalahan yang ditemui pada penelitian ini terkait dengan *routing loop*. *Routing Loop* adalah urutan proses transmisi paket data dalam jaringan eksternal atau jaringan multi-area [6]. Masalah ini terjadi ketika *router* tersambung ke beberapa *router* saat mentransfer data. Proses ini akan terjadi setiap kali selama *router* terhubung ke *router* lain. *Loop* perutean membawa setidaknya 32 byte paket data koneksi jaringan. Hal ini dibuktikan melalui proses koneksi ke grup Internet atau paket *PING* di jaringan. Bayangkan jika ada puluhan *router* yang terhubung dalam satu *router* dan mengirimkan paket *routing loop* maka *router* tujuan akan mengalami data *overflow* yang mungkin menyebabkan kerja *router* menjadi gagal, rute semakin sulit [7]. Contoh dari *routing loop* ini adalah *acknowledge* dan *adjacency* yang ditemukan dalam *routing* OSPF.

Penelitian ini diharapkan dapat menjadi referensi dalam proses transmisi data secara *online*. Komunikasi yang diinginkan dapat berjalan dengan lancar dan meminimalisir kendala dari segi waktu dan kapasitas bandwidth yang dibutuhkan. Penggunaan protokol tergantung pada *routing* yang dilakukan, sehingga transmisi paket data *router* dapat bekerja dengan normal.

TINJAUAN PUSTAKA

Routing

Protokol perutean adalah protokol yang mengelola komunikasi antar *router*, dan mampu bertukar informasi tentang jaringan dan koneksi di antaranya [8]. *Router* menggunakan informasi ini untuk membangun dan meningkatkan tabel *routing*-nya. Pertukaran informasi dalam jaringan internet dikelola oleh protokol *routing* yang ditentukan pada lapisan jaringan dari tujuh lapisan model OSI. *Routing* adalah proses pengiriman data dari satu jaringan ke jaringan lainnya. Dengan *routing* dinamis, mekanismenya dilakukan secara dinamis. Artinya, menentukan jarak tercepat antara perangkat pengirim dan penerima dengan cepat dan akurat. OSPF dan ISIS adalah contoh protokol *routing* dinamis yang menggunakan algoritma *link-state* untuk membuat dan menghitung jalur terpendek ke semua tujuan yang diketahui [9].

Spanning Tree Protocol (STP)

STP (Spanning Tree Protocol) adalah lapisan dua tautan yang bertindak sebagai protokol manajemen redundansi jalur sementara untuk mencegah masalah loop dalam jaringan. STP telah berkembang menjadi protokol yang dengan cepat menghitung port mana yang perlu diblokir untuk melindungi jaringan berbasis VLAN dari loop lalu lintas [6]. Algoritma Spanning Tree (STP) berfungsi untuk menentukan port switch mana dalam jaringan yang harus dikonfigurasi untuk diblokir guna mencegah terjadinya loop [4]. STA menunjuk satu saklar sebagai jembatan akar dan menggunakannya sebagai titik referensi untuk semua perhitungan jalur. Ada empat peran berbeda yang dikonfigurasi secara otomatis selama proses spanning tree [5]:

1. *Root port* => merupakan *port switch* yang paling dekat terhadap *root bridge*. *Root ports* meneruskan *traffic* menuju ke *root bridge*. MAC address merupakan sumber dari *frame* yang diterima pada *root port* dapat digunakan untuk membuat *table* MAC. Hanya satu *root port* yang diperbolehkan per *bridge*.
2. *Designated port*, merupakan semua *non-root ports* yang masih diperbolehkan untuk meneruskan *traffic* pada *network*. Hanya satu *designated port* yang diperbolehkan pada tiap *segment*.
3. *Non-designated port*, merupakan semua *port* yang dikonfigurasi sebagai pemblokir untuk mencegah terjadinya *traffic loop*.
4. *Disabled Port*, merupakan *port* yang dinon-aktifkan secara administratif, *port* yang dinon-aktifkan tidak berfungsi dalam proses *spanning tree*.

Virtual Local Area Network (VLAN)

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi *workstation* [6]. VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan *port*, *MAC addresses* dan sebagainya. Semua informasi yang mengandung penandaan / pengalamatan suatu VLAN (*tagging*) di simpan dalam suatu *database* (tabel), jika penandaannya berdasarkan *port* yang digunakan maka *database* harus mengindikasikan *port-port* yang digunakan oleh VLAN [4]. Untuk mengaturnya maka biasanya digunakan *switch / bridge* yang *manageable* atau yang bisa diatur. *Switch*

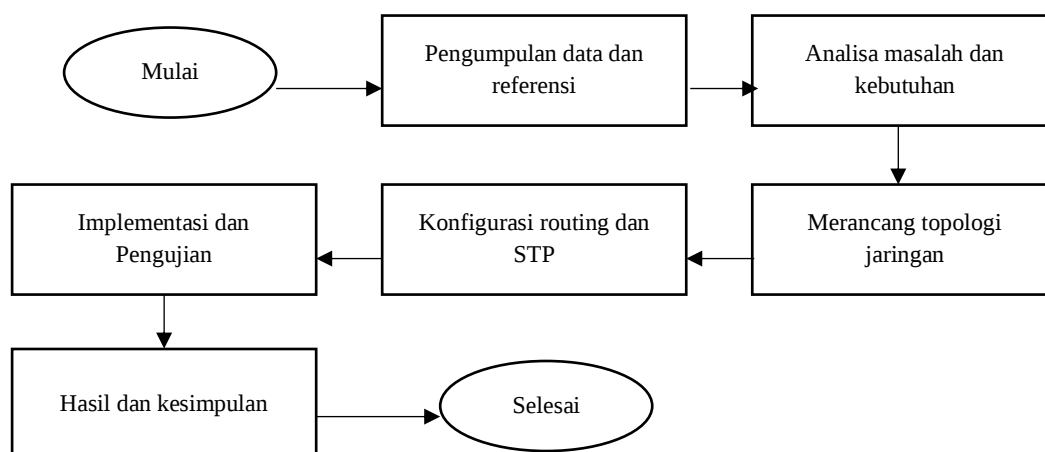
/ *bridge* inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua *switch / bridge* memiliki informasi yang sama. *Switch* akan menentukan kemana data-data akan diteruskan dan sebagainya. atau dapat pula digunakan suatu *software* pengalamatan (*bridging software*) yang berfungsi mencatat / menandai suatu VLAN berserta *workstation* yang didalamnya. untuk menghubungkan antar VLAN dibutuhkan *router* [5].

Protocol Routing OSPF

Open Shortest Path First (OSPF) [10] adalah *Routing Dinamis (dynamic routing)* protokol yang secara dinamis memelihara, mengelola, dan mendistribusikan informasi *routing* di antara jaringan sebagai respon terhadap setiap perubahan jaringan. Istilah "*Autonomous System*" (AS) digunakan di OSPF untuk menggambarkan kumpulan beberapa jaringan berorientasi perutean dengan metode identik dan pengaturan kebijakan yang semuanya dapat dikontrol oleh administrator jaringan [11]. Faktanya, sebagian besar fitur ini digunakan untuk manajemen jaringan yang sangat ekstensif. Akibatnya, OSPF dapat menjadi solusi yang mengurangi kesalahan distribusi informasi perutean dan membuat penambahan informasi perutean menjadi lebih sederhana [7]. OSPF termasuk dalam kelompok IGP (*Interior Gateway Protocol*) karena memiliki kemampuan *Link-State* dan Algoritma *Dijkstra*, yang secara signifikan lebih efektif daripada protokol IGP lainnya. Dalam kegiatannya, OSPF menggunakan protokol sendiri, yaitu protokol 89 [1].

METODOLOGI

Penelitian ini menggunakan metode yang berisikan sekumpulan tahapan demi tahapan untuk mencapai hasil. Representasi tahapannya disajikan sebagai berikut [12]:



Gambar 1. Tahapan Penelitian [13]

Tahap Perancangan

Tahap perancangan merupakan aktivitas yang dilakukan untuk menyiapkan software aplikasi simulasi jaringan menggunakan *graphical network simulator 3 (GNS3)* [14], dan mendesain pembuatan sistem konfigurasi jaringan. Tahap ini dapat dikatakan sebagai tahap pengumpulan beberapa bahan yang dapat disajikan sebagai landasan awal untuk mendefinisikan permasalahan. Pada tahap ini semua permasalahan terkait keamanan jaringan komputer dapat di kumpulkan sehingga ditemukan solusi untuk menyelesaikan masalah tersebut. Tahap perencanaan ini fokus pada kebutuhan terkait solusi pemecahan masalah, yang dibahas agar pelaksanaan tahap-tahap selanjutnya lebih terstruktur dan proporsional. Dalam perencanaan ini aktivitasnya dimulai dengan melakukan analisis. Data yang diperoleh kemudian diolah untuk perancangan sistem analisis jaringan atau simulasi jaringan.

Konfigurasi Spanning Tree Protocol

Dalam topologi bahwa setiap *switch* memiliki beberapa jalur *backup* yang digunakan apabila salah satu koneksi jaringan terjadi kerusakan dapat menggunakan jalur koneksi yang lain agar jaringan masih dapat berjalan dengan normal. Penggunaan jalur yang digunakan sebagai *backup* dapat memperlambat kinerja sebuah jaringan dan akan mengakibatkan terjadinya *loop* dan *broadcast storm*, maka setiap *switch* menggunakan konsep *spanning tree protocol* untuk

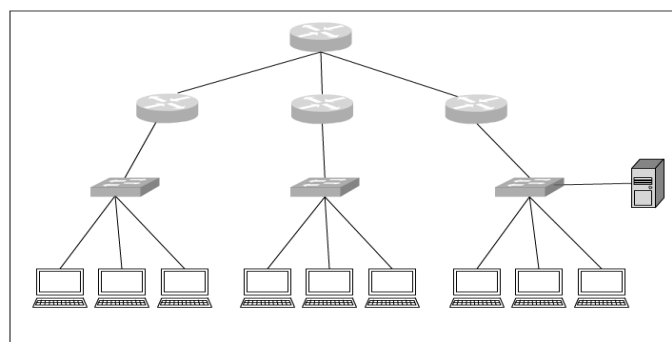
meminimalisir kerugian penggunaan jalur *backup*. Konsep *spanning tree protocol* akan mencegah terjadinya *redundant link* pada jaringan dengan menerapkan beberapa proses algoritma yaitu menentukan nilai *bridge ID* paling rendah, menentukan *root path cost* paling rendah, menentukan *sender bridge ID* paling rendah, dan menentukan port ID paling rendah. Dari penggunaan algoritma *spanning tree protocol* dapat menentukan pemilihan *root bridge*, *root port* untuk setiap *non-root bridge*, dan *designated port* dan *non-designated port* untuk setiap segmen *network* agar terjadi konvergensi. Dalam penelitian ini digunakan *spanning tree protocol*. Penggunaan PVST membuat *spanning tree protocol* dapat dikonfigurasi secara terpisah dan mengakibatkan perbedaan konfigurasi di masing jaringan OSPF sehingga proses menuju konvergensi menjadi lebih cepat.

Langkah langkah yang harus dilakukan ketika melakukan perintah pada konfigurasi *spanning tree protocol* sebagai berikut:

1. *Show spanning-tree* pada switch 1 yang akan dikonfigurasi.
2. *Show spanning-tree* pada switch 2 yang akan dikonfigurasi.
3. Selanjutnya, akan mengubah agar switch I menjadi *root bridge*. Ada dua cara yang bisa kita lakukan. Yang pertama adalah mengubah nilai *priority switch* I agar menjadi lebih kecil dari switch 2. dan yang kedua adalah mengubah nilai *priority switch* 2 agar menjadi lebih besar dari switch 1. Saya akan memilih cara yang pertama, yakni mengubah *priority* pada switch 1.
4. Konfigurasi nya *spanning-tree vlan [ID] priority [nilai_priority]*. 5. Kemudian untuk melihat hasil konfigurasi ketik *show spanning tree*

Rancangan Topologi

Topologi yang dirancang dan digunakan dalam penelitian ini disajikan sebagai berikut:



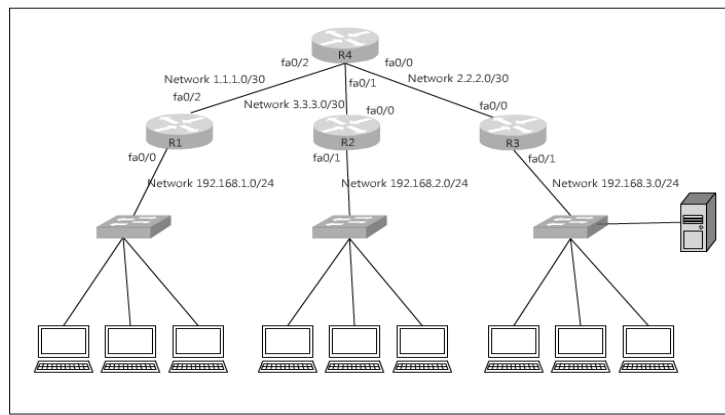
Gambar 2. Rancangan Topologi Jaringan [15]

Gambar 2 adalah rancangan topologi logikal yang paling tepat untuk diterapkan menggunakan metode *spanning tree*. Berdasarkan gambar tersebut dijelaskan bahwa jaringan OSPF yang menggunakan 4 perangkat *router* yang saling terhubung dimana 1 *router* sebagai pusat pengendali jaringan OSPF dan terhubung dengan 3 *router* yang menghubungkan 3 perangkat *switch*, *switch* ini akan terhubung dengan komputer, pada setiap *switch* yang terdapat pada masing-masing 3 perangkat komputer *client* atau *just* sehingga setiap komputer *client* atau *host* saling terhubung dengan lainnya.

HASIL DAN PEMBAHASAN

Rancangan Arsitektur Jaringan OSPF

Arsitektur yang dirancang dalam penelitian ini menggunakan simulator/tools GNS3 [12][14]. Fungsi dari arsitektur ini merupakan gambaran model jaringan OSPF yang dibangun menggunakan metode STP. Dari arsitektur ini dapat dijelaskan secara rinci bagaimana proses yang sesungguhnya berjalan dan dapat mengetahui perangkat-perangkat keras apa saja yang terlibat dalam proses pembangunannya. Berikut keterangan arsitektur jaringannya:



Gambar 3. Rancangan Arsitektur Jaringan OSPF

Berdasarkan gambar 3, terdapat 4 *router* yang digunakan menjalankan protokol routing OSPF. *Server* merupakan perangkat yang digunakan untuk melayani permintaan *client*.

Konfigurasi Jaringan OSPF

Konfigurasi yang diterapkan untuk jaringan OSPF terdiri dari beberapa tahapan. Berikut penjabaran tahapan konfigurasinya:

Network Router 1

Konfigurasi yang digunakan untuk jaringan *router* 1 adalah melakukan pengaturan *IP Address*, perintahnya sebagai berikut:

```
R1 config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z
R1 (config)#int fa 0/0
R1 (config-if)#ip add 1.1.1.1 255.255.255.0
R1 (config-if)#no shut
```

Berdasarkan perintah tersebut dapat diartikan bahwa *router* 1 harus diberikan *IP Address* yang berfungsi untuk meneruskan paket-paket dari sebuah jaringan ke jaringan lainnya.

Network Router 2

Konfigurasi yang digunakan untuk jaringan *router* 2 adalah melakukan pengaturan *IP Address*, perintahnya sebagai berikut:

```
R2 config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#int fa 0/0
R2 (config-if)#ip add 2.2.2.2 255.255.255.0
R2 (config-if)#no shut
```

Berdasarkan perintah tersebut dapat diartikan bahwa *router* 2 harus diberikan *IP Address* yang berfungsi untuk meneruskan paket-paket dari sebuah jaringan ke jaringan lainnya.

Network Router 3

Konfigurasi yang digunakan untuk jaringan *router* 3 adalah melakukan pengaturan *IP Address*, perintahnya sebagai berikut:

```
R3 config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z
```

```
R3 (config)#int fa 0/0
R3 (config-if)#ip add 172.16.1.1 255.255.255.0
R3 (config-if)#no shut
```

Berdasarkan perintah tersebut dapat diartikan bahwa router 3 harus diberikan *IP Address* yang berfungsi untuk meneruskan paket-paket dari sebuah jaringan ke jaringan lainnya.

Network Routing OSPF

Konfigurasi yang digunakan untuk jaringan *routing* OSPF adalah melakukan pengaturan *IP Address*, perintahnya sebagai berikut:

```
R3#config Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z
R3 (config)#router ospf 10
R3 (config-if)#network 2.2.2.0 0.0.0.3 area 1
R3 (config-if)#network 172.16.1.0 0.0.0.255 area 1
```

Berdasarkan perintah tersebut dijelaskan bahwa pada router 3 harus dilakukan konfigurasi protokol jaringan OSPF, tujuannya adalah untuk mendistribusikan informasi jaringan dari satu *router* ke *router* lainnya

VLAN (Virtual Local Area Network)

Konfigurasi VLAN dalam jaringan OSPF perintahnya sebagai berikut:

```
switch1 > enable
switch1#configure terminal
switch1-(config)#vlan database
switch1-(config)#vlan 10 name roy1
```

Tujuan konfigurasi VLAN adalah untuk mengaktifkan *spanning tree*.

Network Spanning Tree

Penjelasan konfigurasi network *spanning tree* dilakukan sebagai berikut:

```
switch1-#show spanning-tree VLAN 1
switch1->enable
switch1-#configure terminal
switch1-(config)#spanning-tree VLAN 20 root primary
switch1-(config)#spanning-tree VLAN 30 root secondary
switch1-(config)#end
switch2->enable
switch2-#configure terminal
switch2-(config)#spanning-tree vlan 20 priority (0-61440)
switch2- (config)#end
```

Perintah tersebut menjelaskan bahwa jaringan *switch* harus dikonfigurasi menggunakan metode *spanning tree* yang dapat mencegah terjadinya *looping routing* pada sebuah network OSPF.

Konfigurasi Server

Berikut perintah yang digunakan untuk konfigurasi *server*:

```
server#conf t
server(config)#int fa 0/0
server(config-if)#ip add 192.168.200.5 255.255.255.0
server(config)#no shut
server(config)#end
server#conf t
server(config)#router ospf 10
```

```

server(config-router)#network 2.2.2.0 0.0.0.3 area 1
server(config-router)#network 2.2.2.1 0.0.0.3 area 1
server(config-router)#network 2.2.2.0 0.0.0.3 area 1
server(config-router)#network 17

```

Route pada Router 1

Tahap ini menjelaskan terkait menampilkan konfigurasi *routing* pada perangkat *router* dalam menerapkan jaringan OSPF, perintahnya sebagai berikut: R3#show IP router

Tujuan perintah tersebut adalah menginformasikan *router* jalur mana yang harus dilewati untuk menuju network tujuan yang berbeda.

Show IP Address Router 1

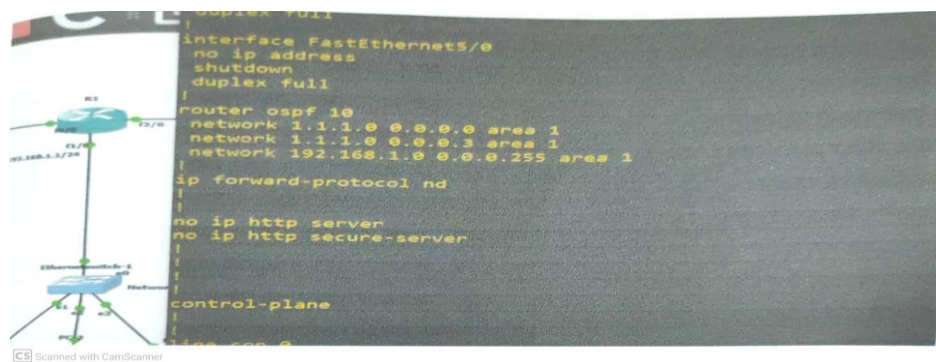
Bagian ini menampilkan konfigurasi *IP Address* pada perangkat *router* dalam menerapkan jaringan OSPF, perintahnya sebagai berikut: R3#show IP int brief

Tujuan perintah tersebut adalah untuk menampilkan informasi dari *ports* yang sudah dilengkapi dengan sebuah alamat IP.

Show Running Config

Bagian ini digunakan untuk menampilkan konfigurasi dari sebuah *router* dan *switch*. Perintahnya sebagai berikut: R3#show running config

Tujuan perintah tersebut adalah untuk menampilkan jaringan OSPF yang telah diterapkan pada perangkat *router* dan *switch*. *Output*-nya dapat dilihat seperti berikut:

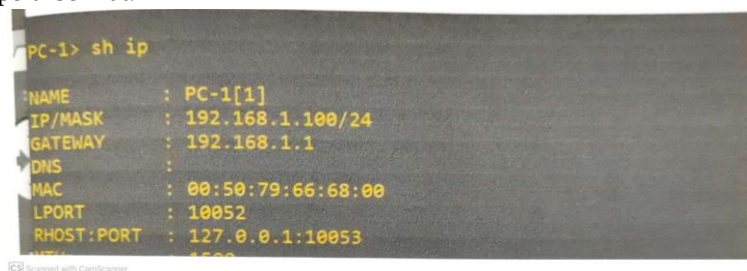


Gambar 4. Konfigurasi Jaringan OSPF

Keterangan pada gambar 4 menjelaskan implementasi jaringan OSPF, dengan maksud mengurangi waktu pemrosesan (*overhead*) *routing* sehingga mempercepat *convergence* dan membatasi ketidakstabilan jaringan.

Konfigurasi IP-Address

Konfigurasi *IP-Address* dimulai dengan perintah untuk menambahkan *IP-Address* ke masing-masing komputer. perintahnya dapat diketik sebagai berikut: “PC-1>Sh IP” dan “PC-1> Ip add 192.168.1.100 255.255.255.0 192.168.1.1”, hasilnya dapat dilihat seperti berikut:



Gambar 5. Konfigurasi IP-Address pada Komputer

Keterangan berdasarkan gambar 5 adalah bahwa setiap alamat yang ada pada setiap komputer berfungsi untuk mempermudah *network* mengenali seluruh komputer *client* / *host* yang telah terpasang.

Pengujian Koneksi antara Router 1 dengan Router 2

Untuk membuktikan bahwa *router* 1 dengan *router* 2 terhubung maka dilakukan pengujian *ping* dari *router* 1 menuju *router* 2, penerapannya memerlukan perintah berikut: “**R1# ping 3.3.3.1**”. Hasil dari perintah tersebut disajikan seperti berikut:

```
R1#X{Ez}
R1#R}p
^
% Invalid input detected at '^' marker.

R1#ping 3.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.1, timeout is 2
.....
Success rate is 0 percent (0/5)
R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2
.....
Success rate is 0 percent (0/5)
```

Gambar 6. Percobaan Koneksi antara Router 1 dengan Router 2

Pengujian Koneksi antara Router 1 dengan Router 4

Untuk membuktikan bahwa *router* 1 dengan *router* 4 terhubung maka dilakukan percobaan *ping* dari *router* 1 menuju *router* 4, untuk penerapannya memerlukan perintah berikut: “**R1# ping 172.16.1.1**”. Hasil dari perintah tersebut disajikan seperti berikut:

```
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
R1#EER{MMX}TT
R1#p}
R1#
R1#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
```

Gambar 7. Percobaan Koneksi antara Router 1 dengan Router 4

Pengujian Koneksi dari Router 1 menuju PC 7

Untuk membuktikan bahwa *router* 1 dengan komputer 7 terhubung maka dilakukan pengujian *ping* dari *router* 1 menuju komputer 7, penerapannya memerlukan perintah berikut: “**R1# ping 192.168.200.2**”. Hasil dari pengujian tersebut disajikan seperti berikut:

```
R1#TTTT{RRR}XXX
R1#M}ppp
R1#
R1#ping 192.168.200.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.2, timeout is 2
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0
```

Gambar 8. Percobaan Koneksi dari Router 1 menuju PC 7

Pengujian Data Delay

Pengujian ini menjelaskan tentang data perhitungan *delay* pada jaringan OSPF menggunakan metode *spanning tree protocol* [11]. Hasilnya akan disajikan dalam dua versi, yaitu: sebelum dan sesudah menggunakan metode tersebut.

Frame 4: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Interface id: 0 (-)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 2, 2019 19:26:10.882964000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1570019170.882964000 seconds
[Time delta from previous captured frame: 7.609145000 seconds]
[Time delta from previous displayed frame: 7.609145000 seconds]
[Time since reference or first frame: 10.484067000 seconds]
Frame Number: 4

Frame 6: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
Interface id: 0 (-)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 2, 2019 19:26:18.028389000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1570019178.028389000 seconds
[Time delta from previous captured frame: 5.117084000 seconds]
[Time delta from previous displayed frame: 5.117084000 seconds]
[Time since reference or first frame: 18.028389000 seconds]
Frame Number: 6

Gambar 9. Data Delay Tidak Menggunakan Metode Spanning Tree Protocol

Dalam pengujian ini telah mencoba untuk menghitung *delay* dari pengiriman paket pertama 10,48406700 dan pengiriman paket kedua 18,028389000. Dari kedua nilai tersebut dapat diperoleh total *delay* menggunakan rumus: **Delay = waktu paket diterima / waktu paket dikirim; Delay = 18,028389000/10,484067000 = 7,544322**. Hasilnya, untuk mengirimkan 1 paket pada arsitektur jaringan OSPF sebelum menggunakan *spanning tree protocol* adalah 7,544322.

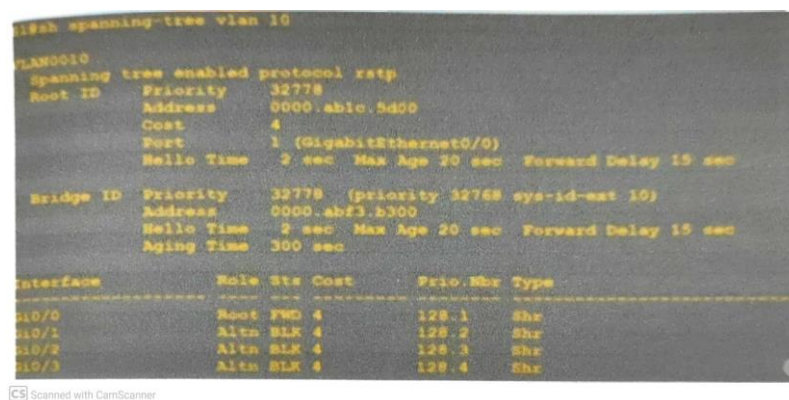
Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Interface id: 0 (-)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 2, 2019 23:52:02.255809000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1570035122.255809000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 43.522094000 seconds]
Frame Number: 7

Gambar 10. Data Delay Menggunakan Metode Spanning Tree Protocol

Dalam pengujian ini telah mencoba untuk menghitung *delay* dari pengiriman pertama 45,543834000 dan pengiriman kedua 43,522094000. Dari kedua nilai tersebut dapat diperoleh total *delay* dengan rumus: **Delay = waktu paket diterima / waktu paket dikirim; Delay = 45,543834000/43,522094000 = 2,02174**. Hasilnya, untuk mengirimkan 1 paket pada arsitektur jaringan OSPF dengan menggunakan *spanning tree protocol* adalah 2,02174.

Hasil Spanning Tree Protocol

Metode ini dapat dilakukan jika saat konfigurasi menampilkan waktu dan *port* yang digunakan. Berikut perintah yang perlu dijalankan: **Switch#sh spanning tree vlan 10**. Hasilnya disajikan seperti berikut:



Gambar 11. Hasil Spanning Tree Protocol

Penjabaran pada gambar 11 adalah perintah untuk menampilkan informasi dari sebuah switch yang sudah dilengkapi dengan konfigurasi *spanning tree*, *output*-nya memiliki *forward delay* pada *root id* sebesar 15 second, kemudian terdapat *forward delay* pada *bridge id* sebesar 15 second. Saat *looping* terjadi pada suatu switch, maka akan terjadi *forwad delay* sekitar 15 detik, selanjutnya switch akan kembali berjalan normal dalam jaringan.

KESIMPULAN DAN SARAN

Dari hasil serangkaian pembahasan dalam penelitian ini, maka dapat ditarik kesimpulan sebagai berikut: Penelitian ini menerapkan protokol jaringan OSPF yang dapat melakukan komunikasi dan pertukaran data antar jaringan dengan koneksi yang telah terhubung atau terbangun. Teknik *spanning tree* digunakan untuk menghindari *looping* atau tabrakan antar data dengan membuat jalur cadangan jika salah satu jalur gagal atau terputus, sehingga konektivitas yang terbangun tidak memerlukan waktu yang lama (*delayed*) dan proses komunikasi berlangsung lancar. Penelitian ini menggunakan *Graphical Network Simulator 3* (GNS3) untuk mensimulasikan implementasi jaringan OSPF menggunakan metode *spanning tree protocol*.

Adapun beberapa saran yang perlu diperhatikan adalah sebagai berikut: Jika terdapat penelitian selanjutnya yang mengangkat tentang cara mencegah *looping*, disarankan melakukan perbandingan menggunakan metode lain sehingga dapat memberikan hasil yang lebih akurat. Pengembangan penelitian berikutnya direkomendasikan menggunakan *router mikrotik* sehingga dapat diketahui *quality of service* (QoS). Menyarankan penelitian berikutnya yang membahas pencegahan *looping* menggunakan protokol jaringan lainnya seperti: *Border Gateway Protocol* (BGP), *Interior Gateway Routing Protocol* (IGRP), dan *Enhanced Interior Gateway Routing Protocol* (EIGRP).

DAFTAR PUSTAKA

- [1] I. Hiswara, K. Khoiriyah, and D. Febriyanto, "Perancangan Jaringan Lan Smk Al-Khairiyah 2 Dengan Menggunakan Metode Ospf," *JEIS J. Elektro dan Inform. Swadharma*, vol. 3, no. 1, pp. 58–66, 2023, doi: 10.56486/jeis.vol3no1.302.
- [2] Y. B. Setiawan, I. Nawawi, and D. Pravitasari, "Desain Infrastruktrur Jaringan Inter-Vlan dengan Keamanan Port Security dan Secure Shell Berbasis Protocol Open Short Path First," vol. 2, no. 1, pp. 250–258, 2022.
- [3] R. Syahputra, Rahmadi Kurnia, and Rian Ferdian, "Analysis of FHRP Design and Implementation in RIPv2 and OSPF Routing Protocols," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 1, pp. 102–108, 2020, doi: 10.29207/resti.v4i1.1490.
- [4] Y. Indrianingsih, H. Wintolo, and E. Y. Saputri, "Spanning Tree Protocol (STP) Based Computer Network Performance Analysis on BPDU Config Attacks and Take Over Root Bridge Using the Linear Regression Method," *J. Online Inform.*, vol. 6, no. 2, p. 155, 2021, doi: 10.15575/join.v6i2.703.
- [5] V. M. J. Renwarin and U. Radiyah, "Implementasi Spanning Tree Protocol (STP) Pada Perancangan Virtual Local Area Network (VLAN) Pada PT Regalindo Sakti Jakarta," *J. Ji-Tech*, vol. 17, no. 1, pp. 6–11, 2021, [Online]. Available: <https://jitech.i-tech.ac.id/index.php/jitech/article/view/179>
- [6] H. Saiyar and M. Noviansyah, "IMPLEMENTASI SPANNING TREE PROTOCOL (STP), VIRTUAL LAN (VLAN), DAN ACCESS LIST (ACL) PADA JARINGAN KOMPUTER BALAI BESAR PELATIHAN KESEHATAN JAKARTA," *J. Akrab Juara*, vol. 4, no. 3, pp. 43–53, 2019.
- [7] W. S. Jati, H. Nurwasito, and M. Data, "Perbandingan Kinerja Protocol Routing Open Shortest Path First (OSPF

-) dan Routing Information Protocol (RIP) Menggunakan Simulator Cisco Packet Tracer,” *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 2, no. 8, pp. 2442–2448, 2018.
- [8] Y. Suhandi, L. Nurlaela, A. Dharmalau, and B. S. Widjojo, “Perancangan Infrastruktur Jaringan Berbasis Aplikasi Packet Tracer dengan Metode Hot Standby Router Protocol,” *J. Teknol. Terpadu*, vol. 8, no. 1, pp. 9–16, 2022, doi: 10.54914/jtt.v8i1.497.
- [9] bamai.uma.ac.id, “Cara Kerja Routing,” *Universitas Medan Area*, 2021. <https://bamai.uma.ac.id/2021/11/17/cara-kerja-routing/>
- [10] H. A. Musril, “Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF),” *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 3, no. 2, pp. 83–88, 2019, doi: 10.30743/infotekjar.v3i2.1055.
- [11] R. H. Sianturi, T. . Diansyah, and I. Lubis, “Application of OSPF Network in Spanning Tree Protocol Method to Prevent Looping Routing,” *J. Comput. Sci. Inf. Technol. Telecommun. Eng.*, vol. 1, no. 2, pp. 44–53, 2020, doi: 10.30596/jcositte.v1i2.4716.
- [12] A. P. A. Kusuma and Asmunin, “Implementasi Simple Port Knocking Pada Dynamic Routing (Ospf) Menggunakan Simulasi Gns3,” *J. Manaj. Inform.*, vol. 5, no. 2, pp. 7–17, 2016.
- [13] F. F. Shodiq and A. Prihanto, “Analisis Perbandingan Performansi Kontroler RYU Dan POX Berbasis Software Defined Network (SDN) Pada Routing OSPF,” *J. Informatics Comput. Sci.*, vol. 3, no. 03, pp. 216–223, 2021, doi: 10.26740/jinacs.v3n03.p216-223.
- [14] I. G. L. P. E. Prisma and B. Chilmi, “Implementasi Simulasi Jaringan Komputer Multi Device Dengan Menggunakan GNS3,” *J. Manaj. Inform.*, vol. 04, no. 01, pp. 77–84, 2015.
- [15] K. A. Santoso, “JURNAL KAJIAN TEKNIK ELEKTRO Vol1.No.1UNIVERSITAS 17 AGUSTUS 1945 JAKARTA Page 67 Konfigurasi dan Analisis Performansi Routing OSPF pada Jaringan LAN dengan Simulator Cisco Packet Tracer versi 6.2,” *J. Kaji. Tek. Elektro*, vol. Vol.1, no. No.1, pp. 67–78, 2017.