Implementasi *Routing* OSPF (*Open Shortest Path First*) *Single Area* Pada Jaringan VPN dengan *Access Site-to-Site*

Muhammad Arif Abdillah[1], Rizki Putra Ramadhan[2], Ardi Tri Yudha[3], Dhani Medianto Saputra[4], Ririn Purnama Sari[5]
[12345]Jurusan Sistem Komputer, Universitas Sriwijaya, Indonesia

*Penulis Korespondensi: arifawantara123@gmail.com

ARTICLE INFO

Article History:
- Received 01 January 2022
- Received in revised form 25 January 2022
- Accepted 19 January 2022
- Available online 31 March 2022

ABSTRAK

Jaringan *Virtual Private Network* (VPN) telah menjadi solusi yang populer dalam mengamankan komunikasi dan menghubungkan jaringan yang terpisah secara geografis. Dalam konteks ini, implementasi *Routing* OSPF (*Open Shortest Path First*) Single Area menjadi krusial dalam memastikan efisiensi dan keamanan dalam pengiriman data antara situs. *Open Shortest Path First* (OSPF) adalah salah satu protokol *Routing* interior yang paling umum digunakan dalam jaringan IP. Proses *Routing* mengatur bagaimana suatu paket pergi dari suatu node sumber ke node tujuan jaringan. Penelitian ini mengkaji penerapan OSPF Single Area pada jaringan VPN dengan akses *Site-to-Site*. Metodologi yang digunakan mencakup analisis kebutuhan jaringan, desain konfigurasi OSPF, dan pengujian kinerja. Hasil penelitian menunjukkan bahwa penerapan OSPF Single Area pada jaringan VPN mampu meningkatkan efisiensi *Routing* dan meningkatkan keamanan komunikasi antara situs secara signifikan. Temuan ini memberikan wawasan yang berharga bagi para praktisi dalam merancang dan mengelola jaringan VPN dengan akses *Site-to-Site*.

Kata Kunci: *OSPF, VPN, Routing, Single Area, Site-to-Site*

ABSTRACT

Virtual Private Network (VPN) networks have become a popular solution for securing communications and connecting geographically separated networks. In this context, the implementation of Open Shortest Path First (OSPF) Single Area Routing is crucial to ensure efficiency and security in data delivery between sites. OSPF is one of the most commonly used interior Routing protocols in IP networks. The Routing process governs how a packet travels from a source node to a destination node in the network. This research examines the implementation of OSPF Single Area in VPN networks with Site-to-Site access. The methodology used includes network requirements analysis, OSPF configuration design, and performance testing. The research findings demonstrate that the implementation of OSPF Single Area in VPN networks can significantly improve Routing efficiency and enhance communication security between sites. These findings provide valuable insights for practitioners in designing and managing VPN networks with Site-to-Site access.

Keywords: OSPF, VPN, Routing, Single Area, Site-to-Site

1. PENDAHULUAN

Di zaman digital saat ini, perkembangan jaringan internet menjadi suatu kebutuhan yang tidak dapat dihindari dalam kehidupan sehari-hari. Hal ini disebabkan oleh pentingnya komunikasi dan akses terhadap informasi yang menjadi prioritas utama bagi banyak orang [1]. Pentingnya keamanan informasi menjadi perhatian utama bagi organisasi dan individu di era digital yang terus berkembang [2]. Dengan keadaan tersebut, perkembangan jaringan internet membutuhkan infrastruktur yang memiliki tingkat kecepatan dan keandalan yang tinggi [3]. Infrastruktur yang baik dan kinerja jaringan yang optimal akan membentuk dasar bagi jaringan yang dapat dipertahankan dalam jangka panjang serta mencegah munculnya masalah jaringan. Seiring dengan pertumbuhan sebuah organisasi, jaringan komputernya juga akan berkembang karena semakin banyaknya perangkat keras yang terhubung ke dalam jaringan perusahaan tersebut. Hal ini memungkinkan untuk lebih mudahnya pengiriman data yang diperlukan bagi kelancaran operasional organisasi [4].

Routing adalah proses memilih rute yang akan ditempuh sebuah paket pada jaringan komputer untuk mengirim lalu lintas jaringan. Dalam proses *Routing* ini, sebuah jaringan digambarkan sebagai sebuah graf berbobot yang memiliki nilai atau bobot tertentu untuk setiap hubungan antara titiknya. Nilai-nilai ini dapat mencakup bandwith, delay network, hopcount, load, reliability, dan biaya komunikasi [5]. Setiap *router* harus menemukan rute yang paling rendah. OSPF adalah protokol *Routing* yang dapat digunakan untuk menentukan jalur pengiriman paket data terbaik di dalam jaringan skala besar. *Routing* dinamis memungkinkan *router* untuk membuat tabel *Routing* nya sendiri tanpa campur tangan pengelola jaringan [6]. Protokol *Routing* merupakan media dalam melakukan komunikasi data dan informasi antara satu sama lainnya [7]. *Routing* protokol bertanggung jawab untuk menemukan dan memberikan rute terbaik serta memperbarui tabel *Routing* jika ada perubahan pada jaringan [8]. Dua jenis *Routing* dinamik adalah IGP (Interior Gateway Protocol) dan EGP (Exterior Gateway Protocol) [9]. Protokol *Routing* IGP digunakan untuk menghubungkan jaringan di dalam kepemilikan autonomous system (AS) yang sama, seperti *Routing* OSPF. Protokol EGP digunakan untuk menghubungkan jaringan di dalam kepemilikan autonomous system (AS) yang berbeda, seperti contohnya adalah *Routing* BGP [10].

Teknologi *Virtual Private Network* (VPN) memfasilitasi akses ke jaringan lokal dari lokasi eksternal melalui internet [11]. Penggunaan VPN merupakan salah satu cara untuk membentuk jalur komunikasi yang aman antara klien dan server remote melalui jaringan publik [12]. Dengan VPN, pengguna dapat mengirim dan menerima data secara aman melalui jaringan publik, memberikan perlindungan yang membuat mereka merasa seolah-olah terhubung secara langsung ke dalam jaringan pribadi [13]. Dengan demikian, VPN memberikan lapisan tambahan perlindungan dan memungkinkan pengguna merasa seolah-olah terhubung secara langsung ke dalam jaringan pribadi, meskipun sebenarnya mereka berada di lokasi eksternal yang jauh.

Dalam menghadapi kompleksitas dan kebutuhan akan keamanan dalam komunikasi data, implementasi *Routing* OSPF (*Open Shortest Path First*) Single Area pada Jaringan VPN dengan Akses *Site-to-Site* menjadi hal yang sangat penting. Penelitian ini bertujuan untuk menyelidiki penerapan OSPF Single Area dalam konteks jaringan VPN dengan akses *Site-to-*

Site. Dengan memahami dan menganalisis metode ini, diharapkan penelitian ini dapat memberikan wawasan yang lebih mendalam tentang bagaimana OSPF dapat dioptimalkan untuk meningkatkan efisiensi dan keamanan dalam pengiriman data antara situs. *Open Shortest Path First* (OSPF) merupakan salah satu jenis protokol *Routing Internal Gateway Protocol* (IGP) yang termasuk dalam kategori protokol *Routing link-state* yang dikonfigurasi dalam sebuah Autonomous System atau di bawah kepemilikan suatu instansi. OSPF mengumpulkan informasi *link-state* dari *router* yang berada dalam satu domain OSPF untuk membentuk grafik topologi jaringan [14]. OSPF melakukan perhitungan seluruh informasi rute paket dengan tujuan menghasilkan jalur terpendek, yang didasarkan pada algoritma Dijkstra. Algoritma Dijkstra diterapkan dalam protokol OSPF untuk menentukan jalur optimal yang harus dilalui oleh paket data dari alamat asal ke alamat tujuan dengan biaya metrik terendah [15]. Karena itu, nilai bobot dari setiap sambungan jaringan dalam domain OSPF diperlukan untuk menemukan jalur terpendek [16].

2. TINJAUAN PUSTAKA

2.1 *Open Shortest Path First (OSPF)*

OSPF merupakan protokol *Routing* yang dikembangkan oleh IETF (*Internet Engineering Task Force*) pada tahun 1987 [17]. *Open Shortest Path First* (OSPF) adalah salah satu jenis *Routing* yang lebih baik, lebih kuat, lebih cepat dari pendahulunya. OSPF bertujuan untuk melampaui keterbatasan distance vector *Routing*. Jika lebih banyak *router* di sebuah area, lebih banyak informasi *router* yang harus dimiliki dalam waktu yang sama, sehingga OSPF adalah pilihan terbaik untuk proses *Routing* [18]. OSPF menggunakan protokol *Routing* interior dengan algoritma linkstate, OSPF menggunakan protokol *Routing link-state*, dengan karakteristik sebagai berikut [19]:

- Protokol *Routing link-state*
- Merupakan open standard protokol *Routing* yang dijelaskan di RFC 2328
- Menggunakan algoritma SPF untuk menghitung cost terendah
- Update *Routing* dilakukan secara floaded saat terjadi perubahan topologi jaringan

Algoritma *Shortest Path First*, yang berasal dari algoritma Djikstra, adalah dasar OSPF. sebagai protokol interior gateway (IGP). Protokol interior gateway, juga dikenal sebagai protokol *Routing* interior, dibuat untuk memungkinkan *router* dan *router* untuk terhubung satu sama lain. OSPF mendistribusikan informasi *Routing*-nya di dalam *router-router* yang tergabung ke dalam jaringan AS, yang dikelola oleh administrator lokal. OSPF menggunakan protokol *Routing link-state*, yang sangat efektif untuk pengiriman update informasi rute. OSPF adalah protokol *Routing* alternatif yang dapat menutupi kelemahan RIP. Selain itu, OSPF menggunakan prinsip multipath, yang memungkinkannya mempelajari berbagai rute dan memilih

lebih dari satu rute untuk menuju host tujuan. OSPF digunakan bersamaan dengan IP, yang berarti paket OSPF dikirim bersamaan dengan header paket data IP [20].

2.2 VPN

VPN merupakan kependekan dari *Virtual Private Network*, yang merujuk kepada sebuah terowongan virtual yang terenkripsi yang menghubungkan satu jaringan dengan jaringan lainnya. VPN Server dan VPN host melakukan proses autentikasi terhadap satu sama lain. VPN memfasilitasi koneksi antara dua jaringan seperti antara kantor dan cabang, atau antara pengguna remote dengan kantor pusat. Selama proses transfer data melalui jaringan VPN, data dienkripsi dan dienkapsulasi untuk menjaga keamanan. Data yang dipindahkan melewati terowongan sehingga terlihat seolah-olah memiliki saluran jaringan tersendiri, padahal sebenarnya proses transfer data tersebut menggunakan jaringan internet atau jaringan publik [21].

Virtual Private Network (VPN) adalah salah satu teknologi komunikasi yang memungkinkan pengguna untuk terhubung ke jaringan publik. Dengan menggunakan VPN, pengguna dapat mengakses jaringan publik dan bergabung dengan jaringan lokal. Dengan demikian, meskipun menggunakan infrastruktur jaringan publik, pengguna dapat memperoleh hak dan pengaturan yang sama seperti saat terhubung ke jaringan lokal atau kantor sendiri. VPN menggunakan jaringan internet berbasis TCP/IP sebagai media intranet, sehingga memungkinkan koneksi yang luas tanpa memerlukan biaya yang besar.

Teknologi VPN menyediakan 2 fungsi utama untuk penggunanya. Fungsi utama tersebut adalah sebagai berikut [22]:

1. *Confidentiality*
   Teknologi VPN memiliki sistem kerja mengEnkripsisemua data yang lewat melaluinya. Dengan menerapkan sistem Enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi Jaringan data *Client* dengan mudah. VPN memiliki teknologi yang dapat menjaga keutuhan data yang *Client*kirim agar sampai ketujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.
2. *Origin Authentication*
   Teknologi VPN memiliki kemampuan untuk melakukan otentikasi terhadap sumber-sumber pengirim data yang akan diterimanya.

Teknologi VPN mengamankan lalu lintas jaringan virtual, memberikan rasa aman bagi semua pemakai jaringan [23]. Untuk menyelesaikan tantangan industri, VPN harus memenuhi persyaratan berikut:

1. Autentikasi Pengguna;
2. Manajemen Pengalamatan;
3. Enkripsi Data;
4. Manajemen Kunci;
5. Dukungan Multiprotocol.

2.3 *Link state Routing*

Algoritma *link-state*, yang juga dikenal sebagai algoritma Dijkstra atau algoritma *Shortest Path First* (SPF), mengintegrasikan informasi topologi dengan informasi database. Berbeda dengan algoritma vector jarak yang tidak memiliki informasi yang akurat tentang jarak jaringan dan tidak mengetahui jarak antar *router*, algoritma *link-state* meningkatkan pemahaman tentang jarak *router* dan interaksinya. Dalam konteks ini, advertisement *link-state* (LSA) digunakan sebagai paket kecil informasi *Routing* yang dikirim antar *router*. Topological database, sebagai kumpulan informasi dari LSA-LSA, dan *Routing* table, sebagai daftar rute dan interface, merupakan komponen penting dalam algoritma *link-state* [24]:

a. Processor overhead
b. Kebutuhan memori
c. Konsumsi bandwidth

2.4 *Routing*

Routing adalah proses menentukan jalur dari host pengirim ke host penerima. *Routing* menentukan rute yang harus diambil oleh data untuk mencapai tujuan yang diinginkan. *Routing* melibatkan pemindahan data dari satu jaringan ke jaringan lain dengan cara meneruskan paket data melalui gateway. Setelah *router* mengetahui sumber dan tujuan data, tabel *Routing* dibuat. *Router* kemudian menggunakan informasi dalam tabel ini untuk menentukan port yang akan digunakan untuk meneruskan paket ke alamat tujuan. *Routing* bertujuan untuk menentukan arah datagram agar mencapai tujuan yang diinginkan. *Router* memerlukan informasi yang tepat untuk melakukan *Routing*, termasuk [25] :

1. Alamat tujuan/destination address.
2. Mengenal sumber informasi.
3. Menemukan rute.
4. Pemilihan rute
5. Menjaga informasi *Routing.*

3. METODE PENELITIAN

Pada bab metodologi penelitian ini menguraikan pendekatan yang digunakan dalam Implementasi *Routing* OSPF (*Open Shortest Path First*) *Single Area* Pada Jaringan VPN dengan *Access Site-to-Site*. Penelitian ini bertujuan untuk mengembangkan sebuah infrastruktur jaringan yang aman dan efisien dengan memanfaatkan teknologi VPN untuk menghubungkan beberapa lokasi secara virtual. Proses implementasi akan dieksplorasi melalui serangkaian tindakan, termasuk konfigurasi perangkat lunak, pengaturan protokol OSPF, dan pengujian kinerja jaringan. Tindakan-tindakan ini dirancang untuk memastikan bahwa VPN *Site to Site Multi Area* menggunakan *Routing* OSPF dapat beroperasi secara optimal,

menyediakan konektivitas yang aman dan efisien antara berbagai lokasi dalam sebuah organisasi.

3.1.Jenis Percobaan

Percobaan yang dilakukan pada jurnal ini ialah Implementasi *Routing* OSPF (*Open Shortest Path First*) *Single Area* Pada Jaringan VPN dengan *Access Site-to-Site*. Secara garis besar, tujuan dari teknologi "VPN" adalah untuk memastikan keamanan jaringan dengan menyediakan jalur koneksi yang aman dan pribadi melalui infrastruktur jaringan publik seperti internet. Ini memungkinkan pengguna untuk mengakses layanan dengan aman dari lokasi mana pun, sambil menjaga kerahasiaan dan integritas data saat berkomunikasi atau beraktivitas *online*.

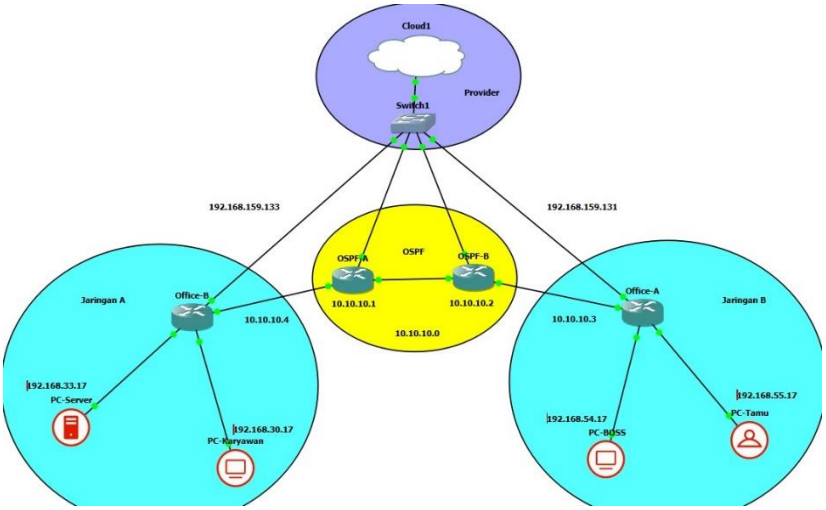
3.2.Alat dan Bahan Percobaan

Tahap Analisa kebutuhan, penulis mengumpulkan perangkat lunak dan perangkat keras yang diperlukan dalam proses pengimplementasian. Adapun alat yang digunakan dalam percobaan ini adalah sebagai berikut:

1. Perangkat Lunak (*Software*)
   a. Cisco Packet Tracer
   b. Mendeley Desktop
   c. *Microsoft Word Student* 2019
2. Sedangkan perangkat keras (*Hardware*) yang dibutuhkan antara lain:
   a. Laptop dengan prosessor AMD Ryzen 5
   b. *Local Drive up to* 512 GB

3.3.Tahap Perancangan Topologi

Topologi jaringan yang kami rancang digunakan untuk mengimplementasikan VPN (*Virtual Private Network*) *Site to Site Multi Area* Berbasis Routing OSPF (*Open Shortest Path First*).



Gambar 1. VPN (*Virtual Private Network*) *Site to Site Multi Area*

Pada topologi gambar 1 diatas menunjukan topologi VPN (*Virtual Private Network*) *Site to Site Multi Area* Berbasis *Routing* OSPF (*Open Shortest Path First*). Pada gambar yang dilabelkan warna ungu merupakan provider penyedia Internet, kmeudian Kanan dan Kiri yang berlabel warna biru merupakan Segmen Jaringan Kantor, kemudian yang di tengah dengan label Kuning merupakan OSPF Tunnel.

Tabel 1. *List* Perangkat yang digunakan

No	Nama Perangkat	Kegunaan	Jumlah Perangkat yang digunakan
1	*Router*	Berfungsi mengarahkan dan mengatur lalu lintas data antara berbagai perangkat dalam jaringan.	4
2	*PC Client*	Melakukan *Tes OSPF (Open Shortest Path First)* apakah sudah berhasil.	2
3	*Cloud untuk Internet dan Akses WinBox*	Melakukan Internet dan Akses WinBox	1
4	*Router Office A*	*(VPN, OSPF* dan *Firewall* pada Jaringan *A)*	1
5	*Router Office B*	*(VPN, OSPF* dan *Firewall* pada Jaringan B*)*	1
6	*Router OSPF B*	Untuk melakukan OSPF	1
7	*Router OSPF A*	Untuk melakukan OSPF	1

8	*PC*	Melakukan *Tes OSPF (Open Shortest Path First)* apakah sudah berhasil.	4

3.4.Tahap Percobaan

Dalam melakukan percobaan, ada beberapa tahapan yang dilakukan, yaitu seperti gambar di bawah ini:

Gambar 2. *Flowchart* Tahapan Percobaan

Berikut adalah penjelasan dari *flowchart* diatas :

1. **Mulai**

   Langkah awal dalam *flowchart*, Proses dimulai dengan studi literatur tentang VPN (*Virtual Private Network*) *Site to Site Multi Area* Berbasis *Routing* OSPF (*Open Shortest Path First*).

2. **Studi Literatur**

   Mencari beberapa jurnal yang terkait sebagai sumber referensi percobaan.

3. **Analisa Kebutuhan**

   Tahap ini sangat penting dalam percobaan ini, Peneliti mengumpulkan perangkat lunak dan perangkat keras yang diperlukan dalam proses pengimplementasian. Apabila tidak ada tahap ini maka tidak bisa menjalankan pengimplementasian.

4. **Perancangan Topologi**

   Pada tahap ini, penulis membuat Topologi yang nantinya akan digunakan untuk pengimplementasian.

5. **Konfigurasi pada Perangkat**

   Setelah perangkat *Cisco* terpasang, konfigurasi perangkat perlu dilakukan pada perangkat tersebut.

6. **Pengujian Koneksi dengan PING**

   Setelah konfigurasi selesai, pengujian koneksi perlu dilakukan untuk memastikan bahwa komunikasi antara *router* berjalan dengan baik. Apabila terdapat kesalahan pada tahap ini, maka secara otomatis, sistem akan menolak untuk ke tahap selanjutnya dan kembali ke tahap konfigurasi, tetapi jika berhasil, akan lanjut ke tahap selanjutnya.

7. **Selesai**

   Setelah semua langkah implementasi, simulasi, dan pengujian selesai, Implementasi VPN (*Virtual Private Network*) *Site to Site Multi Area* Berbasis *Routing* OSPF (*Open Shortest Path First*) dianggap selesai.

4. HASIL DAN PEMBAHASAN

Pada bab ini, hasil dari implementasi *Routing* OSPF (*Open Shortest Path First*) *Single Area* pada jaringan VPN dengan *Access Site-to-Site* akan disajikan dan dibahas secara langkah demi langkah. Setelah melakukan konfigurasi pada setiap protokol, bab ini akan memaparkan hasilnya dengan melakukan hasil akhirnya yaitu menguji respons sistem terhadap kondisi simulasi.

4.1. Konfigurasi pada Setiap Device

Konfigurasi pada setiap *device* merupakan langkah kunci dalam implementasi implementasi *Routing* OSPF (*Open Shortest Path First*) *Single Area* pada jaringan VPN dengan *Access Site-to-Site).* Setiap perangkat dalam jaringan, termasuk router, switch, dan perangkat lainnya, memerlukan penyesuaian khusus untuk memastikan sinkronisasi yang tepat dalam operasi *failover*. Dengan memulai konfigurasi pada setiap perangkat, kita

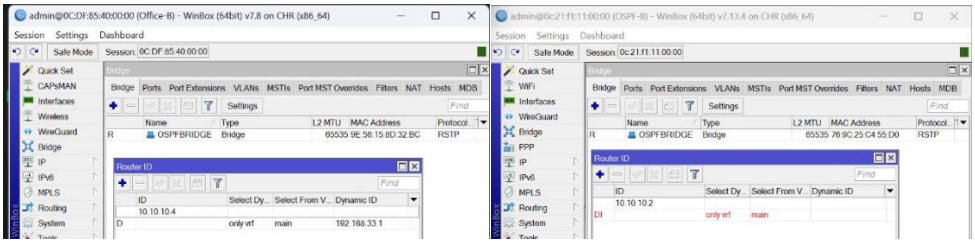
dapat memastikan bahwa setiap komponen jaringan berfungsi optimal dalam mendukung tujuan ketersediaan layanan internet yang tinggi. Ini mencakup pengaturan alamat IP, konfigurasi *interface*, dan penentuan area OSPF yang sesuai untuk setiap perangkat.

4.1.1. Langkah-Langkah *Setup* OSPF *Multi Area*

1. Pengaturan pada *Router* ID Pada semua *Router*

Pada Pengaturan ID *router* (*Router* ID) merupakan langkah awal yang penting dalam konfigurasi OSPF *Multi Area*. Setiap *router* dalam jaringan perlu memiliki identifikasi unik yang disebut sebagai *Router* ID.

Gambar 3. Pengaturan *Router* ID pada *Office* A dan OSPF A

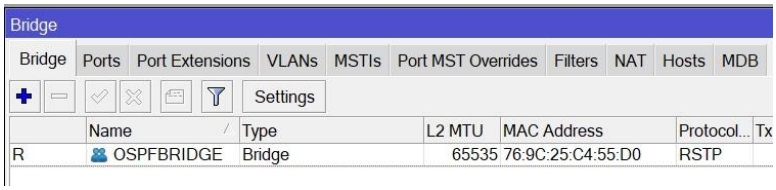


Gambar 4. Pengaturan *Router* ID pada *Office* B dan OSPF B

Jadi dengan melakukan pengaturan yang tepat pada *Router* ID di atas ini, setiap router dalam jaringan akan dapat dikenali secara unik dalam proses *routing* OSPF, yang menjadi dasar untuk pembentukan topologi jaringan dan pertukaran informasi *routing*.

2. OSPF untuk membuat Bridge

Dalam konteks ini, *router* bertindak sebagai "*bridge*" yang menghubungkan area OSPF. Berikut adalah gambar untuk menggunakan OSPF untuk menghubungkan jaringan secara efektif:

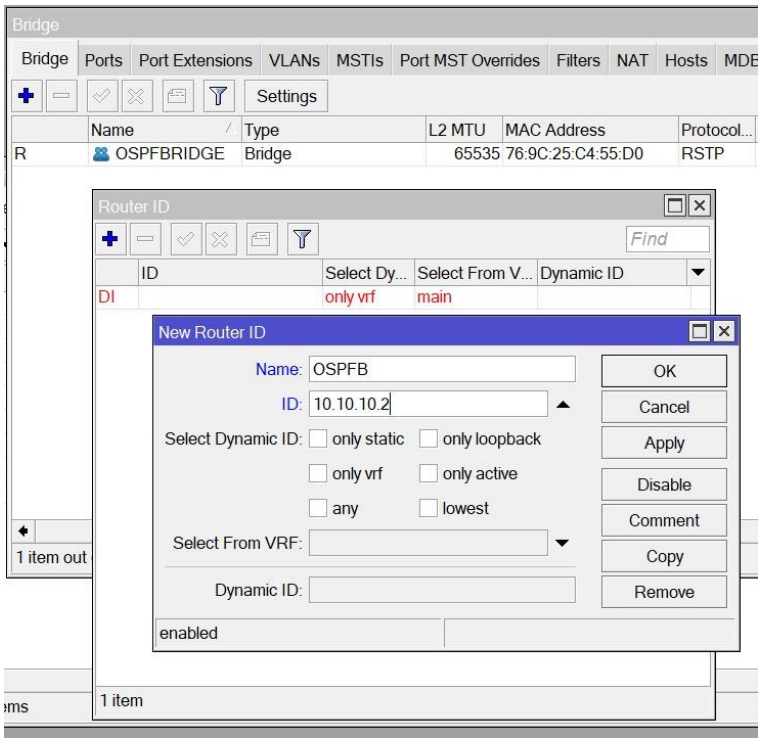


Gambar 5. Pengaturan *OSPF* untuk membuat *Bridge*

Pada gambar 5 di atas menunjukkan konfigurasi *bridge* pada perangkat MikroTik. *Bridge* ini adalah perangkat jaringan yang digunakan untuk menghubungkan dua atau lebih segmen jaringan. Gambar 5 di atas ini menunjukan informasi berupa Nama bridge pada gambar di atas adalah "OSPFBRIDGE", dan dengan alamat MAC 76:9C:25:C4:55:D0.

3. Membuat Router ID

Langkah selanjutnya setelah mengidentifikasi area OSPF adalah membuat *Router* ID. Berikut ini adalah gambar untuk membuat *Router* ID.

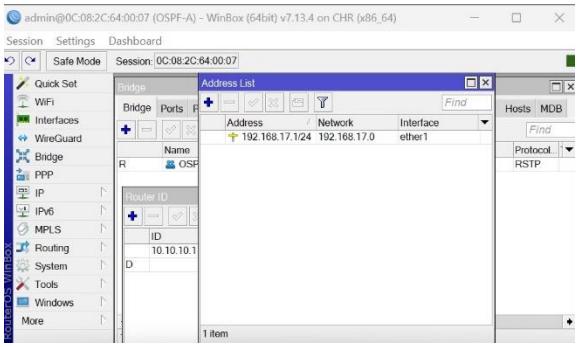


Gambar 6. Membuat *router* ID

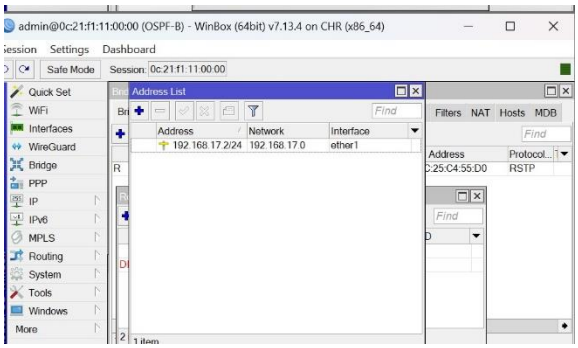
Gambar 6 di atas ini merupakan langkah membuat *router* ID sebagai contoh gambar di atas pada OSPFB dengan ID 10.10.10.2.

4. Tambahkan IP untuk Interface Area OSPF

Setelah membuat *Router* ID, langkah selanjutnya adalah menambahkan alamat IP untuk antarmuka yang akan digunakan dalam area OSPF.



Gambar 7. IP *Address* pada area OSPF A

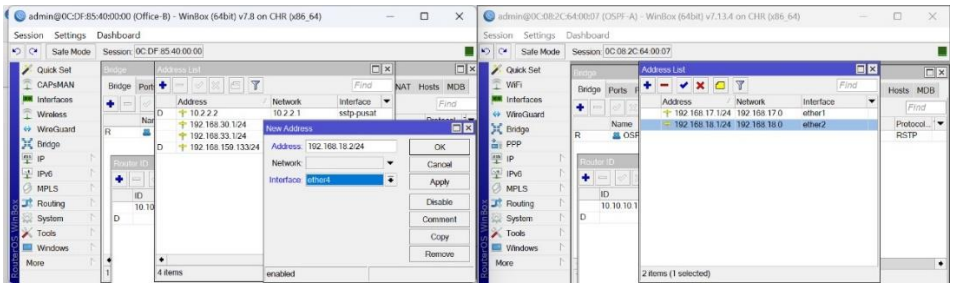


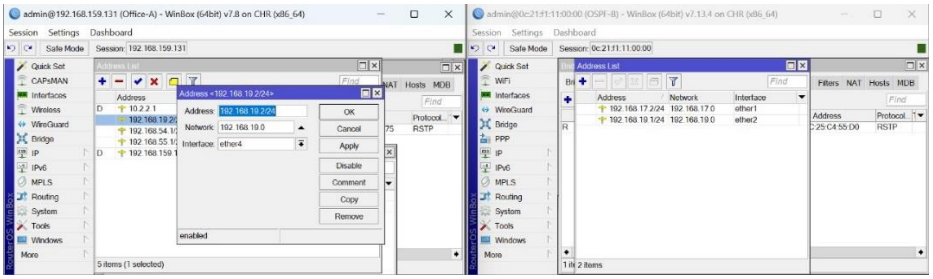
Gambar 8. IP *Address* pada area OSPF B

Pada gambar 7 dan 8 di atas ini merupakan tampilan setalah menambahkan IP *Address* pada area OSPF. Pada area OSPF A memiliki IP 192.168.17.1/24 dengan interface ether 1 dengan OSPF B memiliki IP 192.168.17.2/24 dengan interface ether 1.

5. Membuat Penghubung untuk IP Area VPN dan OSPF

Setelah menambahkan alamat IP untuk antarmuka yang terhubung ke area OSPF, langkah selanjutnya adalah membuat penghubung antara area VPN dan OSPF.

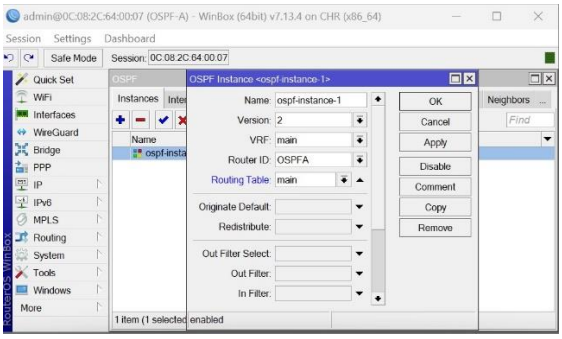




Gambar 9. Tampilan Setiap Router saat meng-*creat* untuk menghubung antara area VPN dan OSPF.

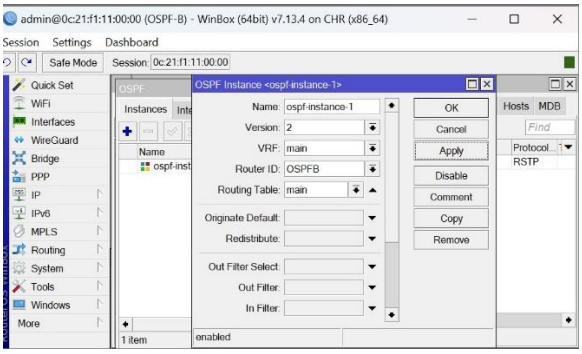
6. Tambahkan OSPF *Instance*

Setelah membuat penghubung antara area VPN dan OSPF, langkah selanjutnya adalah menambahkan OSPF *Instance*, Berikut ini merupakan gambaar saat menambahkan OSPF *Instance*.



Gambar 10. Tampilan *Instance* OSPF pada OSPF A

Pada gambar di atas merupakan Tampilan saat menambahkan OSPF Instance pada OSPF A yang mana pada gambar 10 di atas bersikan infomasi dengan nama ospf-instance-1 dengan version 2 Pada router OSPF A.

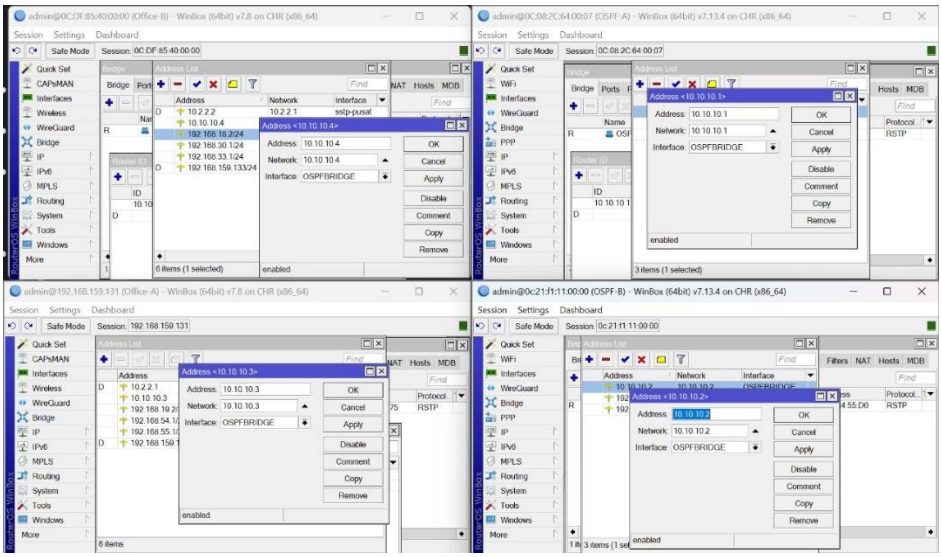


Gambar 11. Tampilan *Instance* OSPF pada OSPF B

Pada gambar di atas merupakan Tampilan saat menambahkan OSPF *Instance* pada OSPF B yang mana pada gambar 11 di atas bersikan infomasi yang sama dengan nama ospf-instance-1 dengan version 2 Pada router OSPF B.

7. Tambahkan IP pada semua router berdasarkan Router ID

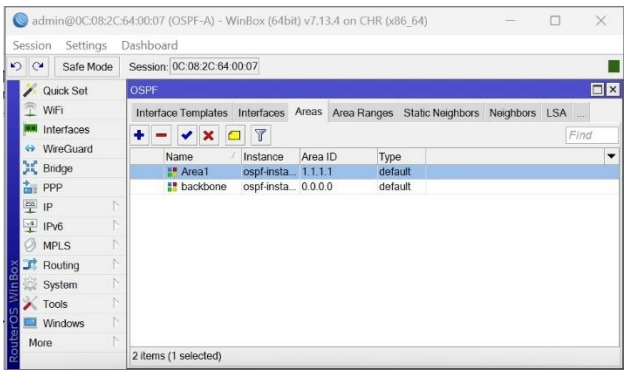
Setelah menambahkan OSPF *Instance,* selanjutnya adalah menambahkan alamat IP pada setiap router sesuai dengan Router ID yang telah ditetapkan sebelumnya.



Gambar 11. Tampilan setiap *router* saat menambahkan IP berdasarkan router ID

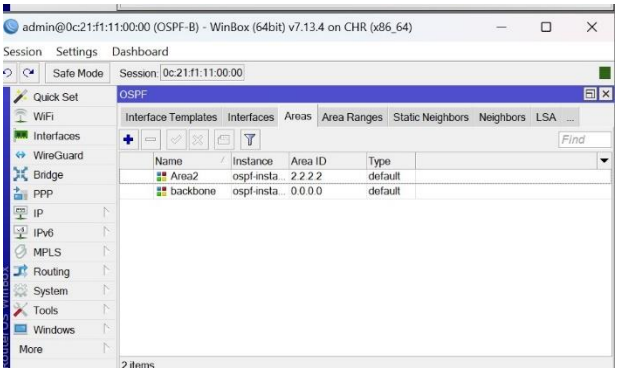
8. Tambahkan *Area* dan *Area* ID baru

Setelah menetapkan alamat IP pada setiap *router* berdasarkan Router ID, langkah selanjutnya adalah menambahkan *Area* dan menetapkan Area ID baru dalam konfigurasi jaringan.



Gambar 12. Tampilan setelah menambahkan area pada OSPF A

Pada gambar 12 di atas Dengan menambahkan area ID baru pada OSPF ini, Router OSPF A akan mengirimkan dan menerima informasi topologi jaringan OSPF dalam area-area yang sesuai, memungkinkan router untuk memilih jalur terpendek untuk mentransmisikan paket data.

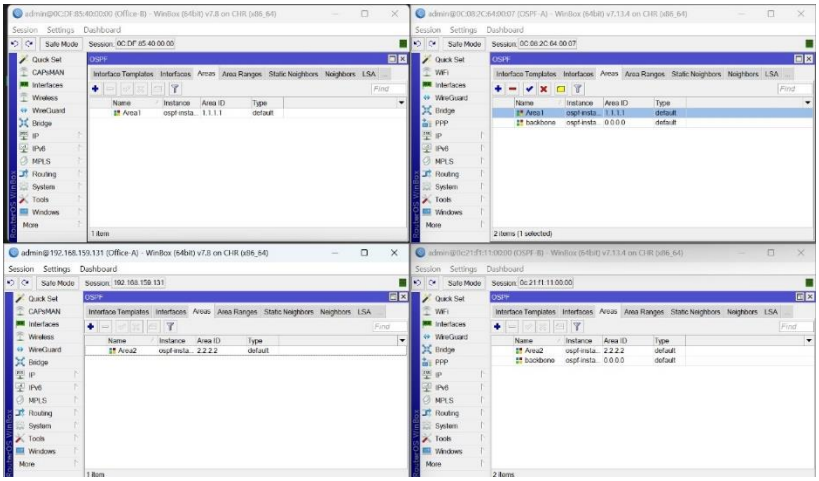


Gambar 12. Tampilan setelah menambahkan area pada OSPF B

Pada gambar 13 di atas dengan menambahkan area ID baru pada OSPF ini, Router OSPF B juga sama akan mengirimkan dan menerima informasi topologi jaringan OSPF dalam area-area yang sesuai, memungkinkan router untuk memilih jalur terpendek untuk mentransmisikan paket data.

9. Tambahkan Area pada *Router Office* dan Setel agar sama pada *Router* OSPF yang terhubung

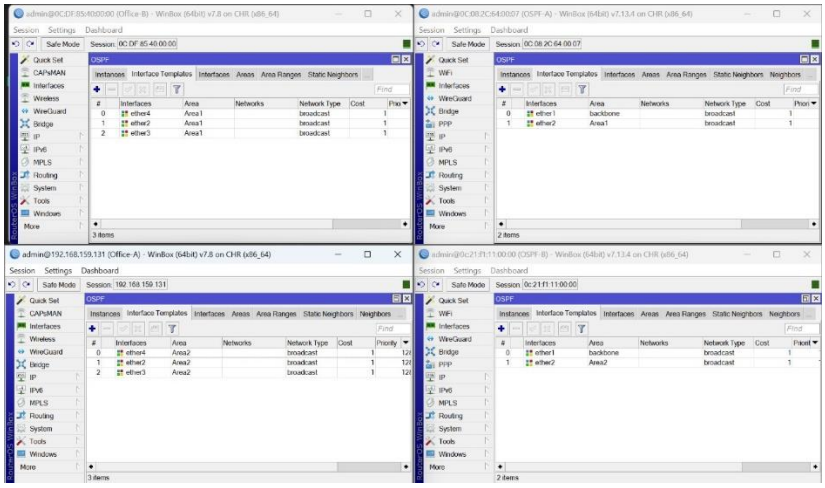
Setelah menetapkan alamat IP pada setiap router berdasarkan Router ID, langkah selanjutnya adalah menambahkan area pada router Office dan memastikan pengaturannya sama pada router OSPF yang terhubung



Gambar 13. Tampilan setelah menambahkan *Router Office* dan menyetel agar sama pada *Router* OSPF yang terhubung

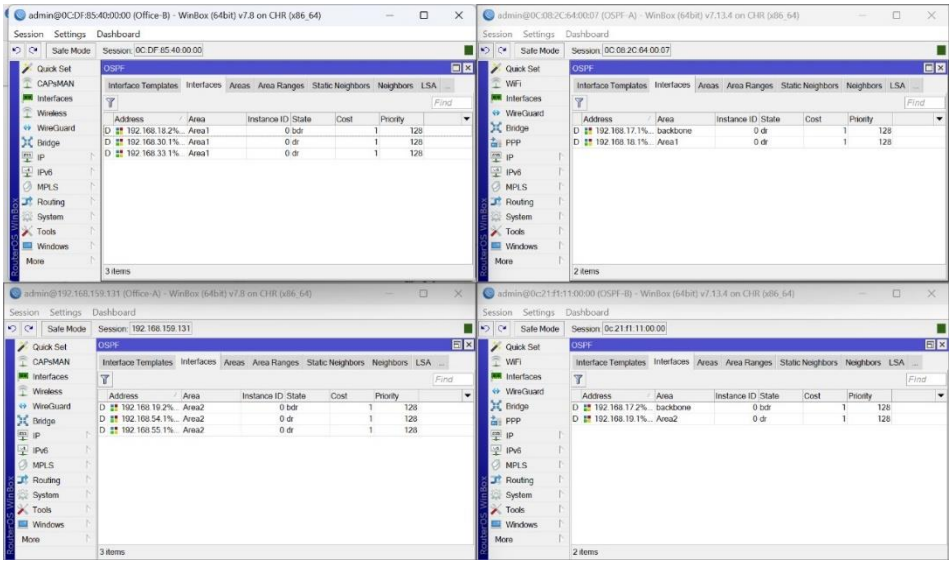
10. Tambahkan *Interface* berdasarkan Area

Langkah berikutnya adalah menambahkan antarmuka pada setiap router berdasarkan area OSPF yang telah ditetapkan sebelumnya. Ini memastikan setiap router terhubung dengan area OSPF yang sesuai, memungkinkan pertukaran informasi routing secara efektif dalam jaringan.



Gambar 13. Tampilan setelah menambahkan Router Office dan menyetel agar sama pada Router OSPF yang terhubung

11. Tampilan OSPF jika sudah Terkoneksi Multi-Area

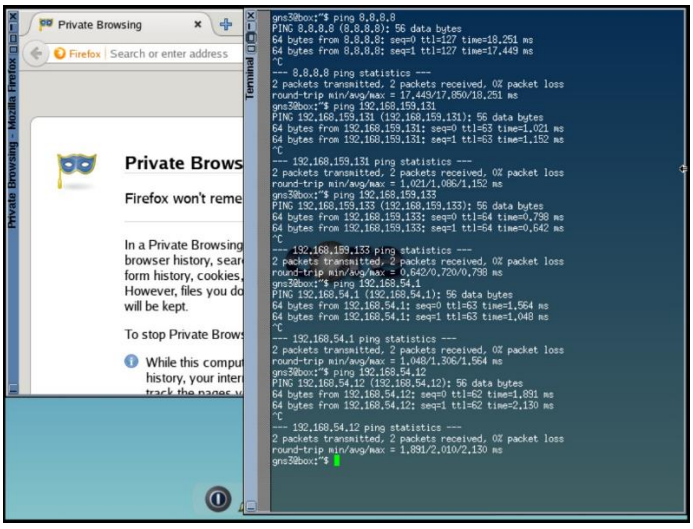


Gambar 14. Tampilan OSPF setelah terkoneksi

4.2. Hasil Percobaan

Berdasarkan konfigurasi jaringan yang telah dikonfigurasi pada bab sebelumnya, maka dilakukan percobaan tersebut sebagai berikut:

4.2.1. Percobaan ping PC A KE B

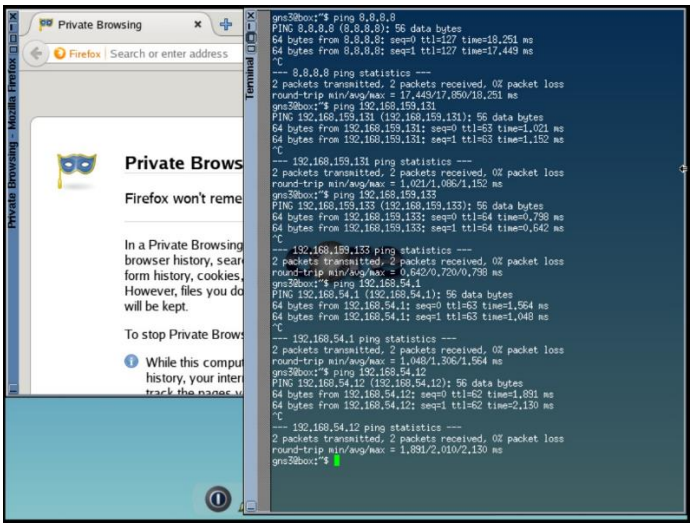


Gambar 15. Tampilan Hasil Ping pada PCA ke PCB

Hasil uji coba ping antara PCA dan PCB berhasil menunjukkan bahwa koneksi antara keduanya berfungsi secara optimal. Saat PC A mengirimkan paket ping ke PCB, PCB menerima dan meresponsnya tanpa hambatan. Keberhasilan respons ini menandakan bahwa paket telah berhasil mencapai tujuannya dan kembali ke pengirimnya, tanpa terdapat gangguan yang signifikan dalam lintasan jaringan.

Percobaan ping yang sukses antara PCA dan PCB menegaskan bahwa keduanya berada dalam jaringan yang sama dan dapat berkomunikasi dengan lancar. Selain itu, hal ini mengindikasikan bahwa konfigurasi IP dan pengaturan routing dalam jaringan telah dilakukan dengan tepat, memungkinkan aliran data yang lancar antara PCA dan PCB.

4.2.2. Percobaan ping PC B KE A



Gambar 16. Tampilan Hasil Ping pada PCB ke PCA

Begitupun sebaliknya Pada gambar 16 di atas Hasil uji coba ping antara PCB dan PCA berhasil menunjukkan bahwa koneksi antara keduanya berfungsi secara optimal. Saat PC B mengirimkan paket ping ke PCA, PCA menerima dan meresponsnya tanpa hambatan. Keberhasilan respons ini menandakan bahwa paket telah berhasil mencapai tujuannya dan kembali ke pengirimnya, tanpa terdapat gangguan yang signifikan dalam lintasan jaringan.

Percobaan ping yang sukses antara PCB dan PCA menegaskan bahwa keduanya berada dalam jaringan yang sama dan dapat berkomunikasi dengan lancar. Selain itu, hal ini mengindikasikan bahwa konfigurasi IP dan pengaturan routing dalam jaringan telah dilakukan dengan tepat, memungkinkan aliran data yang lancar antara PCB dan PCA.

5. KESIMPULAN

Pada percobaan kali ini kami penulis dapat memberi kesimpulan bahwasannya, hasil dari implementasi Routing OSPF (Open Shortest Path First) Single Area pada jaringan VPN dengan Access Site-to-Site dibahas secara rinci. Setelah melakukan konfigurasi pada setiap protokol, hasilnya dievaluasi melalui serangkaian langkah-langkah, termasuk pengujian respons sistem terhadap kondisi simulasi.

Konfigurasi pada setiap perangkat menjadi langkah awal yang krusial dalam mengimplementasikan Routing OSPF (Open Shortest Path First) Single Area pada jaringan VPN dengan Access Site-to-Site. Penyesuaian pada setiap perangkat, termasuk router, switch, dan perangkat lainnya, diperlukan untuk memastikan sinkronisasi yang tepat dalam operasi failover. Dengan memulai konfigurasi pada setiap perangkat, konsistensi dan optimalitas operasional dalam mendukung tujuan ketersediaan layanan internet yang tinggi dapat tercapai. Ini mencakup pengaturan alamat IP, konfigurasi interface, dan penentuan area OSPF yang sesuai untuk setiap perangkat.

Langkah-langkah yang dilakukan termasuk Pengaturan Router ID pada semua Router, OSPF untuk membuat Bridge, Membuat Router ID, menambahkan IP untuk Interface Area OSPF, membuat penghubung untuk IP Area VPN dan OSPF, serta menambahkan OSPF Instance. Langkah-langkah ini memastikan bahwa setiap router dalam jaringan dapat dikenali secara unik, hubungan antara area OSPF dan VPN terjaga, dan bahwa pertukaran informasi routing berjalan lancar.

Selanjutnya, penambahan Area dan Area ID baru pada konfigurasi jaringan membantu dalam pembentukan topologi jaringan yang efisien dan pemilihan jalur terpendek untuk mentransmisikan paket data. Pada akhirnya, pengujian dilakukan melalui percobaan ping antara PC A dan PC B, yang berhasil menunjukkan koneksi antara keduanya berfungsi secara optimal. Hal ini menegaskan bahwa konfigurasi IP dan pengaturan routing dalam jaringan telah dilakukan dengan tepat, memungkinkan aliran data yang lancar antara PC A dan PC B. Kesimpulannya, implementasi Routing OSPF Single Area pada jaringan VPN dengan Access Site-to-Site telah terbukti efektif dalam meningkatkan stabilitas dan kinerja jaringan.

DAFTAR PUSTAKA

[1] A. R. Rachmawati, E. Ramadhan and A. Rohmah, "Aplikasi Smart Province 'Jogja Istimewa': Penyediaan Informasi Terintegrasi dan Pemanfaatannya," *Maj. Geogr. Indones.*, vol. 32, 2018.

[2] H. Z. dan Q. Zhang, "A Comprehensive Survey on Secure Socket Tunneling Protocol (SSTP) in Virtual Private Network (VPN) Systems," *J. Netw. Comput. Appl.*, vol. 167, p. 102753, 2020.

[3] A. Y. K. and H. Sama, "Studi Analisis Kecepatan Internet Telkomsel di Kota Batam: Studi Geografis," vol. 1, 2020.

[4] H. A. Musril, "Penerapan Open Shortest Path First (Ospf) Untuk Menentukan Jalur Terbaik Dalam Jaringan," *J. Elektro dan Telekomun. Terap.*, vol. 4, no. 1, p. 421, 2017, doi: 10.25124/jett.v4i1.989.

[5] H. Nugroho, "Matematika Diskrit dan Implementasinya dalam Dunia Teknologi Informasi," *Deepublish*, 2015.

[6] A. Z. Al Ghivani, "Studi Perbandingan Routing Protokol BGP Dan EIGRP, Evaluasi Kinerja Performansi Pada Autonomous System Berbeda," vol. 7, no. 2, pp. 95–105, 2018.

[7] M. Mufadhol, "Simulasi Jaringan Komputer Menggunakan Cisco Packet Tracer," *J. Transform.*, vol. 9, no. 2, p. 64, 2012, doi: 10.26623/transformatika.v9i2.59.

[8] M. W. and J. Arora, "Improvment of Convergence Delay in OSPF by Using Backup Path Technique," vol. 11, no. 01, 2021.

[9] A. F. Syarief and D. A. Rochmah, "Distribusi Jaringan Publik Menggunakan Routing Ospf Dengan Metode Redistribusi Infrastruktur Terpusat," *J. Ilm. Inform. Komput.*, vol. 26, no. 3, pp. 217–232, 2021, doi: 10.35760/ik.2021.v26i3.5478.

[10] O. K. S. and M. Ihwani, "Analisis Perbandingan Penggunaan Metric Cost dan Bandwidth Pada Routing Protocol OSPF," *J. Penlitian Tek. Inform.*, vol. 01, 2017.

[11] H. Supendar, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," pp. 85–98, 2016.

[12] E. Umam, C., & Roza, "Perancangan Jaringan Keamanan Virtual Private Network (VPN)," pp. 23–30, 2016.

[13] L. C. et Al., "Performance Evaluation of SSTP VPN under Various Network Conditions," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 3, pp. 1245–1258, 2018.

[14] C. M. and E. S. Negara, "Analisis Kinerja Redistribusi Routing Protokol Dinamik," *Kumpul. Jurnal, Ilmu Komput.*, vol. 06, 2019.

[15] A. M. Lidya and A. Mulyani, "Implementasi Dynamik Routing Protokol OSPF," *J. Ilm. Sekol. Tinggi Teknol. Inf. NIIT*, vol. 17, no. 1, pp. 1–5, 2021, [Online]. Available: https://ejournal.upi.edu/index.php/TELNECT/article/view/40806

[16] H. A. Musril, "Penerapan Open Shortest Path First (OSPF) untuk Menentukan Jalur Terbaik dalam Jaringan," 2017.

[17] D. Mahpudin and S. Indriani, "Analisis Kinerja Routing Eigrp Dan Ospf Menggunakan Cisco Packet Tracer," *J. Sist. Komput. Unikom*, vol. 7, no. 1, pp. 1–6, 2018.

[18] A. P. N. Permana and R. Firmansyah, "Distribusi Jaringan Menggunakan Routing Ospf Dengan Metode Redistribution," *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 9, no. 1, pp. 519–532, 2018, doi: 10.24176/simet.v9i1.2030.

[19] Kukuh Aris Santoso, "Konfigurasi dan Analisis Performansi Routing OSPF pada Jaringan LAN dengan Simulator Cisco Packet Tracer versi 6.2 ," *J. Kaji. Tek. Elektro,*

vol. 1, no. 1, pp. 67–1278, 2016.

[20] 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, [Online]. Available: http://j-ptiik.ub.ac.id

[21] I. Ruslianto and U. Ristian, "PERANCANGAN DAN IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN PROTOKOL SSTP (SECURE SOCKET TUNNELING PROTOCOL) MIKROTIK DI FAKULTAS," vol. 4, no. 1, pp. 74–77, 2019.

[22] K. A. Farly, X. B. N. Najoan, and A. S. M. Lumenta, "Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi," *J. Tek. Inform. Unsrat*, vol. 11, no. 1, p. 143279, 2017.

[23] S. Halawa., "Perancangan Aplikasi Pembelajaran Topologi Jaringan Komputer Untuk Sekolah Menengah Kejuruan (Smk)," *Tek. Komput. Dan. J. Ris. Komput.*, pp. 66–71, 2016.

[24] Achmad, "Implementasi Routing Protocol Open Shortest Path First (Ospf) Pada Model Topology Ring," *Fakt. Exacta*, vol. 8, no. 2, pp. 92–99, 2015.

[25] M. R. Ariadi, "Pengertian Routing , Tabel Routing & Protokol Routing.," 2014.