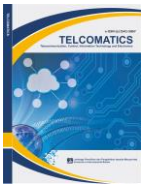
Available online at journal.uib.ac.id/index.php/telcomatics
Volume 8, Issue 1, June 2023

TELCOMATICS

ISSN (online) 2541-5867



Rancangan Jaringan *Highly Available* PT Pundi Mas Berjaya (PMB)

Stefanus Eko Prasetyo*, Gautama Wijaya, Nafisatul Hasanah, Jemmy, Putri Syahfira

Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam, Batam, 29444, Indonesia

ARTICLE INFO

Keywords:
High Availability, Network Hierarchy, Campus Network

Received: December 31, 2022
Revised: May 28, 2023
Accepted: June 25, 2023

***Corresponding author:**
E-mail: stefanus@uib.ac.id (Stefanus Eko Prasetyo)

DOI:
http://dx.doi.org/10.37253/telcomatics.v8i1.7359

ABSTRACT

In the digital age, networks are an important factor for implementing communication and exchanging information. Campus networks, which are private networks specifically designed for a particular institution, are essential for the institution because they provide access to the necessary information and services. However, campus networks are also vulnerable to security threats such as cybercrime and malware attacks. *Firewall* implementation can minimize these threats by controlling access to network services. Pundi Mas Berjaya (PMB), a company that provides software solutions to the global market, requires a highly available and redundant campus network. This research uses Cisco Packet Tracer to design and configure the network required by PMB. Implementing a highly available and redundant campus network with a hierarchical network model will improve the performance of the PMB campus network connectivity and security.

I. PENDAHULUAN

Pada era digital saat ini, jaringan merupakan elemen penting untuk mengimplementasikan komunikasi dan pertukaran informasi antara perangkat dan sistem. Penyebaran teknologi jaringan yang luas, seperti jaringan *wireless*, *ethernet*, dan *bluetooth*, memungkinkan kita untuk terhubung dan berkomunikasi dengan mudah, cepat, dan efisien [1].

Perkembangan teknologi jaringan juga memberikan peluang baru untuk berkomunikasi dan bekerja sama diberbagai bidang industri. Di bidang bisnis, jaringan sangat penting untuk memfasilitasi pertukaran informasi dan kegiatan operasi yang cepat dan efisien. Ini juga memungkinkan perusahaan untuk terhubung dengan pelanggan dan mitra dengan mudah. Selain itu, jaringan membantu perusahaan mengakses berbagai sumber daya dan layanan yang dapat meningkatkan efisiensi dan keuntungan.

Jaringan kampus merupakan salah satu implementasi jaringan yang terbaik untuk menghubungkan suatu institusi, seperti kampus atau universitas, dan perusahaan. Jaringan kampus adalah jaringan pribadi yang dirancang khusus untuk menyediakan konektivitas yang diperlukan untuk komunikasi dalam organisasi atau institusi tertentu. Jaringan kampus sangat penting bagi institusi karena menyediakan akses informasi dan layanan yang diperlukan oleh penggunanya. Namun, jaringan kampus juga menjadi sasaran utama *cybercrime* karena informasi dan data yang tersimpan sering tidak dilindungi dari serangan.

Implementasi *Firewall* merupakan solusi yang efektif untuk menjamin keamanan jaringan kampus. *Firewall* adalah sistem perangkat lunak atau hardware yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. *Firewall* memungkinkan kita untuk mengontrol akses layanan ke jaringan dan meminimalisir ancaman keamanan seperti *cybercrime* dan serangan *malware* [2].

Pundi Mas Berjaya (PMB) adalah perusahaan yang menyediakan solusi perangkat lunak untuk pasar global. Perusahaan ini memberikan solusi bisnis yang berkualitas kepada pelanggannya. PMB memerlukan infrastruktur jaringan kampus yang selalu tersedia dan mudah diakses oleh pelanggannya. Untuk itu, PMB membutuhkan jaringan kampus yang *highly available* (selalu tersedia) dan *redundant* (memiliki beberapa salinan). Dengan jaringan highly available, pelanggan dapat mengakses layanan PMB tanpa gangguan atau *downtime* (waktu tidak tersedia). Dengan jaringan yang redundant, PMB dapat menghandel *traffic* (lalu lintas jaringan) yang tinggi dengan mudah. Jika ada jaringan yang mengalami downtime atau gangguan, jaringan kampus PMB akan secara otomatis membagi *traffic* ke jalur lain.

Implementasi jaringan kampus yang highly available dan redundant dengan model jaringan hirarki akan meningkatkan kinerja konektivitas jaringan kampus di perusahaan PMB dan keamanan jaringan. Dengan demikian, perusahaan PMB dapat memanfaatkan potensi jaringan kampus dengan lebih optimal dan memberikan pelayanan yang lebih baik kepada pelanggan. Rancangan dan implementasi jaringan di kembangkan menggunakan metode Network Development Life Cycle.

II. KAJIAN PUSTAKA

Penelitian [3] membuat desain jaringan dengan performa yang lebih baik dan dapat meningkatkan skalabilitas sehingga proses bisnis organisasi dapat berjalan lancar tanpa adanya

gangguan. Hasil perancangan desain jaringan didasarkan pada model hirarki yang terdapat 3 lapisan, yaitu *Core layer* (Lapisan inti), *Distribution layer* (Lapisan distribusi) dan *Access Layer* (lapisan akses) dengan penerapan Intervlan pada masing-masing gedung kampus. Menggunakan model hirarki untuk jaringan kampus menjadi segmentasi yang baik dalam perancangan infrastuktur jaringan.

Penelitian [4] melakukan analisis untuk meningkatkan kinerja jaringan PT. Surya Antar Jaya dengan melakukan simulasi jaringan menggunakan aplikasi *Cisco Packet Tracer*. Perancangan desain jaringan PT. Antar Surya Jaya menggunakan topologi mesh dan VLAN sebagai pusat komunikasi. Simulasi dari topologi perusahaan tersebut dapat menggunakan *Cisco Packet Tracer*, namun pengujian kecepatan koneksi tidak akan sebaik *Cisco Packet Tracer* dan tidak sepenuhnya akurat.

Penelitian [5] dengan topik simulasi perancangan *spanning tree protocol* dengan topologi *ring* pada multi-akses *virtual local area network*. Tujuan dari penelitian ini adalah melakukan simulasi perancangan *Spanning Tree Protocol* (STP) dalam beberapa VLAN. Hasil simulasi menyatakan STP dapat bekerja baik dalam jaringan yang terdapat lebih dari satu VLAN, STP memonitoring sebuah jaringan agar tidak terjadi *looping* dan dapat mendukung jaringan yang *redundant*.

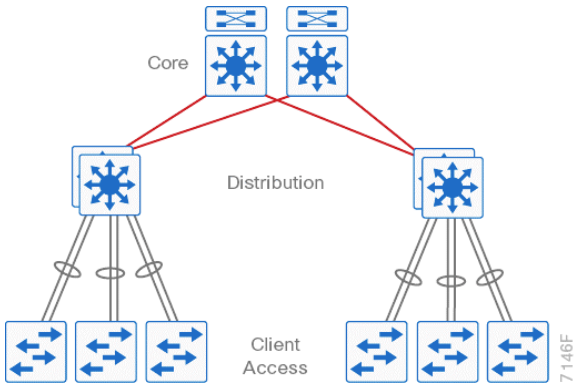
Penelitian [6] mengkaji topik keamanan jaringan di kampus dengan tujuan untuk menganalisis permasalahan keamanan jaringan yang ada di kampus. *Firewall* jaringan kampus yang semula hanya memiliki satu titik fungsi, telah diganti dengan *Firewall* kluster ganda yang terdiri dari dua komputer. Prinsip kerja dari *Firewall* ini adalah jika *Firewall* utama tidak aktif atau mengalami gangguan, maka kinerja *Firewall* akan segera digantikan oleh *Firewall* kedua agar dapat terus menjamin keamanan jaringan tanpa gangguan dari jaringan kampus.

A. Jaringan Kampus (*Campus Network*)

Topologi jaringan adalah susunan komponen jaringan seperti link, node dan lainnya dalam sebuah jaringan komputer. Struktur topologi jaringan dapat ditampilkan dalam bentuk fisik maupun logis. Topologi fisik adalah bentuk fisik dari bagaiaman perangkat terhubung satu sama lain, sementara topologi logis adalah cara dimana data mengalir di dalam jaringan, terlepas dari desain fisiknya.

Jaringan Local Area Network (LAN) adalah jaringan yang menyediakan akses ke layanan dan sumber daya komunikasi jaringan kepada pengguna akhir dan perangkat tersebar di satu lantai atau gedung.

Jaringan kampus dapat dibuat dengan menghubungkan beberapa LAN yang tersebar di wilayah geografis kecil. Desain jaringan kampus dapat bervariasi dari jaringan kecil yang menggunakan satu switch LAN hingga jaringan yang sangat besar dengan ribuan koneksi. Jaringan Kampus LAN menggunakan model desain hirarki untuk memecah desain menjadi kelompok atau lapisan modular. Memecah desain menjadi lapisan memungkinkan setiap lapisan untuk mengimplementasikan funsi tertentu, yang mempermudah desain jaringan, penyebaran dan pengelolaan jaringan [7].

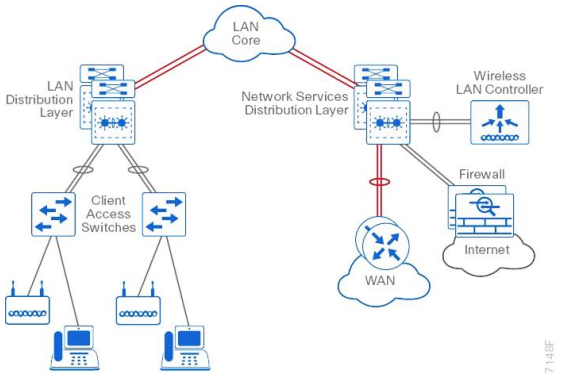


Gambar 1. Konsep Model Jaringan Hirarki

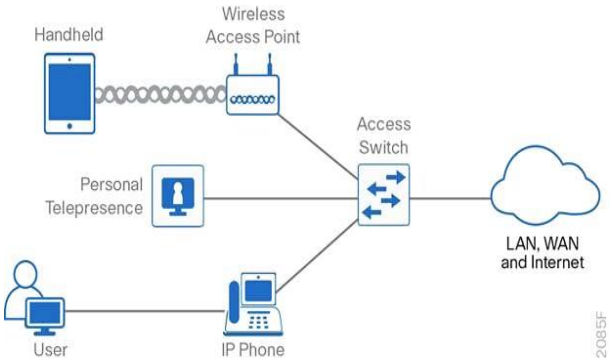
Jaringan model hirarki dibagi menjadi tiga lapisan seperti pada Gambar 1 yaitu Lapisan Inti (*Core Layer*), Lapisan distribusi (*Distribution Layer*), dan Lapisan Akses (*Access Layer).* Lapisan inti merupakan bagian terpenting dari jaringan LAN karena berperan dalam skalabilitas jaringan dan memiliki desain yang paling sederhana. Lapisan distribusi membantu mengatur kontrol kesalahan dan domain, sementara lapisan inti mewakili konektivitas yang terjaga selama 24 jam sehari, 7 hari seminggu, dan 365 hari setahun. Untuk memastikan jaringan bisnis yang modern dan terhubung dengan baik ke sumber daya bisnis, organisasi harus memiliki konektivitas lapisan inti yang mendukung hingga layer 3 untuk meningkatkan ketahanan dan stabilitas jaringan [8].

Lapisan berikutnya adalah lapisan distribusi (*Distribution Layer*) dapat mengurangi biaya operasional dengan meningkatkan efisiensi jaringan, yang menyebabkan kebutuhan memori berkurang, mengelompokkan kegagalan atau perubahan jaringan berdasarkan kesalahan domain, dan memproses sumber daya untuk perangkat di bagian lain dari jaringan. Lapisan distribusi juga meningkatkan ketersediaan jaringan dan kualitas layanan (QoS) dalam aliran aplikasi untuk memastikan bahwa aplikasi penting dan aplikasi multimedia berfungsi sebagaimana yang diharapkan. Topologi LAN menggunakan lapisan distribusi dapat dilihat seperti pada Gambar 2.

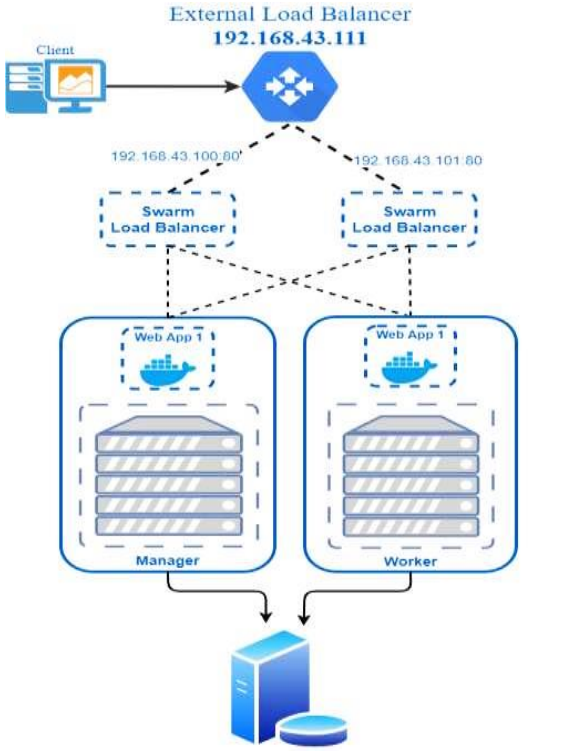
Lapisan akses (*Access Layer)* terhubung langsung dengan jenis perangkat akhir seperti komputer pribadi, telepon IP, AP nirkabel, CCTV, dan lainnya. Lapisan akses dapat mendukung banyak jaringan logis, memberikan keuntungan dari sisi kinerja, manajemen, dan keamanan. Topologi LAN menggunakan lapisan akses dapat dilihat seperti pada Gambar 3.



Gambar 2. Konsep Model Jaringan Lapisan Distribution



Gambar 3. Konsep Model Jaringan Lapisan Akses



Gambar 4. Desain Infrastruktur High Availability Dengan Metode Clustering

B. High Availability

High Availability merupakan suatu konsep yang mengacu pada kemampuan sebuah sistem untuk terus beroperasi tanpa mengalami gangguan atau downtime selama periode waktu yang sudah ditentukan. Ini bermakna bahwa sistem tersebut harus selalu tersedia untuk digunakan oleh pengguna. *High Availability* sangat penting bagi organisasi yang memiliki kebutuhan terhadap sistem yang harus selalu tersedia, seperti sistem pemrosesan transaksi, sistem pendukung keputusan, dan sistem komunikasi. *High Availability* dapat diukur dengan istilah "*nine*," semakin banyak angka sembilan, maka semakin tinggi pula *High Availability* (HA) dari sistem tersebut [9].

High Availability dicapai dengan menggunakan sumber daya bersama yang terhubung dengan beberapa sistem komputer atau node cluster. Jika salah satu node cluster mengalami kegagalan, fungsi tersebut akan ditangani oleh node cluster lainnya. Setelah periode transisi yang sangat singkat, sumber daya bersama tersebut akan tersedia kembali, konsep ini juga disebut dengan *failover* dapat di lihat pada Gambar 4.

C. Redudancy

Redudancy mengacu kepada ketersediaan jaringan dengan cara menambahkan jalur atau link cadangan sebagai jalur alternatif apabila terjadi kegagalan pada jalur utama. *Redudancy* dapat diterapkan pada berbagai lapisan jaringan, termasuk lapisan jaringan model hirarki yaitu *core layer*, *distribution layer*, dan *access layer*. Salah satu metode penerapan redundancy adalah menambahkan jalur cadangan dan menambahkan perangkat cadangan sebagai perangkat alternatif, jenis redundancy ini disebut juga dengan *redundancy link* dan perangkat [9].

III. METODOLOGI PENELITIAN

Metode yang digunakan dalam merancangan jaringan pada PT PMB adalah metode Network Development Life Cycle yang terdiri dari Analisis, Desain, Simulasi Prototyping, Implementasi, Pemantauan/Pengujian, dan Manajemen [10]–[12]. Berikut terdapat beberapa tahapan dalam pelaksanaan penelitian ini.

A. Analisis Kebutuhan

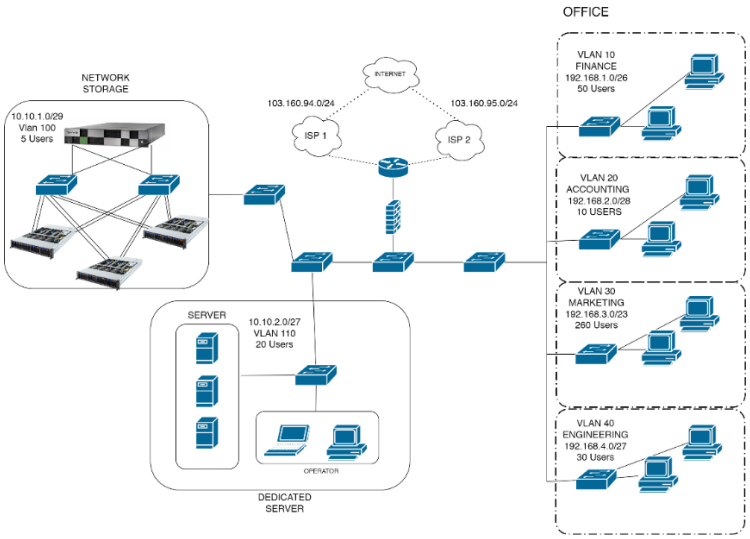
Melakukan analisis kebutuhan infrastruktur yang ada untuk membuat solusi jaringan yang lebih baik agar dapat mendukung *high availability* dan *redundant* serta memperkuat sistem keamanan jaringan Pundi Mas Berjaya. Adapun tahapan yang di lakukan adalah observasi. Tahapan observasi dilakukan secara langsung di perusahaan Pundi Mas Berjaya dengan tujuan melakukan observasi mengenai infrastruktur jaringan data center menuju *end user* di dalam satu gedung. Tahapan ini juga melakukan pengumpulan informasi mengenai spesifikasi dan berapa perangkat yang digunakan untuk mendukung konektivitas jaringan pada perusahaan tersebut.

B. Perancangan Desain Jaringan

Desain jaringan kampus perusahaan Pundi Mas Berjaya menggunakan aplikasi *draw.io*. Pada tahap ini terdapat dua desain arsitektur jaringan kampus PMB, yaitu desain awal jaringan PMB dan solusi yang akan dirancang yang berfokus pada kriteria yang dibutuhkan.

C. Simulasi dan Implementas Jaringan

Melakukan simulasi dari hasil rancangan desain jaringan kampus PMB menggunakan aplikasi *Cisco Packet Tracer*. Simulasi ini bertujuan untuk mengetahui bagaimana melakukan konfigurasi jalannya jaringan yang dirancang dan apakah desain jaringan tersebut dapat berjalan serta memenuhi kriteria *high availability* dan *redundancy*.



Gambar 5. Desain Awal Jaringan Kampus Perusahaan Pundi Mas Berjaya

D. Pengujian

Pada tahap ini dilakukan pengujian *ping* dan *trace route* masing masing perangkat setelah selesai dikonfigurasi untuk mengetahui apakah perangkat perangkat tersebut dapat terhubung dan saling berkomunikasi dengan baik. Tahapan pengujian ini dilakukan dengan mematikan salah satu router maupun *Firewall* dan mencoba kembali *ping* dan *trace route* untuk mengetahui apakah berhasil untuk melakukan *failover* atau gagal.

E. Evaluasi

Setelah jaringan di uji, maka dilakukan tahap evaluasi terhadap jaringan yang telah dirancang. Tahap ini lakukan untuk mengevaluasi secara keseluruhan tentang apakah jaringan tersebut dapat memenuhi semua kriteria yang dibutuhkan dan apakah jaringan tersebut dapat saling berkomunikasi dengan baik sesuai yang dibutuhkan.

IV. Hasil dan Pembahasan

Berdasarkan hasil observasi dari jaringan kampus perusahaan PMB, terdapat struktur jaringan PMB pada gambar 5. Terlihat bahwa desain arsitektur jaringan diatas terlihat bahwa jaringan kampus PMB telah menerapkan model jaringan hirarki dimana sebuah router menjadi *core layer* dengan dua ISP yang tersedia untuk menerapkan *redundancy*, kemudian terdapat *distribution layer* yang menghubungkan *server* dan jaringan *office* atau *end user* serta jaringan *access layer* dimana setiap divisi kantor memiliki *node* switchnya masing masing. Namun masih terdapat beberapa hal yang dikatakan tidak mendukung *high availability* dan *redundant*. Dari desain tersebut, masih terdapat *single point of failure* dimana jika salah satu dari switch mengalami gangguan maka jaringan tersebut akan mengalami *downtime* sehingga akan menggangu layanan jaringan PMB.

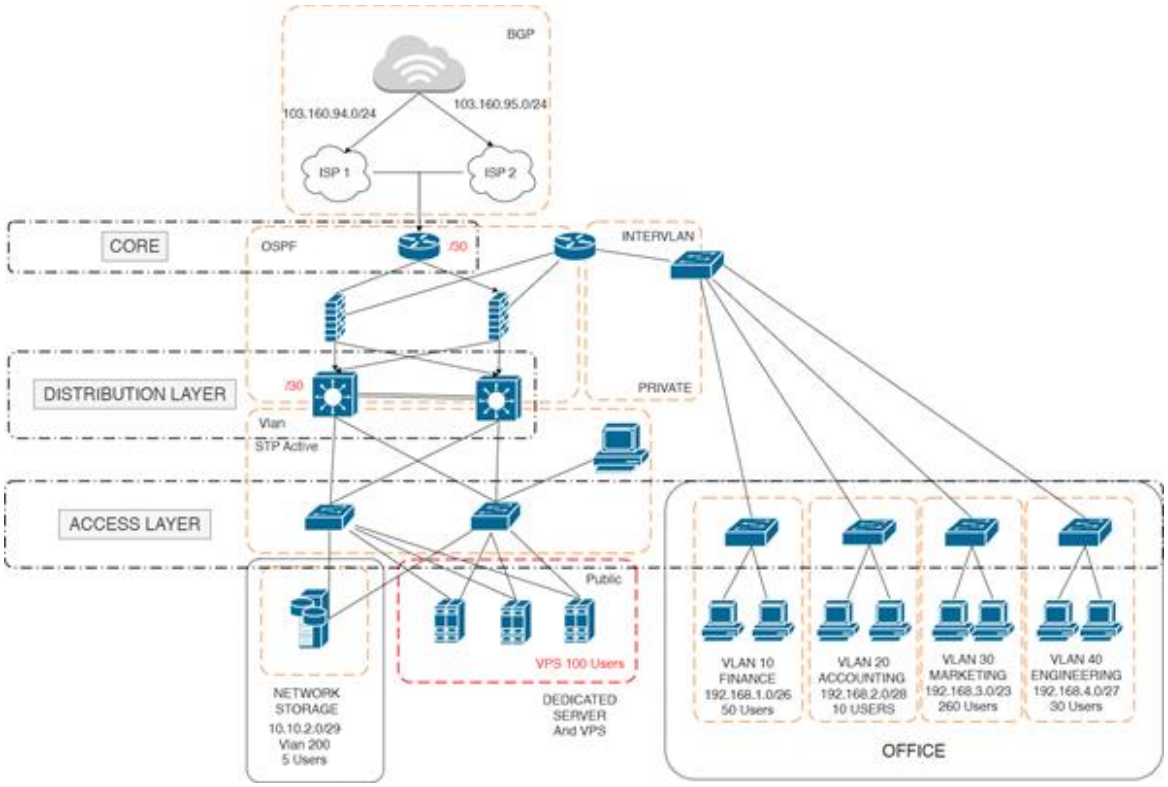
Jaringan Kampus PMB akan didirikan dengan model jaringan hirarki. Model jaringan hirarki akan dibagi menjadi 3 lapisan yaitu lapisan inti (*core layer*) yang merupakan lapisan teratas dari jaringan dan merupakan sumber dari keseluruhan jaringan, lapisan distribusi (*distribution layer*) yang berfungsi untuk menghubungkan lapisan inti dan lapisan akses, dan lapisan akses (*access layer*) merupakan lapisan paling bawah sebagai penghubung pengguna dengan jaringan kampus

Permasalahan jaringan kampus PMB diatas dapat ditangani dengan solusi desain jaringan pada Gambar 6. Dari Gambar 6 dapat dilihat bahwa rancangan jaringan kampus dengan model jaringan hierarki ini bertujuan untuk menerapkan *high availability* dan *redundant* serta mengatasi *single point of failure*. Dapat dilihat bahwa pada desain jaringan tersebut telah menggunakan dua *Firewall* yang terkoneksi dengan masing-masing *router* dan *multilayer switch*. Jika salah satu dari perangkat gagal atau mengalami gangguan, maka komponen yang lain dapat mengambil alih sehingga sistem jaringan tetap dapat berjalan dengan optimal. Selain itu, terdapat satu router yang terkoneksi ke *access layer* menuju bagian office agar dapat membantu mengelola aliran data yang keluar masuk dari dalam jaringan menjadi lebih baik dan membantu meningkatkan kinerja serta meningkatkan keamanan jaringan.

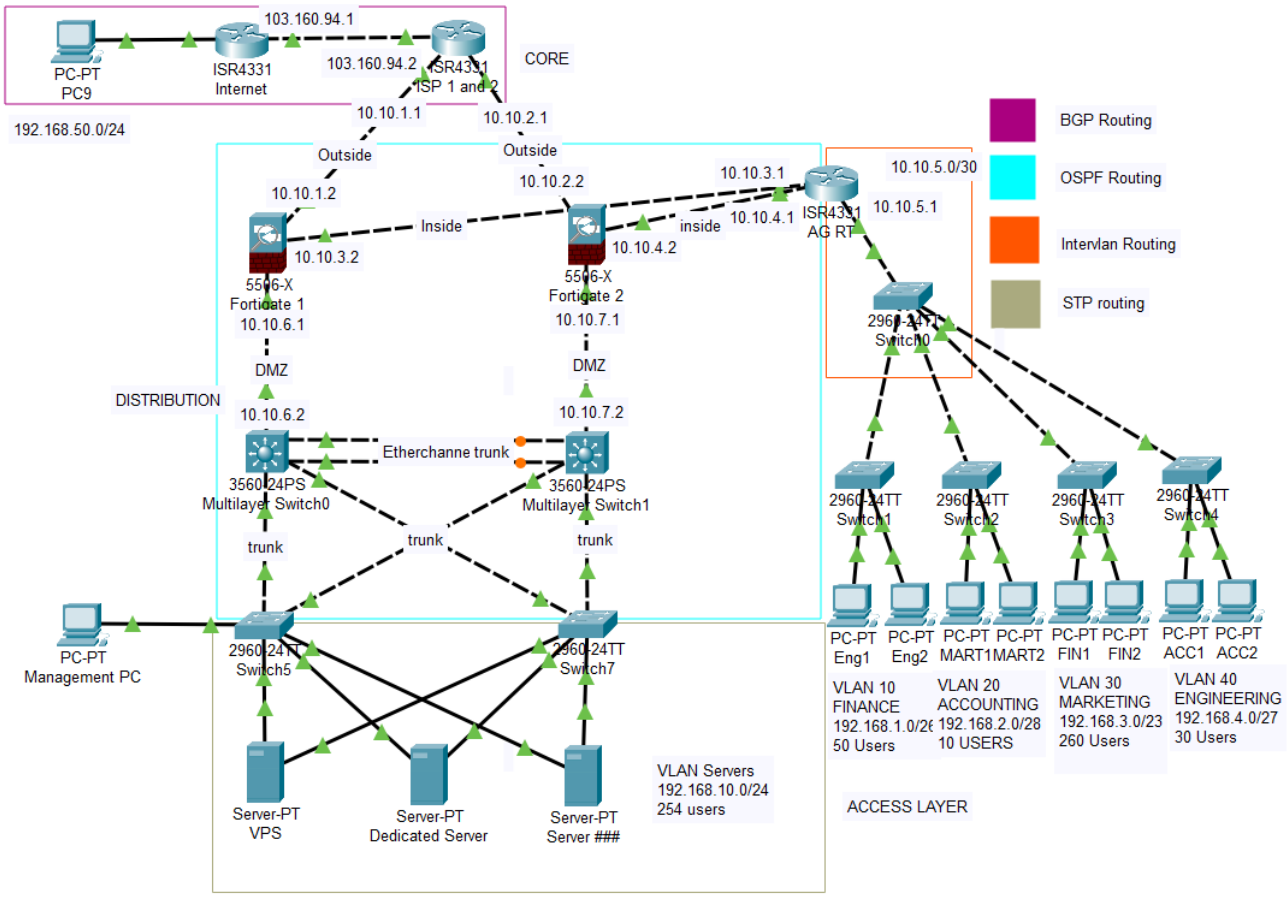
A. Implementasi

Pada implementasi desain jaringan yang telah dirancang disimulasikan menggunakan aplikasi *Cisco Packet Tracer* dengan gambar topologi sebagai berikut:

Sesuai dengan kebutuhan perusahaan PMB, dalam topologi tersebut terdapat satu *router* yang di uji coba dengan 1 ISP pada bagian *core layer* yang terkoneksi keluar internet dan di sekitar jaringan yang ada di gedung dengan melewati *Firewall* Firewall, terdapat 2 *Firewall* dan 2 *multilayer switch* pada bagian *distribution layer*, 7 switch sebagai *access layer* untuk *end user*. Terdapat juga 1 *router* yang terkoneksi dengan 2 *Firewall* pada *distribution layer* dan *access layer* di bagian *office* yang bertujuan untuk meningkatkan keamanan jaringan. Pada topologi tersebut juga ada 5 VLAN yang setiap VLAN mewakili satu divisi. Adapun tabel *addressing* tiap komponen yang dapat dilihat pada Tabel 1.



Gambar 6. Desain Simulasi Jaringan Dengan Aplikasi Cisco Packet Tracer



Gambar 7. Desain Jaringan Perusahaan Pundi Mas Berjaya Yang Highly Available dan Redudant

Tabel 1. Pengalamatan IP

Device	Interface	IP	Subnet
Router ISP	Gig 0/0/0	10.10.1.1 10.10.2.1 103.160.94.1	255.255.255.252
	Gig 0/0/1	10.10.2.1	255.255.255.252
	Gig 0/0/2	103.160.94.2	255.255.0.0
Fortigate 1	Gig 1/1	10.10.1.2	255.255.255.252
	Gig 1/2	10.10.3.2	255.255.255.252
	Gig 1/3	10.10.6.2	255.255.255.252
Fortigate 2	Gig 1/1	10.10.2.2	255.255.255.252
	Gig 1/2	10.10.7.1	255.255.255.252
	Gig 1/4	10.10.4.2	255.255.255.252
Multilayer Switch 0	Fa 0/1	10.10.6.2	255.255.255.252
	Vlan 100	192.168.10.1	255.255.255.0
Multilayer Switch 1	Fa 0/1	10.10.7.2	255.255.255.252
	Vlan 100	192.168.10.1	255.255.255.252
Access Switch 1	Vlan 200	192.168.5.1	255.255.255.252
AG RT	Gig 0/0/0	10.10.3.1	255.255.255.252
	Gig 0/0/1	10.10.4.1	255.255.255.252
	Gig 0/0/2	10.10.5.1	255.255.255.252
	Gig 0/0/2.10 (Vlan10)	192.168.1.1	255.255.255.192
	Gig 0/0/02.20 (Vlan20)	192.168.2.1	255.255.255.240
	Gig 0/0/2.30 (Vlan30)	192.168.3.1	255.255.254.0
	Gig 0/0/2.40 (Vlan40)	192.168.4.1	255.255.255.224

B. Penerapan Protokol *Routing*

Terdapat beberapa *routing* protokol diterapkan pada topologi jaringan ini. Pertama diterapkan *BGP Routing* di bagian Core Layer seperti tampak pada Gambar 8. *BGP Routing* diterapkan pada *core layer* ISP yang terkoneksi keluar internet. Karena BGP dapat mengelola *routing* yang sangat *scalable* dan membuat routing menjadi lebih efisien.

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/
PfxRcd
103.160.94.1    4   100       6       4        6    0    0 00:02:11        4
```

Gambar 8. *BGP Routing* di Bagian *Core Layer*

Selanjutnya *OSPF Routing* diterapkan pada *distribution layer* mulai dari jalur *core layer* yang terkoneksi dengan *Firewall* hingga ke *multilayer switch* dan menuju interface router *access layer office* seperti pada Gambar 9.

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.3 area 0
 network 10.10.2.0 0.0.0.3 area 0
```

Gambar 9. *OSPF Routing* dibagian *Distribution Layer*

Intervlan Routing diterapkan pada *access layer office* dengan router AG-RT seperti tampak pada Gambar 10. *Intervlan* digunakan untuk membagi jaringan *office* menjadi beberapa bagian VLAN yang terisolasi secara logis sehingga setiap VLAN memiliki keamanan yang terpisah dan tidak bisa diakses oleh perangkat.

VLAN akan diberi akses ke masing masing divisi dengan menggunakan satu switch layer-2 untuk masing-masing divisi. Gambar 11-14 adalah salah satu Access VLAN masing-masing pada Divisi Finance, Divisi Accounting, Divisi Marketing dan Divisi Engineering.

```
interface GigabitEthernet0/0/2.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.192
!
interface GigabitEthernet0/0/2.20
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.240
!
interface GigabitEthernet0/0/2.30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0/2.40
 encapsulation dot1Q 40
 ip address 192.168.4.1 255.255.255.224
'
```

Gambar 10. InterVLAN Routing Dibagian Access Layer Office

```
VLAN Name                              Status    Ports
---- --------------------------------- --------
------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   finance                           active    Fa0/2, Fa0/3
20   accounting                        active
30   marketing                         active
40   engineering                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Gambar 11. Salah satu Access VLAN pada Divisi Finance

```
VLAN Name                              Status    Ports
---- --------------------------------- --------
------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14,
Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18,
Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22,
Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   finance                           active
20   accounting                        active    Fa0/2, Fa0/3
30   marketing                         active
40   engineering                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Gambar 12. Salah satu Access VLAN pada Divisi Accounting

```
VLAN Name                              Status    Ports
---- --------------------------------- --------
------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14,
Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18,
Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22,
Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   finance                           active
20   accounting                        active
30   marketing                         active    Fa0/2, Fa0/3
40   engineering                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
```

Gambar 13. Salah satu Access VLAN pada Divisi Marketing

```
VLAN Name                              Status    Ports
---- --------------------------------- --------
------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14,
Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18,
Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22,
Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   finance                           active
20   accounting                        active
30   marketing                         active
40   engineering                       active    Fa0/2, Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Gambar 14. Salah satu Access VLAN pada Divisi Engineering

STP Routing diterapkan *access layer server* dimana terdapat beberapa *switch* yang saling terhubung untuk meningkatkan *high availability*. Penerapan *STP Routing* berguna untuk agar dapat mencegah terjadinya *loop* dan menjaga jaringan tetap stabil dan efisien. Gambar 15 merupakan konfigurasi STP Active-Pasive dimaksud.

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

Gambar 15. Konfigurasi STP Actvie-Pasive

C. Konfigurasi *Firewall* Menggunakan ASA 5506-X

Pada konfigurasi *Firewall* kami menggunakan *Firewall* ASA 5506-X yang ada pada *Cisco Packet Tracer*. Terdapat beberapa konfigurasi yang diterapkan dalam *Firewall* sebagai berikut:

```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.10.1.2 255.255.255.252
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 10.10.3.2 255.255.255.252
!
interface GigabitEthernet1/3
 nameif DMZ
 security-level 50
 ip address 10.10.6.1 255.255.255.252
!
```

Gambar 16. Penerapan Konsep Inside, Outside, dan DMZ Pada Firewall

Pada Gambar 16 diatas, diterapkan tiga konsep routing pada masing-masing *Firewall* yaitu jaringan *inside*, jaringan *outside* dan jaringan DMZ. Pada jaringan *inside* diterapkan pada jalur yang terkoneksi menuju *access layer* router *office.* Dengan *routing inside*, maka *traffic* jaringan yang berasal dari *inside* akan diperiksa oleh *Firewall* sebelum diarahkan masuk ke jaringan DMZ.

Jaringan *outside* adalah jaringan yang terhubung ke *Firewall* dibagian *core* menuju ke internet. Jaringan *outside* tidak terlindung oleh *Firewall*, tetapi akan diperiksa oleh *Firewall* sebelum diarahkan masuk ke jaringan DMZ

Jaringan DMZ diterapkan pada bagian *access layer* menuju *server*, jaringan DMZ adalah jaringan dengan zona terpisah yang terhubung ke *Firewall*, jaringan DMZ akan diperiksa oleh *Firewall* sebelum diarahkan menuju jaringan *outside* maupun *inside.*

```
access-group ACL in interface inside
access-group ACL in interface outside
access-group ACL in interface DMZ
```

Gambar 17. Daftar Access-Group Pada Kongurasi Firewall

Gambar 17 merupakan *access-group* untuk memberi akses routing pada setiap *interface* yang dapat dilihat pada Tabel 2.

Tabel 2. Interface *Firewall*

Device	Interface	IP Address	Jenis Access-Group
Firewall 1	Gig 1/1	10.10.1.2	Outside
	Gig 1/2	10.10.3.2	Inside
	Gig 1/3	10.10.6.1	DMZ
Firewall 2	Gig 1/1	10.10.2.2	Outside
	Gig 1/2	10.10.4.2	Inside
	Gig 1/3	10.10.7.1	DMZ

D. Hasil Pengujian Implementasi

Dengan konfigurasi jaringan diatas, *end user* bagian internet dan *office* bagian *access layer* dapat terkoneksi dengan *server*. Berikut adalah hasil *ping* dari *end user* dan *office* bagian divisi *finance* menuju *server* VPS pada Gambar 18 dan 19.

```
C:\>PING 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=124
Reply from 192.168.10.2: bytes=32 time<1ms TTL=124
Reply from 192.168.10.2: bytes=32 time<1ms TTL=124
Reply from 192.168.10.2: bytes=32 time<1ms TTL=124

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Gambar 18. Hasil Ping End User dari Internet.

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=125
Reply from 192.168.10.2: bytes=32 time<1ms TTL=125
Reply from 192.168.10.2: bytes=32 time=11ms TTL=125
Reply from 192.168.10.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
```

Gambar 19. Hasil Ping Salah Satu End User Office

Terdapat juga *trace route* untuk mengetahui jalan yang dilalui *end user* and *office* menuju *server* seperti yang di tunjukkan pada Gambar 20 dan Gambar 21.

```
Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     192.168.50.1
  2    0 ms     4 ms     0 ms     103.160.94.2
  3    0 ms     0 ms     0 ms     10.10.1.2
  4    0 ms     0 ms     0 ms     10.10.6.2
  5    *        0 ms     0 ms     192.168.10.2

Trace complete.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     192.168.50.1
  2    0 ms     0 ms     0 ms     103.160.94.2
  3    0 ms     0 ms     0 ms     10.10.1.2
  4    0 ms     0 ms     0 ms     10.10.6.2
  5    0 ms     0 ms     0 ms     192.168.10.2

Trace complete.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     192.168.50.1
  2    0 ms     0 ms     0 ms     103.160.94.2
  3    0 ms     0 ms     0 ms     10.10.1.2
  4    0 ms     0 ms     0 ms     10.10.6.2
  5    0 ms     0 ms     0 ms     192.168.10.2

Trace complete.
```

Gambar 20. Hasil Trace Route End User dar Internet

```
Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1   21 ms     0 ms     0 ms     192.168.1.1
  2    0 ms     0 ms     0 ms     10.10.4.2
  3    0 ms     0 ms     0 ms     10.10.7.2
  4    0 ms     0 ms     0 ms     192.168.10.2

Trace complete.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms     0 ms     0 ms     192.168.1.1
  2    0 ms     0 ms     0 ms     10.10.4.2
  3    0 ms     0 ms     0 ms     10.10.7.2
  4    1 ms     0 ms     0 ms     192.168.10.2

Trace complete.

C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms     0 ms     8 ms     192.168.1.1
  2    0 ms     0 ms     0 ms     10.10.4.2
  3    0 ms     0 ms     0 ms     10.10.7.2
  4    0 ms     0 ms     1 ms     192.168.10.2

Trace complete.
```

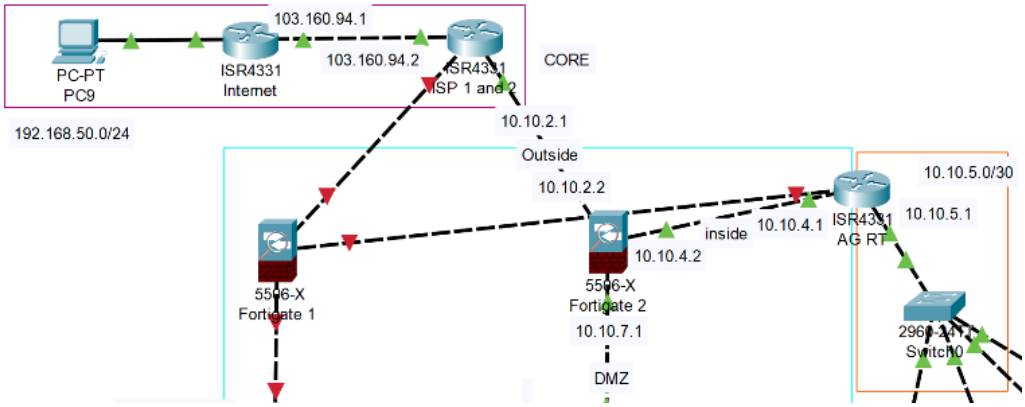
Gambar 21. Hasil Trace Route End User Office

Pengujian *trace route* dilakukan dengan 3 percobaan untuk masing-masing *route* komponen *end user*. Bisa dilihat bahwa kedua *trace route end user* internet maupun *end user office* seperti divisi *finance* melewati *routing interface Firewall* yang sama, yaitu Firewall 2. Hal ini bisa terjadi karena kedua *Firewall* bersifat *Active-Passive*. *Latency* yang di hasilkan juga cukup kecil, Pada jalur *end user* ke internet hanya memperoleh paling besar adalah 4ms pada saat pertama kali melintas jaringan. Sedangkan untuk *end user office* seperti *divisi finance* mendapatkan 21 ms untuk pertama kali melintas jaringan. Namun perlu diketahui bahwa pengujian kecepatan koneksi tidak sepenuhnya akurat dan hasil akan berbeda jika diimplementasi secara langsung [2].

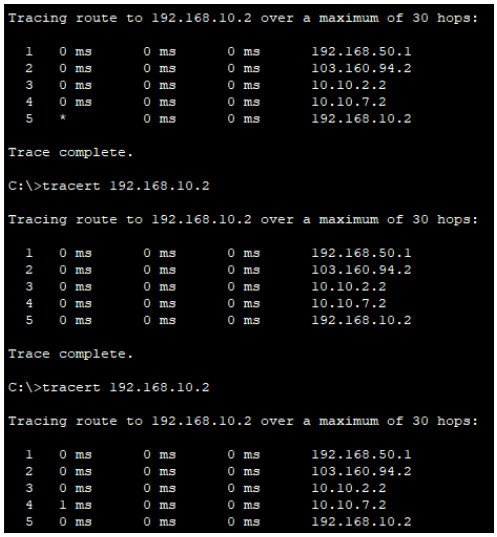
E. Hasil Pengujian High Availability dan Redudant

Pengujian *High Availibility* dan *Redudant* telah dilakukan dengan mematikan salah satu *Firewall* (Firewall 1) seperti pada Gambar 22 berikut:

Pada gambar diatas, ketiga *interface* Firewall 1 telah dimatikan sehingga tidak terjadinya koneksi jaringan yang melewati *Firewall* tersebut. Namun, jaringan tetap dapat berjalan dengan optimal karena terdapat Firewall 2 yang masih aktif sehingga terjadi *failover* dari Firewall 1 ke Firewall 2. Hasil *trace route* setelah *failover* seperti pada gambar 23 berikut:



Gambar 22. Scenario Pengujian Failover



Gambar 23. Hasil Trace Route Failover

Dari Gambar 23, terlihat bahwa *end user* tetap dapat melakukan *ping* menuju *ip server* dengan *route* ip Firewall 2 yaitu 10.10.7.2 dengan *latency* yang sama. Dari hasil pengujian tersebut, dapat dikatakan bahwa jaringan akan tetap berjalan dengan optimal dan tetap dapat dilindungi oleh *Firewall* meskipun terdapat salah satu komponen *Firewall* yang terjadi gangguan ataupun rusak.

V. KESIMPULAN DAN SARAN

Jaringan kampus dengan model jaringan hirarki menjadi solusi terbaik untuk jaringan perusahaan PMB. Model jaringan hirarki memiliki keunggulan seperti *high availability* dan *redundant*. Pada hasil pengujian, konfigurasi jaringan yang diusulkan telah berhasil menghubungkan *end user* bagian internet dan *office* bagian *access layer* menuju sebuah *server* di perusahaan PMB. Pengujian *high availability* dan *redundant* juga berhasil dilakukan dengan hasil *Firewall* melakukan *failover* dan jaringan tetap dapat berjalan dengan optimal.

VI. DAFTAR PUSTAKA

[1] H. Haeruddin *et al.*, "Rancangan Sistem Keamanan Rumah Berbasis IoT dengan Cisco Packet Tracer," *Telcomatics*, vol. 7, no. 1, p. 30, Jul. 2022, doi: 10.37253/telcomatics.v7i1.6767.

[2] Haeruddin, "Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS," vol. 5, no. 3, pp. 848–855, 2021, doi: 10.30865/mib.v5i3.2979.

[3] A. Tantoni, "Perancangan Blueprint Jaringan Intervlan Routing menggunakan Model Hirarki Desain Jaringan pada STMIK Lombok," *TRANSFORMASI*, vol. 15, no. 1, pp. 56–65, Jul. 2019, doi: 10.56357/JT.V15I1.183.

[4] F. Lisika, "LKP : Analisis Jaringan Komputer pada PT. Antar Surya Jaya," 2018.

[5] B. K. Damanik and M. Hamdani, "Simulasi Perancangan Spanning Tree Protocol dengan Topologi Ring pada Multi-Akses Virtual Local Area Network," *SINUSOIDA*, vol. 22, no. 3, pp. 42–49, Jul. 2020, doi: 10.37277/S.V22I3.750.

[6] X. Yang *et al.*, "Research on Network Security of Campus Network," *J Phys Conf Ser*, vol. 1187, no. 4, p. 042113, Apr. 2019, doi: 10.1088/1742-6596/1187/4/042113.

[7] A. K. Anam and T. Nurhastuti, "Perancangan Jaringan LAN Menggunakan Metode HSRP (Hot Standby Router Protocol)di PT.Citra Solusi Pratama," *Jurnal Teknologi Informasi*, vol. 8, 2022, [Online]. Available: http://ejournal.urindo.ac.id/index.php/TI

[8] T. Yusuf and A. A. Slameto, "Perbandingan Kinerja Redundant Link Menggunakan VRRP dan Load Balance pada Mikrotik," *Jurnal Teknologi Informasi*, vol. XVII, no. 2, pp. 11–19, 2022.

[9] J. Sidabutar *et al.*, "Desain Jaringan Komputer Terintegrasi Menggunakan Arsitektur Campus LAN," *Jurnal Jaring SainTek*, vol. 2, no. 1, pp. 25–32, 2020, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jaring-saintek

[10] F. Hadinata, S. E. Prasetyo, and H. Haeruddin, "Analisa Penggunaan Jaringan ZeroTier di Masa Pandemi Covid-2019," *Jurnal Ilmu Komputer dan Bisnis*, vol. 13, no. 1, pp. 85–93, May 2022, doi: 10.47927/jikb.v13i1.276.

[11] H. Haeruddin and E. Efendi, "Analisa Jaringan VPN MPLS L3 dan L2 Dimasa Pandemi COVID-2019 untuk Mendukung Work From Home," *Jurnal Ilmu Komputer dan Bisnis*, vol. XIII, no. 1, pp. 76–84, 2021.

[12] H. Haeruddin and K. Kelvin, "Analisa Penggunaan VPNL2TP dan SSTP di Masa Pandemi Covid-19," *Jurnal Ilmu Komputer dan Bisnis (JIKB) Mei-2022*, vol. XIII, no. 1, pp. 105–114, 2022, doi: 10.47927/jikb.v13i1.279.