JURNAL ELEKTRO DAN INFORMATIKA
SWADHARMA
P-ISSN : 2774 - 5775 | E-ISSN : 2774 - 5767
Volume 2 Nomor 1 – Januari 2022

JEIS
Penerbit
Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM)
Institut Teknologi dan Bisnis Swadharma (ITBS)

ISSN 2774 – 5775 | eISSN 2774-5767

JEIS : JURNAL ELEKTRO DAN INFORMATIKA
SWADHARMA

Volume 02 Nomor 01, Januari 2022

PENERBIT
Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM)
Institut Teknologi dan Bisnis Swadharma Jakarta

Kampus 1 Institut Teknologi dan Bisnis Swadharma Jakarta
Jl. Malaka No.3, Jakarta Barat, 11230
email : jurnal.jeis@swadharma.ac.id
http://ejurnal.swadharma.ac.id/index.php/jeis

PENGANTAR REDAKSI

Dengan ucapan puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa. Karena berkat rahmat dan hidayahnya Jurnal Elektro dan Informatika Swadharma (JEIS) Institut Teknologi dan Bisnis (ITB) Swadharma dapat diterbitkan. Jurnal Ilmiah ini diterbitkan untuk menampung tulisan dan menyebarluaskan ilmu pengetahuan di bidang elekro dan informatika, hasil penelitian dan pengembangan ilmu pengetahuan para sivitas akademika ITB Swadharma maupun kontribusi dari pihak lain.

Jurnal ilmiah ini memuat makalah hasil penelitian, studi literature, pemodelan, simulasi, studi pustaka, dan hasil pemikiran lainnya. Pada edisi Vol. 2 No.1 Januari 2022 ini memuat 10 (sepuluh) karya ilmiah di bidang elektro dan Informatika.

Redaksi mengucapkan terima kasih kepada para penulis yang telah mengirimkan papernya untuk diterbitkan pada edisi ini. Sementara beberapa paper lainnya yang sudah ada di redaksi namun belum dapat diterbitkan akan kami muat pada edisi berikutnya.

Redaksi mengharapkan saran dan kritik yang membangun dari seluruh pembaca, utamanya Sivitas Akademika ITB Swadharma demi meningkatkan mutu jurnal ilmiah pada edisi yang akan datang.

Managing Editor

ISSN 2774 – 5775 | eISSN 2774-5767

JEIS : JURNAL ELEKTRO DAN INFORMATIKA

SWADHARMA

Volume 02 Nomor 01, Januari 2022

DAFTAR ISI

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

IMPLEMENTASI METODE SWOT PADA ANALISIS JARINGAN AREA LOKAL SEKOLAH

Andy Dharmalau[1)], Harun Ar-Rasyid[2)], Muhammad Affan Iskandarsyah[3)]
[1,2,3)]Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma

Correspondence author: Andy Dharmalau, andy.d@swadharma.ac.id, Jakarta, Indonesia

Abstract

The Computer networks as a medium of data communication are currently increasing along with the development of the business world, trade, and education. SMK Bina Karya is an educational institution in the field of business and management where information technology is needed so that learning activities and administrative services run effectivel and effisien. For that we need a computer network. This network device allows the connection of information users remotely. To create a network, it is necessary to understand the concept of computer network topology that will be applied, because the type of topology that will be applied affects the speed of data communication. Local Area Network (LAN) is used as a transmission medium to conduct data transactions between computers and share printers so that it can make work easier. After setting the IP address, training IT Staff in the internal school and tidying up the cable layout, data transmission can run smoothly.

Keywords: computer network, local area network, information technology, star topology

Abstrak

Jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat seiring dengan perkembangan dunia usaha, perdagangan, dan pendidikan. SMK Bina Karya adalah institusi pendidikan di bidang bisnis dan manajemen dimana teknologi informasi sangat dibutuhkan agar kegiatan pembelajaran dan pelayanan tata usaha berjalan dengan efisien dan efektif. Untuk itu dibutuhkan sebuah jaringan komputer. Perangkat jaringan ini memungkinkan adanya hubungan para pengguna informasi dengan jarak jauh. Untuk membuat sebuah jaringan dibutuhkan untuk mengerti akan konsep topologi jaringan komputer yang akan diterapkan, karena jenis topologi yang akan diterapkan mempengaruhi kecepatan komunikasi data. Local Area Network (LAN) digunakan sebagai media transmisi untuk melakukan transaksi data antar komputer dan berbagi printer sehingga bisa mempermudah pekerjaan. Setelah melakukan pengaturan alamat IP, pelatihan SDM IT di internal sekolah dan merapikan tata letak kabel, pengiriman data dapat berjalan lancar.

Kata Kunci: jaringan lokal, komputer, sekolah

A. PENDAHULUAN

Jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat seiring dengan perkembangan dunia usaha, perdagangan, dan pendidikan.

SMK Bina Karya adalah institusi pendidikan di bidang Bisnis dan Manajemen dimana Teknologi Informasi sangat dibutuhkan agar kegiatan pembelajaran dan pelayanan tata usaha berjalan dengan efektif.

Selama ini pelayanan yang berjalan pada tata usaha terdapat beberapa kendala. Seperti yang sering dikeluhkan oleh beberapa guru dan asisten laboratorium komputer, yaitu untuk mendapatkan dan mencetak data murid memerlukan waktu yang lama dikarenakan masih menggunakan flashdisk. Sehingga para guru dan asisten laboratorium komputer harus mengantarkannya ke ruang tata usaha. Sedangkan lokasi dari tempatnya bekerja berada di lantai yang berbeda dengan ruang tata usaha. Untuk itu dibutuhkan sebuah jaringan komputer.

Pengertian Jaringan Komputer adalah sebuah sistem yang terdiri dari kumpulan komputer, printer, dan peralatan lainnya yang saling terhubung (Fitriansyah & Suryadi, 2021). Perangkat jaringan ini memungkinkan adanya hubungan para pengguna informasi dengan jarak jauh. Sehingga Informasi dan data bergerak melalui kabel – kabel yang memungkinkan pengguna jaringan komputer dapat saling bertukar data dan informasi (Suryantoro, Sopian, & Dartono, 2021).

Salah satu kemajuan teknologi informasi di bidang jaringan atau transmisi yang pada saat ini berkembang adalah penggunaan perangkat *Local Area Network* (LAN). *Local Area Network* (LAN) digunakan sebagai media transmisi untuk melakukan transaksi data antar komputer dan berbagi printer sehingga bisa mempermudah pekerjaan (Suryantoro et al., 2021). Teknologi informasi di bidang transmisi perangkat *Local Area Network* (LAN) sangat diperlukan dan banyak digunakan pada dunia pendidikan.

Local Area Network (LAN) di SMK Bina Karya masih belum tertata rapi dalam pengalamatan *IP Address* sehingga banyak terjadi permasalahan *IP Conflict* sehingga harus dilakukan perubahan *IP Address* secara tidak beraturan dan terjadi *IP Conflict* dengan perangkat yang lain. Berbagi data dan printer dengan berbeda lantai masih belum bisa dilakukan dikarenakan *IP Address* yang masih tidak beraturan sehingga hanya bisa terkoneksi dengan internet tetapi tidak bisa terhubung dengan perangkat yang berada didalam jaringan yang sama. Sehingga dibutuhkan dokumentasi *IP Address* secara terstruktur dan rapi agar komunikasi data lancar dan efektif (Nugroho, 2021).

Untuk membuat sebuah jaringan dibutuhkan untuk mengerti akan konsep topologi jaringan komputer yang akan diterapkan, karena jenis topologi yang akan diterapkan mempengaruhi kecepatan komunikasi data.

Pengertian topologi jaringan itu sendiri adalah suatu cara untuk menghubungkan perangkat telekomunikasi yang digunakan antara satu dengan perangkat yang lainnya sehingga membentuk sebuah jaringan (Trilaksono, Hiswara, & Ahmad, 2021).

Untuk membentuk sebuah jaringan dibutuhkan juga *Transmission Control Protocol* (TCP) dan *Internet Protokol* (IP). *Transmission Control Protocol* ini merupakan sebuah standarisasi yang ada pada sistem pengelolaan data untuk bertukar informasi dari satu perangkat komputer dengan beberapa perangkat komputer lainnya.

Protokol TCP ini punya banyak keunikan terutama prinsip kerjanya yang sistematis (Fitriansyah & Suryadi, 2021). *Internet Protocol Address* atau *IP Address* adalah nomor unik yang merupakan bilangan biner yang ditetapkan pada setiap perangkat (misalnya, komputer, *router*,

printer atau lain sebagainya) yang tergabung dalam kumpulan jaringan komputer dengan menggunakan *Internet Protocol* (Dartono, Usanto, & Irawan, 2021).

Pengguna bisa mengirimkan data atau pesan ke komputer lain dengan formasi angka-angka berurutan. Beberapa fungsi dari TCP/IP adalah sebagai berikut:

1. Melakukan pengiriman file yang terenkripsi
2. Menerapkan *remote login* pada komputer yang lain, meski berada pada jarak jauh sekalipun.
3. Mengirim dan menerima *computer mailing*.
4. Membuat fitur *Network File System*, fitur ini digunakan untuk *sharing file* seakan berkas tersebut merupakan milik pribadi pada komputernya.
5. Melakukan *remote execution*, yaitu perintah massal untuk menjalankan produk yang sama pada semua komputer yang tergabung dalam jaringan.
6. Melakukan fitur *name server*.

B. METODE PENELITIAN

Penelitian yang dilakukan dengan menggunakan metode penelitian kualitatif, dengan mengadakan peninjauan lapangan pada bulan April 2021 dengan lokasi penelitian di SMK Bina Karya Jakarta. Pengumpulan data penelitian dilakukan dengan cara sebagai berikut:

Metode Observasi dilakukan untuk mengumpulkan data dengan melakukan pengamatan langsung terhadap cara kerja guru dan asisten laboratorium komputer, dalam melakukan proses berbagi data dan mencetak dokumen. Lalu proses mencetak dokumen dari flashdisk di ruang tata usaha dengan komputer yang disediakan dan mendapatkan data dari operator sekolah.

Metode Wawancara juga dilakukan untuk mendapatkan informasi dengan cara bertanya langsung kepada Asisten Laboratorium Komputer dan salah satu guru di SMK Bina Karya.

Berikut beberapa pertanyaan yang diajukan:

1. Ada berapa pengguna komputer?
2. Ada berapa ruangan yang terkoneksi dengan jaringan?
3. Ada berapa printer yang harus terhubung ke komputer pengguna?
4. Bagaimana pemanfaatan jaringan area lokal untuk berbagi data dan mencetak dokumen?
5. Bagaimana berbagi data dan mencetak dokumen dengan jaringan area lokal di ruang tata usaha?
6. Bagaimana meningkatkan efektivitas dan efisiensi waktu dalam berbagi data dengan jaringan area lokal?

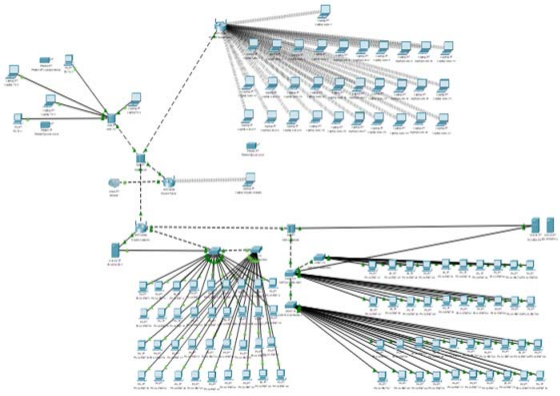
Selain itu juga dilakukan pengumpulan data dengan metode studi pustaka, dilakukan dengan cara mencari bahan berupa materi bacaan berupa buku, jurnal, makalah dan juga melakukan browsing data di internetn.

C. HASIL DAN PEMBAHASAN

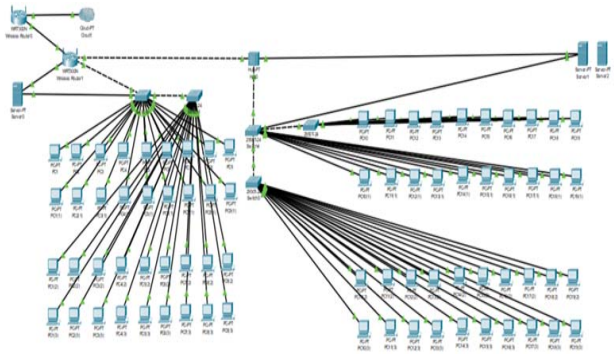
Pada SMK Bina Karya saat ini menggunakan jaringan LAN dengan topologi star untuk keperluan kerja setiap harinya karena jaringan LAN digunakan untuk menghubungkan komputer yang ada untuk saling bertukar data yang mereka kelola dan pemakaian resource hardware seperti: *server*, *modem*, *hub*, *switch* dan *printer*.

Pada saat ini SMK Bina Karya menggunakan topologi star. Jenis topologi jaringan komputer ini paling banyak digunakan dalam penerapan jaringan komputer baik di perkantoran maupun instansi dikarenakan lebih fleksibel dan mudah dalam perawatannya.

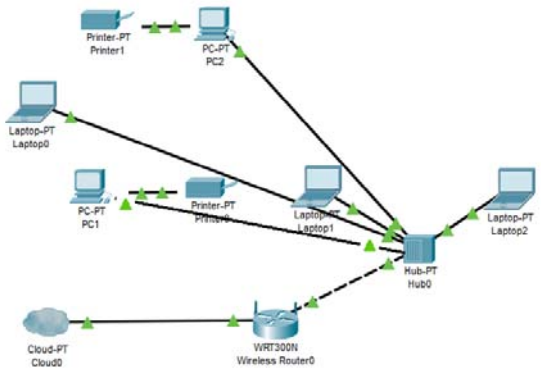
Berikut ini adalah gambartan denah dari topologi jaringan LAN yang pada saat ini digunakan pada SMK Bina Karya.



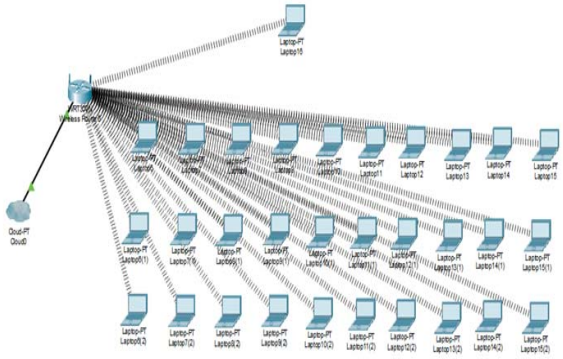
Gambar 1. Topologi LAN di SMK Bina Karya



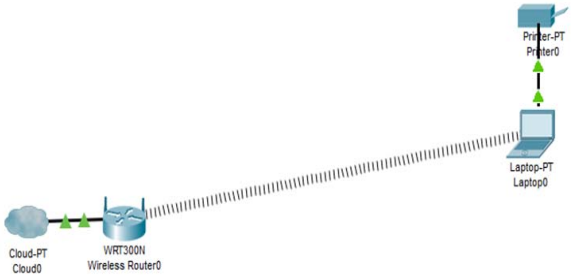
Gambar 2. Topologi Jaringan Ruang Laboratorium Komputer



Gambar 3. Topologi Jaringan Ruang Tata Usaha



Gambar 4. Topologi Jaringan Ruang Guru



Gambar 5. Topologi Jaringan Ruang Kepala Sekolah

Seperti yang dijelaskan sebelumnya, saat ini SMK Bina Karya menggunakan topologi star. Jenis topologi jaringan komputer ini paling banyak digunakan dalam penerapan jaringan komputer baik di perkantoran maupun instansi dikarenakan lebih fleksibel dan mudah dalam perawatannya.

Spesifikasi Perangkat Hardware yang digunakan di SMK Bina Karya.

Komputer kebanyakan menggunakan prosesor Intel core i5, RAM 4GB, HDD 500GB, OPS Windows 7, Microsoft Office 2007, Browser, Myob, SmadAv.

Internet dan Modem menggunakan Hypernet dengan kecepatan 10 Mbps dan

modem menggunakan MikroTik Router untuk mempercepat pengiriman data.

TP-LINK Hub merupakan Hub Distribution Layer yang digunakan untuk mengatur dan mendistribusikan data dengan jumlah port sebanyak 8 untuk menghubungkan pusat internet ke komputer client.

Printer yang digunakan merupakan printer EPSON L5190 dan HP Laserjet M15A di Ruang Tata Usaha yang dikoneksikan langsung ke jaringan lokal yang terhubung ke Komputer TU digunakan secara bersamaan agar mempermudah pengiriman data dari komputer client ke komputer lainnya dan EPSON L310 di Ruang Kepala Sekolah untuk bisa berbagi file ke Komputer TU.

Media Transmisi yang digunakan adalah kabel UTP Cat 5e. Kabel UTP tersebut menghubungkan antara hub dengan komputer client dan printer.

Router yang digunakan adalah Route TP LINK – WR840N di Ruang Laboratorium Komputer dan Ruang Guru. MikroTik di Ruang Kepala Sekolah. Berfungsi sebagai pengatur jaringan yang digunakan oleh komputer client agar pengiriman data ke komputer TU lancar.

Analisa Permasalahan Sistem Jaringan Saat ini. Pada dasarnya hampir semua kegiatan yang ada di SMK Bina Karya melibatkan Jaringan Komputer sebagai bentuk efisiensi kinerja. Contohnya penggunaan jenis hardware yang dipergunakan secara bersamaan (sharing) seperti printer. Namun ada beberapa kendala saat pengiriman file pada masing masing client dikarenakan tata letak kabel jaringan LAN yang ada saat ini tidak teratur dan sering kali terjadi traffic sehingga menyebabkan lambannya pertukaran data dan mempengaruhi kinerja PC.

Berdasarkan proses sistem kerja jaringan diatas khususnya pada saat pengiriman data antar client timbul suatu permasalahan, dikarenakan:

Pemasangan IP Address

Saat ini IP Address di Komputer yang ada di SMK Bina Karya merupakan IP yang dipasang secara DHCP dan tidak sama sehingga untuk melakukan berbagi data dan printer tidak bisa dilakukan serta sering terjadi konflik IP ketika dua alat menggunakan IP Address yang sama.

Sumber Daya Manusia

Saat ini belum ada SDM yang ahli untuk menangani masalah atau kerusakan pada sistem jaringan komputer di SMK Bina Karya. Akibatnya jaringan komputer yang ada jika mengalami kerusakan dapat berdampak melambatnya produktivitas karyawan. Kerusakan pada jaringan komputer ditangani sepenuhnya oleh IT dari luar Sekolah.

Tata Letak Kabel

Saat ini tata letak kabel belum tertata dengan baik dikarenakan masih banyak kabel yang berantakan di lantai sehingga mengganggu jalan pegawai dan berpotensi rusak dan kabel dari suatu komputer belum ada tandanya sehingga sulit jika ada permasalahan untuk mendeteksinya.

Analisis SWOT

Berdasarkan dari uraian struktur jaringan yang ada dan permasalahan, maka semua permasalahan tersebut dianalisa menggunakan metode SWOT. Analisa SWOT yang dilakukan dengan hasil analisanya dipetakan dalam tabel matrik sebagai berikut:

Tabel 1. Matrik SWOT

Strategi Internal		**Stength**	**Weakness**
	1	Perangkat komputer dan *printer* sudah terhubung untuk satu ruangan.	Penyusunan kabel saat ini masih belum sesuai dengan tata letak yang ditentukan sehingga menyebabkan kecelakaan kerja.
	2	Kemudahan dalam berbagi data dalam satu ruangan.	Pengaturan Alamat IP menggunakan *IP Dynamic* dan *IP Static* dalam pengalamatan pada *device* sehingga masih terjadi *IP Conflict*
Strategi External		**Opportunities**	**Threats**
	1	Merancang jaringan untuk pengaturan jaringan disetiap komputer agar menjadi stabil dan efisien.	Jaringan dapat tidak stabil setiap saat.
	2	Pengaturan koneksi jaringan internet akan lebih stabil.	Komunikasi data antar ruangan tidak berjalan dengan baik
Strategi Internal - External		**Strategi S-O**	**Strategi W-O**
	1	Membangun server jaringan agar pengaturan jaringan setiap komputer menjadi stabil dan efisien.	Pemanfaatan server jaringan untuk menstabilkan jaringan.
	2	Mengatur alamat IP jaringan internet agar koneksi lebih baik dan tidak terjadi *IP Conflict*.	Pemanfaatan pelatihan SDM IT dari dalam maupun perekrutan dari luar sekolah agar jika terjadi permasalahan jaringan dapat segera teratasi.
		Strategi S-T	**Strategi W-T**
	1	Menambah perangkat hub untuk dipasang di laboratorium komputer.	Melakukan pengecekan rutin terhadap setiap komputer dan koneksi jaringan agar bekerja secara maksimal.
	2	Mengatur alamat IP agar sesuai dan bisa terhubung dengan satu gedung.	Melatih SDM di internal sekolah dibidang Komputer dan Jaringan.

Usulan Sistem

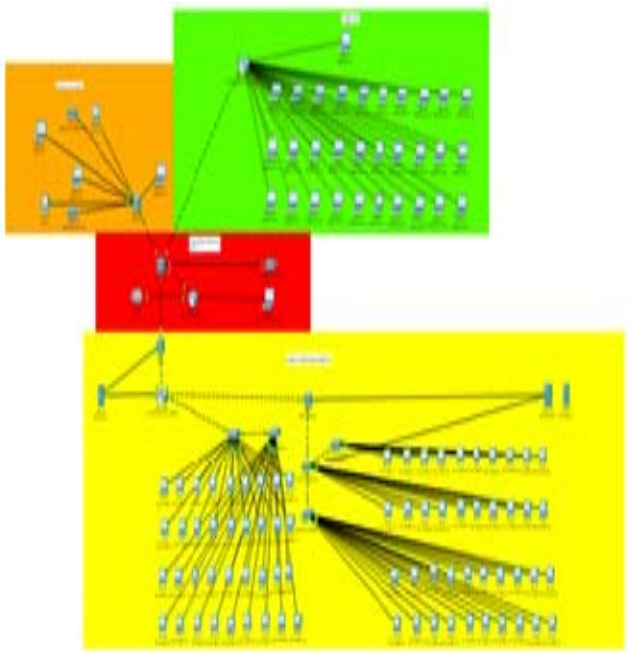
Setelah melakukan pengamatan dan analisa dari jaringan area lokal yang ada saat ini, maka penulis mempunyai beberapa usulan untuk mempermudah pekerjaan yaitu:

1. Atur IP Address pada setiap PC yang terhubung jaringan LAN menjadi Static, ini bertujuan untuk memudahkan komunikasi data dalam satu gedung untuk berbagi data dan printer
2. Memperbaiki tata letak kabel agar tidak mengganggu jalan dan tidak berpengaruh pada pengiriman data

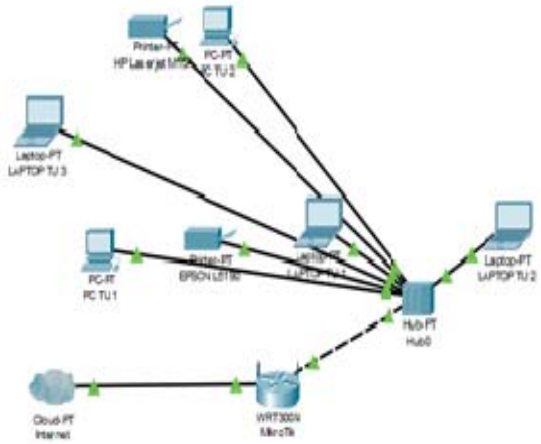
Topologi Usulan LAN

Pada topologi yang diusulkan akan ditambahkan satu unit hub yang akan digunakan untuk mengatur internet antara pusat dengan laboratorium komputer agar dapat bertukar data dengan komputer pusat secara langsung dan mudah.

Berikut ini gambaran usulan dari topologi jaringan LAN untuk SMK Bina Karya

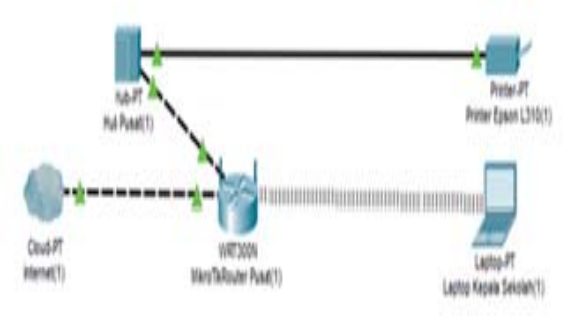


Gambar 6. Topologi Jaringan Usulan di SMK Bina Karya

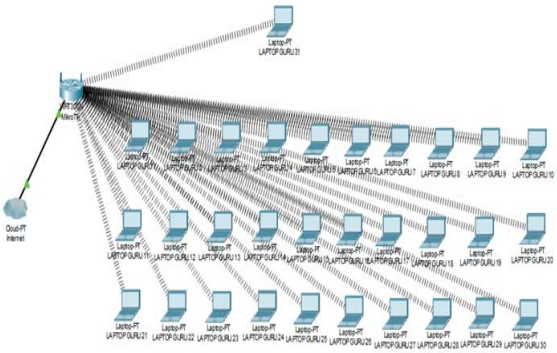


Gambar 7. Topologi Jaringan Usulan Ruang Tata Usaha Sekolah

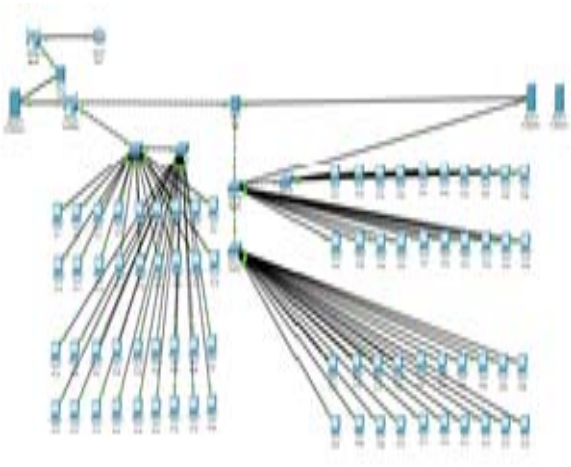
JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767



Gambar 8. Topologi Jaringan Usulan Ruang Kepala Sekolah



Gambar 9. Topologi Jaringan Usulan Ruang Guru



Gambar 10. Topologi Jaringan Usulan Ruang Laboratorium Komputer

Berikut dibawah ini merupakan tabel perbandingan jaringan LAN.

Tabel 2. Perbandingan Area Lokal jaringan LAN

Sistem Jaringan Area Lokal pada SMK Bina Karya	
Sistem yang berjalan	Sistem yang diusulkan
1.Tata Letak Jaringan	1. Tata Letak Jaringan
• Topologi Star	• Topologi Star
Dikarenakan jaringan mudah dikembangkan dan kontrol management lebih mudah karena semuanya terpusat ke satu titik.	Tata letak kabel harus dirapikan agar mempermudah maintenance jika ada kendala.
2. Koneksi Jaringan	2. Koneksi Jaringan
• *IP Address Dynamic*	• *IP Address Static*
Dikarenakan pengaturan *IP Address* secara otomatis lebih mudah tidak perlu pengaturan secara manual dan menghemat waktu pengerjaan.	Dikarenakan pengaturan alamat IP secara manual untuk menghindari permasalahan *IP Conflict* dan menghubungkan seluruh jaringan komputer menjadi satu agar mempermudah *sharing file* dan *printer* sehingga pekerjaan menjadi lebih mudah.

D. PENUTUP

Berdasarkan dari hasil yang telah diuraikan sebelumnya, maka pengalamatan IP Address di SMK Bina Karya tidak teratur karena masih menggunakan IP Dynamic. Tata letak kabel belum tersusun dengan rapi sehingga dapat berpengaruh terhadap kegiatan bekerja. Tidak dapat melakukan sharing file dan printer antar ruangan. Setelah melakukan pengaturan alamat IP, pelatihan SDM IT di internal sekolah dan merapikan tata letak kabel, pengiriman data dapat berjalan lancar.

Mengatur IP Address pada setiap komputer yang terhubung jaringan area lokal menjadi static, ini bertujuan untuk mempermudah dalam komunikasi data dan agar terhindar dari IP Conflict. Menambah perangkat Hub di Laboratorium Komputer sebagai perantara antara komputer server

dengan router. Untuk kedepannya untuk lebih baik dapat menggunakan wireless sehingga akan terlihat lebih rapi dan terhindar dari putusnya jaringan akibat kabel yang terganggu.

E. DAFTAR PUSTAKA

Dartono, Usanto, S., & Irawan, D. (2021). Penerapan metode per connection classifier (pcc) pada perancangan load balancing dengan router mikrotik. Jurnal Elektro Dan Inormatika Swadharma(JEIS), 1(1).

Fitriansyah, A., & Suryadi. (2021). Rancangan E-repositori Untuk Mendukung Knowledge management System (kms) Pada SMA PGRI 24 Jakarta. Jurnal Rekayasa Informasi Swadharma(JRIS), 1(2).

Nugroho, P. A. (2021). Kontrol Lampu Gedung Melalui WIFI ESP8266 Dengan Web Server Lokal. Jurnal Elektro Dan Inormatika Swadharma(JEIS), 01(2).

Suryantoro, H., Sopian, A., & Dartono. (2021). Penerapan Teknologi Fortigate Dalam Pembangunan Jatingan VPN-IP Berbasis IPSEC. Jurnal Elektro Dan Informatika Swadharma(JEIS), 01(1).

Trilaksono, A. R., Hiswara, I., & Ahmad, A. (2021). Rancangan Sistem Diskless Untuk Game Center Menggunakan Aplikasi CCBOOT. Jurnal Elektro Dan Informatika Swadharma, 01, 21–25.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

PERANCANGAN JARINGAN KOMPUTER RT/RW NET MENGGUNAKAN JALUR KOMUNIKASI POWER LINE (PLC) DI PERUMAHAN TAMAN BERDIKARI SENTOSA

Prasetyo Adi Nugroho
Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma

Correspondence author: Prasetyo Adi Nugroho, pras_engineer@yahoo.co.id, Jakarta, Indonesia

Abstract

RT/RW Net is a non-governmental computer network within the scope of RT/RW. Building an RT/RW Net in the Taman Berdikari Sentosa housing estate is a concept where several computers in a housing or block can be connected and can share data and information, express opinions, conduct polls, and even elect RT/RW. The RT/RW net network will be built using a power line (PLC) communication line. Power Line Communication (PLC) is a technology that supports computer networks on a small scale such as a LAN, RW/RW net, which can provide convenience in installation tasks to produce high-speed computer networks. In principle, the Powerline used functions as a medium that converts digital data to electric current so that the data can be sent via a power cable. Building an RT/RW Net network using Power Line is no different from building an RW/RW Net in general. The difference only lies in the data transmission media used, Power Line uses electric cables while RT/RW Net generally uses cables such as UTP, Fiber Optic, Coaxial, and wireless networks.

Keywords: RT/RW Net, Network, Power Line

Abstrak

RT/RW Net adalah jaringan komputer swadaya masyarakat dalam ruang lingkup RT/RW. RT/RW Net perumahan Taman Berdikari Sentosa adalah suatu konsep dimana beberapa komputer dalam suatu perumahan atau blok dapat saling terhubung dan dapat berbagi data serta informasi, mengemukakan, pendapat, melakukan polling, bahkan pemilihan ketua RT/RW. Jaringan RT/RW net dibangun menggunakan jalur komunikasi power line (PLC). Power Line Communication (PLC) merupakan suatu teknologi yang mendukung jaringan komputer dalam skala kecil seperti sebuah LAN, RW/RW net, yang bisa memberikan kemudahan dalam tugas-tugas instalasi untuk menghasilkan jaringan komputer dengan kecepatan tinggi. Secara prinsip Powerline yang digunakan berfungsi sebagai media yang mengubah data digital ke arus listrik agar data tersebut dapat dikirimkan melalui kabel listrik Membangun jaringan RT/RW Net dengan menggunakan Power Line tidak berbeda dengan jaringan pada umumnya. Perbedaannya hanya terletak pada media transmisi data yang digunakan, Power Line menggunakan kabel listrik sedangkan RT/RW Net pada umumnya menggunakan kabel seperti UTP, Fiber Optic, Coaxial serta jaringan wireless.

Kata Kunci: jaringan lokal, komputer, sekolah

A. PENDAHULUAN

Teknologi komunikasi dan informasi semakin hari semakin berkembang dengan teknologi ini bisa menfasilitasi komunikasi antar individu atau kelompok orang yang tidak bertemu secara fisik dilokasi yang sama melainkan antar individu atau kelompok bisa saling berkomunikasi tanpa batas ruang dan waktu. Seiring dengan keinginan komunikasi artar individu atau kelompok tanpa batas itu harus diimbangi dengan teknologi jaringan komunikasi yang bisa mencakup jangkauan yang sangat luas.

RT/RW Net adalah jaringan komputer swadaya masyarakat dalam ruang lingkup RT/RW. Membangun RT/RW Net di perumahan Taman Berdikari Sentosaadalah suatu konsep dimana beberapa komputer dalam suatu perumahan atau blok dapat saling berhubungan dan dapat berbagi data serta informasi, mengemukakan, pendapat, melakukan polling, bahkan pemilihan RT/RW sekalipun.

Perumahan Taman Berdikari Sentosa merupakan perumahan yang terletak di pusat kota DKI Jakarta Timur yang tidak memungkinkan untuk menarik kabel UTP. Oleh karena itu fasilitas RT/RW Net yang akan dibangun di perumahan Taman Berdikari Sentosa untuk memenuhi kebutuhan masyarakat akan internet serta komunikasi masyarakat yang lebih intens tanpa harus meninggalkan pekerjaan rumah tangga serta terbatas dengan cuaca selain itu dengan komunikasi power line lebih mudah untuk mengidentifikasi masalah teknis di lapangan pada saat konektifitas.

Perancangan merupakan penghubung antara spesifikasi kebutuhan dan implementasi. Perancangan merupakan rekayasa representasi yang berarti terhadap sesuatu yang hendak di bangun. Hasil perancangan harus dapat ditelusuri sampai ke spesifikasi kebutuhan dan dapat diukur kualit asnya berdasarkan kriteria-kriteria rancangan yang bagus. Perancangan menekankan pada solusi logis mengenai cara sistem memenuhi kebutuhan.

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer autonomous. Sedangkan definisi lain dari Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan yang lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersamaan.

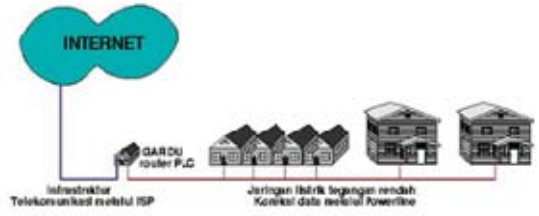
Jadi disimpulkan Jaringan komputer memungkinkan kita bisa bersama-sama untuk meningkatkan penggunaan sumber daya yang ada dalam sebuah perusahaan / organisasi, komunikasi dan arus informasi semakin cepat serta melindungi aset-aset penting perusahaan /organisasi yang semestinya diakses oleh pihak yang berwenang di dalamnya. Khususnya dalam kegiatan proses belajar mengajar karena jaringan ini sangat berperan besar dalam berbagi informasi, aplikasi dan perangkat keras secara bersamaan.

PLC (Power Line Communication) atau komunikasi melalui kabel listrik, juga dikenal sebagai Power Line Digital Subscriber Line (PDSL), mains communication, Power Line Telecom (PLT), Power Line Networking (PLN), atau Broadband over Power Lines (BPL) adalah sistem untuk membawa data pada konduktor yang juga digunakan untuk transmisi tenaga listrik. Sehingga jaringan listrik selain berfungsi sebagai sumber listrik juga menjadi media penghantar komunikasi.

Daya listrik ditransmisikan melalui jalur transmisi tegangan tinggi, yang didistribusikan melalui tegangan menengah, dan digunakan di dalam gedung pada tegangan rendah. PLC dapat diterapkan pada setiap tahap. Kebanyakan teknologi PLC membatasi diri untuk satu set kabel (misalnya, kabel tempat), tetapi beberapa dapat silang antara dua tingkat (misalnya, baik jaringan distribusi dan kabel tempat). Biasanya trafo mencegah menyebarkan

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

sinyal yang memungkinkan beberapa teknologi PLC dijembatani untuk menghubungkan jaringan antar rumah satu dengan rumah yang lainnya.



Gambar 1. Jaringan PLC

B. METODE PENELITIAN

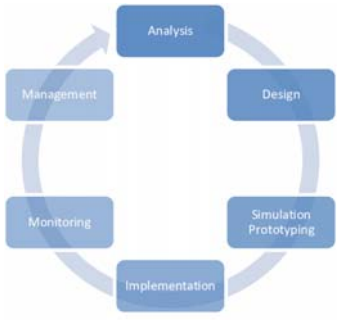
Metode Penelitian yang digunakan dengan cara, yaitu :

1. Studi Lapangan
   Yaitu penelitian langsung ke lingkungan RT/RW Perumahan Taman Berdikari Sensota untuk mendapatkan data serta gambaran dari sistem berjalan.
2. Wawancara
   Teknik pengumpulan datanya melalui wawancara untuk meyakinkan bahwa data yang diperoleh benar-benar akurat.
3. Studi Pustaka
   Pengumpulan data dengan cara mempelajari hal yang berkaitan dengan sistem informasi penjualan, dengan berbagai informasi dari buku-buku, artikel dan website internet.

Dalam perancangan jaringan komputer RT/RW Net menggunakan jalur RT/RW Net menggunakan jalur komunikasi power line (PLC) di perumahan Taman Berdikari Sentosa yaitu metode NDLC (Network Develovement Live Cycle). Dengan metode ini dapat digunakan untuk memandu dimulainya suatu jaringan baru, dan diperluas untuk upgrade jaringan yang ada.

Pengembangan sistem yang dilakukan adalah dengan menggunakan metode pengembangan sistem *Network Development Life Cycle* (NDLC) dengan fase sebagai berikut:

1. *Analisis*. Tahap ini peneliti melakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan *user*, dan analisa topologi / jaringan yang sudah ada saat ini.
2. *Design*. Tahap *Design* ini peneliti membuat gambar *designtopology* jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.
3. *Simulation Prototype.* Dalam membuat simulasi peneliti menggunakan alat Bantu *tools* Microsoft Visio 2007 untuk membangun *topology* yang akan didesain.
4. *Implementation.* Pada tahap ini peneliti membangun jaringan berdasarkan desain yang telah dibuat.
5. *Monitoring*. Pada tahap ini peneliti melakukan *monitoring* keadaan jaringan agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis.
6. *Management*. Tahap ini level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga.



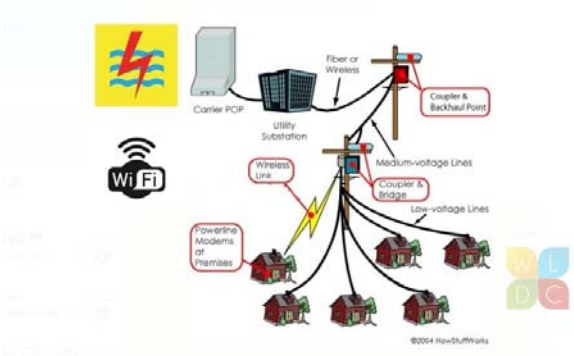
Gambar 2. *Network Development Life Cycle* (NDLC)

Metode pengujian jaringan komputer yang dapat kita lakukan yaitu dengan menggunakan *Ping Test*, perintah yang digunakan yaitu seperti tes koneksi (*PING*) apakah yang paket yang kita kirim berhasil atau tidak, tes rute (*TRACERT*) untuk melihat rute yang dilewati oleh paket untuk sampai tujuan, dan (*IP CONFIG*) untuk melihat *IP address, gateway, DNS server*, dan hampir semua informasi dalam suatu jaringan metode analisis dan desain Sistem.

C. HASIL DAN PEMBAHASAN

Berdasarkan pengamatan lapangan yang dilakukan, Perumahan Taman Berdikari Sentosa terdiri dari 250 rumah, yaitu terbagi dalam bentuk blok per blok dengan pemakaian huruf Kapital, contoh : Blok A1/1. Dilingkungan perumahan terdiri dari 1 RW dan 4 RT. Dari hasi pengamatan, maka dapat didefinisikan beberapa hal sebagai berikut :

1. Media transimisi kabel UTP yang menghubungkan antar ruangan terlalu panjang, sehingga kemungkinan terjadinya *loss data* transmisi sangat besar.
2. Kabel transmisi UTP pemasangannya masih semrawut, tidak efisien dan fleksibel.



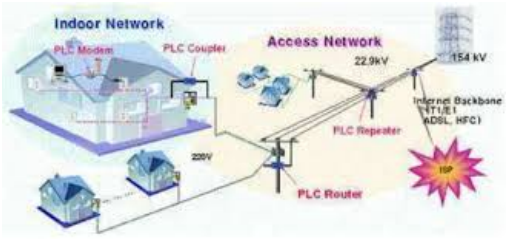
Gambar 3. Topologi Jaringan Sistem

Berjalan Dari hasil analisis sistem dilapangan, maka dapat ditemukan peluang sistem baru antara lain :

1. Penggunaan kabel yang menghubungkan antar ruangan dapat diminimalisir dengan menggunakan media transmisi listrik jala-jala PLN dengan modul PLC.
2. Topologi jaringan yang lebih efisien dan fleksibel, dapat mengurangi kehilangan (loss) paket data.

Perancangan Jaringan Perumahan

Rancangan dan Desain Keseluruhan jaringan didapat dengan meminimalkan penggunakan kabel pada topologi jaringan yang ada, sehingga topologi jaringan menjadi lebih sederhana dan fleksibel.



Gambar 4. Topologi jaringan dengan menggunakan *Powerline*

Adapun spesifikasi hardware yang digunakan terlihat pada tabel1 berikut:

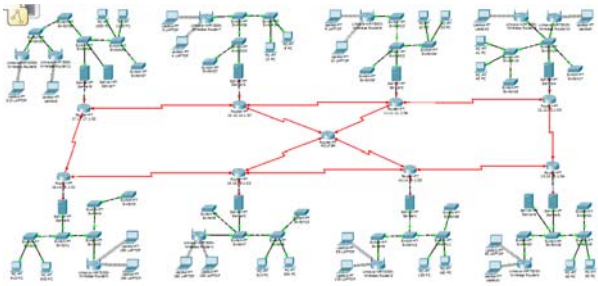
Tabel 1. Spesifikasi Hardware yang digunakan

No	Perangkat	Jml	Spesifikasi Hardware
1	Komputer	80	Intel i3 dan RAM 4 GB
2.	PowerLine Adapter Totolink Model PL200KIT	10	Transfer Rate 200 Mbps
3.	Switch D-Link port Gigabit EasySmart DGS-1100-24	6	Ethernet/ Fast Ethernet 10/100 Mbps

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Jaringan dibagi menjadi 80 jalur. Jalur pertama yang terdiri dari RT.001 terhubung pada *switch* 1 dan 2 dengan konfigurasi kabel *straight*, RT.002 terhubung pada *switch* 3 dan 4 dengan konfigurasi kabel *straight*, RT.003 terhubung pada *switch 5* dan 6 dengan konfigurasi kabel *straight* dan RT.004 terhubung pada *switch 5* dan 6 dengan konfigurasi kabel *straight* dengan konfigurasi kabel *straight*. Dari *switch* langsung terhubung ke *Powerline Adapter* pertama juga menggunakan konfigurasi kabel *straight*. Jalur kedua, ketiga, keempat, kelima, keenam sampai dengan kesepuluh ke *switch* dengan konfigurasi kabel *straight* langsung terhubung ke *Powerline Adapter* 10 juga menggunakan 10 konfigurasi kabel *Straight*.
Hubungan antara kesepuluh jalur ini menggunakan transmisi tegangan jala-jala PLN melalui ke 80 *Powerline adapter*.

1. Simulasi dan *Prototype* Jaringan
   Pada tahapan ini, di bangun suatu prototype sistem yang akan dibangun dan dimplementasikan pada Perumahan Taman Berdikari Sentosa dengan menggunakan emulator. Tahapan ini bertujuan untuk mendemonstrasikan sistem agar berjalan dengan benar.



Gambar 5. Simulasi Jaringan dengan konfigurasi IP Address

2. Implementasi
   Tahapan selanjutnya yaitu implementasi atau penerapan rancangan topologi dan rancangan sistem pada lingkungan nyata.

3. Konfigurasi Modul Powerline
   Modul Powerline yang digunakan adalah PowerLine Adapter Merk Totolink Model PL200KIT. Perangkat ini memiliki kecepatan transfer sampai 200 Mbps. Penggunaan perangkat ini sangat mudah yaitu langsung dihubungkan pada stop kontak listrik dan langsung dihubungkan dengan switch menggunakan kabel *straight*. Powerline yang digunakan ada dua buah

Gambar 6. Powerline Adapter Toto

4. Monitoring
   NDLC mengkategorikan proses pengujian pada tahapan monitoring. Hal ini dikarenakan pengawasan sistem yang sudah dibangun hanya dapat dilakukan jika sistem sudah dapat bekerja sesuai dengan kebutuhan. Proses pengujian (*testing*) dibutuhkan untuk menjamin dan memastikan bahwa sistem yang dibangun sudah memenuhi spesifikasi rancangan.
   Dalam sistem ini, pengujian bersifat fungsional, dimana penguji memberikan *input* dan menghasilkan *output* yang diharapkan. Pengujian dengan menguji konektifitas antara komputer yang berada dalam jaringan. Pengujian dengan menggunakan *PING TEST*. Pengujian dilakukan masing-masing komputer dengan meng-*PING* dengan komputer lainnya dengan menggunakan beragam paket data.

5. Managemen
   Fase terakhir pada model NDLC adalah managemen (pengelolaan). Fase ini meliputi aktifitas perawatan dan

pemeliharaan dari keseluruhan sistem yang sudah dibangun. Namun, seperti penulis jelaskan sebelumnya bahwa tahap pengelolaan merupakan kewenangan dari pihak Kecamatan Martapura, maka penulis hanya terlibat sampai fase sebelumnya yaitu monitoring.

Pembahasan

Dari hasil pengujian yang dilakukan, terlihat bahwa kondisi jaringan yang stabil dengan menggunakan powerline adapter. Dengan adanya powerline maka diharapkan konfigurasi jaringan dan perancangan jaringan dapat lebih efisien dan lebih rapi, karena penggunaan kabel yang banyak digantikan dengan media transmisi listrik jala-jala PLN.

Dapat dilihat bahwa penggunakan switch tidak mempengaruhi kinerja jaringan dengan media transmisi jala-jala listrik. Kemudian untuk restrukturisasi jaringan dapat dengan mudah dilakukan tanpa mengubah susunan jaringan dasarnya.

D. PENUTUP

Setelah uraian diatas, beberapa kesimpulan yang diambil sebagai berikut :

1. PLC menggunakan jaringan kabel listrik untuk komunikasi data tanpa harus menginstal infrastruktur baru.
2. PLC mudah untuk menghubungkan antar user satu dengan lainnya, baik lokal maupun wide area.
3. Menggunakan soket listrik yang ada sebagai concentrator sehingga tidak memerlukan biaya ekstra untuk instalasi kabel. Dengan demikian, restrukturisasi jaringan dapat lebih mudah dilakukan tanpa harus merubah struktur jaringan pokoknya.

Sedangkan saran yang dapat diberikan adalah untuk pengembangan sistem selanjutnya diharapkan kepada semua pihak yang berniat untuk mengadakan penelitian dengan alat serupa, disarankan untuk memberikan tambahan hasil percobaan dengan menggunakan jala-jala listrik 3 fasa, sehingga dapat menghasilkan suatu topologi jaringan yang lebih luas lagi.

E. DAFTAR PUSTAKA

Berger, T. L., Schwager, A., & Garzás, J. J. (2013). Power line communications for smart grid applications. Journal of Electrical and Computer Engineering - Special issue on Power-Line Communications: Smart Grid, Transmission, and Propagation, 3

Febridiani, L. D., & Wibisono, G. (2010). Analisis SWOT untuk Implementasi Voice over Internet Protocol (VoIP) pada Powerline Communication (PLC). Jurnal Informatika LIPI, 1-7

K. H. G. Afrizal Fitriandi, "Rancang Bangun Alat Monitoring Arus dan Tegangan Berbasis Mikrokontroler dengan SMS Gateway," ELECTRICIAN – Jurnal Rekayasa dan Teknologi Elektro, 2016.

Lukitasari, A. Haryadi, and R. H. Y. Perdana, “Implementasi Powerline Communication Untuk Monitoring Penggunaan Arus Di Politeknik Negeri Malang,” Implementasi Power Line Commun. UNTUK Monit. Pengguna. ARUS DI Politek. Negeri Malang, vol. VII, no. 2, pp. 74–78, 2018.

M. Arihutomo, M. Riva and S. , "Sistem Monitoring Arus Listrik Jala-Jala Menggunakan Power Line Carrier," JURNAL TEKNIK ITS, 2012.

Yogi Hariatmoko, Perancangan Manajemen Bandwidth Jaringan RT/RW Net Menggunakan Metode Hierarchical Tokken Bucket(HTB) Pada Router Mikrotrik di Desa Karang Duwet Salatiga,- 2015

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

RANCANG BANGUN SABLON JALUR LAYOUT PCB OTOMATIS BERBASIS PROGRAMMABLE LOGIC CONTROL (PLC)

Irawati[1)], Deasy Kartikasari [2)], Karyadi[3)]
[1,2,3]Prodi Teknik Elektronika, Fakultas Teknologi, ITB Swadharma

Correspondence author: irawati, irawati2182@gmail.com, Jakarta, Indonesia

Abstract

Advances technology in life is also accompanied by innovations from various automation processes, a strong reason that encourages the formation of this PLC-Based Automatic PCB Path Screen Printing tool, starting from students printing PCB by ironing the circuit design results on the PCB, which takes time long enough. At this step, many people experience problems, including the paths on the PCB etching results are broken due to the uneven ironing of the printed results. As a result, the circuit does not work as intended. Therefore, a PCB etching machine is needed that can work automatically. It can produce the desired circuit results in a shorter and better time, The way this PCB screen printing machine works, is to use a Heater (heat element), which is then controlled by the Thermo Controller, and programmed by the PLC, and pushes and pressing using air pressure (pneumatic) which is then determined by the Timer, During the specified time, After finishing the PCB screen printing results are cooled by a 24v DC fan, this tool has specifications with a length of 60cm, width 40cm and height 80cm this machine is designed to minimize time and effort to be faster and get better results.

Keywords: PLC, PCB, Heater

Abstrak

Kemajuan teknologi diiringi dengan inovasi-inovasi dari berbagai proses automatisasi. Alasan kuat yang mendorong terbentuknya alat Sablon Jalur PCB Otomatis Berbasis PLC ini diawali dari siswa yang masih mensablon PCB yaitu dengan menyetrika hasil desain rangkaian pada PCB, yang membutuhkan waktu cukup lama. Pada tahap ini banyak yang mengalami masalah, antara lain jalur pada hasil *etching* PCB banyak yang putus dikarenakan kurang meratanya proses setrika hasil cetak. Akibatnya rangkaian tidak berjalan sesuai dengan yang diinginkan. Oleh karena itu, diperlukan Mesin *etching* PCB yang mampu bekerja secara otomatis. Mesin ini mampu menghasilkan hasil rangkaian yang diinginkan dengan waktu yang lebih singkat dan lebih baik. Cara kerja mesin sablon PCB ini adalah dengan menggunakan *heater* (elemen panas), yang kemudian di kontrol oleh *Thermo Controller*, dan di program oleh PLC, dan menekan menggunakan penekanan angin (*pneumatic*) yang ditentukan oleh *Timer* selama waktu yang telah ditentukan. Setelah selesai hasil pensablonan PCB tersebut didinginkan oleh kipas DC 24v. Alat ini mempunyai spesifikasi dengan panjang 60cm, lebar 40cm dan tinggi 80cm mesin ini dirancang bertujuan untuk meminimalisasi waktu dan tenaga sehingga menjadi lebih cepat dan mendapatkan hasil yang lebih baik.

Kata Kunci: PLC, PCB, Heater

A. PENDAHULUAN

PCB digunakan sebagai dasar semua rangkaian elektronika yang sering kita jumpai, karna papan jenis ini akan menjadi tempat melekatnya komponen elektronika dengan diletakan menggunakan solder yaitu dengan bantuan timah yang di cairkan. PCB dilapisi lapisan logam yang berfungsi sebagai penghubung antar komponen, lapisan logam ini nantinya akan menjadi kabel yang tersusun rapih. Untuk membuat jalur pada PCB maka harus melalui beberapa proses yang tidak mudah, mulai dari menggambar skema rangkaian sampai mensablon jalur pada papan tersebut sebelum akhirnya dilarutkan dalam cairan asam pelarut logam sehingga papan tersebut membentuk jalur. Pada saat ini di laboratorium Teknik Elektronika untuk membuat jalur pada papan PCB masih melakukan pensablonan PCB secara manual menggunakan setrika yang hasilnya kurang baik dan kurang efisien.

Oleh karena itu kami merancang sebuah alat automatisasi untuk teknik pensablonan jalur PCB, yang di gerakan oleh PLC sebagai kontrolnya dan pneumatic sebagai outputnya. Alat ini kami buat untuk mempermudah mahasiswa Teknik Elektro untuk mensablon jalur PCB demi mendapatkan hasil yang lebih baik dari pada melakukan pensablonan secara manual. PLC OMRON CPM1A yang kami gunakan mempunyai spesifikasi 10 input dan 10 output sedangkan dialat ini sendiri hanya menggunakan 3 input yaitu, 1 push button dan 2 limit switch, sedangkan output yang digunakan di alat ini sebanyak 5 output yaitu 4 katup solenoid dan 1 kipas DC 24V.

B. METODE PENELITIAN

Kegiatan penelitian yang dilakukan meliputi:

1. Studi Literatur dan Dasar Teori Studi literatur dilakukan untuk mencari bahan-bahan referensi yang akan digunakan dalam penelitian ini. Dengan mencari buku-buku, jurnal-jurnal mengenai pemilihan prioritas maupun melalui internet.
2. Penentuan rancangan sablon jalur layout PCB
3. Mendesain sablon jalur layout PCB menggunakan software ADS kemudian menganalisanya
4. Simulasi pengambilan data dengan:
   a. Pertama dengan simulasi return loss S11 karena akan menunjukkan frekuensi kerja PA tersebut, selanjutnya menampilkan nilai S21 yang merupakan nilai gain PA tersebut, serta nilai kestabilannya. Setelah itu, maka selanjutnya menampilkan nilai VSWR untuk mengetahui sejauh mana impedance matching yang dihasilkan.
   b. Kedua dengan menampilkan nilai PAE
   c. Ketiga dengan membandingkan antara hasil yang didapat dengan referensi.

C. HASIL DAN PEMBAHASAN

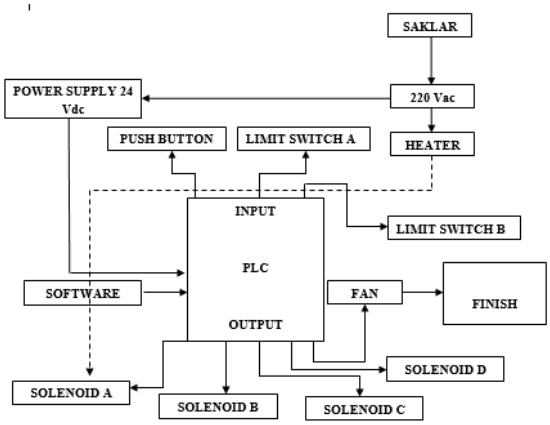
Sistem kontrol Rancang Bangun Sablon Jalur PCB Otomatis Berbasis PLC ini komponen utamanya adalah sebuah heater plat, dimana heater plat disini berfungsi sebagai pemanas yang akan mentransferkan sebuah jalur ke papan PCB. Alasan penggunakan heater plat ini karena heater plat mempunyai panas yang merata diseluruh permukaannya sehingga hasil sablon yang didapat pun jauh lebih baik di banding menggunakan setrika yang hanya menggunakan heater tabung sebagai pemanasnya, dimana heater tabung tidak menghasilkan panas yang merata diseluruh permukaan setrika sehingga hasil yang didapat jika menggunakan setrika pun kurang maksimal.Selain heater adapun otak inti dari alat ini adalah sebuah sistem kontrol yang dikendalikan oleh PLC dimana PLC sendiri terdiri dari input, proses, dan output. Untuk semua masukan system secara otomatis yaitu dengan 2 Limit

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Switch, kemudian diproses oleh PLC dan di gerakan oleh kompresor untuk supply udara ke silinder pneumatik, dan 2 solenoid sebagai pembuka dan penutup udara ke 2 slinder Pneumatik, dan 2 speed control guna untuk mengatur kecepatan tekanan udara, dan output secara manual semua masukan system tersebut menggunakan push button, untuk menggerakan semua system secara manual.

Diagram Blok Sistem

Setelah membuat penjelasan sistem alat, kemudian membuat diagram blok yang terdiri dari perangkat *input,* proses, dan perangkat *output*. Diagram blok Rancang Bangun Sablon Jalur PCB Otomatis Berbasis PLC dapat dilihat pada gambar dibawah ini

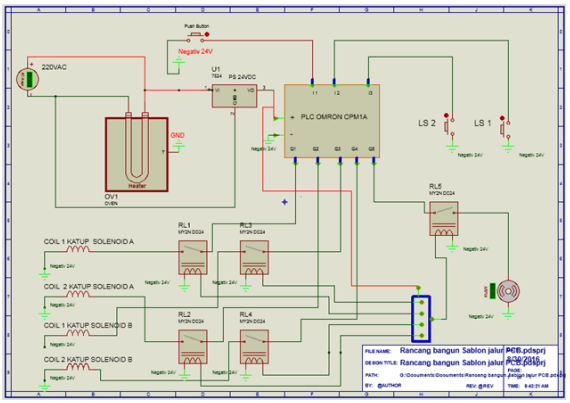


Gambar 1. Blok Diagram Sistem

Pada gambar diatas diagram blok Rancang Bangun Sablon Jalur PCB Otomatis Berbasis PLC ialah saklar berfungsi untuk memutus dan menyambungkan dari sumber tegangan 220Vac. PLC membutuhkan tegangan 24vdc dari power supply 24vdc. Tegangan 220vac ini dibutuhkan untuk menghidupkan heater, dan suhu heater akan di kontrol oleh thermostat yang berfungsi sebagai penstabil suhu yang kita inginkan. Setelah saklar hidup tekan tombol push button untuk menghidupkan solenoid A setelah solenoid A hidup makan akan menggerakan piston silinder press, setelah piston silinder press hidup lalu menekan limit switch A untuk menghidupkan solenoid B dan solenoid C secara on delay, setelah solenoid B hidup maka silinder press pun kembali ke posisi awal, dan secara bersamaan ketika solenoid B hidup maka solenoid C pun hidup untuk menggerakan piston silinder dorong lalu piston menekan limit switch B untuk menghidupkan solenoid D dan kipas, setelah solenoid D hidup maka piston silinder dorong akan kembali ke posisi awal dan kipas akan hidup sesuai timer yang di program, selesai.

Skematik Rancang Bangun Sablon Jalur PCB Otomatis Berbasis PLC

Gambar skematik ini menjelaskan sistem penjaluran keseluruhan dari rancang bangun sablon jalur PCB otomatis berbasis PLC. Apabila terdapat kerusakan dari salah satu komponen kita dapat menanalisanya melalui gambar skematik ini :



Gambar 2. Skematik Rancang Bangun Sablon Jalur PCB Otomatis Berbasis PLC

Berikut ini adalah rancang jadi rancang bangun sablon jalur PCB berbasis PLC

Gambar 3. Hasil rancangan alat

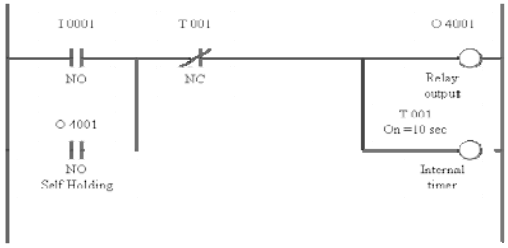
Pengujian dan analisa

Sebuah sistem membutuhkan pengujian dan analisa data. Sebagai refensi pembuatan program, ini akan sangat mempengaruhi kinerja sistem kontrol rancang bangun sablon jalur PCB otomatis berbasis PLC agar menjadi sebuah sistem yang baik dan sempurna karna tanpa adanya sebuah pengujian dan analisa dari sebuah alat tidak akan membuahkan hasil yang sempurna

Pada dasarnya untuk membuat program ladder diagram adalah dengan menghubungkan busbar sisi kiri ke busbar sisi kanan sesuai dengan kondisi dan instruksi yang diinginkan untuk dikerjakan oleh unit PLC dalam menjalankan perintah ke mesin yang dikontrolnya. Jalur operasi kerja itu bisa dibagi dalam 2 bagian, yaitu:

1. Sisi Kiri = merupakan sisi pengkondisian, dimana biasanya terdiri dari rangkaian simbol kontak *NO* dan/atau *NC*, baik yang berasal dari switch input langsung ataupun dari switch internal relay hasil operasi perintah kerja dalam program yang bersangkutan.
2. Sisi Kanan = merupakan sisi perintah kerja, dimana biasanya berupa simbol relay dan bisa dipasang sebagai output langsung ataupun berupa internal relay, timer, *counter* dan operasi-operasi lainnya. Jadi bilamana kondisi-kondisi yang ada di sisi kiri bisa dalam keadaan terhubung semua, maka arus listrik kutub (+) dari busbar kiri akan mengalir dan menghidupkan operasi kerja di sisi kanan yang menempel dengan listrik kutub (-) di busbar kanan.

Contoh Program Leader Diagram



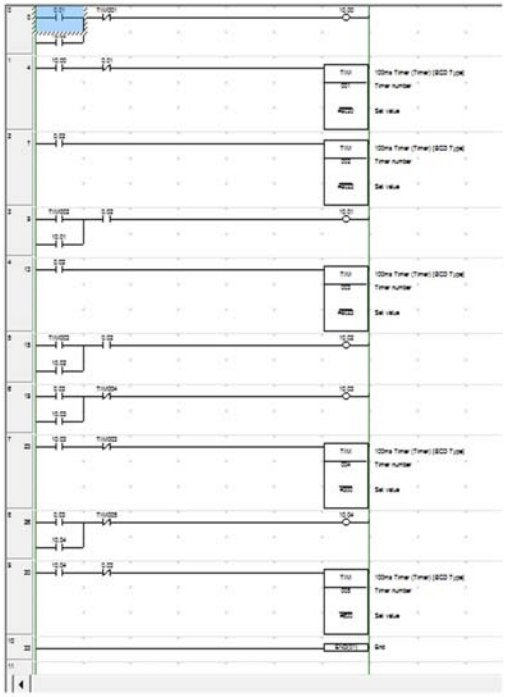
Gambar 4. Program Leader Diagram

1. Kondisi awal/normal:
   Kontak I 0001 terputus, kontak O 4001 terputus, kontak T 001 terhubung, relay *output* O 4001 tidak bekerja, internal timer T 001 tidak bekerja.
2. Saat Push Button I 0001 ditekan:
   Kontak I 0001 terhubung, kontak T 001 masih terhubung, karena internal timer T 001 di *setting ON* setelah 10 detik, maka arus listrik akan mengalir menghidupkan *relay output* O 4001 dan internal timer T 001.
3. Saat Push Button I 0001 dilepaskan kembali:
   Kontak I 0001 terputus, kontak *relay* output O 4001 terhubung, karena relay *output* O 4001 bekerja, kontak T 001 masih terhubung, sehingga arus tetap mengalir menghidupkan relay output O 4001 dan internal timer T 001. Kondisi kontak relay output O 4001 ini disebut *Self Holding* Contact.
4. Saat 10 detik setelah relay output O 4001 dan *internal timer* T 001 bekerja:
   Kontak T 001 terputus karena *internal timer* T 001 dalam kondisi *ON* setelah waktu tunda 10 detik sesuai dengan setting, dan hal ini memutuskan arus listrik yang mengalir ke relay *output* O 4001 dan internal timer T 001, sehingga keduanya segera *OFF* lagi. Dan kondisi kembali ke kondisi awal di atas. Bila dilihat hanya untuk satu baris ladder diagram di atas, akan terlihat sederhana bagi orang yang mengerti skema diagram rangkaian listrik, tetapi justru disinilah kehebatan dibalik kesederhanaan program *ladder diagram*. Kontak poin I 0001, O 4001 dan T 001 itu bisa digunakan dimana saja pada program lanjutan dari ladder diagram di atas.

Dan bila program ini diteruskan ke bawah sesuai dengan kebutuhan program mesin yang bersangkutan, maka program ini akan terlihat sebagai anak tangga yang terus turun ke bawah. Untuk kebutuhan perancang desain rangkaian listrik,

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

penggunaan PLC dengan ladder diagramnya ini sangat membantu mengurangi keruwetan rangkaian listrik dalam panel kontrol, sehingga menjadi ringkas dan kompak. Juga sangat fleksibel saat perancang melakukan modifikasi ataupun upgrade sistem dari rangkaian listrik mesin yang dirancangnya tersebut. Sementara untuk kebutuhan *maintenance* dan trouble *shooting*, penggunaan PLC ini jelas menjadi bantuan mata sang trouble shooter untuk melihat kegagalan apa yang terjadi dengan dengan proses kerja mesin yang sedang diperbaiki. Pengujian leader dari diagram ini menggunakan software cx programmer versi 9.5 pengujian program ini sangatlah penting dari sebuah sistem rancang bangun sablon jalur PCB otomatis berbasis PLC, karena di pengujian ini kita dapat mengetahui apakah program yang kita buat berjalan sesuai dengan keinginan kita atau tidak berikut sebuah program leader diagram untuk rancang bangun sablon jalur PCB otomatis berbasis PLC :



Gambar 5. Program Leader Diagram rancang bangun sablon jalur PCB otomatis berbas

Yang harus dilakukan pertama kali dalam pengujian secara keseluruhan ini adalah memastikan bahwa seluruh komponen *output* tersambung dengan komponen *input. Output*. Pada pengujian ini kami akan menguji suhu serta waktu pada heater untuk mendapkan hasil sablon yang baik.

Tabel 1. Hasil pengujian Sablon PCB

No	Suhu	Waktu Heater Bekerja
1	75C	± 10 menit
2	80C	± 12 menit
3	100C	± 15 menit
4	90C	± 15 menit

Hasil menunjukan bahwa pengujian dari beberapa suhu dan waktu dari percobaan tersebut mendapatkan hasil yang berbeda beda , pada suhu 75c dengan waktu 10 menitt mendapatkan hasil yang kurang baik, hasil dari suhu dan waktu tersebut jalur sablon tidak merekat keseluruhan dengan sempurna pada PCB masih banyak jalur yang terputus, dan percobaan ke 2 dengan suhu 80c waktu mendapatkan hasil yang hampir sempurna namun masih ada sedikit dari bagian jalur yang di sablon tidak merekat, selanjutnya percobaan ke 3 dengan suhu 100c dengan waktu mendapatkan hasil yang sangat buruk dikarenakan suhu yang terlalu panas sehigga kertas OHP meleleh dan pada PCB melengkung akibat suhu yang terlalu panas, dan jalur sablonpun tidak menempel pada PCB, kemudian Percobaan ke 4 dengan suhu 90c dengan waktu mendapatkan hasil yang sangat baik karena suhu yang pas dan timer yang pas pada kertas OHP pun tidak meleleh dan pada PCB tidak melengkung. Dari analisa ke 4 kali percobaan ini dapat di analisa bahwa suhu dan waktu yang akan di terapkan pada alat rancang bangun sablon jalur PCB otomatis berbasis PLC ini akan di tetapkan pada suhu 90c dan waktu yang + 15 menit.

PENUTUP

Berdasarkan perancangan, realisasi dan percobaan, maka penulis membuat kesimpulan, yaitu :

1. Waktu dan suhu yang dibutuhkan untuk mendapat hasil pensablonan jalur ke PCB yang baik dibutuhkan waktu selama 15 menit dengan suhu 90°C.
2. Perbedaan panjang dan lebar PCB tidak mempengaruhi waktu dan suhu yang di tentukan untuk mendapatkan hasil yang baik.
3. Proses pengamplasan sebelum proses penyablonan jalur ke PCB perlu di lakukan demi mendapatkan hasil sablon yang maksimal.
4. Secara keseluruhan fungsi pencetak jalur PCB otomatis berbasis PLC ini bekerja cukup baik, dibuktikan dari hasil percobaan dan pengujian langsung pada alat itu sendiri.

Untuk mendapatkan hasil terbaik PCB yang telah selesai di sablon harus rendam ke air sebelum kertas OHP yang menempel di PCB selesai. Untuk mendapatkan hasil yang maksimal gunakanlah PCB yang berkualitas baik. Agar lebih mendapatkan hasil yang jauh lebih baik pada alat ini bisa ditambahkan matras pada tatakan pensablonan.

E. DAFTAR PUSTAKA

Budiyanto (2003) PLC OMRON CPM1A. Yogyakarta: Gava Media

Krist, Thomas (2000) Dasar-Dasar Pneumatic. Jakarta: Erlangga

Djuandi, F. (2011). Pengenalan Arduino. www. tokobuku. com. Jakarta.

http://repository.usu.ac.id/bitstream/handle/123456789/62649/Chapter%20II.pdf?sequence=4&isAllowed=y

Schenk, Dennis G., et al. "Refrigeration appliance with pulsed defrost heater." U.S. Patent No. 6,694,754. 24 Feb. 2004. (heater)

http://sfprime.net/pcb-etching/

https://www.sparkfun.com/datasheets/Sensors/Temperature/MLX90614_rev001.pdf

Bangun Muhammad Agung. (2014). Arduino For Beginners. Banten: Surya University

Charles Platt, (2013), Encyclopedia of Elektronik components Volume 1, O'Reilly Media, Inc, USA.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

PERANCANGAN PEMBANGKIT MIKROHIDRO PADA SALURAN PDAM MATA AIR LEWAJA KABUPATEN ENREKANG SULAWESI SELATAN

Ismuharram[1)], Irawati[2)], Ria Gazali[3)]
[1,2,3]Prodi Teknik Elektronika, Fakultas Teknologi, ITB Swadharma

Correspondence author: Ismuharram, ismu4success@gmail.com, Jakarta, Indonesia

Abstract

Electrical energy has become a part of our life. In fact, for some people it has become a major need that cannot be eliminated. This can affect the energy sources used in the power generation process. Therefore, the existence of renewable energy sources is needed to increase the energy supply for the community. In this case the author tries to do research to take advantage of the water discharge at the Lewaja Spring PDAM, Enrekang Regency, South Sulawesi as a Micro Hydro Power Plant (PLTMH). apipa, so that production costs can be reduced. In addition, it can provide an overview to the PDAM and the community that the PDAM pipes, which so far have only been used for water distribution, can be used as power plants. The purpose of this research is to determine the discharge and pipe head of PDAM and then the dimensional design of the turbine is based on the potential obtained. The survey was conducted to obtain primary data and secondary data. the main data is data obtained directly, while secondary data is data obtained from documents stored in PDAM Lewaja Springs. From the research, the average discharge is 46,287 L/s under normal conditions, and has a water level of 5,998 m from the turbine location.

Keywords: energy, potential, micro hydro, cross flow turbine

Abstrak

Energi listrik telah menjadi bagian dari kehidupan kita. Bahkan, bagi sebagian orang sudah menjadi yang utama kebutuhan yang tidak dapat dihilangkan. Hal ini dapat mempengaruhi sumber energi yang digunakan dalam proses power generasi. Oleh karena itu, keberadaan sumber energi terbarukan sangat dibutuhkan untuk meningkatkan pasokan energi bagi masyarakat. Dalam hal ini penulis mencoba melakukan penelitian untuk memanfaatkan debit air di PDAM Mata Air Lewaja Kabupaten Enrekang Sulawesi Selatan Sebagai Pembangkit Listrik Tenaga Mikro Hidro (PLTMH) Keuntungan membuat pipa PLTMH PDAM tidak kebutuhan pembuatan bangunan sipil dengan membuat PLTMH hanya dengan memanfaatkan aliran air yang ada di apipa, sehingga biaya produksi dapat ditekan. Selain itu, dapat memberikan gambaran kepada PDAM dan masyarakat bahwa pipa PDAM yang selama ini hanya digunakan sebagai pendistribusian air, dapat digunakan sebagai pembangkit listrik. Tujuan dari penelitian ini adalah untuk menentukan debit dan head perpipaan PDAM dan kemudian dimensional design turbine based pada potensi yang diperoleh. Survei dilakukan untuk mendapatkan data primer dan data sekunder. yang utama data adalah data yang diperoleh secara langsung, edangkan data sekunder adalah data yang diperoleh dari dokumen yang tersimpan di PDAM Mata Air Lewaja. Dari

penelitian didapatkan debit rata-rata sebesar 46,287 L/s pada kondisi normal, dan memiliki ketinggian air (head) 5.998 m dari lokasi turbin.

Kata Kunci: energi, potensi, mikro hidro, turbin aliran silang

A. PENDAHULUAN

Indonesia merupakan negara kepulauan yang luas dan Sebagian besarnya merupakan lautan. pulau yang tersebar ini merupkan salah satu hambatan dalam pendistribusian untuk segala jenis. Oleh sebab itulah negara harus memiliki strategi agar distribusi tidak terlalu menjadi kendala atau bisa diminalisir. Untuk meminimalisir kesulitan pendistribusian maka setiap daerah harus dapat menghasilkan produk lokal baik barang atau jasa. Untuk energi daerah harus melihat keunggulan dan kemungkinan distribusi energi secara efisien dengan harga yang terjangkau. Daerah yang mempunyai sebaran penduduk yang tidak padat akan sangat tidak efisien jika dibangaun pembangkit besar, hal ini tidak sebanding dengan biaya produksinya. Sumber daya fosil tidak dimiliki oleh setiap wilayah. Namun matahari dan air hampir seluruh wilayah Indonesia mempunyai itu. Enrekang merupakan salah satu kabupaten di Sulawesi Selatan, dimana kabupaten ini memiliki daerah yang berbukit dan gunung dengan total luas wilayah 1.820,67 Km2. Dengan jumlah penduduk mencapai 204.827 jiwa Berdasarkan data BPS Kabupaten Enrekang Tahun 2018. Jika jumlah penduduk dibagi dengan luas wilayah maka perkilometer persegi hanya dihuni oleh 112 penduduk. Dengan sebaran penduduk ini maka akan banyak wilayah yang masih membutuhkan listrik alternatif selain listrik yang bersumber dari PLN. Pemanfaatan sumber daya energi baru dan terbarukan semisal air, matahari bisa menjadi sumber energi solutif yang ramah lingkungan untuk daerah yang kepadatan penduduknya rendah.

Dalam melakukan segala aktivitas, kita tidak akan pernah lepas dari energi listrik. Dimanapun kita tinggal, listrik sudah menjadi kebutuhan primer yang sangat dibutuhkan bagi setiap kalangan. Baik di daerah perkotaan, maupun daerah terpencil, kebutuhan akan listrik terus bertambah.

Menurut Peavy, Howard S et.al. (1985) Hal ini dapat berpengaruh terhadap sumber energi yang biasa digunakan untuk pembangkit listrik. Seperti pada pembangkit listrik tenaga uap, energi yang dihasilkan bersumber pada batu bara yang semakin lama jumlahnya akan semakin berkurang. Oleh karena itu, hadirnya sumber-sumber energi yang dapat terbarukan, sangat dibutuhkan untuk menambah pasokan energi bagi masyarakat.

Menurut Soetarno (1975) Pemanfaatan air sebagai pemutar turbin, maka secara tidak langsung kita harus menjaga debit air agar tetap lestari. Sehingga menjaga kelestarian hutan adalah kewajiban bagi masyarakat agar penerangan energi listrik dari mikrohidro senantiasa tetap terjaga.dan menurut Soetarno(1975) Dalam hal ini PDAM sebagai suatu perusahaan pelayanan air bersih kepada masyarakat mempunyai peran yang sangat penting dalam kelangsungan hidup masyarakat luas. Seperti yang telah diketahui pada pendistribusian air bersih sebelum disalurkan ke konsumen, air tersebut ditampung dalam sebuah bak reservoir yang tersedia di lokasi yang dekat dengan sumber air. Sebagai tindak lanjut dari keberadaan bak reservoir milik PDAM, dalam penelitian ini penulis berusaha memanfaatkan aliran dari bak tersebut untuk pembangunan PLTMH. Adapun salah satu keuntungan dari pembuatan PLTMH pada saluran PDAM ini yaitu tidak perlunya pembuatan bangunan sipil karena pembuatan PLTMH ini hanya tinggal memanfaatkan air yang ada dalam bak, sehingga biaya produksinya dapat ditekan.

Untuk membangun sebuah PLTMH beberapa fasilitas yang dibutuhkan antara lain: bangunan pengatur tinggi muka air,

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

pintu pengambilan (intake), saluran pembawa (headrace), bangunan ukur, bak penenang (forebay), pipa pesat (penstock), turbin, dan saluran pembuangan (tailrace). (Kusdiana,2008) Tipe dan kapasitas generator yang digunakan adalah lilitan magnet permanen dengan kapasitas daya 500w.

Dalam membangun pembangkit diperlukan data kebutuhan energi pada daerah yang akan dialiri listrik sehingga energi yang dihasilkan dapat terserap dengan baik oleh masyarakat. Hal ini bisa dilakukan dengan mengukur debit air andalan. Debit air andalan bisa didapat dari stasiun pengamatan debit. Pengukuran debit air juga bisa kita lakukan dengan pengamatan pada sungai atau daerah aliran air yang akan dipasang PLTMH. Dengan menggunakan metode propabilitas rumus weibul.

Pemilihan lokasi sangat penting karena berhubungan dengan penempatan, pemasangan, keamanan dan pendistribusian. Pemilihan lokasi yang tepat akan membuat efisiensi yang bagus dari waktu, biaya dan hasil energi yang dihasilkan.

Tinggi jatuh efektif diperoleh dengan mengurangi tinggi jatuh air total (dari permukaan air pada pengambilan sampai permukaan air yang masuk ke turbin) dengan kehilangan tinggi pada saluran air dapat dirumuskan:

- $Hbruto$ = elevasi upstream – elevasi downstream.
- $Hlosses$ = 10% x $Hbruto$ $Heff$ = $Hbruto - Hlosses$

dimana:

- $Hbruto$ = perbedaan tinggi muka air di hulu dan hilir.
- $Hlosses$ = tinggi kehilangan energi Untuk mendapatkan hasil yang optimal, maka sistem pembangkit harus didesain sedemikian hingga sehingga tekanan maksimal 10% dari head bruto. (Patty, 1995)

Berdasarkan jenis turbin, pertimbangan dan desain structural dari posisi rumah pembangkit akan menentukan jenis turbin yang akan digunakan. Daya yang dihasilkan adalah usaha yang dihantarkan per satuan waktu. Dalam perencanaan PLTMH, daya diperoleh dengan menggunakan rumusan:

P = ŋ x ρ x g x $Heff$ x Q (watt)
1000 m^3x9,81m/s^2x0.015 m^3/s x 2 m = 294.3W

dimana:

P = perkiraan daya yang dihasilkan (kW) 1 watt= 1 $J\ s$ = 1 $Nm\ s$ = 1 $Kg\ m^2\ s^3$

- ρ = massa jenis air (1000 kg/m^3)
- g = percepatan gravitasi (9,81 m/detik^2)
  Q = debit andalan (m^3/detik)
- $Heff$ = tinggi jatuh efektif (m) (Patty, 1995)

Perkiraan daya yang dihasilkan digunakan sebagai asumsi sementara untuk perhitungan selanjutnya.

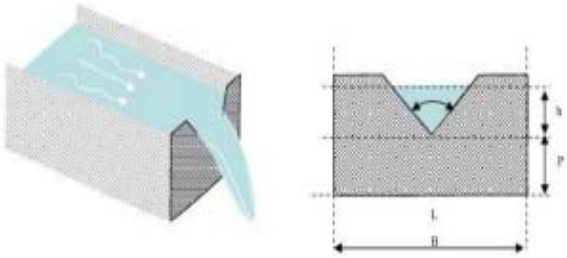
B. METODE PENELITIAN

Menurut Feri yulianto dan Irawati (2021) Kegiatan penelitian yang dilakukan meliputi:

1. Studi Literatur dan Dasar Teori
   Studi literatur dilakukan untuk mencari bahan-bahan referensi yang akan digunakan dalam penelitian ini. Dengan mencari buku-buku, jurnal-jurnal mengenai pemilihan prioritas maupun melalui internet.
2. Penentuan rancangan Mikrohidro PDAM
3. Mendesain Mikrohidro PDAM dan kemudian menganalisanya
4. Pengumpulan Data :
   Pengumpulan data untuk mendapatkan data tentang debit dan head di saluran pipa PDAM. Data berupa data primer yang diambil langsung di lokasi saluran pipa PDAM dan data sekunder yang merupakan data dari PDAM selama kurun waktu satu tahun terakhir.
   Data primer calon lokasi pembangunan PLTMH yang meliputi beda ketinggian

(head) dan debit aliran air. Data primer diambil secara langsung pada saat melakukan survei menggunakan alat ukur yang sudah disediakan di atas. Data diambil menggunakan alat altimeter untuk menentukan ketinggian lokasi, serta sekat V-Notch untuk mendapatkan debit aliran yang ada pada saluran PDAM.

a. Mengukur debit
   Pengukuran dilakukan dengan menggunakan alat V-Notch. Pengukuran dilakukan pada pintu keluar air pada bak Water Treatment Plant (WTP) pipa PDAM.

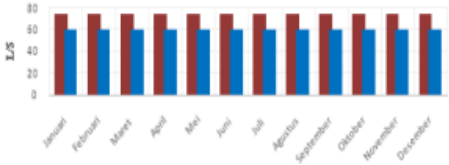


Gambar 1. Sekat Thompson

b. Menentukan Head
   Dalam menentukuan head total, terlebih dahulu mencari ketinggian menggunakan alat altimeter. Dengan demikian, ketinggian jatuh air kotor (head gross) dapat diketahui. Setelah diperoleh ketinggian jatuh airkotor, maka cara berikutnya adalah menentukan headloss yang ada di sepanjang sistem saluran pipa PDAM.

C. HASIL DAN PEMBAHASAN

Data Sekunder merupakan data yang diperoleh dari dokumen yang tersimpan pada kantor PDAM bagian teknik, perencanaan, dan bagian produksi.

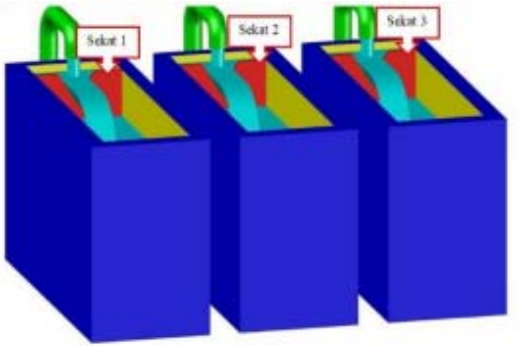


Gambar 2. Debit air

Data sekunder yang diperoleh merupakan data acuan yang dibutuhkan untuk mendapatkan data primer. Adapun data sekunder yang diperoleh adalah data debit aliran. Debit aliran merupakan hal yang cukup penting untuk melakukan studi potensi PLTMH. Hal ini dikarenakan debit dapat mempengaruhi dari desain turbin tersebut.

Data primer merupakan data yang diperoleh dari pengukuran langsung pada bak WTP. Proses pengambilan data menggunakan alat yang sudah terpasang di bak WTP, serta alat lain yang dibutuhkan untuk menentukan potensi PLTMH.

1. Data debit
   Debit yang akan diukur merupakan debit yang masuk ke dalam bak WTP. Di dalam bak tersebut terdapat 3 sekat V-notch yang selanjutnya akan dijumlahkan sehingga diperoleh debit total.



Gambar 3. Posisi sekat pada bak WTP

Pengukuran dilakukan dengan menggunakan mistar, untuk mengukur ketinggian air dalam sekat. Selanjutnya dihitung menggunakan persamaan.

$$Q = 4{,}39 \left(\frac{H}{10}\right)^{2{,}5}$$

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Tabel 1. Data debit pada survei pertama

Pengambilan	Sekat 1		Sekat 2		Sekat 3	
	H (cm)	Debit (l/s)	H (cm)	Debit (l/s)	H (cm)	Debit (l/s)
1	19	21.845	14	10.181	14.4	10.924
2	18.8	21.274	13.8	9.821	14	10.181
3	19.5	23.310	14.2	10.548	13.8	9.821
4	19.4	23.013	14	10.181	14.2	10.548
5	19.3	22.717	13.7	9.644	14.1	10.364
6	19.2	22.424	14.3	10.735	14.4	10.924
7	19.3	22.717	14.5	11.114	13.7	9.644
8	19	21.845	14.1	10.364	13.6	9.469
9	18.5	20.436	14.3	10.735	14.3	10.735
10	18.7	20.993	14.4	10.924	14.4	10.924
Rata-rata		22.057		10.425		10.353
Total						42.836

Tabel 2. Data debit pada survei kedua

Pengambilan	Sekat 1		Sekat 2		Sekat 3	
	H(cm)	Debit (l/s)	H (cm)	Debit (l/s)	H (cm)	Debit (l/s)
1	19.6	23.610	14.5	11.114	15.3	12.711
2	19.9	24.524	14.4	10.924	15.5	13.131
3	19.8	24.217	14.7	11.502	14.9	11.897
4	20	24.834	14.8	11.698	15	12.097
5	19.5	23.310	14.6	11.307	15.5	13.131
6	19.4	23.013	15	12.097	16	14.216
7	20	24.834	14.2	10.548	15.9	13.994
8	19.1	22.133	14.1	10.364	16	14.216
9	19.8	24.217	14.7	11.502	15.8	13.775
10	19.9	24.524	15	12.097	16	14.216
Rata-rata		23.922		11.315		13.338
Total						48.576

Tabel 3. Data debit pada survei ketiga

Pengambilan	Sekat 1		Sekat 2		Sekat 3	
	H (cm)	Debit (l/s)	H (cm)	Debit (l/s)	H (cm)	Debit (l/s)
1	19	21.845	14.5	11.114	14.9	11.897
2	20	24.834	14.6	11.307	14.9	11.897
3	20.1	25.145	14.7	11.502	15	12.097
4	19.9	24.524	14.4	10.924	15.1	12.300
5	19.5	23.310	14.5	11.114	14.9	11.897
6	19.6	23.610	14.6	11.307	15.1	12.300
7	19.7	23.913	14.3	10.735	15.2	12.505
8	19.8	24.217	14.4	10.924	15	12.097
9	20	24.834	14.7	11.502	14.9	11.897

Setelah melakukan beberapa survei, maka diperoleh debit total dengan rata-rata sebagai berikut :

$$Debit\ Total = \frac{Total\ 1 + Total\ 2 + Total\ 3}{3}$$

$$Debit\ Total = \frac{42{,}836 + 48{,}576 + 47{,}449}{3}$$

$$Debit\ Total = 46{,}287\ L/s$$

a. Head kotor

Head kotor merupakan hasil dari pengurangan ketinggian pusat dengan titik lokasi PLTMH. Adapun head kotor yang didapat dari hasil pengukuran diatas adalah sebagai berikut :

Tabel 4.Head kotor

Lokasi	Ketinggian (m)	Head Kotor
Pusat (P)	150,45	
Titik Pertama (A1)	150,25	4,20
Titik Kedua(A2)	150,20	4,25
Titik Ketiga (A3)	147,70	6,75

b. Head Bersih

Head bersih atau head efektif merupakan hasil dari pengurangan head kotor terhadap head kerugian yang ada sepanjang aliran pipa sampai lokasi penempatan.

Tabel 5. Head bersih masing-masing titik

Lokasi	Head Kotor (m)	Head Kerugian(m)	Head bersih (m)
Titik Perama	4,25	0,556	3,644
Titik Kedua	4,25	0,622	3,628
Titik Ketiga	6,75	0,752	5,998

Dari tabel diatas diperoleh head bersih pada masing-masing titik penempatan turbin. Titik ketiga memiliki head bersih paling besar dibandingkan dengan titik pertama ataupun kedua. Sehingga dapat disimpulkan bahwa pemilihan lokasi

penempatan turbin adalah pada lokasi titik yang ketiga, yaitu dengan head bersih 5,998 m.

Daya yang Dibangkitkan Turbin

Setelah diperoleh data debit aliran (Q) = 0,046 m^3/s dan tinggi jatuh (H) = 5,998m maka dapat diperoleh daya air:

Pa = Q . ρ .g .H

= 0,046 m3/s . 1000 kg/m3 = 9,81 m/s2 . 5,998 m = 2706,658 watt = 2,707 Kw

Selanjutnya daya turbin dengan efisiensi direncanakan 76 % adalah sebagai berikut :

$PT = \eta T \; x \; PA$

= 0,76 x 2706,658 watt

= 2057,06 watt = 2,057 Kw

Pemilihan Jenis Turbin

Dalam pemilihan jenis turbin ada beberapa acuan atau dasar sebelum menentukan jenis turbin yang akan digunakan.

Tabel 6. Nilai yang diperlukan untuk menentukan turbin

No	Keterangan (Symbol)	Nilai
1	Putaran Spesifik (N_s)	69,341
2	Head Efektif ($H_{efektif}$)	5,998 m
3	Daya Turbin	2,057 Kw
4	Debit Aliran	0,046 m^3/s

Tabel 7 Pembangkit Listrik berdasarkan daya

Large-Hydro	➢ 100 MW
Medium – Hydro	15MW – 100 MW
Small – Hydro	1 MW – 15 MW
Mini- Hydro	➢ 100 kW
Micro – Hydro	5kW-100kW
Pico-Hydro	< 5kW

Dapat dilihat dari tabel 6, daya yang dihasilkan ialah sebesar 2,057 Kw, untuk menentukan jenis pembangkit listrik berdasarkan daya, dapat dilihat dari tabel 7., maka hasil menunjukan pembangkit listrik jenis Pico-Hydro Ismono H.A., (1999). Dari tabel 6, adapun kecepatan spesifik yang diperoleh adalah sebesar 69,341 adalah jenis turbin crossflow.

D. PENUTUP

Setelah melihat kapasitas air yang diambil oleh PDAM pada Mata Air Lewaja sebesar 15l/det atau sebanding dengan 0.015m3/detik. Bisa didapatkan daya listrik 500w. Tinggi air jatuh hanya diperlukan 2 meter dengan debit air 0.015m3/detik. Kapasitas 500w cukup untuk memberikan energi listrik pada lampu penerang jalan atau untuk 1 rumah. Pembangkit mirkrohidro sangat cocok untuk daerah yang memiliki anak sungai, irigasi, mata air atau aliran PDAM yang bisa dimanfaatkan untuk menghasilkan listrik Setelah melakukan penelitian dan analisis data, maka diperoleh beberapa simpulan sebagai berikut :

PDAM Way Sekampung memiliki debit rata-rata sebesar 46,287 L/s dalam kondisi normal, serta memiliki ketinggian air jatuh (head) sebesar 5,998 m dari lokasi penempatan turbin.

Setelah melakukan beberapa perhitungan, maka pemilihan jenis turbin yang cocok pada saluran pipa PDAM berdasarkan head bersih 5,998 m dan kecepatan spesifik turbin 69,341 adalah jenis turbin crossflow.

Berdasarkan hasil perhitungan yang telah dilakukan, maka potensi yang dimiliki oleh PDAM Way Sekampung dapat menghasilkan daya turbin sebesar 2,057kW.

Hasil perancangan dimensi turbin berdasarkan data primer atau pengambilan langsung yaitu, diameter poros turbin 20 mm, diameter runner 239 mm, panjang sudu 212 mm, ketebalan sudu 2 mm dan jumlah sudut 20.

E. DAFTAR PUSTAKA

Soetarno.1975. Sistem Listrik Mikrohidro untuk melestarikan Desa. Universitas Gadjah Mada. Yogyakarta.

Sujoko, Dwi. 2008. Studi Kelayakan Pemanfaatan Saluran Bak Pelepas Tekan PDAM Untuk PLTMH dan Rancang Bangun Turbin Cross Flow. UGM, Yogyakarta.

Peavy, Howard S et.al. 1985. Environmental Engineering. McGraw-Hill. Singapura.

Ferri Julianto, Irawati. 2021. Perancangan Multi Band Power Amplifier Class-E Pada Frekuensi 900 Mhz, 1800 Mhz, 2300 Mhz, Dan 2600 Mhz. http://ejurnal.swadharma.ac.id/index.php/jeis/article/view/103

Haimerl, L.A. 1960. The Cross Flow Turbine. Jerman Barat.

Ismono H.A., 1999. Perencanaan Turbin Air Tipe Cross Flow UntukPembangkit Listrik Tenaga Mikrohidro di Institud Teknologi Nasional Malang. Skripsi.

Peavy, Howard S et.al. 1985. Environmental Engineering. McGraw-Hill. Singapura.

Soetarno.1975. Sistem Listrik Mikrohidro untuk melestarikan Desa. Universitas Gadjah Mada. Yogyakarta.

Sujoko, Dwi. 2008. Studi Kelayakan Pemanfaatan Saluran Bak Pelepas Tekan PDAM Untuk PLTMH dan Rancang Bangun Turbin Cross Flow. UGM, Yogyakarta.

PERANCANGAN JARINGAN VIRTUAL LAN MENGGUNAKAN METODE PROTOKOL PEER-VLAN SPANNING TREE

Adi Sopian[1)], Khusnul Khoiriyah[2)], Ilham Dwi Putra Gonti[3)]
[1]Program Studi Sistem Informasi, Fakultas Teknologi, ITB Swadharma Jakarta
[2,3]Program Studi Teknik Informatika, Fakultas Teknologi, ITB Swadharma Jakarta

Correspondence author: Adi Sopian, adisopian@swadharma.ac.id, Jakarta, Indonesia

Abstract

The role of computer networks today is very important, starting from the need to share data, software, and communication lines (internet). PT. XYZ is a company engaged in event organizer services. As a modern company, of course, it already has computer network technology to support operational activities. However, along with the increasing needs and users, problems related to security arise and there is no redundancy path between switches. The purpose of this research is to design a VLAN network and create a redundancy path so that it can divide the network segment of each division with broadcast storm prevention technology. Network implementation with Vlan Trunking Protocol to divide network segments between divisions is going well so that there is a backup path between switches so that when one of the lines dies, the network will remain connected.

Keywords: computer network, VLAN, trunking protocol

Abstrak

Peranan jaringan komputer saat ini sangat penting, berawal dari kebutuhan saling berbagi data, software dan jalur komunikasi (internet). PT. XYZ merupakan perusahaan yang bergerak dibidang jasa event organizer. Sebagai perusahaan modern tentunya sudah mempunyai teknologi jaringan computer untuk mendukung kegiatan operasional. Namun seiring dengan meningkatnya kebutuhan serta user, timbul masalah yang berkaitan dengan keamanan dan belum adanya jalur redundansi antar switch. Tujuan dari penelitian ini adalah merancang jaringan VLAN dan membuat jalur redundansi, sehingga dapat membagi segment jaringan tiap divisi dengan teknologi pencegahan broadcast storm. Implementasi jaringan dengan Vlan Trunking Protokol untuk membagi segment jaringan antar divisi berjalan dengan baik sehingga ada jalur backup antar switch agar ketika salah satu Jalur mati, maka jaringan akan tetap terhubung.

Kata Kunci: jaringan komputer, VLAN, trunking protocol

A. PENDAHULUAN

Peranan jaringan komputer saat ini sangat penting, berawal dari kebutuhan saling berbagi data, software dan jalur komunikasi (internet). Fungsi praktis jaringan komputer ini tentu tidak dapat disangkal lagi bagi dunia pendidikan, pemerintahan, pertahanan keamanan, kesehatan, bisnis, keagamaan, dan sosial budaya, semua memanfaatkan jaringan computer sebagai sarana pendukung aktifitas.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

PT. XYZ merupakan perusahaan yang bergerak dibidang jasa event organizer. Sebagai perusahaan modern yang terdiri dari beberapa lantai, tentunya sudah mempunyai teknologi jaringan komputer agar dapat terhubung pada setiap lantai untuk mendukung kegiatan operasional.

Jaringan komputer sendiri merupakan kumpulan dari komputer yang terpisah tetapi saling berhubungan dengan aturan tertentu untuk mengelola anggotanya dalam melakukan pertukaran data (Hasrul & Lawani, 2017; Fitriansyah, Andreansyah, & Abu, 2019). Adanya jaringan komputer ini membuat beberapa pekerjaan dapat diselesaikan secara cepat dan mudah. Pemanfaatan ini tentu membawa dampak positif bagi perusahaan perihal efektifitas dan efisiensi penunjang kerja.

Namun seiring dengan meningkatnya kebutuhan serta user, permasalahan pun timbul yang berkaitan dengan keamanan dan belum adanya jalur redundansi antar switch. Element switching adalah komputer khusus yang dipakai untuk menghubungkan dua kabel transmisi atau lebih. Saat data sampai ke kabel penerima, element switching harus memilih kabel (Diansyah, 2016).

Jaringan Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran dekat sampai beberapa kilometer (Saibi, Kurniabudi, & Rahim, 2014). Jaringan LAN ini seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (resource, misalnya printer) dan saling bertukar informasi (Suryantoro, Sopian, & Dartono, 2021).

Jaringan LAN yang ada digunakan oleh para staff dalam melakukan kegiatannya sehari-hari oleh semua divisi pada segment yang sama sehingga antar divisi bisa saling mengakses data komputer satu sama lain. Hal ini di khawatirkan terjadi pencurian data rahasia perusahaan, serta belum adanya jalur redundansi antar switch, sehingga akan mengakibatkan jaringan terputus ketika salah satu jalur antar switch mengalami masalah atau putus.

Sedangkan pengertian Virtual LAN atau VLAN merupakan sebuah pengelompokan logis dari port yang memiliki lokasi yang independen. Sebuah VLAN akan berjalan seperti yang berada pada layer network 3 yang terpisah. VLAN ID adalah suatu informasi yang ditambahkan pada setiap frame untuk mengijinkan pengiriman frame melalui switch mode trunk, serta untuk memberikan identitas sebuah VLAN dan digunakan nomor identitas VLAN yang dinamakan VLAN ID (Saibi, Kurniabudi, & Rahim, 2014; Fitriansyah, Andreansyah, & Abu, 2019).

Pengertian STP (Spanning Tree Protocol) atau dikenal dengan Protokol Pohon Rentangan (disingkat STP) adalah protokol jaringan yang menjamin topologi jaringan bebas-perulangan untuk penghubung Ethernet LAN (Wiguna, Herlawati, & Santoso, 2013). Fungsi dasar dari STP adalah untuk mencegah pengulangan penghubung dan radiasi siaran yang dihasilkan dari mereka. Pohon rentang juga memungkinkan desain jaringan untuk memasukkan cadang tautan (redundan) untuk menyediakan jalur cadangan otomatis jika tautan aktif gagal, tanpa bahaya dari perulangan yang tidak diinginkan dalam jaringan, atau kebutuhan untuk panduan mengaktifkan / menonaktifkan cadangan tautan ini. Spanning Tree Protocol merupakan protokol yang berada di jaringan switch yang memungkinkan komunikasi pada semua perangkat antara satu sama lain agar dapat mencegah perulangan yang tidak diinginkan dalam jaringan. Jika salah satu segmen jaringan di STP tidak bisa diakses (tidak bisa dijangkau), maka algoritma spanning tree akan mengkonfigurasi ulang spanning tree topologi dan membangun kembali link dengan mengaktifkan standby path (Wiguna, Herlawati, & Santoso, 2013).

Pemilihan root bridge menjadi landasan utama dalam algoritma spanning tree, root bridge adalah switch yang memilih MAC address yang paling rendah dalam topologi. Switch mengirim bridge protocol data unit (BPDU) setiap 2 detik untuk menginformasikan tentang bridge ID (BID) BID berisi MAC Address & priority, Prioritas lebih diutamakan dibanding MAC address (Afdhal, Munadi, & Fachdil, 2015).

VTP (Vlan Trunking Protocol) adalah suatu protokol untuk mengenalkan suatu atau sekelompok VLAN yang telah ada agar dapat berkomunikasi dengan jaringan. Dalam hubungan jaringan LAN dengan ethernet untuk menyambungkan komunikasi dengan menggunakan informasi VLAN, khususnya ke VLAN (Afdhal, Munadi, & Fachdil, 2015).

Berdasarkan infrastruktur jaringan LAN yang digunakan pada perusahaan saat ini, maka pengembangan pun perlu dilakukan untuk memaksimalkan fungsi serta keamanan informasi dan data. Sehingga pada penelitian ini dirancang jaringan LAN agar tiap divisi memiliki jaringan terpisah serta memiliki jalur redundansi yang aman dari *broadcast storm*.

Tujuan dari penelitian ini adalah merancang jaringan VLAN dan membuat jalur redundansi dengan STP pada PT. XYZ. Sehingga diharapkan dapat membagi segment jaringan tiap divisi. Menyediakan jalur redundansi dengan teknologi pencegahan *broadcast storm*.

B. METODE PENELITIAN

Objek Penelitian yang dilakukan pada PT. XYZ yang merupakan perusahaan yang bergerak dibidang jasa event organizer. Pengamatan di lapangan dilakukan pada tanggal 21-25 Juni 2021 di perusahaan PT. XYZ yang berlokasi di Kota Kasablanka Jakarta Selatan.

Untuk memperoleh data-data yang lengkap dan akurat, maka metode yang digunakan adalah penelitian lapangan, dengan Teknik pengumpulan data observasi dan wawancara (interview).

Observasi dilakukan dengan mengadakan pengamatan langsung terhadap permasalahan jaringan dimana seluruh komputer yang terhubung jaringan LAN PT. XYZ dapat akses data computer divisi lain. Dan pengamatan ketika salah satu jalur LAN antar switch mati, maka jaringan yang berada di lantai 1 tidak dapat terhubung dengan lantai 2, begitupun sebaliknya.

Interview dilakukan dengan mengajukan pertanyaan kepada staff IT dan Manager IT yang mengelola jaringan mengenai topologi jaringan yang ada di PT. XYZ saat ini dan pembagian jaringan tiap divisi yang berjalan saat ini serta jika salah satu jalur LAN yang mengkoneksikan antar switch mengalami masalah.

C. HASIL DAN PEMBAHASAN

Pada saat ini perusahaan menggunakan jaringan LAN yang terhubung dengan jaringan internet. Jaringan lokal yang ada menggunakan *router* untuk membagi akses jaringan ke setiap *client* melalui *switch*.

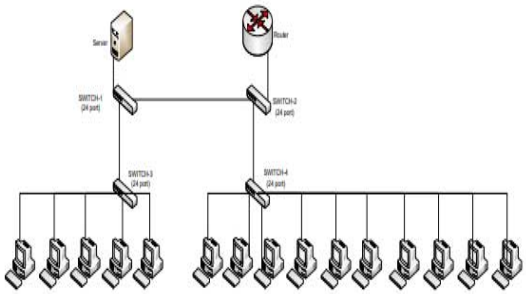
Dari segi keamanan, semua divisi menggunakan jaringan atau segment yang sama sehingga bisa saling mengakses data komputer satu sama lain. Hal ini di khawatirkan terjadi pencurian data rahasia perusahaan. Dari segi *High Availability*, belum adanya jalur redundansi antar *switch*, sehingga akan mengakibatkan jaringan terputus ketika salah satu *switch* mengalami masalah atau mati.

Batasan Sistem

Jaringan yang ada pada PT. XYZ saat ini terdiri dari server yang berfungsi sebagai web server yang digunakan untuk internal dan router untuk akses internet yang disambungkan ke switch agar client dapat mengakses dan mengirim data melalui internet.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Berikut ini adalah topologi jaringan yang berjalan:



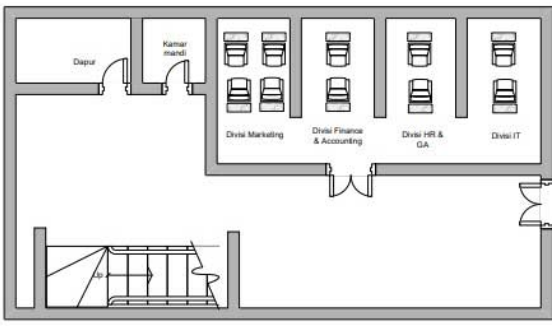
Gambar 1. Topologi LAN Yang Berjalan

Permasalahan yang terjadi di PT. XYZ akan diuraikan dengan menggunakan metode SWOT (*Strength, Weaknes, Opportunity, Threats*), yaitu sebagai berikut:

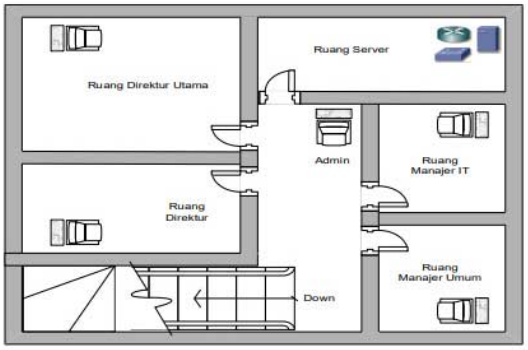
1. **Strength (kekuatan)**
   Jaringan LAN yang ada pada PT. XYZ sudah terkoordinasi dengan cukup baik dan telah memiliki pusat data sendiri. Untuk perangkat jaringan yang ada pada PT. XYZ sudah memenuhi standar untuk perancangan STP dan VTP. Memiliki petugas IT berlatar belakang pendidikan komputer dan jaringan.
2. **Weekness (kelemahan)**
   Belum adanya jalur cadangan yang bertugas membackup jalur data. Semua divisi masih menggunakan segment jaringan yang sama. Masih perlunya adanya penanganan cepat dan tepat apabila terjadi gangguan jaringan.
3. **Opportunities (peluang)**
   Banyaknya sistem-sistem dan perangkat yang dapat mengoptimalkan proses pengiriman data. Tersedianya perangkat lunak yang dapat memonitoring kinerja jaringan.
4. **Threats (ancaman)**
   Banyaknya worm dan virus jaringan seperti trojan yang menyebar di internet. Bila terjadi kerusakan pada port akan mengakibatkan penundaan proses pengiriman data.
5. **Strategi S.O**
   Memudahkan pengimplementasian STP dan VTP agar pengiriman data dapat bekerja secara maksimal.
6. **Strategi W.O**
   Menambahkan sistem STP dan backup jalur data, agar mengoptimalkan proses pengiriman data.
7. **Strategi S.T**
   Memaksimalkan kinerja dalam proses pengiriman data dan mengoptimalkan implementasi STP dengan metode PVST dan VTP. Menambahakan metode sistem backup Cloud atau penyimpanan berbasis internet untuk data-data client.
8. **Strategi W.T**
   Menambahkan perangkat atau sistem yang bertugas untuk mengoptimalkan implementasi STP dan VTP dan dapat mengatasi virus serta membatasi akses menuju situs-situs yang dapat mengancam client.

Rancangan Pemetaan Jaringan

Untuk rancangan pemetaan jaringan diuraikan berdasarkan denah pada setiap lantai, untuk lantai 1 dan lantai 2 akan di gambarkan pada denah sebagai berikut.



Gambar 2. Denah lantai 1



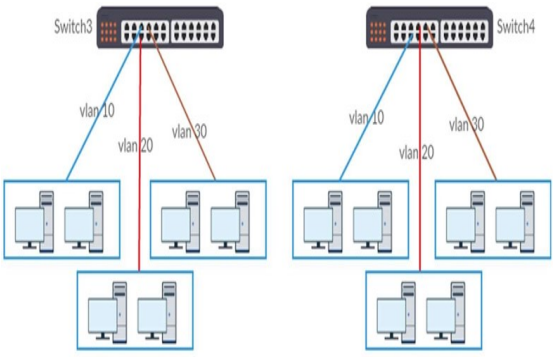
Gambar 3. Denah lantai 2

VLAN di konfigurasikan pada switch catalyst 2960 yang dimiliki. Pada topologi rancangan switch cisco akan menjadi core switch yang mana semua traffic yang ada akan memecah / membagi LAN pada jaringan yang ada menjadi beberapa segment network. Adapun VLAN yang akan digunakan yaitu:

Tabel 1. Network VLAN

VLAN ID	Network	Nama VLAN
VLAN10	172.168.10.0/24	VLAN-ATASAN
VLAN20	172.168.20.0/24	VLAN-MARKETING
VLAN30	172.168.30.0/24	VLAN-KEUANGAN
VLAN40	172.168.40.0/24	VLAN-HR
VLAN50	172.168.50.0/24	VLAN-MANAGEMENT
VLAN60	172.168.60.0/24	VLAN-IT

Berikut ini adalah gambar rancangan vlan yang akan di implementasikan:



Gambar 4. Rancangan Vlan

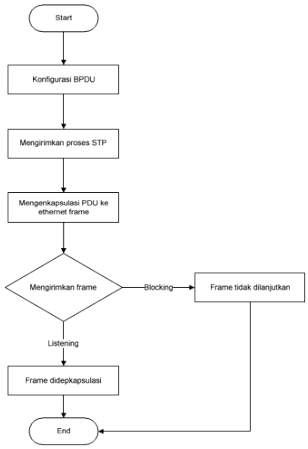
Proses Jaringan STP dan VTP

Dalam proses jaringan perancangan STP dan VTP menggunakan dua layers diantaranya: layer 1 (Pysical layer) dan layer 2 (Data Link Layer). Dari proses layer pada jaringan STP dan VTP terbagi dari dua sisi, layer masuk (In Layers) dan layer keluar (Out Layers).

Proses STP (Spanning Tree Protocol)

Gambar 5. Rancangan *Spanning Tree Protocol*

Proses VTP (VLAN Trunking Protocol)

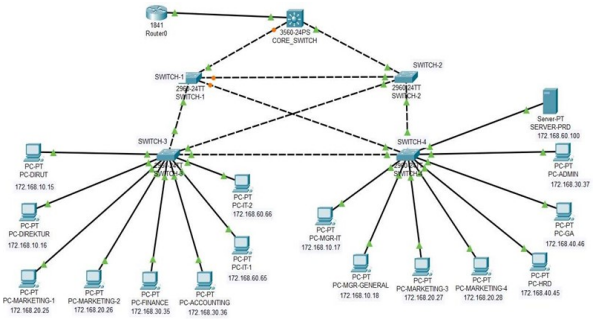


Gambar 6. Rancangan VLAN Trunking Protocol

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Rancangan Implementasi

Rancangan usulan topologi jaringan komputer pada PT. XYZ, dan perbandingan dengan topologi yang saat ini berjalan dengan tampilan hasil sebagai berikut:



Gambar 7. Rancangan topologi Usulan.

Rancangan topologi usulan sudah di uji coba menggunakan software simulasi Cisco Packet Tracer.

Berikut ini adalah tabel hasil Fast Ethernet dari switch ke PC dan switch ke Switch:

Tabel 2. Mapping port pada PC

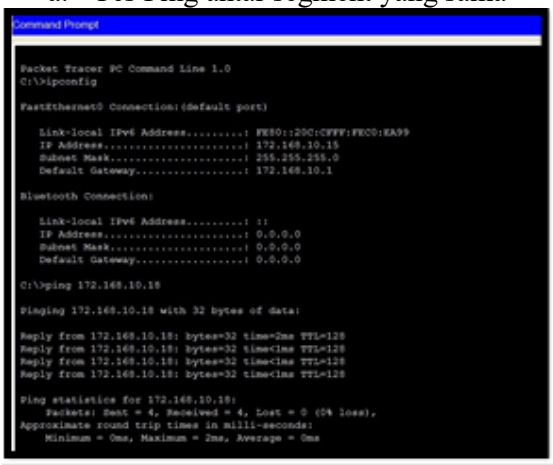
Switch	FastEthernet	PC
Switch3	FastEthernet0/10	PC-DIRUT
	FastEthernet0/11	PC-DIREKTUR
	FastEthernet0/12	PC-MARKETING-1
	FastEthernet0/13	PC-MARKETING-2
	FastEthernet0/14	PC-FINANCE
	FastEthernet0/15	PC-ACCOUNTING
	FastEthernet0/16	PC-IT-1
	FastEthernet0/17	PC-IT-2
Switch4	FastEthernet0/10	PC-MGR-IT
	FastEthernet0/11	PC-MGR-GENERAL
	FastEthernet0/12	PC-MARKETING-3
	FastEthernet0/13	PC-MARKETING-4
	FastEthernet0/14	PC-HRD
	FastEthernet0/15	PC-GA
	FastEthernet0/16	PC-ADMIN
	GigabitEthernet0/1	SERVER-PRD

Tabel 3. Mapping port pada Switch

Switch	FastEthernet	Mode	Switch dan FastEthernet
SWITCH-1	FastEthernet0/2	Trunk	SWITCH-3:FastEthernet0/2
	FastEthernet0/3		SWITCH-2:FastEthernet0/3
	FastEthernet0/4		SWITCH-4:FastEthernet0/4
	FastEthernet0/5		CORE_SWITCH: FastEthernet0/5
SWITCH-2	FastEthernet0/2	Trunk	SWITCH-4:FastEthernet0/2
	FastEthernet0/3		SWITCH-1:FastEthernet0/3
	FastEthernet0/4		SWITCH-3:FastEthernet0/4
	FastEthernet0/6		CORE_SWITCH: FastEthernet0/6
SWITCH-3	FastEthernet0/2	Trunk	SWITCH-1:FastEthernet0/2
	FastEthernet0/3		SWITCH-4:FastEthernet0/3
	FastEthernet0/4		SWITCH-2:FastEthernet0/4
SWITCH-4	FastEthernet0/2	Trunk	SWITCH-2:FastEthernet0/2
	FastEthernet0/3		SWITCH-3:FastEthernet0/3
	FastEthernet0/4		SWITCH-1:FastEthernet0/4

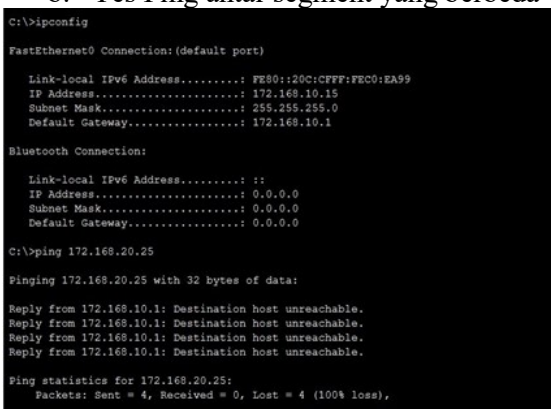
Pengujian

a. Tes Ping antar segment yang sama



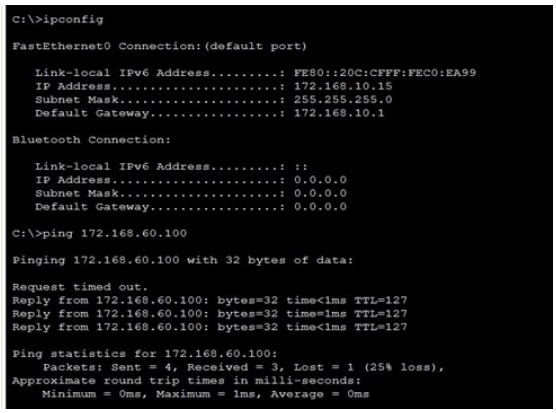
Gambar 8. Tes ping sesama segment

b. Tes Ping antar segment yang berbeda



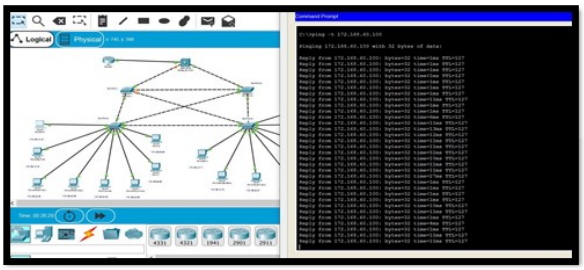
Gambar 9. Tes ping beda segment

c. Tes Ping ke Server

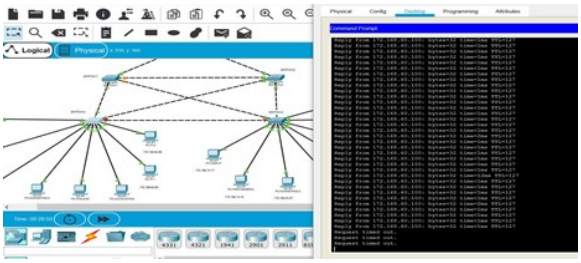


Gambar 10. Tes ping ke server

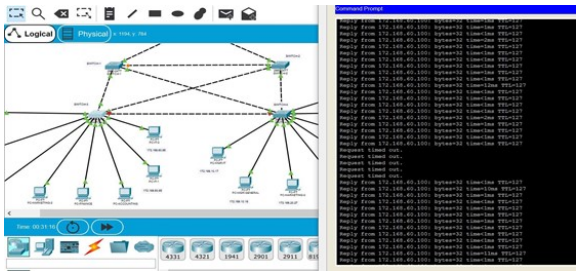
d. Tes memutuskan salah satu Root Port pada switch3



Gambar 11. Tes cabut root port bag 1



Gambar 12. Tes cabut root port bag 2



Gambar 13. Tes cabut root port bag 3

D. PENUTUP

Berdasarkan dari hasil uraian bab-bab sebelumnya, maka dapat diambil kesimpulan, Dalam jaringan yang berjalan pada PT. XYZ, semua divisi menggunakan segment jaringan yang sama. Dalam jaringan yang berjalan pada PT. XYZ belum adanya jalur backup antar switch sehingga jika salah satu jalur mati, maka jaringan lantai 1 dan lantai 2 akan terputus. Dalam perancangan jaringan yang baru akan diimplementasikan STP dan VTP, agar proses pengiriman data dapat bekerja dengan baik tanpa mengalami broadcast storm atau loop. Perangkat yang digunakan pada implementasi STP dan VTP membutuhkan perangkat jaringan diantara router, 4 Switch Akses, 1Switch Core dan kabel UTP yang terhubung ke perangkat – perangkat switch.

PT. XYZ perlu meningkatkan kemampuan personil IT mengenai pemahaman tentang internetwork dan konfigurasi. Implementasi jaringan dengan Vlan Trunking Protokol untuk membagi segment jaringan antar divisi dan membuat jalur backup antar switch agar ketika salah satu Jalur mati, maka jaringan akan tetap terhubung..

E. DAFTAR PUSTAKA

Afdhal, Munadi, R., & Fachdil, I. (2015). Evaluasi Kinerja VLAN Trunking Protocol dengan Metode Spanning Trees

Protocol Menggunakan GNS-3. *Seminar Nasional Dan Expo Teknik Elektro.*

Diansyah, T. M. (2016). *Metode ACL (Access Control List) menggunakan frame relay pada jaringan WAN (Wide Area Network)*. Jakarta: Majalah Ilmiah Warta Dharmawangsa.

Fitriansyah, A., Andreansyah, A., & Abu, S. (2019). Penerapan Static VLAN dan Access List Untuk Meningkatkan Keamanan Jaringan. *Jurnal Teknologi Informatika dan Komputer, Vol. 5, No. 2*, 58-63.

Hasrul, H., & Lawani, A. M. (2017). Pengembangan Jaringan Wireless Menggunakan Mikrotik Router Os Rb750 Pada PT. Amanah Finance Palu. *Jurnal Elektronik Sistem Informasi Dan Komputer, Vol.3 No.1* , 11–19.

Saibi, R., Kurniabudi, & Rahim, A. (2014). Analisa dan Perancangan Jaringan Komputer Menggunakan Metode Virtual Local Area Network (VLAN) (Studi Kasus: Diskominfo Provinsi Jambi). *Jurnal Ilmiah Media Processor, 9(2)*, 185–195.

Suryantoro, H., Sopian, A., & Dartono. (2021). Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan VPN-IP Berbasis IPSEC. *Jurnal Elektro dan Informatika Swadharma, Vol.01 No.1*, 21–25.

Wiguna, A. W., Herlawati, & Santoso, B. (2013). Penerapan Spanning Tree Protocol Terhadap Wide Area Network (WAN) Pada PT. Duta Lestari Sentratama Jakarta. *Techno Nusa Mandiri, Vol.09 No.01*, 10–19.

IMPLEMENTASI VIRTUAL PRIVATE NETWOR MENGGUNAKAN POINT-TO-POINT TUNNELING PROTOCOL

Eka Satryawati[1)], Dwi Agung Pangestu[2)], Ade Surya Budiman[3)]
[1]Prodi Sistem Informasi, Fakultas Komputer, Universitas MH Thamrin Jakarta
[2]Prodi Teknik Informatika, FTI, Universitas Nusa Mandiri, Jakarta
[3]Prodi Teknologi Komputer, FTI, Universitas Bina Sarana Informatika, Jakarta

Correspondence author: Eka Satryawati, ekathufail@gmail.com, Jakarta, Indonesia

Abstract

Today's technological development is very rapid, especially in the field of network security. The field of network security is a matter that will be a very important part because the network security system is used to guarantee the confidentiality, theft, or burglary of data on a company. In its implementation, a VPN network (Virtual Private Network) uses a site-to-site Point to Point Tunel Protocol (PPTP) method to connect between two places that are located far apart. The main facility of using PPTP is being able to use a public-switched telephone network (PSTN) to build a VPN. At PT Indosis Integrasi Jakarta, the place where the author conducts research there are several problems that the author found, namely, when sending data between the head office and branch offices in Bandung, there is no security that ensures that the data is safe. With the current state of the network, uninterested parties will easily access or steal confidential company data.

Keywords: virtual private network, point-to-point tunneling protocol

Abstrak

Perkembangan teknologi dijaman sekarang sangat pesat, khususnya dibidang keamanan jaringan yang sangat mendasar bagi dunia teknologi internet. Dalam teknologi internet dibidang jaringan merupakan suatu hal yang akan menjadi bagian yang sangat penting, karena sistem keamanan jaringan digunakan untuk menjamin kerahasiaan, pencurian, ataupun pembobolan data pada suatu perusahaan. Dalam implementasinya, jaringan VPN (Virtual Private Network) menggunakan metode Point-To-Point Tunneling Protocol (PPTP) site-to-site untuk menghubungkan antara 2 tempat yang letaknya berjauhan. Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTN) untuk membangun VPN pada PT. Indosis Integrasi Jakarta, tempat dimana penulis melakukan riset terdapat beberapa permasalahan yang penulis dapati yaitu saat melakukan pengiriman data-data antara kantor pusat dan kantor cabang Bandung tidak adanya pengamanan yang memastikan bahwa data tersebut aman. Dengan keadaan jaringan saat ini, pihak-pihak yang tidak berkempentingan akan mudah mengakses atau mencuri data perusahaan yang bersifat rahasia.

Kata Kunci: virtual private network, point-to-point tunneling protocol

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

A. PENDAHULUAN

Perkembangan teknologi sekarang ini sangat pesat, khususnya dibidang keamanan jaringan yang sangat mendasar bagi dunia teknologi internet. Dalam teknologi internet dibidang keamanan jaringan merupakan suatu hal yang akan menjadi bagian yang sangat penting, karena sistem keamanan jaringan digunakan untuk menjamin kerahasiaan, pencurian, ataupun pembobolan data pada suatu perusahaan.

Dengan semakin pesatnya teknologi, bukan berarti mengurangi permasalahan yang terjadi pada jaringan komputer. Seperti yang terjadi di PT. Indosis Integrasi, sering terjadi permasalahan keamanan jaringan komputer, ditambah dengan jarak yang cukup jauh antara kantor pusat dengan kantor cabang Bandung, sehingga menyebabkan kendala ketika ada permasalahan keamanan pada jaringan yang terjadi di kantor cabang Bandung tidak dapat diatasi dengan cepat.

Masalah seperti ini dapat terjadi bagi perusahaan yang memiliki kantor cabang yang letaknya berjauhan dengan kantor pusatnya. Untuk itu pihak perusahaan sangat mengharapkan adanya sistem jaringan komputer yang aman agar dapat digunakan untuk mengontrol, memonitoring dan mengatasi permasalahan keamanan jaringan di cabang Bandung secara cepat.

Menurut Prihatin Oktivasari dan Andri Budi Utomo, cara atau sistem yang dapat digunakan untuk melakukan hal tersebut adalah menggunakan Virtual Private Network (VPN). Dengan VPN sebuah instansi dapat memperlebar akses dengan aman terhadap jaringan internalnya melalui jaringan internet dengan biaya yang relatif lebih murah. Seluruh aplikasi dan data yang penting pada jaringan tersebut dapat diakses oleh pihak tertentu saja yang diberikan wewenang tanpa memperhatikan jarak dan tempat dimana diaksesnya (Oktivasari & Utomo, 2016).

Sebuah keamanan dalam berkomunikasi atau dalam pertukaran data, juga tidak memungkinkan pihak lain untuk menyusup ke *traffic* (lalu lintas jaringan) yang tidak semestinya. VPN adalah sebuah cara amanuntuk mengakses *local area network* yang berada pada jangkauan, dengan menggunakan internet atau jaringan umum lainnya untuk melakukan transmisi data paket secara pribadi, dengan enkripsi perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya kedalam *remote-site* (Yuniati, Fitriawan, & Fahdi 2014). Sebuah teknologi jaringan komputer yang dikembangkan oleh perusahaan skala besar yang menghubungkan antara jaringan diatas jaringan lain menggunakan internet yang membutuhkan jalur *privacy* dalam komunikasinya (Triyono, Rachmawati, & Irnawan, 2014).

Dalam implementasinya, jaringan VPN (*Virtual Private Network*) menggunakan metode *Point-To-Point Tunneling Protocol* (PPTP) *site-to-site* untuk menghubungkan antara dua tempat yang berjauhan. *Point-To-Point Tunneling Protocol* (PPTP) merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access point-to-point protocol* (PPP) yang dikeluarkan *Internet Engineering Task Force* (IETE). PPTP merupakan protocol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat dikirimkan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN to LAN dan komputer yang terhubung dangan LAN untuk membuat VPN melalui LAN (Mufida, Irawan, & Chrisnawati, 2017). PPTP merupakan protokol jaringan yang

memungkinkan pengamanan transfer data remote klien ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Rachmawan & Prihanto, 2018). Point to Point Tunneling Protocol (PPTP) merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Putra, Indriyani, & Angraini, 2018).

Berdasarkan uraian permasalahan diatas maka penulis mengusulkan menggunakan metode PPTP pada jaringan VPN dimana ketika terjadi permasalahan jaringan pada kantor cabang Bandung dapat diremote dari kantor pusat dan dapat melakukan sharing file antara kantor pusat dan kantor cabang Bandung. Sehingga lalu lintas data yang dikirim dapat terjaga keamanan dan kerahasiaannya dari ancaman orang yang tidak bertanggung jawab.

B. METODE PENELITIAN

Teknik pengumpulan data yang digunakan oleh penulis adalah :

1. Observasi
   Untuk mendapatkan hasil penelitian yang baik penulis melakukan pengamatan di PT. Indosis Integrasi Jakarta terhadap kondisi jaringan saat ini dan interkoneksi jaringan ke kantor cabang Bandung.
2. Wawancara
   Dalam wawancara ini dilakukan tanya jawab dengan praktisi IT pada PT. Indosis Integrasi Jakarta, Administrator jaringan dan user yang ada di PT. Indosis Integrasi Jakarta dan beberapa orang yang ahli dalam jaringan.
3. Studi Pustaka
   Untuk menelaah masalah secara mendalam dan untuk mencari solusi optimal terhadap permasalahan yang ada, maka penulis juga melakukan studi kepustakaan yaitu dengan mengumpulkan data – data teoritis dalam beberapa jurnal, artikel, dan mempelajari buku – buku dengan maksud untuk mendapatkan teori – teori dan bahan – bahan yang berkaitan dengan masalah tersebut.

Analisa penelitian ini dilakukan sebagai salah satu alat proses untuk pengambilan keputusan, analisa penelitian ini berguna untuk mengurangi ketidakpastian dengan menyediakan informasi yang akurat untuk memperbaiki proses pembuatan keputusan itu. Tahapan penelitian yang penulis lakukan yaitu :

1. Analisa kebutuhan
   Disini penulis juga pengumpulan data membutuhkan sebuah mikrotik yang dirancang agar saling terhubung antar mikrotik dengan menggunakan akses VPN dengan metode PPTP (Point-To-Point Tunnel protocol) dan untuk jaringan penulis menggunakan jaringan yang sudah berjalan di perusahaan PT. Indosis Integrasi Jakarta.
2. Desain
   Penulis menggunakan sebuah mikrotik yang didesain membuat jaringan virtual atau simulasi menggunakan VMware sebagai penghubung agar koneksi antar cabang Bandung seakan - akan jaringan lokal.
3. Testing
   Penulis melakukan testing dengan membuktikan koneksi jaringan antar cabang Bandung yang dirancang berjalan dengan maksimal.
4. Implementasi
   Setelah membuat desain dan sudah melakukan testing berkali – kali sampai sebuah sistem rancang VPN menggunakan Point-to-Point tunnel protocol (PPTP) dengan mikrotik sudah berjalan dan berfungsi dengan maksimal, penulis baru bisa melakukan implementasi, agar pada saat sudah dijalankan tidak ada masalah.

C. HASIL DAN PEMBAHASAN

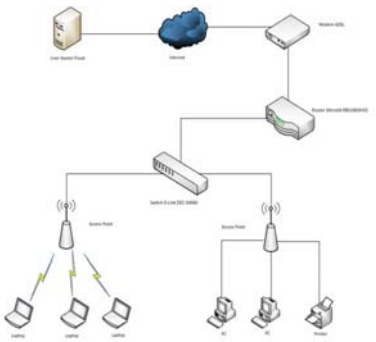
Topologi Jaringan

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

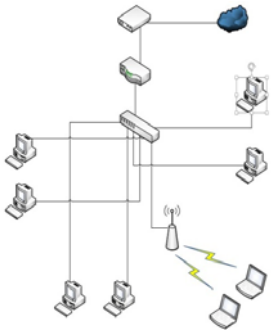
Jaringan komputer pada PT.Indosis Integrasi Jakarta menggunakan star dimana pada topologi tersebut terdapat swith sebagai pusatnya. Server setiap komputer client dan piranti lainnya terhubung dengan menggunakan kabel.

Skema Jaringan

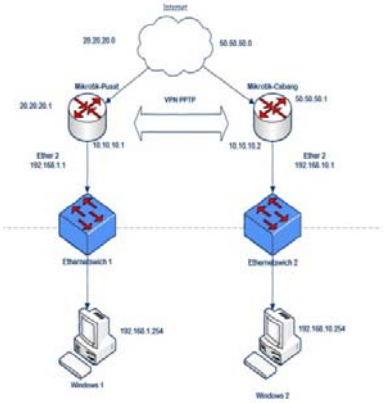
Pada skema jaringan, penulis tetap menggunakan skema jaringan yang sudah berjalan, karena skema jaringan yang sudah berjalan dirasa sudah sangat cukup baik hanya saja ditambahkan 1 buah PC Server untuk disetting menjadi Server VPN, baik dikantor pusat maupun dikantor cabang Bandung, dimana dimasing – masing PC tersebut nantinya bisa mengontrol PC lainnya yang ada pada jaringan di kantor cabang Bandung, sehingga jaringan kantor pusat dan cabang Bandung dapat saling terhubung secara aman menggunakan teknologi *Virtual Private Network* (VPN) dengan menggunakan metode *Point-to-Point Tunneling Protocol* (PPTP).



Gambar 1. Skema Jaringan Kantor Pusat



Gambar 2. Skema jaringan Kantor Bandung



Gambar 3. Skema Jaringan Usulan

Keamanan Jaringan

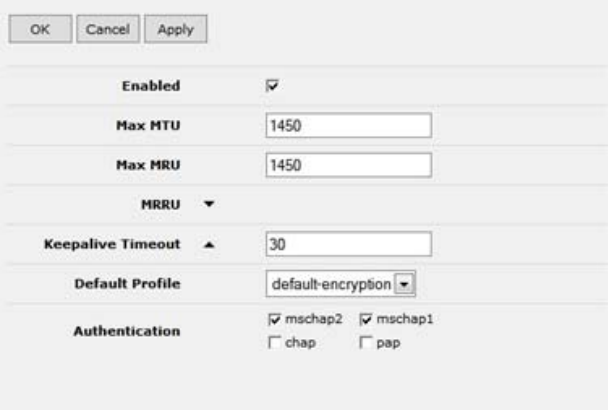
Menggunakan keamanan jaringan sangat diperlukan agar data serta informasi yang ada dapat terjaga dengan baik dan mencegah terjadinya upaya dari pihak lain seperti hacker. Selain dengan menggunakan metode PPTP (Point-to-Point Tunneling Protocol) setiap user yang hendak terhubung kejaringan local masih harus verifikasi user dan password yang diminta oleh komputer server.

Rancangan Aplikasi

Konfigurasi yang akan digunakan yaitu dengan menerapkan metode PPTP (Point-to-Point Tunneling Protocol) yang akan dilakukan pada router mikrotik pada masing–masing kantor. Berikut ini adalah konfigurasi PPTP (Point-to-Point Tunneling Protocol) pada router mikrotik pusat yang berfungsi sebagai server VPN.

Konfigurasi PPTP

Untuk menggunakan fitur PPTP pada router mikrotik, beri tanda cheklist pada enable terlebih dahulu untuk konfigurasi PPTP server pada mikrotik yang akan menjadi server PPTP, pada gambar dibawah adalah mikrotik dikantor pusat yang dipilih untuk menjadi server, masuk ke menu PPP pada menu bar mikrotik disebelah kiri lalu pilih PPTP server pada menu bar lalu checklist pada bagian enable.

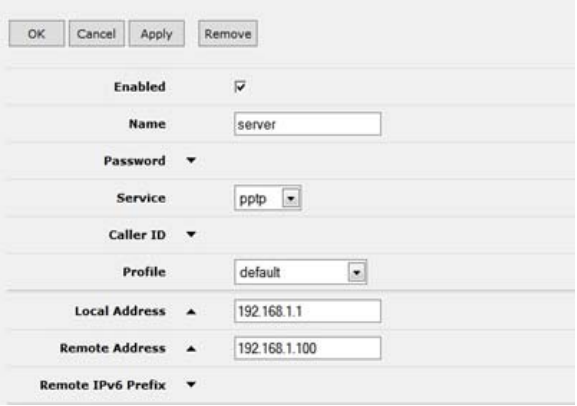


Gambar 4. Konfigurasi PPTP

Konfigurasi user PPTP

Pilih tab secret dimana tab ini berisikan konfigurasi pembuatan username dan password yang akan dapat mengakses jaringan local melalui internet.Pada kolom name isikan nama sesuai keinginan, pada gambar diatas disii dengan nama "server" dan pada password diisi "1234567890".

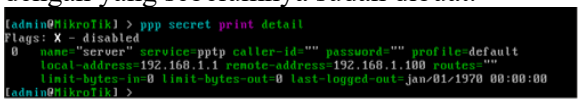
Lalu pada kolom local address diisi dengan IP public atau IP addressrouter mikrotik yang berada dikantor pusat atau yang menjadi server pada kolom remote address diisi dengan alamat IP address yang nantinya akan diberikan pada user apabila sudah berhasil mengakses PPTP server pada router mikrotik yang berada dikantor pusat sudah selesai dibuat, untuk mengakses PPTP VPN tersebut dapat dilakukan pada mikrotik cabang Bandung.



Gambar 5. Konfigurasi user PPTP

Konfigurasi VPN client

Pada bagian connectto diisikan IP address pusat sedangkan untuk kolom username dan password isikan sesuai dengan username dan password sesuai dengan yang sebelumnya sudah dibuat.



Gambar 6. Konfigurasi VPN client

Manajemen Jaringan

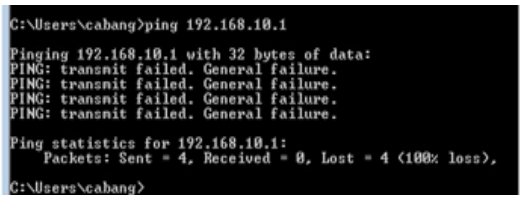
Sangat penting untuk melakukan manajemen jaringan dalam membangun suatu jaringan komputer apalagi jika jaringan sudah sangat luas cakupannya. Agar proses berbagi data lebih terjamin keamanannya dan menjaga jaringan tetap berjalan dengan baik.

Pada penerapannya metode *tunneling protocol* ini sangat membantu administrator jaringan untuk lebih mudah mengawasi, memonitoring jaringan komputer yang sedang berjalan dan pengambilan data tanpa harus melakukan kunjugan ke kantor cabang.

Pengujian Jaringan Awal

Pada tahap pengujian awal dilakukan sebelum adanya penerapan metode tunneling PPTP pada router mikrotik dapat dilihat bahwa setiap user pada masing – masing kantor belum dapat terhubung.

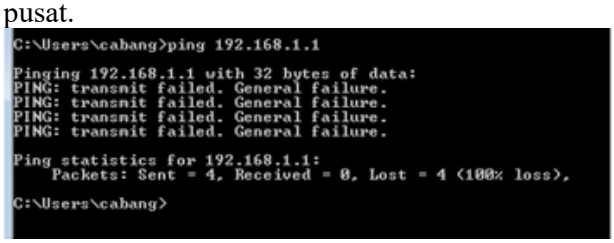
Penulis melakukan test ping pada user yang berada dikantor pusat ke user yang berada dikantor cabang Bandung, dapat dilihat bahwa transmite failed. General failure atau bisa juga disebut system tidak bisa mengirimkan paket ping antara kantor pusat dengan kantor cabang Bandung karena suatu masalah.



Gambar 7. Test Ping pusat – cabang Bandung kondisi awal

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Dari gambar dibawah dapat dilihat bahwa hasil ping juga menunjukkan hasil yang sama dengan percobaan sebelumnya. Hal ini terjadi karena belum terhubungnya kantor cabang Bandung dengan kantor pusat.

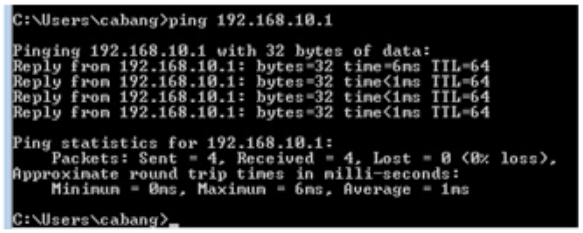


Gambar 8. Test Ping cabang Bandung – pusat kondisi awal

Pengujian Jaringan Akhir

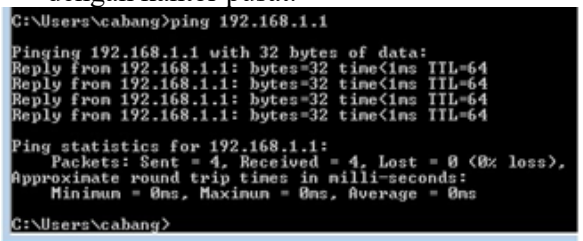
1. **Test Ping**

   Dalam percobaan ini penulis melukan test ping pada user yang berada dikantor pusat ke user kantor cabang,Bandung dapat dilihat bahwa sudah terjalin komunikasi atau jaringan sudah terkoneksi.



Gambar 9. Test Ping pusat – cabang Bandung (Setelah pengujian)

Penulis juga melakukan percobaan yang sama pada user kantor cabang Bandung test ping dengan user yang berada kantor pusat, dapat dilihat bahwa permintaan sudah direspon atau jaringan sudah terkoneksi antar kantor cabang Bandung dengan kantor pusat.

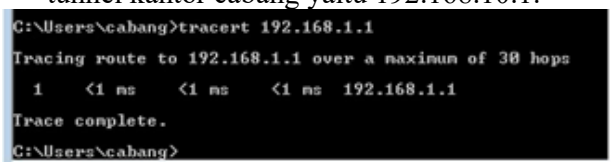


Gambar 10. Ping cabang Bandung – pusat (setelah pengujian)

2. **Test Traceroute**

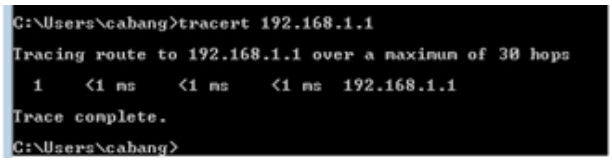
   Kemudian untuk pengetesan traceroute penulis juga melakukan pengentesan "Traceroute" sebelumnya yaitu tiap kantor dan juga melalui jaringan VPN yang sudah terbentuk.

   Gambar dibawah adalah pengetestan trace route dari kantor pusat ke ykantor cabang Bandung dimana dapat dilihat yaitu bahwa rute paket yang dilewati yaitu melaui 192.168.1.1 yaitu gateway LAN kantor pusat dan gateway PPTP tunnel kantor cabang yaitu 192.168.10.1.



Gambar 11. Traceoute pusat ke cabang Bandung (setelah pengujian)

Gambar dibawah adalah pengetestan trace route dari kantor cabang ke kantor pusat dimana dapat dilihat yaitu bahwa rute paket yang dilewati yaitu melalui 192.168.10.1 yaitu gatewayLAN kantor cabang Bandung dan gateway PPTP tunneling kantor cabang Bandung yaitu 192.168.1.1.



Gambar 12. Traceroute cabang Bandung ke pusat (setelah pengujian)

D. PENUTUP

VPN adalah sebuah koneksi Virtual yang bersifat private, disebut demikian karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut private karena jaringan ini merupakan jaringan yang sifatnya private dan tidak semua orang bisa mengaksesnya.

VPN dapat mengirim data antara dua komputer yang melewati jaringan publik

sehingga seolah – olah terhubung secara Point-To-Point.

Data yang dikirimkan dienkapsulasi dan di encripsi kedalam bentuk pecahan data dengan header yang berisi informasi routing untuk mendapatkan koneksi Point-To-Point sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan.

Point-To-Point Tunneling Protocol (PPTP) adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server perusahaan dengan suatu Virtual Private Network (VPN) melalui jaringan data berbasis TCP/IP.

Untuk mendapatkan koneksi bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang ketangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut "Tunneling".

Dengan menggunakan VPN PPTP dapat mengurangi biaya operasional bila dibandingkan dengan menggunakan aplikasi Hamachi untuk mengirim file secara rahasia dan aman.

E. DAFTAR PUSTAKA

Amillia, F., Marzuki, & Agustina. (2014). Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) dan Geographic Routing Protocol (GRP) Pada Mobile Ad Hoc Network. Manet. 12(1), 9–15.

Khasanah, S. N., & Kuryanti, S. J. (2019). Rancangan Virtualisasi Server Menggunakan VMWare Vsphare. EVOLUSI - Jurnal Sains Dan Manajemen, 7(1), 42–46. https://doi.org/10.31294/evolusi.v7i1.5091

Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site Mikrotik VPN dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta.

Muftikhali, Q. E., Yansen, A., Danar, F., Kusumawati, A., & Hidayat, S. (2018). Optimasi Algoritma Genetika Dalam Menentukan Rute Optimal Topologi Cincin Pada Wide Area Network. 13(1), 1–6.

Oktivasari, P., & Utomo, A. B. (2016). Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol Analysis of Virtual Private Network Using Openvpn and Point To. Jurnal Penelitian Komunikasi Dan Opini Publik, 20(2), 185–202.

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. 3(2), 260–267.

Rachmawan, A., & Prihanto, A. (2018). Jurnal Perbandingan Protokol L2TP dan PPTP Untuk Membangun Jaringan Intranet Di atas VPN. 53–57.

Triyono, J., Rachmawati, Y., & Irnawan, F. D. (2014). Analisa Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data. 1(2), 112–121.

Varianto, E., & Badrul, M. (2015). Implementasi Virtual Private Network dan Proxy Server Menggunakan Clear OS Pada PT. Valdo Internasional. 1(1), 54–65.

Yuniati, Y., Fitriawan, H., Fahdi, D., & Patih, J. (2014). Analisa Perancangan Server VOIP (Voice Internet Protocol) Dengan OpenSource Asteriks dan VPN (Virtual Private Network). 12(1), 112–121.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

PENERAPAN USER CENTERED DESIGN (UCD) PADA WIREFRAME DESAIN USER INTERFACE DAN USER EXPERIENCE APLIKASI SINOPSIS FILM

Muhammad Syarif Hartawan
Fakultas Teknik, Universitas Krisnadwipayana

Correspondence author: Muhammad Syarif Hartawan, muhammadsyarif@unkris.ac.id, Jakarta

Abstract

The purpose of this research is as a prototype for the application of User Centered Design in the development of User Interface Design and User Experience on the Film Synopsis android application. In developing android applications, the design of the User Interface (UI) and User Experience (UX) is a very important initial stage in using the application. This UI/UX will provide a user experience in using and interacting with this android application. In this article, we explain how UI/UX is designed in Film Synopsis using a User Centered Design (UCD) approach. At UCD there are 4 (four) stages in the UI/UX approach, namely analysis, design, evaluation, and implementation. Users will be involved in evaluating the designs that are made, so that the designs that are formed (made) can be improved for the convenience of users or android application users.

Keywords: user centered design, user interface design, user experience

Abstrak

Tujuan dari penelitian ini adalah sebagai prototype penerapan *User Centered Design* dalam pengembangan *User Interface Design* dan *User Experience* pada aplikasi android Sinopsis Film. Dalam pengembangan aplikasi android perancangan *User Interface* (UI) dan *User Experience* (UX) merupakan tahapan awal yang sangat penting dalam penggunaan aplikasi. UI/UX ini akan memberikan pengalaman pengguna dalam menggunakan serta berinteraksi pada aplikasi android ini. Dalam artikel ini menjelaskan bagaimana UI/UX dirancang pada Sinopsis Film menggunakan pendekatan *User Centered Design* (UCD). Di UCD ada 4 (empat) tahapan dalam pendekatan UI/UX yaitu analisis, desain, evaluasi, dan implementasi. User atau pengguna akan dilibatkan dalam melakukan evaluasi desain yang dibuat, sehingga desain yang dibentuk akan dapat diperbaiki guna kenyamanan user atau pengguna aplikasi android.

Kata Kunci: desain berbasis pengguna,desain antarmuka pengguna

A. PENDAHULUAN

Dengan meningkatnya jumlah film yang beredar di pasaran, tentunya akan membuat calon penonton merasa kesulitan dalam menentukan film mana yang akan ditonton. Untuk mengatasi masalah tersebut terdapat beberapa cara yang dapat dilakukan, misalnya mencari di situs web penyedia layanan film, membaca deskripsi film, atau

menanyakan kepada teman, dan lain sebagainya.

Untuk mendapatkan kenyamanan dalam akses informasi yang cepat dan update merupakan salah satu tuntutan dari suatu aplikasi perusahaan yang mengandalkan penyampaian informasi kepada customer maupun masyarakat saat ini (Hartawan, 2019). Aplikasi Android saat ini telah berkembang sangat cepat menjadi salah satu alternatif media informasi yang dapat dihandalkan dalam penyampaian informasi. Disamping itu, media aplikasi android juga memungkinkan penggunanya untuk mendapatkan update data informasi, sehingga informasi dengan cepat dapat diakses kapan saja dan dimana saja.

Namun dalam aplikasi android masih ada permasalahan dalam desain *user interface* yang dibutuhkan oleh pengguna aplikasi android. *Interface* atau antarmuka berfungsi menjembatani pengguna dengan aplikasi tersebut. Karena aplikasi yang satu dengan aplikasi yang lain memiliki desain interface yang berbeda-beda, sehingga harus disesuaikan kembali fungsi dan kebutuhan aplikasi itu sendiri.

Dalam aplikasi sinopsis film ini membutuhkan desain interface yang dapat memenuhi kebutuhan informasi pengguna secara spesifikasi. Dalam upaya memberikan tampilan awal yang baik kepada pengguna aplikasi sinopsis film memerlukan desain *User Interface* (UI) dan *User Experience* (UX) yang ramah pengguna. Pada level individu, desain user interface dapat mengubah hidup banyak orang, sehingga penting desain sesuai dengan kebutuhan pengguna. Dari penjelasan tersebut desain user interface mempunyai peran yang penting dalam efektivitas suatu aplikasi android (Mazumder & Das, 2014).

User Interface (UI) adalah saat sistem dan pengguna dapat saling berinteraksi satu dengan lainnya melalui perintah seperti halnya menggunakan konten dan memasukan data. Sedangkan *User Experience* (UX) disebutkan sebagai pengalaman pengguna yang terkait dengan reaksi, persepsi, perilaku, emosi dan pikiran pengguna saat menggunakan sistem (Joo, 2017).

Terdapat beberapa pilihan pendekatan dalam merancang UI/UX, namun yang terkenal hanya *Human Centered Design* (HCD) dan *User Centered Design* (UCD). HCD adalah pendekatan yang berfokus kepada semua pengguna, baik potensial, ataupun tidak akan menjadi objek uji coba dalam proses pengumpulan data dan proses evaluasi dari desain yang sedang dirancang (Wijaya, 2019). Sedangkan pendekatan UCD berfokus pada calon pengguna yang spesifik, misalnya jenis kelamin dan rentang usia (Abras, Maloney-Krichmar, & Preece, 2004). Proses perancangan dari kedua pendekatan HCD dan UCD dilakukan dengan proses wawancara dan proses perancangan desain pengguna.

Wireframe adalah sebagai kerangka awal sebelum halaman website atau antarmuka sebuah aplikasi didesain. *Wireframe* merupakan tahapan penting dalam sebuah desain produk yang harus dipahami dengan baik. *Wireframe* merupakan tahap penting sebelum *stakeholder* menyetujui letak-letak informasi untuk aplikasi sebelum desain *user interface* di buat.

Berdasarkan latar belakang diatas maka penelitian ini dilakukan untuk mempresentasikan perancangan UI/UX pada aplikasi android. Adapun tujuan penelitian ini adalah untuk melihat 4 (empat) tahapan dalam pendekatan UI/UX yaitu analisis, desain, evaluasi, dan implementasi.

B. METODE PENELITIAN

Dalam perancangan UI/UX ini ada 4 (empat) langkah yang akan dilakukan yaitu :

1. Tahapan Analisa
   Proses analisis dilakukan saat pertama kali akan memulai seluruh proses perancangan, proses ini sangatlah penting

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

untuk mendapatkan gambaran awal sesuai dengan ekspektasi pengguna.

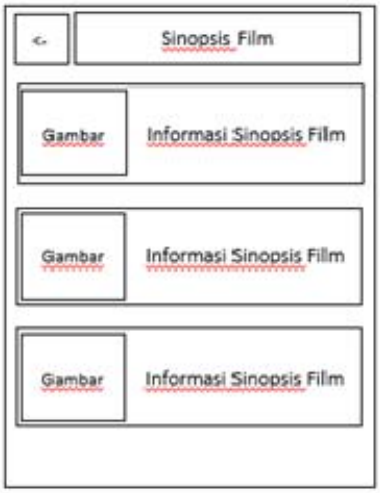
2. Tahapan Desain
   Tahapan proses desain adalah membuat sebuah prototype desain *wireframe* untuk aplikasi android yang dapat di evaluasi pada tahapan percobaan. Proses *prototyping* bagi pengembang sistem memiliki tujuan untuk mendapatkan informasi respon pengguna terhadap sistem melalui interaksi pengguna dengan *prototype* yang dikembangkan, alasannya karena *prototype* cukup menggambarkan versi awal dari sistem yang sesungguhnya (Purnomo, 2017). Proses pembuatan desain *prototype* adalah karena *prototype* dapat ditambah ataupun dikurangi secara mudah sesuai dengan proses pengembangan. Manfaat yang tidak kalah penting adalah dapat menghemat waktu, dana dan sumber daya.
3. Tahapan Evaluasi
   Tahapan Evaluasi desain *wireframe* UI/UX dilakukan dalam penyelesaian desain *prototype* dilakukan pada evaluasi desain *prototype* UI/UX. Dalam tahapan evaluasi dilakukan berulang kali guna mendapatkan umpan balik terus menerus terhadap desain *wireframe* yang telah dibuat, siklus ini dilakukan secara intensif sampai memperoleh desain *wireframe* UI/UX yang paling sesuai oleh pengguna. Tahapan proses evaluasi ini sesuai dengan pendekatan UCD yang sangat berfokus pada *end user* atau pengguna. Teknik yang digunakan dalam proses evaluasi adalah dengan memperlihatkan hasil desain dari proses tahapan sebelumnya dihadapan *end user* atau pengguna akhir.
4. Tahapan Implementasi
   Dalam tahapan implementasi rancangan desain UI/UX yang telah dievaluasi. Proses terakhir dalam perancangan desain UI/UX ini adalah tahapan proses implementasi dalam bentuk aplikasi android. Tahapan proses implementasi dilakukan dengan cara pembuatan rancangan desain aplikasi dengan menggunakan android studio.

C. HASIL DAN PEMBAHASAN

Berikut adalah hasil-hasil dari perancangan wireframe UI/UX pada aplikasi android sinopsis film menggunakan pendekatan UCD. Dalam gambar di bawah ini di dapat desain wireframe UI/UX pada tahapan awal. Desain ini merupakan desain home pada aplikasi.

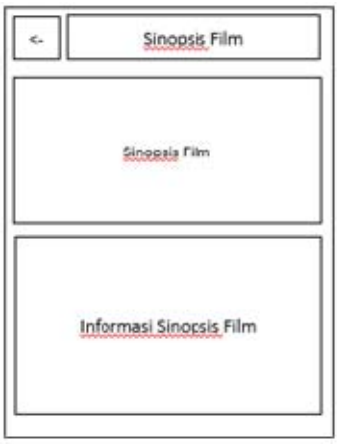
Gambar 1. Wireframe desain home awal.

Wireframe desain berikutnya adalah merupakan desain *halaman Informasi Sinopsis Film* pada aplikasi.



Gambar 2. Wireframe desain halaman pemilihan informasi atau cerita sinopsis film.

Pada wireframe desain berikutnya adalah merupakan desain wireframe *Informasi Cerita Film* yang telah dipilih pada aplikasi *Sinopsis Film* pada aplikasi.

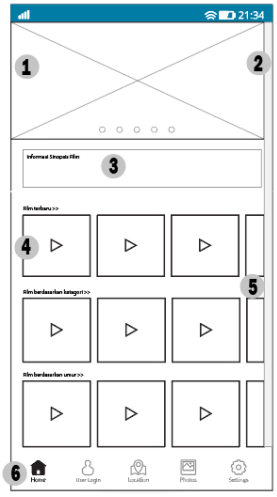


Gambar 3. Wireframe desain halaman pemilihan informasi atau cerita sinopsis film.

Hasil Perbaikan Wireframe Desain

Desain *Wireframe* di bawah ini merupakan hasil evaluasi berkali-kali sehingga di dapat desain *wireframe* UI/UX pada tahapan implementasi.

Dalam gambar 5 di bawah ini merupakan hasil revisi desain dari gambar 1 dan 2, dikarena kan pada desain halaman utama wajib menampilkan informasi yang dibutuhkan oleh end user atau pengguna akhir aplikasi android.



Gambar 4. Hasil Revisi Desain

Deskrispsi Visual Komponen Desain wireframe

1. Gambar Film.
2. Scroll Bar.
3. Teks Informasi.
4. Tampilan gambar film.
5. Penanda tampilan scroll ke kanan.
6. Navigasi

Fungsi Komponen Desain Wireframe

1. Menampilkan gambar film
2. Untuk menggulung layar aplikasi android ke bawah dan ke atas.
3. Memberikan informasi sinopsis film sesuai dengan tampilan gambar diatasnya.
4. Gambar film sekaligus untuk menampilkan langsung trailer film.
5. Menandakan bahwa pada bagian ini layar dapat di geser ke kiri dan kanan.
6. Navigasi utama yang dapat mengakses home, user login informasi, lokasi bioskop, foto-foto film, dan setting untuk dapat sesuai kebutuhan.

D. PENUTUP

Hasil desain wireframe UI/UX disimpulkan bahwa penggunaan metode UCD pada pembuatan desain wireframe ini mampu memberikan tata letak yang baik dari letak navigasi terhadap aplikasi android sinopsis film, selain tata letak yang tersusun rapi, terdapat juga informasi desain guna kebutuhan pengguna pada saat untuk mencari informasi saat simulasi proses desain awal terhadap rancangan UI/UX versi terakhir juga bisa dilakukan dengan baik.

E. DAFTAR PUSTAKA

Abras, C., Maloney-Krichmar, D., & Preece, J. (2004). *Encyclopedia of Human-Computer Interaction.* Thousand Oaks: Sage Publications. (inpress). Retrieved from https://www.academia.edu/download/6190316/10.1.1.9 4.381.pdf /

Hartawan, M. S. (2019). Analisis User Experience Untuk User Interface Pada Website fortis.id. *Jurnal Teknologi Informasi ESIT, vol. XIV, no. 01*, 51-56.

Joo, H. (2017). A Study on Understanding of UI and UX, and Understanding of Design According to User Interface Change. *International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20* , 9931-9935 .

Mazumder, F. K., & Das, U. K. (2014). Usability Guidelines For Usable User Interface . *IJRET: International Journal of Research in Engineering and Technology Vol 03*, 79-82.

Purnomo, D. (2017). Model Prototyping Pada Pengembangan Sistem Informasi. *Jurnal Informatika Merdeka Pasuruan (JIMP), Vol.2 No.2, ISSN 2503-1945*.

Wijaya, A. S. (2019, May 31). *User Centered Design*. Retrieved from School Of Information Systems, Binus University: https://sis.binus.ac.id/2019/05/31/user-centered-design/

OPTIMALISASI ROUTING MENGGUNAKAN SATU AUTONOMOUS SYSTEM NUMBER (ASN) BORDER GATEWAY PROTOCOL (BGP)

Muhammad Arif Zaky Zamany[1)], Hendra Supendar[2)], Sulistianto Sutrisno Wanda[3)]
[1,2,3]Prodi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri

Correspondence author: Sulistianto SW, sulistianto.sow@nusamandiri.ac.id, Jakarta, Indonesia

Abstract

Network routing that still uses two as numbers on the border gateway protocol, which allows the second as number to be a backup, which can be said to be ineffective. Moreover, the admin cannot know the backhoul network interference before monitoring a mass disturbance, so routing is switched manually. A Border Gateway Protocol is a path vector routing protocol that coordinates the routing of packets through multiple administrative domains by computing routes between every IP address the packet passes. Certain routers, called BGP speakers, are assigned to run the protocol. BGP speakers across different Autonomous Systems (AS) are interconnected in order to exchange routing information. BGP supports a feature called multihoming, which means connecting to multiple ISPs from different routers or points in the network. by using BGP one As Number, routing can choose the best or shortest path.

Keywords: network routing, BGP, autonomous, protocol

Abstrak

Pada *Network Routing* yang masih menggunakan dua *Autonomous System Number* pada *Border Gateway Protocol* yang memungkinkan *Autonomous System Number* kedua di jadikan *backup*, bisa dibilang tidak efektif. Terlebih lagi Admin tidak dapat mengetahui gangguan jaringan *backhoul* sebelum termonitor gangguan masal, sehingga *routing* dialihkan secara manual. *Border Gateway Protocol* adalah protokol jalur vektor yang mengkoordinasikan perutean paket melalui beberapa domain administratif dengan menghitung rute antara setiap alamat IP yang dilewati paket. *Router* tertentu, disebut *speaker BGP*, ditugaskan untuk menjalankan protokol. Dalam BGP, *Autonomous System* (AS) yang berbeda saling berhubungan untuk bertukar informasi *routing*. BGP mendukung fitur yang disebut *multihoming*, yang berarti menghubungkan ke beberapa ISP dari *router* atau titik yang berbeda dalam jaringan, dengan menggunakan BGP satu *Autonomous System Number*, routing bisa memilih jalur terbaik atau terpendek.

Kata Kunci: routing jaringan, BGP, autonomous, protokol

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

A. PENDAHULUAN

Dunia Perbankan saat ini membutuhkan informasi dan teknologi yang cepat dan tepat dalam menjalankan setiap transaksi nasabah yang sudah dapat dilakukan melalui *Internet Banking*, *Mobile Banking*, ATM, maupun langsung datang ke *Teller*/CS untuk menjalankan transaksi tersebut. Dalam menjalankan transaksi ini didukung oleh koneksi jaringan internet yang disediakan oleh masing-masing *Internet Service Provider* (ISP) yang bekerja sama dengan perbankan. Sehingga dengan adanya layanan internet dan perkembangan teknologi yang baik maka seluruh komponen transaksi akan berjalan dengan lancar.

Sebagaimana diketahui dengan perkembangan ilmu pengetahuan dan teknologi saat ini telah dikembangkan sistem yang dinamakan *Border Gateway Protocol* (BGP) yang berfungsi sebagai *switching* atau peralihan jaringan. Peralihan ini akan dilakukan jika pada jaringan utama mengalami gangguan.

BGP adalah protokol *routing* inti dari internet yg digunakan untuk melakukan pertukaran informasi *routing* antar jaringan. BGP bekerja dengan cara memetakan sebuah tabel IP *network* yang menunjuk ke jaringan yang dapat dicapai antar *Autonomous System (AS)* (Putra Yasa W, Rochim, & Christiyono, 2014). Menurut Paresmana (2009), *Border Gateway Protocol* (BGP) merupakan protokol *routing* standar yang bertujuan untuk memilih jalur *interdomain* yang berdasarkan pada *path vector* protokol. Fungsi utama BGP ini adalah mempertukarkan *network reachability* information antar *BGP router* dengan *router* BGP lain. *Autonomous System* merupakan suatu set *routing* dalam domain yang dikelola oleh satu otoritas sehingga pengaruhnya dapat langsung diketahui oleh *router* maupun *peer–router*. Dengan adanya informasi ini, dapat dibentuk grafik dari *AS path* yang saling terkoneksi sehingga dapat menghindari terjadinya *routing loop* (Nurhayati & Sulistianingsih, 2016).

Border Gateway Protocol (BGP) dapat diimplementasikan sebagai fungsi *switching routing* internet dari *main link* ke *backup link*. Dalam mengimplementasikan BGP ini, dibahas cara kerja BGP terhadap jaringan dalam mengatasi dan mengoptimalisasikan jaringan di dalam lingkungan perusahaan. Disamping itu juga dilakukan pembahasan peran utama BGP dalam jaringan internet, sehingga manfaat BGP berguna bagi kelancaran dan keamanan terhadap jaringan internet di perusahaan. Bagaimana merancang sistem dan mengimplementasikan BGP sebagai fungsi switching routing internet dari main link ke backup link. Ataupun load balance dari kedua ISP yang di gunakan dan jenis transmisinya.

Proses *routing* adalah suatu hal yang tidak bisa ditinggalkan oleh seorang admin jaringan. *Routing* merupakan teknik bagaimana menghubungkan komunikasi beberapa *router*. Sering ditemui seorang admin bingung dalam memilih jenis *routing* yang akan digunakan, karena masing masing *routing* memiliki kelebihan dan kekurangan. Parameter *packet loss* adalah salah satu kunci menentukan kinerja *routing* yang terbaik.

Kinerja sistem jaringan dengan menggunakan BGP lebih baik dibandingkan tanpa BGP. Perbandingan parameter rata-rata *latency* diperoleh nilai 0% (hampir tanpa *latency*) artinya kecepatan akses lebih cepat dibandingkan tanpa BGP, parameter *traceroute* (kontel lokal) 50% lebih baik dibandingkan tanpa BGP, namun untuk *traceroute* (kontel non lokal) memiliki nilai presentase yang sama hal ini dikarenakan seluruh *prefix* non lokal hanya didapatkan dari *port backbone* lama (Ernawati & Endrawan, 2018)

B. METODE PENELITIAN

Penelitian yang dilakukan dengan menggunakan metode penelitian eksperimental, berdasarkan pengalaman saat bekerja di PT. Bank Tabungan Pensiun Nasional dengan lokasi penelitian Jakarta. Pengumpulan data penelitian dilakukan dengan cara sebagai berikut:

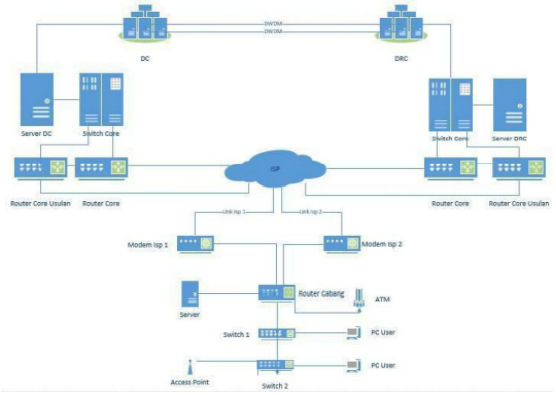
1. Metode Observasi dengan mengadakan observasi langsung di tempat penulis bekerja mulai 1 September hingga 30 Desember 2018, yang berkaitan langsung dengan monitoring lalu lintas data dari pusat ke cabang BTPN di seluruh Indonesia.
2. Metode Wawancara juga dilakukan untuk untuk menambah pengetahuan dan referensi dari pihak IT terkait untuk standart yang di gunakan.
3. Metode Studi Pustaka dilakukan dalam Pencarian langsung referensi terhadap landasan teori yang di gunakan selama eksperimen di Bank Tabungan Pensiun Nasional sebagai penunjang penelitian berkenaan dengan penelitian tentang *Border Gateway Protocol* (BGP) Menggunakan *Autonomous System* (AS).

C. HASIL DAN PEMBAHASAN

Topologi Jaringan

Topologi jaringan komputer adalah teknis, cara, dan aturan di dalam merangkai dan menghubungkan berbagai komputer dan perangkat terhubung lainnya ke dalam sebuah jaringan komputer, sehingga membentuk sebuah hubungan yang bersifat geometris (Pratama & Arief, 2015).

Pada penelitian ini, topologi jaringan menggunakan topologi yang sama, hanya mengusulkan untuk mengaktifkan 1 *router core* cadangan yang selama ini menjadi *backup* pada DC dan DRC untuk memisahkan 2 *provider* (Indosat dan Icon+) yang sering kali gangguan dan menyebabkan *flaping* sehingga mempengaruhi *link* lainnya, di hubungkan dengan IP *peer to peer* /30.



Gambar 1. Topologi Usulan

Router yang ada

```
JKT-MB-011DC-NR001-WM001#sh run int Gi0/1/1
Building configuration...

Current configuration : 231 bytes
!
interface GigabitEthernet0/1/1
 description LINK TO rO2-wm2-JKTMP
 ip address 10.1.127.245 255.255.255.252
```

Router Cadangan

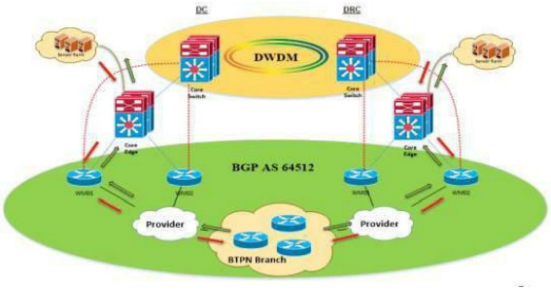
```
JKT-MB-011DC-NR002-WM002#sh run int Gi0/0/1
Building configuration...

Current configuration : 144 bytes
!
interface GigabitEthernet0/0/1
 description LINK to rO1-wm1-JKTMP
 ip address 10.1.127.246 255.255.255.252
```

Gambar 2. Konfigurasi *Peer to Peer Router Core*

Skema Jaringan

Pada skema jaringan, ada perubahan yang signifikan dan yang merupakan poin terpenting, yang sebelumnya menggunakan 2 *as number Border Gateway Protocol* yang di mana *as number* 64512 merupakan *main link* ke arah DC, mengusulkan untuk menghilangkan *as number backup* 64513 menjadi 64512 di DRC agar *load balance* ke ke dua *data center*.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

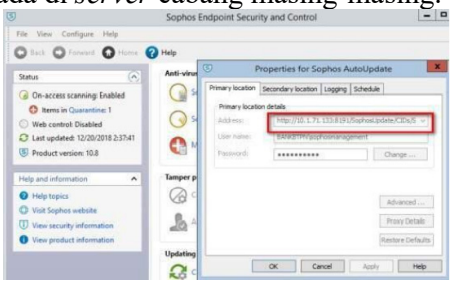


Gambar 3. Skema Usulan

Keamanan Jaringan

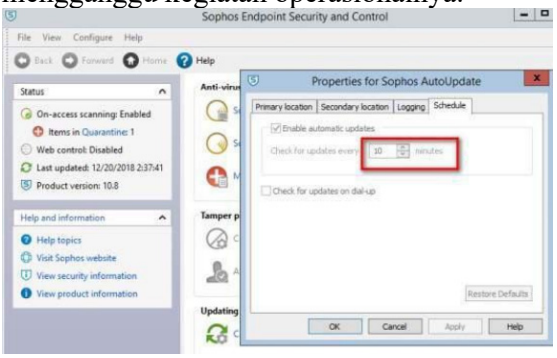
Menurut Internet Engineering Task Force (IETF), VPN merupakan suatu bentuk private internet yang melalui public network (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Prosedur enkripsi dilakukan terhadap data yang melalui VPN, sehingga keamanannya terjamin (Mulyadin, Sholeh, & Iswahyudi, 2016).

Di samping jaringan VPN sudah termasuk cukup aman untuk keamanan jaringan pada suatu jaringan yang cukup besar dan memiliki banyak *client*, di perlukan suatu mekanisme pengaturan jadwal *update* data manajemen *bandwidth*, di mana kendala *trafic full* sering terjadi saat jam-jam sibuk di karenakan suatu PC sedang update *windows* atau *antivirus*, disarankan untuk menggunakan *check point* pada satu PC di cabang yang kemudian PC *client* yang lain tinggal *update* di PC tersebut, sehingga tidak melakukan pemborosan *bandwidth* ke tiap-tiap PC. Dari gambar di bawah ini adalah *default check point* yang masih berada di *server*, *capture* ini disarankan hanya untuk *server* di cabang saja, untuk *client* lokasi *check point* nya berada di *server* cabang masing-masing.



Gambar 4. Check Point Anti Virus

Manajemen *bandwidth link* ke cabang ataupun *link* ke PC, untuk *update antivirus* nya di jadwalkan otomatis setiap hari pada jam setelah *office hour* agar tidak mengganggu kegiatan operasionalnya.



Gambar 5. Jadwal *Update* Anti Virus

Rancangan Aplikasi

Aplikasi yang digunakan untuk membandingkan konfigurasi usulan ini adalah dengan *secure* CRT untuk masuk ke CLI konfigurasi dari *router* yang nantinya dapat di lihat pada pengujian awal dan akhir, selain itu PRTG *traffic grapher* dan *ping ploter* juga digunakan untuk mengetahui *bandwidth* keluar masuk dan monitoring *availability link* serta *routing* per *hoop* bisa di ketahui.

Manajemen Jaringan

Menurut (Azza Roisatul, 2016) Manajemen Jaringan adalah suatu usaha untuk memelihara seluruh sumber jaringan dalam keadaan baik. Karena saat ini jaringan sangat kompleks, dinamika dan terdiri atas kompenen yang tidak dapat diandlkan, peralatan yang baik diperlukan untuk mengelola jaringan tersebut (Azzha, 2016).

Untuk manajemen jaringan merekomendasikan cabang yang memiliki lebih dari satu *link* untuk menggunakan *link* dengan berbeda jenis transmisi, seperti Metro – Mpls, Fiber Optik – tembaga – Radio, ataupun ditanyakan terlebih dahulu ke pada *provider* jalur mana yang di gunakan untuk meminimalisir gangguan

yang di sebabkan kerusakan di daerah tertentu secara bersamaan. Juga bisa menanyakan kepada *provider* apakah ada jalur *backup* ataupun kesepakatan lain bila *link* terlalu lama di perbaiki.

Pengujian Jaringan

Pada tahap pengujian jaringan, membandingkan proses pengujian pertama adalah sebelum di masukan rancangan usulan dengan sesudah rancangan usulan dengan *traceroute* guna mengetahui perbedaan *hoop* yang di lewati sebelum dan sesudahnya. Di uji langsung di jaringan BTPN yang aktif dengan mengambil beberapa contoh sample cabang yang berbeda dari sisi jenis transmisi, *bandwidth* dan perangkat yang di gunakan. Membedakan tampilan awal (*background* putih) dan tampilan usulan (*background* hitam).

Pengujian Awal

Awal Pengujian jaringan awal di mulai dengan konfigurasi *border gateway protocol* di sisi *router* cabang dan sisi *backhoul* dengan *as number* awal *backhou*l 64512 dan 64513, juga akan membahas *tunneling* untuk mengalokasikan *bandwidth* yang tersedian dengan membagi antara aplikasi *core banking* dan aplikasi *transaksional* lainnya.

Berikut beberapa *capture* pada tahap pengujian awal, membedakan tampilan awal (*background* putih) dan tampilan usulan (*background* hitam) :

a. Pengujian *border gateway protocol* dengan dua *as number*
   Capture di bawah ini menjelaskan *as number border gateway internal* di *router* 64534 dengan dua provider berbeda Indosat dan Telkom. Masih menggunakan dua *as number* yang berbeda 64512 dan 64513 untuk ke masing- masing *backhoul* nya.

```
r-0021-01#sh run | s router bgp
router bgp 64534
 bgp log-neighbor-changes
 network 10.66.134.0 mask 255.255.255.248
 network 10.66.134.127 mask 255.255.255.255
 network 10.66.134.128 mask 255.255.255.128
 network 10.66.201.0 mask 255.255.255.248
 network 10.66.201.8 mask 255.255.255.248
 network 10.66.201.64 mask 255.255.255.224
 network 10.66.201.127 mask 255.255.255.255
 network 10.66.201.128 mask 255.255.255.128
 neighbor 10.130.64.1 remote-as 64512
 neighbor 10.130.64.1 description "DC-ICON+-0021"
 neighbor 10.130.64.1 filter-list 2 out
 neighbor 10.130.64.2 remote-as 64513
 neighbor 10.130.64.2 description "DC-ICON+-0021"
 neighbor 10.130.64.2 filter-list 1 out
 neighbor 10.131.0.1 remote-as 64512
 neighbor 10.131.0.1 description "DC-INDOSAT-0021"
 neighbor 10.131.0.1 filter-list 2 out
 neighbor 10.131.0.2 remote-as 64513
 neighbor 10.131.0.2 description "DR-INDOSAT-0021"
 neighbor 10.131.0.2 filter-list 1 out
 maximum-paths 2
```

Gambar 6. *Capture* Konfiguasi BGP Cabang

Router BGP 64534 adalah *as number BGP* di cabang Madiun 0021, menggunakan dua *network* 10.66.134.0/24 dan 10.66.201.x/24 yang di *advertice* ke *as number BGP* DC (64512) dan *as number* DR (64513). Dalam configurasi BGP tersebut IP 60 *gateway* Indosat 10.131.0.1 dan 10.130.64.2 masih *remote* ke *as number BGP* DRC 64513.

```
neighbor 10.131.0.49 remote-as 64534
neighbor 10.131.0.49 peer-group INDOSAT
neighbor 10.131.0.49 description "DC-INDOSAT-0021"

neighbor 10.130.64.20 remote-as 64534
neighbor 10.130.64.20 peer-group ICON
neighbor 10.130.64.20 description "DR-ICON+-0021"
```

Gambar 7. *Capture* Konfigurasi BGP Backhoul

Konfigurasi BGP di sisi *backhoul* DC dan DRC, sama persis hanya beda deskripsinya saja. IP yang di gunakan di cabang 10.131.0.49 dan 10.130.64.20, *remote* langsung ke *as number BGP* yang ada di cabang 64534. kemudian melakukan *traceroute* untuk aplikasi yang berada di DRC aplikasi / *server* yang ada di DRC memiliki IP 10.2.x.x seperti yang sudah di jelaskan sebelumnya, masih melewati

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

backhoul DC terlebih dahulu kemudian ke DRC menggunakan *link* DWDM. 10.131.0.1 dan 10.130.64.1 merupakan *gateway* dari *provider* Indosat dan Icon+ yang berada di DC.

```
r-0021-01#traceroute 10.2.71.118
Type escape sequence to abort.
Tracing the route to 10.2.71.118
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.1 16 msec
    10.130.64.1 16 msec
    10.131.0.1 16 msec
  2 10.1.2.10 [AS 64512] 16 msec
    10.1.2.6 [AS 64512] 16 msec
    10.1.2.10 [AS 64512] 16 msec
  3 172.31.127.14 16 msec
    172.31.127.6 16 msec
    172.31.127.14 16 msec
  4 172.31.88.2 20 msec 20 msec 20 msec
  5 172.31.5.34 20 msec 20 msec 20 msec
  6 172.31.5.14 80 msec 20 msec 20 msec
```

Gambar 8. *Capture Traceroute Server* DRC

```
r-0021-01#traceroute 10.1.0.7
Type escape sequence to abort.
Tracing the route to 10.1.0.7
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.1 16 msec
    10.130.64.1 16 msec
    10.131.0.1 16 msec
  2 10.1.2.10 [AS 64512] 16 msec
    10.1.2.6 [AS 64512] 16 msec
    10.1.2.10 [AS 64512] 16 msec
  3 172.31.127.2 72 msec
    172.31.127.6 16 msec
    172.31.127.2 16 msec
  4 172.31.1.30 16 msec
    172.31.1.22 16 msec
    172.31.1.30 16 msec
  5 172.31.1.42 20 msec 20 msec 20 msec
  6 10.1.0.7 [AS 64512] 20 msec 20 msec 28 msec
```

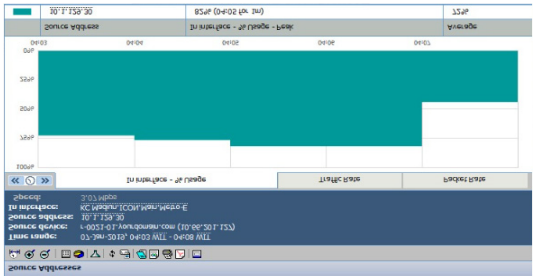
Gambar 9. *Capture Traceroute Server* DC

Bandingkan kedua *routing* di atas, saat akses Ke *server* yang berbeda *data center*, *gateway* nya tetap melewati DC.

```
r-0021-01#sh bgp sum
BGP router identifier 10.66.201.127, local AS number 64534
BGP table version is 62, main routing table version 62
17 network entries using 2516 bytes of memory
44 path entries using 2816 bytes of memory
7 multipath network entries and 14 multipath paths
15/5 BGP path/bestpath attribute entries using 2040 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
7 BGP filter-list cache entries using 112 bytes of memory
BGP using 7588 total bytes of memory
BGP activity 17/0 prefixes, 259/215 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.130.64.1     4        64512   45771   45766       62    0    0 4w0d            10
10.130.64.2     4        64513      10       6       60    0    0 00:00:20        8
10.131.0.1      4        64512    6009    6005       62    0    0 3d18h           10
10.131.0.2      4        64513       9       5       60    0    0 00:00:28        9
```

Gambar 10. *Capture* BGP Sum

b. Pengujian jaringan awal *tunneling*
Pengujian awal *tunneling* ini di khususkan untuk aplikasi *non core banking*, menggunakan *backup link* yang ada di cabang atau *persentase bandwidth* cabang yang di gunakan. Tidak ada konfigurasi sebelum di adakan *tuneling*, namun tetap mencoba *capture traceroute* dan *bandwidth* saat sebelum menggunakan *tunneling*.



Gambar 11. *Captrure Bandwidth* sebelum Penggunaan *Tunneling*

Sebelum menggunakan *tunnel*, aplikasi 10.1.129.30 (*server* DC) saat akses *traffic* hampir memenuhi *bandwidth* di cabang. Keuntungannya memang saat akses lebih cepat, namun saat akses aplikasi yang lebih *urgent* (aplikasi *core banking*) akan sangat terganggu bila di akses bersamaan.

```
r-0021-01#traceroute 10.1.129.30
Type escape sequence to abort.
Tracing the route to 10.1.129.30
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.1 16 msec
    10.130.64.1 16 msec
    10.131.0.1 16 msec
  2 10.1.2.10 [AS 64512] 16 msec
    10.1.2.6 [AS 64512] 16 msec
    10.1.2.10 [AS 64512] 16 msec
  3 10.1.134.1 [AS 64512] 16 msec 16 msec 20 msec
  4 10.1.128.2 [AS 64512] 20 msec 20 msec 16 msec
```

Gambar 12. *Capture Traceroute* sebelum Penggunaan *Tunnelling*

Dari *capture* di atas, sebelum penggunaan *tunneling*, *bandwidth* di dominasi beberapa menit oleh aplikasi *non core banking*. *Bandwidth* tersebut di peroleh saat mengirim dan menerima email, di sisi *routing* juga terlihat masih menggunakan *gateway* yang sama di DC 10.131.0.1 dan 10.130.64.1.

Pengujian Jaringan Akhir

Pada tahap pengujian jaringan akhir, akan memberikan beberapa konfigurasi

yang telah dicoba diterapkan untuk usulan pemecahan masalah tersebut. Konfigurasi pertama yang diubah adalah *as number border gateway protocol* yang berada di DRC dari 64513 ke 64512 (sama dengan *as number* di DC).

```
router bgp 64512
 bgp log-neighbor-changes
 network 10.1.0.0 mask 255.255.0.0
 network 10.2.0.0 mask 255.255.0.0
 network 10.5.0.0 mask 255.255.0.0
 network 10.64.0.0 mask 255.224.0.0
 network 10.66.197.104 mask 255.255.255.252
 network 10.107.0.176 mask 255.255.255.252
 network 172.67.0.16 mask 255.255.255.248
 network 172.68.0.16 mask 255.255.255.248
 network 192.168.32.0
 network 192.168.96.0
```

Gambar 13. *Captrure as number BGP* pada *Backhoul*

```
r-0021-01#sh run | s router bgp
router bgp 64534
 bgp log-neighbor-changes
 network 10.66.134.0 mask 255.255.255.248
 network 10.66.134.127 mask 255.255.255.255
 network 10.66.134.128 mask 255.255.255.128
 network 10.66.201.0 mask 255.255.255.248
 network 10.66.201.8 mask 255.255.255.248
 network 10.66.201.64 mask 255.255.255.224
 network 10.66.201.127 mask 255.255.255.255
 network 10.66.201.128 mask 255.255.255.128
 neighbor 10.130.64.1 remote-as 64512
 neighbor 10.130.64.1 description "DC-ICON+-0021"
 neighbor 10.130.64.1 filter-list 2 out
 neighbor 10.130.64.2 remote-as 64512
 neighbor 10.130.64.2 description "DC-ICON+-0021"
 neighbor 10.130.64.2 filter-list 1 out
 neighbor 10.131.0.1 remote-as 64512
 neighbor 10.131.0.1 description "DC-INDOSAT-0021"
 neighbor 10.131.0.1 filter-list 2 out
 neighbor 10.131.0.2 remote-as 64512
 neighbor 10.131.0.2 description "DR-INDOSAT-0021"
 neighbor 10.131.0.2 filter-list 1 out
 maximum-paths 2
```

Gambar 14. *Captrure as number BGP* pada Cabang

```
r-0021-01#sh bgp sum
BGP router identifier 10.66.201.127, local AS number 64534
BGP table version is 62, main routing table version 62
17 network entries using 2516 bytes of memory
44 path entries using 2816 bytes of memory
7 multipath network entries and 14 multipath paths
15/5 BGP path/bestpath attribute entries using 2040 bytes of memory
3 BGP AS-PATH entries using 104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7476 total bytes of memory
BGP activity 17/0 prefixes, 259/215 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.130.64.1     4        64512   45807   45803       62    0    0 4w0d            10
10.130.64.2     4        64512     401     311       62    0    0 00:33:43         8
10.131.0.1      4        64512    6046    6042       62    0    0 3d19h           10
10.131.0.2      4        64512      45      42       62    0    0 00:33:51         9
r-0021-01#
```

Gambar 15, *Capture BGP* Sum sesudah

Berikut hasil *traceroute* aplikasinya :

```
r-0021-01#traceroute 10.2.71.118
Type escape sequence to abort.
Tracing the route to 10.2.71.118
VRF info: (vrf in name/id, vrf out name/id)
  1 10.131.0.2 16 msec 16 msec 20 msec
  2 10.2.194.2 [AS 64512] 20 msec 20 msec 20 msec
  3 172.31.127.109 20 msec 20 msec 20 msec
  4 172.31.5.34 20 msec 20 msec 20 msec
  5 172.31.5.14 20 msec 20 msec 20 msec
```

Gambar 16. *Traceroute* Aplikasi DRC Sesudah

Dapat terlihat dari *routing* di bandingkan sebelumnya, *hoop* yang di lewati lebih sedikit, karena tidak melewati DC terlebih dahulu. 10.131.0.2 adalah *gateway* dari Indosat yang berada di DRC.

Untuk pengujian *tunneling* mencoba mengkonfigurasi di *link* Icon+ karena dari hasil *traceroute* aplikasi *core banking* 10.1.0.7 mendahulukan *link* Indosat.

```
r-0021-01#sh ip ro 10.1.0.7
Routing entry for 10.1.0.0/16
  Known via "bgp 64534", distance 20, metric 96
  Tag 64512, type external
  Last update from 10.130.64.1 12:40:14 ago
  Routing Descriptor Blocks:
  * 10.131.0.1, from 10.131.0.1, 12:40:14 ago
      Route metric is 96, traffic share count is 1
      AS Hops 1
      Route tag 64512
      MPLS label: none
    10.130.64.1, from 10.130.64.1, 12:40:14 ago
      Route metric is 96, traffic share count is 1
      AS Hops 1
      Route tag 64512
      MPLS label: none
```

Gambar 17. Menampilkan *Link* yang Lebih Dominan

```
interface Tunnel0
 description ***Tunnel madiun 0021**
 bandwidth 1024
 ip address 10.107.2.38 255.255.255.252
 ip mtu 1500
 ip flow ingress
 ip flow egress
 ip nat outside
 ip virtual-reassembly in
 tunnel source 10.130.64.20
 tunnel destination 10.130.64.1
end
```

Gambar 18. Konfigurasi *Tunneling* di Cabang

Kemudian *static* kan IP aplikasi yang akan di alihkan ke *tunnel* 0, berikut konfigurasinya :

```
r-0021-01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r-0021-01(config)#ip route 10.1.129.30 255.255.255.255 Tunnel0 name EMAIL_Zimbra_DC
r-0021-01(config)#
```

Gambar 19. Konfigurasi IP *Static* ke *Tunneling* di Cabang

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Untuk *tunneling* sama dengan BGP, konfigurasi di dua sisi Cabang dan *backhoul*, kali ini hanya menggunakan *backhoul* sisi DC karena IP yang di coba adalah IP DC dan menggunakan *link* Icon+ karena *link* Indosat lebih dominan, bukan karena indosat *mainlink*. Karena di sini metro – metro adalah *loadbalance*.

```
interface Tunnel21
 description ***KC_Madiun Tunnel madiun 0021***
 bandwidth 1024
 ip address 10.107.2.37 255.255.255.252
 ip mtu 1500
 ip flow ingress
 ip flow egress
 keepalive 3 10
 tunnel source 10.130.64.1
 tunnel destination 10.130.64.20
end
```

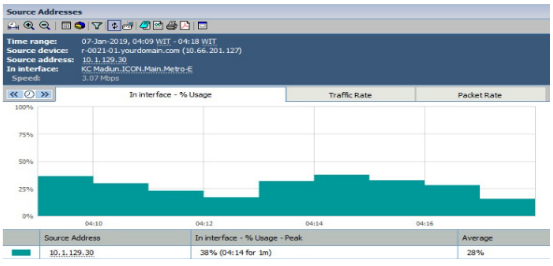
Gambar 20. Konfigurasi IP *Static* ke *Tunneling* di *Backhoul*

Berikut hasil dan bandingkan *traceroute* untuk IP aplikasi/*server* yang sudah di *static* kan ke *tunnel* :

```
r-0021-01#traceroute 10.1.129.30
Type escape sequence to abort.
Tracing the route to 10.1.129.30
VRF info: (vrf in name/id, vrf out name/id)
  1 10.107.2.37 20 msec
    10.107.15.5 20 msec
    10.107.2.37 20 msec
  2 10.1.2.6 [AS 64512] 20 msec
    10.1.2.10 [AS 64512] 20 msec
    10.1.2.6 [AS 64512] 20 msec
  3 10.1.134.1 [AS 64512] 20 msec 20 msec 20 msec
  4 10.1.128.2 [AS 64512] 20 msec 20 msec 20 msec
```

Gambar 21. Konfigurasi IP *Static* ke *Tunneling* di Cabang

Aplikasi *e-mail* 10.1.129.30 sudah melewati *tunnel*. Dan sementara *link* utama bebas dari *trafic* ip 10.1.129.30.



Gambar 22. *Netflow Trafic E-mail* sudah masuk ke Tunnel ke pusat (setelah pengujian)

D. PENUTUP

Hasil yang diperoleh setelah dilakukan analisa dan perancangan pembangunan jaringan komputer yang dibangun memberikan catatan penting dan kemungkinan perbaikan yang perlu dilakukan untuk pengembangan jaringan komputer selanjutnya.

Berdasarkan hasil riset pada PT. Bank Tabungan Pensiun Nasional (BTPN), menemukan beberapa permasalahan jaringan dan melakukan usulan jaringan dengan pengujian jaringan, yaitu :

1. Optimalisasi perangkat-perangkat jaringan di BTPN yang selama ini di jadikan cadangan, bisa di aktifkan sehingga routing menggunakan perangkat tersebut dan tidak membebani akses link DC – DRC.
2. Penggunaan BGP lebih disarankan karena saat BGP di nonkatifkan, pihak BTPN masih bisa memonitor link nya (saat intermitten).
3. Penggunakan BGP Load Balance DC – DRC dengan mengubah as number yang sama saat simulasi terbukti efektif mengurangi jalur routing.
4. Mengurangi traffic yang memenuhi bandwidth cabang dan link DC - DRC menggunakan tunneling berfungsi menjaga traffic tidak full untuk memberi bandwidth yang available untuk akses aplikasi core banking nya. Namun aplikasi yang di maksud menggunakan tunnel tidak dapat full akses bandwidth karena dibatasi bandwidth tunnel.
5. Gangguan yang di sebabkan provider, karena gangguan link ataupun flapping pada metro-E dengan cara provider masing-masing masih belum optimal, maka diusulkan untuk mengikuti dari Icon+ filtering mac address sebelum integrasi di perangkat jaringan BTPN.

E. DAFTAR PUSTAKA

Azzha, R. (2016). *Dasar Manajemen Jaringan dan Telekomunikasi*. Retrieved from Kompasiana: https://www.kompasiana.com/roisatulazza/5743de158c7e612207649eaa/dasar-manajemen-jaringan-dan-telekomunikasi

Ernawati, T., & Endrawan, J. (2018). Peningkatan Kinerja Jaringan Komputer dengan Border Gateway Protocol (BGP) dan Dynamic Routing (Studi Kasus PT Estiko Ramanda). *Khazanah Informatika, Vol.4 No.1*, 35-41.

Mulyadin, T., Sholeh, M., & Iswahyudi, C. (2016). Implementasi Routing Open Shortest Path First (OSPF) Melalui Tunnel Open VPN. *Jurnal JARKOM, vol. 4, no. 1*, 62-70.

Nurhayati, A., & Sulistianingsih, D. W. (2016). Simulasi Border Gateway Protocol (Bgp) Untuk Layanan Paket Data Menggunakan Simulator Gn3. *Jurnal ICT Penelitian Dan Penerapan Teknologi, 7(12)* , 12-23.

Pratama, A. P., & Arief, M. (2015). *Perancangan dan Analisis Desain Jaringan Wire dan Wireless dengan Pendekatan Green Network di Gedung Karang Fakultas Rekayasa Industri Universitas Telkom.* Bandung: Universitas Telkom.

Putra Yasa W, I. G., Rochim, A. F., & Christiyono, Y. (2014). Desain Dan Simulasi Internal Border Gateway Protocol (Ibgp) Menggunakan Graphical Network Simulator (Studi Kasus Pada Jaringan Universitas Diponegoro). *Transmisi, 16(1)*, 20-25.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

IMPLEMENTASI PCI-DSS UNTUK KEAMANAN DATA KARTU PEMBAYARAN PADA PT DHARMA LAUTAN NUSANTARA

Fahrizal[1)], Ade Surya Budiman[2)], Muhammad Rifqi Anuar[3)]
[1]Sistem Informasi, FTI, Universitas Bina Sarana Informatika
[2,3]Teknologi Informasi, FTI, Universitas Bina Sarana Informatika

Correspondence author: Fahrizal, fahrizal.fzl@bsi.ac.id, Jakarta, Indonesia

Abstract

The quality of service provided by the company must be maintained including providing transaction facilities using a secure credit card so that it can provide the best to customers and aims to increase the sense of trust in the company in making payments using credit cards. The method used to improve information security and corporate networks is to implement network security in accordance with the Payment Card Industry Data Security Standard (PCI-DSS) standard. The method used in this study is to identify data and communications that are the focus of security in compliance with PCI DSS, reduce the scope of security by implementing network segmentation by determining the classification of devices, communication lines and people into three categories based on the presence or absence of a relationship to data. credit cards, namely Cardholder Data Environment (CDE), Shared Network and Corporate Local Area Network. (LAN) Then manage the data communication traffic between the three segments according to compliance with the PCI DSS standard.

Keywords: PCI-DSS, VLAN, ACL'S, AAA, network security

Abstrak

Kualitas pelayanan yang diberikan perusahaan harus tetap dijaga diantaranya memberikan fasilitas bertransaksi menggunakan kartu kredit yang aman sehingga dapat memberikan yang terbaik kepada pelanggan dan bertujuan untuk meningkatkan rasa kepercayaan kepada perusahaan dalam melakukan pembayaran menggunakan kartu kredit. Cara yang diterapkan untuk meningkatkan keamanan informasi serta jaringan perusahaan yaitu dengan mengimplementasikan keamanan jaringan sesuai dengan standar *Payment Card Industry Data Security Standard* (PCI-DSS). Metode yang digunakan dalam penelitian ini yaitu dengan mengidentifikasi data dan komunikasi yang menjadi fokus pengamanan dalam kepatuhan terhadap PCI DSS, memperkecil ruang lingkup pengamanan dengan mengimplementasikan segmentasi jaringan dengan cara menentukan penggolongan perangkat, jalur komunikasi dan orang kedalam tiga kategori berdasarkan ada atau tidaknya hubungan terhadap data kartu kredit yaitu *Cardholder Data Environment* (CDE), *Shared Network* dan *Corporate Local Area Network* (LAN). Kemudian mengatur lalu lintas komunikasi data antar ketiga segmen tersebut sesuai kepatuhan terhadap standar PCI DSS.

Kata Kunci: PCI-DSS, VLAN, ACL'S, AAA, keamanan jaringan

A. PENDAHULUAN

Kartu kredit merupakan salah satu alat pembayaran yang banyak digunakan karena kemudahan kenyamanan dan kecepatan yang ditawarkan pada setiap transaksinya. Berdasarkan data Bank Indonesia penggunaan kartu kredit periode September 2021 tercatat mengalami kenaikan sebesar 13,07%. Namun penggunaan kartu kredit memiliki risiko keamanan karena rentan terhadap pencurian data yang utamanya pencurian terhadap uang pemilik kartu kredit yang saat ini dikenal dengan istilah *carder*. *Carding* adalah bentuk kejahatan menggunakan nomor kartu kredit orang lain untuk dibelanjakan (*non face to face transaction*) tanpa sepengetahuan pemiliknya yang sah. Transaksi lazimnya dilakukan secara elektronik. Pelaku kejahatan kartu kredit atau *carder* memperoleh data kartu kredit dengan beberapa cara yaitu dengan rekayasa sosial atau *social engineering* yaitu dengan cara berpura-pura sebagai Bank penerbit kartu kredit *(acquirer*) menghubungi pemegang kartu melalui telepon, email dan sebagainya dengan alasan mengadakan undian atau memerintahkan nasabah untuk segera mengganti kartu kreditnya hingga nasabah tersebut percaya dan memberikan informasi data kartu kreditnya. Atau juga dengan menggunakan teknologi informasi yang rentan dilakukan oleh oknum yang memiliki akses ke komputer dan perangkat jaringan yang melakukan pencatatan *(create)*, pemprosesan *(process)*, penyimpan *(save)*, mentransmisikan (*transmit*) dan menerima (*receive)* yang dalam standar Payment Card Industry (PCI) Data Security Standard (DSS) perangkat-perangkat tersebut masuk dalam lingkup *Cardholder Data Environment* (CDE). Atau juga oknum yang memiliki akses ke perangkat yang dapat berkomunikasi tanpa pembatasan dan pencatatan (log) ke perangkat-perangkat CDE. Tindakan kejahatan tersebut dapat dilakukan oleh orang yang bekerja di perusahaan yang menerima pembayaran menggunakan kartu kredit yang oleh standar PCI DSS disebut *merchant.* Karena itulah PCI Security Standards Council's (SSC) yang terdiri atas *brand* American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Inc. dan Visa Europe mensyaratkan standar kepatuhan bagi setiap *acquirer*, *merchant* dan setiap organisasi baik itu besar maupun kecil yang menerima, mentransmisikan, atau menyimpan data pemegang kartu/ *Card Holder Data* (CHD) apapun yang termasuk dalam SSC, untuk mengimplementasikan standar yang disebut sebagai PCI DSS.

PT Dharma Lautan Nusantara sebagai *merchant* yang mengutamakan kualitas layanan terhadap pelanggan dengan cara mengimplementasikan PCI DSS untuk memberikan rasa aman ketika bertransaksi atau melakukan pembayaran menggunakan kartu kredit dengan melakukan pembenahan dari sisi jaringan komputer yang aman sesuai rekomendasi dari persyaratan / *requirement* PCI DSS. Dalam tulisan ini akan dibahas tentang *requirement* yang dipersyaratkan PCI DSS bagi merchant dalam menyediakan keamanan data dalam bertransaksi menggunakan kartu kredit. Dalam tulisan ini untuk membentuk sistem jaringan komputer yang *secure.*

Maksud dalam tulisan ini dapat dirumuskan sebagai berikut :

1. Bagaimana memperkecil ruang lingkup pengamanan data pada jaringan PT Dharma Lautan Nusantara.
2. Bagaimana meningkatkan keamanan lalu lintas data pada jaringan PT Dharma Lautan Nusantara.
3. Bagaimana mengimplementasikan keamanan data pada jaringan PT Dharma Lautan Nusantara sesuai dengan persyaratan standar PCI-DSS.

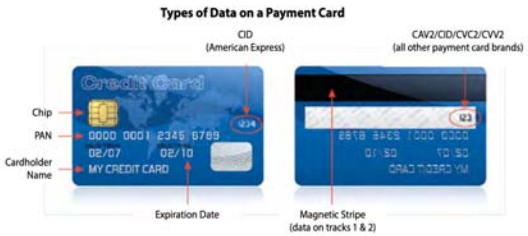
Penelitian ini memperoleh referensi dari standar PCI DSS dan beberapa publikasi dokumen dan jurnal yang terkait yaitu:

1. *PCI DSS Quick Reference Guide Understanding the Payment Card Industry*

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Data Security Standard version 3.2.1, yang diterbitkan oleh PCI SSC. Dalam publikasi tersebut dijelaskan tentang pengertian PCI DSS, Card Holder Data yang menjadi object data yang harus dilindungi seperti pada gambar 1 yaitu:

a. Informasi data yang terdapat pada Chip kartu
b. *Primary Account Number* (PAN)
c. Nama pemegang kartu
d. Tanggal berlaku kartu
e. *Credit Card Identification Code* (CID)
f. Informasi pada *magnetic stripe* dan
g. Tiga angka di belakang kartu (CAV2/CID/CVC2/CVV2)



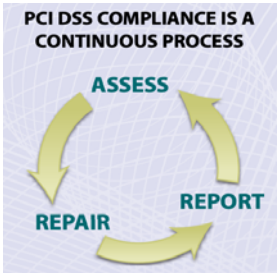
Gambar 1. *Cardholder Data* atau Tipe Data pada Kartu Pembayaran

Pada dokumentasi ini juga dijelaskan 12 *requirement* seperti pada table 1dibawah ini

Tabel 1. Requirement PCI-DSS

Goal	PCI DSS Requirement
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti- virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Pada dokementasi tersebut juga terdapat informasi framework yang digunakan oleh PCI DSS yang diperlihatkan pada gambar 2 di bawah ini.



Gambar 2 . Framework PCI DSS

2. Informasi suplemen yang diterbitkan oleh PCI SSC dengan judul *"Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation"*. Dalam publikasi ini dijelaskan tentang *requirement* dan rekomendasi dari PCI DSS untuk *merchant* dalam mengimplementasi standar keamanan data dengan mengidentifikasi data yang harus diamankan, memperkecil scope pengamanan dengan segmentasi jaringan dan mengatur alur komunikasi dari dan

ke segmen *CDE* yang menjadi fokus pengamanan.

3. *PCI DSS Compliance IT Checklist* yang diterbitkan oleh security matriks. berisi daftar 12 *requirement* PCI DSS yang harus dipenuhi oleh pengelola sistem Teknologi Informasi (TI).
4. Jurnal yang berjudul "Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5" yang ditulis oleh Bagus Puji Santoso, Eva Hariyanti dan Eto Wuryanto. Dalam jurnal ini dibahas tentang bagaimana membuat panduan tata kelola keamanan informasi untuk konfigurasi firewall yang sesuai dengan kerangka kerja PCI DSS v.3.1 dan COBIT 5 dimana penyusunan panduan tersebut dilakukan dalam tiga tahap yaitu Tahap pertama adalah penyusunan prosedur pengelolaan keamanan informasi untuk firewall configuration yang terdiri dari tahap analisis pemetaan proses, tahap penyusunan prosedur dan tahap penentuan peran dan deskripsi kerja. Tahap kedua adalah tahap verifikasi panduan yang dilakukan melalui pemberian kuesioner penilaian. Tahap ketiga adalah tahap perbaikan panduan.
5. Buku *Cisco PCI Solution for Retail 2.0 Design and Implementation Guide* yang disusun oleh Christian Janoff dan Bart McGlothin yang berisi *guide*/ petunjuk untuk implementasi jaringan komputer menggunakan perangkat Cisco untuk solusi berbagai bisnis retail 2.0 untuk perusahaan kecil hingga besar.

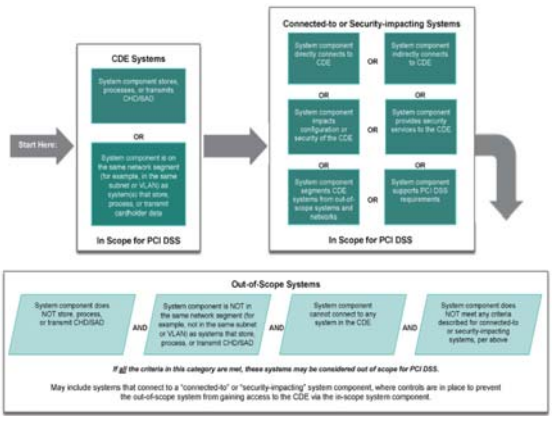
B. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu metode penelitian implementasi (*Implementation Research*) dengan sistem yang diimplementasi yaitu standar PCI DSS untuk menerapkan keamanan data. Ruang lingkup dari standar PCI DSS yaitu berlaku untuk semua komponen sistem yang disertakan atau terhubung ke lingkungan data pemegang kartu atau disebut dengan *Cardholder Data Environment* (CDE). Lingkungan data pemegang kartu (CDE) terdiri dari orang, proses, dan teknologi yang menyimpan, memproses, atau mengirimkan data pemegang kartu yang disebut sebagai *Cardholder Data* (CHD) atau juga termasuk data otentikasi yang bersifat sensitif yang disebut *Sensitive Authentication Data* (SAD).

Agar sesuai dengan framework standar PCI DSS penulis menggunakan tahapan proses sebagai berikut yaitu.

Assess

Mengidentifikasi semua lokasi data CHD/SAD, menginventarisasi asset TI dan proses bisnis untuk pemrosesan kartu pembayaran dan menganalisis kerentanan yang dapat mengekspos data pemegang kartu. Untuk mengidentifikasi berbagai perangkat yang termasuk dalam ruang lingkup standar digunakan diagram kategori scope pada gambar 3.



Gambar 3. Penentuan kategori dalam Ruang lingkup PCI DSS

Gambar 3 memperlihatkan bagaimana komponen sistem dapat dikategorikan menggunakan tiga pertanyaan dibawah ini :

1. Apakah terdapat data akun *Cardholder Data* (CHD) / *Sensitive Authentication Data* (SAD)) yang disimpan, diproses, atau dikirim pada komponen itu ?

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

2. Apakah terdapat konektivitas antara komponen tersebut dengan sistem dan *Cardholder Data Environment* (CDE) / SAD ?
3. Apakah komponen tersebut sistem dapat mempengaruhi keamanan pada *Cardholder Data Environment* (CDE) ?

Untuk identifikasi yang lebih lengkap dilakukan audit perangkat dengan menggunakan matriks tabel 2 dibawah ini.

Tabel 2. kategori pelingkupan PCI-DSS

Sistem Tipe	Deskripsi	Ruang Lingkup dan Penerapan
CDE Sistem	1. Komponen system menyimpan, memproses atau mengirimkan CHD/SAD. Atau 2. Komponen system berada di segmen jaringan yang sama, misalnya dalam satu subnet atau dalam satu VLAN yang sama dengan system yang menyimpan, memproses dan mengirim CHD / SAD.	Sistem ini ● Berada dalam ruang lingkup untuk PCI DSS ● Harus dievaluasi terhadap semua persyaratan PCI DSS untuk menentukan penerapan setiap persyaratan.
Terhubung kepada dan/atau berdampak pada sistem keamanan	1. Komponen system yang berada pada jaringan yang berbeda (atau subnet atau VLAN), tetapi dapat terhubung ke atau mengakses CDE (misal melalui konektivitas jaringan internal) Atau 2. Komponen system yang dapat terhubung ke atau mengakses CDE melalui system lain – misalnya, melalui server lompat yang menyediakan akses ke CDE. Atau 3. Komponen sistem dapat mempengaruhi konfigurasi atau keamanan CDE, atau cara penanganan CHD / SAD -- misalnya, server pengalihan web atau server resolusi nama. Atau 4. Komponen sistem menyediakan layanan keamanan untuk CDE -- misalnya, pemfilteran lalu lintas jaringan, distribusi patch, atau manajemen otentikasi. Atau 5. Komponen system mendukung persyaratan PCI DSS seperti server waktu dan server penyimpanan log audit. Atau 6. Komponen sistem menyediakan segmentasi CDE dari sistem dan jaringan di luar cakupan -- misalnya, firewall yang dikonfigurasi untuk memblokir lalu lintas dari jaringan yang tidak terpercaya.	Sistem ini: ● Berada dalam ruang lingkup untuk PCI DSS. Meskipun koneksi terbatas pada port atau layanan tertentu pada sistem tertentu, sistem tersebut termasuk dalam cakupan untuk memverifikasi bahwa kontrol keamanan yang berlaku sudah diterapkan. ● Harus dievaluasi terhadap sebuah persyaratan PCI DSS untuk menentukan penerapan setiap persyaratan. ● Tidak boleh menyediakan jalur akses terhadap sistem CDE dan sistem di luar cakupan.
Diluar lingkup/*Out of Scope*	Komponen system yang tidak termasuk kategori A dan B	Sistem ini harus dipisahkan dari system CDE dan tidak boleh ada komunikasi dari dan ke CDE.

Repair

Memperbaiki kerentanan yang teridentifikasi, menghapus CHD/SAD yang

tidak perlu dengan aman, dan menerapkan proses bisnis yang aman. Jika salah satu atau lebih pernyataan pada tabel 1 diatas benar maka perangkat tersebut termasuk dalam ruang lingkup standar PCI DSS, dan wajib diterapkan sesuai dengan rekomendasi yang ada pada table 1 kolom ruang lingkup dan penerapan. Berdasarkan table 1, kategori perlingkupan PCI-DSS mencakup sistem yang terhubung ke dan yang berdampak pada keamanan. Kategori ini mengambil prioritas dan dievaluasi sebelum kategori sistem di luar cakupan dipertimbangkan. Untuk dipertimbangkan di luar ruang lingkup, sistem harus memenuhi semua kriteria kategori di luar cakupan dan tidak ada kriteria kategori yang lebih tinggi.

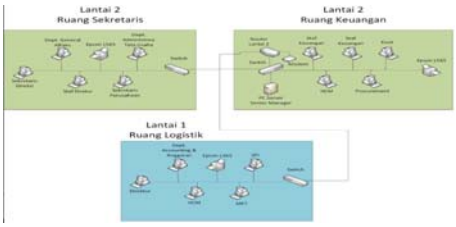
Report

Mendokumentasikan penilaian dan rincian perbaikan, dan mengirimkan laporan kepatuhan ke bank yang mengakuisisi dan merek kartu yang berbisnis dengan perusahaan. Pada tahap ini hanya dilakukan sampai mendokumentasikan penilaian, rincian perbaikan dan melakukan pengetesan konfigurasi jaringan, namun tidak mengirimkan laporan kepatuhan untuk sertifikasi PCI DSS.

C. HASIL DAN PEMBAHASAN

Kondisi Jaringan yang Ada (Existing Network)

Skema jaringan yang diperlihatkan pada gambar 4 merupakan skema jaringan yang disederhanakan dan alamat IP dari setiap perangkat juga tidak penulis perlihatkan untuk menjaga kerahasiaan perusahaan. Penggunaan alamat IP dalam penelitian ini tidak menggunakan alamat IP yang sebenarnya akan diimplementasikan karena bersifat rahasia dan untuk menjaga keamanan informasi perusahaan.



Gambar 4. Skema Jaringan Awal

Berdasarkan wawancara dari bagian departemen Teknologi Informasi dan pengamatan dari skema jaringan pada object penelitian, penggunaan alamat IP pada setiap perangkat masih menggunakan satu jaringan atau satu subnet saja, tidak ada pembatasan antara departemen atau antar lantai sehingga perlu perbaikan dari sisi disegmentasi jaringan dengan menerapkan virtual local area network (VLAN).

Berdasarkan wawancara dan dokumen prosedur perusahaan didapatkan proses bisnis yang berhubungan dengan Cardholder Data secara langsung yang ada di perusahaan terdapat pada bagian kasir, komputer kasir yang berada di lantai II ruang keuangan berfungsi sebagai tempat pembayaran para pelanggan dan pegawai. Alat pembayaran yang digunakan merupakan mesin *Electronic Data Capture* (EDC) yang berfungsi untuk pembayaran transaksi non tunai, baik dengan kartu kredit maupun kartu debit. Komputer kasir juga terhubung dengan server yang menyediakan sistem *Point of Sales* (POS) yang bertujuan untuk meningkatkan keamanan data sekaligus mengurangi risiko kehilangan data pada kasir walaupun hanya merecord data nama pelanggan dan transaksi yang dilakukan. Berdasarkan hal tersebut dapat disimpulkan mesin EDC yang ada di kasir termasuk dalam lingkup *Cardholder Data Environment* (CDE) karena terdapat kegiatan memproses dan mengirimkan Cardholder data (CHD) yang dapat memproses, memyimpan, dan mengirimkan data pemegang kartu atau data otentikasi pembayaran yang sensitif.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Secara fungsi proses bisnis dan keterlibatan setiap perangkat dengan CHD dan SAD diperlihatkan pada table 3 berikut.

Tabel 3 Tabel Kategori Perangkat Existing

No	Nama Komputer	Keterlibatan dengan CHD	Keterangan berdasar Tabel 1
1	Departement accounting dan anggaran	Tidak ada	Kategori C
2	Direktur	Tidak ada	Kategori C
3	Human Capital Management (HCM)	Tidak ada	Kategori C
4	MKT	Tidak ada	Kategori C
5	SPI	Tidak ada	Kategori C
6	Sekretaris Direksi	Tidak ada	Kategori C
7	Departemen General Affairs	Tidak ada	Kategori C
8	Staff Direksi	Tidak ada	Kategori C
9	Sekretaris Perusahaan	Tidak ada	Kategori C
10	Departemen Administrasi Tata Usaha	Tidak ada	Kategori C
11	Staff Keuangan 1	Ada	kategori A2
12	Staff Keuangan 2	Ada	kategori A2
13	Kasir	Ada	kategori A1
14	PC Server Senior Manager	Ada	kategori A2
15	HCM	Tidak ada	Kategori C
16	Procurement	Tidak ada	Kategori C
17	Router	Ada	kategori A1
18	Modem	Ada	kategori A1
19	Switch Lantai 1	Tidak ada	Kategori C
20	Switch Lantai 2	Ada	ketegori A1
21	Komputer Tim IT	Ada	kategori B

Berdasarkan wawancara dari tim IT didapatkan kesesuaian sistem jaringan komputer saat ini dengan 12 *requirement* yaitu:

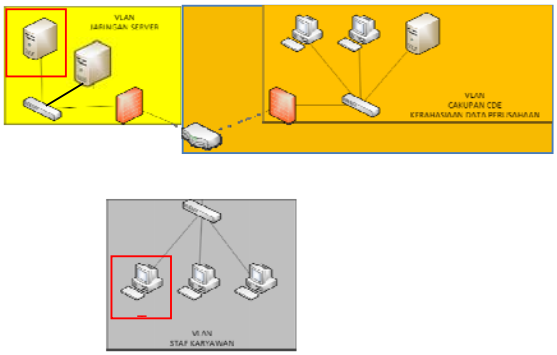
1. Telah terdapat sistem *firewall* pada setiap diperangkat komputer dan router, sehingga hanya karyawan yang diberi izin yang dapat mengakses setiap komputer masing-masing. Hal ini sesuai dengan *requirement* 1 dan 8 PCI DSS.
2. Setiap perangkat yang ada telah diterapkan password yang harus dirubah secara berkala. Hal ini sesuai dengan *requirement* ke 2, 6 dan 12 PCI DSS.
3. Transaksi yang langsung menggunakan kartu hanya dilakukan pada mesin EDC tang telah memiliki fasiltas *Point to Point Encryption*. Hal ini sesuai dengan *requirement* PCI DSS nomer 3 dan 4.
4. Telah terdapat *software antivirus* pada setiap komputer dan diupdate secara berkala. Hal ini sesuai dengan *requirement* PCI DSS nomer 5
5. *Swipe* kartu pembayaran hanya dilakukan 1 kali yaitu pada mesin EDC. Hal ini sesuai dengan *requirement* PCI DSS nomer 7
6. Pada object penelitian telah terdapat pembatasan secara fisik ke perangkat jaringan. Hal ini sesuai dengan *requirement* PCI DSS nomer 9
7. Pada aplikasi perusahaan yang menghubungkan komputer yang terindikasi sebagai CDE dengan server yang tidak terindikasi sebagai CDE telah menerapkan komunikasi yang terenkripsi. Hal ini sesuai dengan *requirement* PCI DSS nomer 4

Berdasarkan infrastruktur yang ada dan proses bisnis perusahaan yang berhubungan dengan CHD/SAD dan sepatuhan terhadap standar PCI DSS didapatkan prioritas gap sebagai berikut.

1. Tidak adanya pemisahan atau segmentasi jaringan terhadap perangkat yang termasuk dalam CDE firewall hanya menahan kemungkinan serangan dari luar perusahaan. Hal ini belum sesuai dengan requirement PCI DSS nomer 1 dan 3,
2. Tidak adanya pembatasan akses komunikasi antar perangkat terutama akses dari dan ke perangkat CDE. Hal ini belum sesuai dengan requirement PCI DSS nomer 1 dan 3,
3. Tidak adanya sistem pencatatan akses/log yang dibuat dari perangkat komputer tim IT ke system CDE. Hal ini

belum sesuai dengan requirement PCI DSS nomer 1 dan 3,

Untuk memperkecil ruang lingkup keamanan data CHD/SAD sekaligus memperkecil area CDE maka diterapkan segmentasi jaringan dengan membagi jaringan menjadi tiga segmen dengan sistem *subnetting* jaringan.



Gambar 5. Skema Jaringan Usulan

Dalam skema jaringan usulan selain membagi jaringan menjadi 3 kelompok subnet yaitu

1. Area CDE
   Area ini terdiri atas perangkat komputer dan jaringan yang terindikasi berhubungan dengan CHD dan SDA yang tidak dapat dilakukan eliminasi karena kebutuhan pada proses bisnis perusahaan. Setiap komputer pada area ini memiliki sistem autentikasi yang ketat, penggunaannya hanya berhubungan dengan *Point of Sales* dan diaudit secara berkala.
2. Area jaringan Server (*Shared*)
   Area ini terdiri atas komputer server-server perusahaan yang salah satunya terkoneksi dengan server PoS yang berada di Area CDE. Area ini juga dikenal sebagai area *De Military Zone* (DMZ) karena diakses juga oleh Area Staff Karyawan yang merupakan diluar Scope PCI DSS.
3. Area Staff Karyawan (Corporate LAN)
   Pada Area ini berisi berbagai perangkat yang telah terindikasi tidak berhubungan dengan system CDE kecuali komputer khusus untuk keperluan *remote maintenance* ke dalam sistem CDE via server *Authentication, Authorization, Accounting* (AAA) yang disediakan untuk tim IT.

Konfigurasi pada Switch

Pada switch diterapkan 3 VLAN yang akan diisi dengan ketiga jaringan subnet pada penjelasan sebelumnya. Pada switch juga menerapkan port security dengan mengidentifikasi setiap MAC address yang terhubung terutama pada port VLAN terutama untuk jaringan CDE dan jaringan server(Shared).

```
Switch CDE
Switch>en
Switch#
Switch(vlan)#vlan 10 name CDE
VLAN 10 added:
Name: CDE
Switch(vlan)#vlan 20 name Shared
VLAN 20 added:
Name: Shared
Switch(vlan)#vlan 30 name corp
VLAN 30 added:
Name: corp
Switch(vlan)#ex
Switch#conf t
Switch(config)#int range fa0/1-3
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 10
Switch(config-if-range)#int range fa0/4-22
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 30
Switch(config-if-range)#int range fa0/23-24
Switch(config-if-range)#switchport mode
access
Switch(config-if-range)#switchport access
vlan 20
Switch(config-if-range)#int range gig0/0-1
```

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

```
interface range not validated - command
rejected
Switch(config)#int gig0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0060.3E81.EAC7
Found duplicate mac-address
0060.3e81.eac7.
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0090.2BAD.39A8
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 00D0.D344.8D67
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#

Switch(config)#int fa0/23
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0005.5E4D.1E3A
Switch(config-if)#switch port-security
violation protect
Switch(config-if)#int fa0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security mac-
address 0001.9739.0209
Switch(config-if)#switch port-security
violation protect
```

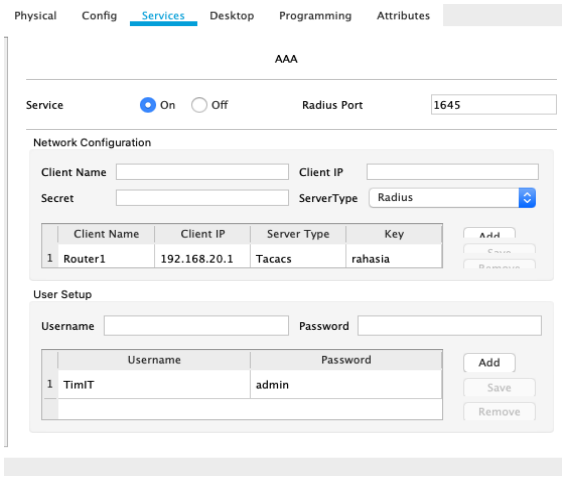
Konfigurasi Router

```
Router#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#no sh
Router(config-if)#ip add 192.168.10.1
255.255.255.0
Router(config-if)#int gig0/1
Router(config-if)#no sh
Router(config-if)#ip add 192.168.20.1
255.255.255.0
Router(config-if)#int gig0/2
Router(config-if)#no sh
Router(config-if)#ip add 192.168.30.1
255.255.255.0
Router(config-if)#exit
```

Konfigurasi ACL's

```
Router(config)#access-list 1 deny
192.168.30.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#int gig0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#ex
Router(config)#access-list 2 deny
192.168.10.0 0.0.0.255
Router(config)#access-list 2 permit any
Router(config)#int gig0/2
Router(config-if)#ip access-group 2 out
Router(config-if)#ex
```

Konfigurasi server AAA dengan TACACS+



Gambar 6. Konfigurasi TACACS+ di Server AAA

Konfigurasi pada Router

```
Router1#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router1(config)#aaa new-model
Router1(config)#aaa authentication login
default local
Router1(config)#username admin password
admin
Router1(config)#username timIT password
admin
Router1(config)#aaa authentication login
AAA-SERVER group tacacs+ local
Router1(config)#line console 0
Router1(config-line)#login authentication
AAA-SERVER
Router1(config-line)#exit
Router1(config)#tacacs-server host
192.168.20.2
Router1(config)#tacacs key rahasia
Router1(config)#ex
Router1#
%SYS-5-CONFIG_I: Configured from
console by console
Router1#debug aaa authentication
AAA Authentication debugging is on
Router1#exit
```

Pengujian Jaringan

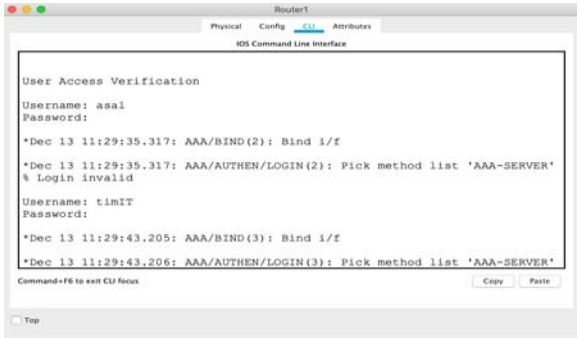
Pengujian jaringan dilakukan dengan menggunakan simulasi packet tracer yang mempresentasikan lingkungan jaringan yang telah diusulkan.

1. Pengujian port security
   Pada pengujian ini dilakukan penggantian port yang terhubung dengan komputer CDE dengan komputer yang mac addressnya tidak terdaftar di switch di jaringan CDE. hasilnya komputer yang mac addressnya tidak terdaftar tersebut tidak dapat ping ke jaringan walaupun ip addressnya disamakan dengan Ip address di network CDE.
2. Pengujian ACLS
   Pengujian dilakukan dengan test ping dari komputer yang terhubung ke corporate LAN ke jaringan CDE dan sebaliknya. Hasil pengujian didapatkan tidak ada paket ping yang Kembali atau request timed out. dan dicek ke router dengan perintah show access-list

```
Router1#show access-list
Standard IP access list 1
10 deny 192.168.30.0 0.0.0.255 (5
match(es))
20 permit any (2 match(es))
Standard IP access list 2
10 deny 192.168.10.0 0.0.0.255 (2
match(es))
20 permit any (1 match(es))
```

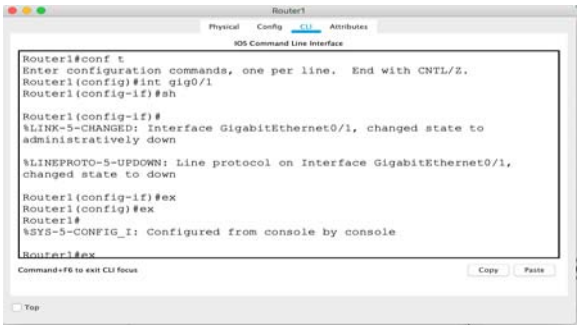
   Artinya router berhasil menahan koneksi dari CDE ke corporate LAN dan sebaliknya. Sedangkan koneksi ke jaringan server/ shared network bisa dilakukan.
3. Pengujian TACACS+
   Pengujian akses ke router dengan konfigurasi TACACS+ seperti lampiran gambar di bawah ini

Gambar 7. Login Router dengan otentikasi yang benar

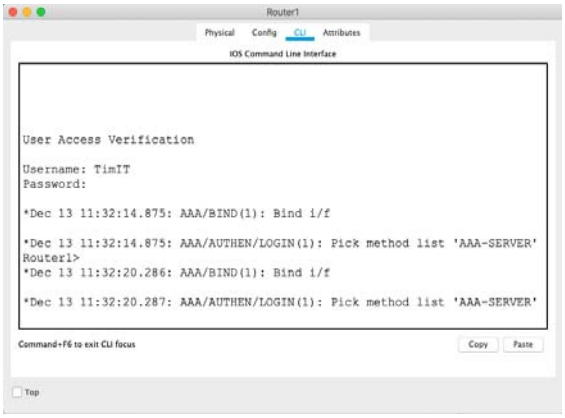


JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

Gambar 8 Login Router dengan otentikasi yang salah

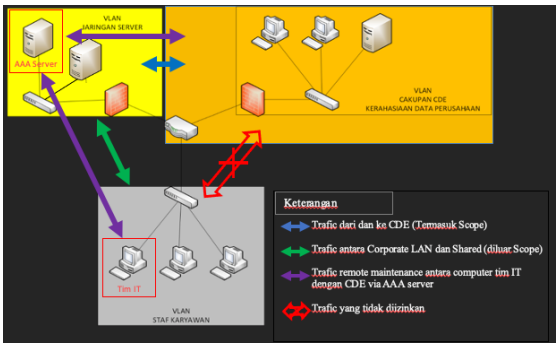


Gambar 9 mematikan koneksi ke AAA server



Gambar 10 login router ketika koneksi ke AAA server terputus

Dengan begitu untuk konfigurasi router, Tim IT wajib terverifikasi melalui AAA server. Gambar 11 berikut merupakan skematik diagram komunikasi hasil tes konfigurasi dan telah sesuai dengan dokumen PCI DSS *Scouping* and *Network Segmentation*.



Gambar 11. Skema hasil tes komunikasi antar jaringan

D. PENUTUP

Berdasarkan hasil penelitian dan pengujian Implementasi Keamanan Jaringan Berdasarkan Standar PCI-DSS yang telah dilakukan, maka dapat diambil kesimpulan yaitu :

1. Menerapkan Access Control List (ACL) untuk mengontrol setiap client yang ingin berinteraksi dengan client lain yang sangat dijaga kerahasiaan datanya.
2. Menerapkan segmentasi jaringan VLAN dan port security untuk memperkecil cakupan jaringan.
3. Menerapkan TACACS+ dapat digunakan untuk menyediakan remote maintenance yang terauthentikasi dan aman.
4. Dengan menerapkan keamanan jaringan berstandar PCI-DSS dapat mengurangi risiko pelanggaran keamanan data dalam bertransaksi menggunakan kartu pembayaran.

Saran untuk penelitian lanjut yaitu perlu diadakan penelitian untuk penetration testing berdasarkan standar PCI-DSS untuk lebih mengetahui tingkat keamanan jaringannya. Pada penelitian ini juga belum sampai pada tingkat pelaporan/ report untuk mendapatkan pengakuan dan sertifikat dari PCI SSC bahwa perusahaan telah menerapkan standar kepatuhan PCI DSS.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada PT Dharma Lautan Nusantara yang telah memberi kesempatan untuk melakukan penelitian.

E. DAFTAR PUSTAKA

Checklists, I. T. (2019). *PCI DSS COMPLIANCE REQUIREMENT 01*.

Dihni, vika A. (2021). Nilai Transaksi Kartu Kredit Naik 13,07% pada Agustus 2021.

Databoks.Katadata.Co.Id, *September*, 2021.

Janoff, C., Architect, V. S., Ise, C. M. O., & Systems, C. (2011). *Cisco PCI Solution for Retail 2 . 0 Design and Implementation Guide*.

Panjaitan, L. T. (2017). Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang- Undang Informasi dan Transaksi Elektronik no.11 Tahun 2008. *Jurnal Telekomunikasi Dan Komputer*, *3*(1), 1. https://doi.org/10.22441/incomtech.v3i1.1111

PCI Security Standards Council. (2017). *Information Supplement : Guidance for PCI DSS Scoping and Network Segmentation*. *December*, 26.

PCI SSC. (2018). PCI DSS Quick Reference Guide 3.2.1. *PCI Security Standard Documents*, 1–40. *https://www.pcisecuritystandards.org/security_standards/documents.php*

Santoso, B. P., Hariyanti, E., & Wuryanto, E. (2016). Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5. *Journal of Information Systems Engineering and Business Intelligence*, *2*(2), 67. Available at: *https://doi.org/10.20473/jisebi.2.2.67-73*

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

PENERAPAN METODE *VIRTUAL ROUTER REDUNDANCY PROTOCOL* (VRRP) PADA YAYASAN MASJID AL IKHLAS

Usanto S[1)], Lela Nurlaela[2)] Purwono[3)]
[1]Program Studi Sistem Informasi, Fakultas Teknologi, ITB Swadharma Jakarta
[2,3]Program Studi Teknik Informatika, Fakultas Teknologi, ITB Swadharma Jakarta

Correspondence author: Usanto S, usanto.s@swadharma.ac.id, Jakarta, Indonesia

Abstract

The computer network is a very important aspect of our life today. Without a computer network, we cannot communicate with one another if separated by distance and time. Therefore, the availability of computer networks today is very important to support communication and even to support our work 24 hours a day. In line with these developments, there are still many network problems, especially at the Al Ikhlas Mosque Foundation, one of these factors is the lack of maintenance in terms of hardware that is not supported with the appropriate specifications. Based on the problems encountered and the results of the analysis using the SWOT method, it was concluded that there is a need to optimize the development of network technology at Masjid Al Ikhlas Foundation as an innovation in security issues and network smoothness by applying the VRRP (Virtual Router Redundancy Protocol) method. To support the VRRP method, it is necessary to conduct training for employees of the Masjid Al Ikhlas Foundation in the field of IT technology to deal with increasingly rapid technological developments, and it is also necessary to perform routine maintenance on network devices.

Keywords: network, VRRP, mikrotik

Abstrak

Jaringan komputer merupakan aspek penting kehidupan kita saat ini. Tanpa adanya jaringan komputer kita tidak dapat berkomunikasi antara satu dengan lainnya yang terpisah oleh jarak dan waktu. Maka itu ketersediaan jaringan komputer saat ini sangat penting untuk menunjang komunikasi dan pekerjaan kita selama 24 jam setiap harinya. Sejalan dengan perkembangan tersebut, masih banyak ditemukan berbagai masalah jaringan, khususnya pada Yayasan Masjid Al Ikhlas, salah satunya adalah kurangnya pemeliharaan *hardware* dengan tidak didukung oleh spesifikasi yang sesuai. Dari hasil analisa dengan menggunakan metode SWOT disimpulkan perlunya pengoptimalan perkembangan teknologi jaringan di Yayasan Masjid Al Ikhlas sebagai sebuah inovasi dalam masalah keamanan serta kelancaran jaringan dengan menerapkan metode VRRP (*Virtual Router Redundancy Protocol*). Untuk mendukung hal ini maka perlu dilakukan pelatihan kepada karyawan Yayasan Masjid Al Ikhlas dalam bidang teknologi IT untuk menghadapi perkembangan teknologi yang semakin cepat, dan juga perlu melakukan maintenance pada perangkat-perangkat jaringan secara rutin.

Kata Kunci: jaringan komputer, VRRP, mikrotik

A. PENDAHULUAN

Jaringan komputer merupakan aspek yang begitu penting dalam kehidupan kita saat ini. Tanpa adanya jaringan komputer kita tidak dapat berkomunikasi antara satu dengan yang lainnya jika dipisahkan oleh jarak dan waktu. Maka dari itu ketersediaan jaringan komputer saat ini sangatlah penting untuk menunjang komunikasi bahkan untuk menunjang pekerjaan kita selama 24 jam setiap harinya. Jaringan komputer merupakan kumpulan komputer, printer dan peralatan lainnya yang terhubung antara satu dengan yang lain Silitonga & Morina (2014:19).

Secara umum jaringan komputer terbagi menjadi 3 jenis, yaitu:

1. LAN (Local Area Network), LAN (Local Area Network) merupakan jaringan komputer terkecil untuk pemakaian pribadi. LAN (Local Area Network) memiliki skala jangkauan 1KM hingga 10KM, dalam bentuk koneksi wired (kabel), wireless (nirkabel), maupun kondisi keduanya" (Pratama, 2015:32).
2. MAN (Metropolitan Area Network), Metropolitan Area Network atau disingkat dengan MAN adalah jaringan komputer yang mencakup area kampus, perkantoran, pemerintahan ataupun kota, biasanya menghubungkan jaringan area lokal dengan menggunakan teknologi backbone yang berkecepatan tinggi, (Haryanto & Riadi, 2014:1372).
3. WAN (Wide Area Network), merupakan jaringan yang mencakup wilayah yang luas (seperti kota, daerah atau negara) menggunakan saluran telekomunikasi (communication channel) yang menggabungkan berbagai macam media seperti jalur telepon, kabel dan gelombang radio, (Firmansyah, 2014:105).

Mikrotik router adalah perangkat keras (hardware) router buatan Mikrotik yang menjalankan sistem RouterOS, dan merupakan salah satu perangkat yang bisa digunakan sebagai gateway atau sebagai penghubung antar jaringan, selain sebagi gateway yang handal juga terdapat beberapa fitur yang sangat diperlukan dalam penggelolaan jaringan seperti firewall, DNS Server DHCP Server, bandwidth manajemen dan masih banyak fitur yang lainya, (Iwan Sofana, 2017:8)

Iwan Sofana (2013:4) menjelaskan bahwa: "wireless adalah jaringan tanpa kabel yang menggunakan media penghantar gelombang cahaya infrued atau laser. Saat ini sudah semakin banyak public area atau lokal tertentu yang menyediakan layanan wireless network".

Dalam menjaga kestabilan komunikasi pada jaringan yang kompleks, misalnya pada Virtual Local Area Network (VLAN), diperlukan protokol yang dapat menjaga jaringan dari terputusnya komunikasi. Virtual Router Redundancy Protocol (VRRP) merupakan suatu protokol yang digunakan untuk mempertahankan komunikasi dengan menerapkan sistem redundansi pada router. Saat antarmuka utama mengalami masalah, VRRP akan secara otomatis memindahkan komunikasi ke antarmuka cadangan.

Topologi adalah aturan yang mendeskripsikan komputer, printer, dan piranti lain terhubung via jaringan. Dilihat dari topologinya, sebuah jaringan juga bisa dibagi-bagi menurut beberapa bagian. Winarno dan Zaki (2013:41)

Menurut Raharjo, Pernando, & Fauzi (2019:88). VRRP merupakan protokol yang secara dinamis menunjukan satu atau lebih virtual router menjadi gateway router didalam jaringan LAN. VRRP pada dasarnya tidak mendukung fitur dari load balancing

Sedangkan dalam hasil penelitian Michael & Ghozali (2018:1) menjelaskan bahwa Untuk menjamin kelancaran pengiriman data dari LAN menuju router gateway, diperlukan router backup. Protokol yang digunakan pada router

backup adalah Virtual Router Redundancy Protocol (VRRP). VRRP merupakan sebuah interface dari router OS Mikrotik yang memungkinkan untuk membuat beberapa router sebagai gateway dari jaringan lokal yang berada satu segment. Hasil pengujian menunjukkan kehilangan data saat VRRP bekerja hanya 3,8%, jauh lebih kecil dibandingkan dengan kehilangan data pada saat routing protokol Open Shortest Path First (OSPF) bekerja untuk mengalihkan trafik ke jaringan lain bila ada router yg tidak bekerja. Pengujian dengan Jperf menunjukan throughput dengan VRRP dan tanpa VRRP sebesar 219079 Kbits/s. Menggunakan VRRP tidak berpengaruh pada throughput bandwidth.

Serta dalam hasil penelitian Kuswanto & Rahman (2019:60) menyatakan bahwa VRRP menggunkan failover dinamis untuk memastikan ketersediaan router yang aktif dengan menggunakan alamat IP route default Virtual Router atau disebut VR, pada reudancy ini menyediakan cadangan alamat ip gateway sehingga jika router master VR tidak tersedia lalu lintas jaringan akan dialihkan ke router backup secara otomatis tanpa ada pengaturan manual dari administrator jaringan. Penelitian ini menggunakan beberapa referensi yang berkaitan dengan objek penelitian diantaranya yaitu, dengan penerapan protokol VRRP permasalahan pada router dapat teratasi, jika terjadi permasalahan pada router, downtime pada jaringan dapat dihindari. Virtual router redudancy protocol (VRRP) pada jaringan berbasis Ipv6, perpindahan koneksi dari router utama ke router backup dapat dilakukan dengan baik sesuai dengan standar ITU-T. Penerapan VRRP yang digunakan diantara dua router, memungkinkan router cadangan untuk mengganti router utama dengan segera tanpa menunggu waktu yang ditentukan, dengan biaya yang dikeluarkan cukup efektif untuk penerapkan metode ini.

Namun sejalan dengan perkembangan tersebut, masih banyak ditemukan berbagai masalah jaringan, khususnya pada Yayasan Masjid Al Ikhlas, salah satunya masalah yang sering terjadi yaitu kegagalan dalam mengakses jaringan internet dan web mail akibat dari permasalahan hardware ataupun software. Maka dari itu diperlukanya backup jaringan sebagai antisipasi permasalahan tersebut dengan tujuan agar jaringan yang ada pada Yayasan Masjid Al Ikhlas bisa berjalan dengan baik.

B. METODE PENELITIAN

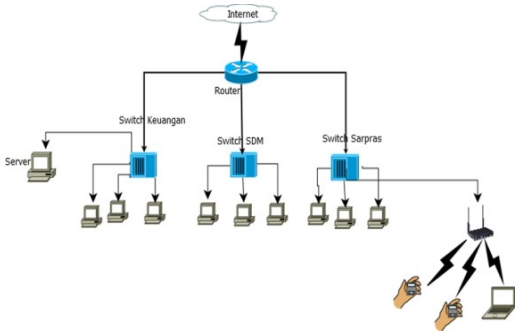
Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Penelitian ini menggunakan metode penelitian kualitatif dengan menggunakan pendekatan penelitian pengamatan (observasi) merupakan suatu proses yang kompleks, suatu proses yang tersusun dari berbagai proses biologis dan psikologis, Sugiyono, 2017:145). Observasi melakukan penelitian secara langsung tentang instalasi jaringan dan topologi jaringan yang digunakan di Yayasan Masjid Al Ikhlas yang berada di jalan Cipete III No. 10, Cipete Selatan, Cilandak, Jakarta Selatan.

Wawancara digunakan sebagai teknik pengumpulan data apabila ingin melakukan studi pendahuluan untuk menentukan permasalahan yang harus diteliti, (Sugiyono, 2017:137), dan Studi Pustaka langkah-langkah ilmiah dalam mengumpulkan data dengan mencari referensi pendukung, (Chaidir & Rino, 2019:252). Studi pustaka dilakukan dengan mencari referensi jurnal-jurnal dan buku-buku yang terkait dengan tehnik informatika khususnya mengenai jaringan Virtual Router Redundancy Protocol (VRRP). Untuk pengumpulan data sekunder yang dilakukan untuk memperoleh keterangan dan data dari literatur yang berupa buku, majalah, makalah, internet yang relevan dengan landasan teori atas masalah yang diteliti agar diperoleh suatu pemahaman yang mendalam serta menunjang proses

pembahasan mengenai masalah-masalah yang telah diidentifikasi.

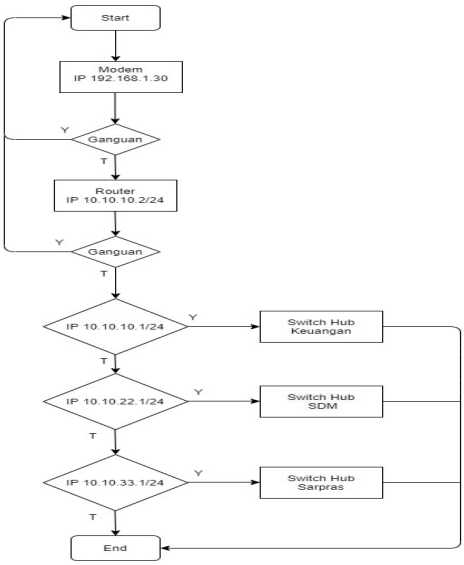
C. HASIL DAN PEMBAHASAN

Sistem berjalan di Yayasan Masjid Al-Ikhlas mengunakan sistem *tree*. Alurnya mengunakan 1 router. Dari internet dihubungkan ke Router lalu dibagi ke switchhub dan server, dari switchhub dibagi ke komputer yang ada serta dibagi ke wifi. Smartphone dan laptop mendapatkan arus internet yang berasal dari wifi. Berikut ini gambar topologi jaringan yang ada di Yayasan Masjid Al-Ikhlas.



Gambar 1. Gambar Topologi Jaringan

Gambar flowchart untuk menjelaskan alur sistem yang berjalan di YMAI dapat dilihat padagambar 2



Gambar 2. Flowchart sistem berjalan

Deskripsi Sistem

Pada Penelitian ini, telah menganalisa topologi yang digunakan pada Yayasan Masjid Al-Ikhlas yaitu topologi *tree*. Pada topolagi ini modem dengan *IP Address* 192.168.1.30, *Subnet Mask*: 255.255.255.0, *Gateway*: 192.168.1.1 masuk ke *router mikrotik* dirubah menjadi IP Address 10.10.10.2/24, *Subnet Mask*: 255.255.255.0, *Gateway*: 10.10.10.1. Didalam *router* tersebut dibagi menjadi 3 vlan, yaitu vlan keuangan, vlan SDM, serta vlan sarpras.

Tabel 1 IP Addres per Devisi

Devisi	*IP Addres*	*Subnet*	*Gateway*
Keuangan	10.10.10.2 – 10.10.10.254	255.255.255.0	10.10.10.1
SDM	10.10.22.2 - 10.10.22.254	255.255.255.0	10.10.22.1
Sarpras	10.10.33.2 - 10.10.33.254	255.255.255.0	10.10.33.1

Topologi *tree* adalah topologi yang terbentuk dari gabungan antara beberapa switch yang terhubung berbentuk seperti tangkai pohon, adapun SWOT pada topologi *tree* yaitu:

1. *Strengh* (kelebihan)
   a. memudahkan mendeteksi kerusakan ataupun kesalahan jaringan.
   b. Mudah membangun jaringan yang luas
   c. Mengatasi keterbatasan dari topologi *star* yang memiliki keterbatasan pada titik koneksi hub ataupun switch
   d. Manajemen data yang baik
2. *Weakness* (kekurangan) :
   a. Hub ataupun switch menjadi peran penting

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

b. Mengeluarkan biaya yang cukup banyak karena menggunakan banyak kabel
c. Jika komputer yang ada ditingkat tinggi mengalami masalah, maka komputer yang berada dibawah juga akan mengalami masalah

3. *Opportunities* (Peluang)
   a. Berkembangnya teknologi yang sangat pesat mempermudah dalam memilih jaringan keamanan
   b. Banyaknya produsen *mikrotik* memudahkan memilih jenis *mikrotik* yang sesuai kebutuhan.
4. Threat (Ancaman)
   a. Terjadi *down*-nya internet karena kendala dari *hardware* (Routerboard) menyebabkan tingkat produktifitas karyawan menjadi menurun.
   b. Kurangnya penerapan otomatisasi dalam hal mem-backup *hardware*, menurut penulis hal tersebut yang menjadi permasalahan jaringan, terutama dalam dunia perbankan yang mencakup kebutuhan akses jaringan yang stabil.
   c. Penempatan jalur kabel yang kurang rapih yang dapat memicu timbulnya gangguan pada jaringan.

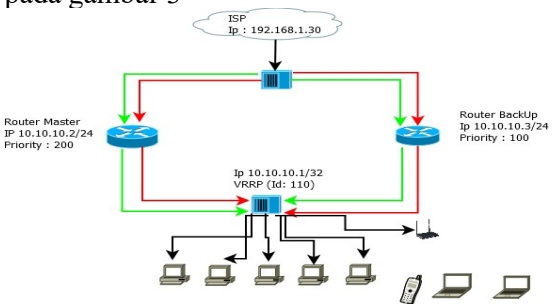
Berdasarkan permasalahan yang dihadapi dan atas hasil analisa dengan menggunakan metode SWOT disimpulkan perlunya pengoptimalan perkembangan teknologi jaringan di Yayasan Masjid Al Ikhlas sebagai sebuah inovasi dalam masalah keamanan serta kelancaran jaringan dengan menerapkan metode VRRP *(Virtual Router Redundancy Protocol)*.

Analisa Kebutuhan

Untuk merancang ulang jaringan perlu diketahui terlebih dahulu *topologi* jaringan yang sedang berjalan yaitu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam rancangan jaringan usulan yang kami rancang untuk Yayasan Masjid Al-Ikhlas tetap menggunakan *topologi* jaringan yang masih berjalan di Yayasan tersebut yaitu menggunakan *Topologi Star*, dimana *topologi* ini yang menghubungkan beberapa komputer dengan menggunakan perangkat yaitu *hub* atau *switch*, hingga memberntuk jaringan komputer yang merupakan gabungan antara teknologi komputer dan teknologi komunikasi

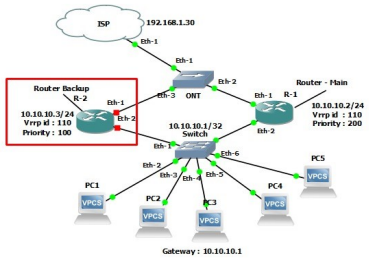
Deskripsi Sistem Usulan

Topologi Sisitem Usulan Dapat dilihat pada gambar 3

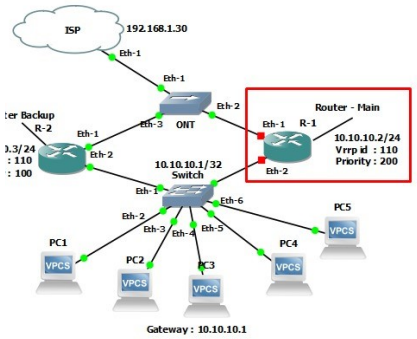


Gambar 3. Gambar Topologi Usulan

Didalam sistem usulan ini menambahkan 1 buah switch hub serta 1 buah *Router*. Switch tambahan ini berfungsi sebagai penghubung dari ISP ke router. *Router* yang kami gunakan menjadi 2 buah. Yang pertama sebagai router utama (*Router Master*) dan yang kedua sebagai router cadangan (*router backup*) dan dapat dlilihat pada gambar 4 dan 5.

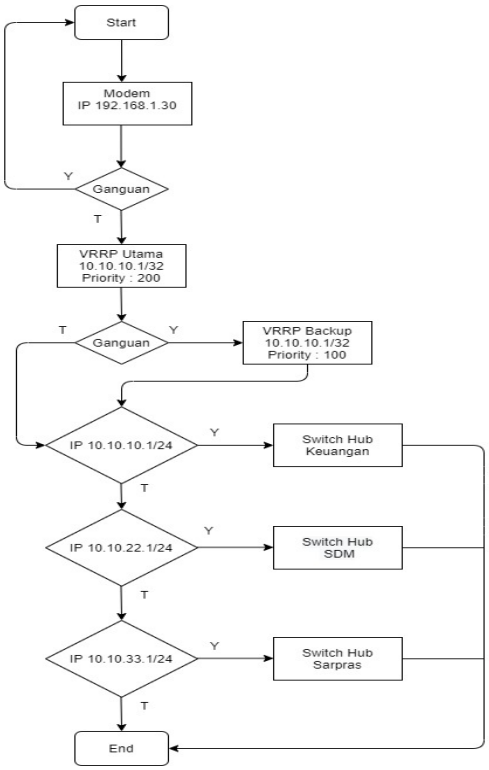


Gambar 4. Topologi Usulan *router backup down*



Gambar 5. Topologi Usulan *router main down*

Secara lengkap cara kerja sistem usulan bisa dapat dilihat pada gambar 6.



Gambar 6. Gambar Flowchart sistem usulan

Deskripsi Sistem Menyeluruh

Kebutuhan sistem ini dikumpulkan yang akan digunakan dalam penerapan sistem failover pada router menggunakan protokol VRRP diantaranya yaitu, dua buah routerboard mikrotik dengan tipe Router Board 850Gx2 dengan Router Os versi 608, untuk pengalamatan perangkat router dan client digunakan alamat ip address 10.10.10.2/24, dan untuk alamat ip virtual pada interface VRRP yaitu 10.10.10.1/32 di konfigurasi pada kedua router yang akan digunakan sebagai gateway jaringan lokal, sedangkan untuk komunikasi antar router akan menggunakan sebuah *virtual router ID* dengan angka 110 pada masing-masing router, untuk menentukan *router primary* dan *router backup* yaitu dengan menambahkan *priority* pada masing-masing interface VRRP dengan ketentuan, pada *router primary* diberikan *priority* 200, sedangkan pada *router backup* diberikan *priority* 100. Selain kebutuhan konfigurasi pada router dibutuhkan juga aplikasi pendukung untuk menerapkan sistem ini diantaranya aplikasi *winbox* versi 3.18 yang digunakan untuk konfigurasi *router mikrotik*, dan aplikasi *command prompt* pada *microsoft windows* yang digunakan untuk uji koneksi *failover* pada router.

Pada tahap desain dibuat rancangan *topologi* yang akan diterapkan pada perancangan ini, *topologi* yang digunakan yaitu menggunakan *topologi star*, pada *topologi* juga di lakukan pembagian alamt ip address untuk kedua router dan ip address untuk client. Pada tahap ini juga di lakukan rancangan konfigurasi apa saja yang akan di lakukan pada *router* mulai dari penentuan alamat interface VRRP, *virtual router ID*, sampai dengan penetuan nilai priority pada masing-masing *router*. Selain konfigurasi VRRP, semua *router* juga di konfigurasi sebagai *gateway* dan *dns server*.

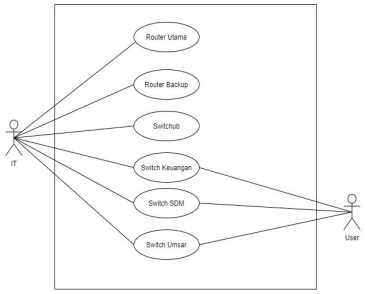
Spesifikasi Proses

Penentuan *router primary* akan dilakukan dengan melakukan pengecekan *in state* dimana jika nilai *priority* pada VRRP adalah 200 maka ip akan mengirim paket *advertisment* dan *broadcast* permintaan ARP dan koneksi akan dialirkan pada *master state* atau *router primary* akan aktif

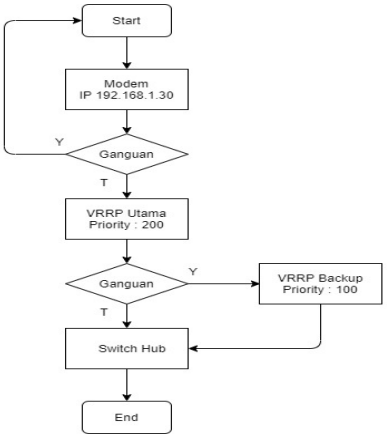
JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

dan sebaliknya jika berada pada status *backup state* jika ip pada jaringan mengirimkan paket *advertisment* dan *broadcast* permintaan ARP, maka *backup state* tidak akan menjawab permintaan ARP, jika *router primary* tidak aktif maka nilai *priority* 100 pada *router backup* yang akan dijadikan sebagai *master state*.

Berikut penjelasan alur spesifikasi proses bisa dapat dilihat pada gambar 7 dan 8



Gambar 7. Use Case Diagram



Gambar 8. Alur Spesifikasi Proses

Rancangan Modul

Dalam merancang penelitian kami menggunakan IP statis (*ether*1) yang digunakan untuk menghubungkan ke ISP sedangkan IP lokal (*ether*2) digunakan untuk menghubungkan ke client. IP statis dan IP Lokal sama-sama *IP Address* untuk pengalamatan pada jaringan komputer dengan memberikan sederet angka pada komputer (*host*), router atau peralatan jaringan lainnnya. Menurut Joefrie (2013:297) menjelaskan bahwa "*Transmission Control Protocol/Internet Protocol* adalah salah satu jenis protokol yang memungkinkan kumpulan komputer untuk berkomunikasi dan bertukar data di dalam satu jaringan. Sedangkan yang dimaksud dengan *protokol* adalah himpunan aturan yang telah ditetapkan yang mengatur bagaimana dua atau lebih proses berkomunikasi dan berinteraksi untuk saling bertukar data.

Menurut Zam (2014:55) menjelaskan bahwa: "IP *address* adalah alamat unik yang diberikan komputer dalam sebuah jaringan. Disebut unik karna satu alamat hanya boleh dimiliki oleh satu komputer". IP *address* merupakan suatu alamat yang digunakan untuk identitas masing-masing pada komputer, sehingga pada saat mengirim dan menerima paket data ataupun berkomunikasi memungkinkan meminimalisir terjadinya *collision*.

IP address terdiri dari dua bagian, yaitu Network ID dan Host ID. Berikut *gambar IP address router* yang kami gunakan:

Tabel 2. *IP Address* Router dan Router Backup Router Ether 1 Ether 2 VRRP

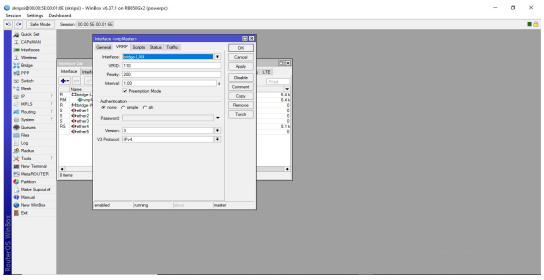
Router	Ether 1	Ether 2	VRRP	Nilai Priority
Router master	192.168.1.30	10.10.10.2/24	10.10.10.1/32	200
Router Backup	192.168.1.30	10.10.10.3/24	10.10.10.1/32	100

Virtual ID adalah identitas dari virtual router yang dikonfigurasikan dengan range antara 1-255. Nilai VRID yang digunakan harus sama dengan router utama, agar router backup mendapatkan ID dan hak akses yang sama. Priority adalah nilai prioritas yang

digunakan pada masing-masing router master dan router backup dengan nilai range 1-255. Sedangkan Nilai *priority* digunakan untuk menetukan router mana yang digunakan sebagai router master. Untuk itu router utama harus memiliki nilai priority lebih tinggi dari pada nilai priority pada router backup**.**

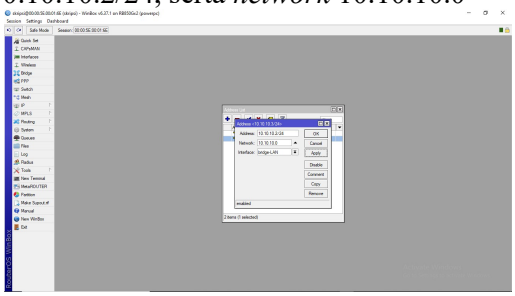
Rancangan Tampilan

Pada tampilan berikut penomeran VRID 110, *priority* 200 dan *interval* 1.00.



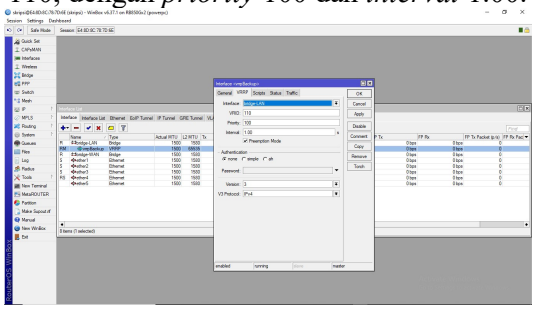
Gambar 9. Tampilan *setting* VRRP Utama

Pemberian *IP addres* pada VRRP Utama 10.10.10.2/24, serta *network* 10.10.10.0



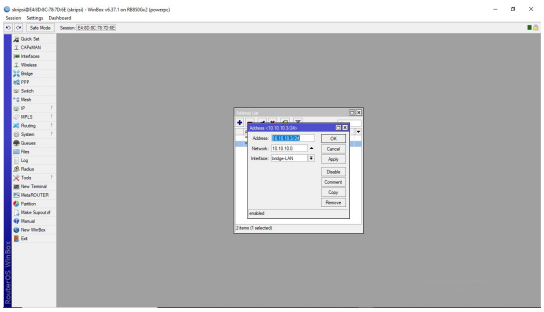
Gambar 10. Tampilan IP VRRP Utama

Pada tampilan berikut penomeran VRID 110, dengan *priority* 100 dan *interval* 1.00.



Gambar 11. Tampilan setting VRRP *Backup*

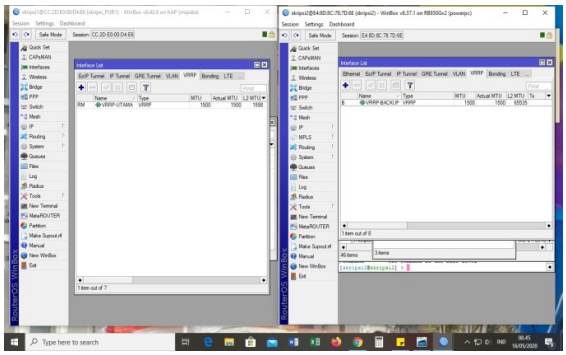
Pemberian *IP addres* pada VRRP Utama 10.10.10.3/24, serta *network* 10.10.10.0 .



Gambar 12. Tampilan IP VRRP *Backup*

Rancangan Implementasi

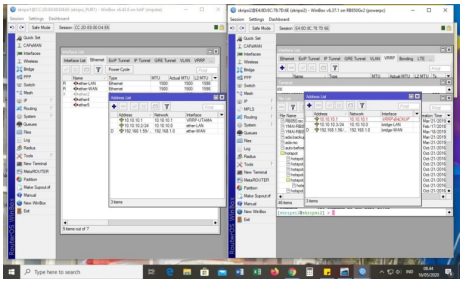
Pada tahap implementasi VRRP dilakukan pengujian pada komputer *client.* Komputer *Client* diberi IP 10.10.10.5 dan dilakukan test untuk membuka *browser*. Pada saat membuka *browser* itu dilakukan pengecekan jalur yang dilalui. Dibawah ini adalah gambar tampilan VRRP Utama berada dalam posisi *running* dengan tanda RM artinya sedang berjalan. Sedangkan VRRP Backup berada dalam posisi *backup* dengan tanda B.



Gambar 13.Tampilan 2 buah VRRP

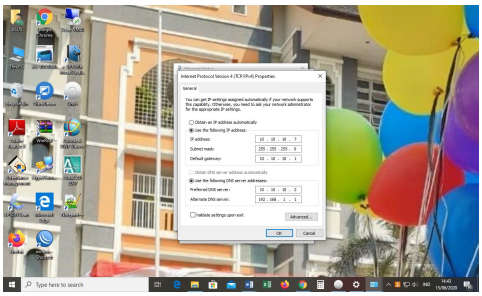
Didalam *adrres list* juga terlihat jelas VRRP Utama bekerja ditunjukan dengan tanda tulisan hitam artinya *trafic* melalui VRRP utama. Sedangkan VRRP *Backup stanby* (sedang tidak bekerja) ditunjukan dengan tulisan merah.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 01 JANUARI 2022
ISSN 2774 – 5775 | eISSN 2774-5767



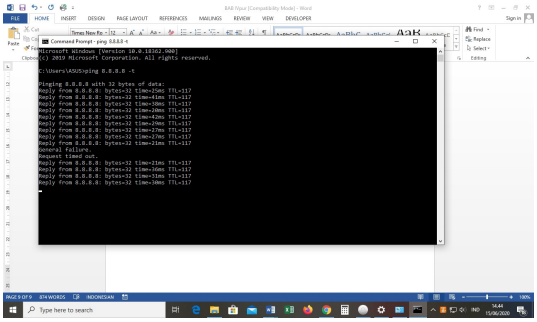
Gambar 14. Tampilan kerja VRRP

Pada tahap pengujian, komputer diberi IP *Address* 10.10.10.7 . *Subnet Mask* 255.255.255.0 . *Gateway* 10.10.10.1 . *DNS server* 10.10.10.2.



Gambar 15. Tampilan pengisian IP komputer

Selanjutnya dilakukan pengujian jaringan dengan cara melakukan ping terhadap google atau IP 8.8.8.8. Hasilnya terlihat pada bagian pertama berjalan lancar ketika melewati VRRP Utama. Bersamaan dengan itu, VRRP utama sengaja dimatikan untuk melihat apakah VRRP *Backup* berfungsi dengan baik. Terlihat ada *Request timed out* (RTO) waktu VRRP Utama dimatikan. Setelah itu koneksi kembali normal setelah melewati VRRP *Backup*.



Gambar 16. Tampilan pengujian koneksi

D. PENUTUP

Berdasarkan hasil penelitian yang dilakukan terhadap pembuatan Aplikasi Kriptografi dan Steganografi, ada beberapa hal yang dapat disimpulkan,yaitu :

1. Untuk mengamankan sebuah pengiriman informasi dalam bentuk teks di perlukan aplikasi kriptografi untuk proses enkripsi dan deskripsi dengan metode RSA.
2. Aplikasi dapat melakukan enkripsi dan dekripsi terhadap pesan dengan masukan kunci yang yang digunakan pada saat proses.
3. Untuk mengimplementasikan proses memasukan dan mengeluarkan teks pada file gambar atau disebut dengan steganografi menggunakan metode Parity Coding pada aplikasi.
4. Mengimplementasikan teknik parity coding pada perangkat mobile phone dengan cara pesan diubah menjadi bilangan biner, memilih gambar dan diproses gambar diubah menjadi biner dan setiap 8 bit akhir dimasukan 1 bit biner pesan.
5. Perangkat lunak yang digunakan untuk mengimplementasikan steganografi gambar dengan teknik Parity Coding pada berkas image berhasil dibangun. Kebutuhan fungsional dari perangkat lunak seperti proses penyembunyian dan ekstraksi pesan serta penggunaan kunci sudah dapat dilakukan dengan benar.
6. Pada proses ekstraksi, pesan atau informasi yang disisispkan pada file gambar uji dalam aplikasi Steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan.

Agar rancangan jaringan yang diusulkan dapat digunakan dengan baik ada

beberapa saran yang penulis berikan pada Yayasan Masjid Al Ikhlas, sebagai berikut :

1. Pengembangan Perlunya pelatihan kepada karyawan Yayasan Masjid Al Ikhlas dalam bidang teknologi IT untuk menghadapi perkembangan teknologi yang semakin cepat.
2. Upgrade perangkat RB750 dengan RB450G, dengan tujuan meningkatkan daya transfer lebih cepat dan juga meningkatkan performa yang lebih baik.
3. Menyediakan perangkat keras cadangan lain yang berkaitan tentang kelancaran dan keamanan agar akses jaringan tetap berjalan dengan lancer dan aman.
4. Melakukan maintenance tampilan dengan menggunakan background dan interface yang lebih menarik.

E. DAFTAR PUSTAKA

Haryanto, M. D., & Riadi, I. (2014). Analisis Dan Optimalisasi Jaringan Menggunakan Teknik Load Balancing (Studi Kasus : Jaringan UAD Kampus 3)

Joefrie, Y. Y., Teknik, F., Elektro, J. T., & Tadulako, U. (2013). Perancangan Program Simulasi Perintah Dasar Jaringan Komputer.

Kuswanto, H., & Rahman, T. (2019). Failover Gateway Menggunakan Protokol Virtual Router Redundancy Protocol (VRRP) pada Mikrotik Router.

Raharjo, M., Pernando, F., & Fauzi, A. (2019). Perancangan Performansi Quality Of Service Dengan Metode Virtual Routing Redudancy Protocol (VRRP), V (1), 87–92.https://doi.org/10.31294/jtk.v4i2

Ricky Firmansyah (2014). Rancang Bangun Jaringan Komputer Dengan Kabel Listrik Sebagai Media Transmisi Untuk Komunikasi Data

Silitonga, P., & Morina, I. S. (2014). Analisis QoS (Quality of Service) Jaringan Kampus dengan Menggunakan Microtic Routerboard, III(2).

Sofana, Iwan. 2013. Membangun Jaringan Komputer. Bandung: Informatika.

Sofana, Iwan. 2017. Jaringan Komputer Berbasis Mikrotik. Bandung: Informatika.

Winarno, Edy ST,M.Emg. Ali Zaki. SmitDev Community. Membangun Jaringan di Windows XP hingga Windows 8. Jakarta: PT Elex Media Komputindo.

Yosua Michael, Theresia Ghozali, 2018. Protokol Virtual Router Redundancy Sebagai Backup Route Gateway Menggunakan Router Mikrotik

Zam, Elvy Zamidra. 2014. Cara Mudah Membuat Jaringan Wireless. Jakarta: PT Elex Media Komputindo.

Alamat Redaksi
Kampus 1 Institut Teknologi dan Bisnis Swadharma
Jl. Malaka No.3, Tambora, Jakarta Barat
emal : jurnal.jeis@swadharma.ac.id

9 772774 577002