

IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* MENGUNAKAN ZEROTIER BERBASIS OPENWRT

TUGAS AKHIR

“Disusun Untuk Memenuhi Syarat Kelulusan Program Strata I Pada
Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangka Raya”



OLEH

MUHAMMAD DIMAS WAHYU PRAYOGA
NIM C2055201022
PROGRAM STUDI TEKNIK INFORMATIKA

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2024**

**IMPLEMENTASI *VIRTUAL PRIVATE NETWORK*
MENGUNAKAN ZEROTIER BERBASIS OPENWRT**

TUGAS AKHIR

“Disusun Untuk Memenuhi Syarat Kelulusan Program Strata I Pada
Sekolah Tinggi Manajemen Informatika Dan Komputer
(STMIK) Palangka Raya”

OLEH

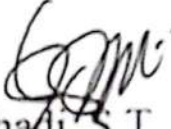
MUHAMMAD DIMAS WAHYU PRAYOGA
NIM C2055201022
PROGRAM STUDI TEKNIK INFORMATIKA

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKA RAYA
2024**

PERSETUJUAN
IMPLEMENTASI VIRTUAL PRIVATE NETWORK MENGGUNAKAN
ZEROTIER BERBASIS OPENWRT

Tugas Akhir ini telah Disetujui Untuk Diujikan pada
Tanggal 11 juli 2024

Pembimbing I,


Abdul hadi, S.T., M.Kom
NIK. 108505102021101

Pembimbing II,


Catharina Elmayantie, M.Pd.
NIK. 197610252015003

Mengetahui

Suparno, M.Kom
NIK. 196901041995105

PENGESAHAN

IMPLEMENTASI VIRTUAL PRIVATE NETWORK MENGGUNAKAN ZEROTIER BERBASIS OPENWRT

Tugas Akhir ini telah Diujikan, Dinilai, dan Disahkan Oleh Tim Penguji pada
Tanggal 11 Juli 2024

Tim Penguji Tugas Akhir :

1. Sam'ani, S.T., M.Kom.
Ketua



.....

2. Elia Zakharia, M.T.
Sekretaris



.....

3. Amaya Andri Damaini, S.Kom., M.T.
Anggota

.....

4. Abdul Hadi, S.T., M.Kom.
Anggota



.....

5. Catharina Elmayantie, M.Pd.
Anggota



.....

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini :

Nama Mahasiswa : **MUHAMMAD DIMAS WAHYU PRAYOGA**

NIM : **C2055201022**

Menyatakan bahwa Tugas Akhir dengan judul :

IMPLEMENTASI VIRTUAL PRIVATE NETWORK MENGGUNAKAN ZEROTIER BERBASIS OPENWRT

Adalah hasil karya saya dan bukan merupakan duplikasi atau plagiasi sebagian ataupun seluruhnya dari karya orang lain, kecuali bagian yang sumber informasi dicantumkan.

Pernyataan ini dibuat dengan sebenar-benarnya secara sadar dan bertanggung jawab, saya bersedia menerima sanksi berupa pembatalan Tugas Akhir apabila terbukti melakukan duplikasi atau plagiasi terhadap Tugas Akhir atau karya ilmiah yang sudah ada.

Palangkaraya, 11 Juli 2024

Yang Membuat Pernyataan

Muhammad Dimas Wahyu Prayoga

MOTTO DAN PERSEMBAHAN

“ Setiap pertanyaan selalu ada jawaban

setiap kegagalan akan menemukan jalan ”

Kupersembahkan Untuk :

- Kepada yang terkasih kedua orang tua penulis, yaitu Bapak Nooripansyah dan Ibu Herlina serta kedua adik penulis, terimakasih yang tak terhingga yang telah memberikan banyak dukungan, nasehat serta doa kepada penulis.
- Kepada Dosen pembimbing bapak Abdul Hadi, S.T., M.Kom dan Ibu Catharina Elmayantie, M.Pd yang telah bersedia membimbing penulis dalam penulisan tugas akhir ini.
- Kepada seluruh keluarga terutama mamayi dan mama tiara yang banyak sekali membantu dan mendukung penulis selama masa perkuliahan.
- Kepada sahabat penulis yaitu Para Pecinta Wanita dan king akmal winandy yang banyak membantu dalam proses penulisan tugas akhir ini.
- kepada teman-teman angkatan 2020 yang telah memberikan semangat kepada penulis dan terimakasih kepada seluruh dosen STMIK Palangka Raya.

INTISARI

MUHAMMAD DIMAS WAHYU PRAYOGA, C2055201022, 2024.

Implementasi *Virtual Private Network* Menggunakan Zerotier Berbasis OpenWRT, Pembimbing I Abdul Hadi, S.T., M.Kom., Pembimbing II Catharina Elmayantie, M.Pd.

Bidang Sekretariat adalah salah satu bidang yang ada di Dinas Koperasi Usaha Kecil dan Menengah (UMKM) Provinsi Kalimantan Tengah kota Palangka Raya. Berdasarkan hasil observasi dan wawancara yang dilakukan penulis dengan bapak Eddy Jonathan selaku staff bidang sekretariat, diketahui bahwa pada bidang sekretariat belum menerapkan jaringan VPN dimana antar komputer masih melakukan sharing folder atau file dan data menggunakan jaringan publik, Oleh sebab itu hal ini tentunya menyebabkan beberapa permasalahan seperti pengaksesan data oleh pihak yang tidak berwenang, misalnya pemantauan, pencurian data, dan penyadapan. Berdasarkan hasil observasi dan wawancara yang dilakukan maka penulis memberikan solusi yaitu menggunakan jaringan VPN menggunakan zerotier agar pengguna dapat dengan aman dalam melakukan sharing folder dan data. juga membantu pekerjaan menjadi lebih efektif dan efisien tanpa takut untuk pemantauan dan pencurian data.

Pada penelitian ini penulis menggunakan metode *Research and Development* (RnD), yang dimulai dari melakukan tahapan analisis dan yang terakhir adalah tahap pengujian. Penulis menggunakan 3 metode pengumpulan data yaitu, observasi, wawancara, dan metode kepustakaan. Untuk kebutuhan hardware penulis menggunakan Laptop, STB *type* B860H, Modem dan *MicroSD 8GB* lalu untuk kebutuhan Software penulis menggunakan sistem operasi *Windows* dan Zerotier.

Berdasarkan hasil dari penelitian ini penulis menemukan ip publik yang sama atau tidak berubah pada saat sebelum dan sesudah mengaktifkan vpn zerotier dan ip publik berubah ketika menggunakan vpn lain. Berdasarkan hasil pengujian, implementasi vpn menggunakan zerotier dapat berjalan dengan baik dan membantu meningkatkan konektivitas pada saat melakukan sharing folder atau transfer data yang dilakukan dan memudahkan pengguna untuk mengakses dari manapun dengan aman sehingga mengoptimalkan kinerja.

Kata Kunci : Implementasi, Jaringan, VPN, Zerotier, OpenWRT, RnD.

ABSTRACT

MUHAMMAD DIMAS WAHYU PRAYOGA, C2055201022, 2024.

Implementation of a Virtual Private Network Using OpenWRT Based
Zerotier, Advisor I Abdul Hadi, S.T., M.Kom., Advisor II Catharina
Elmayantie, M.Pd.

The Secretariat field is one of the fields in the Small and Medium Enterprises Cooperatives (UMKM) Department of Central Kalimantan Province, Palangka Raya City. Based on the results of observations and interviews conducted by the author with Mr. Eddy Jonathan as secretariat staff, it is known that the secretariat has not implemented a VPN network where computers still share folders or files and data using public networks, therefore this certainly causes several problems. such as accessing data by unauthorized parties, for example monitoring, data theft and wiretapping. Based on the results of observations and interviews conducted, the author provides a solution, namely using a VPN network using zerotier so that users can safely share folders and data. It also helps work become more effective and efficient without fear of monitoring and data theft.

In this research the author used the Research and Development (RnD) method, which starts from carrying out the analysis stage and the last is the testing stage. The author used 3 data collection methods, namely, observation, interviews, and library methods. For hardware needs the author uses a laptop, STB type B860H, Modem and 8GB MicroSD, then for software needs the author uses the Windows and Zerotier operating systems.

Based on the results of this research, the author found that the public IP was the same or did not change before and after activating Zerotier VPN and the public IP changed when using another VPN. Based on the test results, implementing VPN using Zerotier can run well and help improve connectivity when sharing folders or transferring data and making it easier for users to access it from anywhere safely, thereby optimizing performance.

Keywords: Implementation, Network, VPN, Zerotier, OpenWRT, RnD.

KATA PENGANTAR

Puji syukur kita ucapkan atas kehadiran Allah SWT yang hingga saat ini masih memberikan kita nikmat iman dan kesehatan, sehingga penulis diberi kemampuan untuk menyelesaikan Tugas Akhir ini yang berjudul “IMPLEMENTASI *VIRTUAL PRIVATE NETWORK* Menggunakan *ZEROTIER* Berbasis *OPENWRT*”. Tugas Akhir ini disusun untuk untuk memenuhi syarat dalam memperoleh gelar Sarjana Komputer di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangka Raya.

Tak lupa penulis juga mengucapkan terimakasih yang sebanyak-banyaknya kepada setiap pihak yang telah mendukung serta membantu penulis selama proses penyelesaian Tugas Akhir ini. Ucapan terima kasih penulis sampaikan pada:

1. Eddy Jonathan, sebagai staff bidang sekretariat dan narasumber dalam penelitian ini.
2. Abdul Hadi, S.T., M.Kom., sebagai dosen pembimbing I
3. Catharina Elmayantie, M,Pd., sebagai dosen pembimbing II

Maka dari itu penulis dengan senang hati menerima kritik dan saran yang membangun dari para pembaca. Penulis berharap Tugas Akhir ini dapat bermanfaat bagi semua pihak.

Palangka Raya, 11 Juli 2024

Penulis

DAFTAR ISI

PERSETUJUAN	ii
PENGESAHAN.....	iii
PERNYATAAN KEASLIAN.....	iv
MOTTO DAN PERSEMBAHAN.....	v
INTISARI	vi
ABSTRACT.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR.....	xii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Perumusan Masalah	3
1.3. Batasan Masalah	3
1.4. Tujuan dan Manfaat	4
1.4.1. Tujuan	4
1.4.2. Manfaat	4
1.5. Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Kajian Teori.....	7
2.1.1. Implementasi.....	7
2.1.2. Jaringan Komputer.....	7
2.1.3. <i>Virtual Private Network (VPN)</i>	8
2.1.4. Zerotier.....	13
2.1.5. OpenWRT	14
2.1.6. <i>Set Top Box (STB)</i>	16
2.1.7. Linux	17
2.2 Penelitian Relevan	18
BAB III METODOLOGI PENELITIAN	21
3.1. Tinjauan Umum	21

3.2.	Jenis Penelitian.....	21
3.3.	Desain Penelitian	21
3.4.	Instrumen Penelitian	24
3.5.	Analisis Kebutuhan.....	25
3.5.1.	Kebutuhan perangkat keras.....	25
3.5.2.	Kebutuhan perangkat lunak	25
3.6.	Desain	26
3.6.1.	Desain Perangkat.....	26
3.6.2.	Desain Usulan Implementasi Perangkat.....	27
BAB IV HASIL DAN PEMBAHASAN.....		28
4.1	Hasil	28
4.1.1	Implementasi.....	28
4.1.2	Pengujian.....	40
4.2	Pembahasan.....	48
BAB V KESIMPULAN DAN SARAN		51
5.1	Kesimpulan	51
5.2	Saran	52

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka	19
Tabel 4.1 Pengujian pada cmd	43
Tabel 4.2 pengujian pada tools Whatis MyIP Address	43

DAFTAR GAMBAR

Gambar 2 1 Cara Kerja VPN	8
Gambar 2.2 Set Top Box.....	16
Gambar 3.1 Bagan Alur	22
Gambar 3.2 Flowchart Alur Penelitian.....	23
Gambar 3.3 Desain perangkat	26
Gambar 3.4 Desain Usulan Perangkat	27
Gambar 4.1 Folder OpenWRT	29
Gambar 4.2 Boot Microsd menggunakan Rufus.....	30
Gambar 4.3 File Uboot.bin	31
Gambar 4.4 File OpenWRT yang diboot di MicroSD	31
Gambar 4.5 Wifi STB	32
Gambar 4.6 Halaman Login STB	33
Gambar 4.7 Tampilan OpenWRT	33
Gambar 4.8 Tampilan menu System OpenWRT	34
Gambar 4.9 Tampilan menu System <i>OpenWRT</i>	34
Gambar 4.10 Halaman <i>Login Zerotier Server</i>	35
Gambar 4.11 Buat <i>Network Zerotier Server</i>	35
Gambar 4.12 <i>Network Zerotier Server</i>	36
Gambar 4.13 <i>IP Zerotier Server</i>	36
Gambar 4.14 <i>Network ID Zerotier</i> pada <i>Zerotier</i>	37
Gambar 4.15 <i>Network Address perangkat Zerotier Server</i>	37
Gambar 4.16 <i>Zerotier Client join Network Zerotier Server</i>	38
Gambar 4.17 <i>Add Network Zerotier Server</i>	39
Gambar 4.18 <i>Zerotier client terhubung dengan Zerotier Server</i>	40
Gambar 4.19 Akses kekomputer server	41
Gambar 4.20 Tampilan <i>Sharing Folder</i>	41
Gambar 4.21 Isi dari <i>sharing folder</i>	42
Gambar 4.22 Halaman <i>xampp server</i> yang diakses di komputer <i>client</i>	43
Gambar 4.23 Komputer <i>Client ping Server</i>	43
Gambar 4.24 <i>IP Publik Vpn Zerotier</i>	45
Gambar 4.25 <i>Ip publik Vpn</i> lain.....	45
Gambar 4.26 test keamanan <i>login</i> menggunakan <i>wifi</i>	46
Gambar 4.27 test keamanan menggunakan <i>vpn zerotier</i>	47
Gambar 4.28 <i>Speedtest</i> sebelum menggunakan <i>vpn zerotier</i>	47
Gambar 4.29 <i>Speedtest</i> menggunakan <i>vpn zerotier</i>	48

DAFTAR LAMPIRAN

Lampiran 1. Surat Tugas Pembimbing Tugas Akhir

Lampiran 2. Lembar Konsultasi Bimbingan Tugas Akhir

Lampiran 3. Surat Ijin Penelitian

Lampiran 4. Lembar Wawancara

Lampiran 5. Dokumentasi Penelitian

Lampiran 6. Surat Tugas Penguji Sidang Tugas Akhir

Lampiran 7. Berita Acara Penilaian Sidang Tugas Akhir

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan era digital yang semakin maju, penggunaan jaringan komputer dan konektivitas internet telah menjadi salah satu elemen kunci dalam operasional sehari-hari perusahaan, institusi pendidikan, dan individu. Salah satu sektor yang penting adalah bidang sekretariat pada kantor Dinas Koperasi Usaha Kecil dan Menengah (UMKM). Dalam hal ini, perlindungan terhadap informasi dan data yang ada di dalam jaringan menjadi sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Oleh karena itu, kebutuhan akan jaringan yang andal, aman, dan skalabel menjadi semakin penting.

Sekretariat merupakan salah satu bidang yang ada di Dinas Koperasi Usaha Kecil dan Menengah (UMKM) Provinsi Kalimantan Tengah kota Palangka Raya. Bidang sekretariat melibatkan berbagai tugas administratif dan dukungan operasional yang mendukung kegiatan sehari-hari, salah satu yang dilakukan bidang sekretariat adalah menangani dokumen dan data yang bersifat rahasia. Oleh karena itu, implementasi *Virtual Private Network* (VPN) menjadi salah satu langkah esensial untuk melindungi data ini dari potensi ancaman keamanan dan akses yang tidak sah. Selain itu, dalam era kerja yang dinamis, dimana mobilitas karyawan menjadi hal umum, VPN memungkinkan akses jarak jauh dengan tetap menjaga keamanan.

Virtual Private Network merupakan jaringan *private* yang berjalan di jaringan publik. VPN memungkinkan siapa saja yang memiliki otorisasi khusus untuk mengakses jaringan internal dari luar melalui jaringan internet. Sehingga pengguna dapat mengakses sumber daya, data, dan memperoleh izin serta pengaturan yang sama seperti terhubung pada jaringan lokal di tempat (Dewi et al.,2020).

Namun, saat ini bidang sekretariat belum menerapkan jaringan VPN dan komputer yang berisi data-data penting yang bersifat rahasia masih rentan terhadap serangan seperti sniffing dan serangan siber lainnya. Hal ini tentunya menyebabkan beberapa permasalahan seperti pengaksesan data dan hak akses oleh pihak yang tidak berwenang, misalnya pemantauan dan penyadapan (Syawaludin M, 2019).

Berdasarkan permasalahan tersebut, muncul kebutuhan untuk mengimplementasikan jaringan *Virtual Private Network* (VPN) zerotier berbasis OpenWRT di bidang sekretariat dengan judul penelitian "Implementasi *Virtual Private Network* menggunakan Zerotier berbasis OpenWRT" di Bidang sekretariat pada Dinas Koperasi Usaha Kecil dan Menengah. Alasan penulis menggunakan VPN Zerotier dengan *Set Top Box* adalah untuk menggabungkan fungsi VPN sebagai keamanan komunikasi dengan tunneling yang terenkripsi dan zerotier yang memungkinkan akses *resource* dimanapun, dengan menggunakan STB OpenWRT penulis dapat melakukan hal-hal seperti memodifikasi pengaturan jaringan.

1.2. Perumusan Masalah

Berdasarkan dari latar belakang di atas masalah yang diangkat oleh penulis yaitu bagaimana cara mengimplementasi *Virtual Private Network* menggunakan Zerotier Berbasis OpenWRT di bidang sekretariat pada kantor Dinas Usaha Kecil dan Menengah Provinsi Kalimantan Tengah kota Palangka Raya.

1.3. Batasan Masalah

Dalam penelitian ini penulis memberikan batasan agar tidak menyimpang dari tujuan guna mendapatkan hasil yang optimal. Batasan masalah dalam penelitian ini adalah sebagai berikut :

- a. Implementasi *VPN* Zerotier menggunakan OpenWRT 23.05.0 Rc1 ini hanya mempermudah pengguna untuk menghubungkan perangkat atau jaringan secara aman melalui jaringan publik (internet) dan pengguna bisa mengakses dari jarak jauh selama ada jaringan internet.
- b. Perangkat yang digunakan yaitu *Set Top Box* (STB) B860H
- c. Tempat penelitian dilakukan di bidang Sekretariat.
- d. perangkat yang akan dihubungkan dengan Zerotier adalah *Access Point*, STB, dan Komputer/ laptop.
- e. Pengujian ini menggunakan Traceroute dan pengujian langsung akses perangkat yang ada di server zerotier.

1.4. Tujuan dan Manfaat

1.4.1. Tujuan

Tujuan penelitian ini adalah untuk melakukan implementasi *Virtual Private Network* menggunakan *Zerotier* Berbasis *OpenWRT* di bidang sekretariat pada kantor Dinas Usaha Kecil dan Menengah. Provinsi. Kalimantan Tengah Kota Palangka Raya.

1.4.2. Manfaat

a. Bagi penulis

Manfaat yang diperoleh dari penulis adalah dapat menerapkan ilmu yang telah dipelajari dan dapat menambah wawasan tentang pengimplementasian sebuah jaringan di bidang sekretariat pada kantor Dinas Usaha Kecil dan Menengah provinsi Kalimantan tengah.

b. Bagi pengguna

Penulisan tugas akhir ini memberikan manfaat bagi pengguna sebagai referensi dalam membangun suatu jaringan yang dapat mengakses *resource* dimanapun dan keamanan komunikasi dengan *tunneling* yang terenkripsi.

c. Bagi STMIK Palangkaraya

Manfaat yang diberikan kepada kampus STMIK Palangkaraya adalah sebagai penambah referensi judul tugas akhir yang tersedia di Perpustakaan Stmik Palangkaraya nantinya.

1.5. Sistematika Penulisan

Adapun sistematika penulisan dalam penulisan tugas akhir ini terdiri dari beberapa bab dan masing-masing bab membahas dan menguraikan pokok permasalahan yang berbeda, sebagai gambaran di sini penulis menyertakan garis-garis besarnya yaitu ;

BAB I PENDAHULUAN

Pada bagian bab ini di uraikan mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat, metode penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini menjelaskan teori-teori yang didapat dari sumber relevan untuk digunakan sebagai panduan dalam penelitian serta penyusunan tugas akhir.

BAB III METODE PENELITIAN

Bab ini berisikan tentang proses tahapan yang dilakukan oleh penulis dalam mengumpulkan data atau informasi yang diperlukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan tentang hasil implementasi dan juga hasil pengujian dari penelitian yang dilakukan oleh penulis, pada bab ini juga berisi tentang pembahasan dari implementasi yang telah dilakukan

BAB V KESIMPULAN DAN SARAN

Pada bab terakhir ini, penulis menjelaskan mengenai kesimpulan dari penelitian yang telah dilakukan oleh penulis, dan juga berisi saran kepada peneliti selanjutnya untuk melanjutkan penelitian yang ada

BAB II

LANDASAN TEORI

2.1 Kajian Teori

2.1.1. Implementasi

Implementasi merupakan tahapan yang sangat menentukan berhasil atau gagal nya suatu proyek yang akan dibangun (Chandra et al., 2021)

Implementasi yaitu suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara matang dan terperinci. Implementasi biasanya dilakukan setelah perencanaan sudah dianggap sempurna.

2.1.2. Jaringan Komputer

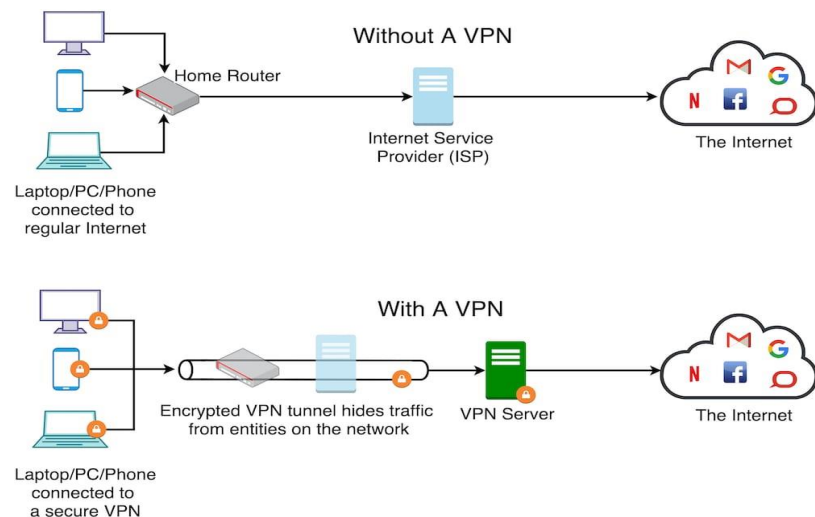
Jaringan komputer adalah komputer dalam jumlah besar yang saling terhubung dan mengerjakan kebutuhan komputasional disebuah organisasi. Dua komputer dianggap terhubung jika komputer tersebut dapat bertukar informasi (Sari, 2020).

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer, dalam bahasa populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer, dan perangkat lain seperti router, switch dan sebagainya. Alat yang bisa terhubung dengan satu lainnya untuk memudahkan memahami jaringan komputer para ahli sudah membagi beberapa klasifikasi,

seperti berdasarkan area atau skala, berdasarkan media penghantar, dan berdasarkan fungsi.

2.1.3. *Virtual Private Network (VPN)*

Menurut (Musril, 2019) *Virtual Private Network (VPN)* merupakan suatu bentuk private internet melalui *public network* (internet), dengan menekankan pada keamanan data dan akses global.



Gambar 2 1 Cara Kerja VPN

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan kita dapatkan hak dan pengaturan yang sama seperti halnya berada dalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. Berikut adalah beberapa protokol vpn:

1). PPTP (*Point-to-Point Tunneling Protokol*)

PPTP adalah protokol yang memungkinkan transfer data yang aman antara klien dan server menggunakan *VPN* berbasis IP (Pamungkas et al.,2021)

PPTP adalah protokol yang digunakan untuk melindungi transfer data dari client ke server melalui TCP/IP. Protokol ini mampu mengenkripsi data antar koneksi dengan cara merubah paket PPTP menjadi Ip

2). L2TP/IPsec (*Layer 2 Tunneling Protocol with IPsec*).

L2TP adalah standar yang memungkinkan lalu lintas Point-to-Point protokol dibawa antara jaringan yang berbeda. Protokol L2TP merupakan *tunneling* yang menggabungkan dua bagian *tunneling propriety*, yaitu Cisco L2F (Layer 2 Forwarding) dan PPTP (Point-to-Point Protokol) dari microsoft. L2TP dikombinasikan dengan IPSec, menyediakan *tunneling* keamanan dan lingkungan untuk Internet Protokol (IP), *Internet Packet Exchange* (IPX), dan protokol berbasis paket lainnya pada jaringan IP apapun (Pamungkas et al.,2021)

L2TP adalah gabungan dari dua buah protokol *tunneling* berbeda, yakni *Layer 2 Forwarding* (L2F) dan *Point-to-point Tunneling* Protokol (PPTP). Protokol ini digunakan untuk membuat *Virtual Private Dial Network* (VPDN) yang memungkinkan membawa semua jenis protokol komunikasi. Sebagai contoh, L2TP

sering dikombinasikan dengan protokol keamanan lain seperti IPSec untuk membangun koneksi VPN yang lebih aman.

3). OpenVPN

OpenVPN adalah salah satu VPN yang baru dan aman, untuk pengimplementasian masih jarang. Meskipun perlu menginstal software pihak ketiga. OpenVPN juga memiliki dua otentikasi mode yaitu *Static key* dan TLS. Perbedaannya, pada *static key* mode menggunakan *pre-shared key* yang dibagi antar dua pengguna sebelum proses *tunneling* dimulai. Pada mode TLS menggunakan *socket secure layer*, *transport layer security*, dan sertifikat untuk otentikasi dan pertukaran kunci (Rante,2016).

OpenVPN adalah sebuah protokol *open-source* yang biasanya digunakan untuk membangun koneksi *site-to-site* dan *point-to-point*. Jenis VPN yang menggunakan protokol ini umumnya memiliki sistem keamanan tradisional berdasarkan SSL dan TLS.

4). IPsec (Internet Protocol Security)

IPSec merupakan protokol yang digunakan untuk mengamankan transmisi datagram pada jaringan berbasis TCP/IP (Wicaksana,2021)

IPSec adalah jenis protokol yang dipakai untuk melindungi komunikasi dan transfer data melalui jaringan IP (Internet Protokol). Protokol ini bekerja dengan cara memverifikasi *session* sekaligus mengenkripsi semua paket data selama koneksi berlangsung. Selain

itu, IPSec merupakan metode yang digunakan untuk mengamankan IP datagram Ketika paket data ditransmisikan. Protokol ini bekerja pada *network layer* yang merupakan lapisan ketiga dalam model referensi jaringan OSI. Sehingga, setiap data pada layer di atasnya bisa diamankan.

5). SSTP (Secure Socket Tunneling Protocol)

SSTP adalah protokol yang berfungsi atau dirancang untuk melakukan proses *tunneling*. Keamanan data dalam hal ini menjadi prioritas utama, dengan adanya proses *enkapsulasi* dan *otentikasi* menjadikan *tunnel* sebagai salah satu dari banyak cara untuk mengamankan data dalam suatu jaringan (Hidayat,2019).

SSTP adalah protokol VPN populer untuk membuat terowongan VPN antara klien dan server. Biasanya digunakan untuk mengamankan akses jarak jauh ke jaringan pribadi melalui internet. Microsoft mengembangkan SSTP untuk menggantikan protokol PPTP dan L2TP/IPSec yang kurang aman. SSTP biasanya digunakan untuk melindungi koneksi VPN Windows asli.

6). WireGuard

WireGuard adalah VPN gratis dan *open source* yang bertujuan untuk menggantikan IPsec dan OpenVPN. Ini didasarkan pada protokol kriptografi baru yang berasal dari Noise Protokol Framework (Benjamin lipp et al.,2019).

WireGuard adalah protokol komunikasi sumber terbuka untuk menyiapkan Virtual Private Network (VPN) yang aman. Menggunakan kriptografi primitif tingkat lanjut untuk mengamankan data yang dipertukarkan, ia menyegelnya dalam terowongan terenkripsi. Meskipun awalnya dibangun di kernel Linux pada tahun 2015, sekarang tersedia secara gratis untuk berbagai sistem operasi.

Protokol ini dikembangkan oleh satu-satunya peneliti keamanan Jason Donenfeld, yang sedang bereksperimen dengan opsi yang ada. Karena kebanyakan memiliki kinerja yang buruk dan sulit diatur, kesimpulan yang wajar adalah menyederhanakan keseluruhan arsitektur. Oleh karena itu, WireGuard dimaksudkan untuk menjadi protokol VPN yang disederhanakan yang dapat mengungguli persaingan dan memberikan keamanan jaringan yang jauh lebih baik.

7). IKEv2/IPsec (Internet Key Exchange Version 2 with IPsec)

IKEv2 adalah protokol penerowongan, berdasarkan IPsec, yang membangun komunikasi VPN aman antara perangkat VPN dan menentukan proses negosiasi dan otentikasi untuk asosiasi keamanan IPsec (SA). Berbagai penyedia VPN menyebut kombinasi ini sebagai IKEv2/IPsec, atau IKEv2 VPN. IKEv2/IPsec adalah campuran dari protokol manajemen kunci (IKEv2) dan terowongan dan terowongan pengangkutan data (IPsec).

2.1.4. Zerotier

ZeroTier adalah solusi VPN yang dikembangkan pertama kali pada tahun 2011 oleh ZeroTier, Inc. ZeroTier itu sendiri masih dalam proses pengembangan dan memberikan penawaran antara penggunaan gratis dan juga berbayar. (Hadinata dkk, 2022)

ZeroTier adalah sebuah platform jaringan definisi perangkat lunak (SDN) yang menyediakan solusi VPN (*Virtual Private Network*) yang sederhana, aman, dan hemat biaya. VPN ZeroTier dirancang untuk menghubungkan perangkat atau komputer secara aman melalui Internet, seolah-olah mereka berada dalam jaringan lokal yang sama. (VPN). Ini memungkinkan akses yang aman dan *terenkripsi* ke sumber daya jaringan yang terletak di berbagai lokasi geografis.

Zerotier adalah salah satu solusi VPN yang menghadirkan kemudahan penggunaan dan manajemen yang tinggi. Dengan arsitektur jaringan *peer-to-peer* yang inovatif, Zerotier memungkinkan pembentukan jaringan pribadi dengan mudah dan aman tanpa harus menghadapi kerumitan konfigurasi jaringan tradisional.

Perlu di ketahui untuk dasar teori pada zerotier terdapat beberapa istilah-istilah jaringan pada zerotier (Setyawan,2023).

1. *Node*: ini adalah setiap perangkat yang terhubung ke jaringan ZeroTier. *Node* dapat berperan sebagai *PLANET (node pusat)*,

LEAF (*node* biasa), atau *RELAY* (*node* yang bertindak sebagai *relay* untuk perangkat lain).

2. *PLANET*: ini adalah *node* pusat dalam jaringan Zerotier. Ini bertanggung jawab untuk mengelola koneksi dan informasi tentang *node* lain dalam jaringan. Biasanya, ada beberapa *PLANET* dalam jaringan besar.
3. *LEAF*: ini adalah *node* biasa dalam jaringan Zerotier. *Node LEAF* terhubung ke *PLANET* untuk mendapatkan informasi tentang jaringan dan perangkat lainnya.
4. *RELAY*: ini adalah *node* yang bertindak sebagai *relay*. Jika dua perangkat tidak dapat berkomunikasi secara langsung (misalnya, karena alamat IP *internal* atau *firewall*), data dapat diarahkan melalui *node relay*.
5. *Address (ZT Address)*: setiap perangkat dalam jaringan Zerotier memiliki alamat unik yang disebut “*ZT Address*”. Alamat ini digunakan untuk mengidentifikasi perangkat dalam jaringan.
6. *Network*: ini adalah jaringan virtual yang dibuat menggunakan Zerotier. Semua perangkat yang terhubung dengan jaringan yang sama dapat berkomunikasi layaknya berada jaringan lokal yang sama.

2.1.5. OpenWRT

OpenWRT sistem adalah sistem operasi router berfitur lengkap dan mudah dimodifikasi yang ditulis dari awal. Itu adalah salah

satunya tiga firmware utama dari router utama. Ini adalah perangkat tertanam yang sangat modular dan sangat otomatis Sistem Linux dengan komponen jaringan yang kuat dan skalabilitas yang hanya mempertahankan yang terkait dengan jaringan fitur yang Anda inginkan tanpa menambah beban, yang menjadikan perangkat untuk komunikasi jaringan kecepatan komunikasi sangat meningkat, sangat cocok untuk pengembangan *gateway* (Jiang et al., 2019)

OpenWrt adalah sebuah sistem operasi berbasis Linux yang dirancang khusus untuk perangkat jaringan seperti router, *access point*, dan perangkat jaringan serupa. Ini adalah proyek sumber terbuka yang memungkinkan pengguna untuk mengganti perangkat lunak asli yang biasanya ada di perangkat jaringan mereka dengan sistem operasi yang lebih kuat dan fleksibel.

Reyre OpenWRT adalah sebuah firmware khusus untuk STB (*Set Top Box*) yang berbasis OpenWRT, sebuah sistem operasi Linux untuk perangkat jaringan. Reyre OpenWRT juga mendukung aplikasi Reyre STB OpenWRT apk, yang mempermudah pengguna untuk mengakses berbagai *firmware* melalui *smartphone* dan juga membantu dalam proses konfigurasi perangkat STB OpenWRT dan menawarkan antarmuka yang mudah dan menyeluruh. Aplikasi ini dikembangkan oleh Nobz, Lutfi Ibtihaji ilham, Ryan Fauzy, Gebang Kiidiw, STB OpenWRT dan DD WRT/OpenWRT Indonesia.

2.1.6. *Set Top Box* (STB)

Set Top Box (STB) adalah alat yang berisikan perangkat decoder yang berfaedah untuk mengatur saluran *televisi* yang akan diterima, selanjutnya dipilih sesuai kepentingan, dan juga decoder akan memeriksa hak akses pengguna atas saluran tersebut, selanjutnya akan memproduksi keluaran berupa gambar, suara, dan layanan lainnya (Ardiansyah et al.,2022).



Gambar 2.2 *Set Top Box*

Cara kerja *Set Top Box* ini yang melakukan pekerjaan satu arah dan juga bisa melakukan pekerjaan tanpa campur tangan manusia, STB bisa diberitahukan sebagai salah satu perangkat teknologi informasi. STB merupakan alat yang bisa ditanamkan *firmware* OpenWRT sehingga pengguna dapat melakukan pengaturan seperti menginstal aplikasi tambahan, memodifikasi pengaturan jaringan dan bahkan menjalankan perangkat sebagai server kecil.

2.1.7. Linux

Linux adalah sistem operasi yang bersifat *open source* dan bebas (*free*) di bawah lisensi GNU (GNU is not Unix) GPL (*General Public License*) . Arti kata *open source* adalah pada Linux kode sumber yang menjadi inti diikutsertakan dalam program sehingga dapat dilihat oleh siapa saja tanpa harus menandatangani suatu perjanjian khusus. Arti kata bebas atau *free* mengacu pada kebebasan bukan berarti bebas biaya. Linux bebas untuk diduplikasikan, dimodifikasi, dan disebarluaskan baik (Sampurno,2019)

Linux adalah sistem operasi berbasis GNU/Linux yang bersifat *open source* dan memiliki banyak varian seperti *Debian, Slackware, Open suce, Archlinux, Redhat* dan sebagainya. Walaupun sangat banyak varian GNU/Linux hanya menyediakan aplikasi yang sudah ditentukan yang mungkin kurang bermanfaat oleh pengguna sehingga hal ini mengakibatkan banyak pengguna yang melakukan *remastering* untuk memunuhi kebutuhannya. *Remastering* adalah proses membuat sistem operasi baru dengan mengurangi atau menambahkan fitur-fiturnya dari distro GNU/Linux yang telah ada.

2.2 Penelitian Relevan

Sub bab ini menguraikan penelitian yang relevan, penelitian sebelumnya yang memiliki topik serupa atau mendekati sama. Penulis menggunakan acuan kepustakaan yang bersumber pada penelitian sebelumnya. Hal ini berguna sebagai referensi bagi peneliti. Berikut tinjauan pustaka pada Tabel 2.1.

Tabel 2. 1 Tinjauan Pustaka

No	Penulis/ Tahun	Topik	Metode	Pembahasan	Hasil
1.	Suyoso, Y.A., & Yuliana / 2021	Analisa Penggunaan Jaringan ZeroTier di Masa Pandemi Covid-2019	Network Development Life Cycle (NDLC)	Penelitian ini menganalisis penggunaan jaringan ZeroTier sebagai solusi VPN selama bekerja dari rumah karena pandemi Covid-19.	Hasil penelitian menunjukkan bahwa penggunaan jaringan ZeroTier dapat meningkatkan keamanan dan privasi data dalam pertukaran informasi melalui jaringan internet.
2.	Theovan Gracia Stefana Putra & Indrastanti R. Widiarsari / 2022	Rancangan Virtual Private Server Pada Kantor Kelurahan Menggunakan ZeroTier	-	Penelitian ini membahas tentang bagaimana merancang sebuah jaringan VPN pada kantor kelurahan menggunakan ZeroTier	Dalam penelitian yang dilakukan, maka didapatkan sebuah kesimpulan bahwa Kantor Kelurahan Banyuanyar dapat menjalankan fungsi dan tugasnya dengan maksimal dengan memanfaatkan jaringan internet yang sudah terhubung keseluruhan desa ditambah terdapat 2 buah server virtual yang dibuat dan dijalankan di dalam ZeroTier yang dapat diterapkan sebagai VPS dan VPN. Penerapan Virtual Private Server ini bisa digunakan untuk segala jenis server dan dapat digunakan sesuai dengan kebutuhan dari Kantor Kelurahan Banyuanyar. Dengan penerapan virtualisasi dapat memberikan efisiensi biaya dan memberikan kinerja maksimal untuk menunjang pekerjaan di Kantor Kelurahan Banyuanyar karena Virtual Private Server dapat digunakan di dalam berbagai jenis perangkat dan sistem operasi. Penggunaan beberapa software seperti Syncthing dan ZtnCui juga memberikan kemudahan keamanan dalam segi akses dan berkirim data serta memberikan kenyamanan untuk para staf yang bekerja. Dengan memaksimalkan jaringan yang berada diseluruh desa Virtual Private Server ini dapat diakses oleh para staf dimana dan kapan saja tanpa rasa khawatir dengan keamanan yang ada.
3.	Rodolfo Bruno Hecht dkk, / 2021	Analisis kelayakan akses jarak jauh ke	Network Development	Penelitian ini membahas tentang bagaimana menganalisis kelayakan akses jarak jauh ke jaringan nirkabel industri melalui vpn	Hasil penelitian ini menunjukan pekerjaan yang dilator belakang oleh salah satu kebutuhan utama jaringan industri, yaitu melakukan pengendalian dan pemantauan

No	Penulis/ Tahun	Topik	Metode	Pembahasan	Hasil
		jaringan nirkabel industri melalui VPN	Life Cycle (NDLC)		jaringan industri dengan cara yang aman, menganalisis skenario latensinya Ketika jaringan diakses jarak jauh. Sebagai cara untuk mengatasi masalah ini, diusulkan akses jarak jauh menggunakan vpn yang disediakan SDN, menghubungkan host jarak jauh yang di pasang secara geografis jauh dari jaringan industri, ke gerbang industri yang di pasang di laboratorium.
4.	Saul Andres Sanchez Gutierres / 2022	Implementasi VPN dengan Zerotier one untuk pengelolaan sumber Daya Jaringan Server file di perusahaan konsultan	Top Down	Penelitian ini membahas tentang bagaimana pengelolaan sumber daya jaringan Server file di perusahaan	Hal ini menunjukan bagaimana penerepan jaringan pribadi virtual Zero Tier One meningkatkan kinerja akses terhadap informasi dan memfasilitasi pengelolaan sumber daya.
5.	Andy Setyawan/2023	Remote Access pada Jaringan lokal Menggunakan VPN Zerotier	-	Penelitian ini membahas tentang bagaimana mengimplementasikan solusi remote access pada jaringan lokal rumah untuk menghubungkan jaringan kantor dengan jaringan rumah secara aman	Hasil penelitian ini menunjukan bahwa penggunaan jaringan yang berbeda bisa dilakukan secara aman dengan menggunakan VPN Zerotier

BAB III

METODOLOGI PENELITIAN

3.1. Tinjauan Umum

Tempat yang dijadikan penelitian untuk mengimplementasikan penelitian penulis dilakukan pada bidang sekretariat Dinas Koperasi Usaha Kecil dan Menengah, beralamat Jl. Willem A. Samad No. 7, Menteng, Kecamatan Jekan Raya, Kota Palangka Raya, Kalimantan Tengah.

Perangkat yang tersedia di bidang sekretariat terdapat 1 acces point, 1 printer dan 1 komputer.

3.2. Jenis Penelitian

Menurut Prof. Dr. Nana Syaodih Sukmadinata dalam bukunya Metode Penelitian dan Pendidikan, beliau menyebutkan bahwa Penelitian dan Pengembangan atau *Research and Development (R&D)* adalah suatu proses atau langkah-langkah untuk mengembangkan suatu produk baru, yang dapat dipertanggungjawabkan.

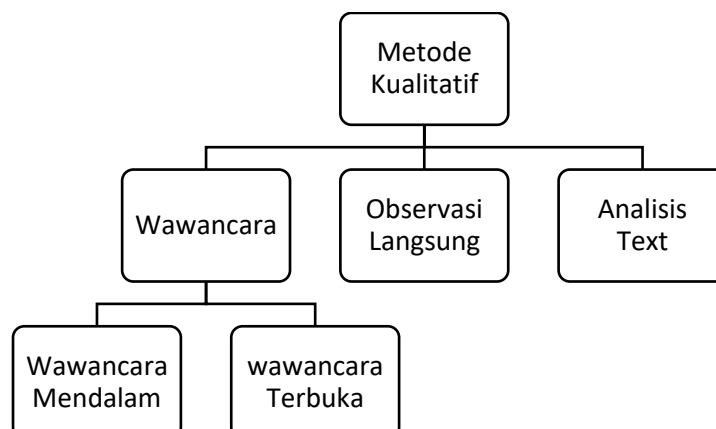
Penelitian pengembangan *Research and Development (R&D)* adalah jenis penelitian yang digunakan untuk mengembangkan sistem tertentu dan menguji keefektifan sistem tersebut. Peneliti melakukan pengembangan berupa sistem jaringan yang berfungsi untuk mempermudah pekerjaan yang dilakukan melalui jaringan secara aman.

3.3. Desain Penelitian

Penulis menggunakan desain penelitian Kualitatif karena menggunakan model-model matematik, statistik atau komputer. karena

beorientasi pada teori yang telah ada sebelumnya. Data yang diambil harus memenuhi syarat-syarat data yang baik, yaitu (1) data harus akurat; (2) data harus relevan; (3) data harus uptodate. Metode penelitian kualitatif biasanya dilakukan dengan cara wawancara, observasi dan analisis teks.

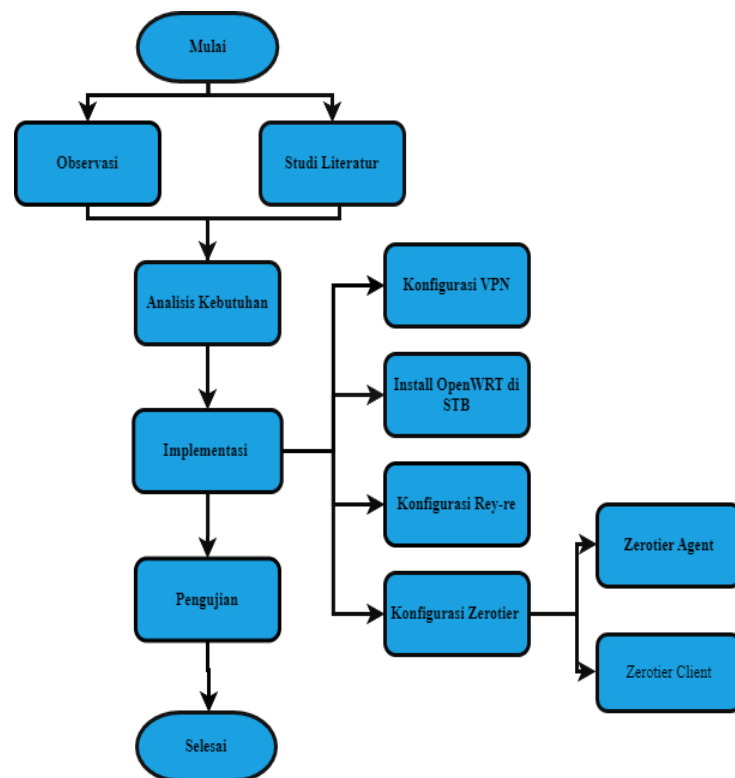
Metode kualitatif terdiri dari tiga cara pengumpulan data: (1) wawancara mendalam, wawancara dengan format pertanyaan terbuka; (2) observasi langsung; dan (3) pemanfaatan dokumen tertulis, termasuk sumber-sumber tertulis dari hasil wawancara terbuka pada kuesioner dan catatan program. Data wawancara biasanya didapatkan dari kutipan langsung dari responden tentang pengalaman, opini, perasaan dan pengetahuannya. observasi terdiri dari deskripsi yang mendalam tentang kegiatan suatu kegiatan. dokumen tertulis berasal dari kutipan-kutipan yang dianalisis, atau berupa hasil rekaman, surat menyurat, laporan resmi, hasil survei, dan lain sebagainya.



Gambar 3.1 Bagan Alur

3.3.1 Desain Proses Penelitian

Pada desain proses, penulis mendeskripsikan proses dari sistem dimana dalam pendeskripsikan ini penulis menggunakan flowchart, sehingga memudahkan penulis dan pembaca dalam memahami proses awal sampai dengan penyelesaian konfigurasi *Virtual Private Network* menggunakan Zerotier berbasis OpenWRT seperti pada gambar berikut.



Gambar 3.2 Flowchart Alur Penelitian

Penjelasan alur pada gambar di awali dengan mulai lalu proses selanjutnya peneliti melakukan observasi pada Dinas Koperasi Usaha Kecil dan Menengah Provinsi Palangka Raya dan studi literatur dengan mencari referensi jurnal dengan judul yang

menyerupai. Lalu melakukan analisis kebutuhan guna untuk mengetahui apa saja yang diperlukan sebelum melakukan implementasi. Proses pertama yang dilakukan dalam implementasi adalah melakukan konfigurasi VPN, lalu Install OpenWRT di STB, setelah itu penulis melakukan konfigurasi Rey-re dan melakukan konfigurasi zerotier. Ketika penulis selesai melakukan konfigurasi zerotier *client* ke zerotier *server*. selanjutnya, penulis melakukan tahap pengujian dengan cara melakukan *Sharing folder* antar komputer, melakukan pengujian *Protocol http*, melakukan pengujian *Traceroute* sebelum dan sesudah meangaktifkan zerotier, pengujian *ip publik* dengan vpn lain, pengujian keamanan menggunakan *wireshark*, dan pengujian *speedtest*.

3.4. Instrumen Penelitian

Dalam melakukan penelitian yang berjudul Implementasi *Virtual Private Network* menggunakan Zerotier berbasis OpenWRT pada bidang sekretariat, penulis menggunakan beberapa metode pengumpulan data, yaitu sebagai berikut :

a. Metode Kepustakaan

Penulis mengumpulkan data melalui beberapa media kepustakaan seperti buku, jurnal dan lain-lain yang digunakan sebagai sumber referensi penulis dalam melakukan penelitian.

b. Metode Observasi

Penulis melakukan pengamatan secara langsung ke lokasi penelitian yaitu Dinas Koperasi Usaha Kecil dan Menengah Provinsi Kalimantan Tengah kota Palangka Raya untuk memperoleh data yang diinginkan.

c. Metode Wawancara

Penulis mengumpulkan data dengan melakukan wawancara atau proses tanya jawab untuk mendapatkan data pendukung penelitian yang dilakukan penulis. Pada tahap ini penulis melakukan wawancara kepada bapak Eddy Jonathan selaku staff bidang sekretariat mengenai perangkat dan jaringan yang ada guna mengumpulkan informasi yang diperlukan dalam penelitian.

3.5. Analisis Kebutuhan

Kebutuhan yang digunakan dalam penelitian ini sebagai berikut.

3.5.1. Kebutuhan perangkat keras

- a. Laptop Lenovo KI5DJ09, Prosesor AMD A4-9 RADEON R3, 4 COMPUTE CORES 2C+2G
- b. *Set Top Box* B860H
- c. Modem
- d. *Micro SD 8GB* dan *Card Reader*

3.5.2. Kebutuhan perangkat lunak

- a. Sistem Operasi Windows 10 *Home Single Language*,
- b. OpenWRT 23.05,0-rc3 dengan v23.05.2 dan Reyre Clash-Wall 23.08.23, memungkinkan pengguna untuk mengoptimalkan

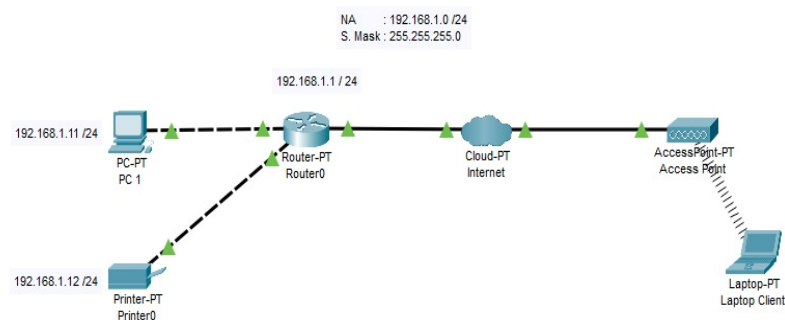
dan menyesuaikan konfigurasi perangkat router sesuai kebutuhan.

- c. Zerotier versi 1.12.2 , untuk melakukan akses jarak jauh.

3.6. Desain

3.6.1. Desain Perangkat

Desain perangkat ini gambaran posisi perangkat dalam jaringan yang ada pada Dinas Koperasi Usaha Kecil dan Menengah Provinsi Kalimantan Tengah kota Palangka Raya. Pada desain ini belum di terapkannya tahap implementasi. Berikut desain perangkat dapat dilihat pada gambar berikut.

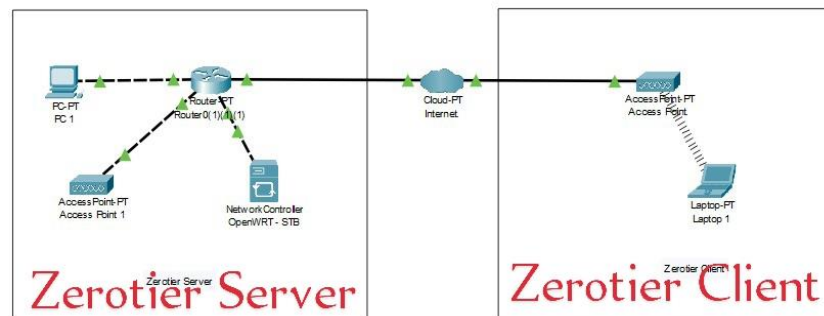


Gambar 3.3 Desain perangkat

Pada gambar 3.3 laptop client tidak bisa mengakses ke router yang terhubung ke perangkat lain karena memiliki jaringan yang berbeda.

3.6.2. Desain Usulan Implementasi Perangkat

Berikut perencanaan desain perangkat yang diusulkan pada Dinas Koperasi Usaha Kecil dan Menengah Provinsi Kalimantan Tengah kota Palangka Raya. Berikut bisa dilihat pada gambar berikut.



Gambar 3.4 Desain Usulan Perangkat

Pada gambar 3.4 komputer *client* sudah bisa mengakses ke komputer *server* yang terhubung ke perangkat lain dengan lokasi yang berbeda dan *netwrok* yang berbeda menggunakan *STB OpenWRT* yang sudah di konfigurasi zerotier.

BAB IV

HASIL DAN PEMBAHASAN

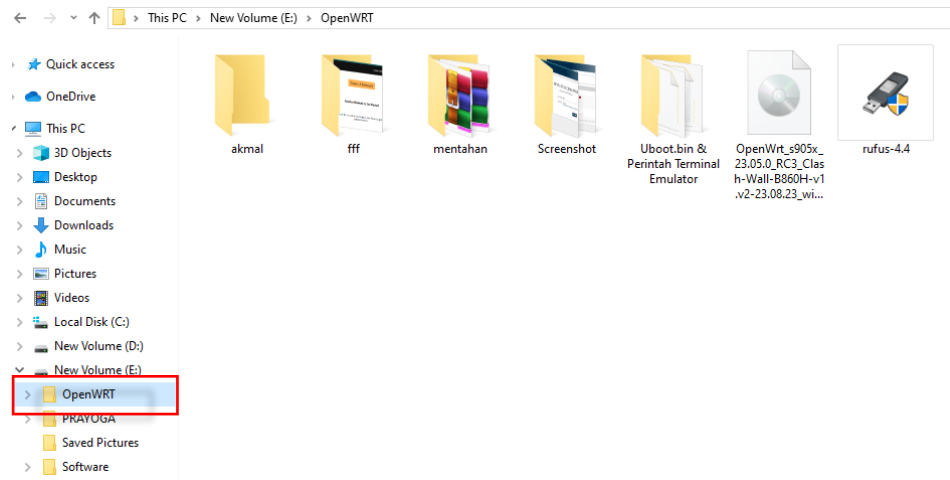
4.1 Hasil

Hasil dari penelitian ini merupakan sebuah implementasi jaringan *Virtual Private Network Zerotier* berbasis *OpenWRT* yang memungkinkan pengguna melakukan akses remote jarak jauh dengan jaringan yang berbeda, serta setelah dilakukan implementasi maka dilakukan pengujian akses dan pengujian routing yang ada, antara lain adalah pengujian *sharing folder*, *protocol http*, *traceroute*, pengujian *ip publik* dengan vpn lain, pengujian keamanan menggunakan *wireshark*, dan pengujian *speedtest*.

4.1.1 Implementasi

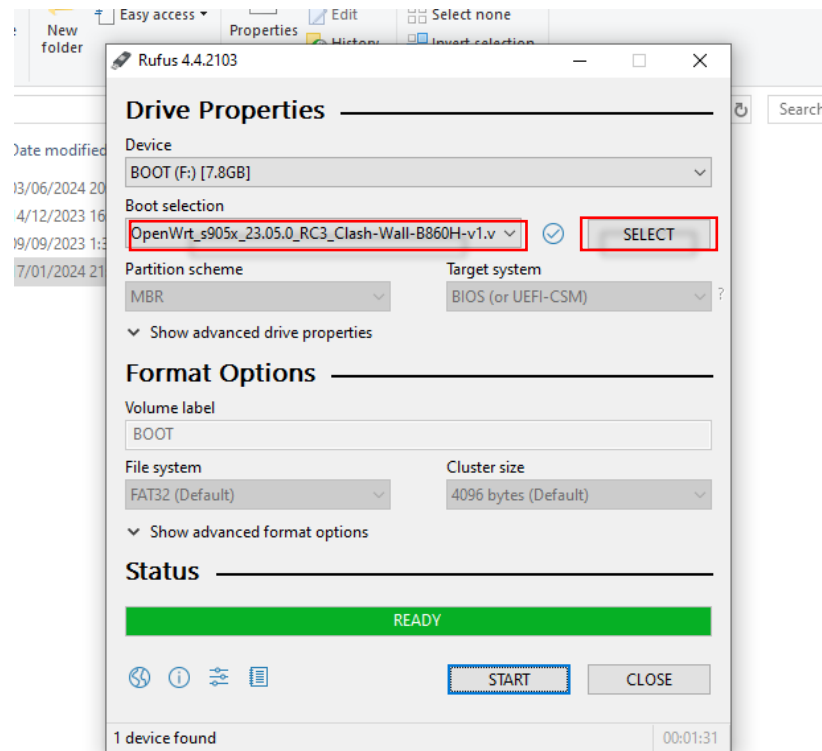
a. Install OpenWRT

Untuk dapat melakukan penginstalan OpenWRT pada STB, pertama-tama buat folder khusus untuk file firmware OpenWRT dan siapkan *file firmware* OpenWRT pada folder yang telah dibuat seperti pada Gambar 4.1.



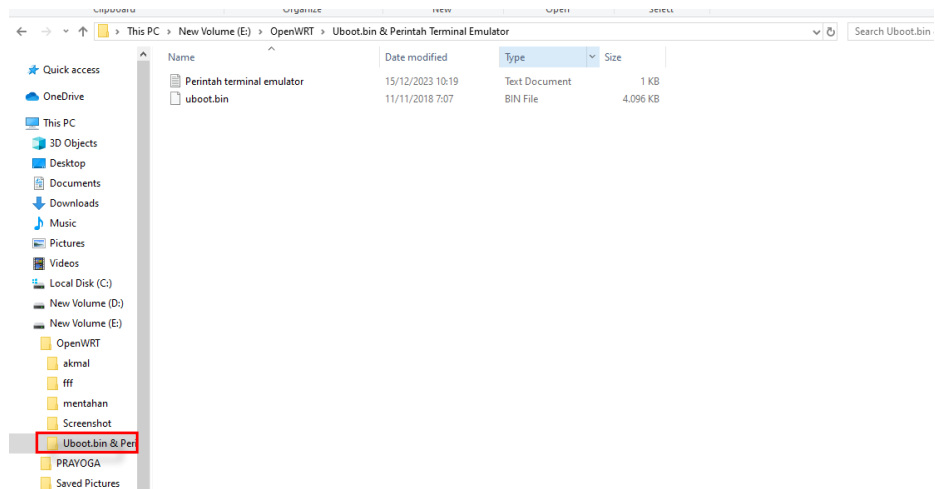
Gambar 4.1 Folder OpenWRT

Setelah itu pasangkan *Micro SD* pada *Card Reader* dan hubungkan ke laptop. lalu buka aplikasi rufus klik bagian *select* dan pilih *file firmware* OpenWRT lalu klik star pada aplikasi rufus dan tunggu hingga selesai seperti pada Gambar 4.2.

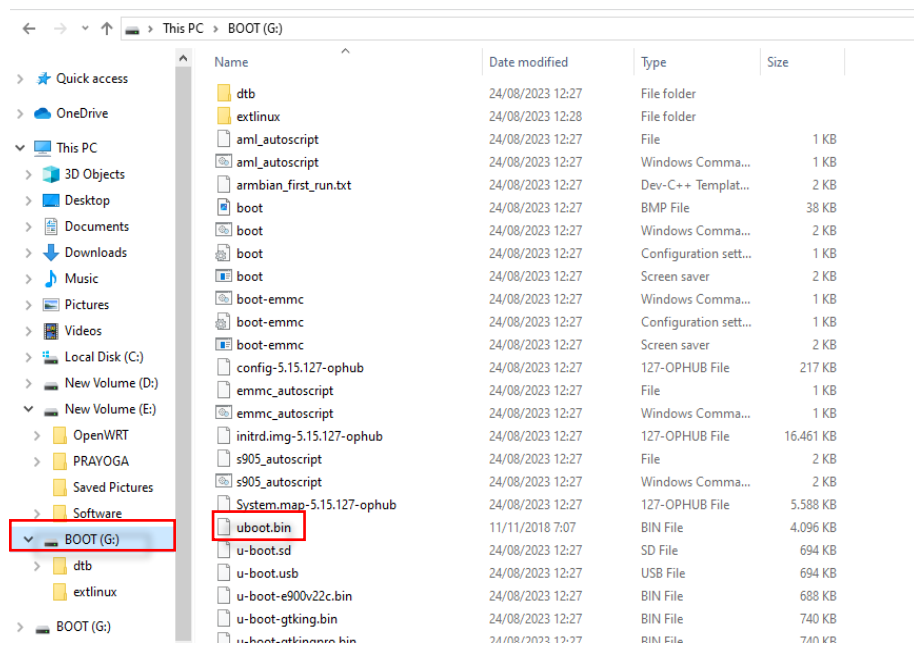


Gambar 4.2 Boot *Microsd* menggunakan Rufus

Setelah itu pindahkan file dengan nama uboot.bin yang ada di folder OpenWRT ke *microsd* yang sudah di boot seperti pada Gambar 4.3 dan Gambar 4.4, lalu cabut *microsd* pada *card reader* dan masukan *microsd* pada STB (*Set Top Box*).



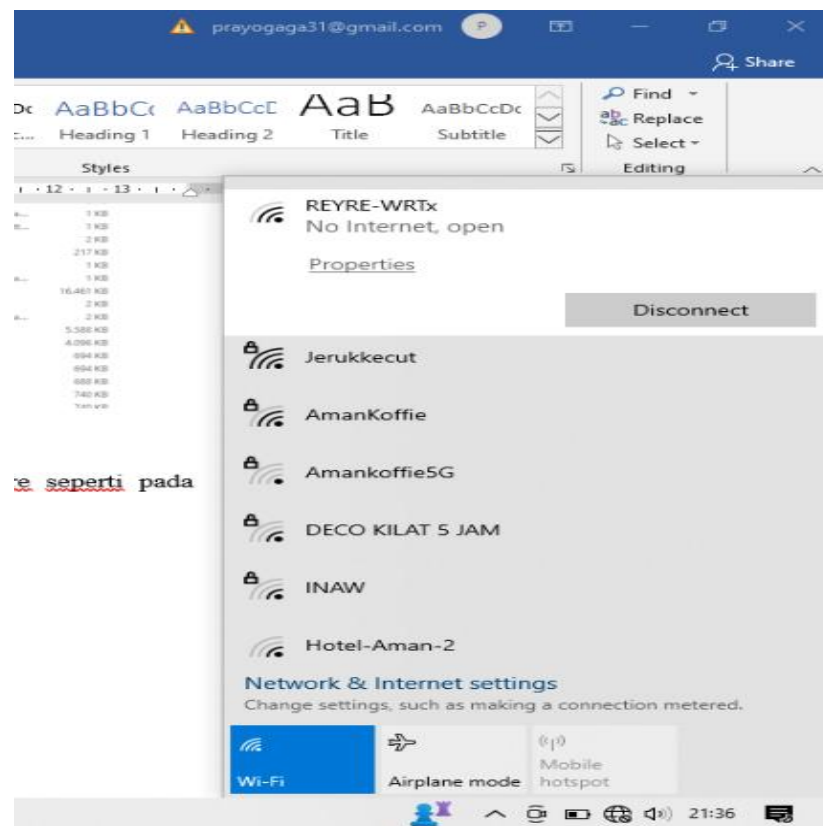
Gambar 4.3 File Uboot.bin



Gambar 4.4 File OpenWRT yang diboot di MicroSD

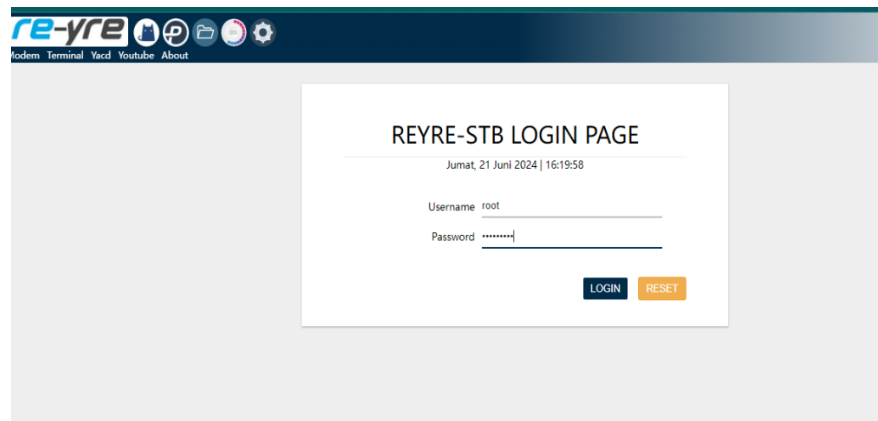
b. Konfigurasi Reyre

Koneksikan laptop/pc ke STB menggunakan wifi Reyre seperti pada Gambar 4.5.



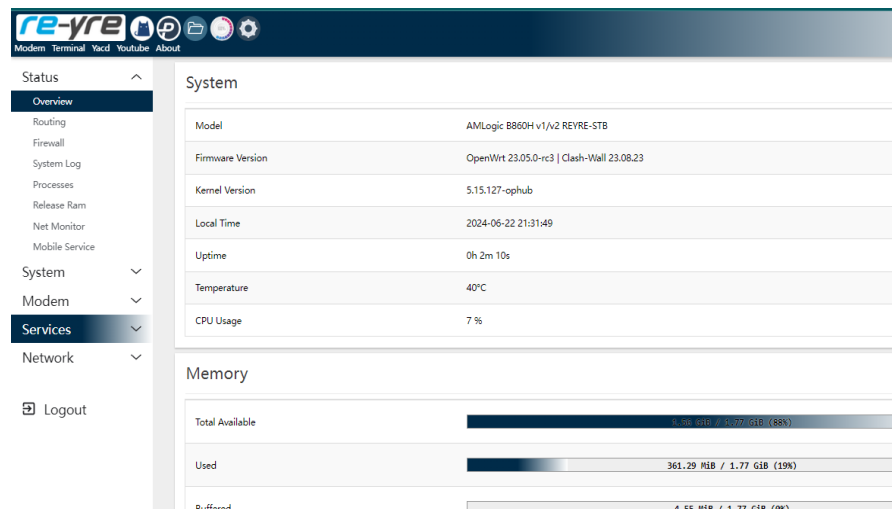
Gambar 4.5 Wifi STB

Lalu buka browser dan ketikkan alamat Ip 192.168.1.1 setelah itu akan muncul halaman *login*, masukan *username* dan *password* seperti pada Gambar 4.6.



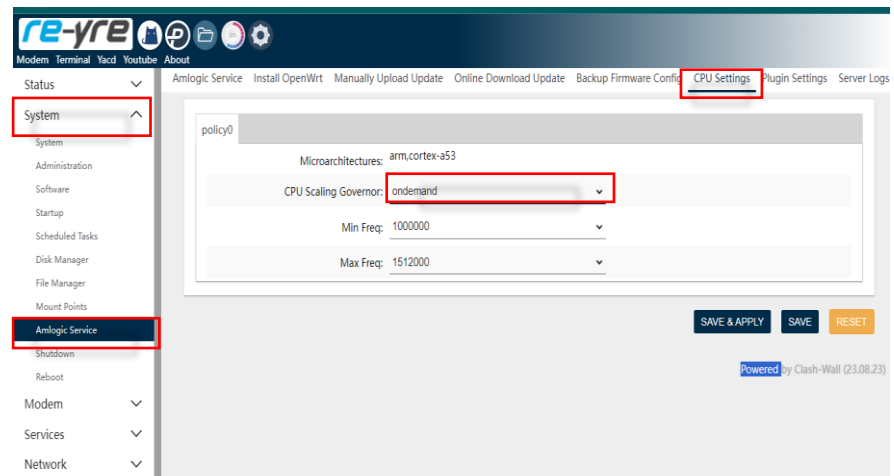
Gambar 4.6 Halaman Login STB

Setelah itu akan masuk ke dalam halaman *website* seperti pada Gambar 4.7.



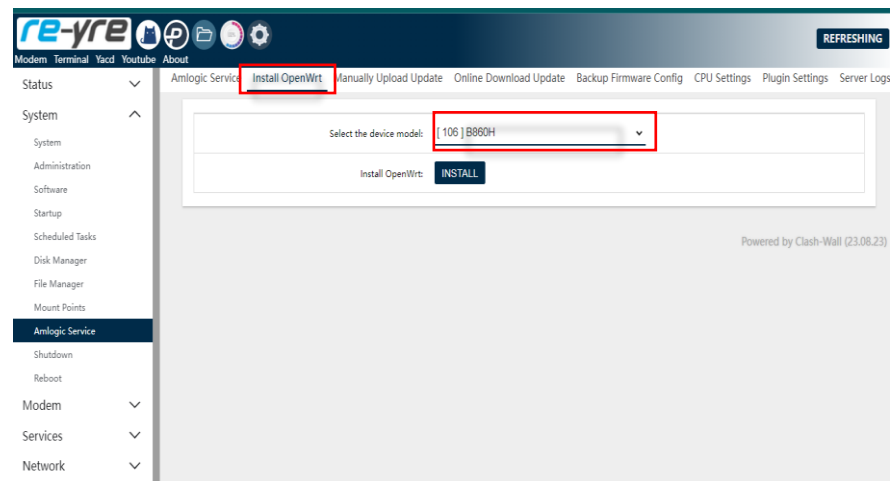
Gambar 4.7 Tampilan OpenWRT

Setelah itu masuk ke bagian *system* pilih *Amlogic service* lalu pilih bagian *cpu setting* seperti pada gambar berikut. selanjutnya pilih bagian *install openwrt* dan klik *install* seperti pada Gambar 4.8.



Gambar 4.8 Tampilan menu *System* OpenWRT

Selanjutnya pilih bagian *Install Openwrt* dan pilih *Select device* sesuai dengan *type* STB yang digunakan dan klik *install* seperti pada Gambar 4.9.

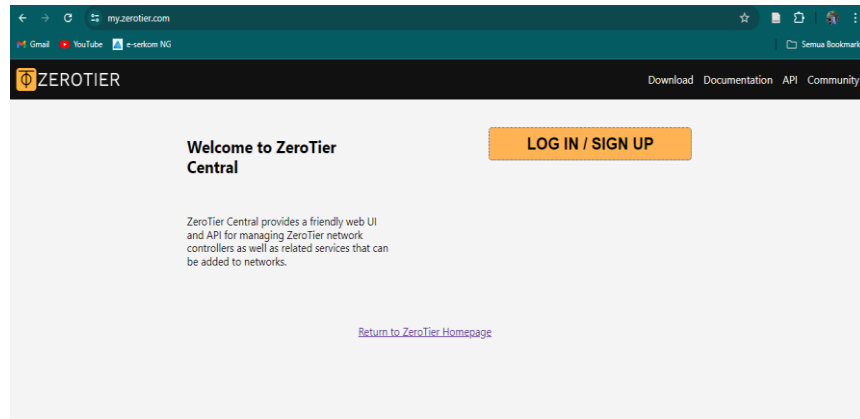


Gambar 4.9 Tampilan menu *System OpenWRT*

c. Konfigurasi Zerotier

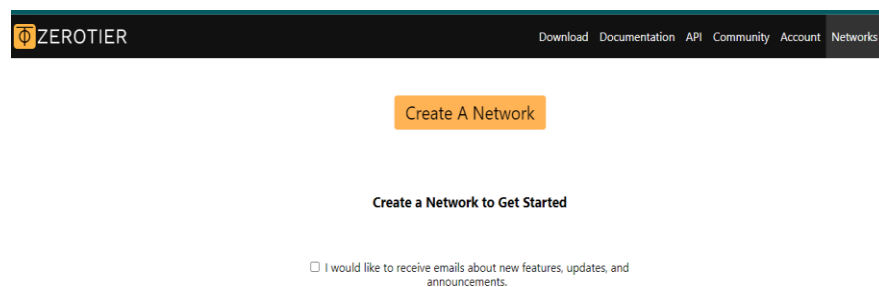
1). Zerotier Server

Untuk melakukan konfigurasi Zerotier pertama buka *website* zerotier pada *browser* lalu lakukan *login* seperti pada Gambar 4.10.



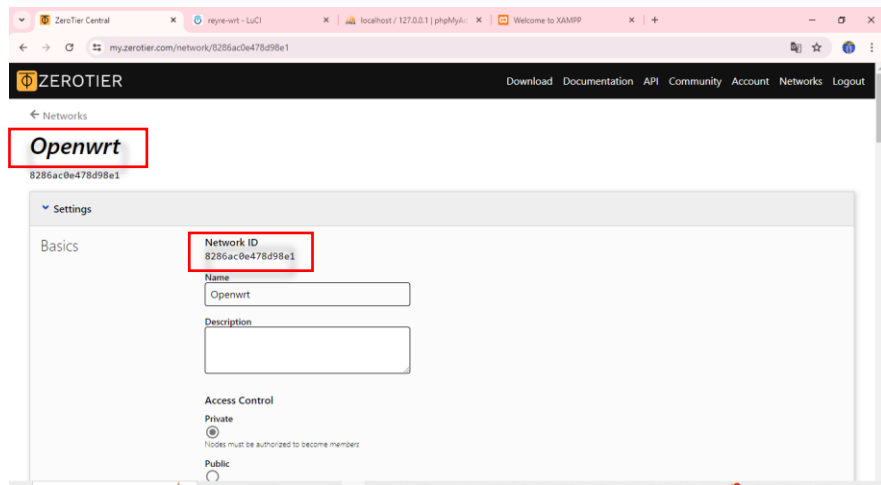
Gambar 4.10 Halaman *Login Zerotier Server*

Setelah itu *klik* bagian *create network* untuk mendapatkan *network id* dari Zerotier seperti pada Gambar 4.11.

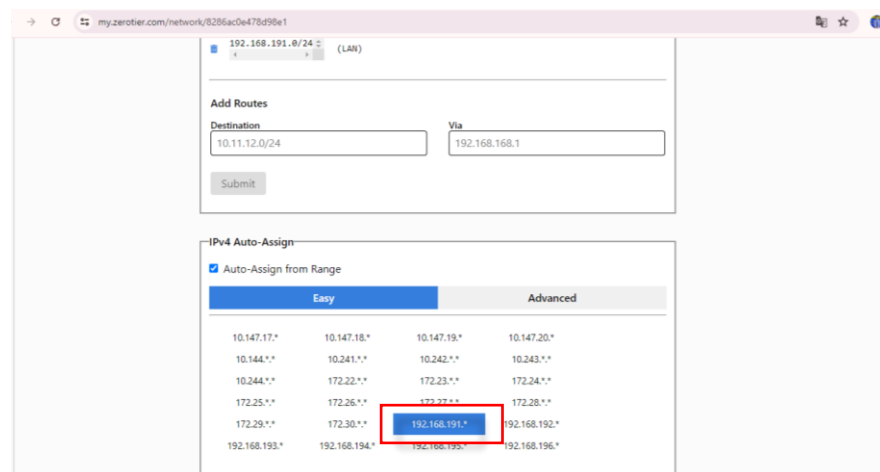


Gambar 4.11 Buat *Network Zerotier Server*

Setelah mendapatkan *network id* dari zerotier ubah nama sesuai pengguna, lalu pilih ip sesuai dengan kebutuhan seperti pada Gambar 4.12 dan Gambar 4.13.

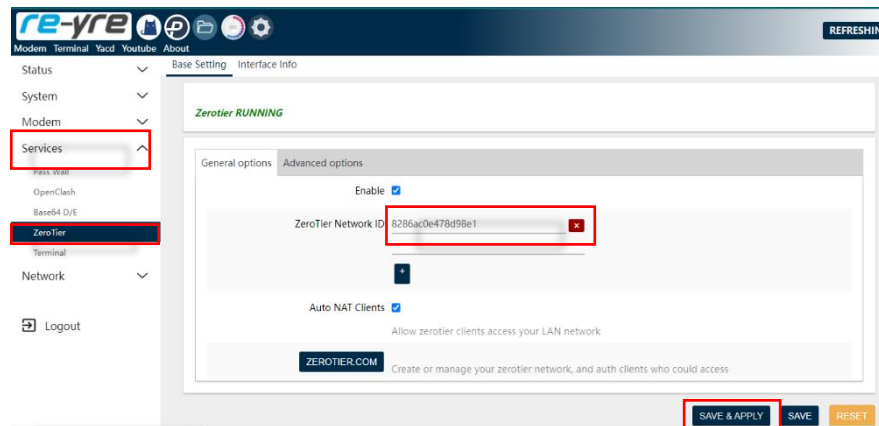


Gambar 4.12 Network Zerotier Server



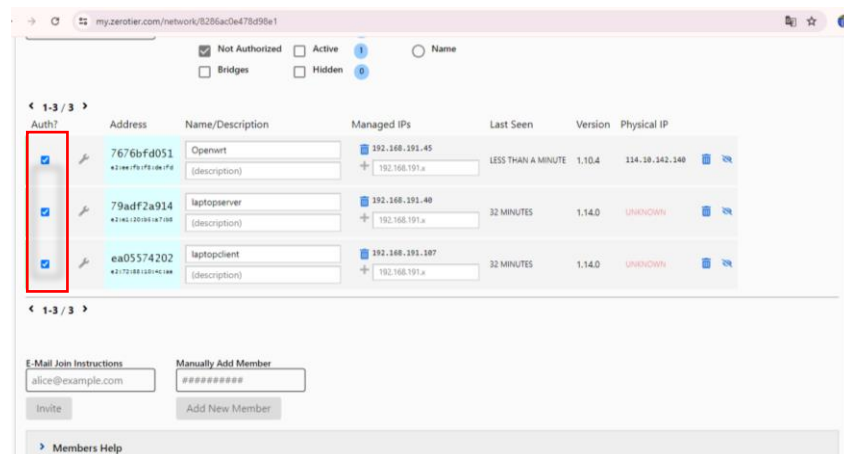
Gambar 4.13 IP Zerotier Server

Setelah itu masuk ke Reyre buka bagian *servis* pilih *zerotier* dan masukan *Network Id* dari *Zerotier* lalu *save and apply* seperti pada Gambar 4.14



Gambar 4.14 *Network ID Zerotier pada Zerotier*

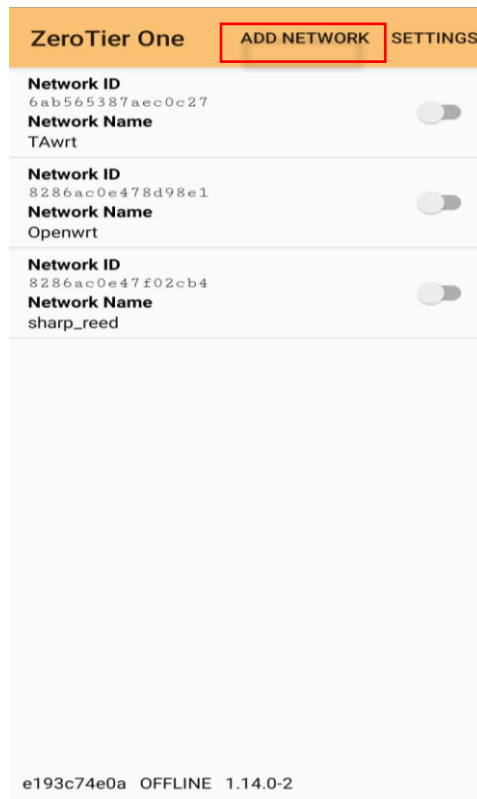
Kemudian akan muncul *network address* perangkat yang akan di hubungkan dengan zerotier dan ceklis perangkat mana saja yang diinginkan untuk terhubung seperti pada gambar 4.15.



Gambar 4.15 *Network Address perangkat Zerotier Server*

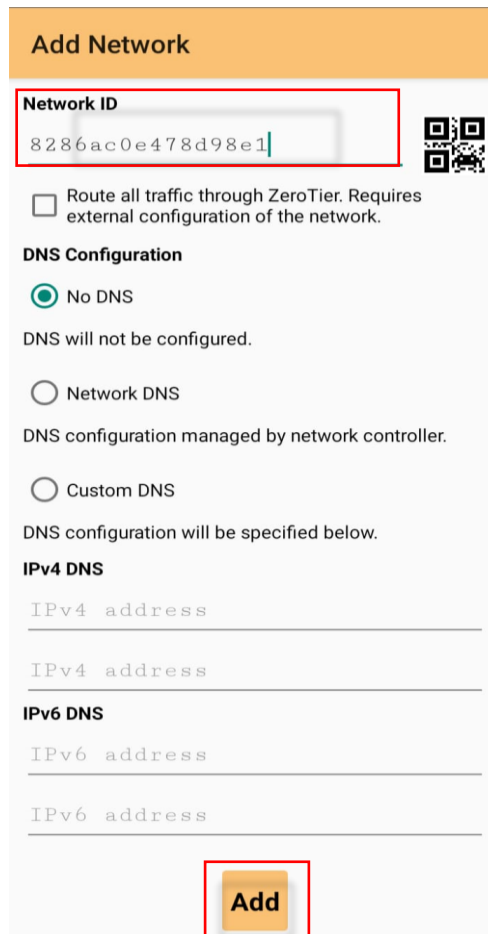
2. Zerotier Client

Masuk ke aplikasi Zerotier yang telah diinstal di *laptop* dan *smartphone* dan klik *add network* seperti pada Gambar 4.16.



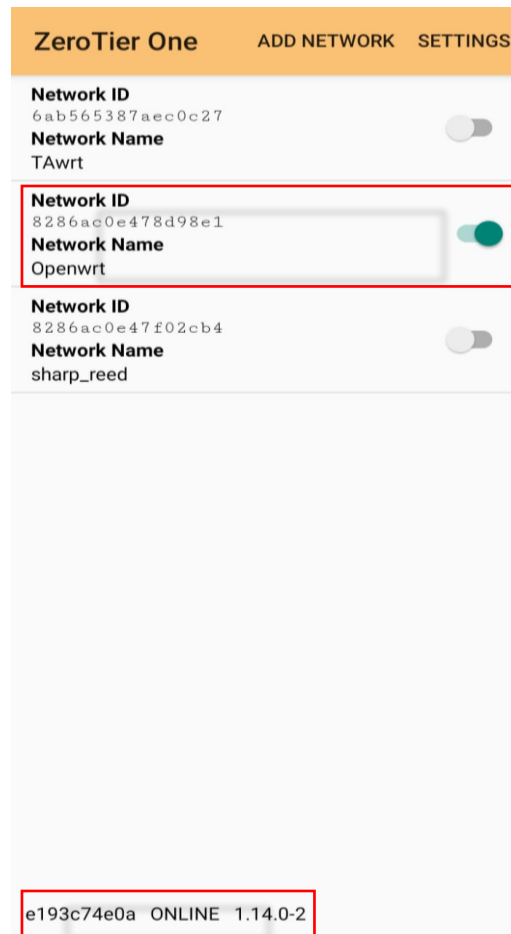
Gambar 4.16 Zerotier Client join Network Zerotier Server

Setelah itu masukan Network id dari Zerotier server dan klik Add seperti pada Gambar 4.17.



Gambar 4.17 *Add Network ZeroTier Server*

Setelah itu klik tombol on pada samping *network* dan apabila berhasil terkoneksi ke ZeroTier *server* maka akan muncul tulisan *online* seperti gambar 4.18.



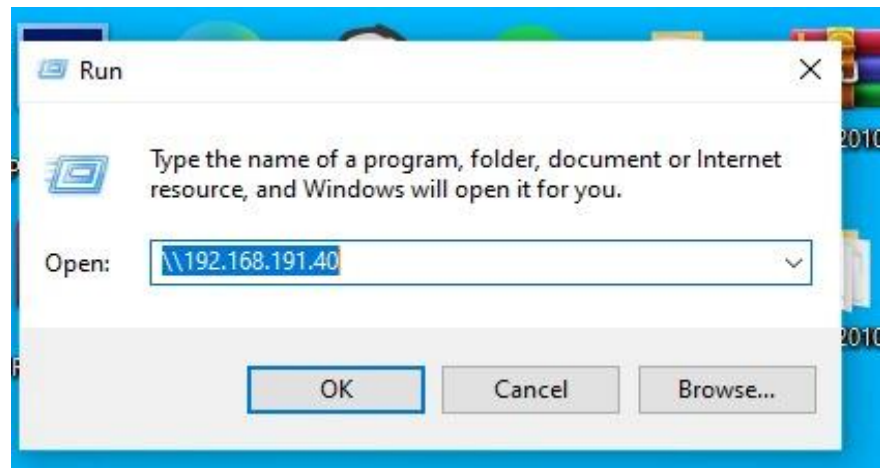
Gambar 4.18 Zerotier client terhubung dengan Zerotier Server

4.1.2 Pengujian

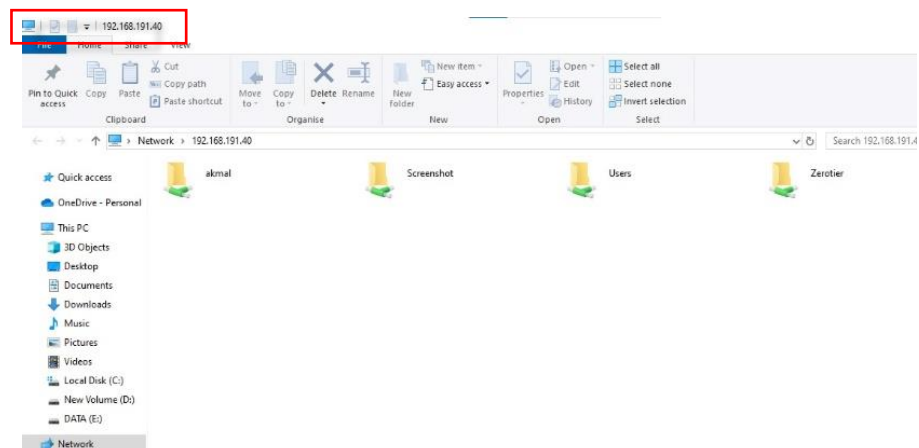
a. *Sharing folder*

Setelah melakukan implementasi maka dilakukan pengujian untuk mengetahui apakah implementasi *VPN* Zerotier berbasis OpenWRT berhasil atau gagal, yang pertama adalah melakukan pengujian dengan melakukan *Sharing Folder* antar komputer *server* dan komputer *client* dengan jaringan yang berbeda apakah berhasil atau gagal. Berdasarkan hasil pengujian yang dilakukan oleh penulis, maka pengujian *sharing folder* berhasil meski komputer *server* dan

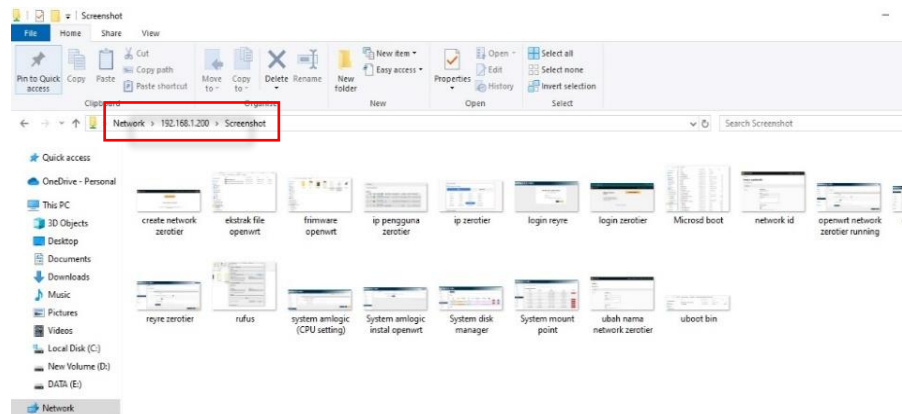
komputer *client* menggunakan dua jaringan yang berbeda. Karena komputer *client* yang digunakan sudah terhubung dengan jaringan *VPN Zerotier server*. Untuk hasil *Sharing Folder* antar komputer dilihat pada Gambar 4.19, Gambar 4.20 dan Gambar 4.21.



Gambar 4.19 Akses kekomputer server



Gambar 4.20 Tampilan *Sharing Folder*



Gambar 4.21 Isi dari *sharing folder*

b. Protocol *http*

Pengujian yang kedua adalah melakukan pengujian *protocol http* dimana komputer *client* melakukan akses ke komputer *server* yang menuju ke halaman *xampp* yang ada di komputer *server*, dimana pengujian ini dilakukan agar mengetahui apakah komputer *client* bisa mengakses halaman *xampp* yang sama walau dengan jaringan yang berbeda, apabila komputer *client* dapat melakukan akses seperti pada gambar 4.22 dibawah ini, berarti pengujian akses *xampp* dari komputer *client* ke komputer *server* dapat dikatakan berhasil.



Gambar 4.22 Halaman *xampp server* yang diakses di komputer *client*

c. *Traceroute*

Pengujian yang ketiga adalah melakukan pengujian *traceroute* dimana pengujian ini dilakukan agar mengetahui apakah komputer *client* yang sudah terkoneksi ke zerotier dapat terhubung dengan komputer *server*. oleh karena itu penulis melakukan pengujian *test ping* dari komputer *client* ke komputer *server* bertujuan untuk mengetahui apakah sudah saling terhubung antar komputer. Berdasarkan hasil pengujian yang dilakukan penulis, bahwa komputer *server* dan komputer *client* sudah terhubung melalui jaringan zerotier seperti pada Gambar 4.23.

```
C:\Users\ASUS>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.200: bytes=32 time=12ms TTL=128
Reply from 192.168.1.200: bytes=32 time=9ms TTL=128
Reply from 192.168.1.200: bytes=32 time=15ms TTL=128
Reply from 192.168.1.200: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 15ms, Average = 10ms

C:\Users\ASUS>
```

Gambar 4.23 Komputer *Client ping Server*

1. Pengujian Traceroute

Tabel 4.1 pengujian pada cmd

No.	Hop route sebelum mengaktifkan Zerotier	Hop route sesudah mengaktifkan Zerotier	Tujuan
1.	140.213.10.79	140.213.10.79	Detik.com
2.	192.168.1.1	192.168.1.1	
3.	192.168.18.1	192.168.18.1	
4.	10.2.0.1	10.2.0.1	

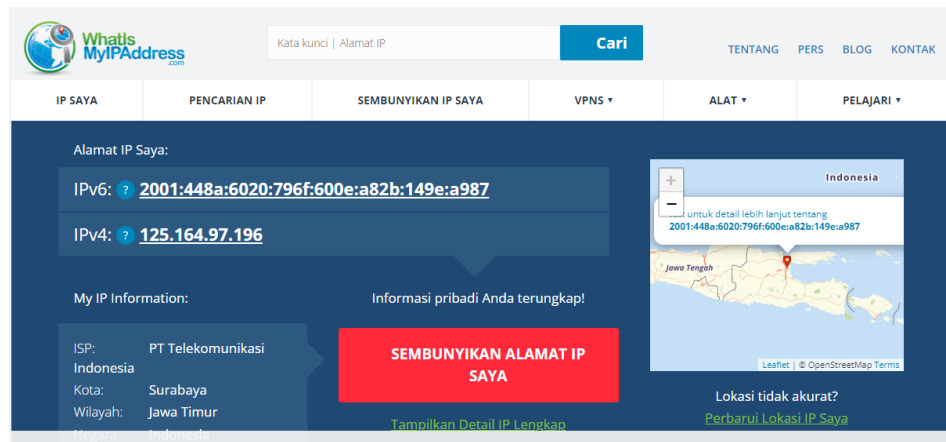
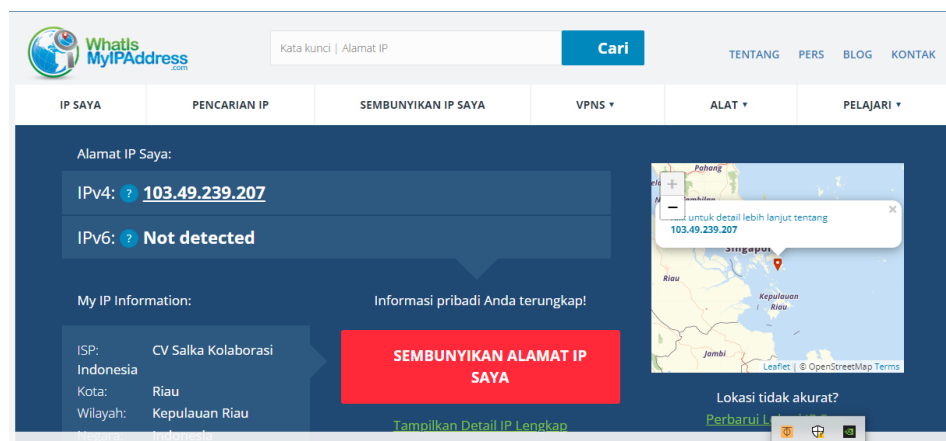
2. pengecekan IP Publik

Tabel 4.2 Pengujian pada *tools Whatis MyIp Address*

No.	IP Publik sebelum mengaktifkan Zerotier	IP Publik sesudah mengaktifkan Zerotier	Ip Publik sesudah mengaktifkan VPN lain
1.	125.164.97.196	125.164.97.196	103.49.239.207

d. pengujian Ip publik dengan Vpn Zerotier dan Vpn lain

Pengujian yang keempat adalah pengujian pengecekan ip publik menggunakan tools Whatis MyIP Address dengan menggunakan Vpn Zerotier dan Vpn lain.

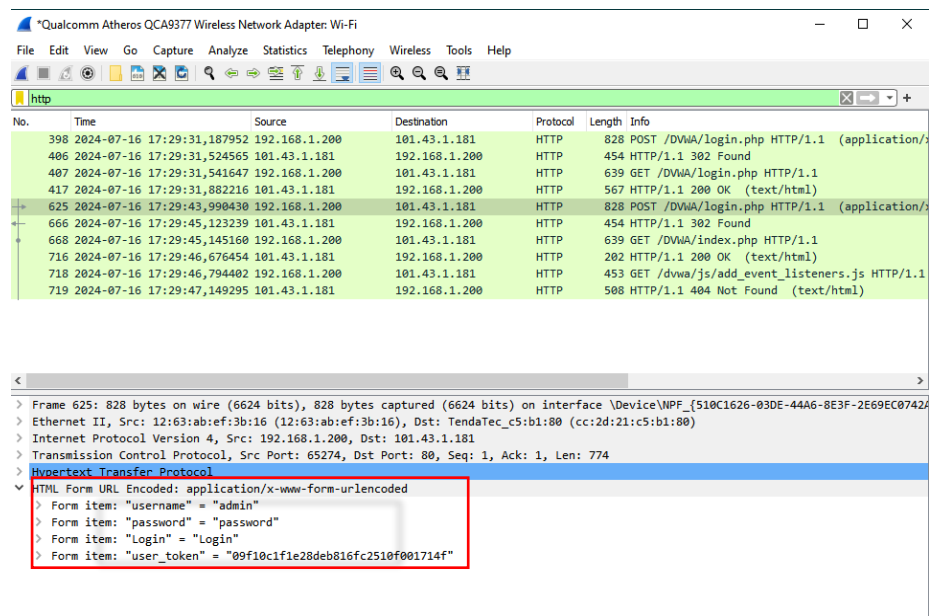
Gambar 4.24 *IP Publik Vpn Zerotier*Gambar 4.25 *Ip publik Vpn lain*

e. Pengujian keamanan menggunakan Wireshark

Pengujian yang kelima adalah pengujian keamanan aktivitas lalu lintas jaringan seperti melakukan *login* pada *website* dengan menggunakan Wireshark sebelum dan sesudah terhubung ke jaringan vpn zerotier, dimana pengujian ini dilakukan untuk mengetahui

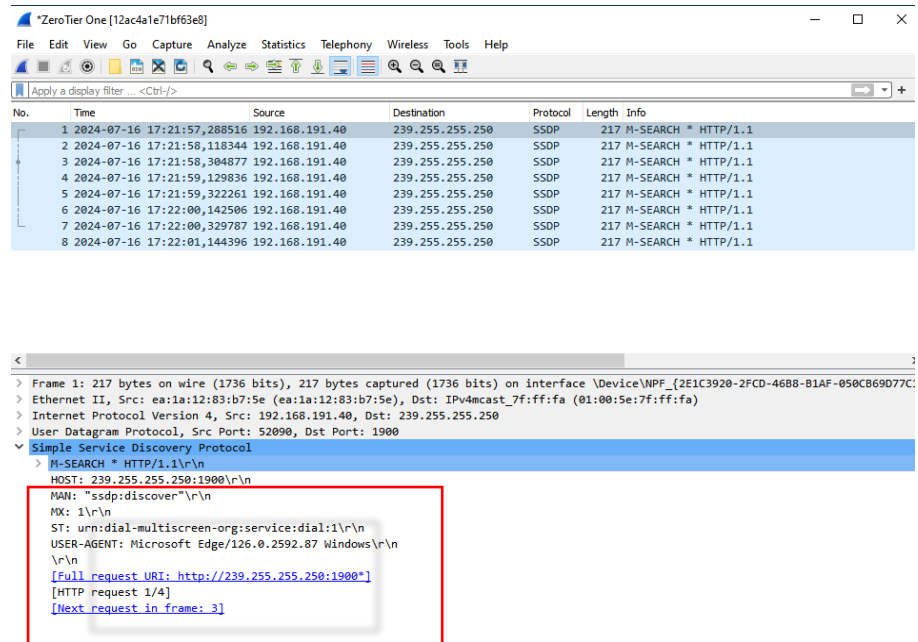
apakah aktivitas *login* yang dilakukan menggunakan jaringan vpn zerotier sudah aman. Berdasarkan hasil pengujian penulis, bahwa aktivitas lalu lintas dalam melakukan *login* pada *website* yang belum terhubung ke jaringan vpn zerotier masih dapat terlihat dan sesudah terhubung ke jaringan vpn zerotier aktivitas *login* sudah tidak dapat terlihat, seperti pada gambar 4.26 dan gambar 4.27.

1. Pengujian menggunakan jaringan wifi



Gambar 4.26 test keamanan *login* menggunakan *wifi*

2. Pengujian menggunakan vpn zerotier

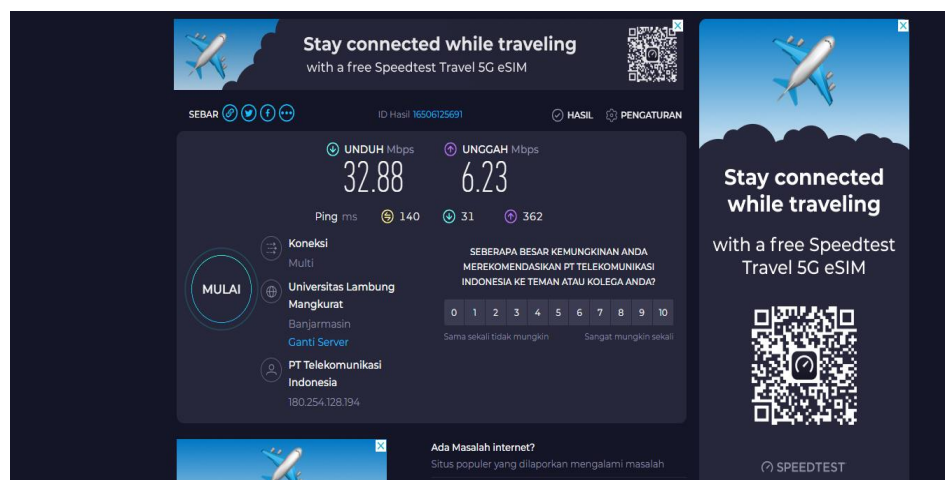


Gambar 4.27 test keamanan menggunakan vpn zerotier

f. pengujian Speedtest

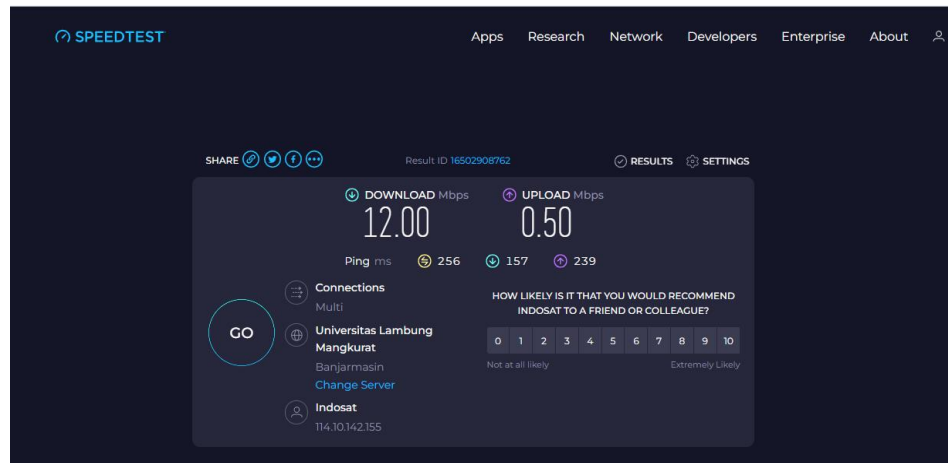
Pengujian keenam adalah pengujian Speedtest untuk membandingkan kecepatan internet sebelum dan sesudah menggunakan Vpn Zerotier

1. Pengujian Speedtest menggunakan jaringan wifi



Gambar 4.28 Speedtest sebelum menggunakan vpn zerotier

2. Pengujian Speedtest menggunakan jaringan vpn zerotier



Gambar 4.29 *Speedtest* menggunakan vpn zerotier

4.2 Pembahasan

Berdasarkan dari semua tahapan yang sudah dilakukan, baik dari tahap perancangan sampai dengan tahap implementasi dan pengujian menghasilkan sebuah kesimpulan bahwa semua tahapan konfigurasi yang sudah dilakukan berjalan dengan baik dan menghasilkan sebuah implementasi *Virtual Private Network* menggunakan zerotier berbasis OpenWRT, pembahasan lebih lanjut mengenai konfigurasi Reyre dan konfigurasi Zerotier adalah sebagai berikut:

a. Konfigurasi Reyre

Berdasarkan hasil dari implementasi maka konfigurasi reyre berjalan dengan baik, baik dari penginstalan hingga menghubungkan dengan zerotier untuk menghubungkan reyre dengan zerotier kita masuk ke bagian *service* pada reyre lalu klik bagian zerotier dan

masukan *network id* zerotier *server* seperti pada gambar 4.14, lalu klik *save and apply*.

b. konfigurasi Zerotier

Konfigurasi pada zerotier *server*, berdasarkan pada gambar 4.12, Ketika sudah mendapatkan *network id* yaitu 8286ac0e478d98e1, lalu yang pertama dilakukan adalah memilih ip yang tersedia pada zerotier *server* seperti pada gambar 4.13. penulis memilih IP 192.168.191*.

Selanjutnya melakukan konfigurasi pada zerotier *client*, pertama masukan *network id* zerotier *server* pada zerotier *client* dengan cara klik *Add network* pada zerotier *server* dan masukkan *network id* 8286ac0e478d98e1 dan klik *add* seperti pada gambar 4.16, lalu setelah itu masuk kembali ke zerotier *server* seperti pada gambar 4.14 lalu *ceklis network address* yang diijinkan untuk terhubung ke zerotier *server*.

c. Pengujian Zerotier

Pada pengujian traceroute penulis melakukan perbandingan sebelum dan sesudah mengaktifkan zerotier dengan tujuan Detik.com dan mendapatkan hasil seperti pada tabel 4.1, bahwa Hop Route tetap sama. Selanjutnya penulis melakukan pengecekan IP Publik pada *Tools What is My Ip Address* sebelum dan sesudah menggunakan Zerotier dan mendapatkan Ip publik yang sama, setelah itu penulis melakukan pengecekan Ip Publik menggunakan VPN lain dan mendapatkan IP publik yang berbeda seperti pada tabel 4.

d. Pengujian wireshark

Setelah itu penulis melakukan pengujian keamanan menggunakan wireshark sebelum dan sesudah terhubung ke vpn zerotier dan penulis mendapatkan bahwa aktivitas *login* yang belum terhubung ke vpn zerotier dapat terlihat, seperti pada gambar 4.26 dan aktivitas *login* sudah tidak dapat terlihat ketika sudah terhubung ke vpn zerotier seperti pada gambar 4.27.

e. Pengujian Speedtest

Selanjutnya penulis melakukan test kecepatan jaringan sebelum dan sesudah terhubung ke vpn zerotier, dengan menggunakan tools Speedtest dan mendapatkan hasil bahwa jaringan yang terhubung ke vpn zerotier akan menurun kecepatan internetnya dibanding sebelum terhubung ke jaringan vpn zerotier seperti pada gambar 4.28 dan gambar 4.29.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan tentang perancangan dan implementasi *Virtual Private Network* menggunakan *Zerotier* berbasis *OpenWRT* dapat disimpulkan sebagai berikut:

- a. Berdasarkan hasil dari pengujian yang dilakukan maka dapat disimpulkan bahwa perancangan dan implementasi *VPN* menggunakan *Zerotier* dapat berjalan dengan baik, dan kedua komputer server dan komputer *client* dapat saling terhubung dengan jaringan yang berbeda selama komputer *client* terkoneksi ke *zerotier server*.
- b. Implementasi *VPN Zerotier* yang dilakukan oleh penulis, merupakan solusi yang efektif dan efisien untuk dapat mengoptimalkan penggunaan akses jarak jauh yang aman dengan jaringan berbeda menggunakan *zerotier*.
- c. Berdasarkan hasil dari pengujian *vpn zerotier*, dapat disimpulkan bahwa untuk melakukan *folder sharing* hanya dapat dilakukan oleh komputer *client* yang diberikan akses oleh komputer *server* menggunakan *vpn zerotier*.
- d. Berdasarkan hasil dari pengujian *VPN Zerotier*, *Ip* komputer tidak berubah meski menggunakan *VPN* dari *Zerotier*, dan *Ip* komputer akan berubah ketika menggunakan *VPN* lain.

5.2 Saran

Adapun saran yang dapat diberikan penulis untuk penelitian selanjutnya adalah sebagai berikut:

- a. Untuk penelitian selanjutnya agar bisa membandingkan kecepatan dan latensi sebelum dan sesudah menggunakan zerotier.
- b. Dalam penelitian ini, penulis masih menghubungkan dari komputer ke komputer.
Untuk peneliti selanjutnya agar bisa menambahkan perangkat yang terhubung seperti printer.
- c. Untuk peneliti selanjutnya agar dapat mealokasikan alamat ip komputer *server* menjadi satu alamat ip yang sama agar memudahkan komputer *client* untuk melakukan akses remote.

DAFTAR PUSTAKA

- Amarudin, A., & Riskiono, S. D. (2019). Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan *Virtual Private Network* (Vpn). *Jurnal Teknoinfo*, 13(2), 100-106.
- Ardiansyah, M. F., Diansyah, T. M., & Liza, R. (2022). Penggunaan *Set top box* Bekas untuk Dimanfaatkan sebagai *Cloud Server*. *Blend Sains Jurnal Teknik*, 1(2), 88-96.
- Candra, A. M., Samsugi, S. & Jupriyadi, 2021. Perancangan dan Implementasi *Controller Access Point System Manager (CAPSMAN)* Mikrotik Menggunakan Aplikasi Winbox. Issue TELEFORTECH.
- Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (*Virtual Private Network*) Dengan Metode PPTP (*Point To Point Tunneling Protokol*) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI: Jurnal Sains dan Manajemen*, 8(1).
- Hadinata, F., Prasetyo, S. E., & Haeruddin, H. (2022). Analisa Penggunaan Jaringan ZeroTier di Masa Pandemi Covid-2019. *Jurnal Ilmu Komputer dan Bisnis*, 13(1), 85-93.
- Jiang, H., Wang, Q., Zhang, G., & Fan, J. (2019, March). *Design and Implementtationg of an IPsec VPN Gateway Base on OpenWRT*. In *Journal of Physics: Conference Series* (Vol. 1176, No. 4, p. 042007). *IOP Publishing*.
- Kurniawan, D. F. (2023). Implementasi *Software Defined Network dan Virtual Private Network* menggunakan ZeroTier pada Perangkat Pengukur dan Pengendali Tegangan DC (*Doctoral dissertation*, Universitas Gadjah Mada).
- Lipp, B., Blanchet, B., & Bhargavan, K. (2019, June). *A mechanised cryptographic proof of the WireGuard virtual private network protocol*. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 231-246). *IEEE*.
- Marsela, A., Khairil, K., & Aspriyono, H. (2024). Penerapan Zerotier Dalam Membangun File Server Pada Kantor Desa Dusun Baru II Kabupaten Bengkulu Tengah. *Jurnal Penelitian Rumpun Ilmu Teknik*, 3(1), 111-120.
- Pamungkas, A. P., Putra, M. R., & Hafizh, M. (2021). Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko-muko. *Jurnal KomtekInfo*, 8(3), 189-194.

- Putra, T. G. S., & Widiyari, I. R. (2022). Rancangan *Virtual Private Server* Pada Kantor Kelurahan Menggunakan ZeroTier. *Building of Informatics, Technology and Science (BITS)*, 4(2), 352-360.
- Ruslianto, I. (2019). Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura. *CESS (Journal of Computer Engineering, System and Science)*, 4(1), 74-77.
- Sánchez Gutiérrez, S. A. (2022). *Implementación de una VPN con Zero Tier One para la gestión de recursos de un servidor de archivos en una empresa de consultoría*.
- Sampuno, D. S., Noertjahyana, A., & Setiawan, A. (2019). Implementasi pembuatan distro linux untuk keperluan laboratorium informatika. *Jurnal Infra*, 7(1), 210-213.
- Setyawan, A. (2023). *Remote Access Pada Jaringan Lokal Menggunakan VPN Zerotier (Doctoral dissertation, Universitas Teknologi Digital Indonesia)*.
- Slameto, A. A., & Hidayat, R. (2019). *Comparative Analysis of PPPOE and SSTP Performance in Microtic (Analisis Perbandingan Kinerja PPPOE dan SSTP Pada Mikrotik)*. *Jurnal KomtekInfo*, 6(2), 107-116.
- Syawaludin, M. (2019). Penerapan Algoritma Rivest Shamir Adleman (RSA) pada Virtual Private Network (VPN) untuk Meningkatkan Keamanan Jaringan Internet/Muhammad Syawaludin/15150026/Pembimbing I: Adiat Pariduddin/Pembimbing II: Alam Supriyatna.
- Umaroh, L., & Rifauddin, M. (2020). Implementasi *Virtual Private Network* (Vpn) Di Perpustakaan Universitas Islam Malang. *Jurnal Dokumentasi dan Informasi*, 42(2), 193-201.
- Wicaksana, P., Hadi, F., & Hadi, A. F. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, 8(3), 169-175.

LAMPIRAN



**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA**

Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS

No.58/STMIK-3.C.2/KP/II/2024

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama- nama tersebut di bawah ini :

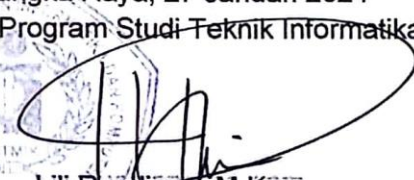
1. Nama : Abdul Hadi, S.T., M.Kom.
NIK : 198505102021101
Sebagai Pembimbing I Dalam Pembuatan Program
2. Nama : Catharina Elmayantie, M.Pd.
NIK : 197610252015003
Sebagai Pembimbing II Dalam Penulisan Tugas Akhir

Untuk membimbing Tugas Akhir mahasiswa :

- Nama : M. Dimas Wahyu Prayoga
NIM : C2055201022
Program Studi : TEKNIK INFORMATIKA (55201)
Tanggal Perubahan : 25 Januari 2024
Judul Tugas Akhir : Implementasi Virtual Private Network Menggunakan Zerotier Berbasis OpenWRT
Keterangan : Perubahan judul TA setelah seminar proposal TA

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 27 Januari 2024
Ketua Program Studi Teknik Informatika,


Lili Rusdiana, M.Kom.
NIK: 198707282011007

Tembusan :

1. Pembimbing I dan II
2. Mahasiswa yang bersangkutan
3. Arsip



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

(STMIK) PALANGKARAYA

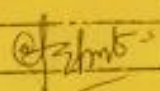
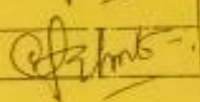
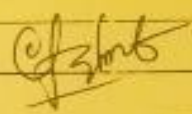
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya

email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

KARTU KEGIATAN KONSULTASI
TUGAS AKHIR

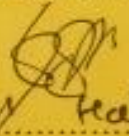
Nama Mahasiswa : Muhammad Dimas Wahyu Prayoga
NIM : 22055201022
Tanggal Persetujuan Judul : 12 Agustus 2023
Judul Tugas Akhir : Implementasi Virtual Private Network menggunakan
ZeroTier Berbasis OpenWRT

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	12/10/2023	09/11/2023	Perbaikan bab 1 latar belakang masalah, perbaikan bagian masalah, dan tujuan.	SR
	29/11/2023		tambahkan teori serta konsep, tambahkan alur flowchart, dan desain, tambahkan pengujian	SR
	25/11/2023	27/11/2023	lengkapi teori, jadikan bagian	SR
	5/1/2024	6/1/2024	tambah pengujian, subbab - serta pengujian, desain gambar topologi.	SR
	11/1/2024		AKK Seminar (dengan ceklis daftar isi, gambar dll)	SR
	18/12/2023	15/12/2023	Tambahkan sumber kutipan, Perbaiki isi Tujuan, Desain Penelitian, Instrumen Penelitian, SDA, Jadwal Penelitian dan Penulisan.	SR
	10/1/2024	12/1/2024	Penulisan Latar Belakang, Tujuan, Penelitian Relevan, Jenis Penelitian, Desain Penelitian, metode observasi dan Daftar pustaka.	SR

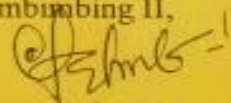
No.	Tanggal Koreksi		Uraian	Tanda Tangan
	Terima	Kembali		
	13/01/2024	13/01/2024	Jenis Penelitian dan Daftar pustaka	
	16/01/2024	16/01/2024	Acc Seminar	
	15/06/2024	15/06/2024	menghubungkan Payre P Penulisan ke internet	
	21/06/2024	21/06/2024	menghubungkan Zerotier ke Payre dan komputer	
	27/06/2024	27/06/2024	melakukan Pengujian	
	1/07/2024	1/07/2024	melakukan Pengujian dan Penulisan Bab IV dan bab V	
	3/07/2024	3/07/2024	Acc Endang	
	2/07/2024	2/07/2024	penulisan Intisari, kata pengantar, suran dan Bab V	
	3/07/2024	3/07/2024	Abstrak dan lampiran	
	4/07/2024	4/07/2024	Acc Sidang	

Menyetujui :

Dosen Pembimbing I,


 Abdurrahman

Dosen Pembimbing II,


 Catharina Elmāyantje, M.Pd.



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK PALANGKARAYA

Jl. G. Obos No. 114 – Telp. 0536-3224593 – Fax. 0536-3225515 Palangka Raya
Email: humas@stmikplk.ac.id – Website: www.stmikplk.ac.id

Nomor : 935/STMIK-C2/Ak/XII/2023
Lampiran : -
Perihal : Permohonan Izin Penelitian dan Pengumpulan Data untuk Tugas Akhir

Kepada

Yth. **Kepala Dinas Koperasi Usaha Kecil Dan Menengah**

Jl. Willem A. Samad No. 7, Menteng, Kec. Jekan Raya, Kota
Palangka Raya, Kalimantan Tengah

Dengan hormat,

Sehubungan dengan penyusunan Tugas Akhir mahasiswa sebagai persyaratan kelulusan Program Studi Teknik Informatika (S1) pada STMIK Palangkaraya, maka dengan ini kami sampaikan permohonan izin penelitian dan pengumpulan data bagi mahasiswa kami berikut:

Nama : MUHAMMAD DIMAS WAHYU PRAYOGA
NIM : C2055201022
Prodi (Jenjang) : Teknik Informatika (S1)
Thn. Akad. (Semester) : 2023/2024 (7)
Lama Penelitian : 15 Desember 2023 s.d 15 Desember 2023
Tempat Penelitian : Dinas Koperasi

Dengan judul Tugas Akhir:

Implementasi Virtual Private Network menggunakan Zerotier berbasis OpenWRT

Adapun ketentuan dan aturan pemberian informasi dan data yang diperlukan dalam penelitian tersebut menyesuaikan dengan ketentuan/peraturan pada instansi Bapak/Ibu.

Demikian permohonan ini disampaikan, atas perhatian dan kerja samanya diucapkan terima kasih.

Palangka Raya, 15 Desember 2023

Ketua,

Suparno, M.Kom.
NIK. 196901041995105

LEMBAR WAWANCARA

A: PENANYA

B: PENJAWAB

Pertanyaan 1

A : Apakah pada bidang sekretariat ini sudah tersedia layanan internet pak?

B : Pada bidang ini sudah tersedia layanan internet yang dapat digunakan untuk kegiatan pekerjaan sehari-hari kantor.

Pertanyaan 2

A : Apakah ada urgensi ketika ingin menggunakan internet pak ?

B : untuk saat ini urgensinya ketika ingin menggunakan internet seperti membuka website resmi kantor yang berisi data-data penting yang sebagian bersifat rahasia masih rentan terhadap serangan seperti pemantauan jaringan mas.

Pertanyaan 3

A : Apakah disini sudah mengimplementasikan *Virtual Private Network* (VPN) pak?

B : Belum mas untuk saat ini belum ada implementasi *Virtual Private Network* (VPN) hanya menggunakan jaringan internet biasa saja.

Pertanyaan 4

A : Apabila diimplementasikan sebuah *Virtual Private Network*, perangkat apa saja yang mau dihubungkan dengan *Virtual Private Network* menggunakan Zerotier ini ?

B : untuk sekarang mungkin perangkat yang mau dihubungkan adalah komputer, access point, dan printer saja mas.

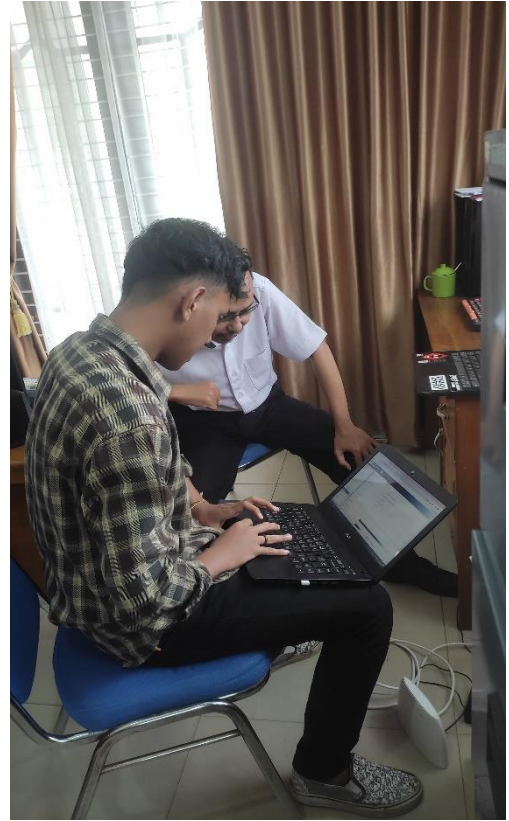
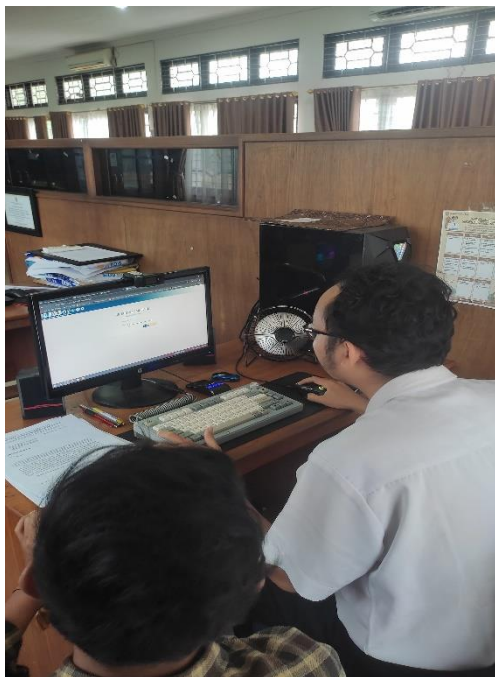
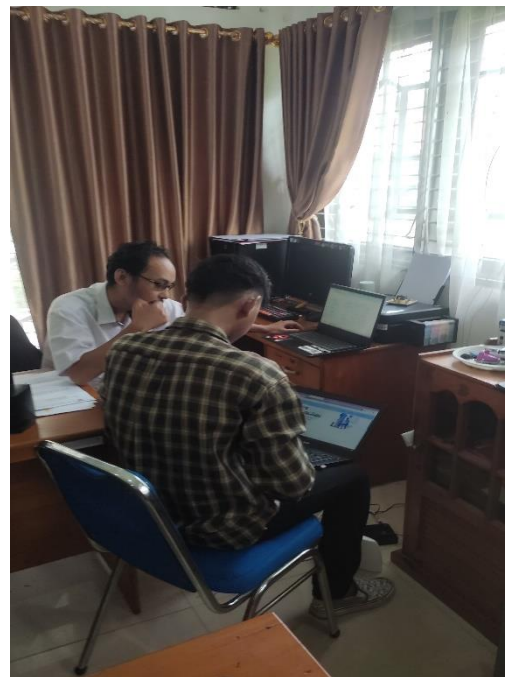
Mengetahui

Staff Bagian Sekretariat,



Eddy Jonathan

Lampiran Dokumentasi penelitian





SURAT TUGAS PENGUJI TUGAS AKHIR

No. 168/STMIK-3.C.2/KP/VII/2024

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan kepada nama- nama berikut :

1. Nama : Sam'ani, S.T., M.Kom.
NIK : 197703252005105
Sebagai Ketua
2. Nama : Elia Zakharia, M.T.
NIK : 199205262016104
Sebagai Sekretaris
3. Nama : Amaya Andri Damaini, S.Kom., M.T
NIK : 199309042018001
Sebagai Anggota
4. Nama : Abdul Hadi, S.T., M.Kom.
NIK : 198505102021101
Sebagai Anggota
5. Nama : Catharina Elmayantie, M.Pd.
NIK : 197610252015003
Sebagai Anggota

Tim Penguji Tugas Akhir Mahasiswa :

Nama : M. Dimas Wahyu Prayoga
NIM : C2055201022
Hari/ Tanggal Ujian : Kamis, 11 Juli 2024
Waktu : 10.00 WIB
Judul Tugas Akhir : Implementasi Virtual Private Network Menggunakan Zerotier Berbasis OpenWRT

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 09 Juli 2024
Ketua Program Studi Teknik Informatika,


Lili Rusdiana, M.Kom.
NIK. 198707282011007

Tembusan :

1. Dosen Penguji
2. Mahasiswa yang Bersangkutan
3. Arsip



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA

Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

BERITA ACARA
UJIAN TUGAS AKHIR

Periode (Bulan) : Juli Tahun 2024

1. Hari/Tanggal Ujian : Kamis / 11 Juli 2024
2. Waktu (Jam) : 10.00 WIB sampai dengan WIB
3. Nama Mahasiswa : M. Dimas Wahyu Prayoga
4. Nomor Induk Mahasiswa : C2055261022
5. Program Studi : Teknik Informatika
6. Tahun Angkatan : 2020
7. Judul Tugas Akhir : Implementasi Virtual Private Network
Menggunakan Zerotier Berbasis
OpenWRT

8. Dosen Penguji :
- | Nama | Nilai | Tanda Tangan |
|-------------------|-------|--------------|
| 1. Sam'ani | = | (.....) |
| 2. Elia Z | = | (.....) |
| 3. Amaga Andri D. | = | (.....) |
| 4. Abdul Hadi | = | (.....) |
| 5. Catharina E | = | (.....) |

9. Hasil Ujian : LULUS / ~~TIDAK LULUS~~ *) NILAI = 83,9
- Dengan Perbaikan/ Tanpa Perbaikan *)

10. Catatan Penting :
1. Lama Perbaikan : 10 hari
 2. Jika lebih dari 1 (satu) bulan dikenakan sanksi berupa denda sebesar Rp. 600.000,- (Enam ratus ribu rupiah) per bulan dari tanggal ujian
 3. Jika lebih dari 3 (tiga) bulan dari tanggal ujian maka hasil ujian dibatalkan dan wajib mengajukan judul dan pembimbing baru

Palangka Raya, 11 Juli 2024

Mengetahui :
Ketua Program Studi Teknik Informatika,
Lili Rusdiana, M.Kom.
NIK. 198707282011007

Ketua Penguji,
Sam'ani
NIK.

Tembusan:

1. Arsip Prodi Teknik Informatika
2. Mahasiswa yang bersangkutan

Dibawa saat konsultasi perbaikan dengan dosen penguji

*) Coret yang tidak perlu