

## PERANCANGAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN MIKROTIK *ROUTER* PADA *MANAGEMENT BANDWIDTH* DI CV. ALGI PIN BANDUNG

Deri Andriyana Juhana<sup>1</sup>, Soecipto<sup>2</sup>, Ani Amaliyah<sup>3</sup>

<sup>1,2,3</sup>Program Studi Teknik Informatika Universitas Islam Nusantara, Bandung, Indonesia

<sup>1</sup>deriandriyana17@gmail.com, <sup>2</sup>soecipto.akademik@gmail.com, <sup>3</sup>anidata@yahoo.com

### Abstrak

Teknologi Informasi (TI) sangat besar manfaatnya di segala bidang, termasuk bidang pemerintahan, lembaga pendidikan maupun perusahaan swasta. Perkembangan TI juga diiringi dengan perkembangan sistem jaringan yang sangat pesat pula. Selain menggunakan komputerisasi, banyak instansi pemerintahan, lembaga pendidikan maupun perusahaan swasta yang sudah memanfaatkan sistem jaringan guna kelancaran aktifitas kerjanya.

Saat ini perusahaan – perusahaan yang bergerak di bidang non TI membutuhkan TI dalam mencapai tujuan bisnisnya. Sistem keamanan jaringan yang baik adalah sistem keamanan jaringan yang dapat memberikan keamanan terhadap jaringan komputer yang dimiliki perusahaan tersebut yang juga dapat memenuhi kebutuhan penggunaannya. Begitupun dengan *management bandwidth* harus dilakukan perencanaan yang baik agar dapat digunakan secara maksimal oleh pengguna jaringan komputer tersebut.

CV. Algi Pin merupakan suatu unit usaha persekutuan komanditer yang bergerak pada bidang produksi pin PILKADA. Permasalahan yang terjadi pada CV. Algi Pin adalah terletak pada jaringannya yang kurang terstruktur dan koneksi internet yang lambat, belum adanya pembagian *bandwidth* tiap *access point* serta pembagian *bandwidth* untuk kepentingan user yang berbeda belum tertata dengan baik dan menyebabkan hak akses yang belum optimal, permasalahan selanjutnya adalah akses ke perangkat wifi jaringan, dimana untuk login ke jaringan hanya menggunakan keamanan berbasis *Wired Equivalent Privacy (WEP)* yang penulis rasa keamanan tersebut belum cukup optimal.

**Metode** penelitian menggunakan metode deskriptif. Model pengembangan jaringan komputer yang digunakan adalah *Network Development Life Cycle (NDLC)*.

**Tujuan** adalah menghasilkan rancangan sistem keamanan jaringan menggunakan mikrotik *router* pada *management bandwidth*, dan pengoptimalan sistem keamanan *login* jaringan di CV Algi Pin agar lebih aman bagi para *user*.

**Kata kunci:** *Perancangan, Sistem Keamanan Jaringan, Mikrotik Router Box, Manajemen Bandwidth, Network Development Life Cycle.*

### I. PENDAHULUAN

Teknologi Informasi (TI) sangat besar manfaatnya di segala bidang, termasuk bidang pemerintahan, lembaga pendidikan maupun perusahaan swasta. Perkembangannya sangat pesat dalam berbagai aktivitas kehidupan dan memberikan kesempatan untuk dimanfaatkan secara tepat (Herry, Soecipto, and Ani Amaliyah, 2021).

Perkembangan TI juga diiringi dengan perkembangan sistem jaringan yang sangat pesat pula. Selain menggunakan komputerisasi, banyak instansi pemerintahan, lembaga pendidikan maupun perusahaan swasta yang sudah memanfaatkan sistem jaringan guna kelancaran aktivitas kerjanya.

Saat ini perusahaan – perusahaan yang bergerak di bidang non TI membutuhkan TI dalam mencapai tujuan bisnisnya. Sistem keamanan jaringan yang baik adalah

sistem keamanan jaringan yang dapat memberikan keamanan terhadap jaringan komputer yang dimiliki perusahaan tersebut yang juga dapat memenuhi kebutuhan penggunaannya. Begitupun dengan *management bandwidth* harus dilakukan perencanaan yang baik agar dapat digunakan secara maksimal oleh pengguna jaringan komputer tersebut.

CV. Algi Pin merupakan suatu unit usaha persekutuan komanditer yang bergerak pada bidang produksi pin PILKADA. Permasalahan yang terjadi pada CV. Algi Pin adalah terletak pada jaringannya yang kurang terstruktur dan koneksi internet yang lambat, belum adanya pembagian *bandwidth* tiap *access point* serta pembagian *bandwidth* untuk kepentingan user yang berbeda belum tertata dengan baik dan menyebabkan hak akses yang belum optimal, permasalahan

selanjutnya adalah akses ke perangkat *wifi* jaringan, dimana untuk *login* ke jaringan hanya menggunakan keamanan berbasis *Wired Equivalent Privacy (WEP)* yang penulis rasa keamanan tersebut belum cukup optimal.

### Identifikasi Masalah

Identifikasi masalah yang ada adalah sebagai berikut: Berdasarkan hasil pengamatan dan observasi yang sudah dilakukan penulis maka penulis merumuskan beberapa pokok permasalahan yang terjadi di CV. Algi Pin yaitu sebagai berikut:

- Sistem keamanan untuk masuk ke jaringan belum tertata dengan baik dan masih menggunakan metode standar.
- Kecepatan *bandwidth* untuk karyawan biasa dan staff tidak ada perbedaan yang seharusnya dibagi berdasarkan tingkat kepentingan penggunaan *bandwidth*.
- Tidak adanya pengaturan *bandwidth* untuk tiap *access point* di lokasi perusahaan dimana pada saat rapat berlangsung pengguna mengeluhkan kecepatan internet yang kurang cepat karena manajemen *bandwidth* yang belum teratur.
- Kesulitan dalam memantau penggunaan jaringan bagi pimpinan perusahaan.

### Rumusan Masalah

Sesuai dengan latar belakang yang telah diuraikan di atas, maka dirumuskan beberapa permasalahan sebagai berikut :

- Membuat sistem keamanan *login* berbasis web dimana untuk *user* yang ingin mengakses sistem jaringan, masuk menggunakan aplikasi *login* berbasis web.
- Pembagian penggunaan internet yang berbeda berdasarkan tingkat jabatan di dalam perusahaan dan tiap perangkat *access point* yang berbeda untuk memaksimalkan penggunaan internet.
- Pemblokiran akses terhadap *Facebook*, *Youtube*, *PUBG Mobile* dan *Mobile Legends Bang Bang* pada saat jam bekerja.
- Mengatur keamanan jaringan *router* agar tidak disalahgunakan oleh pihak luar.
- Membuat aplikasi berbasis *web* untuk memantau penggunaan jaringan untuk pimpinan.

### Tujuan Penelitian

Adapun tujuan yang diharapkan tercapai dalam penelitian di CV. Algi Pin ini adalah:

- Menghasilkan rancangan sistem keamanan jaringan mikrotik *router* pada manajemen *bandwidth* di

CV. Algi Pin Bandung

- Mengoptimalkan sistem keamanan *login* jaringan di CV Algi Pin agar lebih aman bagi *user*.
- Mengoptimalkan penggunaan *internet* di perusahaan agar lebih optimal dan tidak saling berebut satu sama lain.
- Pengoptimalan penggunaan internet untuk setiap perangkat jaringan yang ada.
- Pemblokiran akses *social media* dan *game* agar kinerja karyawan tidak terganggu.

## STUDI PUSTAKA

### Manajemen Jaringan

Pengelolaan jaringan dapat didefinisikan sebagai OAM & P (operasional, administrasi, pemeliharaan, dan penyediaan) jaringan dan layanan. Tipe pengoperasian berkaitan dengan operasi sehari-hari dalam menyediakan layanan jaringan. (Subramanian, 2000).

### Manajemen Bandwidth

*Bandwidth Management System (BMS)* adalah sebuah metode yang diterapkan untuk mengatur besarnya *bandwidth* yang akan digunakan oleh masing-masing *user* di sebuah jaringan sehingga penggunaan *bandwidth* akan terdistribusi secara merata (Muklas, Suspendar and SW, 2020).

Ada beberapa metode yang dapat diterapkan untuk mengimplementasikan *bandwidth management* ini diantaranya melalui *proxy server*, QoS atau *traffic shapping*, atau pembatasan *bandwidth* atau *limiter*.

Di dalam dunia internet sering di dengar istilah *limiter* atau pembatasan kecepatan untuk melakukan akses ke internet. Ada beberapa jenis sistem *limiter* yang biasa di aplikasikan ke *router*, mulai dari yang *simple* hingga yang kompleks.

Dalam penelitian ini digunakan dua metode untuk *bandwidth management queue tree* dan *PCQ*.

### 1. Queues Tree

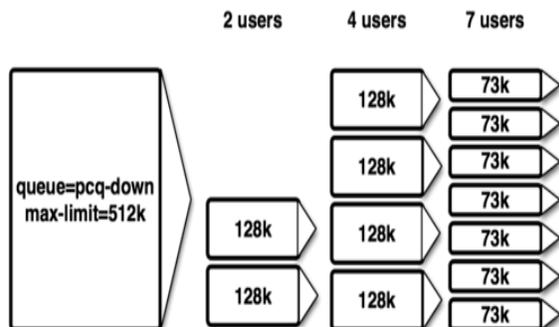
*Queues tree* adalah pelimitan yang sangat rumit karena pelimitan ini berdasarkan protocol *ports IP Address* bahkan kita harus mengaktifkan fitur *Mangle* pada *Firewall* jika ingin menggunakan *Queue Tree*, *Queues Tree* berfungsi untuk memlimit *bandwidth* pada mikrotik yang mempunyai dua koneksi internet karena paket marknya lebih berfungsi dari pada di *Simple Queues*. *Queues tree* juga digunakan untuk membatasi satu arah koneksi saja baik itu *download* maupun *upload* (Pratama, Susilo and Coastera, 2018).

Metode *Queues tree* merupakan metode yang cukup rumit dalam melakukan konfigurasinya. Keunggulan yang terdapat pada metode *Queues tree* adalah kita dapat mengalokasikan *bandwidth Internet Control Message Protocol (ICMP)*. Jadi, ketika *bandwidth* yang terdapat pada klien penuh, *ping time* nya masih dapat stabil.

## 2. Peer Connection Queue

*Per Connection Queue (PCQ)* merupakan pengaturan manajemen *bandwidth*. Dengan menggunakan *PCQ* walaupun jumlah komputer *client* sejumlah puluhan atau bahkan ratusan, hanya diperlukan satu atau dua konfigurasi *queue*. Metode ini *PCQ* ini dapat diterapkan pada *simple queue* maupun *queue tree* (Dewi and Rachmawati, 2018). Pengaturan manajemen *bandwidth* bersifat *massive*. Dengan menggunakan *PCQ* walaupun jumlah komputer *client* sejumlah puluhan atau bahkan ratusan, hanya diperlukan satu atau dua konfigurasi *queue*. Metode ini *PCQ* ini dapat diterapkan pada *Simple Queue* maupun *Queue Tree*.

### pcq-rate=128000

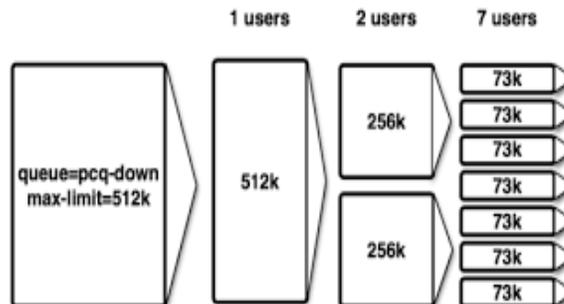


Gambar 1.1 PCQ Rate

*PCQ Classifier* berfungsi mengklasifikasikan arah koneksi, Misalnya jika *Classifier* yang digunakan adalah *src-address* pada *Local interface*, maka aliran *PCQ* akan menjadi koneksi *upload*. Begitu juga dgn *dst-address* akan menjadi *PCQ download*.

*PCQ rate* berfungsi untuk membatasi *bandwidth* maksimum yang bisa didapatkan. Dengan memasukkan angka pada *rate* ini (default: 0) maka maksimal *download* yang akan didapatkan per *IP* akan dibatasi mis. 128k (kbps).

### pcq-rate=0



Gambar 1.2 PCQ Rate

## 3. Quality of Services (QoS)

*Quality of Service (Mutu Layanan)* merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diharapkan. Kinerja jaringan komputer dapat bervariasi akibat beberapa masalah, seperti halnya masalah *bandwidth*, *latency* dan *jitter*, yang dapat membuat efek yang cukup besar bagi banyak aplikasi. Sebagai contoh, komunikasi suara (seperti *VoIP* atau *IP Telephony*) serta *video streaming* dapat membuat pengguna frustrasi ketika paket data aplikasi tersebut dialirkan di atas jaringan dengan *bandwidth* yang tidak cukup, dengan *latency* yang tidak dapat diprediksi, atau *jitter* yang berlebihan. Fitur *Quality of Service (QoS)* ini dapat menjadikan *bandwidth*, *latency*, dan *jitter* dapat diprediksi dan dicocokkan dengan kebutuhan aplikasi yang digunakan di dalam jaringan tersebut yang ada. Dalam hal ini PT. *Exhibition Network* Indonesia belum melakukan pengaturan dalam hal manajemen *bandwidth* sehingga sering mendapati masalah ketika ada *user* yang mengakses paket data yang besar secara bersamaan (Ardianto, Alfaresi and Yuansyah, 2018).

*Quality of Service (QoS)* merupakan mekanisme jaringan yang memungkinkan aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan yang diterapkan. Tujuan dari *QoS* adalah untuk memenuhi kebutuhan-kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. Performansi mengacu ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi (Arifin., 2012).

*QoS* mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. *QoS* menawarkan kemampuan untuk mendefinisikan atribut-atribut layanan jaringan yang disediakan, baik

secara kualitatif maupun kuantitatif (Febriyanti, Raharjo and Sholeh, 2017).

Dalam melakukan pengukuran parameter *QoS* (*Quality of Service*) suatu jaringan, memerlukan acuan yang dijadikan sebagai standar dalam melakukan pengukuran kualitas jaringan. *TIPHON* digunakan sebagai standar dalam menentukan kategori parameter

Kategori Degradasi	Packet Loss	Indeks
Sangat Bagus	0%	4
Bagus	3%	3
Sedang	15%	2
Jelek	25%	1

(Aji and Kharisma, 2019).

Berikut ini merupakan beberapa parameter *QoS* yang akan digunakan dalam mengukur performasi jaringan, yaitu :

### 1. Throughput

*Throughput* digunakan untuk mengetahui jumlah paket yang diterima dalam keadaan baik terhadap waktu total transmisi yang dibutuhkan dari *server* hingga ke *end user*. Perhitungan *throughput* membutuhkan data primer panjang data yang diterima dan waktu proses *download* data yang didapatkan dari penangkapan data dari *software Network Analyzer Wireshark* (Saniya, Priyono and Ambarwati, 2013).

Dengan kata lain *Throughput* yaitu kecepatan (*rate transfer*) data yang efektif yang diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

Tabel 1.1 *Throughput*

Kategori Throughput	Throughput	Indeks
Sangat Bagus	100%	4
Bagus	75%	3
Sedang	50%	2
Jelek	<25%	1

(Sumber : TIPHON)

Adapun persamaan yang digunakan untuk mengukur *throughput* adalah sebagai berikut :

$$Throughput = \frac{\text{Paket data diterima}}{\text{Lama Pengamatan}} \quad (1)$$

$$Throughput = \frac{\text{Throughput}}{\text{Alokasi Bandwidth User}} \times 100\% \quad (2)$$

### 2. Packet Loss

*Packet Loss* merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima. Nilai *packet loss* sesuai dengan versi TIPHON sebagai berikut:

Tabel 1.2 *Packet Loss*  
(Sumber : TIPHON)

Adapun persamaan yang digunakan mengukur *packet loss* adalah:

Packet

$$\text{Loss} = \frac{\text{Paket data dikirim} - \text{paket data diterima}}{\text{Paket data dikirim}} \times 100\% \quad (3)$$

### 3. Jitter

Hal ini diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan *jitter*. *Jitter* lazimnya disebut *variasi delay*, berhubungan erat dengan *latency*, yang menunjukkan banyaknya *variasi delay* pada transmisi data di jaringan. *Delay* antrian pada router dan switch dapat menyebabkan *jitter*. Terdapat empat kategori penurunan performansi jaringan berdasarkan nilai *peak jitter* sesuai dengan versi TIPHON, yaitu:

Tabel 2.3 *Jitter*

(Sumber : TIPHON)

Kategori Degradasi	Peak Jitter	Indeks
Sangat Bagus	0 ms	4
Bagus	0 s/d 75 ms	3
Sedang	75 s/d 125 ms	2
Jelek	125 s/d 225 ms	1

Adapun persamaan yang digunakan untuk mengukur *jitter* adalah:

$$Jitter = \frac{\text{Total Variasi Delay}}{\text{Total Paket Diterima}} \quad (4)$$

$$\text{Total Variasi Delay} = \text{Delay} - (\text{Rata-rata Delay}) \quad (5)$$

#### 4. Delay

Adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ketujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Menurut versi TIPHON, besarnya *delay* dapat diklasifikasikan sebagai berikut:

Tabel 2.4 *Latency*  
 (Sumber : TIPHON)

Untuk mengukur *delay* digunakan persamaan sebagai berikut:

$$\text{Delay} = \frac{\text{Paket Leght}}{\text{Link Bandwidth}}$$

##### a. Jaringan

Jaringan komputer adalah terhubungnya dua komputer atau lebih dengan kabel penghubung (pada beberapa kasus, tanpa kabel atau *wireless* sebagai penghubung), sehingga antar komputer dapat saling tukar informasi (Muklas, Supendar and SW, 2020).

##### b. Jenis Jaringan Komputer

Menurut Kadir (2003:347) Secara umum bentuk/jenis jaringan komputer berdasarkan area kerja dibedakan menjadi tiga kelompok, yaitu :

1. *LAN (Local Area Network)* adalah jaringan komputer yang mencakup area dalam satu ruang, satu gedung, atau beberapa gedung yang berdekatan.
2. *MAN (Metropolitan Area Network)* adalah jaringan yang cakupannya meliputi suatu kota. *MAN* menghubungkan *LAN LAN* yang lokasinya berjauhan.
3. *WAN (Wide Area Network)* dirancang untuk menghubungkan komputer-komputer yang terletak pada suatu cakupan geografis yang luas, seperti hubungan dari satu kota ke kota lain dalam suatu Negara, dengan menggunakan ISP maka komputer dapat saling komunikasi hingga jaraknya melintasi sampai antar benua (Doni, 2015).

##### c. Mikrotik

Mikrotik merupakan sebuah perusahaan produsen penyedia perangkat jaringan komputer yang berkantor di Latvia. Mikrotik *Router OS* adalah produk utama

perusahaan ini. Sistem operasi berbasis kernel Linux ini dirancang untuk menangani kebutuhan pengelolaan jaringan komputer baik jaringan jangka kecil, sedang, maupun jaringan dengan skala besar. Produk router ini memiliki banyak fitur salah satunya adalah kemampuan sebagai *captative hotspot gateway*, dengan fitur tersebut mikrotik dapat mengarahkan pengguna yang terkoneksi ke jaringan *hotspot* ke alamat *web* tertentu yang telah ditentukan. Dalam pemasarannya mikrotik hadir dalam berbagai jenis, baik *router board*, perangkat *wireless*, maupun *OS* yang dapat di install langsung pada sebuah *PC* (Idrus, 2016).

Kategori Latensi	Besar Delay	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	>450 ms	1

Mikrotik adalah adalah sistem operasi komputer dan perangkat lunak komputer yang digunakan untuk menjadikan komputer biasa menjadi *router*, mikrotik di bedakan menjadi dua yaitu operation sistem mikrotik bisa dikenakan mikrotik os dan mikrotik *board*, untuk mikrotik *board* tidak memerlukan komputer dalam menjalankannya cukup menggunakan *board* yang sudah *include* dengan mikrotik os. Mikrotik os mencakup fitur yang dibuat khsus untuk IP *network* dan jaringan *wireless* (Ontoseno, Haqqi and Hatta, 2017). Mikrotik sekarang ini banyak digunakan oleh *ISP*, *provider hotspot*, ataupun oleh pemilik warnet. Mikrotik *OS* menjadikan computer menjadi *router network* yang handal yang dilengkapi dengan berbagai fitur dan *tool*, baik untuk jaringan kabel maupun *wireless* (Sujalwo, 2011).

##### d. Unified Modeling Language (UML)

*Unified Modeling Language (UML)*. Adalah sebuah “bahasa” yang telah menjadi standard dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak, yaitu : *class diagram*, *use case diagram*, *activity diagram*, *sequence diagram*. (Amaliyah et al., 2021)

##### e. Sistem Keamanan Jaringan

Menurut Didha (2007:7), mengatakan bahwa pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses

yang tidak sah, atau penggunaan secara ilegal dari komputer dan jaringan. Dan dalam keamanan jaringan satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalah gunakan, *system* keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil di tembus.

Salah satu *system* keamanan jaringan komputer adalah *firewall*. *Firewall* adalah sebuah pembatas antar jaringan *local* dengan jaringan lainnya yang sifatnya *public* atau dapat diakses oleh siapapun sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya ancaman yang datang dari jaringan.

*Firewall* bekerja dengan mengamati paket IP atau *Internet Protocol* yang melewatinya. Berdasarkan konfigurasi dari *firewall* maka akses dapat diatur berdasarkan IP *address*, *port*, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall*. *Firewall* dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai tinggal melakukan konfigurasi dari *firewall* tersebut. *Firewall* juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah *server* (baik *UNIX* maupun *Windows NT*), yang dikonfigurasi menjadi *firewall*.

*Firewall* dapat dikategorikan menjadi 2 berdasarkan cara fungsi kerjanya dan keduanya dapat dilakukan pada sebuah perangkat komputer atau dilakukan secara terpisah. Dua fungsi *firewall* yaitu:

#### 1) Fungsi *Filtering*

*Firewall* bekerja pada *level* jaringan biasa disebut *packet filter*. *Firewall* tipe ini biasanya berupa *router* yang melakukan fungsi *packet filtering* berdasarkan parameter-parameter tertentu : alamat sumber, protokol, nomor *port* dan isi. Dari membandingkan informasi yang diperoleh pada paket-paket trafik dengan kebijaksanaan yang ada pada tabel akses, maka tindakan yang diberlakukan adalah :

- a. Melewatkan paket data ke tujuannya (*client* atau *server*)
- b. Mem-blok paket data

#### 2) Fungsi *Proxy*

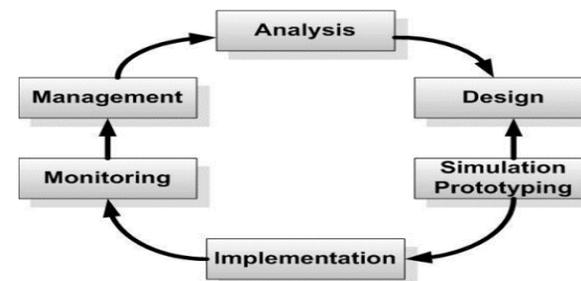
*Firewall* pada *level* aplikasi (*application level gateway*) ini berfungsi sebagai penghubung antara komputer *client* dengan jaringan luar. Pada koneksinya, paket-

paket IP tidak pernah diteruskan secara langsung, namun ditranslasi dan diwakilkan oleh *gateway* aplikasi tersebut yang berfungsi sebagai saluran dan penterjemah dan menggantikan fungsi *client*. *Proxy* akan melerai semua *request* dari *client* kepada *server* yang sesungguhnya, kemudian melerai balik semua hasil respon *real server* kepada *client* kembali.

## II. METODOLOGI PENELITIAN

### Metode Perancangan Sistem

Penulis menggunakan model pengembangan sistem *NDLC* (*Network Development Life Cycle*). Secara spesifik *NDLC* dan kegiatan yang dilakukan penulis dalam penelitian ini adalah sebagai berikut:



Gambar 2.1 Siklus *Network Development Life Cycle*

Menurut (Goldman, 2001), *NDLC* adalah kunci dibalik proses perancangan jaringan komputer. *NDLC* merupakan model mendefinisikan siklus proses pembangunan atau pengembangan sistem jaringan komputer. Kata *cycle* (siklus) adalah kata kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara eksplisit seluruh proses dan terhadap pengembangan sistem jaringan yang berkesinambungan.

### Analisis Kebutuhan

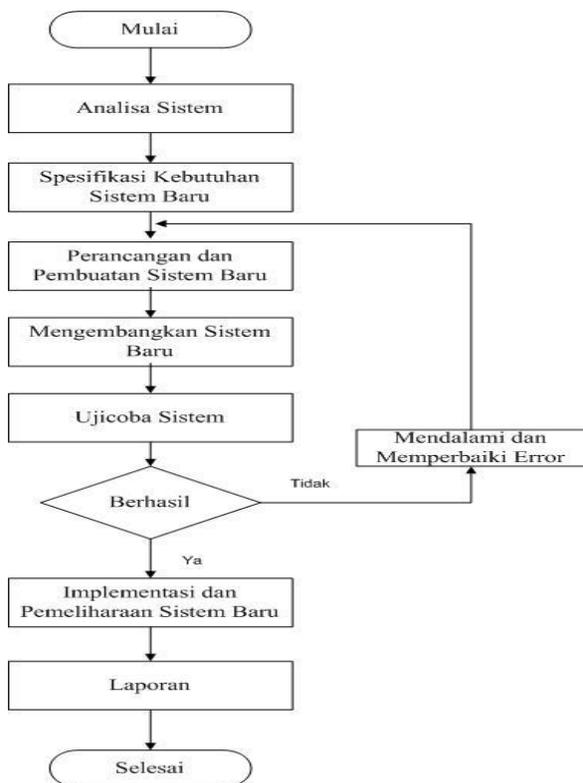
Dari siklus hidup pengembangan sebuah sistem pada metode *NDLC*. Dalam tahap ini akan dijelaskan berbagai macam kebutuhan-kebutuhan apa saja yang harus dipenuhi oleh sebuah sistem. Adapun kebutuhan yang diperlukan antara lain:

1. Kebutuhan Perangkat Keras
  - a. *Personal Computer* (PC) atau laptop dengan *Processor* CPU Intel Core I5 (2.7 GHz)
  - b. Memori 4 GB
  - c. *Hardisk* 500 GB
  - d. *Access Point* Netis WF2210 & Tenda N301
  - e. Monitor, *Keyboard*, dan *Mouse*

2. Kebutuhan Perangkat Lunak
  - a. Sistem Operasi *Windows 10*
  - b. *Mikrotik Router OS*
  - c. *MY SQL*
  - d. *XAMPP*
  - e. *Winbox*
  - f. *Wireshark*

**Tahapan Penelitian**

Penelitian ini terbagi menjadi 5 tahapan, yaitu tahap analisa manajemen jaringan, analisa permasalahan, rancangan pembuatan sistem baru, implementasi dan yang terakhir pengujian

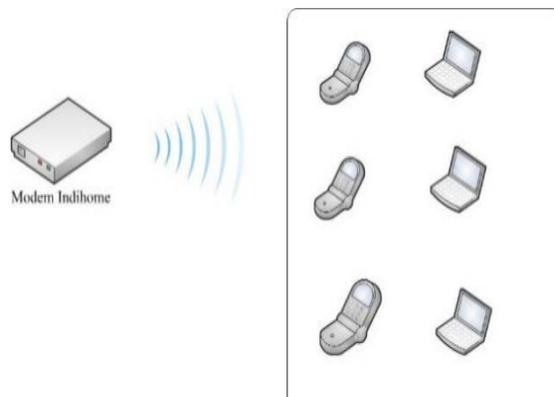


Gambar 2.2 Tahapan Penelitian

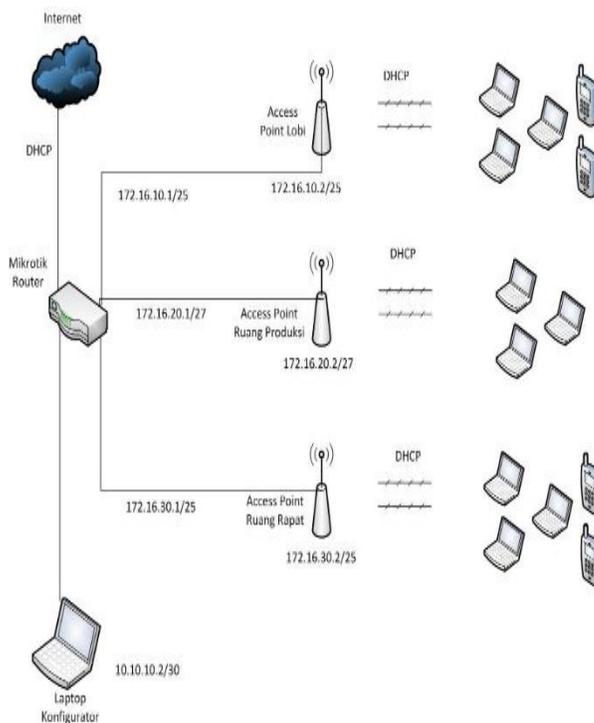
**1. Perancangan Topologi**

Perancangan tahap ini, penulis menentukan topologi dan simulasi yang akan dibangun dan mendefinisikan parameter – parameter konfigurasi yang dibutuhkan untuk menjamin sistem keamanan jaringan yang akan dibangun dapat berjalan dengan baik. Pada tahap ini dirancang suatu skema implementasi infrastruktur dengan hasil sebagai berikut dan memberikan gambaran *topologi* yang sudah ada sebagai

perbandingan:



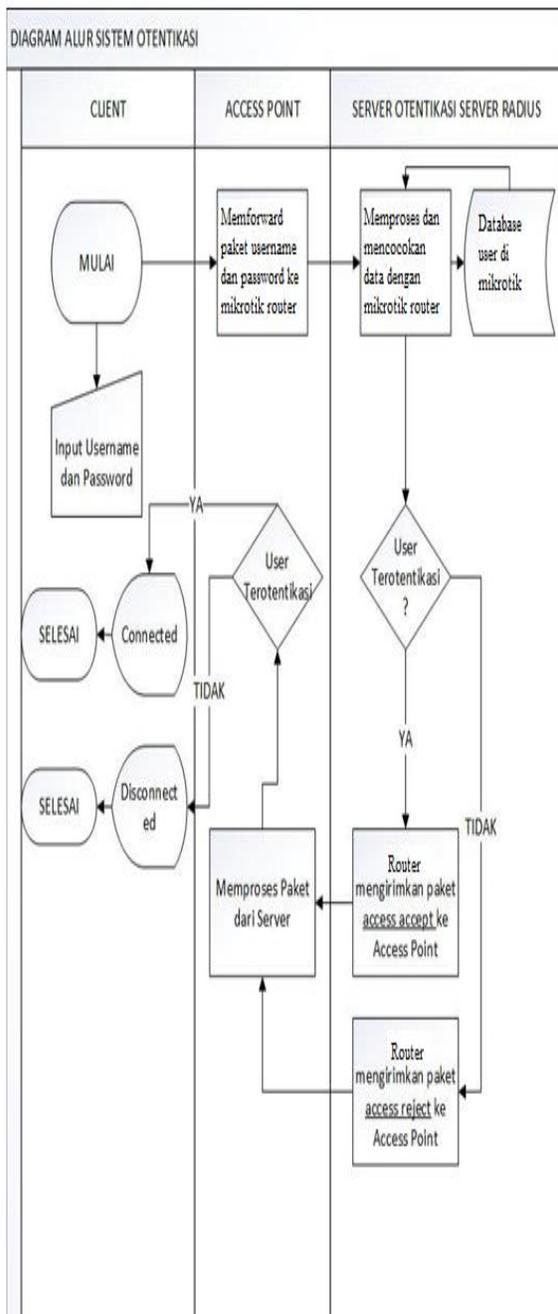
Gambar 2.3 Topologi Lama



Gambar 2.4 Topologi Baru

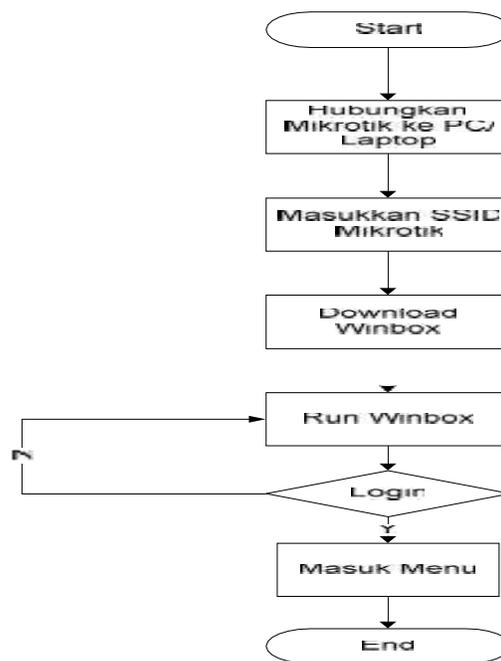
**2. Desain Sistem**

Penulis menggunakan diagram alur untuk menggambarkan dan mendefinisikan alur koneksi fungsionalitas sistem yang akan penulis bangun, sehingga dapat dengan jelas diidentifikasi dan dipahami dengan lebih mudah.



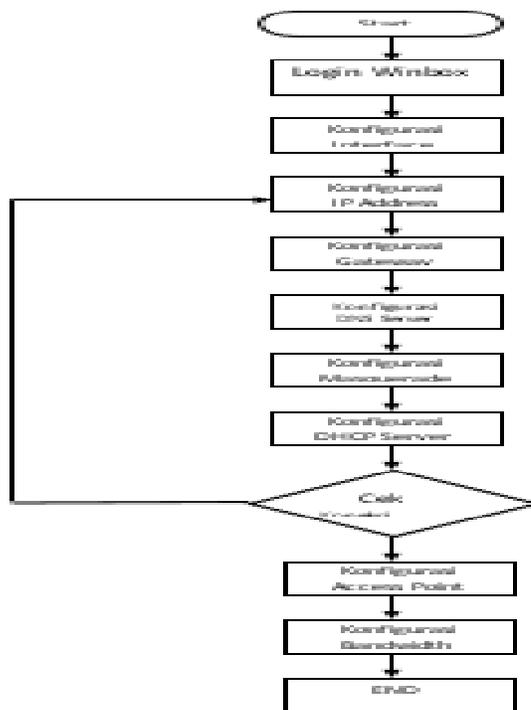
Gambar 2.5 Digram Alur Sistem Otentikasi

- a. **Rancangan Flowchart**
- i. *Flowchart Mikrotik*



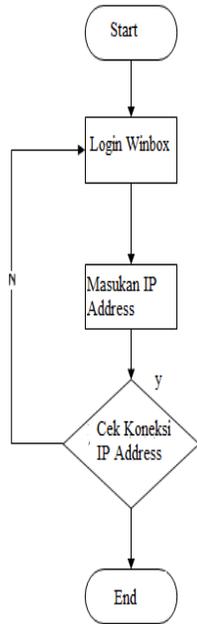
Gambar 2.6 Flowchart Mikrotik

- ii. **Flowchart Konfigurasi**



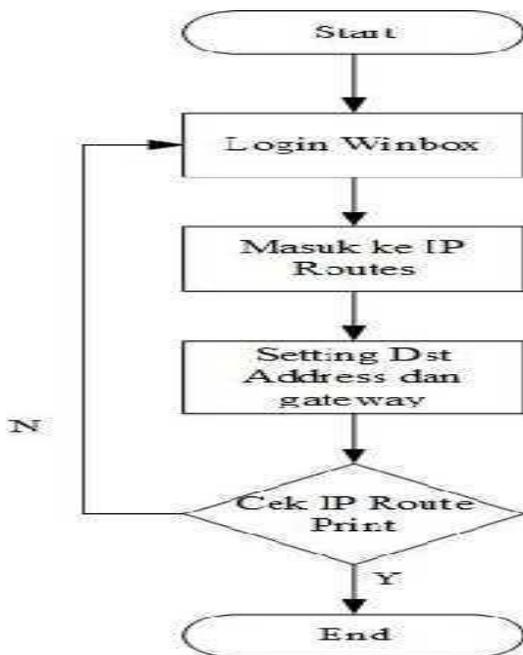
Gambar 2.7 Flowchart Konfigurasi

iii. *Flowchart Konfigurasi IP Address*



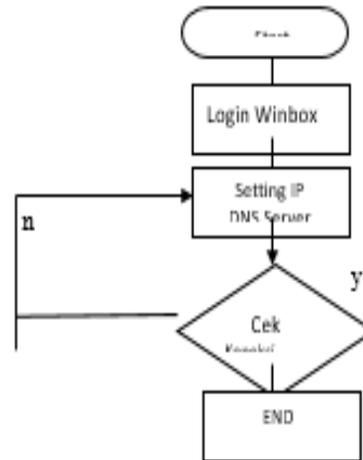
Gambar 2.8 *Flowchart konfigurasi IP Address*

iv. *Flowchart Konfigurasi Gateway*



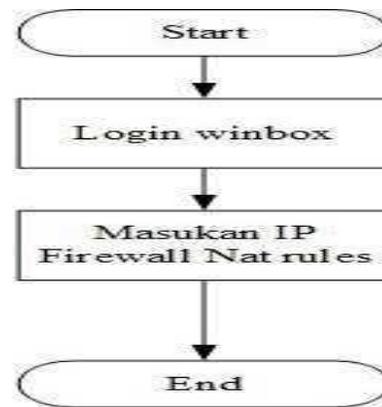
Gambar 2.9 *Flowchart Konfigurasi Gateway*

v. *Flowchart Konfigurasi DNS Server*



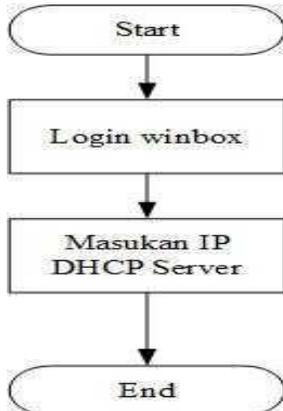
Gambar 2.10 *Flowchart Konfigurasi DNS Server*

vi. *Flowchart Konfigurasi Masquerade*



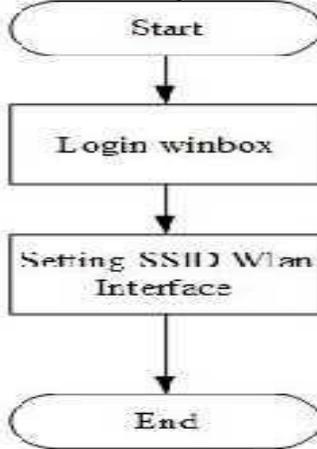
Gambar 2.11 *Flowchart Konfigurasi Masquerade*

vii. *Flowchart Konfigurasi DHCP Server*



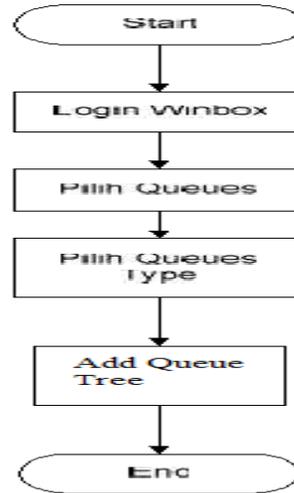
Gambar 2.12 *Flowchart* Konfigurasi *DHCP Server*

viii. *Flowchart* Konfigurasi *Access Point*



Gambar 2.13 *Flowchart* Konfigurasi *Access Point*

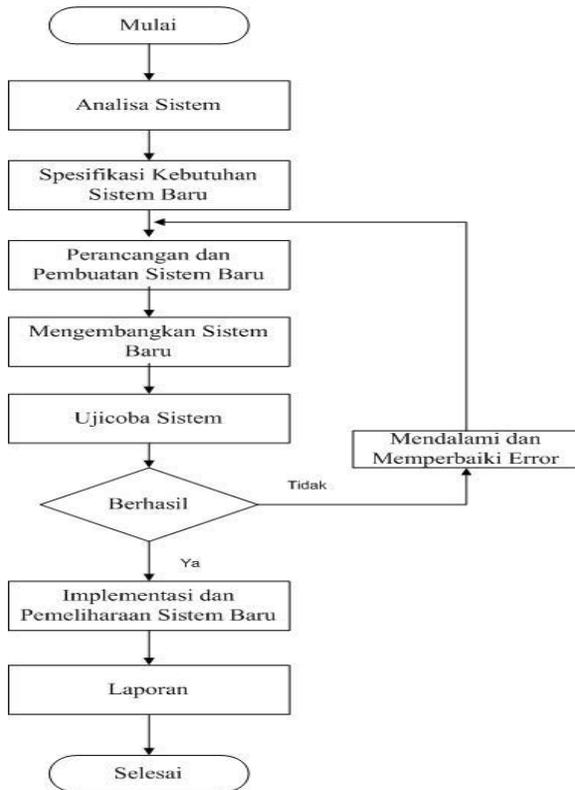
ix. *Flowchart* Konfigurasi *Bandwidth*



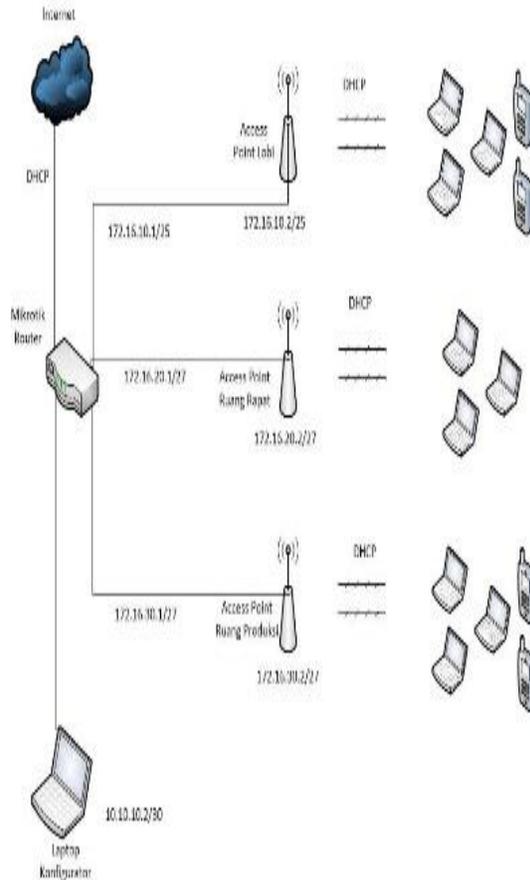
Gambar 2.14 *Flowchart* Konfigurasi *Bandwidth*

b. **Mekanisme Kerja Penelitian**

Pendefinisian gambaran umum proses kerja penelitian skripsi. Penulis mendefinisikan dan merepresentasikan metode dan alur proses penelitian, elemen-elemen, beserta interkoneksinya satu sama lainnya yang penulis terapkan pada penelitian skripsi ini dengan menggunakan pendekatan terhadap model *NDLC* dengan menggunakan media diagram model proses berikut:



Gambar 2.15 Manisme Kerja Penelitian



Gambar 3.1 Topologi Sistem

### III. IMPLEMENTASI

#### a. Implementasi

Implementasi adalah pelaksanaan dari rancangan yang telah dirancang. Implementasi tersebut adalah sebagai berikut:

##### i. Alur Sistem

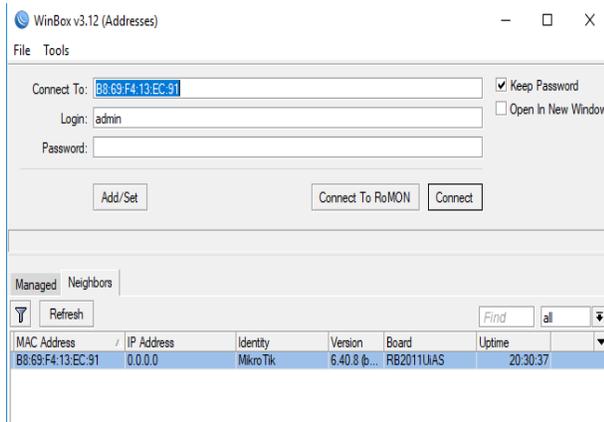
Untuk mengkoneksikan perangkat jaringan, diperlukan Topologi yang digunakan untuk mengoptimalkan jaringan *wireless* dan melakukan pengujian *QoS (Quality of Service)* dimana pada sistem ini memerlukan 1 buah *router*, 3 buah *access point*, 5 kabel UTP dan 1 buah laptop / PC sebagai konfigurator dan beberapa perangkat client, sebagai berikut

#### b. Konfigurasi Router Mikrotik

##### i. Setting IP Mikrotik

Konfigurasi *Routing* statik adalah merupakan jalur perutean (*routing*) secara manual. mikrotik akan memberikan jalur perutean (*routing*) secara otomatis jika menambahkan *ip address* di *interface* (antarmuka). Statik *routing* sangat diperlukan jika ingin menghubungkan perangkat jaringan yang memiliki *subnet* yang berbeda, jadi memerlukan perangkat yang bisa melakukan proses *routing*. Dalam penelitian ini, akan dilakukan cara menghubungkan perangkat jaringan dengan IP yang berbeda, disini akan melakukan pengaturan secara statik pada mikrotik.

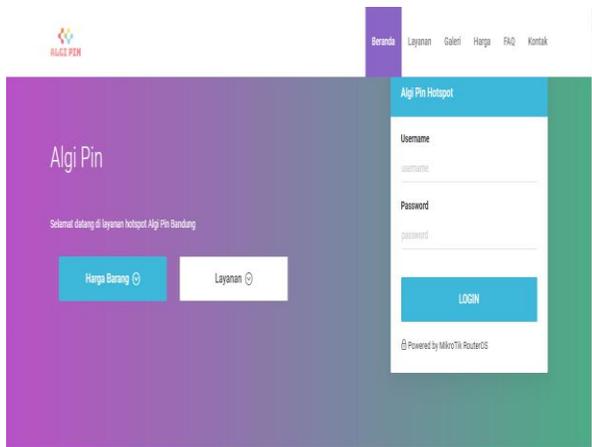
##### ii. Login ke Winbox



Gambar 3.2 Tampilan Login Winbox

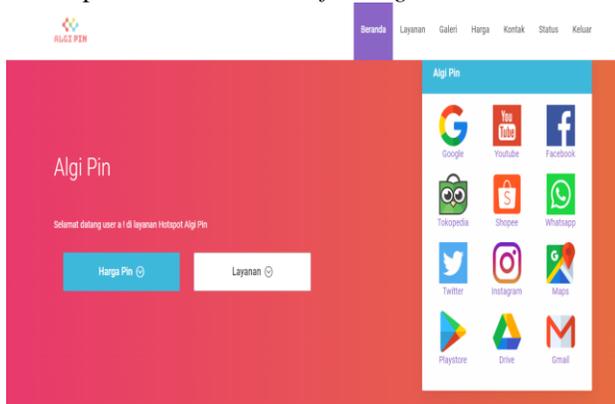
c. **Interface Sistem**

i. Implementasi Login Page Mikrotik Tamu



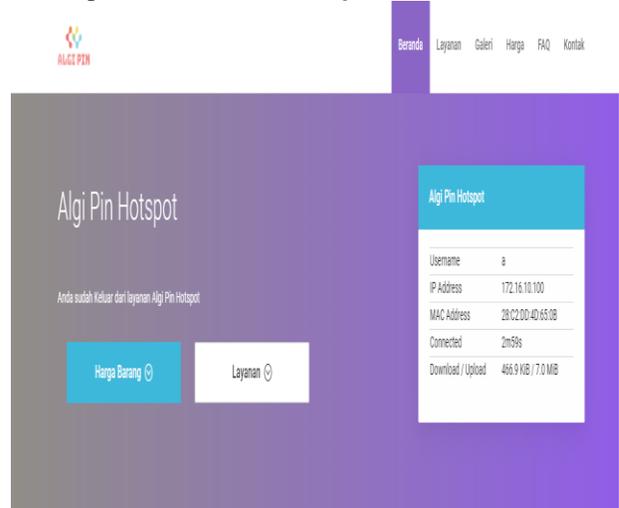
Gambar 3.3 Implementasi Login Page Mikrotik Tamu

ii. Implementasi Halaman After Login Tamu



Gambar 4.4 Implementasi Halaman After Login Tamu

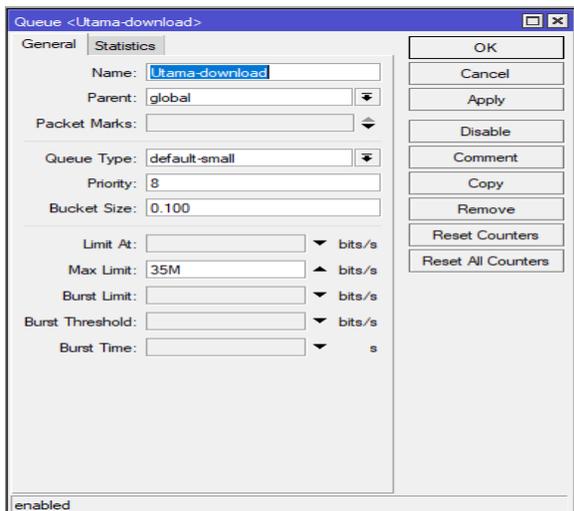
iii. Implementasi Halaman Log Out Tamu



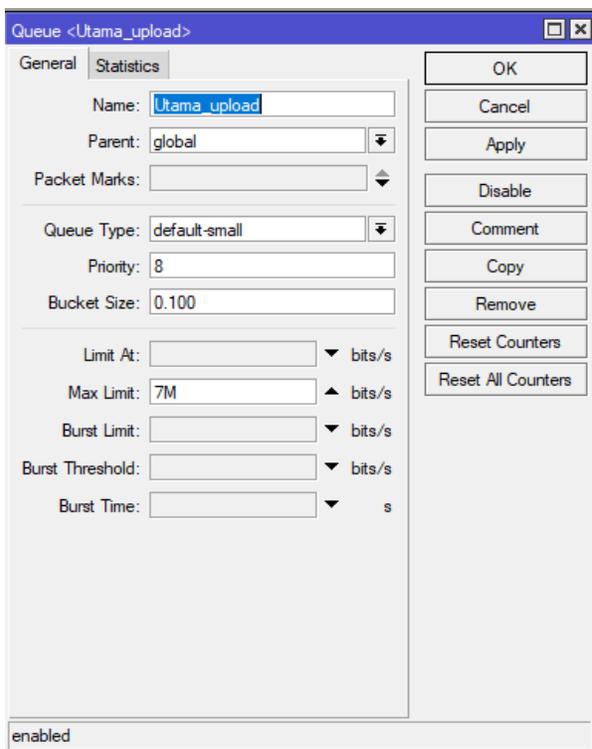
Gambar 3.5 Implementasi Halaman Log Out Tamu

d. **Konfigurasi Bandwidth Mikrotik**

Penulis menggunakan *Queues Tree* dan *PCQ* untuk melakukan manajemen *bandwidth* karena dapat melakukan pengaturan *bandwidth share* dengan menerapkan limitasi bertingkat dengan *bandwidth* utama sebesar 35 Mbps untuk *download* dan 7 Mbps untuk *upload*, maka untuk lebih mudah konfigurasi penulis mengimplementasikan *bandwidth* utama di *Queue Tree* dengan cara klik > *Queues* > *Queue Tree* > *add* isikan parameter *name* "Utama-download" *parent* "global" dan *max limit* "35M" untuk *download* dan untuk *upload* dapat diisi dengan parameter *name* "Utama-upload" *parent* "global" dan *max limit* "7M".



Gambar 3.6 Konfigurasi Parent Global Download



Gambar 3.7 Konfigurasi Parent Global Upload

**e. Blokir Sosmed dan Game**

Pada sistem pemblokiran situs-situs dan game dilakukan dengan menggunakan metode *blocking* *tls* dan *blocking port* TCP dan UDP hal ini disesuaikan karena hal tersebut tidak ada hubungannya dengan proses bisnis dan kinerja karyawan. Hal tersebut dapat

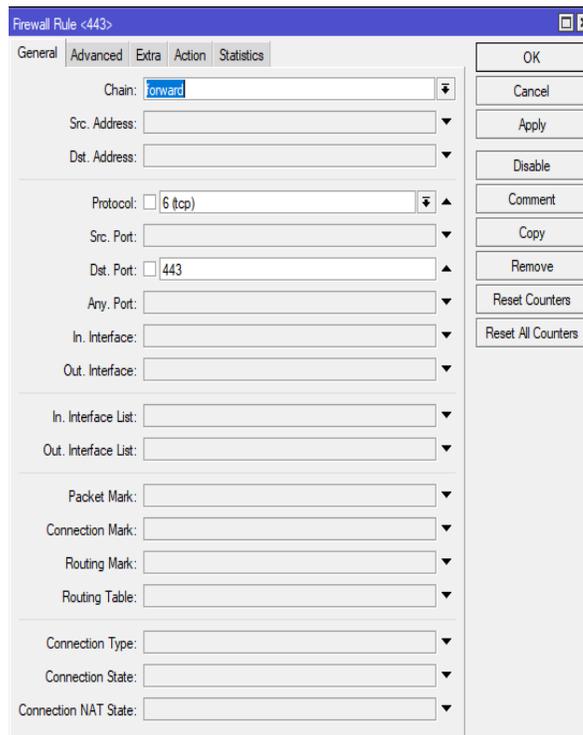
membuat karyawan lebih fokus dan berkonsentrasi dalam bekerja.

**i. Blokir Facebook**

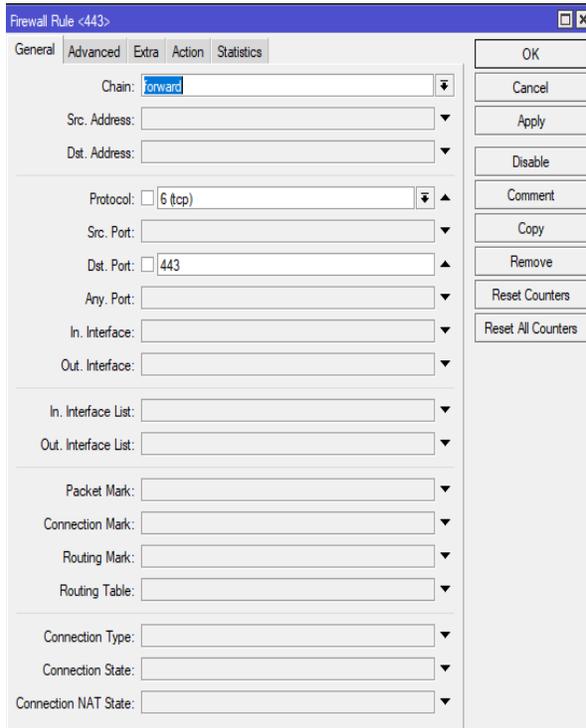
Buat firewall rule dengan cara klik IP > Firewall isikan chain forward > *protocol* TCP dan untuk destination portnya 443 kemudian untuk TLS *host* bisa di isi “\*.facebook.com” dan action reject seperti pada gambar 4.8 Konfigurasi *Firewall Blocking Facebook*, di bawah ini.

**ii. Blokir Youtube**

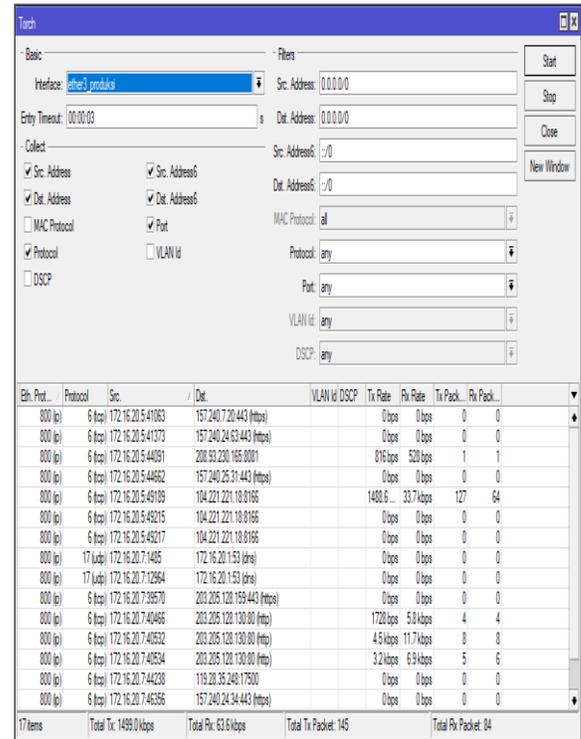
Buat firewall rule dengan cara klik IP > Firewall isikan chain forward > *protocol* TCP dan untuk destination portnya 443 kemudian untuk TLS *host* bisa di isi “\*googlevideo.com” dan action reject seperti pada gambar 4.9 Konfigurasi *Firewall Blocking Youtube* di bawah ini.



Gambar 3.8 Konfigurasi Firewall Blocking Facebook



Gambar 3.9 Konfigurasi Firewall *Blocking Youtube*



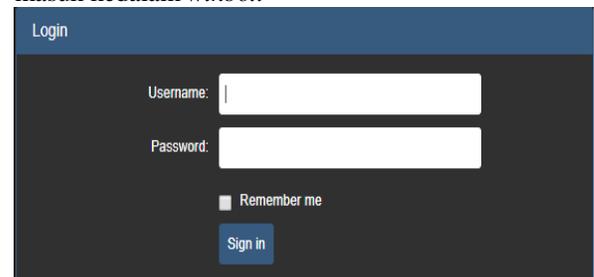
Gambar 3.10 128 List Koneksi *Game PUBG Mobile*

### iii. Blokir PUBG Mobile

Untuk memblokir *game* penulis memilih untuk memblokir *port game* daripada *IP game* yang digunakan karena khawatir aplikasi yang lain akan terganggu hal pertama yang dilakukan yaitu menangkap koneksi dari *PUBG Mobile* ke mikrotik dengan menggunakan *torch* yang dimaksudkan untuk mengetahui *port* berapa saja yang digunakan oleh *PUBG Mobile*, *torch* dapat dibuka di *winbox* dengan cara *Tool > Torch*

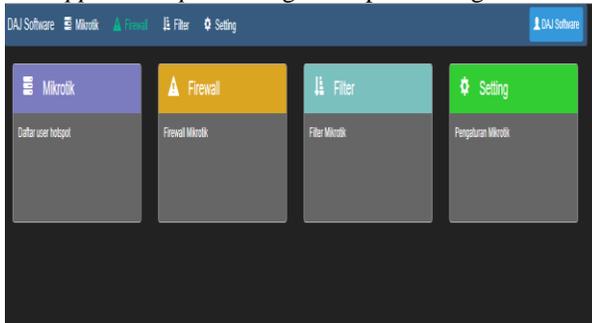
### f. Implementasi Web Panel Admin

Implementasi panel admin dibuat dengan memanfaatkan *service API (Application Programmable Interface)* di mikrotik yang memungkinkan jaringan komputer bisa saling berkomunikasi dengan *web application* atau *web site* sekalipun, pembuatan panel admin ini bertujuan untuk mempermudah tugas admin dan pimpinan dalam memantau aktivitas karyawan dan kelancaran bisnis perusahaan dimana nantinya melalui panel admin ini pimpinan bisa melihat daftar karyawan yang terkoneksi dengan *internet* perusahaan serta terdapat beberapa informasi penting, serta bisa mempermudah mematikan dan menyalakan fitur *blocking* tanpa harus masuk kedalam *winbox*



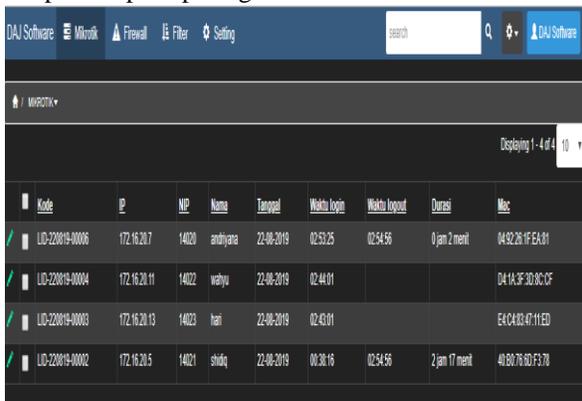
Gambar 3.11 Halaman *Login Panel Admin*

Setelah pengguna memasukan *username* dan *password* yang benar maka pengguna akan memasuki *dashboard web application panel* dengan tampilan sebagai berikut.



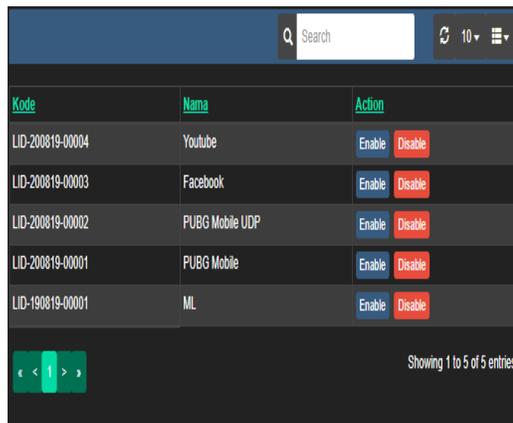
Gambar 3.12 Beranda Panel Admin

Untuk melihat pengguna yang mengakses jaringan mikrotik admin dapat melihat di tab mikrotik dengan tampilan seperti pada gambar di bawah.



Gambar 3.13 User Tab List

Pada halaman ini pengguna dapat melihat no induk pegawai, nama, tanggal, waktu *login*, waktu *logout*, durasi dan *mac address panel* tab ini tidak diketahui karyawan karena dikhususkan untuk memantau kinerja karyawan dalam bekerja sekaligus mengecek keberadaan karyawan didalam lingkungan kerja. Sedangkan untuk mematikan dan menyalakan konfigurasi *block game* dan *social media* pengguna bisa melihatnya di tab filter dengan tampilan sebagai berikut.



Gambar 3.13 Tab Filter Panel Admin

#### IV. KESIMPULAN

- 1) Perancangan sistem keamanan jaringan komputer, menjadikan jaringan komputer CV Algi Pin dapat lebih optimal karena dapat digunakan hanya untuk kepentingan bisnis di CV Algi Pin, dan untuk penggunaan WIFI tidak akan Tarik menarik *bandwidth* karena telah memiliki *bandwidth* sendiri-sendiri.
- 2) Jaringan CV Algi Pin memiliki keamanan yang lebih baik dari sebelumnya sehingga terhindar dari akses pengguna yang tidak diinginkan dan dapat menunjang kelancaran bisnis di CV Algi Pin tanpa harus khawatir dengan serangan luar.
- 3) Penggunaan panel admin dapat memudahkan admin dan pimpinan dalam mengontrol karyawan dan meringankan beban *bandwidth* karena memiliki *short cut* untuk memblokir *social media* dan game.

#### DAFTAR PUSTAKA

Amaliyah, A. Soecipto, *et al.* (2021) 'Perancangan aplikasi absensi pegawai menggunakan metode waterfall', 3, pp. 1–13.

erry Nurfajar, Soecipto, Ani Amaliyah (2021) Perancangan Aplikasi Panduan Fitness Dengan Metode Waterfall Berbasis Android pada Smartphone, Telematika pp. 1-12.

Aji, S.W. and Kharisma, R.S. (2019) 'Manajemen User Dan Pengelolaan Bandwidth Pada Jaringan Hotspot Menggunakan Router Mikrotik', *Information Tehnology Journal*, 1(2), pp. 1–5.

Ardianto, F., Alfaresi, B. and Yuansyah, R.A. (2018) 'Jaringan Hotspot Berbasis Mikrotik Menggunakan

- Metode Otentikasi Pengguna’, *Jurnal Surya Energy*, 2(2), p. 167.
- Dewi, L.C.K. and Rachmawati, R.Y. (2018) ‘ANALISIS MANAJEMEN BANDWIDTH MENGGUNAKAN METODE PCQ DENGAN MIKROTIK 951Ui-2HnD’, *Jurnal Jarkom*, 6(1), pp. 24–34.
- Doni, F.. (2015) ‘Optimalisasi Jaringan Wireless Dengan Router Mikrotik Studi Kasus Kampus Bsi Tangerang’, *175.45.187.195*, II(1), p. 31124.
- Febriyanti, E., Raharjo, S. and Sholeh, M. (2017) ‘Perbandingan Manajemen Bandwidth Menggunakan Metode FIFO (First In First Out) dan PCQ (Peer Connection Queue) Pada Router Mikrotik (Studi Kasus Pada Laboratorium Komputer Jaringan, Institut Sains & Teknologi AKPRIND Yogyakarta)’, *Jurnal JARKOM*, 5(2), pp. 89–98.
- Idrus, A. (2016) ‘Sistem Monitoring Jaringan PT. Exhibition Network Indonesia Dengan The Dude Berbasis Mikrotik’, *Informatics for Educators and Professionals*, 1(1), p. 234408.
- Muklas, Supendar, H. and SW, S. (2020) ‘Optimalisasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Filtering Dan Manajemen Bandwith Pada PT. Intav Prima Solusindo’, *Tekinfor*, 21(1), pp. 104–111.
- Ontoseno, R.D.H., Haqqi, M.N. and Hatta, M. (2017) ‘Limitasi Pengguna Akses Internet Berdasarkan Kuota Waktu Dan Data Menggunakan Pc Router Os Mikrotik’, *Teknika: Engineering and Sains Journal*, 1(2), p. 125.  
<https://doi.org/10.51804/tesj.v1i2.134.125-130>.
- Pratama, A.A., Susilo, B. and Coastera, F.F. (2018) ‘Manajemen Bandwidth Dengan Queue Tree Pada Rt / Rw-Net Menggunakan Mikrotik’, *Rekursif*, 6(2), pp. 31–42.
- Saniya, Y., Priyono, W.A. and Ambarwati, R. (2013) ‘Sistem Manajemen Bandwidth dengan Prioritas Alamat IP Client’, *Jurnal Penelitian*, pp. 1–6.
- Sujalwo, S. (2011) ‘Manajemen Jaringan Komputer dengan Menggunakan Mikrotik Router’, *Komuniti: Jurnal Komunikasi dan Teknologi Informasi*, 2(2), pp. 32–43.