

BAB II LANDASAN TEORI

2.1 Tinjauan Pustaka

Menurut penelitian yang dilakukan (Rahman, 2018) yang berjudul "Implementasi Interface Virtual Local Area Network dan Firewall pada Mikrotik dan Switch Manajemen" menjelaskan bahwa router Mikrotik memiliki fungsi sebagai alat penghubung jaringan luar dan jaringan lokal menjadi satu jaringan. Pengaturan *firewall* pada mikrotik dapat memisahkan dan menyeleksi lalu lintas dalam jaringan sehingga jumlah *broadcast* dari suatu jaringan lebih rendah dan lebih mudah untuk dimonitor. Mikrotik tersebut digunakan sebagai alat untuk mendeteksi kegagalan koneksi, memonitor lalu lintas transfer data dan data masuk dan keluar, beserta akses web.

Menurut penelitian (Nurfauzi et al., 2018) yang berjudul "Implementasi "Firewall Filtering Web dan Manajemen Bandwith Menggunakan Mikrotik" menjelaskan bahwa firewall yang terdapat pada router mikrotik melakukan perlindungan terhadap keamanan jaringannya dengan melakukan proses filter data dan melakukan pemeriksaan data yang menentukan data diperbolehkan masuk atau ditolak. *Firewall* pada router tersebut juga berperan sebagai penghubung dan menerima *proxy host* yang diamankan. Pada saat yang sama, firewall memberikan akses point hanya untuk IP yang diberikan.

Menurut penelitian yang dilakukan (Aprilianto, Fadila, & Muslim, 2019) dengan judul "Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik" menjelaskan bahwa *firewall* yang dikonfigurasi dalam sistem mikrotik memeriksa data yang diterima dan melacak koneksi tersebut diijinkan

atau ditolak. Penggunaan *Firewall* digunakan untuk menyaring user yang terkoneksi dan melakukan penghalangan akses dari user yang diblokir.

Menurut penelitian yang dilakukan oleh (Siddik, 2017). Dengan judul “Implementasi Mikrotik Router Board 750 Sebagai Firewall Blok Situs Pada Jaringan Lan” Menjelaskan bahwa *firewall* merupakan alat yang digunakan sebagai alat keamanan jaringan yang berfungsi untuk memfilter akses web atau situs yang kemungkinan mengandung konten yang tidak pantas meskipun telah diblokir sesuai peraturan pemerintah namun masih tetap dapat diakses. Dengan menutup sistem yang negatif maka akan menguntungkan client dan mengurangi terjadinya jenis penyerangan pada jaringan yang tersedia.

Penelitian yang dilakukan (Fu, Hsu, Kao, Tsai, & Tseng, 2017) dengan judul “*An Autoblocking Mechanism for Firewall Service*” menjelaskan Firewall dapat dirancang untuk melakukan fungsinya untuk menjaga keamanan dari serangan luar secara otomatis yang mematikan IP sumber dari jaringan tersebut.

Hasil yang dilakukan adalah mengurangi jalur lalu lintas yang signifikan dan meningkatkan stabilitas jaringan.

Hasil Penelitian dari para peneliti dapat disimpulkan bahwa *Firewall* adalah sistem konfigurasi keamanan jaringan yang memiliki cara kerja menyaring dan menyeleksi serta memonitor jalur lalu lintas jaringan dan user untuk masuk ke dalam jaringannya. Keamanan jaringan yang menggunakan firewall bergantung pada user yang mengkonfigurasi jaringan tersebut.

2.2 Landasan Teori

2.2.1 Jaringan Komputer

Jaringan komputer adalah sistem didalam sebuah area yang terdiri dari komputer dan alat jaringan lainnya yang melakukan tugas dengan waktu yang sama. Tujuan dari dilakukan rancangan jaringan komputer adalah melakukan pengolahan data, dan informasi (Yudianto, 2014). Untuk tercapainya tujuan tersebut, setiap bagian dari jaringan harus melakukan layanannya dengan baik dinamakan dengan istilah *client-server*, dan umumnya dipakai untuk seluruh sistem komputer (Kodama, Nakagawa, Tanouchi, & Kameyama, 2016).

Berdasarkan jangkauannya, jaringan komputer dibedakan menjadi 5 jenis, yaitu:

1. *Local Area Network (LAN)*

Local Area Network adalah komunikasi antar jaringan yang menghubungkan beberapa perangkat dan melakukan pertukaran data yang dilakukan di dalam jaringan yang terhubung (Rahman, 2018).

2. *Metropolitan Area Network (MAN)*

Metropolitan Area Network adalah komunikasi antar jaringan yang memiliki jangkauan lebih besar dari LAN ,umumnya dipakai sebagai penghubung antar wilayah dalam satu provinsi. (Nadir, Ali, Hossain, & Parvez, 2015)

3. *Wide Area Network (WAN)*

Wide Area Network adalah komunikasi antar jaringan yang memiliki jangkauan lebih luas dari LAN dan WAN, biasanya digunakan sebagai

jaringan antar negara dengan menggunakan media seperti satelit atau kabel dalam bawah laut (Nadir et al., 2015).

4. *Wireless Local Area Network (WLAN)*

Wireless Local Area Network adalah sistem jaringan yang menggunakan media gelombang radio untuk media transmisi, untuk memberikan koneksi pada semua pemakai dalam area tersebut. (Kusriyanto & Putra, 2017).

5. *Radio Area Network (RAN)*

Radio Area Network adalah Bagian dari sistem telekomunikasi yang menghubungkan perangkat individu ke bagian lain dari jaringan melalui koneksi radio. RAN berada di antara peralatan pengguna, seperti ponsel, komputer atau mesin yang dikendalikan dari jarak jauh, dan menyediakan koneksi dengan jaringan intinya (Wu, Zhang, Hong, & Wen, 2015).

Berdasarkan fungsi, komputer dibedakan menjadi 2 tipe yaitu jaringan yaitu Jaringan *peer-to-peer* (P2P) dan jaringan *Client-server*.

Dalam jaringan *peer-to-peer*, peran dari seluruh komputer yang dihubungkan dalam jaringan setara, tidak ada yang lebih mendominasi. Dalam jaringan tersebut, setiap user yang merupakan bagian dalam jaringan memungkinkan untuk berkomunikasi. Sedangkan dalam jaringan *Client-server* terdapat komputer yang berfungsi sebagai pusat untuk mengatur peran setiap komputer, seperti komunikasi, *server* adalah peran untuk tugas komputer yang mengontrol jaringan dan sebagai pusat utama, dan komputer lainnya disebut *client* (Wu et al., 2015).

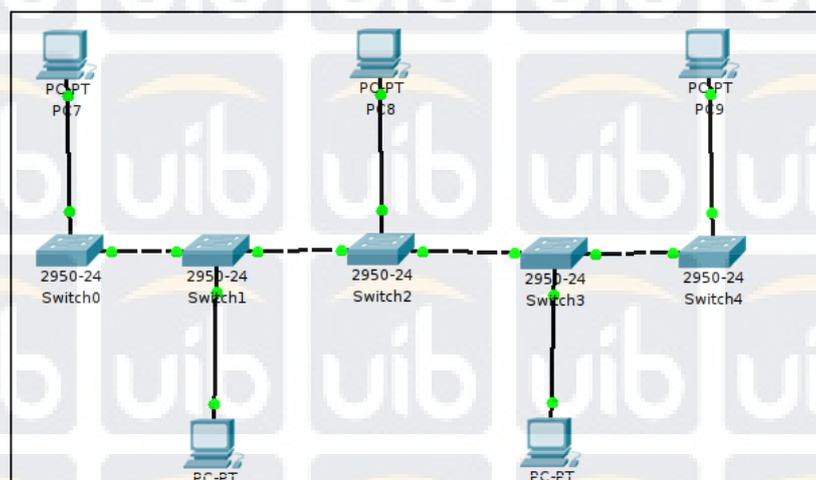
2.2.2 Topologi Jaringan komputer

Topologi adalah sebuah peta pola penghubung antara jaringan komputer, Pola tersebut memiliki peran yang kuat untuk hak akses dan tujuan yang diberikan dan dibuat berdasarkan kondisi geografis pada masing-masing terminal. Topologi dibagi menjadi topologi bus, topologi ring, topologi mesh dan topologi star. (Chandra & Kosdiana, 2018)

1. Topologi *Bus*

Topologi *Bus* adalah keadaan jaringan yang dimana terdapat *backbone* tunggal sebagai penghubung node-node. Karakteristik Topologi tersebut adalah satu kabel panjang yang menghubungkan seluruh perangkat pada topologi tersebut, kabel tersebut yang memiliki tugas sebagai *backbone*. konektor T adalah kabel yang biasa digunakan pada topologi bus. Konektor tersebut dipakai untuk mengatur dan memisahkan jalur dengan tujuan agar perangkat dapat dihubungkan pada kabel utama (E. Kurniawan, 2016) seperti Gambar

1.

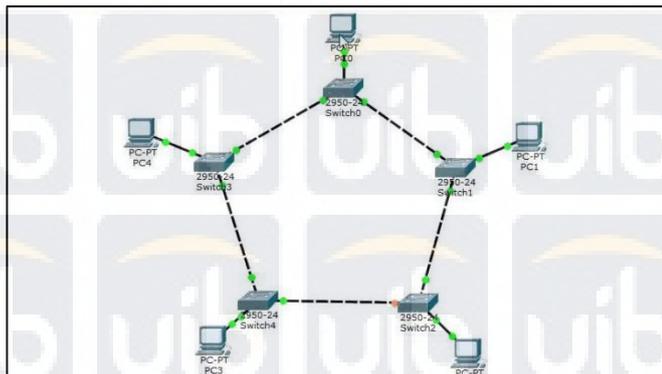


Gambar 1 Topologi Bus

2. Topologi Ring

Topologi Ring adalah keadaan dalam sebuah jaringan dimana perangkat hubungan pada setiap jaringan terdapat node awal yang terhubung dengan yang terakhir sehingga berbentuk seperti cincin (E. Kurniawan, 2016).

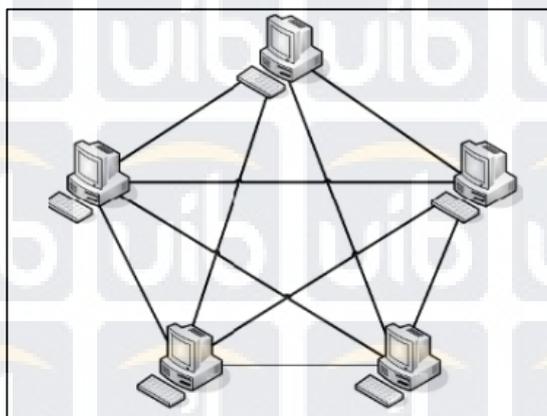
Topologi Ring dapat dilihat pada Gambar 2



Gambar 2 Topologi Ring

3. Topologi Mesh

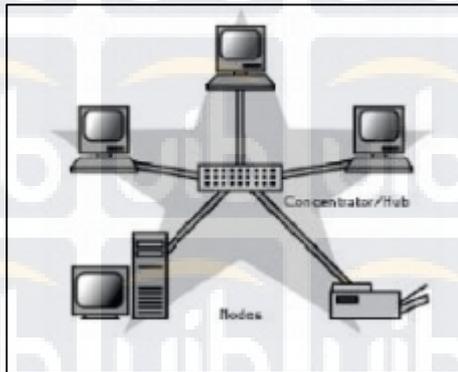
Topologi *mesh* menggunakan jaringan dimana setiap perangkat jaringan terhubung satu sama lain. Dalam topologi tersebut, komputer dapat saling komunikasi tanpa perantara komputer lain (E. Kurniawan, 2016). Topologi Mesh dapat dilihat pada Gambar 3.



Gambar 3 Topologi Mesh

4. Topologi Star

Topologi suatu jaringan yang menggunakan satu perangkat jaringan sebagai pusat penghubung dari berbagai macam perangkat komputer dikenal dengan istilah topologi *star* (E. Kurniawan, 2016). Topologi Star dapat dilihat pada Gambar 4.

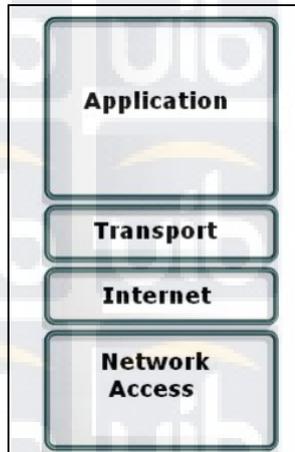


Gambar 4 Topologi Star

2.2.3 Protokol Komunikasi

Protokol adalah sebuah peraturan yang dibuat untuk menjaga operasi unit fungsional dapat berjalan dengan baik. Protokol mempunyai beberapa fungsi diantaranya adalah enkapsulasi, segmentasi, kontrol koneksi, pengiriman sesuai order, *Flow* kontrol, *Error* kontrol dan fungsi lainnya. (Wibowo, 2018). Peran protokol sangat dibutuhkan dikarenakan merupakan pedoman yang wajib dilakukan dalam membangun sebuah jaringan. Protokol sendiri mempunyai manfaat yang penting, seperti pengiriman dan pembagian informasi antara perangkat satu dan yang lainnya. Selain itu, protokol juga memiliki peran dalam pengontrolan dan pengaturan pada koneksi, memberikan serta melakukan perintah pada sebuah jaringan, memberikan layanan yang berbasis dan elektronik, dan manfaat lainnya. Terdapat 2 protokol komunikasi, yaitu:

1. Model referensi TCP/UDP



Gambar 5 Model TCP/UDP

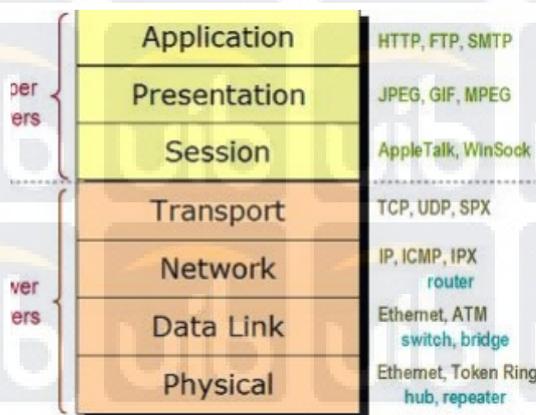
TCP/IP memiliki kumpulan set yang dimana protokol utamanya yaitu *Transmission control protocol* dan *internet protocol*. Model ini memiliki tujuan untuk membuat komunikasi antara komputer yang mempunyai perbedaan dalam karakteristiknya dalam *hardware* maupun *software*. TCP/IP memiliki karakteristik seperti *open protocol standart*, yaitu perkembangannya terlepas dari *hardware* dan sistem operasi, Terpisah dari perangkat keras jaringan khusus, Memiliki skema pengamatan yang dapat dikendalikan secara spesifik. (E. Kurniawan, 2016)

TCP/IP terdiri dari empat layer yang tiap layer-nya mempunyai tujuan yang beragam dimulai dengan *Application Layer* sampai *Network Access Layer*. (E. Kurniawan, 2016)

Application Layer berfungsi menangani layer tingkatan atas, seperti *encoding* dan dialog kontrol untuk mengizinkan suatu hubungan komunikasi pada aplikasi terhadap jaringan. *Transport Layer* memberikan layanan pengiriman menuju tujuan data dari sumbernya. Selain itu, layer tersebut juga merombak dan

membentuk kembali data dari *application layer* menuju hal yang sama antara sumber dan tujuan data. *Layer* berikut terdiri atas dua protokol yaitu TCP dan UDP. TCP mempunyai orientasi terhadap keaslian data sedangkan UDP pada pemakaian komunikasi data. *Internet Layer* berperan untuk mencari rute terbaik untuk dilewati paket data dalam sistem. *Network Access Layer* bertugas dalam mengontrol semua paket IP untuk dapat terjadinya komunikasi melalui medium fisik jaringan, yaitu LAN dan WAN (E. Kurniawan, 2016).

2. Model Referensi OSI



Gambar 6 Model OSI

Model referensi OSI menyediakan kondisi dasar perancangan pada jaringan komputer berdasarkan kompatibilitas antara produk dan teknologi yang tersedia. (E. Kurniawan, 2016)

Pada Model OSI, ada tujuh layer yang menggambarkan fungsi – fungsi jaringan yaitu *Application Layer*, *Presentation Layer*, *Session Layer*, *Transport Layer*, *Network Layer*, *Data Link Layer*, dan *Physical Layer* (E. Kurniawan, 2016).

Application Layer merupakan yang terdekat dengan pengguna, layer ini memiliki tujuan sebagai layanan dari jaringan kepada *user*. *Presentation Layer*

melakukan pengolahan data yang telah tersedia dari layer aplikasi supaya data yang terkirim bisa dianalisa oleh aplikasi dalam sistem lainnya. *Session Layer* berfungsi untuk mengontrol sesi komunikasi. *Transport Layer* berfungsi untuk memecahkan data dan menyusun kembali data yang dipecah untuk menjadi sebuah data yang dapat dianalisa. *Network Layer* menyediakan pengiriman informasi di antara puncak sistem yang melewati jaringan komunikasi secara terus menerus dan berperan sebagai pemilih alur terbaik dalam komunikasi antar jaringan. *Data Link Layer* menyediakan alamat komputer, pesan *error*, dan pesanan dalam pengiriman data. *Physical Layer* berfungsi untuk membangun data menjadi bit (E. Kurniawan, 2016).

2.2.4 Peralatan Jaringan

Untuk membuat dua atau lebih komputer terhubung, diperlukan peralatan jaringan yang bertujuan untuk menghubungkan komputer-komputer tersebut. (Pimenidis et al., 2017) Peralatan jaringan terdiri dari

1. Router



Gambar 7 Router

Router adalah alat pada jaringan yang berperan sebagai perantara yang tugasnya menghubungkan dua jaringan atau lebih yang berbeda. Contohnya 192.168.50.0/24 dan 10.10.10.0/24

2. Switch



Gambar 8 Switch

Switch merupakan peralatan jaringan yang berfungsi untuk menghubungkan dua perangkat atau komputer dalam jaringan yang sama.

3. Kabel LAN



Gambar 9 Kabel LAN

Kabel LAN digunakan untuk menghubungkan port-port yang terdapat dalam perangkat jaringan.

4. Bridge



Gambar 10 Bridge

Bridge adalah alat jaringan berfungsi untuk menambah area jaringan dan membuat sebuah segmen jaringan.

5. Repeater



Gambar 11 Repeater

Repeater adalah perangkat jaringan digunakan untuk menambah jangkauan sinyal wifi dari server.

2.2.4. Jaringan berbasis Internet

Internet adalah sarana yang menghubungkan jutaan komputer untuk saling berkomunikasi dan berinteraksi. Internet juga merupakan sarana yang efisien untuk melakukan komunikasi jarak jauh maupun di lokal perusahaan. Fasilitas yang disediakan oleh internet (Ilmu Berazam, Marubah Siringo, Pranata, & Sitohang, 2018), adalah sebagai berikut.

1. WWW (*World Wide Web*), merupakan halaman pada internet yang menampilkan informasi yang dapat berupa gambar, teks, dan lainnya.
2. FTP (*File Transfer Protocol*), merupakan aplikasi yang berfungsi untuk melakukan terjadinya pertukaran data.
3. IRC (*Internet Relay Chatting*), merupakan aplikasi yang digunakan untuk melakukan komunikasi dengan menggunakan modus teks.

E-mail (*Electronic mail*), merupakan sarana pengiriman surat melalui internet dalam bentuk surat.

2.2.5 Routing

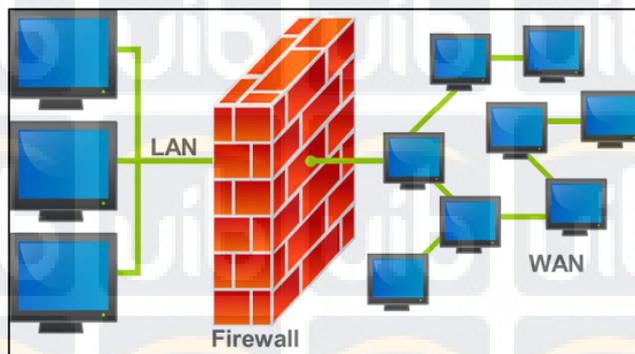
Routing adalah proses pencarian dan pemilihan lalu lintas data di dalam jaringan. Protokol dalam routing dibedakan menjadi tiga, yaitu : *distance vector*, *link state* dan *hybrid*. Routing dalam penentuan jalur lalu lintas datanya dibedakan menjadi dua yaitu *Static Routing* dan *Dynamic Routing*. (Pambudi & Muslim, 2017),

Dalam *Static Routing*, *Router* dikonfigurasi untuk menentukan jalur data sesuai dengan yang dikonfigurasi oleh user. Penggunaan metode ini sangat cocok untuk jaringan skala kecil sedangkan dalam *Dynamic Routing*, *Router* dikonfigurasi untuk menentukan jalur datanya secara otomatis yang dikonfigurasi melalui *routing protocol* (Pambudi & Muslim, 2017),.

2.2.6 Firewall

Firewall merupakan perangkat lunak dalam komputer yang melakukan penyaringan pada lalu lintas jaringan untuk menentukan data yang dinyatakan tidak

membahayakan dan melakukan pencegahan terhadap lalu lintas data yang dianggap membahayakan. Firewall biasanya dipasang pada perangkat keras jaringan yang menghubungkan jaringan lokal dan jaringan luar (Elmallah & Gouda, 2017).



Gambar 12 Firewall

Firewall memiliki kateristik

berikut (A. X. Liu et al., 2017).

1. Seluruh transaksi yang terjadi dari dalam jaringan menuju internet , wajib untuk melewati firewall. Hal ini dilakukan dengan memblokir atau memutuskan komunikasi semua akses terhadap jaringan Lokal, kecuali dapat melewati firewall.
2. Hanya transaksi yang dikenali atau dianggap aman yang dapat melewati , hal ini dilakukan dengan membuat *policy* atau peraturan pada penyetelan konfigurasi pada keamanan jarinagan.
3. *Firewall* haruslah kebal dan relatif kuat terhadap serangan dari luar. hal ini menunjukkan pengguna dari sistem bisa diandalkan dengan *operating system* yang aman.

Firewall sendiri menggunakan teknik sebagai berikut untuk melakukan fungsinya (A. X. Liu et al., 2017).

1. *Service Control*

Firewall melakukan pemeriksaan alamat IP bahkan melengkapi kelengkapan dari sebuah layanan sebelum memasuki layanan jaringan yang dijadikan tujuan dari pengiriman.

2. *Direction Control*

Firewall melakukan filter berdasarkan permintaan terhadap layanan dan diperbolehkan untuk melewati *firewall*

3. *User Control*

berdasarkan pengguna dalam melakukan layanan, artinya ada pengguna yang memiliki hak atau tidak dalam melakukan layanan, hal ini terjadi apabila pengguna tidak diijinkan melewati system tersebut. Biasanya digunakan sebagai pembatasan user dari jaringan lokal untuk melakukan layanan internet, dan juga sebaliknya

4. *Behaviour control*

Didasarkan dari seringnya layanan itu dipakai, yang mempengaruhi penyaringan dan pengontrolan data yang melewati layanan jaringan.

Firewall dibagi menjadi dua jenis yaitu *personal firewall* dan *network firewall*. *Personal firewall*, mempunyai tujuan dalam perlindungan komputer yang terhubung dalam jaringan dari serangan yang tidak diketahui. Perkembangan sistem ini adalah program yang dibentuk untuk menjaga keamanan komputer secara keseluruhan, dan ditambahkan dengan beberapa fitur pengamanan lainnya seperti

proteksi *virus, malware, spam*, dan lainnya termasuk dengan sistem IDS (*Intrusion Detection system*). *Network Firewall* bertujuan untuk mengontrol keamanan dalam sebuah jaringan. *Network firewall* umumnya terletak pada perangkat jaringan seperti *router* atau pada perangkat lunak yang terdapat pada server. Paket *firewall* tersebut bersifat transparan dan menggunakan routing untuk menentukan paket atau jalur data yang diperbolehkan (A. X. Liu et al., 2017).

Pada Router Mikrotik terdapat fitur-fitur firewall yang meliputi inspeksi paket, paket content, kualitas paket, besar paket, penyaringan protokol, *Layer 7* Protokol, alamat MAC, jarak port ke port, Protokol IP, dan lainnya (Muzakir & Ulfa, 2019).

Ada tiga chain tersedia pada firewall yang terdapat di mikrotik yaitu *Input*, *Forward* dan *Output*.

2.2.7 Network Development Life Cycle (NDLC)

NDLC merupakan metode perancangan yang dibuat berdasarkan pada proses pembangunan yang biasanya digunakan sebagai perancangan proses bisnis dan infrastruktur (Kunci, 2019). NDLC terdiri dari enam tahapan yaitu analisa, desain, simulasi, implementasi, pemantauan, dan manajemen (Supriadi, Fahmi, & Imtihan, 2018).

1. Analisis : Tahap pertama yang dilakukan adalah analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa jaringan yang sudah ada saat ini (Supriadi et al., 2018).

2. Wawancara, tahap yang dilakukan selanjutnya dengan pihak yang terkait dari struktur manajemen puncak sampai posisi yang bawah untuk mendapat data yang tepat dan lengkap. Dalam kasus dalam perancangan sistem informasi biasanya disertai *brainstorming* untuk mengatasi masalah yang diberikan karena karakteristik yang beragam (Supriadi et al., 2018).
3. Survey langsung lapangan, dalam tahap analisis tersebut, survey dilakukan di lapangan untuk memperoleh hasil secara tepat dan keseluruhan sebelum masuk ke tahap selanjutnya. Seperti menganalisa topologi dari sebuah organisasi (R. Kurniawan, 2016).
4. Implementation :. Dalam tahap ini, pemakaian akan menerapkan segala hal yang telah direncanakan dan di design pada tahap sebelumnya (Supriadi et al., 2018).
5. Monitoring : tahap ini merupakan tahapan yang berperan penting, dikarenakan untuk memastikan kerja dari jaringan komputer dan sistem komunikasi bekerja sesuai yang diharapkan dan tercapainya hasil yang diharapkan pada awal perancangan dari user pada awal perancangan yaitu analisa, maka diperlukan untuk dilakukan *monitoring* pada tahap ini. *Monitoring* adalah aktivitas analisa yang dilakukan pada Infrastruktur hardware , seperti menganalisa keadaan reliabilitas terhadap sistem yang telah dirancang ,Menganalisa jalur paket data dalam jaringan. Pendekatan umumnya digunakan dalam tahap tersebut adalah pendekatan Network Management. Melalui metode ini semua perangkat dan kegiatan dalam

sebuah jaringan dapat diperhatikan secara keseluruhan (Supriadi et al., 2018).

6. Management, pada tahapan tersebut, salah satu hal yang wajib diperhatikan adalah masalah pengaturan, yaitu kebijakan perlu dirancang untuk mengontrol agar sistem yang berhasil dirancang dapat berjalan sesuai dengan ekspektasi dan dapat beroperasi dalam jangka waktu lama sehingga tahap reliabilitas terjaga. Pengaturan bergantung terhadap kebijakan pada peringkat manajemen dan strategi dalam bisnis yang dilakukan perusahaan tersebut. Personil harus dapat mendukung atau menggunakan gagasan yang setara dengan strategi yang dilakukan dalam bisnis perusahaan (Supriadi et al., 2018).

2.3 Tools yang digunakan

2.3.1 Mikrotik Routerboard

Mikrotik adalah perangkat jaringan yang berperan sebagai penghubung jaringan yang sama dan jaringan yang berbeda dengan penggunaan fitur-fitur yang terdapat didalamnya. Fitur-fitur dalam mikrotik ,yaitu: Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, dan masih banyak lagi fitur lainnya. MikroTik routerOS merupakan sistem operasi Linux base(Supendar & Siregar, 2018).

2.3.2 Winbox

Winbox adalah aplikasi komputer sederhana yang berfungsi untuk mengatur konfigurasi *router* Mikrotik dengan tampilan GUI. Peranan winbox adalah untuk melakukan konfigurasi router yang terhubung pada jaringan yang sedang terhubung. Selain konfigurasi, perangkat lunak tersebut juga dapat melihat dan memantau trafik data yang sedang terjadi (Issa, 2016).