

BAB II

KAJIAN PUSTAKA

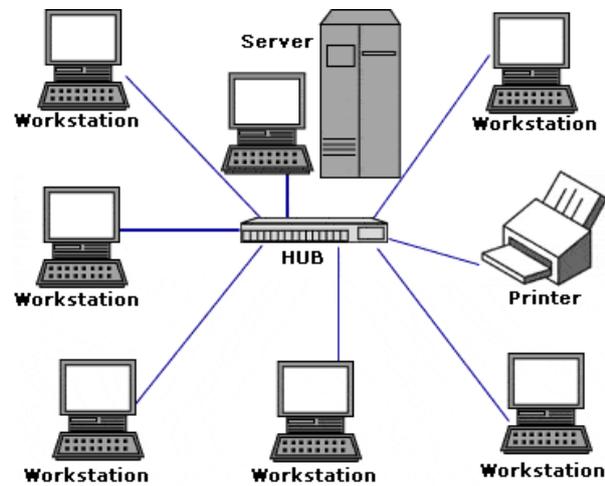
2.1 Teori Dasar

Dalam teori dasar menjelaskan hal-hal umum jaringan yang mendasari materi penelitian. Berikut adalah konsep dan penjelasan tentang jaringan komputer, standar jaringan komputer, jenis jaringan komputer, model *OSI layer*, *Firewall* dan *Mikrotik*.

2.1.1 Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan dari komputer, printer, dan peralatan lainnya yang terhubung dalam satu kesatuan dan membentuk suatu sistem tertentu. Informasi bergerak melalui kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar informasi (data), mencetak data pada printer yang sama dan dapat secara simultan menggunakan program aplikasi yang sama (Maslan & Wangdra, 2012, p. 2).

Jaringan komputer merupakan sistem yang terdiri atas dua atau lebih komputer serta perangkat-perangkat lainnya yang saling terhubung. Media pernghubung tersebut dapat berupa kabel atau nirkabel sehingga memungkinkan para pengguna jaringan komputer melakukan pertukaran informasi, seperti berbagi file, dokumen, data serta menggunakan perangkat keras dan perangkat lunak yang terhubung ke jaringan (Utomo, 2012, p. 1).



Gambar 2.1 Jaringan Komputer

2.1.2 Standar Jaringan Komputer

Standarisasi masalah jaringan diselenggarakan oleh badan dunia seperti ISO (*International Organization for Standardization*), ITU (*International Telecommunication Union*), ANSI (*American National Standard Institute*), NCITS (*National Committee for Information Technology Standardization*), bahkan juga oleh lembaga asosiasi profesi IEEE (*Institute of Electrical and Electronics Engineers*) dan ATM-Forum di Amerika. Pada prakteknya bahkan vendor-vendor produk LAN juga memakai standar yang dihasilkan IEEE. IEEE banyak membuat standarisasi peralatan telekomunikasi seperti yang tertera pada tabel berikut (Maslan & Wangdra, 2012, pp. 53–54):

Tabel 2.1 Badan Pekerja di IEEE

<i>Working Group</i>	Bentuk Kegiatan
IEEE802.1	Standarisasi <i>interface</i> lapisan atas HILI (<i>High Level Interface</i>) dan <i>Data Link</i> termasuk MAC (<i>Medium Access Control</i>) dan LLC (<i>Logical Link Control</i>).
IEEE802.2	Standarisasi lapisan LLC.
IEEE802.3	Standarisasi lapisan MAC untuk CSMA/CD (10Base5, 10Base2, 10BaseT, dll.)
IEEE802.4	Standarisasi lapisan MAC untuk Token Bus.
IEEE802.5	Standarisasi lapisan MAC untuk Token Ring.
IEEE802.6	Standarisasi lapisan MAC untuk MAN-DQDB (<i>Metropolitan Area Network-Distributed Queue Dual Bus.</i>)
IEEE802.7	Grup pendukung BTAG (<i>Broadband Technical Advisory Group</i>) pada LAN.
IEEE802.8	Grup pendukung FOTAG (<i>Fiber Optic Technical Advisory Group.</i>)
IEEE802.9	Standarisasi ISDN (<i>Integrated Services Digital Network</i>) dan IS (<i>Integrated Services</i>) LAN.
IEEE802.10	Standarisasi masalah pengamanan jaringan (<i>LAN security.</i>)
IEEE802.11	Standarisasi masalah <i>wireless</i> LAN dan CSMA/CD bersama IEEE802.3
IEEE802.12	Standarisasi masalah 100VG-AnyLAN
IEEE802.14	Standarisasi masalah <i>protocol</i> CATV

Sumber: (Maslan & Wangdra, 2012)

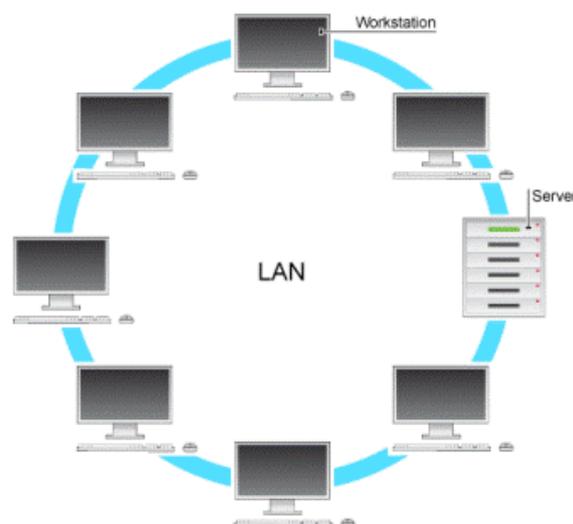
2.1.3 Jenis Jaringan Komputer

Dalam jaringan komputer, jenis-jenis jaringan komputer dapat dibedakan berdasarkan ruang lingkup, berdasarkan topologi, berdasarkan fungsi, dan berdasarkan media penghantar (Utomo, 2012):

2.1.3.1 Berdasarkan Ruang Lingkup

a. LAN (*Local Area Network*)

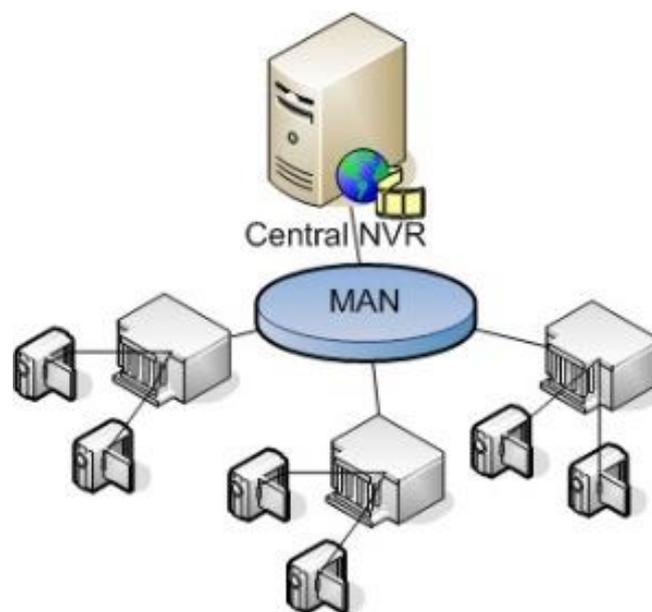
LAN adalah suatu kumpulan komputer, dimana terdapat beberapa unit komputer (*client*) dan satu unit untuk bank data (*server*). Antara masing-masing *client* maupun antara *client* dan *server* dapat saling bertukar *file* maupun saling menggunakan *printer* yang terhubung pada unit-unit komputer yang terhubung pada jaringan LAN (Sugeng, 2010, p. 19).



Gambar 2.2 LAN (*Local Area Network*)

b. MAN (*Metropolitan Area Network*)

MAN jaringan ini dibangun untuk kebutuhan ruang lingkup yang besar, bisa mencakup suatu kota. Misalnya sekolah/perusahaan tertentu mempunyai sebuah LAN pada area sekolah/perusahaannya, kemudian beberapa sekolah/perusahaan dalam kota tersebut dapat saling terhubung dan membentuk sebuah MAN (Utomo, 2012, p. 3).

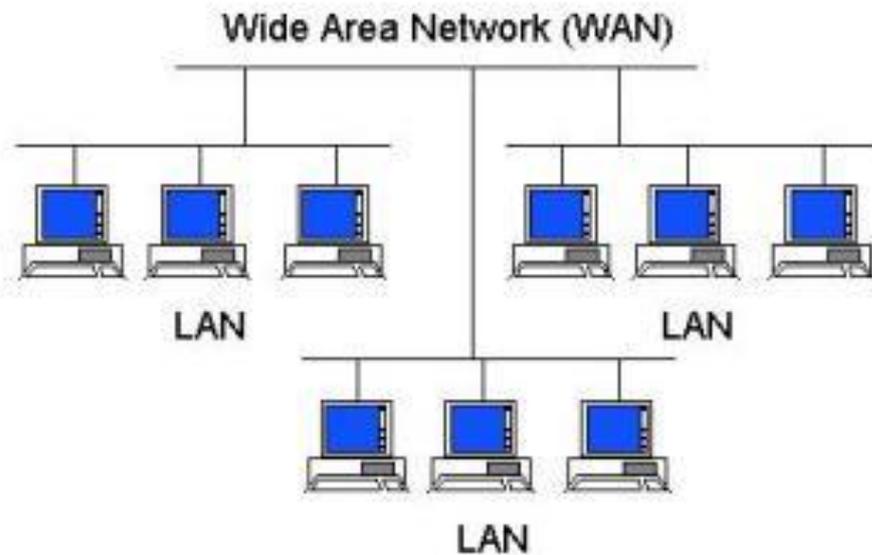


Gambar 2.3 MAN (*Metropolitan Area Network*)

c. WAN (*Wide Area Network*)

WAN merupakan jaringan komputer dengan cakupan area yang lebih luas dan biasanya akan menghubungkan beberapa kesatuan jaringan komputer yang lebih banyak. Koneksi antarjaringan dengan cakupan luas tersebut akan memudahkan kita berbagi sumber yang ada sehingga proses

berbagi antarkomputer/jaringan dapat dilakukan secara lintas daerah, kota, negara, bahkan benua (Utomo, 2012, p. 3)



Gambar 2.4 WAN (*Wide Area Network*)

2.1.3.2 Berdasarkan Topologi

a. Topologi Bus

Jenis topologi ini menghubungkan setiap komputer/node dengan sebuah kabel komunikasi melalui sebuah kardi antarmuka (*card interface*) komputer, setiap komputer dapat berhubungan dengan komputer yang lain yang ada dalam jaringan tersebut (Utomo, 2012, p. 4).

b. Topologi Ring

Komputer-komputer dalam jenis topologi ini akan dihubungkan dengan sebuah kabel tunggal dan membentuk bagan seperti sebuah cincin.

Pada jaringan ini tidak terdapat komputer pusat, sehingga semua komputer mempunyai kedudukan yang sama (Utomo, 2012, p. 5).

c. Topologi *Star*

Jenis topologi ini beberapa komputer akan dihubungkan dengan satu pusat komputer sehingga semua *control* berbagi sumber daya (*resources*) dalam jaringan yang diperlukan juga akan dipusatkan pada satu titik, ketika akan mengirim data ke komputer lainnya, komputer harus melalui komputer pusat terlebih dahulu. Dalam topologi jenis ini, ketika komputer pusat mengalami gangguan semua komputer *client* juga akan terganggu (Utomo, 2012, p. 6).

d. Topologi *Extended Star*

Dasar topologi ini adalah topologi bintang hanya ditambah pengulang (*Repeater*) berupa hub atau pengalih (*switch*) sehingga semakin memperluas jaringan yang jaraknya berjauhan (Utomo, 2012, p. 7).

e. Topologi *Cascading Star*

Jenis topologi ini juga hampir sama dengan bintang diperluas, akan tetapi beberapa jaringan bintang yang dibuat tersebut dihubungkan ke sebuah simpul pusat untuk mengontrol semuanya (Utomo, 2012, p. 8).

f. Topologi *Mesh*

Jaringan jenis topologi ini mempunyai jalur ganda pada setiap node/simpul jaringan. Semakin banyak jumlah komputer yang ada dalam jaringan, semakin sulit pemasangan kabel akan menjadi berlipat ganda (Utomo, 2012, p. 8).

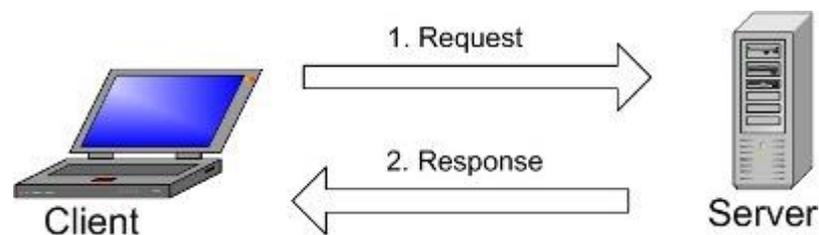
g. Topologi *Tree*

Topologi jenis ini merupakan kombinasi antara topologi bintang dan topologi bus. Topologi ini terdiri atas kumpulan topologi bintang yang dihubungkan dalam topologi bus sebagai jalur *backbone* (Utomo, 2012, p. 9).

2.1.3.3 Berdasarkan Fungsi

a. Jaringan *Client-Server*

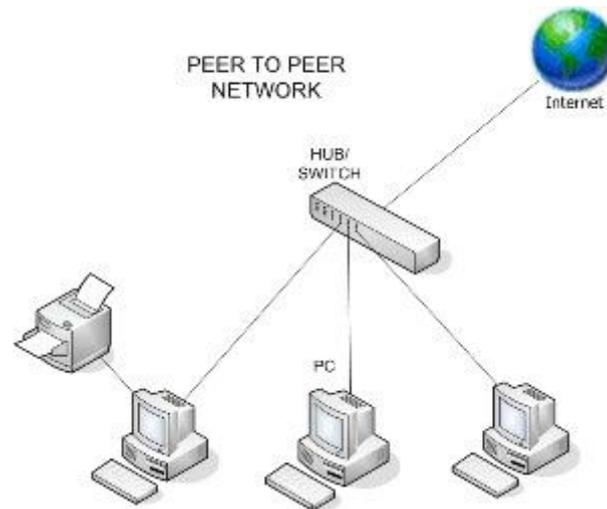
Pada jaringan ini terdapat satu komputer yang disiapkan sebagai komputer *server* yang akan melayani komputer lainnya yang berfungsi sebagai *client* (Utomo, 2012, p. 10).



Gambar 2.5 Jaringan *Client-Server*

b. Jaringan *Peer-to-peer*

Pada jaringan ini sebuah komputer langsung dihubungkan ke komputer lainnya dan dapat saling berbagi sumber daya pada masing-masing komputer. Pada jenis jaringan ini biasanya hanya akan diterapkan untuk jumlah komputer yang tidak terlalu banyak (Utomo, 2012, p. 11).



Gambar 2.6 Jaringan *Peer-to-Peer*

2.1.3.4 Berdasarkan Media Penghantar Jaringan

a. Menggunakan Kabel (*Wired Networking*)

Jaringan ini menggunakan kabel sebagai media penghantarnya. Data akan mengalir melalui kabel. Kabel yang digunakan biasanya berbahan tembaga atau serat optik (*fiber optic*). Bahan tembaga biasanya digunakan untuk jaringan LAN, sedangkan jenis MAN atau WAN biasanya menggunakan gabungan antara kabel tembaga dan kabel optik (Utomo, 2012, p. 12).

b. Menggunakan Media Udara (*Wireless*)

Jaringan komputer ini tidak menggunakan kabel. Media penghantar antarkomputernya menggunakan gelombang radio. Frekuensi yang digunakan untuk jaringan komputernya tinggi, yaitu 2,4 GHz dan 5 GHz (Utomo, 2012, p. 12).

2.1.4 Model OSI Layer

OSI adalah suatu standar komunikasi antarmesin yang terdiri atas 7 lapisan. Ketujuh lapisan tersebut mempunyai peran dan fungsi yang berbeda satu terhadap yang lain. Setiap *layer* bertanggung jawab secara khusus pada proses komunikasi data. Misal, suatu *layer* bertanggung jawab untuk membentuk koneksi antarperangkat, sementara *layer* lainnya bertanggung jawab untuk mengoreksi terjadinya error selama proses pengiriman paket data berlangsung. Model OSI dibagi menjadi 2 tingkatan group yaitu: *upper layer* dan *lower layer*. Untuk *upper layer* fokus pada aplikasi pengguna dan file direpresentasikan di komputer. Sedangkan *lower layer* berfokus pada *network engineering* yang membuat *hardware* (Maslan & Wangdra, 2012, pp. 37–38)

2.1.4.1 Lapisan Fisik (*Physical Layer*)

Physical Layer atau lapisan fisik melakukan fungsi pengiriman dan penerimaan bit stream dalam medium fisik. Dalam lapisan ini kita akan mengetahui spesifikasi mekanikal dan elektrikal dari media transmisi serta antarmukanya.

Hal-hal penting yang dapat dibahas lebih jauh dalam lapisan fisik ini adalah:

1. Karakteristik fisik dari media dan antarmuka.
2. Representasi *bit-bit*.

Dalam hal ini lapisan fisik harus mampu menerjemahkan *bit* 0 atau 1, termasuk pengkodean dan bagaimana mengganti sinyal 0 ke 1 atau sebaliknya.

3. *Data rate* (laju data).
4. Sinkronisasi *bit*.
5. *Line configuration* (Konfigurasi saluran). Misalnya: *point-to-point* atau *point-to-multipoint configuration*.
6. Topologi fisik. Misalnya: *mesh topology*, *star topology*, *ring topology*, atau *bus topology*.
7. Mode transmisi. Misalnya: *half-duplex mode*, *full-duplex (simplex) mode*.

Lapisan Fisik pada LAN di antaranya:

1. *Ethernet/IEEE 802.3, Baseband LAN* beroperasi 10 Mbps melalui kabel koaksial.
2. 100-Mbps *Ethernet* (Fast Ethernet) *High-speed LAN*.
3. 1000-Mbps *Ethernet* (Gigabit Ethernet), *High-speed LAN*.
4. *Fiber Distributed Digital Interface* (FDDI), 100-Mbps *token-passing, dual-ring LAN* menggunakan kabel *fiber optic*.
5. *Token Ring/IEEE 802.5, Token passing LAN* yang beroperasi pada kecepatan 4 atau 16 Mbps dengan topologi *star*.

Lapisan Fisik pada WAN di antaranya:

1. *Serial Interface (async & sync)*
2. *High-speed serial Interface* (HSSI)

3. X.21 (Jaringan X.25)

(Sukmaaji & Rianto, 2008, pp. 16–17)

2.1.4.2 Lapisan Jalur Data (*Data Link Layer*)

Pada *Layer-2 (Data Link Layer)* komunikasi data dilakukan dengan menggunakan identitas berupa alamat simpul fisik yang disebut sebagai alamat *hardware* atau *hardware address*. Proses komunikasi antara komputer atau simpul jaringan hanya mungkin terjadi, bila kedua belah pihak mengetahui identitas masing-masing melalui alamat fisik (*physical address*). Bentuk topologi yang digunakan ditentukan oleh protokol *Data Link*. Sebagai contoh adalah BUS untuk teknologi *Ethernet*. *RING* untuk teknologi *Token Ring* ataupun teknologi FDDI. Selain ketiga bentuk topologi tersebut pada komunikasi serial terdapat topologi point-to-point atau point-to-multipoint pada jaringan yang menggunakan teknologi *Frame Relay* dan ATM.

Penanganan kesalahan komunikasi yang terjadi pada lapisan *Data Link* menggunakan pendeteksian *error* dan menginformasikan kepada lapisan di atasnya, bahwa terjadi kesalahan transmisi. Kendali kesalahan yang bisa dilakukan pada lapisan ini hanya mendeteksi dan tidak melakukan perbaikan kesalahan (*errorcorrection*). *Data link* akan mengubah *BYTES* (1 *byte* = 8 *bit*) yang diterima dari lapisan fisik menjadi satuan data yang disebut dengan *FRAME*. *FRAME* terdiri dari *FRAME-HEADER* (identitas yang menjelaskan *frame*) dan *DATA*. Selain *FRAME-HEADER*, informasi lain yang ditambahkan adalah FCS (*Frame Check Sequence*). penjabarannya adalah sebagai berikut:

<i>Frame-Header</i>	DATA	<i>Frame Sequence</i>	<i>Check</i>
---------------------	------	---------------------------	--------------

Frame-Header berisi informasi yang dibutuhkan oleh protokol *Data Link*.

Secara umum, informasi yang terdapat dalam frame header:

1. *Hardware address (MAC ADDRESS)* Pengirim
2. *Hardware address (MAC ADDRESS)* Penerima
3. *Flag*
4. *Control Bits*

Teknologi *Ethernet*, *Token Ring*, dan FDDI menggunakan 48 bit *Media Acces Control (MAC)* sebagai *hardware address*. Dari 48 bit ini, 24 bit awal ditentukan oleh standar internasional (IEEE) dan 24 bit sisanya adalah perusahaan pembuat kartu jaringan (*Network Interface Card*). Sebagian penomoran yang diberikan IEEE di antaranya adalah:

<i>Vendor NIC</i>	Nomor MAC (24 bit awal)
<i>Cisco Systems</i>	00 00 0C
<i>3Com Corporation</i>	00 02 AF
<i>Hewlett-Packard Company</i>	08 00 09
<i>Apple Computer</i>	08 00 07

Pada teknologi WAN, *Frame Relay* menggunakan DLCI (*Data Link Control Identifier*). ATM menggunakan VPI/VCI (*Virtual Path Identifier/Virtual Channel Identifier*), dan X25 menggunakan X.21 sebagai *hardware address*.

Tugas utama lapisan *data link* dalam proses komunikasi data adalah:

1. *Framing* : membagi bit stream yang diterima dari lapisan *network* menjadi unit-unit data yang disebut *frame*.
2. *Physical addressing* : definisi identitas pengirim dan/atau penerima yang ditambahkan dalam *header*.
3. *Flow control* : melakukan tindakan untuk membuat stabil laju *bit* jika *rate* atau laju *bit Stream* berlebih atau berkurang.
4. *Error control* : penambahan mekanisme deteksi dan retransmisi *frame-frame* yang gagal terkirim.
5. *Communication control* : menentukan *device* yang harus dikendalikan pada saat tertentu jika ada dua koneksi yang sama.

(Sukmaaji & Rianto, 2008, pp. 17–19)

2.1.4.3 Lapisan Jaringan (*Network Layer*)

Pada lapisan ini terjadi proses pendefinisian alamat logis (*logical addressing*), kemudian mengombinasikan multiple data *link* menjadi satu *internetwork*. Lapisan *Network* bertanggung jawab untuk membawa paket dari satu simpul ke simpul lainnya dengan mengacu pada *logical address*. Fungsi lain adalah sebagai *packet forwarder* (penerus). Lapisan *Network* sebagai *packet forwarder* mengantarkan paket dari sumber (*Source*) ke tujuan (*destination*) yang disebut dengan istilah *routing*.

Ada dua tugas pokok lapisan *network* yaitu:

1. *Logical addressing*

pengalamatan secara logis yang ditambahkan pada *header* lapisan *network*. Pada jaringan TCP/IP pengalamatan logis ini populer dengan sebutan *IP address*.

2. *Routing*

Hubungan antarjaringan yang membentuk *internetwork* membutuhkan metode jalur alamat agar paket dapat ditransfer dari satu *device* yang berasal dari jaringan satu menuju *device* lain pada jaringan yang lain. Fungsi *routing* didukung oleh *routing protocol* yaitu protokol yang bertujuan mencari jalan terbaik menuju tujuan dan tukar-menukar informasi tentang topologi jaringan dengan *router* yang lainnya. Protokol *routing* ini misalnya *Border Gateway Protocol (BGP)*, *Open Shortest Path First (OSPF)*, *Routing Information Protocol (RIP)*. (Sukmaaji & Rianto, 2008, p. 19).

2.1.4.4 Lapisan *Transport (Transport Layer)*

Lapisan *transport* bertanggung jawab terhadap pengiriman *source-to-destination (end-to-end)* yang dapat dijelaskan sebagai berikut:

1. *Service-point addressing*

Suatu komputer sering menjalankan berbagai macam program aplikasi ataupun *services* berlainan pada waktu bersamaan. Karena itu, lapisan

transport ini tidak hanya menangani pengiriman *source-to-destination* dari komputer satu ke komputer yang lain, namun lebih spesifik kepada *delivery* jenis *message* untuk aplikasi yang berlainan. Dengan demikian, setiap *message* yang berlainan aplikasi harus memiliki alamat tersendiri yang disebut *service point address* atau yang lebih umum disebut *port address* (*port* 80 : *www*, *port* 25 : *SMTP*).

2. *Segmentation* dan *reassembly*

Sebuah *message* dibagi dalam segmen-segmen yang terkirim. Setiap segmen memiliki *sequence number*. *Sequence number* berguna bagi lapisan *transport* untuk merakit (*reassembly*) segmen-segmen yang terpecah menjadi *message* yang utuh.

3. *Connection control*

Pada lapisan *transport* terdapat dua kondisi yakni *connectionless* atau *connection-oriented*. Fungsi dari *connection control* adalah mengendalikan kondisi tersebut.

4. *Flow control*

Seperti halnya lapisan data *link*, lapisan *transport* bertanggung jawab untuk melakukan kontrol aliran (*flow control*). Bedanya dengan *flow control* di lapisan data *link* adalah dilakukan untuk *end-to-end*.

5. *Error control*

Fungsi tugas ini sama dengan tugas *error control* di lapisan data *link*, namun berorientasi *end-to-end*.

Dalam jaringan berbasis TCP/IP protokol yang terdapat pada lapisan ini adalah *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) (Sukmaaji & Rianto, 2008, p. 20).

2.1.4.5 Lapisan Sesi (*Session Layer*)

Lapisan sesi membuka, merawat, mengendalikan, dan melakukan terminasi hubungan antarsimpul. Lapisan Aplikasi dan Presentasi melakukan request dan menunggu response yang dikoordinasikan oleh lapisan di atasnya misalnya:

1. RPC (*Remote Procedure Call*) Protokol yang mengeksekusi program pada komputer remote dan memberikan nilai balik kepada komputer lokal sebagai hasil eksekusi tersebut.
2. Netbios API : *Session layer application programming interface*
3. NFS (*Network File System*)
4. SQL (*Structured Query Language*)

(Sukmaaji & Rianto, 2008, p. 21)

2.1.4.6 Lapisan Presentasi (*Presentation Layer*)

Berfungsi untuk mentranslasikan data yang akan ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam *level* ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga *Network*

shell (*Virtual Network Computing* (WVC) atau *Remote Desktop Protocol* (RDP)). Lapisan presentasi melakukan *coding* dan konversi data misalnya format data untuk *image* dan *sound* (JPG, MPEG, TIFF, WAV, dan lain-lain), konversi EBCDIC-ASCII. presentasi *Big Endian* dan *Little Endian*, Kompresi, dan Enkripsi. (Sukmaaji & Rianto, 2008, p. 21)

2.1.4.7 Lapisan Aplikasi (*Application Layer*)

Aplikasi adalah layanan/*service* yang mengimplementasikan komunikasi antarsimpul. *Application Layer* berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan mengatur bagaimana aplikasi dapat mengakses jaringan dan membuat pesan-pesan kesalahan. Beberapa hal yang dilakukan oleh lapisan aplikasi: mengidentifikasi mitra komunikasi, aplikasi *transfer* data, *Resource Availability*, dan lapisan aplikasi terkait dengan aplikasi *end-user*.

Protokol-protokol pada lapisan aplikasi di antaranya:

1. *File Transfer Protocol* (FTP) protokol standar untuk transfer file komputer antar mesin dalam sebuah *internetwork*.
2. *Simple Mail Transfer Protocol* (SMTP) merupakan salah satu protokol yang umum digunakan untuk pengiriman surat elektronik di internet. Protokol ini digunakan untuk mengirimkan data dari komputer pengirim ke *server* surat elektronik penerima yang didukung oleh POP3 dan IMAP.
3. *Hypertext Transfer Protocol* (HTTP) protokol yang dipergunakan untuk transfer dokumen dalam *World Wide Web* (WWW). Protokol ini adalah

protokol ringan, tidak berstatus dan generik yang dapat digunakan berbagai macam tipe dokumen. (Sukmaaji & Rianto, 2008, pp. 21–22)

2.2 Teori Khusus

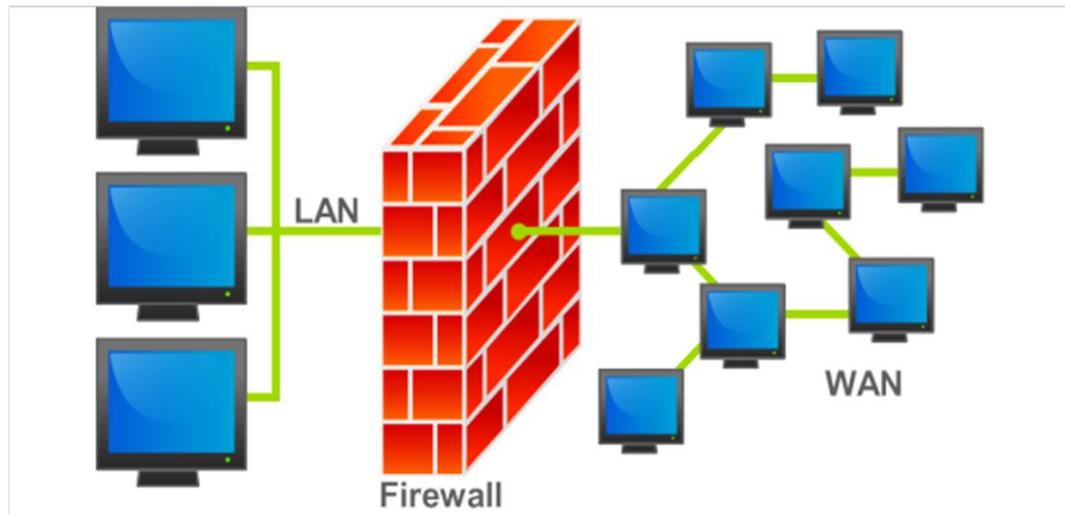
Dalam teori khusus, memuat dan menjelaskan variabel yang digunakan dalam penelitian yang mendukung materi penelitian. Berikut adalah konsep atau variabel yang menjadi latar belakang penelitian, sehingga setiap indikator dapat dijelaskan.

2.2.1 Firewall

Firewall merupakan perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan menentukan apakah sebuah paket data bisa masuk dan keluar dari suatu jaringan maka *firewall* berperan untuk melindungi jaringan dari serangan yang berasal dari jaringan luar (*outside network*) (Towidjojo, 2016, p. 43).

Firewall adalah sebuah system atau perangkat yang bertugas untuk mengatur lalu lintas jaringan computer yang dianggap aman untuk melewatinya dan mencegah lalu lintas yang dianggap tidak aman untuk melewatinya. Umumnya *firewall* diletakkan didalam sebuah gateway atau *router* yang menjembatani sebuah jaringan dengan jaringan lainnya. *Firewall* digunakan untuk

mengontrol hak akses terhadap siapa saja yang memiliki akses terhadap jaringan internal dari pihak luar.



Gambar 2.7 Letak firewall di jaringan komputer

Secara umum *firewall* dibagi menjadi 2 jenis, yaitu:

- *Personal Firewall*
- *Dan Network Firewall*

Personal firewall adalah sebuah program yang digunakan untuk melindungi personal komputer di jaringan dari akses yang tidak diinginkan. *Firewall* jenis ini biasanya sudah terbungel ke dalam program antivirus komersial, hampir semua antivirus yang berbayar sudah mengikut sertakan fungsi *firewall* ke dalamnya.

Sedangkan *network firewall* adalah sebuah program atau alat yang digunakan untuk melindungi sebuah jaringan computer lokal dari akses yang tidak diinginkan. *Network firewall* ini bentuknya dapat berupa perangkat lunak (*software*) atau pun perangkat keras (*hardware*) (Athailah, 2013, pp. 6–7).

Firewall atau tembok-api adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya. Tembok-api umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar.

Parameter proteksi

- a. IP Address
- b. Domain Name
- c. Protokol
- d. Port

(Hikmaturokhman, Purwanto, & Munadi, 2010)

2.2.1.1 Tugas Firewall

Dalam meningkatkan cara kerja *firewall*, maka tugas *firewall* adalah:

- Melakukan *Filtering*

Mengharuskan semua *traffic* yang ada untuk dilewatkan melalui *firewall* bagi semua proses pemberian dan pemanfaatan layanan informasi, jadi semua aliran paket data dari dan menuju *firewall*, diseleksi berdasarkan nomor IP *address*, alamat *Port* dan arahnya.

- Mengimplementasikan kebijakan *security*

Dalam suatu jaringan, *firewall* harus dapat mengetahui siapa saja yang boleh masuk atau mengakses suatu sistem. Apabila akses tersebut tidak diperbolehkan (ilegal), maka *firewall* harus berubapaya menggagalkan akses tersebut sesuai dengan kebijakan *security* yang telah diberikan.

- Sebagai alat perekam

Firewall harus mampu mencatat atau merekam semua informasi yang mencurigakanyang masuk atau yang keluar melalui *firewall* dengan mengamati paket IP dan Nomor *Port* yang mencurigakan (Maslan & Wangdra, 2012, p. 151).

2.2.1.2 Karakteristik *firewall*

1. Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati *firewall*. Hal ini dapat dilakukan dengan cara membatasi secara fisik semua akses terhadap jaringan lokal, kecuali melewati *firewall*.
2. Hanya kegiatan yang terdaftar/dikenal yang dapat melewati atau melakukan hubungan. Hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal.
3. *Firewall* harus kebal atau relatif kuat terhadap serangan.
(Sukmaaji & Rianto, 2008, pp. 188–189)

2.2.1.2 Keuntungan Menggunakan *Firewall*

1. *Firewall* dapat kita gunakan untuk membatasi penggunaan sumber daya informasi.
2. Seluruh akses dalam jaringan dapat kita kontrol melalui *firewall*.
3. *Firewall* dapat kita gunakan untuk mengawasi semua service yang berjalan.
4. *Firewall* dapat mencatat dan merekam semua kegiatan yang berjalan melewatinya.
5. *Firewall* dapat menerapkan suatu kebijakan sekuriti (*Security policy*).
6. *Firewall* dapat mencegah suatu paket yang di rasa mencurigakan oleh sistem.
7. *Firewall* dapat sedikit menghambat pergerakan para penyerang yang mencoba memasuki sistem (Maslan & Wangdra, 2012, p. 152).

2.2.1.3 Teknik Pengamanan *Firewall*

- *Service control* : Berdasarkan tipe-tipe *service* yang digunakan dan boleh diakses baik untuk ke dalam ataupun keluar *firewall*.
- *Direction Control* : Berdasarkan arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diizinkan melewati *firewall*.
- *User control* : Berdasarkan pengguna/user untuk dapat menjalankan suatu layanan, artinya ada user yang dapat dan ada yang tidak dapat

menjalankan suatu servis. Hal ini dikarenakan *user* tersebut tidak diizinkan untuk melewati *firewall*.

- *Behavior Control* : Berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya *firewall* dapat memfilter *e-mail* untuk menanggulangi/mencegah *spam*. (Sukmaaji & Rianto, 2008, p. 189)

2.2.1.4 Tipe-Tipe Firewall

1. Paket *Filtering Router/Bridge*

Mengatur semua paket IP baik yang menuju, melewati atau akan dituju oleh paket tersebut. Penyaringan paket ini dikonfigurasi untuk menyaring paket yang akan ditransfer dua arah. Aturan penyaringan didasarkan pada header IP dan *transport header*, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol *transport* yang digunakan (UDP, TCP), serta nomor *port* yang digunakan. Kelebihan dari tipe ini adalah mudah untuk diimplementasikan, transparan untuk pemakai, relatif lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal autentikasi.

Serangan yang dapat terjadi pada *firewall* dengan tipe paket filter adalah:

- a) *IP address spoofing* : *Intruder* (penyusup) dari luar dapat melakukan dengan cara menyertakan/menggunakan *ip address* jaringan lokal yang telah diizinkan untuk melalui *firewall*.
- b) *Source routing attacks* : Tipe ini tidak menganalisis informasi *routing* sumber -IP, sehingga memungkinkan untuk *bypass firewall*.
- c) *Tiny Fragment attacks* : *Intruder* membagi IP ke dalam bagian-bagian (*fragment*) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini didesain untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP *header*. Penyerang berharap hanya bagian (*fragment*) pertama yang akan diperiksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat ditanggulangi dengan cara menolak semua paket dengan protokol TCP dan memiliki Offset = 1 pada IP *fragment* (bagian IP).

Beberapa perangkat lunak berbasis *Linux/UNIX* yang dapat digunakan untuk melakukan IP *filtering* antara lain:

- a) *ipfwadm* : merupakan standar dari sistem *Linux* yang dapat diaktifkan pada *level kernel*
- b) *ipchains* : versi baru dari *Linux kernel* paket *filtering* yang diharapkan dapat menggantikan fungsi *ipfwadm*
- c) *iptables* : versi *linux* 2.4 ke atas menggunakan aplikasi *iptables* ini.
- d) *pf (packer filter)* : aplikasi ini berada pada sistem operasi OpenBSD

Selain pada sistem *Linux/Unix*, pada perangkat jaringan juga menggunakan paket filter *firewall* misalnya adalah cisco IP *access-list*.

2. *Application-Level Gateway*

Application-level Gateway juga dikenal sebagai *proxy server* yang berfungsi untuk memperkuat/menyalurkan arus aplikasi. Tipe ini akan mengatur semua hubungan yang menggunakan *layer* aplikasi, baik itu FTP, HTTP, GOPHER, dan lain-lain. Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi misalnya FTP untuk mengakses secara remote, maka *gateway* akan meminta user memasukkan alamat remote host yang akan diakses.

Saat pengguna mengirimkan user ID serta informasi lainnya yang sesuai, *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada *remote host*, dan menyalurkan data di antara kedua titik. Apabila data tersebut tidak sesuai, maka *firewall* tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada tipe ini *firewall* dapat dikonfigurasi hanya mampu mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati *firewall*. Kelebihannya adalah relatif lebih aman daripada tipe paket *filtering router* dan lebih mudah untuk memeriksa (audit) dan mendata (*log*) semua aliran data yang masuk pada *level* aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan *gateway*. *Gateway* akan memeriksa dan meneruskan semua arus dari dua arah.

3. *Circuit-level Gateway*

Tipe ketiga ini merupakan sistem yang berdiri sendiri, atau juga dapat merupakan fungsi khusus yang terbentuk dari tipe *application-level gateway*. Tipe ini tidak mengizinkan koneksi TCP end to end (langsung).

Cara kerja : *Gateway* akan mengatur kedua hubungan tcp tersebut. Satu antara *gateway* dengan TCP pada pengguna lokal (*inner host*), serta satunya lagi antara *gateway* dengan TCP pengguna luar (*outside host*). Saat dua buah hubungan terlaksana, *gateway* akan menyalurkan TCP *segment* dari satu hubungan ke lainnya tanpa memeriksa isinya. Fungsi pengamanannya terletak pada penentuan hubungan mana yang diizinkan. Penggunaan tipe ini biasanya dikarenakan administrator percaya dengan pengguna *internal (internal users)*. (Sukmaaji & Rianto, 2008, pp. 189–192)

2.2.2 *Mikrotik*

Mikrotik merupakan sebuah merek dari sebuah perangkat jaringan, pada awalnya *Mikrotik* hanyalah sebuah perangkat lunak atau *software* yang di-*install* dalam komputer yang digunakan untuk mengontrol jaringan, tetapi dalam perkembangannya saat ini telah menjadi sebuah *device* atau perangkat jaringan yang andal dan harga yang terjangkau, serta banyak digunakan pada *level* perusahaan penyedia jasa *internet (ISP)* (Athailah, 2013, p. 17).



Gambar 2.8 *Mikrotik RouterBoard*

Mikrotik adalah sistem operasi independen berbasis *Linux* khusus untuk komputer yang difungsikan sebagai *router*. *Mikrotik* didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks (Riadi, 2011).

2.2.2.1 Sejarah *Mikrotik*

Mikrotik pada awalnya dimulai saat dua orang ahli jaringan, yaitu John Trully dan Arnis Riekstins berhasil membuat *routing* jaringan ke jaringan yang lebih luas, sehingga hal ini menjadi visi *Mikrotik* sampai saat ini, yaitu "*Routing the World*".

John Trully berkebangsaan Amerika, tetapi bermigrasi ke Latvia, sebuah negara yang menjadi tetangga Rusia. Bersama dengan Arnis Riekstins asli Latvia, mereka bekerja sama untuk membuat sebuah perangkat yang benar-benar dapat diandalkan untuk pekerjaan *routing* jaringan.

Dimulai dengan membuat *Mikrotik* yang berbasiskan *kernel Linux*, mereka berdua membangun sebuah ISP berkecepatan 2Mbps dan bernama Aeronet, di Moldova, sebuah negara tetangga Latvia. Baru setelah itu mereka melayani 5 pelanggan pertamanya di Latvia.

Dari sinilah sistem operasi *Mikrotik* dikembangkan, di mana pada awal visi mereka ingin membuat sebuah *router* yang andal, dan dapat diinstall dengan mudah pada komputer biasa dan memiliki fitur dan fasilitas yang cukup lengkap.

Selain membuat sistem operasinya, *mikrotik* juga membuat perangkat *router* yang diberi nama *RouterBoard*. Jika dibandingkan dengan perangkat sejenis yang dibuat oleh *vendor* lain dengan fungsi dan fitur yang sama, harga perangkat yang dibuat *mikrotik* ini jauh sekali lebih ekonomis (Athailah, 2013, pp. 18–20).

2.2.2.2 Fitur-Fitur *Mikrotik*

Fitur-fitur yang tersedia pada *Mikrotik* di antaranya adalah sebagai berikut:

- *Firewall* dan NAT
- *Routing - Static Routing*
- *Hotspot*
- *Point-to-point tunneling protocols (PPTP)*
- *Simple tunnels*
- IPSec
- *Web proxy*
- *Chaching DNS client*

- DHCP
- *Universal Client*
- VRRP
- UpnP
- NTP
- *Monitoring/Accounting*
- SNP
- M3P
- MNDP
- Dan *Tools* jaringan lainnya

(Athailah, 2013, p. 19)

2.2.2.3 Lisensi Mikrotik

Lisensi pada *Mikrotik* adalah menggunakan *level*, dengan *level* ini Anda dapat membeli lisensi pada *level* yang sesuai dengan yang anda butuhkan. Dan *level* ini dengan mudah dapat Anda naikkan tingkatnya pada saat Anda membutuhkan fitur yang lebih tinggi lagi dengan *level* yang Anda miliki saat ini.

Tingkatan *level* pada lisensi *mikrotik* adalah sebagai berikut:

- *Level 0* (gratis)

Pada *level* ini Anda tidak memerlukan lisensi untuk menggunakannya dan penggunaan fitur ini hanya dibatasi selama 24 Jam setelah instalasi dilakukan.

- *Level 1* (*Demo*)

Pada *level* ini Anda dapat menggunakan *mikrotik* secara penuh, semua fungsi yang disediakan oleh *mikrotik* dapat Anda gunakan. Namun, waktu penggunaan *mikrotik* dalam *level* ini dibatasi sampai 24 (dua puluh empat) jam saja, setelah ini fitur-fitur yang aktif sebelumnya akan dikunci secara otomatis.

- *Level 3*

Lisensi *level* ini sudah mencakup lisensi *level 1* (satu), dan dilengkapi dengan kemampuan untuk mengatur semua perangkat keras yang berbasis alamat protokol internet (*IP address*), baik itu *ethernet Card*, maupun *hotspot* nirkabel yang bertipe *client*.

- *Level 4*

Lisensi *level 4* ini isinya adalah cakupan lisensi *level 1* dan 3, serta ditambah fitur untuk mengelola jaringan nirkabel tipe akses poin.

- *Level 5*

Lisensi *level 5* isinya adalah cakupan lisensi *level 1*, 3, dan 4, serta ditambah fitur untuk mengelola hotspot nirkabel lebih banyak.

- *Level 6*

Ini adalah *level* lisensi yang tertinggi di *mikrotik*, pada lisensi *level 6* ini Anda akan diberikan fitur-fitur yang ada pada semua *level* lisensi *mikrotik* sebelumnya, serta ditambah tanpa ada limitasi apa pun.

(Athailah, 2013, pp. 20–21)

2.3 *Tools*

Pada penelitian ini peneliti menggunakan beberapa perangkat atau instrumen yang dijadikan sebagai alat guna merancang jaringan yang akan dirancang nantinya, peneliti menggunakan alat yang digunakan adalah sebagai berikut:

- a. *Internet Service Provider (ISP)*
- b. *Mikrotik RB 750*
- c. *Winbox*
- d. *Switch*
- e. *Laptop/komputer*
- f. *Kabel UTP*

2.4 **Penelitian Terdahulu**

Berdasarkan konsep teoritis yang telah diuraikan, maka penelitian ini mengacu pada penelitian terdahulu untuk memperkuat hasil penelitian yang akan dilakukan. Penelitian terdahulu dapat dijabarkan sebagai berikut:

1. Nama : Hikmaturokhman, Adnan dan Rendy
Judul : ANALISIS PERANCANGAN DAN IMPLEMENTASI
*FIREWALL DAN TRAFFIC FILTERING MENGGUNAKAN CISCO
ROUTER*
ISSN/ISBN : 1979-2328
Vol/No/Tahun : 2010

Berdasarkan hasil penelitian yang dilakukan, Rangkaian sistem yang dibangun dari simulasi menggunakan *packet tracer 5.0* dan kemudian diterapkan pada *cisco router 1721* berfungsi untuk mengizinkan paket data tertentu maupun menolak paket data tertentu juga. Sistem penolakan maupun pengijinan suatu paket data menggunakan salah satu fitur dari OSI *router* yaitu *Access-List*. Dalam hal ini *access-list* berperan sebagai *traffic filtering* yang apabila diimplementasikan lebih lanjut akan menjadi sebuah *firewall*. *Access-list* yang digunakan bertipe *Extended access list* dimana *extended access-list* akan membantu menentukan alamat sumber dan tujuan serta *protocol* dan nomer *port* yang mengidentifikasi aplikasi. Dengan menggunakan tipe ini akan lebih efisien memperbolehkan user mengakses dan menghentikan pengaksesan *host* tertentu (Hikmaturokhman et al., 2010).

2. Nama : Imam Riadi

Judul : OPTIMALISASI KEAMANAN JARINGAN
MENGUNAKAN PEMFILTERAN APLIKASI BERBASIS *MIKROTIK*

ISSN/ISBN : 2087-8737

Vol/No/Tahun : Vol.1/No.1/2011

Berdasarkan hasil penelitian yang dilakukan, Aplikasi *router* menggunakan *mikrotik* yang dihasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna, sehingga aplikasi tersebut tidak dapat diakses oleh pengguna

sesuai dengan ketentuan yang telah rancang dan sepakati sebelumnya (Riadi, 2011).

3. Nama : Shaymaa W Abdulatteef
Judul : *AN IMPLEMENTATION OF FIREWALL SYSTEM USING MIKROTIK ROUTER OS*
ISSN/ISBN : 1991-8941
Vol/No/Tahun : Vol.6/No.2/2012

Berdasarkan hasil penelitian yang dilakukan, menyimpulkan bahwa desain ini memberikan biaya yang relatif rendah, solusi keandalan yang tinggi, karena tercepat dan termurah salah satu teknik *firewall* adalah *packet filtering* dan karena *Mikrotik Router OS* memberikan hasil yang sama dari lingkungan nyata (Abdulatteef, 2012).

4. Nama : Uprit, Bhavan dan Arjun
Judul : *NETWORK SECURITY USING LINUX / UNIX FIREWALL*
ISSN/ISBN : 2277-7733
Vol/No/Tahun : Vol.2/No.4/2014

Berdasarkan hasil penelitian yang dilakukan, Saran dan metode yang diusulkan dapat menyebabkan jaringan dan *server* yang aman membawa beban tinggi dan status kebuntuan. Keamanan *default* yang diberikan oleh *LINUX / UNIX* ditambahkan ke keamanan *firewall Untangle*. Sedangkan *linux / unix* bertindak sebagai *platform* yang aman untuk menerapkan kebijakan keamanan yang didefinisikan oleh

administrator jaringan. Sesi penghentian sesi aplikasi yang tidak diinginkan dan tertunda menyebabkan *load balancing* yang mengarah ke kinerja tinggi dan pengaturan *server* klien yang aman (Uprit, Bhavan, & Arjun, 2014).

5. Nama : Fitriastuti dan Utomo
 Judul : IMPLEMENTASI BANDWIDTH MANAGEMENT DAN *FIREWALL* SYSTEM MENGGUNAKAN *MIKROTIK* OS 2.9.27
 ISSN/ISBN : 2088–3676
 Vol/No/Tahun : Vol. 4/No. 1/2014

Berdasarkan hasil penelitian yang dilakukan, Dengan menggunakan *mikrotik* OS 2.9.27 dapat dihasilkan *router* yang berfungsi sebagai perangkat limiter dan *firewall* system. Dengan menggunakan *firewall* filter *rules* dan dipadukan dengan *layer 7 protocols* dapat di buat sebuah *router* yang berfungsi sebagai pembatas akses ke beberapa situs yang diinginkan. Dengan menggunakan *limiter queue tree* dan *firewall mangle* dapat dibedakan kecepatan browsing maupun *download*. Implementasi trafik HIT yang digabungkan dengan *proxy server* dapat di jalankan pada *router* dengan *mikrotik Router OS* (Fitriastuti & Utomo, 2014).

6. Nama : Dwiyatno, Putra dan Krisnaningsih
 Judul : PENERAPAN OSPF *ROUTING* , *DE-MILITARIZED ZONE* , DAN *FIREWALL* PADA *MIKROTIK ROUTERBOARD* DINAS KOMUNIKASI DAN INFORMATIKA DEPOK
 ISSN/ISBN : 2406-7768

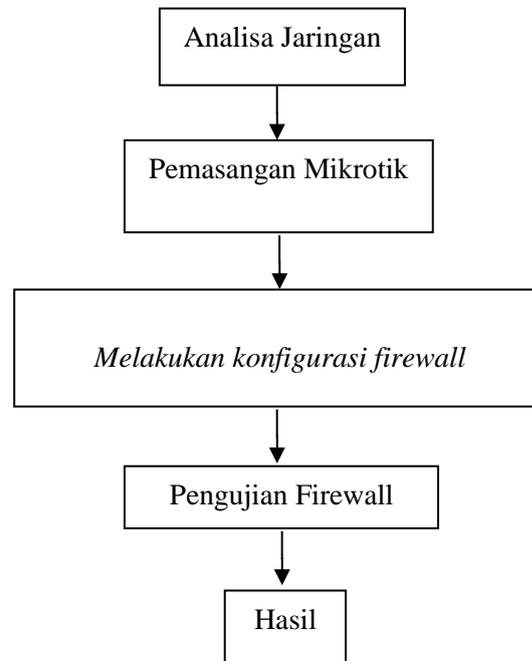
Vol/No/Tahun : Vol. 2/2014

Berdasarkan hasil penelitian yang dilakukan, Kecepatan transfer data yang lambat pada jaringan DISKOMINFO Depok yang disebabkan oleh serangan-serangan baik dari pihak luar maupun dalam jaringan karena belum adanya hak akses antara *client-server*. Permasalahan tersebut dapat teratasi oleh sistem *firewall* rules yang telah dikonfigurasi dalam alat jaringan *mikrotik* termasuk pengamanan *server* dengan *DMZ Rules*. *Routing protocol* yang telah diubah dari *static* menjadi *OSPF* membuat jalannya jaringan data menjadi lebih baik dan lebih cepat, serta admin dapat mengelola jaringan lebih baik dan mudah. Keamanan jaringan menjadi lebih baik dengan adanya konfigurasi yang tidak sesuai dengan konfigurasi default pada awal ketika pembelian alat jaringan, admin pun dapat melakukan pengelolaan alat-alat jaringan yang saling terkoneksi dengan baik (Dwiyatno, Putra, & Krisnaningsih, 2015).

2.5 Kerangka Pemikiran

Kerangka pemikiran merupakan pernyataan kerangka konsep pemecahan masalah yang telah dirumuskan untuk mendapatkan suatu kesimpulan. Sebagai kerangka pemikiran penelitian ini, maka peneliti akan memberikan gambaran guna menjawab perumusan masalah yang telah disebutkan pada awal usulan penelitian ini.

Dari teori yang telah dibahas di atas, maka penulis dapat menyimpulkan suatu kerangka pikiran sebagai berikut:



Gambar 2.9 Kerangka Pemikiran

Pada gambar di atas menjelaskan tentang prosesnya implementasi *firewall* pada sebuah jaringan komputer. Pertama-tama dilakukan analisa terhadap jaringan yang ada. Setelah itu akan melakukan pemasangan *router mikrotik* dan mengkonfigurasi *firewall* pada *router mikrotik*. Kemudian akan didapatkan hasil dari pengujian *firewall* pada *client*.