BAB II
DASAR TEORI

2.1 KAJIAN PUSTAKA

Penelitian terkait perancangan dan analisa desain jaringan internet VPN (*Virtual Private Network*) sebelumnya telah melakukan beberapa penelitian [1 dan 2]. Penelitian Syariful Ikhwan, Ahya Amalina melakukan analisa perancangan jaringan VPN pada Dinhubkominfo Kabupaten Banyumas. Dengan memanfaatkan teknologi VPN sebagai sistem keamanan jaringan dan membangun *tunnel* antara kedua kantor, beberapa *tunneling* yang digunakan diantaranya *Point to Point Tunneling Protocol* (PPTP) dan *Layer Two Tunneling Protocol* (L2TP). Berdasarkan dari penelitian ini difocuskan pada pertukaran layanan FTP, dimana parameter QoS yang digunakan yaitu *jitter, throughput, delay dan packet loss* dengan memberi beban trafik yaitu 512 kbps, 1024 kbps, dan 2048 kbps. Hasil yang diperoleh peneliti bahwa rata-rata nilai delay pada L2TP lebih banyak sampai 41% dibandingkan saat menggunakan PPTP, dengan rata-rata throughput PPTP naik sampai 34% dibandingkan dengan L2TP, dan rata-rata jitter pada PPTP lebih besar sampai 44% dibanding dengan L2TP, namun packet loss yang terjadi pada masing-masing layanan adalah 0 [4].

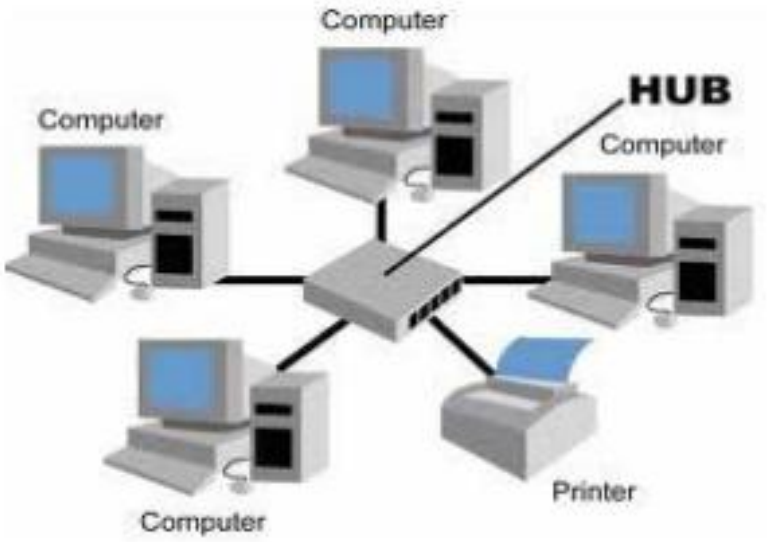
Penelitian Herman Kuswanto melakukan implementasi jaringan VPN menggunakan protokol EoIP. Perancangan jaringan VPN dilakukan dengan konfigurasi EoIP *tunnel* pada kedua router untuk jalur penghubung antar kantor cabang. Berdasarkan implementasi yang dilakukan ada beberapa tahapan yang diuji dalam perancangan jaringan tersebut, dengan mengkonfigurasi di masing – masing router beserta alamat IP dan tahapan pengujian selanjutnya dilakukanlah tes ping dari Router 1 ke PC *Client* dan selanjutnya tes ping Router 2 ke PC *Client*. Dengan digunakannya protokol EoIP Tunel, kantor yang mempunyai koneksi internet dan mendapatkan *bandwidth* internet tersebut, dapat juga memanfatkan jaringan publik/internet tersebut sebagai jalur jembatan penghubung privasi/internet antar dua atau lebih kantor cabang, sehingga antara kantor cabang tersebut terhubung dalam suatu satu segmen yang sama di jaringan internet,

walaupun dalam aspek keamanan EoIP tidak memperbolehkan enkripsi seperti VPN-IP, namun untuk sisi *administration* dapat mengaktifkan fungsi *firewal/filtering* dan monitoring pada interface EoIP [2].

Dedy Cahyadi melakukan perancangan jaringan keamanan dengan fitur *tunneling Virtual Interface EoIP*. Metode yang digunakan pada peracangan yaitu membuat *bridge* antar perangkat MikrotikRouterOS sehingga menjadi terhubung dalam satu segmen jaringan intranet contohnya VPN-IP yang melakukan enkapsulasi ulang mempunyai enkripsi di dalam paket-paket data tersebut, dengan menggunakan jaringan ADSL *Speedy* Telkom (*public network*/internet). Sedangkan untuk segi keamanan administrator dapat mengaktifkan fungsi *firewall/filtering* dan memonitoring pada *interface* - *interface* EoIP, berdasarkan dari hasil perancangan bagian *tunnel Virtual Interface EoIP* lebih lemah dari VPN-IP, disarankan agar koneksi EoIP lancar diperjelaslah kontrak QoS dari pihak telkom ketika akan berlangganan layanan ADSL Speedy dan juga jangan digunakan untuk *fail over system* jika menggunakan ISP yang sama [1].

2.2 SISTEM JARINGAN LOKAL AREA *NETWORK*

Sistem Jaringan (*network*) sebagai kumpulan perangkat (sering disebut dengan *node*) dihubungkan melalui media atau saluran komunikasi. Jaringan *Lokal Area Network* (LAN) merupakan jaringan pribadi dan menggabungkan komputer dalam satu kantor, gedung, atau kampus. Jaringan LAN itu berupa komunikasi dua komputer pribadi (personal komputer) dan sebuah printer atau jaringan yang lengkap termasuk fasilitas komunikasi suara *(voice)* gambar *(image)* dan gambar bergerak (video). Jarak LAN jangkauan yang dibatasi hanya beberapa kilometer saja. Topologi yang digunakan LAN biasanya hanya satu jenis. Jaringan komputer LAN hanya dirancang untuk melakukan pemakaian bersama sebuah perangkat *(resource sharing)* antar komputer pribadi atau anjungan kerja *(workstation)* [5].



Gambar 2.1 Jaringan *Local Area Network* [6].

2.2.1 Sistem *Local Area Network*

Local Area Network (LAN) adalah sistem jaringan komputer dengan luas area lokal ataupun luas tertentu. Jaringan LAN sendiri menghubungkan sejumlah komputer, komputer mini, dan komputer pribadi, sehingga dapat digunakan untuk mengakses ke komputer dan peralatan pendukung (periferal), seperti printer maupun harddisk. Jaringan LAN menyediakan komunikasi berkecepatan yang sangat tinggi pada komputer dan terminal yang satu sama lainnya terhubung dengan jarak yang tidak terlalu jauh, seperti bangunan kantor ataupun pabrik. Sistem LAN juga menyediakan fasilitas sebagai berikut [5].

a. Resource Sharing

Pemakaian sumber daya bersama (printer modern) yang terpasang di server.

2) Information Sharing

Pemakaian bersama program aplikasi dan data yang tersimpan dalam suatu jaringan (server) yang dapat diakses bersama.

3) Network Access Control

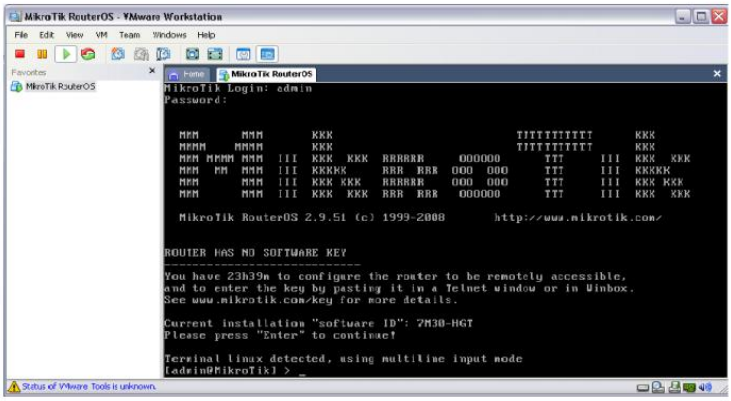
Pemakaian keamanan jaringan komputer yang berusahan menyatukan titik kerja akhir komunikasi pada teknologi keamanan (seperti antivirus dan *firewall*), pengesahan user atau sistem, dan pelaksanaan keamanan jaringan.

2.3 MIKROTIK ROUTER OS

Router adalah suatu perangkat yang melewatkan paket *Internet Protocol* (IP) dari suatu jaringan ke jaringan yang lainnya, yang mempergunakan metode *addressing* serta protokol tertentu agar bisa melewatkan paket data tersebut. Router dengan kemampuan melewatkan paket IP dari satu jaringan ke jaringan lainnya kemungkinan memliki banyak jalur diantara keduanya. Router-router tersebut saling tersambung didalam jaringan internet ikut serta dalam sebuah algoritma routing yang terdistribusi menentukan jalur terbaik yang dilalui paket *Internet Protocol* (IP). Dalam suatu proses merouting ini dilakukanlah dengan cara *hop by hop*. *Internet Protocol* (IP) tidak mengetahuinya jalur yang keseluruhannya menuju setiap tujuan paket. Pada IP routing mempunyai IP *address* yang disediakan pada router berikutnya yang menurutnya lebih dekat dari *host* tujuannya. Adapun pada router beroperasi di layer tiga *Open System Interconnection* (OSI) yang dipergunakan untuk melakukan berupa segmentasi pada jaringan lokal. Fungsi dari Router adalah sebagai berikut :

a. Mengetahui alamat IP maupun logika *Address Source* dan *Destination* dengan cara menentukan routing dari jaringan lokal ke lokal lainnya.
b. Menyimpan routing dengan menentukan jalur terbaik antar LAN ke WAN.
c. Perangkat di layer 3 *Open System Interconnection* (OSI) Layer.
d. Bisa juga berupa "box" atau sebuah OS yang menjalankan sebuah daemon routing .

MikroTik RouterOS sendiri merupakan sebuah operasi *Linux base* yang diperuntukkan sebagai network router, yang didesain memberikan kemudahan bagi pengguna. Administrasinya pun dapat dilakukan yaitu *Windows Application* (WinBox). Selain itu pun dengan instalasi bisa dilakukannya pada standard komputer PC (Personal Computer). Dimana PC yang akan dijadikan router mikrotik tidak memerlukan *resource* yang cukup besar dalam penggunaan standard, contohnya untuk *gateway*. Dalam keperluan beban yang tidak kecil (*network* yang kompleks, routing yang rumit) lebih disarankannya untuk mempertimbangkan untuk pemilihan *resource* PC yang memungkinkan memadai [7].



Gambar 2.2 Tampilan Pada MikroTik [7].

2.4 *VIRTUAL PRIVATE NETWORK* (VPN)

Virtual Private Network (VPN) merupakan sebuah koneksifitas antara satu jaringan sesama jaringan yang lain secara privasi dengan melalui jaringan Internet (publik). Disebut juga Virtual Network dikarenakan VPN menggunakan jaringan internet sebagai media perantaranya bias juga koneksinya bukan secara langsung. Dan bias disebut juga Private Network dikarenakannya VPN memiliki sifat privasi dalam artian hanya orang-orang tertentu yang bisa mengaksesnya. Dalam data yang dikirimkan melewati VPN terenkripsi jadi cukup aman dan rahasianya tetap terjaga, meskipun hanya dikirimkannya melalui jaringan internet, itulah arti atau definisi dari VPN tersebut.

2.4.1 Fungsi VPN

1. Kerahasiaan (*Confidentially*).

VPN merupakan teknologi memakai jaringan internet ataupun jaringan publik yang tentu sangat rawan terhadap pencurian informasi maupun file data. Maka itu VPN mempergunakan metode enkripsi untuk mengacak data yang lewat. Dengan memakai metode enskripsi itu, untuk keamanan data akan lebih terjaminnya dari pencurian data tersebut. Andaikan ada pihak yang mampu menyadap data yang lewat jaringan internet maupun untuk jalur dari VPN itu sendiri, namun belum mengetahui juga yang menyadap dapat membaca data tersebut karena datanya sebelumnya telah teracak-acak. Adapun fungsi dari

confidentially ini bisa disimpulkan agar ketika data yang di kirimkan bisa diakses oleh orang-orang yang diijinkan saja.

2. Keutuhan data (*Data Integrity*).

VPN itu mempunyai teknologi yang mampu menjaga keutuhan informasi ataupun data, awal dari data tersebut yang dikirim hingga sampai ke tujuannya. Sehingga datanya pada saat pengiriman kemungkinan terhindar dari berbagai macam-macam gangguan seperti datanya rusak, hilang, maupun dimanipulasi oleh pihak yang tidak bisa bertanggung jawab.

3. Autentikasi sumber (*Origin Authentication*).

Dari kemampuan VPN tersebut mampu melakukan *authentication* terhadap sumber dari pengiriman datanya yang akan di terima. VPN pun mampu melakukan pemeriksaan kepada data masuk hingga mengakses informasi dari sumbernya, setelah itu alamat dari sumber data tersebut akan di setujui jika proses autentifikasinya berhasil, dan juga VPN tersebut mampu menjamin semua datanya yang di kirimkan maupun yang diterima berasal dari sumber yang memang benar-benar semestinya, maupun informasi ataupun data yang dikirimkan oleh pihak lain dan data yang dipalsukan tersebut [8].

2.5 ROUTING

Routing merupakan proses penentuan jalur terbaik sebuah data dalam suatu jaringan. jenis routing memiliki 2 jenis, yaitu : *static routing* dan *dynamic routing. protocol routing* dapat diartikan aturan router yang saling berkomunikasi [9]. didalam pembuatan rancangan pada jaringan, pemilihan pada perancangan *routing protocol* yang akan membuat jaringan dapat menentukan jalur manakah yang lebih baik dalam pengiriman data dari komputer ke komputer tujuan dan dapat lebih meningkatkan kualitas pada suatu layanan pada jaringan tersebut.

2.5.1 IPv4 *(Internet Protocol versi 4)*

IPv4 merupakan identifikasi pengalamatan jaringan yang digunakan dalam *protocol* TCP/IP. Panjang totalnya adalah 32 bit dan dibagi berdasarkan *octet* dan setiap *octet* berukuran 8 bit dengan dipisahkan oleh tanda titik. Secara teori, pada IP *address* tidak boleh sama dengan *host* yang lain. Untuk memudahkan IP *address* dibentuk dan diatur dalam pembagian IP address. Pada IPv4 memiliki

lima bagian kelas yang berbeda – beda antara lain kelas A. B, C, D, dan E berikut penjelasan pada masing – masing kelas [10].

1. Kelas A

   Pada IP kelas A memiliki *range* IP address yaitu dari 0.0.0.0 s/d 127.255.255.255. Sedangkan IP *private* yaitu 10.0.0.0 s/d 10.255.255.255.

2. Kelas B

   Pada IP kelas B memiliki *range* IP address yaitu dari 128.0.0.0 s/d 192.255.255.255. Sedangkan alamat IP *private* yaitu 172.16.0.0 s/d 172.31.255.255.

3. Kelas C

   Pada IP kelas C memiliki *range* IP address yaitu dari 192.0.0.0. s/d 233.255.255.255. Sedangkan alamat IP *private* pada kelas C yaitu 192.168.0.0 s/d 192.168.255.255.

4. Kelas D

   Pada alamat IP kelas D ini hanya digunakan untuk *multicasting.*

5. Kelas E

   Pada alamat IP kelas E digunakan untuk penelitian pada masa yang akan datang.

2.6 *TUNNELING*

Tunneling adalah suatu teknologi yang ditugaskan untuk menangani hingga menyediakan koneksi point-to-point dari sumber tujuannya. Untuk teknologi ini disebut *tunnel* dikarenakan koneksi point-to-point ini sebenarnya terbentuk dengan melintasi jaringan umum tetapi tidak memperdulikan paket-paket data milik orang lain yang sama-sama bersamaan melintasi jaringan umum tersebut, tapi koneksi ini cuma melayani saat trasnportasi data dari pembuatnya. Koneksifitas point-to-point ini sebetulnya tidak benar-benar ada tetapi datanya yang dikirim terlihat seperti benar-benar melewati koneksi pribadi yang bersifat point-to-point .

Untuk teknologi tersebut dibikin dengan diatur IP *Address* dan IP Routing, sehingga antara *tunnel* sumber dan tunnel tujuan bisa saling berkomunikasi dengan pengalamatan *Internet Protocol* (IP) melalui jaringan tersebut, bila

komunikasi antar sumber dengan tujuan dari tunnel tidak mampu berjalan baik, maka disitulah tunnel yang terbentuk dan VPN tidak dapat terbuat. Setelah tunnel itu terbentuk dengan baik, point-to-point tersebut bisa langsung dipergunakan untuk mengirimkan dan menerima datanya. Dalam implementasi VPN, dikarenakan tunnel tersebut tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. Tunnel dilengkapi dengan sebuah sistem *encription* agar menjaga data yang telah dilewatinya [11].

2.6.1 *Point-to-point Tunneling Protocol* (PPTP)

Point-to-point Tunneling Protocol (PPTP) adalah protokol jaringan yang memungkinkannya pengamanan pengiriman data dari remote *client* ke server dengan membuatnya salah satu VPN melalui TCP/IP. Teknologi jaringan PPTP juga adalah pengembangan *remote access point-topoint protocol* (PPP) yang dikeluarkannya *Internet Engineering Task Force* (IETE). PPTP tersebut merupakan protokol jaringan yang merubah paket PPP menjadi IP datagram agar bisa dikirimkannya melalui internet. PPTP ini bisa digunakan dijaringan privasi LAN to LAN dan komputer yang tesambung dangan LAN untuk membuat VPN melalui LAN tersebut. Keunggulan paling utama dari pemakaian PPTP yaitu dapat dipergunakan *Public Switched Telephone Network* (PSTN) untuk membangun VPN tersebut. Pembuatannya PPTP tersebut memakan biaya yang cukup kecil dan lebih mudah digunakan secara luas, menjadikan salah satu solusi untuk *remote user* dan *mobile user* dikarenakan PPTP mampu memberikan keamanan serta *encryiption* komunikasi melalui PSTN maupun internet. Umumnya terdapat dua dipergunakan dalam PPTP, yaitu [11]:

a. *Client* PPPT, utama kerja PPTP dimulai dari sebuah *remote* atau PPTP *client* yang membutuhkannya akses ke sebuah LAN *private* dari sebuah perusahaan. Pengaksesannya dicoba dengan itu menggunakan ISP lokal.
b. Untuk *PPTP Server,* setelah *client* membuat koneksifitas antara PPP ke ISP, dengan melakukan panggilan yaitu *Dial-Up* yang selanjutnya dibuat melalui koneksifitas PPP yang sudah ada, dan data yang dikirimkan menggunakan koneksi tersebut dalam bentuk IP *datagram* yang berisikan paket PPP yang telah ter-*enkapsulation*. Sedangkan panggilan yang berikutnya tersebut

selanjutnya menciptakan koneksitifitas VPN ke server PPTP pada *LAN* privasi. Koneksi tersebut (melalui panggilan yang kedua ini) yang diistilahkannya sebagai *tunneling*.

2.6.2 *Layer Two Tunneling Protocol* (L2TP)

L2TP adalah salah satu *tunneling* yang dibekerjakan di layer 2, L2TP merupakan *tunneling* protokol pengembangan dari PPTP pada Microsoft dan *Layer 2 Forwarding* (L2F) dari Cisco. protokol *tunneling* yang digunakan untuk mendukung VPN. Protokol L2TP tidak menyediakan enkripsi atau kerahasiaan dengan sendirinya, protokol ini bergantung pada enkripsi yang dilewatinya dalam sebuah terowongan untuk memberikan privasi. L2TP dalam pertukaran paket yang dikategorikan sebagai paket kontrol atau paket data. Pada L2TP memberikan kehandalan fitur dalam paket kontrol, namun tidak ada keandalan untuk paket data [4].

2.6.3 *Ethernet over IP* (EOIP)

Ethernet over IP (EoIP) *Tunneling* adalah protokol MikroTik RouterOS yang menciptakan terowongan *Ethernet* di antara dua router di atas koneksi IP. Terowongan EoIP dapat berjalan di atas terowongan PPTP atau koneksi lain yang mampu mengangkut IP. Bila fungsi penjembatan dari router diaktifkan, semua lalu lintas *Ethernet* (semua protokol *Ethernet*) akan dijembatani sama seperti jika memiliki antarmuka *Ethernet* dan kabel fisik antara dua router (dengan *bridging enabled*). Protokol ini membuat beberapa skema jaringan dengan mem-*bridge* LAN melalui internet, melalui *tunnel* yang terenkripsi, dan *bridge* LAN dijaringan *wireless* [12]:

2.7 *BRIDGE*

Bridge merupakan suatu alat jaringan yang menyambungkan kedua jaringannya di lapisan sambungan data (*data link layer*). *Bridge* ini tidak me-*route* paketnya pada lapisan jaringan (*network layer*). Hanya saja secara sederhana mengulangkan paket antara dua jaringan di sambungan lokal (*link-local*). *Bridge* ini pun juga merupakan metode koneksifitas yang menggabungkan dua atau

lebihnya *interface* bertipe *ethernet* atau sejenisnya, seandai-andai berada didalam *segmen network* yang sama. Dimana suatu proses *Bridging* pada *layer data link*. Dengan mengaktifkannya *bridge* pada dua buah *interface* akan menonaktifkan fungsi berjalannya routing diantara kedua *interface* tersebut. *Ethernet Bridge* itu adalah dua atau lebih *(multiple) ethernet/network* segmen yang dihubungkan menghubungkan pada layer *data link* (layer 2) dari model OSI. Bridge itu memiliki kesamaan dengan perangkat *repeater* ataupun *hub* yang menghubungkan segmen *network* pada *layer physical*, sedemikian rupa sebuah bridge itu beraktifitas dengan teknik *forwarding packet* yang biasa dipergunakan dalam *packet-switching* dijaringan komputer tersebut, yakni *traffic* dari satu *network* diatur/dikelola ketimbang seolah-olah *broadcast* ulang ke *segment network* yang saling berhempitan. Network bridge memiliki ciri khas [1]:

2.7.1 Jenis – Jenis *Bridge*

Bridge memiliki beberapa jenis yang diantaranya :

a. *Transparent Bridge*

   Terutama ditemukan di lingkungan Ethernet, dan sebagian besar digunakan untuk menjembatani jaringan yang memiliki tipe media yang sama. *Bridge* menyimpan tabel alamat tujuan dan antarmuka keluar.

b. *Source Route Bridge*

   Terutama ditemukan di lingkungan Token Ring. *Bridge* hanya meneruskan berdasarkan indikator routing yang terdapat dalam frame. Endstations bertanggung jawab untuk menentukan dan memelihara tabel alamat tujuan dan indikator routing.

c. *Translational Bridge*

   Hanya digunakan untuk menjembatani data antar jenis media yang berbeda. Ini biasanya digunakan untuk beralih antara Ethernet dan FDDI atau Token Ring ke Ethernet.

d. *Source Route Translational Bridging (SR/TLB)*

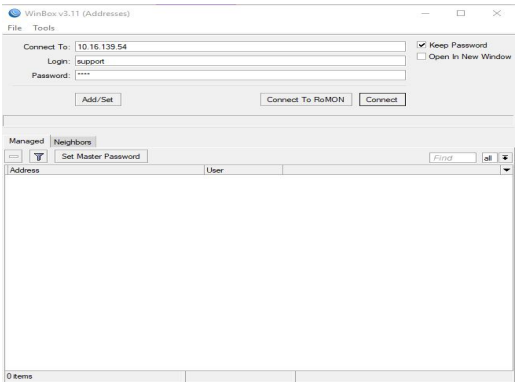
kombinasi penjembatan sumber-sumber dan penjembatan *transparan* (tidak terlihat) yang memungkinkan komunikasi di lingkungan campuran *ethernet*

dan*token ring*. Penempatan tanpa indikator *routing* antara *token ring* dan *ethernet* itu juga disebut SR / TLB.

Menjembatani terjadi pada lapisan data-link, yang mengendalikan arus data, menangani kesalahan transmisi, memberikan pengalamatan fisik, dan mengelola akses ke media fisik. Jembatan menganalisis frame yang masuk, membuat keputusan forwarding berdasarkan frame tersebut, dan meneruskan frame ke tujuan mereka. Terkadang, seperti di SRB, bingkai berisi keseluruhan jalan menuju tujuan. Dalam kasus lain, seperti dalam menjembatani transparan, frame diteruskan satu hop pada satu waktu menuju tempat tujuan. Jembatan bisa berupa remote atau lokal. Jembatan lokal menyediakan koneksi langsung antara banyak segmen LAN di wilayah yang sama [13].

2.8 WINBOX

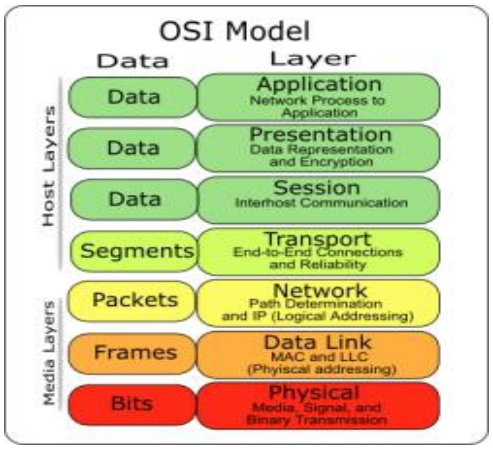
Winbox adalah sebuah *utility* yang digunakan untuk melakukan remote ke server mikrotik kita dalam mode GUI. Jika untuk mengkonfigurasi mikrotik dalam text mode melalui PC itu sendiri, maka untuk mode GUI yang menggunakan winbox ini kita mengkonfigurasi mikrotik melalui komputer client. Fungsi utama winbox adalah untuk konfigurasi mikrotik, tugas utama winbox adalah untuk mengkonfigurasi atau mengatur mikrotik dengan mode GUI, fungsi winbox ada tiga pertama atur mikrotik router, kedua untuk *setting bandwidth* jaringan internet, ketiga untuk seting memblokir sebuah situs dan bisa sebagai *sahring data* [14]:



Gambar 2.3 Tampilan WinBox [14].

2.9 OSI LAYER

Pada suatu jaringan membutuhkan komponen dan perangkat dalam *standart protocol* yang dapat digunakan oleh perangkat tersebut. Salah satu standar *protocol* yang dikembangkan oleh ISO (*International Standard Organization)* yaitu OSI (*Open System Interconnection)*. OSI *Layer* merupakan model referensi yang mendefinisikan *standart* koneksi untuk sebuah komputer [15]. Model OSI juga dapat mempunyai suatu tujuan utama yaitu untuk mendesain jaringan serta juga memahami fungsi *layer* masing – masing yang berhubungan dengan jaringan komunikasi. Pada *Layer* OSI (*Open System Interconnection)* dibagi menjadi 7 *layer* yaitu :



Gambar 2.4 *Layer* OSI (*Open System Interconnection)* [16].

Pada gambar diatas yaitu 2.4 merupakan suatu urutan pada OSI *Layer* tersebut, pada OSI ini mempunyai tugas atau fungsi model yang berbeda – beda pada setiap *Layer* nya. Untuk itu berikut ulasan kegunaan dari masing – masing fungsi OSI : [16].

1. *Physical Layer,* lapisan yang berada sangat dekat dengan *user,* bertanggung jawab atas proses data menjadi bit, dan mengrimkan serta menjaga koneksi.
2. *Data Link Layer,* berfungsi sebagai salah satu pengelolaan atau menyediakan prosedur pengiriman data didalam sebuah jasringan dan juga menentukan suatu bit – bit data yang dikelompokkan menjadi format yang disebut sebagai *frame.*

3. *Network Layer,* berfungsi sebagai pengendali operasi subnet dan mendefiniskan alamat IP dan membuat *header* pada paket – paket.
4. *Transport Layer,* berfungsi sebagai pengiriman data secara *end-to-end*. Pada lapisan ini bertanggung jawab terhadap keselamatan data.
5. *Session Layer,* berfungsi sebagai membangun, mensinkronkan, dan menjaga sistem yang berkomunikasi dan mengakhiri suatu hubungan komunikasi.
6. *Presentation Layer,* berfungsi untuk mentranslasikan suatu data yang akan ditansmisikan oleh sebuah aplikasi kedalam format yang dapat ditransmisikan melalui jaringan tersebut. Dan jika untuk memastikan bahwa apakah suatu data dapat terbaca oleh suatu sistem.
7. *Application Layer,* berfungsi sebagai melayani *remote* terminal dan mengatur bagaimana aplikasi dapat mengkases jaringan .

2.10 *QUALITY Of SERVICE* (QoS)

Quality of Service (QoS) adalah metode yang berguna dalam pengukuran pada suatu jaringan manakah yang lebih baik untuk setiap nilai parameternya. QoS memiliki kemampuan untuk menyediakan prioritas pada aplikasi *user,* dan aliran data, QoS bertugas dapat mengetahui kinerja dari performansi dari setiap parameter yang ada, parameter - parameter yang disebutkan didalam *Quality of Service* terdiri dari *throughput, delay,* dan *packet loss* [17].

2.10.1 *Packet Loss*

Packet Loss meruapakan sebagai kegagalan paket mencapai tujuan atau bisa disebut dengan hilangnya jumlah paket dalam proses pengiriman menuju penerima. kegagalan paket disebabkan antara lain :

a. Terjadinya tabrakan dalam jaringan, dan *memory* yang terbatas.
b. Pada trafik terjadiya *overload* pada jaringan.
c. Kegagalan pada penerima yang disebabkan karena *overflow* terjadi karena *buffer.*

Adapun untuk nilai *Packet Loss* yang didapatkan jika semakin kecil nilai jumlah data yang hilang, maka semakin baik [17]. Pada *Packet Loss* memiliki *standard* untuk kualitas sebagai berikut.

Tabel 2.1 Kategori *Packet Loss* [15]

Kategori Degrasi	Paket Loss
Sangat bagus	0%
Bagus	3%
Sedang	15%
Buruk	25%

$$Paket\ Loss = \frac{(jumlah\ paket\ yang\ diterima - paket\ terkirim)}{Jumlah\ Paket\ Yang\ diterima} X\ 100\% \quad [2.1]$$

2.10.2 Throughput

Throughput adalah kecapatan (*rate*) transfer data efektif, yang diukur dalam bps. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama *interval* waktu tertentu dibagi oleh durasi *interval* waktu tersebut[17]. Rumus *throughput* yang digunakan;

$$Throughput = \frac{Jumlah\ data\ yang\ dikirm}{Waktu\ pengiriman\ data} \quad [2.2]$$

2.10.3 Delay

Delay merupakan sebagai waktu tunda pada suatu data yang diproses pada jaringan atau waktu yang dibutuhkan pada data untuk menempuh jarak dari suatu *node* ke *node* lainnya sebagai tujuannya [18]. Berikut *standart delay.*

Tabel 2.2 Kategori *Delay* [17]

Kategori Degrasi	*Delay*
Sangat bagus	<150 ms
Bagus	150 ms s/d 300 ms
Sedang	300 ms s/d 450 ms
Buruk	>450 ms

$$Delay = \frac{Total\ Waktu}{Jumlah\ total\ paket} \quad [2.3]$$