BAB 2
LANDASAN TEORI

2.1 Profil Instansi

Profil CyberCity Networks meliputi sejarah, visi, misi, logo, tujuan, dan struktur organisasi CyberCity Networks.

2.2 Sejarah Instansi

CyberCity Networks adalah sebuah perusahaan yang bergerak di bidang *Internet Service Provider* dalam skala kecil yang mulai beroperasi sejak tahun 2009 dengan nama CyberCity Bandung yang pada intinya menangani jasa koneksi *internet* dengan area terbatas misalnya satu komplek perumahan, satu kelurahan atau satu wilayah. Pada tahun 2012 diputuskan untuk menggantikan nama dengan nama CyberCity Network dengan layanan yang sama yaitu seputar jasa koneksi *internet*.

CyberCity Networks berkomitmen menghadirkan layanan koneksi *internet* dengan support terbaik yang senantiasa siap setiap saat membantu pelanggan yang terdiri dari berbagai level kemampuan dan pengalaman dengan sebuah motto "*Committed to perfection of our internet service*".



Gambar 2.1 Logo CyberCity Networks

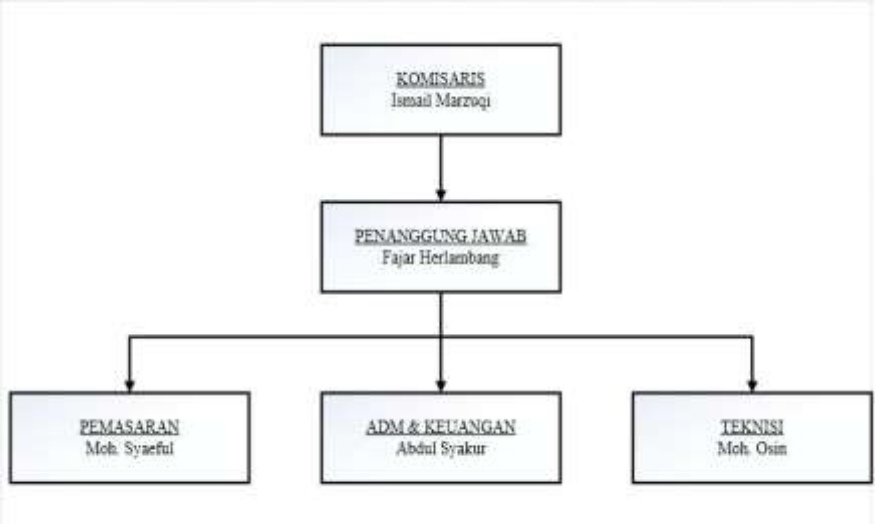
2.3 Visi dan Misi Instansi

Berikut adalah Visi dan Misi CyberCity Networks :

1. Membangun provider RT-RW NET yang dapat memberikan kesempatan kepada masyarakat luas untuk mendapatkan akses *Internet* murah.
2. Membangun aplikasi di lingkungan masyarakat, serta menjadikan *internet* murah dan memasyarakat.

2.4 Struktur Organisasi

Struktur organisasi merupakan kerangka yang menunjukan seluruh kegiatan untuk mencapai tujuan organisasi, hubungan antara fungsi serta wewenang dan tanggung jawabnya. Struktur organisasi di CyberCity Networks dijelaskan pada gambar 2.2. sebagai berikut :



Gambar 2.2 Struktur Organisasi CyberCity Networks

2.5 Deskripsi Pekerjaan

Deskripsi pekerjaan adalah seperangkat fungsi dan tugas tanggung jawab yang dijabarkan ke dalam kegiatan pekerjaan. Tugas dan tanggung jawab dari struktur organisasi yang terdapat pada gambar 2.2.

a. Komisaris

   Melakukan proses *controling* terhadap jalannya perusahaan. Memberikan masukkan yang positif demi kemajuan perusahaan kepada Penanggung Jawab.

b. Penanggung Jawab

   Bertanggung jawab penuh terhadap jalannya perusahaan. Melakukan proses analisa terhadap perkembangan perusahaan. Mengkoordinasikan semua pihak didalam organisasi sehingga semua proses didalam perusahaan dapat berjalan dengan baik dan lancar.

c. Manajer Pemasaran

   Bertanggung jawab terhadap target penjualan perusahaan. Membuat strategi marketing.

d. Manajer Administrasi dan Keuangan

   Bertanggung jawab terhadap proses administrasi organisasi serta kebutuhan operasional organisasi dalam menjalankan bisnisnya dan bertanggung jawab terhadap pelaporan keuangan.

e. Manajer Teknis

   Bertanggung jawab terhadap segala masalah teknis yang terjadi disisi NOC maupun yang terjadi disisi pelanggan.

2.6 Landasan Teori

Landasan Teori bertujuan memberikan gambaran dari teori yang terkait dalam perancangan aplikasi. Landasan teori yang diuraikan merupakan hasil studi literatur, baik dari buku, maupun situs *internet*.

2.7 Pengertian Sistem

Sistem adalah kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu. Sistem ini menggambarkan suatu kejadian-kejadian dan kesatuan yang nyata adalah suatu objek nyata, seperti tempat, benda, dan orang-orang yang betul-betul ada dan terjadi [14].

Suatu sistem adalah seperangkat elemen yang membentuk kumpulan atau procedure-procedure/ bagan-bagan pengolahan yang mencari suatu tujuan bagian atau tujuan bersama dengan mengoprasikan data dan/atau barang pada waktu rujukan tertentu untuk menghasilkan informasi dan/atau energi dan/atau barang [14].

2.8 Sistem Billing

Billing berasal dari bahasa Inggris yaitu *bill (noun)*, yang artinya bukti transaksi pembayaran. Maka *billing (adv)* dapat juga diartikan mengirim bukti transaksi, atau mengumumkan bukti transaksi.

Sistem billing merupakan sistem yang membantu para usahawan untuk mengatur dan mencatat segala transaksi yang terjadi. Contohnya bagi para pengusaha warung *internet*, *billing* sistem digunakan untuk memonitoring pengguna dan pemasukan warnetnya. Sedangkan jika bagi usaha di bidang rumah sakit sistem billing digunakan untuk mencatat proses pelayanan, mulai pasien datang sampai dengan pasien pulang. Menghitung biaya yang harus dibayar pasien secara otomatis, serta memberikan informasi sebagai analisa pengambilan keputusan secara cepat dan akurat [10].

2.9 Pengertian Jaringan Komputer

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer *autonomous*. Dalam bahasa populer dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti router, switch, dan sebagainya) yang saling terhubung satu sama lain melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (nirkabel). Informasi berupa data akan mengalir dari satu komputer ke komputer lainnya atau dari satu komputer ke perangkat yang lain, sehingga masing-masing komputer yang terhubung tersebut bisa saling bertukar data atau berbagi perangkat keras [1].

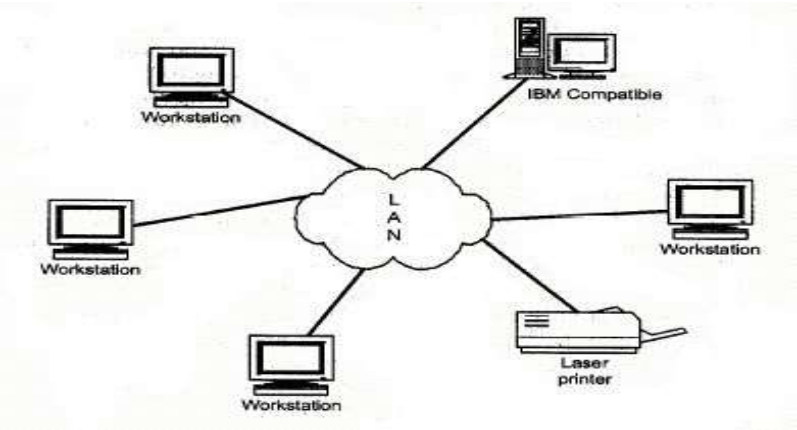
Jaringan komputer dapat dibedakan berdasarkan luas area geografisnya. Ada tiga kategori utama jaringan komputer yaitu :

1. LAN *(Local Area Network)*

LAN *(Local Area Network)* adalah jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor perusahaan atau pabrik-pabrik untuk memakai bersama *resource* (misalnya, printer) dan saling bertukar informasi.

LAN mempunyai ukuran yang terbatas, yang berarti bahwa waktu transmisi pada keadaan terburuknya terbatas dan dapat diketahui sebelumnya. Dengan mengetahui keterbatasannya, menyebabkan adanya kemungkinan untuk menggunakan jenis desain tertentu. Hal ini juga memudahkan manajemen jaringan.

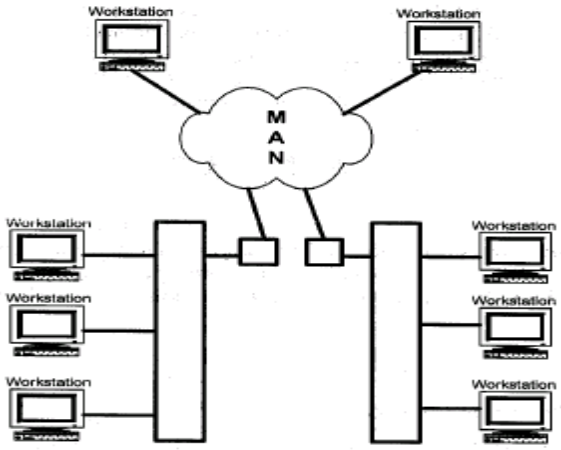
Seperti halnya saluran pelanggan telepon yang dipakai di daerah pedesaan. LAN seringkali menggunakan teknologi transmisi kabel tunggal. LAN tradisional beroperasi pada kecepatan mulai 10 sampai 100 Mbps dengan delay rendah (puluhan *microsecond*) dan mempunyai faktor kesalahan yang kecil. LAN-LAN modern dapat beroperasi pada kecepatan yang lebih tinggi, sampai ratusan mega*bit*/detik. Skema jaringan LAN dapat dilihat pada gambar 2.3.



Gambar 2.3 Skema jaringan LAN [2].

2. MAN *(Metropolitan Area Network)*

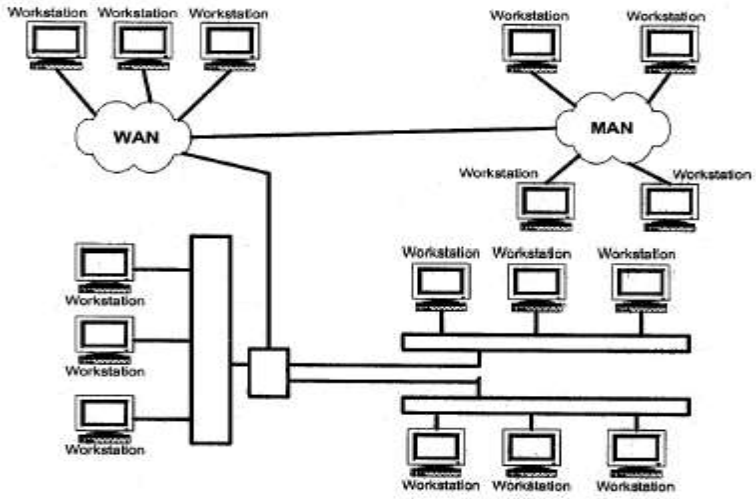
Merupakan jaringan komputer yang meliputi area seukuran kota atau gabungan beberapa LAN yang dihubungkan menjadi sebuah jaringan besar. MAN bisa saja berupa gabungan jaringan komputer beberapa sekolah atau beberapa kampus. MAN dapat diimplementasikan pada *wire* maupun *wireless network.* MAN dapat memanfaatkan jaringan TV kabel yang umumnya menggunakan kabel jenis *coaxial* atau serat optik. Skema jaringan MAN dapat dilihat pada gambar 2.4.



Gambar 2.4 Skema jaringan MAN [2].

3. WAN *(Wide Area Network)*

Jaringan komputer yang mencakup area lokasi yang lebih luas, dengan melibatkan kesatuan komputer yang lebih banyak. Hal ini sudah jelas berbeda dengan MAN atau mungkin LAN yang dibatasi dengan ruang dan bangunan. WAN tidak dibatasi dengan ruang ataupun bangunan bahkan cakupannya bisa sampai dengan antar benua. Skema jaringan WAN dapat dilihat pada gambar 2.5.



Gambar 2.5 Skema jaringan WAN [2].

Berdasarkan media penghantar, jaringan komputer dapat dibagi menjadi dua jenis yaitu [1] :

1. *Wire Network*

   Wire Network adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data ditransmisikan pada kabel. Kabel yang umum digunakan pada jaringan komputer biasa menggunakan bahan dasar tembaga. Ada juga jenis kabel lain yang menggunakan bahan fiber optik atau serat optik. Bahan tembaga banyak digunakan pada LAN. Sedangkan untuk MAN dan WAN menggunakan gabungan kabel tembaga dan serat optik.

2. *Wireless Network*

   Wireless Network adalah jaringan komputer yang menggunakan media penghantar berupa gelombang radio atau cahaya (*infrared* atau *laser*). Saat ini sudah semakin banyak pusat perbelanjaan, airport, rumah sakit, dan lokasi lain yang menyediakan layanan *wireless network*. Sehingga pengguna dapat dengan mudah melakukan akses *Internet* menggunakan handphone, laptop, PDA, dan perangkat mobile lainnya. Frekuensi yang digunakan *wireless network* biasanya 2.4 GHz dan 5.8 GHz. Sedangkan

penggunaan *infrared* dan *laser* umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah titik saja (disebut *point to point*).

Berdasarkan pola pengoperasian atau fungsi masing-masing komputer maka jaringan komputer dapat dibagi menjadi [1] :

a. Client Server

Client server adalah jaringan komputer yang salah satu komputernya difungsikan sebagai *server* atau komputer yang memberikan pelayanan kepada komputer lain. *Server* melayani komputer lain yang disebut *client*. Layanan yang diberikan bisa berupa akses *web*, *e-mail*, *file* atau yang lain. *Client server* banyak dipakai oleh *Internet* dan Intranet.

b. Peer to Peer

Peer to peer adalah jenis jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan *access* dari / ke komputer lain. *Peer to Peer* banyak diimplementasikan pada LAN. Walaupun dapat juga diimplementasikan pada MAN, WAN, atau *Internet*, namun hal ini kurang lazim. Salah satu alasannya adalah masalah manajemen dan *security*. Cukup sulit mengawasi *security* pada jaringan *peer to peer* manakala pengguna jaringan komputer sudah sangat banyak.

2.9.1 Manfaat Jaringan Komputer

Pemanfaatan teknologi jaringan ini tentu saja tidak tanpa alasan, karena para ahli komputer telah berhasil meyakinkan para pengguna jaringan bahwa berbagai bentuk keuntungan dan efisiensi akan diperoleh dengan memanfaatkan teknologi jaringan komputer untuk perangkat-perangkat komputer yang ada yaitu [2]:

a. Resource sharing

Kemampuan berbagi pakai sumber daya baik berupa perangkat keras maupun perangkat lunak yang terdapat dan terhubung dengan jaringan komputer tersebut.

b. Integrasi data

Memungkinkan terjadinya pengintegrasian data dari berbagai terminal pemasukan data dan transaksi kedalam pusat pengolahan data sehingga memudahkan untuk memperoleh informasi yang akurat setiap saat.

c. Distributed processing

Pembangunan jaringan komputer ini dapat mencegah ketergantungan kepada komputer pusat. Setiap proses data tidak harus dilakukan pada satu komputer saja, melainkan dapat didistribusikan ke komputer lainnya.

d. Keamanan data

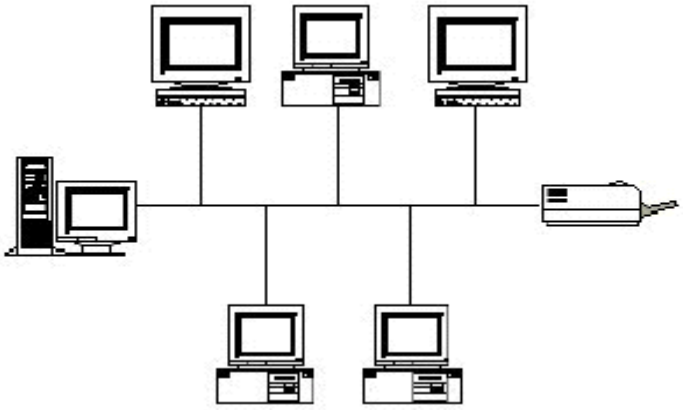
Sistem keamanan jaringan komputer memudahkan dalam melakukan perlindungan terhadap data yang terpusat pada *server*. Jaminan keamanan data tersebut dapat diberikan melalui pengaturan hak akses para pemakai dan password.

2.10 Topologi Jaringan

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer yang lainnya sehingga membentuk jaringan. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya. Berikut jenis-jenis topologi dasar jaringan diantaranya [1]:

1. Topologi *bus*

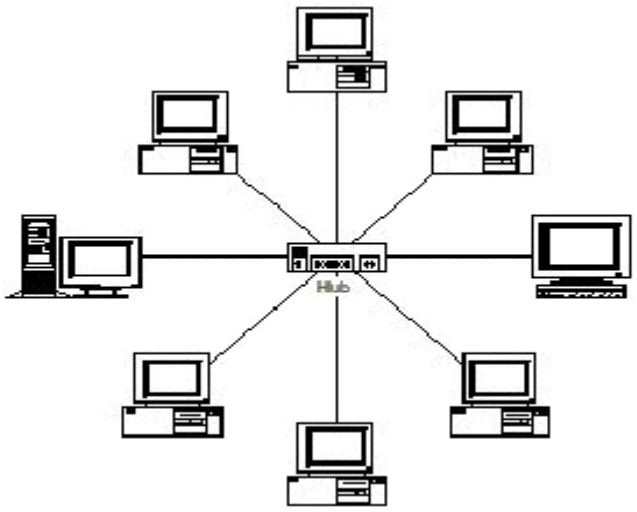
Topologi *bus* yaitu topologi yang di setiap terminalnya terhubung ke sebuah jalur utama komunikasi data. Informasi atau data yang akan dikirim dan diambil harus melalui jalur utama komunikasi data dan melewati *workstation* (komputer). Gambar 2.6 menunjukan bentuk topologi *bus*.



Gambar 2.6 Topologi *Bus* [1].

2. Topologi *Star* (Bintang)

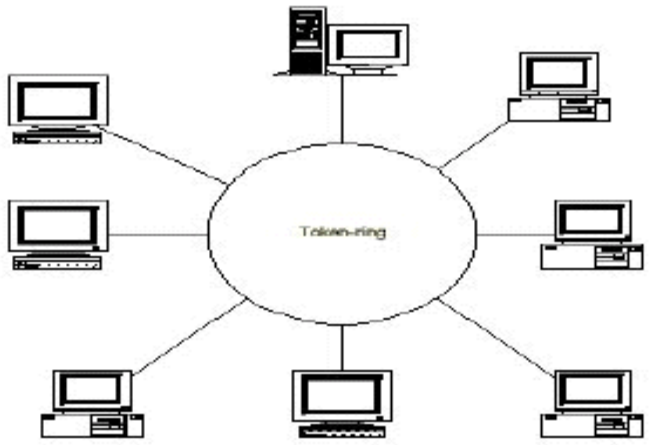
Topologi *Star* yaitu topologi yang memiliki pusat berupa *hub* atau *switch* yang berfungsi untuk menghubungkan dan meneruskan pengiriman data antara perangkat. Kelebihan dari topologi *start* adalah mudah melakukan pelacakan ketika terjadi suatu masalah fisik, mudah untuk melakukan penambahan dan pengurangan perangkat, jika terjadi suatu masalah pada suatu jalur maka tidak mempengaruhi jalur lain. Gambar 2.7 menunjukan topologi *star*.



Gambar 2.7 Topologi *Star* [1].

3. Topologi *Ring* (Cincin)

Topologi *ring* yaitu topologi yang mana setiap perangkat terhubung secara seri dengan yang lain hingga membentuk suatu lingkaran yang tertutup (*loop*). Kelebihan dari topologi ini adalah mudah dalam pembangunannya dan biaya untuk pembangunan topologi ini masih lebih murah dibandingkan dengan topologi *star*. Gambar 2.8 menunjukan topologi *ring*.



Gambar 2.8 Topologi *Ring* [1].

2.11 Protokol Jaringan

Protokol jaringan adalah perangkat aturan yang digunakan dalam jaringan. Protokol adalah aturan main yang mengatur komunikasi diantara beberapa komputer didalam sebuah jaringan sehingga komputer-komputer anggota jaringan dan komputer beberapa platform dapat saling berkomunikasi. Semua jenis-jenis jaringan komputer menggunakan protokol. Aturan-aturan protokol adalah termasuk didalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data [2].

2.11.1 Jenis-Jenis Protokol

a. Token Ring

Dalam suatu token ring, suatu pola *bit* khusus yang disebut token bergerak mengelilingi terminal-terminal kapan saja walaupun terminal dalam keadaan diam. Ketika suatu terminal ingin mentransmisikan suatu *frame,* terminal tersebut harus meraih token itu. Oleh karena hanya ada satu token, maka hanya satu terminal saja yang dapat melakukan transmisi pada saat yang sama. Dengan metode ini, maka tidak akan terjadi tumbukan dalam pengiriman data. Pada metode ini suatu terminal harus menunggu giliran pada waktu yang relatif lebih lama bila akan mengirim data. Namun tidak mungkin terjadi tumbukan sinyal data, karena saat pengiriman data merupakan waktu ekslusif bagi terminal pengirim [2].

b. Ethernet

Ethernet bekerja berdasarkan *broadcast* network, dimana setiap node menerima setiap transmisi data yang dikirim oleh sebuah node menggunakan metode CSMA/CD (*carier sense multiple access/collision detection*) [2].

c. ATM (Asynchronus Transfer Mode)

ATM memiliki kecepatan transfer data yang tinggi, yaitu mencapai 150 Mbps atau lebih. Teknologi ATM ini sangat cocok digunakan untuk pengiriman data dalam bentuk video, CD audio dan gambar. ATM bekerja pada model topologi *star,* dengan menggunakan *fiber optic cable* ataupun *twisted pair cable*. ATM pada umumnya digunakan untuk menghubungkan dua atau lebih *Local Area Network* (LAN) [2].

d. FDDI (Fiber Distributed Data Interface)

Merupakan protokol yang digunakan untuk transmisi pada jaringan yang menyerupai *token passing ring* yang meningkatkan kinerja jaringan. Hal ini dimungkinkan FDDI menggunakan serat optik dengan kecepatan 100 Mbps. FDDI dapat menghubungkan sampai 500

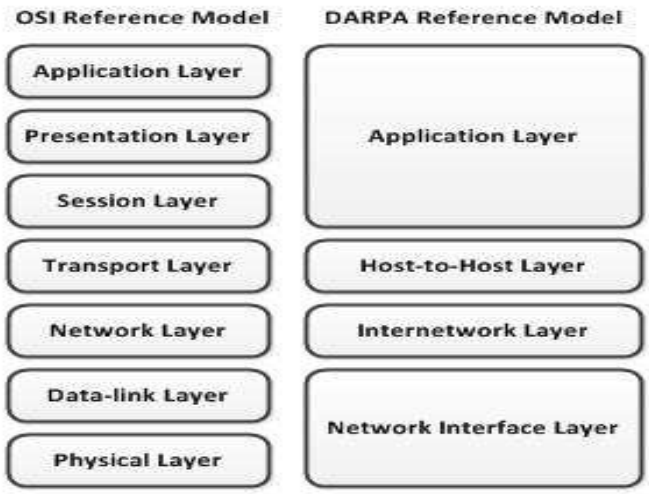
terminal dengan jarak maksimum 2 km. Disamping itu FDDI memiliki kemampuan untuk menghubungkan lebih dari satu jaringan lokal [2].

e. **TCP/IP *(Transmission Control Protokol/Internet Protokol)***

Adalah sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada *Wide Area Network* (WAN). TCP/ IP terdiri dari sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Protokol ini merupakan komunikasi utama dalam *internet* serta intranet. Merupakan protokol yang sangat banyak digunakan untuk jaringan komputer. Protokol ini hanya menggunakan 4 layer dalam pengiriman datanya, yaitu: *Aplication, transport, internet,* dan *network layer* [2].

2.12 Model OSI Layer (*Open System Interconection*)

Model OSI adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan *Internasional Organization for Standardization* (ISO) di Eropa pada tahun 1977. OSI sendiri merupakan singkatan dari Open System Interconnection. Model ini disebut juga dengan "Model tujuh lapis OSI" (*OSI seven layer model*). Gambar model OSI Layer dapat dilihat pada gambar 2.9 [1].



Gambar 2.9 Model OSI Layer [1].

2.12.1 Lapisan OSI Layer (*Open System Interconection*)

a. Phisical Layer

Lapisan terendah ini mengatur singkronisasi pengiriman dan penerimaan data, spesifikasi mekanik, elektrik dan *interface* antar terminal, seperti besar tegangan, frekuensi, koneksi pin dan jenis kabel.

b. Data Link Layer

Pada lapisan ini data diubah dalam bentuk paket, sinkronisasi paket yang dikirim maupun yang diterima, persiapan saluran antar terminal, pendeteksian kesalahan yang terjadi saat pengiriman data dan pengendalian akses saluran.

c. Network Layer

Lapisan ini menentukan rute pengiriman dan pengendalian kemacetan, agar data sampai ditempat tujuan dengan benar.

d. Transport Layer

Lapisan ini mengatur keutuhan data, menerima data dari lapisan *session* dan meneruskannya ke lapisan *Network*. Lapisan ini juga memeriksa apakah data sudah sampai dialamat yang dituju.

e. Session Layer

Lapisan ini menyiapkan saluran komunikasi dan terminal dalam hubungan antar terminal, mengkoordinasikan proses pengiriman dan penerimaan serta mengatur pertukaran data.

f. Presentation Layer

Pada lapisan ini dilakukan konversi data agar data yang dikirim dapat dimengerti oleh penerima, kompresi teks dan penyandian data.

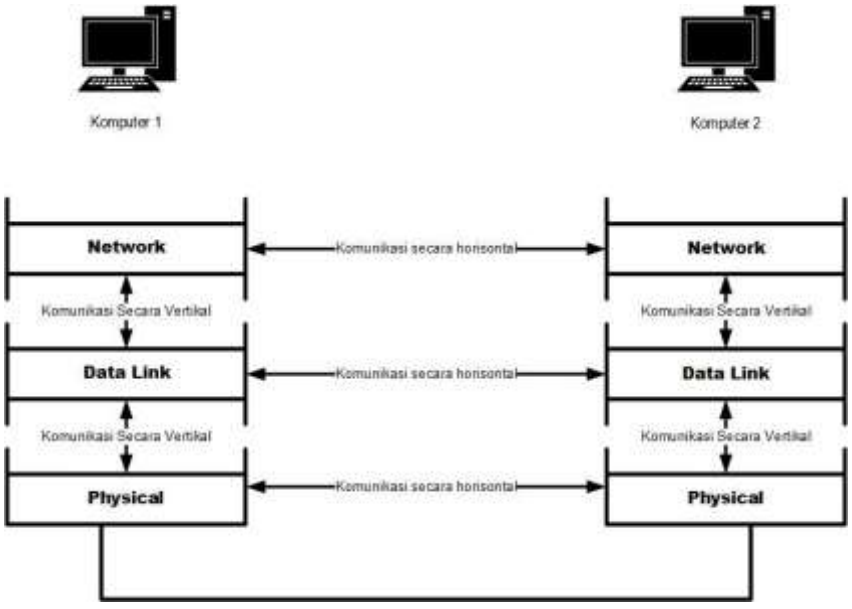
g. Application Layer

Lapisan paling tinggi ini mengatur interaksi pengguna komputer dengan program aplikasi yang dipakai. Lapisan ini juga mengatur pemakaian bersama data dan peralatan, pengiriman file dan pemakaian database.

2.12.2 Komunikasi OSI Layer (*Open System Interconection*)

Suatu layer dapat berkomunikasi secara “vertikal” dengan layer lain yang berada tepat dibawah atau diatasnya. Sebagai contoh, layer *Data Link* dapat berkomunikasi dengan layer *Physical* atau *Network.* Namun layer *Data Link* tidak bisa berkomunikasi dengan layer *Application.*

Suatu layer juga dapat berkomunikasi secara “horizontal” dengan layer yang sama pada *host* lain. Misalkan layer *Data Link* berkomunikasi dengan layer *Data Link* pada *host* yang lain. Komunikasi layer secara horizontal bersifat virtual, artinya tidak akan terjadi secara langsung sebagaimana yang dilakukan pada komunikasi vertikal. Ilustrasi komunikasi antar layer dapat dilihat pada gambar 2.10 [2].



Gambar 2.10 Komunikasi antar layer [2].

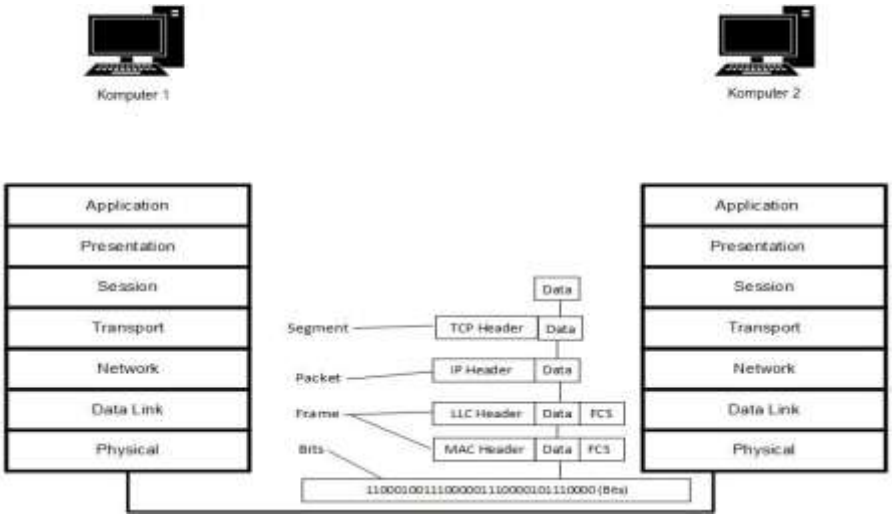
Informasi yang mengalir dari satu layer ke layer yang lain akan mengalami perubahan bentuk atau transformasi untuk memahaminya, perhatikan ilustrasi berikut yang menggambarkan transformasi informasi dari layer *Application* hingga layer *Physical* [1].

a. Informasi berawal dari layer *Application*. Informasi kemudian melewati layer *Presentation* dan layer *Session*. Pada tahap ini biasanya belum dilakukan transformasi data. Informasi yang melalui ketiga layer ini disebut PDU (*Protocol Data Unit*) atau data saja.
b. Setelah sampai di layer *Transport*, data akan mengalami transformasi ke bentuk lain yang disebut segment.
c. Segment mengalir ke layer *Network* dan kemudian diubah menjadi paket.
d. Paket mengalir ke layer *Data Link* dan kemudian diubah menjadi *frame*.
e. Terakhir, *frame* mengalir ke layer *Physical* dan kemudian diubah menjadi *bits* atau *bit-bit*. Pada layer ini, *bit-bit* diubah besaran fisik, seperti arus listrik, gelombang elektromagnetik, dan sebagainya.

Proses pengubahan bentuk dari satu layer ke layer berikutnya dilakukan dengan menambahkan *header* khusus. Inilah yang disebut dengan *encapsulation* atau *enkapsulasi*. Proses enkapsulasi terjadi berulang-ulang hingga data diubah menjadi *bit-bit*. Kemudian *bit-bit* ini dikirim ke *host* target melalui media jaringan.

Setelah informasi berupa *bit-bit* sampai di *host* target maka proses kebalikannya, yaitu melepas *header* satu persatu dari layer terbawah hingga ke layer paling atas akan dilakukan. Proses melepas *header* ini disebut *de-encapsulation* atau *de-enkapsulasi*.

Proses *enkapsulasi* dan *de-enkapsulasi* dapat dianalogikan dengan pengiriman barang via pos. Barang yang dikirim akan dibungkus, diberi alamat, diantarkan ke kantor pos. Selanjutnya petugas pos akan mengantarkannya ke alamat tujuan. Setelah sampai di tujuan, si penerima dapat membuka bungkusnya kembali. Proses enkapsulasi dapat dilihat pada gambar 2.11.



Gambar 2.11 Proses enkapsulasi [2].

2.13 IP Address *(Internet Protocol)*

IP adalah protokol yang mengatur bagaimana suatu data dapat dikenal dan dikirim dari satu komputer ke komputer lain. IP bersifat *connectionless protokol*. Ini berarti IP tidak melakukan *error detection* dan *recovery*. IP tidak dapat melakukan *handshake* (pertukaran kontrol informasi) saat membangun sebuah koneksi, sebelum data dikirim. Padahal *handshake* merupakan salah satu syarat agar sebuah koneksi baru dapat terjadi. Dengan demikian, IP bergantung pada *layer* lainnya untuk melakukan *handshake*.

Adanya IP Address merupakan konsekuensi dari penerapan *Internet* Protokol untuk mengintegrasikan jaringan komputer *Internet* di dunia. Seluruh *host* (komputer) yang terhubung ke *Internet* dan ingin berkomunikasi memakai TCP/IP harus memiliki IP Address sebagai alat. Pengenal *host* pada network. Secara logika, *Internet* merupakan suatu network besar yang terdiri dari berbagai sub network yang terintegrasi. Oleh karena itu, suatu IP Address harus bersifat unik untuk seluruh dunia. Tidak boleh ada satu IP Address yang sama dipakai oleh dua *host* yang berbeda. Untuk itu, penggunaan IP Address di seluruh dunia dikoordinasi oleh lembaga sentral *Internet* yang dikenal dengan IANA (*Internet Assigned Number Authority*) [1].

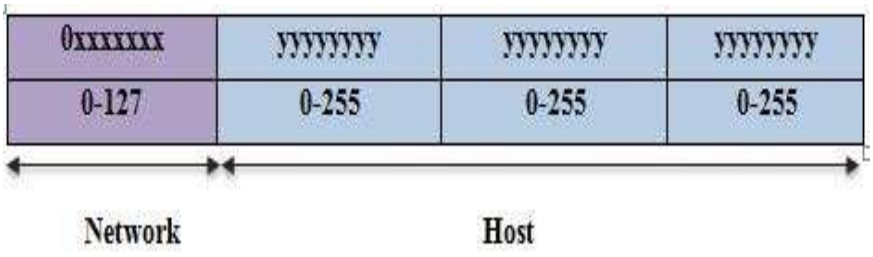
2.13.1 Kelas IP Address

IPV4 dipisahkan menjadi 2 bagian, yakni bagian *bit* network dan bagian *bit host*. *Bit network* berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan *bit host* berperan dalam identifikasi *host* dalam suatu *networks*. Jadi seluruh *host* yang tersambung dalam jaringan yang sama memiliki *bit network* yang sama [1].

Sebagian dari *bit-bit* bagian awal dari IP Address merupakan *network bit*/ *networks number*, sedangkan sisanya untuk *host*. Garis pemisah antara bagian *network* dan *host* tidak tetap, bergantung kepada kelas *network*. Ada 3 kelas address yang utama dalam TPC/IP, yakni kelas A, kelas B dan kelas C. Perangkat lunak *internet* Protokol menentukan pembagian jenis kelas ini dengan menguji beberapa *bit* pertama dari IP Address. Pembagian 3 address kelas yang utama adalah sebagai berikut :

1. **Kelas A**

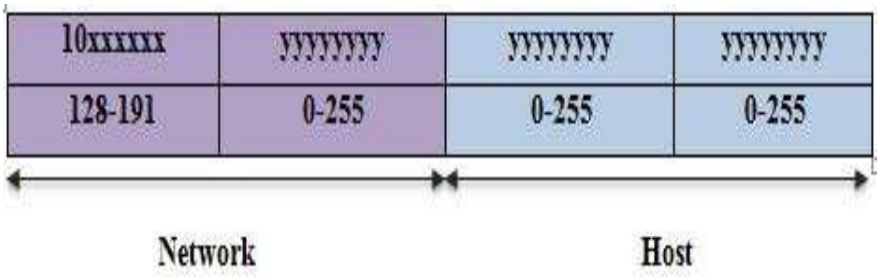
   Ciri IP Address kelas A adalah jika *bit* pertama dari IP Address adalah 0. *Bit* ini dan 7 *bit* berikutnya (8 *bit* pertama) merupakan *bit-bit networks* (*network bit*) dab boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 24 *bit* terakhir merupakan *bit host*. Untuk lebih jelasnya dapat dilihat pada gambar 2.12.



Gambar 2.12 IP Address kelas A [1].

2. Kelas B

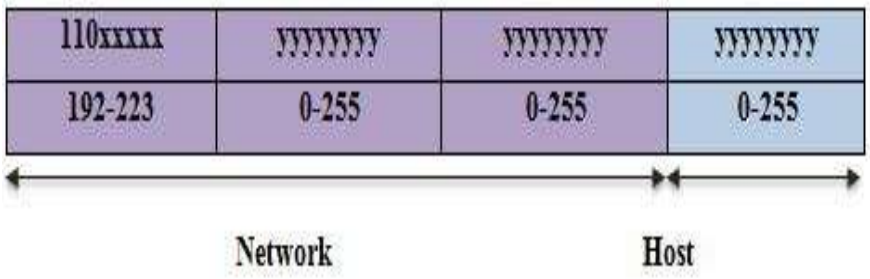
Ciri IP Address kelas B adalah jika 2 *bit* pertama adalah 10. Dua *bit* ini dan 14 *bit* berikutnya (16 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 16 *bit* terakhir merupakan *bit host*. Untuk lebih jelasnya dapat dilihat pada gambar 2.13.



Gambar 2.13 IP Address kelas B [1].

3. Kelas C

Ciri IP kelas C adalah jika 3 *bit* pertama adalah 110. Tiga *bit* ini dan 21 *bit* berikutnya (24 *bit* pertama) merupakan *bit network* dan boleh bernilai berapa saja (kombinasi angka 1 dan 0), sedangkan 8 *bit* terakhir merupakan *bit host*. Untuk lebih jelasnya dapat dilihat pada gambar 2.14.



Gambar 2.14 IP Address kelas C [1].

2.13.2 Jenis IP Address

1. IP Public

   Alamat IP Publik adalah alamat IP yang digunakan oleh sebuah perangkat jaringan yang terhubung langsung ke *internet* untuk mengidentifikasikan dirinya ke *internet*. Koneksi lalu lintas data yang dilakukan di *internet* menggunakan alamat IP Publik ini. IP Publik dapat dilihat pada gambar 2.15.

Class	1st Octet DEC range	1st Octet BIN	Start Address	Finish Address	1st Octet High Order Bits	Network/ Host	Default Subnet Mask
A	1-126	00000001-01111110	0.0.0.0	126.255.255.255	0	N.H.H.H	255.0.0.0
B	128-191	10000000-10111111	128.0.0.0	191.255.255.255	10	N.N.H.H	255.255.0.0
C	192-223	11000000-11011111	192.0.0.0	223.255.255.255	110	N.N.N.H	255.255.255.0

Gambar 2.15 IP Publik [1].

2. IP Private

   Alamat IP Private adalah alamat IP yang diberikan untuk komputer-komputer yang tidak diakses secara publik melainkan hanya diakses di dalam jaringan lokal (LAN) sehingga tidak membutuhkan pemetaan ke luar. IANA (*Internet Assigned Numbers Authority*) telah mengalokasikan 3 buah blok IP untuk digunakan sebagai IP Private dan tidak boleh digunakan sebagai IP Publik. IP Private dapat dilihat pada gambar 2.16.

Kelas A	10.0.0.0 – 10.255.255.255	16.777.216 hosts
Kelas B	172.16.0.0 – 172.31.255.255	1.048.576 hosts
Kelas C	192.168.0.0 – 192.168.255.255	65.536 hosts

Gambar 2.16 IP Private [1].

2.14 DNS (*Domain Name System*)

DNS (*Domain Name System*) adalah pemberian nama yang mudah diingat pada sistem dan layanan yang membantu manusia berinteraksi dengan jaringan. Ketika piranti yang berlainan sedang berkomunikasi antara satu dengan yang lainnya, alamat IP dan *Physical Address* (MAC) akan membuat sulit seseorang menghafalnya. Oleh sebab itu DNS digunakan untuk memudahkan manusia dalam berinteraksi dengan piranti dalam jaringan tertentu karena sifatnya yang merubah alamat IP menjadi barisan karakter yang mudah diingat manusia [5].

2.15 DHCP (*Dynamic Host Configuration Protocol*)

DHCP (*Dynamic Host Configuration Protocol*) adalah satu layanan yang berfungsi untuk menentukan alamat IP dan informasi IP lain secara dinamis dalam sebuah sistem. DHCP bekerja sebagai model *server client* dimana suatu sistem yang tidak memiliki alamat IP membuat permintaan kepada *server* dan kemudian *server* memberikan IP dan sistem menerima IP tersebut untuk mengakses jaringan atau sumber lain [5].

2.16 Metode PPPoE (*Point to Point Protocol over Ethernet*)

Kerja standar untuk protokol PPPoE diterbitkan oleh IETF pada tahun 1999. IETF spesifikasi untuk PPPoE adalah RFC 2516. PPPoE memperluas kemampuan asli PPP dengan memungkinkan koneksi *point to point virtual* atas arsitektur jaringan *multipoint Ethernet*. PPPoE adalah protokol yang banyak digunakan oleh ISP untuk menyediakan *Digital Subscriber Line* (DSL) kecepatan tinggi layanan *internet*, layanan yang paling populer adalah ADSL. Kesamaan antara PPP dan PPPoE telah menyebabkan adopsi luas dari PPPoE sebagai pilihan protokol untuk menerapkan kecepatan tinggi akses *internet*. Penyediaan layanan dapat menggunakan *server* autentikasi yang sama untuk sesi PPP dan PPPoE, menghasilkan penghematan biaya. PPPoE menggunakan metode standar enkripsi, autentikasi dan kompresi yang ditentukan oleh PPP [10].

PPPoE dikonfigurasi sebagai titik ke titik sambung antara dua *port Ethernet*. Sebagai sebuah protokol *tunneling*, PPPoE digunakan sebagai landasan yang efektif untuk transportasi paket IP pada *layer* jaringan. IP dibalut melalui sambungan PPP dan menggunakan PPP sebagai virtual *dial-up* hubungan antara poin pada jaringan. Dari perspektif pengguna, PPPoE sesi dimulai dengan menggunakan koneksi perangkat lunak pada mesin klien atau router. Inisialisasi sesi PPPoE melibatkan identifikasi alamat perangkat *remote* kontrol akses media (MAC) [11]. Berikut adalah kelebihan menggunakan metode PPPoE:

1. Terdapat user *authentication*
2. Interface PPPoE *server* yang terhubung dengan PPPoE *client* tidak memiliki IP karena PPPoE bekerja pada layer 2 OSI dengan tujuan menghindari terjadinya serangan *Denial of Service* (DoS) dan *IP detection* kepada *server* utama.
3. Fasilitas *cut-off* oleh PPPoE untuk *user* yang menggunakan program tambahan peningkat *bandwidth* (seperti download *accelerator*). Penggunaan *internet* setiap usernya dipantau secara oleh administrator sistem. Secara default PPPoE akan melakukan *cut-off* (memutuskan) koneksi *user* yang lebih tinggi (*burst mode*) dari koneksi yang ditetapkan untuk menjaga kestabilan jaringan.

2.17 Perangkat Keras Jaringan

Perangkat keras jaringan adalah perangkat komputer yang menghubungkan komputer dengan komputer lainnya agar dapat berinteraksi dan saling transfer data. Berikut ini adalah perangkat keras jaringan komputer [2]:

2.17.1 *Server*

Sebuah *server* merupakan sebuah komputer yang berisi program, baik sistem operasi maupun program aplikasi yang menyediakan pelayanan kepada komputer atau program lain yang sama ataupun berbeda.

Sebagai contoh dalam mengelola pengiriman file, *database* atau menerima *email* pada saat yang bersamaan dengan tugas yang lain. *Server* juga harus menyimpan informasi dan membaginya dengan cepat [2].

2.17.2 Workstation

Keseluruhan komputer yang terhubung ke file *server* dalam sebuah jaringan. Dimana komputer ini sebagai tempat kerja atau pengolahan data yang diakses dari *server*. Komputer ini hanya merupakan perpanjangan dari *server*. Tetapi sekarang ini *workstation* sebagian besar menggunakan *Personal Computer (PC)* [2].

2.17.3 NIC (*Network Interface Card*)

Sebuah kartu jaringan dan merupakan perangkat yang menyediakan media untuk menghubungkan antar komputer kedalam sistem jaringan. Dilihat dari interfacenya umumnya terbagi dua yaitu PCI dan ISA. Terdapat juga beberapa *card* diperuntukkan khusus untuk laptop atau notebook dengan socket PCMCIA. Gambar *Network Interface Card* dapat dilihat pada gambar 2.17.



Gambar 2.17 NIC (*Network Interface Card*) [1].

2.17.4 Switch

Switch merupakan suatu *device* pada jaringan yang secara konseptual berada pada layer 2 (*Data link Layer*) dan layer 3 (*Network Layer*). Maksudnya, switch pada saat pengiriman data mengikuti MAC address pada NIC (*Network Interface Card*) sehingga *switch* mengetahui kepada siapa paket ini akan diterima. Jika ada *collision* yang terjadi merupakan *collision* pada *port-port* yang sedang saling berkirim paket data. Misalnya ketia ada pengiriman paket data dari *port* A ke *port* B dan pada saat yang sama ada pengiriman paket data dari *port* C ke *port* D, maka tidak akan terjadi tabrakan (*collision*) karena alamat yang dituju berbeda dan tidak menggunakan jalur yang sama. Semakin banyak *port* yang tersedia pada *switch*, tidak akan mempengaruhi *bandwitch* yang tersedia untuk setiap *port*.

Ketiak paket data dikirim melalui salah satu *port* pada *switch*, maka pengiriman paket data tersebut tidak akan terlihat dan tidak terkirim ke setiap *port* lainnya sehingga masing-masing *port* mempunyai *bandwith* yang penuh. Hal ini menyebabakan kecepatan *transfer* data lebih terjamin. Gambar *switch* dapat dilihat pada gambar 2.18 [1].



Gambar 2.18 Switch [1].

2.17.5 Repeater

Fungsi utama adalah untuk memperkuat sinyal. Sinyal yang diterima dari satu segmen kabel LAN ke segmen LAN berikutnya akan dipancarkan kembali dengan kekuatan sinyal asli pada segmen LAN pertama, sehingga dengan adanya *repeater* ini, jarak antara dua jaringan komputer dapat diperluas. Gambar *repeater* dapat dilihat pada gambar 2.19 [1].



Gambar 2.19 Repeater [1].

2.17.6 Bridge

Bridge digunakan untuk menghubungkan dua buah LAN dan memungkinkan paket data dari satu LAN ke LAN yang lain. Sebuah *bridge* menyediakan sambungan antara dua tipe LAN yang sama, misalnya *Ethernet* LAN dan *Token passing*. Dengan *bridge* dapat memperluas jaringan LAN, sehingga semua segmen yang saling berhubungan satu sama lainnya menjadi bagian dari LAN yang lebih besar. Gambar *bridge* dapat dilihat pada gambar 2.20 [1].



Gambar 2.20 Bridge [1].

2.17.7 Router

Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan yang lain yang mungkin memiliki banyak jalur diantara keduanya. Router juga dapat digunakan untuk menghubungkan sejumlah LAN sehingga trafik yang dibangkitkan oleh suatu LAN terisolasikan dengan baik dengan trafik yang dibangkitkan oleh LAN lain. Router bisa berupa sebuah *device* yang dirancang khusus untuk berfungsi sebagai router (*dedicated router*), atau bisa juga berupa sebuah PC yang difungsikan sebagai router. Gambar router dapat dilihat pada gambar 2.21 [1].



Gambar 2.21 Router [1].

2.18 Keamanan Jaringan

Keamanan jaringan adalah melindungi jaringan, tetapi melindungi dalam hal ini adalah masih mempunyai artian luas. Keamanan tidak hanya tentang menjaga orang-orang didalam jaringan dari dunia luar. Akan tetapi juga menyediakan akses ke dalam jaringan dengan cara yang dikehendaki, dipersilahkan orang-orang di dalam jaringan itu untuk bekerja sama [1].

Ada beberapa elemen tentang keamanan jaringan yaitu:

1. Integritas (*Integrity)*
   Data yang diterima mestilah sama dengan yang diinginkan.
2. Kehandalan (*Reliability)*
   Data dapat digunakan secara baik tanpa ada halangan.
3. Ketersediaan (*Availability)*
   Ketersediaan data jika diperlukan.
4. Keamanan (*Security*)
   Data yang dikirim maupun yang diterima dilindungi dari akses yang tidak diinginkan.

2.19 Hotspot

Hotspot atau area *hotspot* adalah tempat khusus yang disediakan untuk mengakses *internet* menggunakan peralatan *Wi-Fi*. Umumnya layanan *hotspot* bersifat gratis. Dengan berbekal laptop atau PDA maka koneksi *internet* dapat dilakukan secara cuma-cuma.

Biasanya pengguna terlebih dulu harus melakukan *registrasi* ke penyedia layanan *hotspot* untuk mendapatkan *login* dan *password*. Kemudian pengguna dapat mencari area *hotspot*, seperti pusat perbelanjaan, kafe, hotel, kampus, bandara udara, dan tempat-tempat umum lainnya. Proses otentikasi dilakukan ketika *browser* diaktifkan [1].

2.20 WLAN (*Wireless Local Area Network*)

Wireless Local Area Network (WLAN) adalah jaringan komputer yang menggunakan frekuensi radio dan *infrared* sebagai media transmisi data. *Wireless LAN* sering disebut sebagai jaringan nirkabel atau jaringan *wireless* [1].

Proses komunikasi tanpa kabel ini dimulai dengan bermunculan peralatan berbasis gelombang radio, seperti *walkie talkie, remote control, cordless phone, ponsel*, dan peralatan radio lainnya. Lalu adanya kebutuhan untuk menjadikan komputer sebagai barang yang mudah dibawa (*mobile*) dan mudah dihubungkan dengan jaringan yang sudah ada. Hal-hal seperti ini akhirnya mendorong pengembangan teknologi *wireless* untuk jaringan komputer.

Pada akhir 1970-an IBM mengeluarkan hasil percobaan mereka dalam merancang WLAN dengan teknologi IR (*infrared*), perusahaan lain seperti Hewlett-Packard (HP) menguji WLAN dengan RF (*radio frequency*). Kedua perusahaan tersebut hanya mencapai data rate 100 Kbps. Karena tidak memenuhi standar IEEE 802 untuk LAN yaitu 1 Mbps maka produknya tidak dipasarkan. Baru pada tahun 1985, *Federal Communication Commision* (FCC) menetapkan pita *Industrial, Scientific and Mediacal* (ISM band) yaitu 902-928 MHz, 2400-2483.5 MHz dan 5725-5850 MHz yang bersifat tidak terlisensi, sehingga pengembangan WLAN secara komersial memasuki tahap serius. Barulah pada tahu 1990 WLAN dapat dipasarkan dengan produk yang menggunakan teknik *spread spectrum* pada pita ISM, frekuensi terlisensi 18-19 GHz dan teknologi IR dengan data rate > 1 Mbps. Pada tahun 1997, sebuah lembaga independen bernama IEEE membuat spesifikasi/ standar WLAN pertama yang diberi kode 802.11. Peralatan yang sesuai standar 802.11 dapat bekerja pada *frekuensi* 2,4 GHz, dan kecepatan transfer data (*throughput*) teoritis maksimal 2Mbps. Pada bulan juli 1999, IEEE kembali mengeluarkan spesifikasi baru bernama 802.11b. Kecepatan transfer data teoritis maksimal yang dapat dicapai adalah 11 Mbps. Kecepatan transfer data sebesar ini sebanding dengan *Ethernet tradisional* (IEEE 802.3 10Mbps atau 10Base-T). Peralatan yang menggunakan standar 802.11b juga bekerja pada *frekuensi* 2,4Ghz.

Pada tahun 2002, IEEE membuat spesifikasi baru yang dapat menggabungkan kelebihan 802.11b dan 802.11a. Spesifikasi yang diberi kode 802.11g ini bekerja pada frekuensi 2,4GHz dengan kecepatan transfer data teoritis maksimal 54Mbps. Peralatan 802.11g kompatibel dengan 802.11b, sehingga dapat saling dipertukarkan. Misalnya saja sebuah komputer yang menggunakan kartu jaringan 802.11g dapat memanfaatkan *access point* 802.11b, dan sebaliknya. Pada tahun 2006, 802.11n dikembangkan dengan menggabungkan teknologi 802.11b, 802.11g. Teknologi yang diusung dikenal dengan istilah MIMO (*Multiple Input Multiple Output*) merupakan teknologi *Wi-Fi* terbaru. MIMO dibuat berdasarkan spesifikasi Pre-802.11n. Kata "Pre-" menyatakan "*Prestandard* version of 802.11n". MIMO menawarkan peningkatan *throughput*, keunggulan *reabilitas*, dan peningkatan jumlah klien yang terkoneksi. Serta dapat menghasilkan kecepatan transfer data sebesar 108Mbps [2].

Secara umum perbandingan diantara keempat standar dimaksud dapat dijabarkan seperti pada tabel dibawah ini:

Tabel 2.1 Perbandingan Standar *Wireless LAN* [2].

	802.11a	**802.11b**	**802.11g**	**802.11n**
Standard Approved	Juli 1999	Juli 1999	June 2003	Not yet ratified
Maximum Data Rate	54 Mbps	11 Mbps	54 Mbps	600Mbps
Modulasi	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
RF Band	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz or 5GHz
Channel Width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz

Sedangkan bila dilihat dari sisi kompatibilitas dengan standar yang lain, maka dapat dijabarkan seperti tabel berikut ini:

Tabel 2.2 Family Standar *Wireless LAN* [2].

Family Standar Wireless LAN		
Standar	**Band Frequensi**	**Compatibele**
802.11b	2,4 GHz	b
802.11a	5 GHz	a
802.11g	2,4 GHz	b.g
802.11n	2,4 GHz	b,g,n

2.21 Firewall

Firewall merupakan suatu cara /sistem / mekanisme yang diterapkan baik terhadap *hardware*, *software* maupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan atau kegiatan semua segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation*, *server*, router, atau *local area network* (LAN) [1].

Firewall adalah suatu cara untuk membatasi informasi yang masuk dan keluar dari jaringan lokal. Pada umumnya *host* firewall terhubung ke *internet* dan LAN lokal, dan akses LAN ke *internet* hanya dapat melalui firewall. Dengan demikian firewall dapat mengendalikan apa yang diterima dan dikirim dari *internet* dan LAN lokal [1].

Firewall secara umum diperuntukkan guna melayani:

1. Mesin/komputer

   Setiap individu yang terhubung langsung ke jaringan luar atau *internet* dan menginginkan semua yang terdapat pada komputernya terlindungi.

2. Jaringan

   Firewall berguna pada jaringan komputer dengan berbagai jenis topologi, baik milik perusahaan, organisasi, atau yang lain.

Firewall memiliki beberapa karakteristik:

1. Seluruh hubungan dari dalam keluar harus melewati firewall. Hal ini dapat dilakukan dengan membatasi semua akses jaringan lokal kecuali melewati firewall terlebih dahulu.

2. Hanya sebuah kegiatan yang terdaftar/ dikenal yang dapat melakukan hubungan.
3. Firewall sendiri harus kebal terhadap serangan yang terjadi apabila ada upaya merusak firewall yang telah ditentukan.

Firewall memiliki beberapa teknik:

1. *Service Control* (kendali terhadap layanan):
   Firewall ini digunakan dengan cara mengecek alamat IP *address* dan nomor *port* yang digunakan, baik pada protokol TCP dan UDP.
2. *Direction Control* (kendali terhadap arah):
   Firewall akan berjalan berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.
3. *User Control* (kendali terhadap pengguna):
   Firewall akan berjalan saat dimana user diijinkan/ tidak menjalankan suatu *service*. Biasanya digunakan untuk membatasi akses *user* dari jaringan lokal untuk mengakses keluar demikian pula sebaliknya.
4. *Behavior Control* (kendali terhadap perlakuan):
   Firewall berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya: sistem pengecekan dan menyaring *email* yang berbentuk *spam*.

Dalam membangun sebuah jaringan diperlukan langkah-langkah yang tepat untuk membangun firewall. Langkah-langkah tersebut antara lain :

1. Mengidentifikasi bentuk jaringan yang dimiliki, dengan mengetahui bentuk jaringan yang dimiliki, khususnya topologi yang akan digunakan dan protokol jaringannya akan memudahkan mendesain sebuah firewall.
2. Menentukan kebijakan merupakan hal yang harus dilakukan pada saat sebuah firewall akan diterapkan yang meliputi :
   a. Menentukan apa saja yang perlu dilayani.
   b. Menentukan individu atau kelompok mana yang akan dikenai kebijakan tersebut.

c. Menentukan layanan yang dibutuhkan oleh setiap individu atau kelompok yang menggunakan jaringan.
d. Berdasarkan penentuan layanan tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuat firewall tersebut aman.
e. Menerapkan kebijakan tersebut.

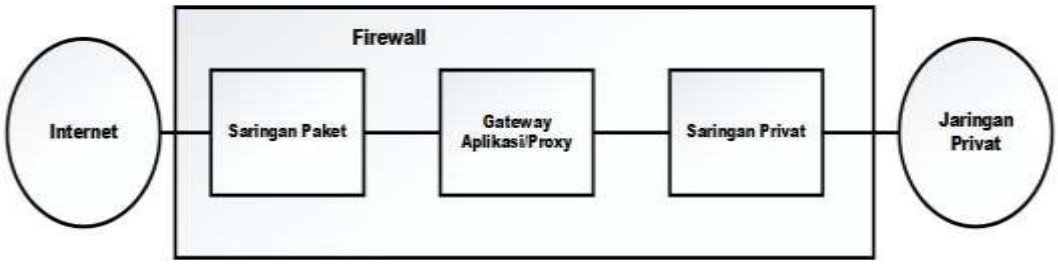
3. Menyiapkan *software* maupun *hardware* yang akan mendukung seperti *ip chains*, *iptables* dan sebagainya.
4. Melakukan tes konfigurasi dimana penguji terhadap firewall yang telah dibuat untuk mengetahui bagaimana hasil yang diperoleh setelah dibuatnya firewall tersebut.

Ada empat jenis firewall antara lain :

1. *Packet Filtering* : Firewall jenis ini menyaring paket data berdasarkan alamat dan opsi-opsi yang sudah ditentukan untuk paket tersebut dan bekerja dalam level IP paket data dan membuat keputusan mengenai tindakan selanjutnya (diteruskan atau tidak diteruskan) berdasarkan kondisi dari paket tersebut.
2. *Circuit Gateways:* Firewall jenis ini bekerja pada *layer transport* pada jaringan, dimana koneksi diautorisasi berdasarkan alamat. Seperti halnya *Packet Filtering*, *Circuit Gateways* biasanya tidak dapat memonitor trafik data yang mengalir antara satu jaringan dengan jaringan yang lain.
3. *Application Gateways:* Firewall tipe ini juga disebut sebagai firewall berbasis *proxy*. Beroperasi pada level aplikasi dan dapat mempelajari informasi pada level data aplikasi seperti perintah FTP atau URL yang diakses lewat HTTP.
4. *Hybrid Firewall:* Firewall jenis ini menggunakan elemen-elemen dari satu atau lebih tipe firewall. Sistem *hybrid* ini seringkali digunakan untuk menambahkan layanan baru secara cepat pada sistem firewall yang sudah tersedia.

Sebuah firewall berfungsi mencegat dan mengontrol trafik antar jaringan dengan tingkat kepercayaan (*level of trust*) yang berbeda-beda. Dalam difinisi Chesswick dan Bellovin, ia menyediakan sebuah jejak yang dapat ditelusuri. Firewall merupakan tempat yang cocok untuk mendukung autentikasi pengguna yang kuat sebaik komunikasi *privat*e antara dua firewall. Firewall juga merupakan tempat yang tepat untuk memfokuskan keputusan tentang ancaman dan untuk menjalankan aturan keamanan. Firewall dapat mencatat aktifitas *internet*work dan membatasi wilayah cakupan dari sebuah organisasi.

Firewall dapat memeriksa *header* paket untuk menentukan layanan IP, atau layanan lainnya dari lapisan OSI yang lebih tinggi, yang dibawa oleh paket. Apabila penyaringan tipe ini dipadukan dengan penyaringan pada lapisan *network*, pengaman yang diberikan firewall akan jauh lebih handal. Sebagai contoh, pada sebuah *server gateway*, *e-mail*, *firewall* dapat dikonfigurasikan untuk menolak semua paket yang datang ke *gateway*, terkecuali yang diminta dan dibutuhkan oleh software *gateway*. Sehingga *traffic* selain *e-mail* tidak akan memasuki jaringan *private* via gateway *e-mail* Firewall yang menjalankan fungsi penyaringan pada lapisan-lapisan OSI bagian atas terkadang disebut sebagai *gateway*. Konsep Firewall dengan fungsi penyaringan paket dan aplikasi dapat dilihat pada gambar 2.22 [5].



Gambar 2.22 Firewall dengan fungsi penyaringan paket dan aplikasi [5].

2.22 *Voucher*

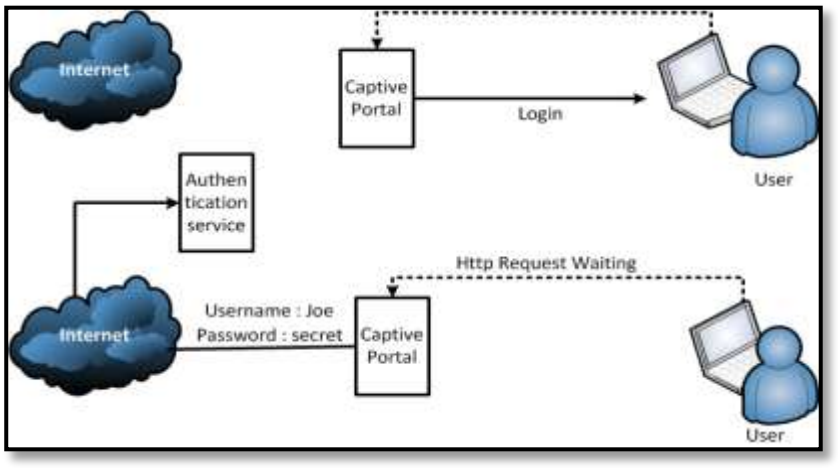
Voucher adalah pencatatan, metode dan prosedur tertentu yang dibuat untuk pengawasan pembayaran-pembayaran atau pengeluaran-pengeluaran uang. Dalam artian umum *voucher* berarti suatu dokumen yang berfungsi sebagai bukti pengesahan atau otorisasi pembayaran, seperti misalnya faktur yang telah disetujui untuk dibayar ataupun dokumen sebagai bukti atas pembayaran yang telah dilakukan, istilah *voucher* disini mempunyai arti yang sempit yaitu *voucher* berarti formulir khusus untuk mencatat data yang relevan mengenai suatu kewajiban dan rincian pembayarannya [15].

2.23 *Captive Portal*

Captive portal merupakan suatu teknik autentikasi dan pengamanan data yang lewat dari *network* internal ke *network* eksternal. *Captive portal* sebenarnya merupakan mesin router atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik, sampai *user* melakukan *registrasi* terlebih dahulu kedalam sistem. Secara umum *captive portal* memiliki fungsi untuk mencegah atau memblokir koneksi yang tidak diinginkan dan mengarahkan *client* ke protokol tertentu (*client* tidak terdaftar) [5].

Pada saat seorang pengguna berusaha untuk melakukan *browsing* ke *internet*, *captive portal* akan memaksa pengguna yang belum terauthentikasi untuk menuju ke *authentication web* dan akan diberi *form login* termasuk informasi tentang hotspot yang sedang digunakan. Berikut adalah cara kerja *captive portal* [5].

1. User dengan *wireless client* diizinkan untuk terhubung *wireless* untuk mendapatkan IP *address* (DHCP).
2. *Block* semua *traffick* kecuali yang menuju ke *captive portal* (*registrasi*/otentikasi berbasis *web*) yang terletak pada jaringan.
3. *Redirect* atau belokkan semua *traffick web* ke *captive portal*.
4. Setelah *user* melakukan *registrasi* atau *login*, izinkan akses ke jaringan *internet*.



Gambar 2.23 Cara kerja *Captive Portal* [5].

Pada proses autentikasi dengan menggunakan teknik *captive portal* pengguna yang belum terdaftar atau tidak memiliki hak akses tidak dapat terhubung dan mengakses layanan Hotspot CyberCity Networks. *Captive portal* akan melakukan *redirecting* pengguna yang belum terdaftar ke halaman autentikasi ketika pengguna melakukan akses ke jaringan internet dengan menggunakan *web browser*.

2.24 Sejarah Mikrotik RouterOS™

Mikrotik adalah sebuah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentuknya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang berkewarganegaraan Amerika yang berimigrasi ke Latvia. Di Latvia ia berjumpa dengan Arnis, seorang sarjana Fisika dan Mekanik sekitar tahun 1995.

John dan Anis mulai me-*routing* dunia pada tahun 1996 (misi Mikrotik adalah me-*routing* seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi *Wireless-LAN* (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangga Latvia, baru kemudian melayani lima pelanggannya di Latvia.

Prinsip dasar mereka bukan membuat *Wireless* ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilangka yang melayani sekitar 400 pengguna.

Linux yang pertama kali digunakan adalah kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staff Research and Development (R&D) Mikrotik yang sekarang menguasai dunia routing dinegara-negara berkembang. Menurut Arnis, selain staf di lingkungan Mikrotik, mereka juga merekrut tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan Mikrotik secara marathon [5].

2.24.1 Pengertian Mikrotik RouterOS™

Mikrotik RouterOS™ adalah sistem operasi yang dirancang khusus untuk *network* router. Dengan sistem operasi ini, kita dapat membuat router dari komputer rumahan (PC). Mikrotik RouterOS™ inipun dapat melakukan hampir semua fungsi *networking* dan beberapa fungsi *server* [5].

Keunggulan Mikrotik RouterOS™ ini antara lain:

1. Membuat PC yang murah menjadi sebuah router yang handal.
2. Pembaharuan versi secara berkala.
3. Memiliki banyak fitur.
4. Memiliki *user interface* yang mudah dan konsisten.
5. Ada banyak cara untuk mengakses dan mengontrol.
6. Instalasi cepat dan mudah.
7. Memungkinkan *upgrade hardware*.
8. Alternatif *interface* yang dapat digunakan cukup banyak.

2.24.2 Fitur-Fitur Mikrotik

1. Address List : Pengelompokan IP Address berdasarkan nama.
2. Asynchronous : Mendukung serial PPP *dial-in* / *dial-out*, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, *Radius, dial on demand*, modem pool hingga 128 ports.
3. Bonding : Mendukung dalam pengkombinasian beberapa antarmuka *ethernet* ke dalam 1 pipa pada koneksi cepat.
4. Bridge : Mendukung fungsi *bridge spining tree, multiple bridge interface, bridging firewalling*.
5. Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar *peer to peer*.
6. DHCP : Mendukung DHCP tiap antarmuka, *DHCP Relay, DHCP Client, multiple network DHCP, static and dynamic DHCP leases*.
7. Firewall dan NAT : Mendukung pemfilteran koneksi *peer to peer, source NAT* dan *destination NAT*. Mampu memfilter berdasarkan MAC, IP Address, *range port*, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. Hotspot : *Hotspot gateway* dengan otentikasi RADIUS. Mendukung limit data rate, SSL, dan HTTPS.
9. IPSec : Protokol AH dan ESP untuk IPSec, MODP Deffie-Hellmann groups 1, 2, 5, MD5 dan algoritma SHA1 hashing, algoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-256, *Perfect Forwarding Secresy (PFS)* MODP groups 1,2,5.
10. ISDN : Mendukung ISDN *dial-in*/*dial-out*. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
11. M3P : MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
12. MNDP : *MikroTik Discovery Neighbour Protokol*, juga mendukung *Cisco Discovery Protokol* (CDP).

13. Monitoring / *Accounting* : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
14. NTP : Network Time Protokol untuk *server* dan *clients*, sinkronisasi menggunakan system GPS.
15. *Point to Point Tunneling Protocol* : PPTP, PPPoE dan L2TP *Access Consentrator*; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2, otentikasi dan laporan Radius, enkripsi MPPE, kompresi untuk PPoE, limit data rate.
16. Proxy : Cache untuk FTP dan HTTP *proxy server*, HTTPS *proxy*, *transparent proxy* untuk DNS dan HTTP, mendukung protokol SOCKS, mendukung *parent proxy*, *static* DNS.
17. Routing : Routing statik dan dinamik, RIP v1/v2, OSPF v2, BGP v4.
18. SDSL : Mendukung *Single Line DSL*, mode pemutusan jalur koneksi dan jaringan.
19. Simple Tunnel : *Tunnel IPIP dan EoIP* (*Ethernet over IP*).
20. SNMP : *Simple Network Monitoring Protocol* mode akses *read-only*.
21. Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media ttypes, sync-PPP, Cisco HDLC, *Frame Relay line protokol*, ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A), Frame Relay jenis LMI.
22. Tool : *Ping*, *Traceroute*, *bandwidth test*, *ping flood, telnet, SSH, packet sniffer*, Dinamik DNS *update*.
23. UpnP : Mendukung antarmuka *Universal Plug and Play*.
24. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan *ethernet* dan *wireless*, *multiple* VLAN, VLAN *bridging*.
25. VoIP : Mendukung aplikasi *voice over IP*.
26. VRRP : Mendukung *Virtual Router Redudant Protocol*.
27. Winbox : Aplikasi mode GUI untuk me*remote* dan mengkonfigurasi Mikrotik RouterOS.

2.25 API (*Application Programming Interface*)

Application Programming Interface adalah kumpulan fungsi atau kumpulan kode program yang berfungsi mengkomunikasikan sebuah program dengan *kernel* dari sebuah sistem operasi. API mikrotik adalah kumpulan fungsi, layanan/ *service* yang digunakan untuk mengkomunikasikan data yang ada pada Mikrotik RouterOS^{TM} untuk dapat dihubungkan menggunakan aplikasi bahasa pemrograman tertentu untuk menyimpan data maupun digunakan untuk mengakses mikrotik itu sendiri. Cara menggunakan API adalah dengan cara mengimpor *package*/ *class import* yang ada dan mengaktifkan *service* API pada mikrotik [5].

2.26 PHP (*Hypertext Preprocessor*)

PHP adalah bahasa pemrograman *server-side* yang bersifat *open source.* PHP merupakan bahasa permrograman yang bersifat dinamis karena halaman yang akan ditampilkan dibuat saat halaman itu diminta oleh *user*. Mekanisme ini menyebabkan informasi yang diterima user selalu yang terbaru (*up to date*). PHP merupakan *script* yang dapat terintegrasi dengan HTML (*Hypertext Markup Language*) [7].

2.27 CSS *(Cascading Style Sheet)*

Cascading Style Sheet (CSS) merupakan salah satu bahasa pemrograman web untuk mengendalikan beberapa komponen dalam sebuah *web* sehingga akan lebih terstruktur dan seragam.

Sama halnya *styles* dalam aplikasi pengolahan kata seperti Microsoft Word yang dapat mengatur beberapa *style*, misalnya *heading*, subbab, *bodytext*, *footer*, *images*, dan *style* lainnya untuk dapat digunakan bersama-sama dalam beberapa berkas (file). Pada umumnya CSS dipakai untuk memformat tampilan halaman *web* yang dibuat dengan bahasa HTML.

CSS dapat mengendalikan ukuran gambar, warna bagian tubuh pada teks, warna tabel, ukuran border, warna border, warna *hyperlink*, warna mouse over,

spasi antar paragraf, spasi antar teks, margin kiri, kanan, atas, bawah, dan parameter lainnya. CSS adalah bahasa *style sheet* yang digunakan untuk mengatur tampilan dokumen. Dengan adanya CSS memungkinkan kita untuk menampilkan halaman yang sama dengan format yang berbeda [7].

2.28 API PHP *Class*

API PHP *class* merupakan sebuah *class scripting* PHP yang dirancang oleh pihak Developer Mikrotik untuk menghubungkan antara PHP dengan Mikrotik Router. Melalui *Script* PHP *class* ini PHP dapat bekerja untuk mengakses dan mengeksekusi berbagai perintah Router Mikrotik. Salah satunya menambahkan, mengedit maupun menghapus user hotspot. PHP *class* ini bersifat sebagai penghubung antara PHP dengan Mikrotik, untuk melakukan *explorasi scripting* sepenuhnya [11].

2.29 MySQL

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL atau yang dikenal dengan DBMS (*database management system*), *database* ini *multithread*, multi-user. Kekuatan MySQL tidak ditopang oleh sebuah komunitas, seperti Apache, yang dikembangkan oleh komunitas umum, dan hak cipta untuk kode sumber dimiliki oleh pemilik masing-masing, tetapi MySQL didukung penuh oleh sebuah perusahaan profesional dan komersil, yakni MySQL AB dari swedia.

MySQL sebenarnya merupakan turunan salah satu konsep utama dalam *database* sejak lama, yaitu SQL (*Structured Query Languange*). Sebagai *database server*, MySQL dapat dikatakan lebih unggul dibandingkan *database server* lainnya, terutama dalam kecepatan [7].

Berikut ini beberapa keistimewaan MySQL, antara lain :

a. *Portability*

   MyAQL dapat berjalan stabil pada berbagai sistem operasi *Windows. Linux, FreeBSD, Mac Os X Server, Solaris, Amiga,* dan masih banyak lagi.

b. *Multi User*

MySQL dapat digunakan beberapa user dalam waktu yang bersamaan tanpa mengalami masalah atau konflik.

c. *Security*

MySQL memiliki beberapa lapisan sekuritas seperti *level subnetmask*, nama *host*, dan ijin akses user dengan sistem perizinan yang mendetail serta *password* terenkripsi.

d. *Scalability dab Limits*

MySQL mampu menangani database dalam skala besar, dengan jumlah *record* lebih dari 50 juta dan 60 ribu tabel serta 5,7 milyar baris. Selain itu batas *indeks* yang dapat ditampung mencapai 32 *indeks* pada tiap tabelnya.

2.30 Gateway

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda [1].

2.31 Perangkat Pemodelan Berorientasi Objek (*Object Oriented*)

Perangkat pemodelan adalah suatu strategi pembangunan perangkat lunak yang mengorganisasikan perangkat lunak sebagai kumpulan objek yang berisi data dan operasi yang diberlakukan terhadapnya. Metodologi berorientasi objek merupakan suatu cara bagaimana sistem perangkat lunak dibangun melalui pendekatan objek secara sistematis. Metode berorientasi objek didasarkan pada penerapan prinsip-prinsip pengelolaan kompleksitas. Metode berorientasi objek meliputi rangkaian aktivitas analisis berorientasi objek, perancangan berorientasi objek, pemrogramman berorientasi objek, dan pengujian berorientasi objek [6].

Perangkat analisis berorientasi objek (*object oriented*) antara lain :

1. *Unified Modelling Language* (UML)

UML (*Unified Modeling Language*) merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks –teks pendukung untuk menspesifikasikan, menggambarkan, membangun, dan dokumentasi dari sistem perangkat lunak. Tujuan UML adalah :

a. Memberikan model yang siap pakai, bahasa pemodelan visual yang ekspresif untuk mengembangkan dan saling menukar model dengan mudah dan dimengerti secara umum.
b. Memberikan bahasa pemodelan yang bebas dari berbagai bahasa pemrograman dan proses rekayasa.
c. Menyatukan praktik-praktik terbaik yang terdapat dalam pemodelan UML menyediakan beberapa *notasi dan artifact standar* yang bisa digunakan sebagai alat komunikasi bagi para pelaku dalam proses analisis dan desain. Artifact didalam UML didefinisikan sebagai informasi dalam bentuk yang digunakan atau dihasilkan dalam proses pengembangan perangkat. Contohnya adalah *source code* yang dihasilkan oleh proses pemrograman.

2. *Use Case Diagram*

Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Yang ditekankan adalah "apa" yang diperbuat sistem, dan bukan "bagaimana". *Use Case* dilakukan oleh satu *actor* yang digambarkan dengan simbol orang yang dihubungkan dengan garis yang menunjukan hubungan komunikasi. Setiap *Use Case* harus diberi nama yang menyatakan apa hal yang dicapai dari hasil interaksi dengan *Actor.* Nama *Use Case* boleh terdiri dari beberapa kata dan tidak boleh ada *Use Case* yang memiliki nama yang sama [6].

3. *Class Diagram*

Diagram kelas menggambarkan tipe-tipe objek dalam *system* dan berbagai jenis hubungan atau relasi statis yang ada diantara mereka. Diagram ini memberikan gambaran umum dari sistem. Seperti tipe-tipe dari objek dengan menunjukan kelasnya dan *relationship* yang diantara mereka, serat penjelasan detail tiap-tiap kelas ke dalam model suatu *system. Class diagram* bersifat *static*

(tidak berubah) yang akan menunjukan apa itu interaksi tapi tidak menjelaskan apa yang terjadi ketika mereka melakukan interaksi [6].

4. *Activity Diagram*

Activity diagram memodelkan alur kerja *(work flow).* Sebuah proses bisnis dan urutan aktifitas dalam suatu proses. Diagram ini sangat mirip dengan sebuah *flowchart* karena kita dapat memodelkan sebuah alur kerja dari aktifitas keaktifitas lainnya atau dari suatu aktifitas kedalam keadaan sesaat (*state)* [6].

5. *Squence Diagram*

Diagram sequence merupakan gambaran interaksi antar objek di dalam dan di sekitar sistem berupa *massage* yang digambarkan terhadap waktu. Diagram ini secara khusus berasosiasi dengan *use Case. Diagram sequence* juga digunakan untuk menggambarkan skenario atau rangkain langkah-langkah apa yang seharusnya terjadi sebagai respons dari sebuah *event* untuk menghasilkan sesuatu didalam *Use case* sebagai *output.* Untuk *massage* digambarkan sebagai garis berpanah dari satu objek ke objek lainnya. Pada fase desain berikutnya, *message* dipetakan menjadi operasi/metode dari *class. Activation bar* menunjukan lamanya eksekusi sebuat proses, biasanya diawali dengan sebuah *message*. Berikut ini adalah contoh dari *diagram sequence* [6].

6. *Deployment Diagram*

Diagram *deployment* atau *deployment diagram* menunjukan konfigurasi komponen dalam proses eksekusi aplikasi. Diagram *deployment* juga dapat digumakan untuk memodelkan hal-hal berikut.

1. Sistem tambahan (*embedded system*) yang menggambarkan rancangan *device*, *node*, dan *hardware*.
2. Sistem *client*/*server*
3. Sistem terdistribusi murni
4. Rekayasa ulang aplikasi

2.32 Kuesioner

Kuesioner terdiri dari sejumlah pertanyaan dicetak atau diketik dalam urutan yang pasti di formulir atau set bentuk. Kuesioner dikirimkan kepada responden yang diharapkan untuk membaca dan memahami pertanyaan dan menulis jawaban dimaksudkan dalam kuesioner itu sendiri. Sebagai bentuk umum dari kuesioner itu dapat dibagi menjadi kuesioner terbuka dan tertutup.

a. Kuesioner terbuka adalah pertanyaan dari suatu kuesioner yang memberikan kebebasan penuh kepada responden untuk menjawabnya dan tidak ada jawaban alternatif.
b. Kuesioner tertutup adalah kuesioner yang memberikan jawaban alternatif yang telah ditentukan oleh pembuat kuesioner. Pertanyaan disajikan dengan tepat dan kata-kata yang sama dalam urutan yang sama untuk semua responden.

2.33 Skala Data yang digunakan

Skala data yang digunakan untuk pengukuran variabel independen adalah skala *likert*. Skala *likert* adalah skala yang digunakan untuk mengukur sikap pendapat dan persepsi seseorang atau sekelompok orang tentang fenomena sosial [16]. Dengan skala *likert*, maka variabel yang akan diatur dijabarkan menjadi indikator variabel. Kemudian indikator tersebut dijadikan sebagai titik tolak untuk menyusun *item-item* instrumen yang dapat berupa pernyataan atau pertanyaan. Data yang telah terkumpul melalui angket, kemudian diolah kedalam bentuk kuantitatif, yaitu dengan cara menetapkan skor jawaban yang dapat dilihat pada tabel 2.3.

Tabel 2.3 Penilaian Skala Likert

Alternatif	Skor
Sangat Setuju	5
Setuju	4
Ragu-Ragu	3
Tidak Setuju	2
Sangat Tidak Setuju	1

Kemudian dengan teknik pengumpulan data kuesioner, maka instrument tersebut misalnya diberikan kepada 30 orang yang diambil secara random. Dari 30 orang tersebut setelah dilakukan analisis misalnya:

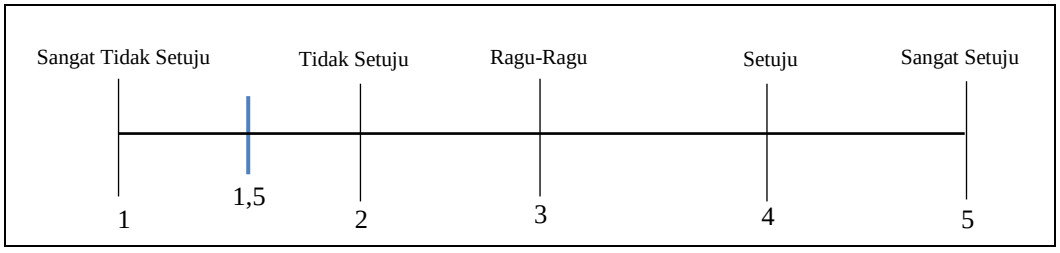
1. Sebanyak 16 orang menjawab Sangat Setuju (SS)
2. Sebanyak 5 orang menjawab Setuju (S)
3. Sebanyak 4 orang menjawab Ragu-Ragu (RR)
4. Sebanyak 3 orang menjawab Tidak Setuju (TS)
5. Sebanyak 2 orang menjawab Sangat Tidak Setuju (STS)

Data interval tersebut kemudian dianalisis dengan menghitung rata-rata jawaban berdasarkan skoring setiap jawaban dari responden. Berdasarkan skor yang telah ditetepkan dapat dihitung sebagai berikut:

Jumlah skor untuk 16 orang yang menjawab SS =16x5= 80
Jumlah skor untuk 5 orang yang menjawab S = 5 x5= 25
Jumlah skor untuk 4 orang yang menjawab RR = 4x5= 20
Jumlah skor untuk 3 orang yang menjawab TS = 3x5= 15
Jumlah skor untuk 2 orang yang menjawab STS = 2x5= 10

Jumlah Total Nilai = 150

Jumlah skor yang diperoleh dari penelitian adalah 150. Jadi berdasarkan data itu maka tingkat persetujuan yaitu jumlah total nilai dibagi jumlah responden = (150 : 100)= 1,5 secara kontinum dapat dilihat pada gambar 2.24.



Gambar 2.24 Pengolahan Hasil Kuesiner Secara Kontinum

Jadi berdasarkan data yang diperoleh dari 30 responden maka rata-rata 1,5 terletak pada daerah Tidak setuju.

2.34 Metode Pengujian Sistem

Metode pengujian sistem untuk mengetahui efektifitas dari *software* yang digunakan selain memberikan kesempatan kepada siswa untuk mengoprasikan dan melakukan pengecekan terhadap laporan yang dihasilkan melalui *software*. Metode pengujian sistem terdiri dari Pengujian *White-box* dan Pengujian *Black-box* [17].

2.34.1 Pengujian Black-Box

Pengujian yang dilakukan untuk antarmuka perangkat lunak, pengujian ini dilakukan untuk memperlihatkan bahwa fungsi-fungsi bekerja dengan baik dalam arti masukan yang diterima dengan benar dan keluaran yang dihasilkan benar-benar tepat, pengintegrasian dari eksternal data berjalan dengan baik.

Metode pengujian *black-box* memfokuskan pada requirement fungsi dari perangkat lunak, pengujian ini merupakan komplenetari dari pengujian *white-box*. Pengujian *white-box* dilakukan terlebih dahulu pada proses pengujian, sedangkan pengujian *black-box* dilakukan pada tahap akhir dari pegujian perangkat lunak. Proses yang terdapat dalam proses pengujian *black-box* yaitu analisis batasan nilai yang berlaku untuk setiap data [17].

2.35 Tools yang Digunakan

Tools yang digunakan untuk membangun aplikasi ini meliputi *Notepad ++* dan *XAMPP*.

2.35.1 Notepad ++

Notepad++ adalah sebuah *text editor* yang sangat berguna bagi setiap orang dan khususnya bagi para developer dalam membuat program. Notepad++ menggunakan komponen *Scintilla* untuk dapat menampilkan dan meyuntingan

teks dan berkas kode sumber berbagai bahasa pemrogramman yang berjalan diatas sistem operasi Microsoft Windows.

Selain manfaat dan kemampuannya menangani banyak bahasa pemrogramman, Notepad++ juga dilisensikan sebagai perangkat *free*. Jadi, setiap orang yang menggunakan tidak perlu mengeluarkan biaya untuk membeli aplikasi ini karena *sourceforge.net* sebagai layanan yang memfasilitasi Notepad++ membebaskannya untuk digunakan [10].

2.35.2 XAMPP

XAMPP adalah satu paket komplit web *server* yang mudah dipasang di berbagai sistem operasi. Dalam paketnya sudah terkandung Apache (*Web server*), MySQL (database), PHP (*server side scripting*), dan berbagai pustaka bantu lainnya. XAMPP tersedia untuk Linux, Windows, MacOS maupun Solaris sehingga sangat memudahkan membuat web *server multiplatform* [10].