BAB 2
TINJAUAN PUSTAKA

2.1. Profil Instansi

PT Blesslink Rema merupakan perusahaan jasa PCO (*Professional Congress Organizer*) yang berdiri sejak tahun 1992. PT. Blesslink Rema menyediakan jasa profesional dengan spektrum yang luas yang mencakup penyusunan perencanaan dan anggaran, persiapan tempat, izin kegiatan, kesekretariatan, akomodasi dan transportasi. Selain jasa PCO, PT. Blesslink juga menyediakan jasa profesional dalam bidang *Special Interest Tour, Tailored Made Tour*, dan *Party Organizer.*

2.1.1 Tempat dan Kedudukan

PT. Blesslink Rema

Kantor Pusat : Jl. Sunda No 50A, Bandung 40112

Kantor Cabang : Komp. Buncit Mas Blok B-10,
Jl. Mampang Prapatan Raya No. 108, Jakarta12670

2.1.2 Visi dan Misi

Visi dari PT. Blesslink Rema adalah menjadi salah satu perusahaan jasa PCO handal dan terkemuka di Indonesia.

Misi dari PT. Blesslink Rema adalah menyediakan jasa profesional dengan spektrum yang luas yang mencakup :

- Menyusun perencanaan dan anggaran
- Mempersiapkan tempat penyelenggaraan
- Mengurus izin kegiatan
- Menyelenggarakan kegiatan kesekretariatan mulai dari menjaring peserta sampai menyebarkan undangan dan mengkoordinasikan kegiatan promosi.

- Menyusun persiapan prapasca perjalan
- Mempersiapkan perangkat peragaan
- Mengatur akomodasi dan tranportasi peserta
- Mengurus kemudahaan bea, cukai, dan keimigrasian bagi alat-alat perangkat kongres dan pameran.
- Membantu peserta mengurus kelengkapan dokumen perjalanan sampai pada program-program lain yang mendukung kegiatan

2.1.3 Logo Instansi

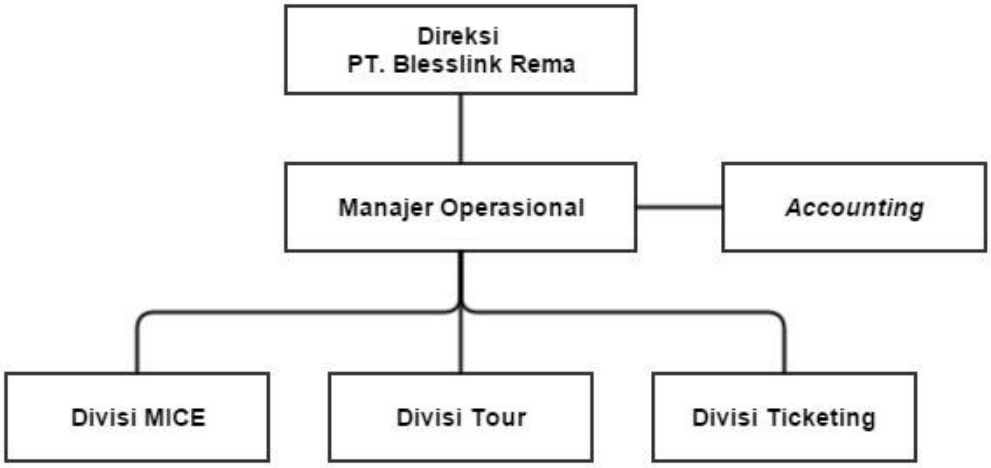
Berikut ini adalah logo dari PT. Blesslink Rema [3]



Gambar 1.1. Logo PT. Blesslink Rema

2.1.4 Struktur Organisasi

Berikut ini adalah struktur organisasi yang ada di PT. Blesslink Rema



Gambar 2.2. Struktur Organisasi

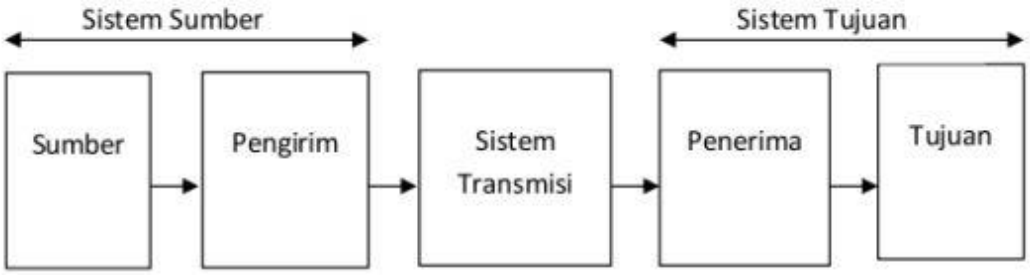
2.2. Komunikasi

Komunikasi berasal dari bahasa latin yaitu *communis* yang berbagai atau menjadi milik bersama. Komunikasi dapat diartikan sebagai proses penyampaian suatu pernyataan dari sumber kepada penerima.

2.2.1 Komunikasi Data

Komunikasi data adalah proses pengiriman dan penerimaan data atau informasi dari 2 buah *device* atau lebih yang terhubung kedalam sebuah jaringan komputer. Komunikasi data juga dapat diartikan sebagai proses menampilkan, mengubah, menginterpretasikan, atau mengolah informasi antara manusia dan mesin.

Proses komunikasi secara umum melibatkan beberapa elemen yaitu pengirim (*transmitter*), penerima (*receiver*) dan sebuah medium transmisi untuk tempat mengalirnya informasi [4]. Elemen-elemen tersebut dapat dilihat pada gambar 2.2.



Gambar 2.3. Sistem Komunikasi

Keterangan :

a. Sumber

   Membangkitkan data atau informasi yang akan ditransmisikan

b. Pengirim

   Data atau informasi yang dibangkitkan oleh sistem sumber tidak ditransmisikan langsung dalam bentuk aslinya. Sebuah *transmitter* cukup memindahkan dan menandai informasi dengan cara yang sama seperti menghasilkan sinyal-sinyal elektromagnetik yang dapat ditransmisikan melewati beberapa sistem transmisi berurutan.

c. Sistem transmisi

   Merupakan jalur transmisi tunggal (single transmission line) atau

   merupakan jaringan kompleks yang menghubungkan sumber dan tujuan.

d. Penerima

   Berfungsi menerima sinyal dari sistem transmisi dan menggabungkan ke

   dalam bentuk tertentu yang dapat ditangkap dan dimengerti oleh tujuan

   (*destination*)

e. Tujuan

   Menangkap data yang dihasilkan oleh receiver.

2.3. Jaringan Komputer

Jaringan komputer merupakan sekumpulan komputer yang saling terhubung dan dapat saling berkomunikasi dengan bertukar data atau informasi. Jaringan komputer pada dasarnya merupakan perpaduan teknologi komputer dan teknologi komunikasi [5].

2.3.1. Manfaat Jaringan Komputer

Perkembangan teknologi komputer saat ini berkembang sangat cepat.

Banyak sekali manfaat yang dapat diperoleh dalam suatu jaringan komputer. Manfaat-manfaat tersebut diantaranya adalah :

a. Jaringan komputer memungkinkan seseorang untuk mengakses file yang dimilikinya atau file orang lain yang telah diizinkan untuk diakses dimanapun dan kapanpun.
b. Jaringan komputer memungkinkan proses pengiriman data berlangsung cepat dan efisien.
c. Jaringan komputer memungkinkan adanya sharing *hardware* antar client.
d. Jaringan komputer memungkinkan seseorang berhubungan dengan orang lain di berbagai negara dengan komunikasi lewat teks, gambar, audio, dan video secara real-time.
e. Jaringan komputer dapat menekan biaya operasional seperti pemakaian kertas, pengiriman surat atau berkas, telepon, serta pembelian *hardware*.

2.3.2. Klasifikasi Jaringan Komputer

Pembagian klasifikasi jaringan komputer dibagi menjadi berdasarkan skala, metode koneksi, hubungan fungsional (Arsitektur Jaringan), dan topologi jaringan [5]

2.3.2.1. Berdasarkan Skala

a. ***Local Area Network*** (LAN)

LAN biasanya diterapakan pada suatu gedung dalam suatu komplek perkantoran atau sekolah. LAN adalah jaringan yang dibatasi oleh area kecil, umumnya dibatasi oleh area lingkungan seperti sekolah dan biasanya tak lebih dari 1 KM^2 (Kilo Meter Persegi). Kecepatan akses LAN dimulai dari 1 Mbps hingga 1 Gbps

b. ***Metropolitan Area Network*** (MAN)

MAN merupakan suatu jaringan yang cakupannya meliputi suatu kota. MAN menghubungkan LAN-LAN yang lokasinya berjauhan. Jangkauan MAN bisa mencapai 10 km sampai ratusan kilometer. Kecepatan akses MAN mulai dari 1 Mbps hingga 1 Gbps.

c. ***Wide Area Network*** (WAN)

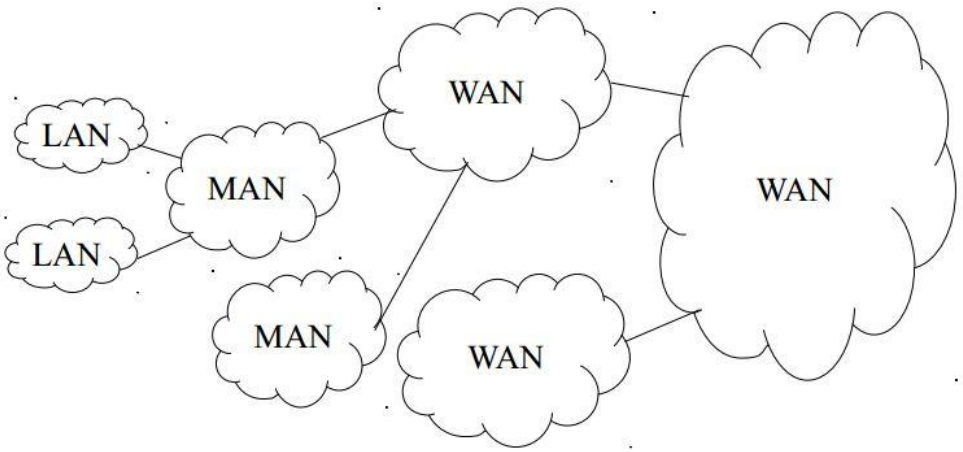
WAN dirancang untuk menghubungkan komputer-komputer yang terletak

pada suatu cakupan geografis yang lebih luas dari MAN, seperti hubungan dari satu kota ke kota yang lain di dalam suatu negara. Cakupan WAN bisa meliputi 100 km sampai 1.000 km bahkan lebih. Kecepatan akses WAN sangar bervariasi mulai dari 1 sampai 100 Gbps.

b. ***Global Area Network*** (GAN)

GAN merupakan gabungan dari WAN dalam suatu negara dan menghubungkannya dengan WAN dari negara lain sehingga banyak negara dapat terhubung kedalam jaringan komputer global. Kecepatan akses GAN bervariasi mulai dari 1 hingga 100 Gbps.

Perbedaan LAN, MAN, WAN dan GAN bisa dilihat pada gambar 2.3



Gambar 2.4. Interaksi antara LAN, MAN, WAN dan GAN

2.3.2.2. Berdasarkan Media Transmisi

Secara global metode koneksi pada jaringan dibagi dua menjadi wired dan *wireless*

2.3.2.2.1. *Wired* (Kabel)

Metode koneksi ini memerlukan kabel sebagai penghubung komunikasi. Jenis kabel yang biasa dipakai adalah Fiber Optic, Coaxial STP, dan UTP [4]

a. Fiber Optic

Kabel Fiber optic mempunyai kemampuan mentransmisi sinyal melalui jarak yang relatif jauh dan mempunyai kecepatan yang baik dari pada kabel coaxial ataupun kabel lainnya. Kabel ini sangat baik digunakan untuk fasilitas konferensi radio atau layanan interaktif.



Gambar 2.5. Kabel Fiber Optik

b. Coaxial

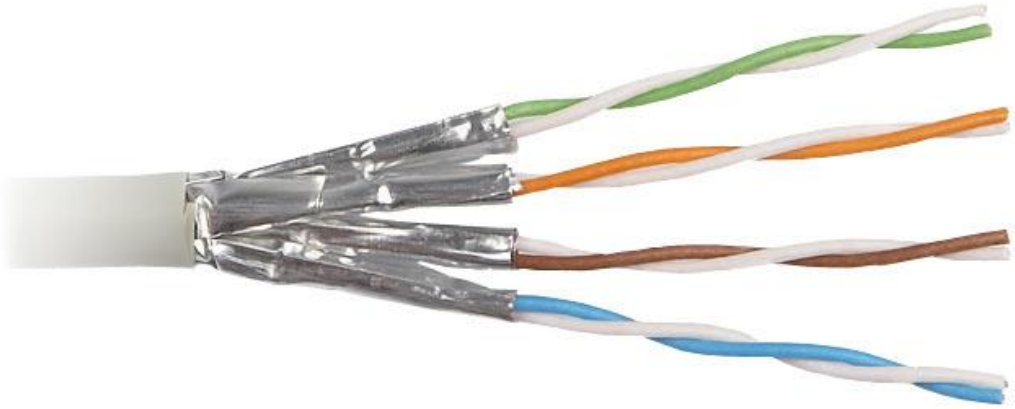
Kabel coaxial adalah kabel yang memiliki satu copper conductordi bagian tengahnya. Sebuah lapisan plastik menutupi diantara konduktor dan lapisan pengaman serat besi. Lapisan serat besi tersebut membantu menutupi gangguan dari arus listrik, lalu lintas kendaraan atau mesin, dan komputer. Tipe konektor untuk kabel jenis ini adalah konektor *Bayone-Neill-Concelman* (BNC).



Gambar 2.6. Kabel Coaxial

c. STP (*Shielded Twisted Pair*)

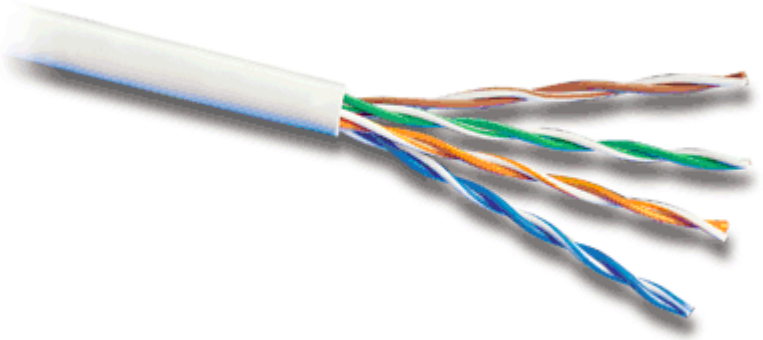
Tipe kabel STP memiliki pelindung yang melindungi data transmisi dari induksi magnetis dari lingkungan sekitar. Selain itu pelindung dari STP ini juga berfungsi untuk mencegah keboran transmisi data. Kabel ini relatif lebih mahal daripada UTP namun cenderung lebih cocok digunakan di luar ruangan.



Gambar 2.7. Kabel STP

d. UTP (*Unshielded Twisted Pair*)

Berbeda dengan STP, kabel UTP tidak memiliki pelindung didalamnya ini menyebabkan kabel UTP lebih flexibel untuk di atur dan sangat cocok digunakan didalam ruangan. Kabel ini relatif lebih murah namun rawan terjadi induksi magnetis dan kebocoran transmisi.



Gambar 2.8. Kabel UTP

2.3.2.2.2. Wireless (Nirkabel)

Metode koneksi ini tidak memerlukan kabel sebagai penghubung tapi menggunakan gelombang elektromagnetik seperti infra red, bluetooth, dan wifi

a. Infra red

Infra red merupakan salah satu media transmisi nirkabel yang memanfaatkan gelombang rendah (infra) untuk mentransmisikan data. Dalam penggunaannya transmitter harus secara langsung (direct) mengarah pada reciever tanpa ada penghalangan karena sifat dari infra red yang tak dapat menembus materi selain itu rentang jarak infra red kurang dari 4 meter. Infra red dapat mentransmisikan data hingga 4 Mbps.

b. Bluetooth

Bluetooth merupakan sebuah teknologi yang mampu mentransmisikan data secara nirkabel dengan gelombang radio. Berbeda dengan infra red, bluetooth yang memiliki sifat omni (menyebar kesagala arah) tidak mengharuskan mengarahkan transmitter dan receiver secara langsung dalam penggunaannya. Cakupan area bluetooh sampai 10 meter. Bluetooth sendiri memiliki kecepatan tranfer data hingga 10 Mbps

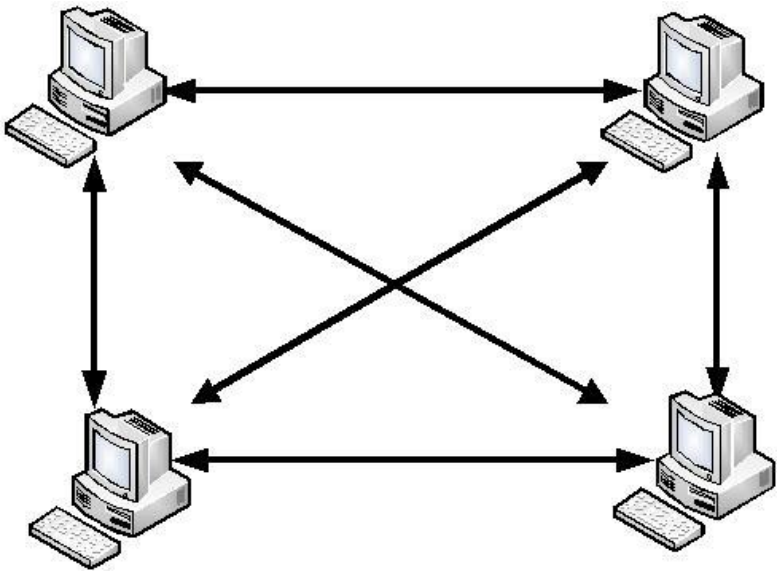
c. Wifi

Wifi atau wireless fidelity adalah sebuah teknologi yang memanfaatkan gelombang radio sebagai perantara untuk dapat bertukar data. Teknologi wifi yang dapat mentransfer data tanpa memerlukan kabel sebagai perantara (Nirkabel) membuat teknologi ini banyak digunakan di banyak tempat dimana pengguna mesti tetap selalu terkoneksi meski memiliki mobilitas yang tinggi.

2.3.2.2.3. Berdasarkan Arsitektur Jaringan

a. *Peer to Peer*

Peer to peer merupakan sebuah model hubungan pada jaringan komputer dengan membagi sumber daya yang ada dikomputer baik berupa file atau layananan printer dan lain lain. Dengan model hubungan ini komputer akan saling terhubung satu sama lain secara langsung seperti pada gambar 2.8. Model hubungan ini cocok untuk jaringan skala kecil karena tidak memerlukan server serta konfigurasi yang relatif mudah

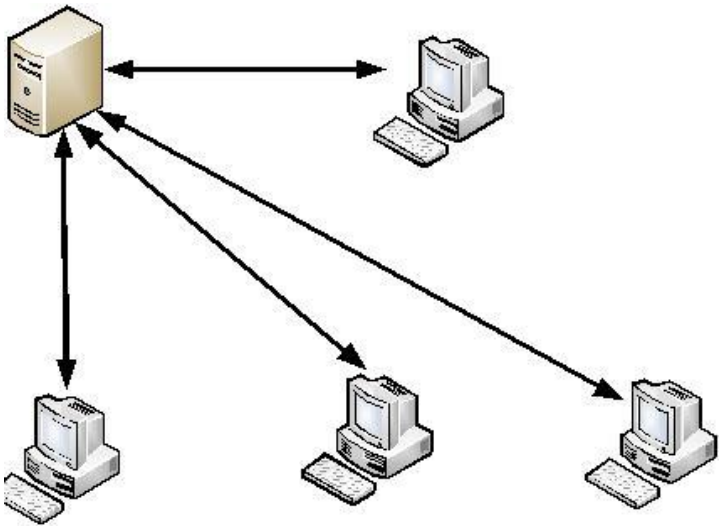


Gambar 2.9. *Peer to peer*

b. *Client-Server*

Berbeda dengan model *peer to peer,* model hubungan *Client-server* merupakan sebuah model jaringan komputer terpusat dimana ada sebuah komputer yang bertindak sebagai *server* (pusat) dan terhubungan dengan beberapa komputer lainnya yang bertindak sebagai *client* gambar 2.9. Dengan model jaringan komputer *client-server*

seluruh aktifitas komunikasi data akan terpantau di server sehingga keamanannya jauh lebih terjamin. Selain itu *client-server* juga memungkinkan pengguna untuk menggunakan sebuah aplikasi di server yang digunakan secara bersamaan seperti *file server, mail-server, web server,* dan *database server*



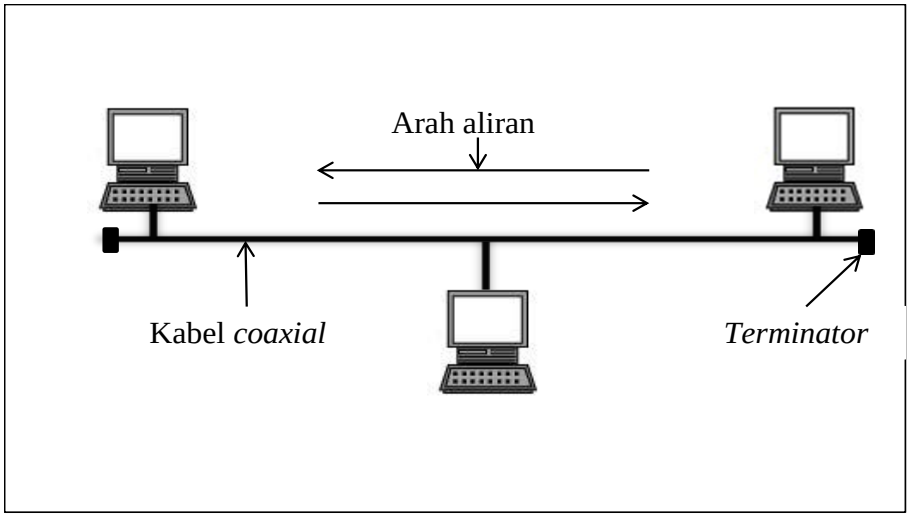
Gambar 2.10. *Client Server*

2.3.2.2.4. Berdasarkan Topologi Jaringan

Berdasarkan topologi jaringan, jaringan komputer dibagi menjadi 4 macam yaitu :

a. Topologi Bus

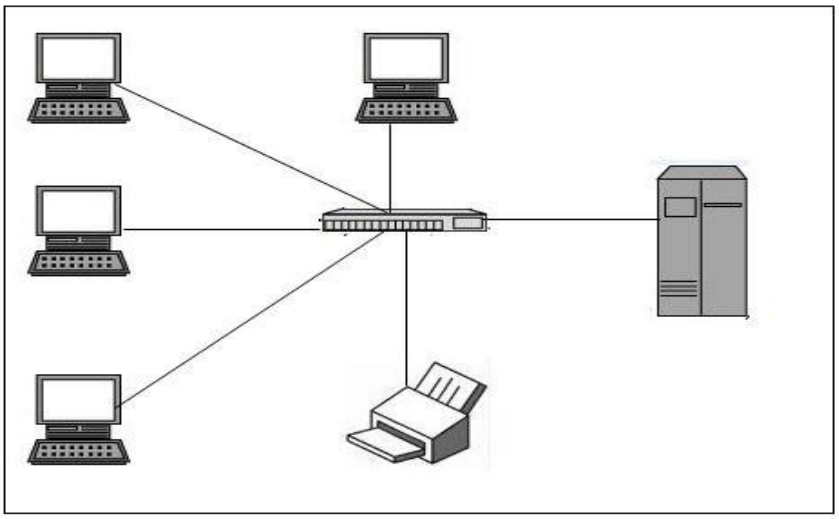
Pada topologi ini jaringan terdiri hanya dari satu saluran (kabel utama) yang menghubungkan beberapa komputer. Pada kedua ujung jaringan diakhiri dengan sebuah terminator (gambar 2.10.). Apabila kabel utama terputus akan menyebabkan jaringan mati total, karena kabel backbone (kabel utama) merupakan satu-satunya jalan bagi lalu lintas data.



Gambar 2.11. Topologi Bus

b. Topologi Star

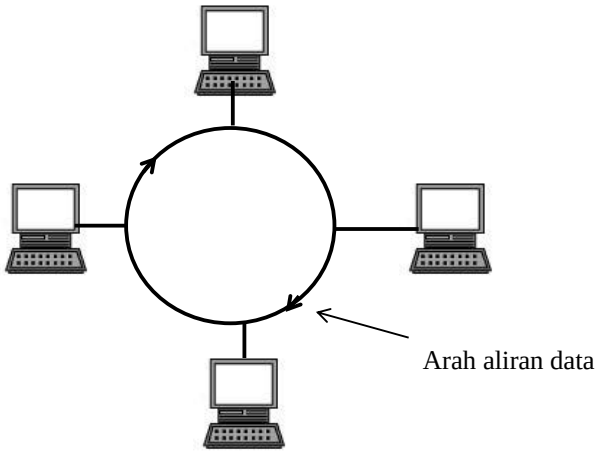
Pada topologi Star ini setiap node berkomunikasi langsung dengan konsentrator kemudian disebarkan keseluruh node yang terhubung (gambar 2.11.). Jika salah satu node atau salah satu kabel teminal rusak, maka jaringan masih tetap dapat berkomunikasi.



Gambar 2.12. Topologi Star

c. Topologi Ring

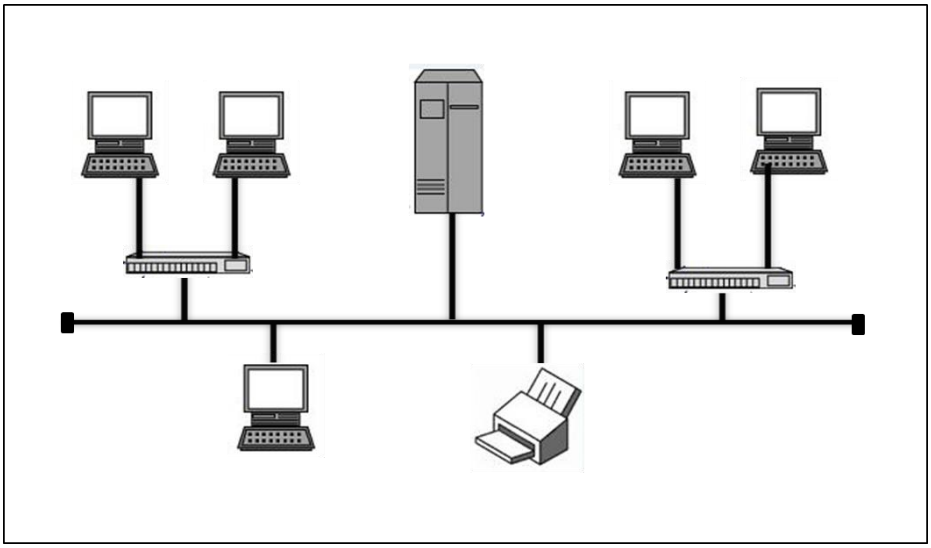
Topologi ring menggunakan kabel backbone (kabel utama) yang berbentuk cincin. Setiap komputer terhubung dengan kabel backbone, pada ujung kabel akan dihubungkan kembali dengan komputer pertama (gambar 2.12).



Gambar 2.13. Topologi Ring

d. Topologi Tree

Topologi tree disebut juga sebagai topologi star-bus, topologi ini merupakan penggabungan antara topologi star dan bus. Topologi tree digunakan untuk menghubungkan beberapa LAN dengan LAN lain. Media penghubung antar LAN yaitu menggunakan hub, masing-masing hub merupakan akar dari masing-masing pohon. Topologi ini dapat mengatasi permasalahan pada topologi bus yaitu masalah broadcast traffic, dan permasalahan pada topologi star yaitu keterbatasan kapasitas port hub



Gambar 2.14. Topologi Tree

2.4. Model Referensi OSI

Untuk menyelenggarakan komunikasi berbagai macam vendor komputer diperlukan sebuah aturan baku yang standar dan disetejui berbagai pihak. Seperti halnya dua orang yang berlainan bangsa, maka untuk berkomunikasi memerlukan penerjemah/interpreter atau satu bahasa yang dimengerti kedua belah pihak. Dalam dunia komputer dan telekomunikasi interpreter identik dengan protokol.

Untuk itu maka badan dunia yang menangani masalah standarisasi ISO (International Standardization Organization) membuat aturan baku yang dikenal dengan nama model referensi OSI (Open System Interconnection). Dengan demikian diharapkan semua vendor perangkat telekomunikasi haruslah berpedoman dengan model referensi ini dalam mengembangkan protokolnya [5].



Gambar 2.15. Model Referensi OSI

Setiap protokol berkomunikasi dengan *peer* (pasangan) protokol yang sama dalam layer yang sama dalam remote-system misalnya FTP lokal merupakan *peer* dari FTP remote. Jadi secara abstrak setiap protokol hanya peduli terhadap komunikasi dengan *peer*-nya, tak perduli dengan layer di bawah dan di atasnya.

Model OSI terdiri dari 7 lapisan (layer) mulai dari lapisan Physical Layer sampai dengan Aplication layer. Berikut penjelasan setiap lapisan dari Model OSI :

1. *Physical Layer*

Lapisan pertama ini berfungsi untuk mengatur sinkronisasi pengiriman dan penerimaan data, spesifikasi mekanis dan elektris, menerapkan prosedur untuk membangun, mengirimkan data/informasi dalam bentuk digit biner.

2. *Data link layer*

Lapisan kedua ini akan memberikan transfer data/informasi yang meyakinkan kepada lapisan fisik dalam bentuk paket yang dilengkapi dengan SYNC, *error control*, dan *flow control.* Pada lapisan ini juga dilakukan persiapan untuk mengaktifkan, memelihara dan memutuskan

suatu hubungan komunikasi, pendeteksian kesalahan yang mungkin terjadi pada saat pengiriman data dan pengendalian.

3. ***Network Layer***

Lapisan ketiga ini berfungsi memberikan layanan data dengan menentukan rute pengiriman dan mengendalikannya sehingga tidak terjadi kemacetan dan data dapat sampai ditempat tujuan dengan baik.

4. ***Transport Layer***

Lapisan keempat ini menjamin bahwa data yang diterima atau dikirimkan dari atau ke session layer dalam keadaan utuh, urut, tanpa duplikasi dan bebas dari kesalahan. Data yang diterima dari session layerkemudian akan dikirimkan ke network layer.Lapisan ini juga akan memeriksa apakah data telah sampai di tempat tujuan dengan baik.

5. ***Session Layer***

Lapisan kelima ini bertugas untuk memberikan Pengontrolan terhadap kerja sama antar komputer yang sedang berkomunikasi

6. ***Presentation Layer***

Lapisan keenam ini akan melakukan konversi agar data/informasi yang dikirimkan dimengerti oleh perngirim dan juga oleh penerima. Selain itu, dapat juga dilakukan kompresi dan enkripsi data agar keamanan data terjamin.

7. ***Aplication Layer***

Lapisan ketujuh merupakan lapisan yang bertugas untuk mengatur interaksi antara pengguna komputer dengan program aplikasi yang dipakai. Lapisan ini merupakan lapisan tertinggi pada

model referensi OSI, biasanya berupa program atau aplikasi pada tingkatan layanan informasi.

Model referensi OSI terdiri dari tujuh lapisan, mulai dari lapisan fisik sampai dengan aplikasi. Model referensi ini tidak hanya berguna untuk produk-produk LAN saja, tetapi dalam membangung jaringan Internet sekalipun sangat diperlukan. Hubungan antara model referensi OSI dengan protokol Internet bisa dilihat dalam Tabel 2.1.

Tabel 2.1. Hubungan Model Referensi OSI dengan Protokol Internet

MODEL OSI		**TCP/IP**	**PROTOKOL TCP/IP**	
NO	**LAPISAN**		**PROTOKOL**	**FUNGSI**
7			DHCP	Distribusi IP pada jaringan dengan jumlah IP yang terbatas
			DNS	Database nama domain mesin dan nomer IP
			FTP	Transfer file
			HTTP	Transfer file HTML dan Web
			MIME	Mengirim file binary dalam bentuk tesk

	Aplication	Aplication	NNTP	Menerima dan mengirim newsgroup)
			POP	Mengambil mail dari server
			SMB	Transfer berbagai server file DOS dan Windows
6	Presentation		SMTP	Pertukaran mail
			SNMP	Manajemen jaringan
			Telnet	Akses jarak jauh
			TFTP	Transfer file
5	Session		NETBIOS	BIOS jaringan standar
			RPC	Pemanggilan jarak jauh
			SOCKET	Input output nuntuk network jenis BSD-UNIX
4	Transport	Transport	TCP	Pertukaran data berorientasi
			UDP	Pertukaran data non-orientasi (connectonless(
3			IP	Menetapkan routing

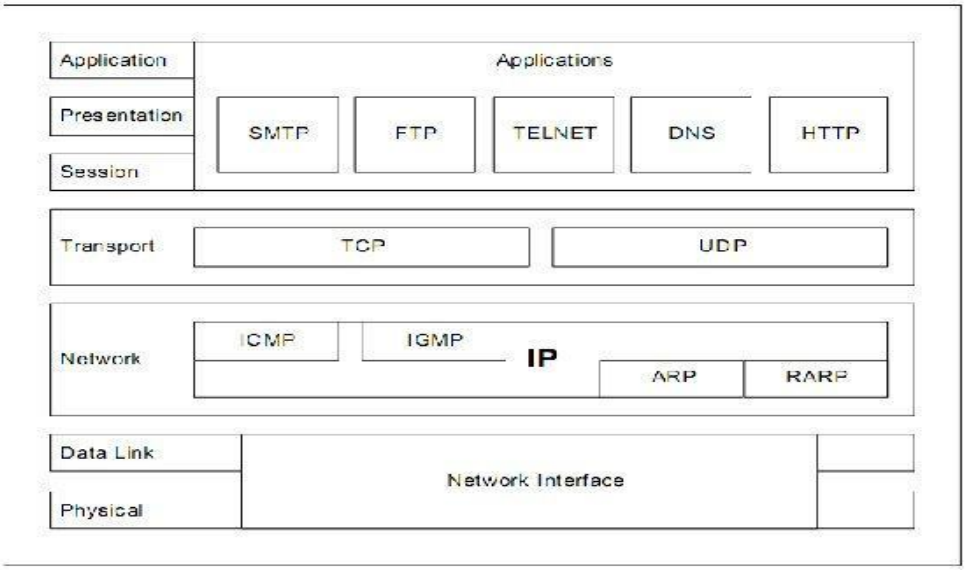
	Network	Internet	RIP	Memilih routing
			ARP	Mendapatkan informasi hardware dari nomer IP
			RARP	Mendapatkan nomer IP dari hardware
2	Datalink	Network	PPP	Point ke point
			SLIP	Menggunakan sambungan serial
1	Physics	Ethernet, FDDI, ISDN, ATM		

2.5. TCP/IP

TCP/IP dikembangkan mengacu pada model Open System Interconnection (OSI), dimana, layer-layer yang terdapat pada TCP tidak persis sama dengan layer-layer yang terdapat pada model OSI. Dengan menggunakan protokol yang sama yaitu TCP/IP, perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. TCP/IP pada awal perkembangannya digunakan oleh Defense Advanced Research Project Agency (DARPA) untuk membangun jaringan untuk keperluan militer. Nama TCP/IP sendiri diambil dari nama protokol pada layer network yaitu Internet Protocol (IP) dan protokol pada layer transfort yaitu Transmission Control Protocol (TCP). Dengan mengacu pada nama ini, TCP/IP internet kemudian sering disebut sebagai Internet [6]

TCP/IP(Transmission Control Protocol/Internet Protocol) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain di

dalam jaringan internet. TCP/IP merupakan salah satu perangkat lunak jaringan komputer (networking software) yang terdapat dalam sistem, dan dipergunakan dalam komunikasi data dalam local area network (LAN) maupun Internet. TCP/IP dinamakan dari dua protokol yang paling penting di dalamnya yaitu TCP singkatan dari transfer control protocol dan IP singkatan dari Internet Protocol. TCP/IP menjadi satu nama karena fungsinya selalu bergandengan satu sama lain dalam komunikasi data. TCP/IP saat ini dipergunakan dalam banyak jaringan komputer lokal (LAN) yang terhubung ke Internet. Protokol ini tidaklah



dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protocol (protocol suite). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Arsitektur protokol TCP/IP ini dapat dimodelkan dengan empat layer sebagaimana yang dapat dilihat pada gambar 2.15.

TCP/IP terdiri dari empat lapis kumpulan protokol yang bertingkat. Empat tingkat itu adalah :

1. **Network Interface Layer**

Bertanggung jawab mengirim dan menerima data ke dan dari media fisik (berupa kabel, serat optik atau gelombang radio), maka dari itu harus mampu menerjemahkan sinyal listrik menjadi digital yang dimengerti komputer.

2. Internet Layer

Bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol yaitu:

a. IP (Internet Protocol) berfungsi untuk menyampaikan paket data ke alamat yang tepat, IP memiliki sifat sebagai *unrealieble* (ketidakandalan: tidak menjamin datagram yang terkirim sampai tujuan), connectionless, datagram delivery service.

b. ARP (Address Resolution Protocol) Protokol yang digunakan untuk nenemukan alamat Hardware dari host/komputer yang terletak pada network yang sama.

c. ICMP (Internet Control message protokol) Protokol yang digunakan untuk mengirimkan pesan dan melapor kegagalan pengiriman data.

3. Transport Layer

Transport Layer merupakan layer ketiga yang berada diantara *Internet Layer* dan *Aplication Layer*. Layer ini bertanggungnjawab untuk autentifikasi komunikasi antara device (*host to host).*

4. Aplication Layer

Terletak semua aplikasi yang menggunakan protokol TCP/IP.Fungsi masing-masing layer / lapisan protokol serta aliran data pada layer TCP / IP diatas, dapat dicontohkan dengan mengggunakan analogi yang sangat sederhana.

2.5.1 Kelas IP

Alamat IP versi 4 dibagi ke dalam beberapa kelas, dilihat dari oktet pertamanya, seperti terlihat pada tabel. Sebenarnya yang menjadi pembeda kelas IP versi 4 adalah pola biner yang terdapat dalam oktet pertama (utamanya adalah bit-bit awal/*high-order bit*), tapi untuk lebih mudah mengingatnya, akan lebih cepat diingat dengan menggunakan representasi desimal [6].

Tabel 2.2. Kelas IP

Kelas Alamat IP	**Oktet pertama (desimal)**	**Oktet pertama (biner)**	**Digunakan oleh**
Kelas A	1–126	0xxx xxxx	Alamat *unicast* untuk jaringan skala besar

Kelas B	128–191	10xx xxxx	Alamat *unicast* untuk jaringan skala menengah hingga skala besar
Kelas C	192–223	110x xxxx	Alamat *unicast* untuk jaringan skala kecil
Kelas D	224–239	1110 xxxx	Alamat *multicast* (bukan alamat *unicast*)
Kelas E	240–255	1111 xxxx	Direservasikan;umumnya digunakan sebagai alamat percobaan (eksperimen); (bukan alamat unicast)

a. IP Kelas A

Alamat-alamat kelas A diberikan untuk jaringan skala besar. Nomor urut bit tertinggi di dalam alamat IP kelas A selalu diset dengan nilai **0** (nol). Tujuh bit berikutnya—untuk melengkapi oktet pertama—akan membuat sebuah network identifier. 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan host identifier. Ini mengizinkan kelas A memiliki hingga 126 jaringan, dan 16,777,214 host tiap jaringannya. Alamat dengan oktet awal 127 tidak diizinkan, karena digunakan untuk mekanisme Interprocess Communication (IPC) di dalam mesin yang bersangkutan.

b. IP Kelas B

Alamat-alamat kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diset ke bilangan biner **10**. 14 bit berikutnya (untuk melengkapi dua oktet pertama), akan membuat sebuah *network identifier*. 16 bit sisanya (dua oktet terakhir) merepresentasikan *host identifier*. Kelas B dapat memiliki 16,384 network, dan 65,534 host untuk setiap network-nya

c. IP Kelas C

Alamat IP kelas C digunakan untuk jaringan berskala kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diset ke nilai biner **110**. 21 bit selanjutnya (untuk melengkapi tiga oktet pertama) akan membentuk sebuah *network identifier*. 8 bit sisanya (sebagai oktet terakhir) akan merepresentasikan *host identifier*. Ini memungkinkan pembuatan total 2,097,152 buah network, dan 254 host untuk setiap network-nya.

d. IP Kelas D

Alamat IP kelas D disediakan hanya untuk alamat-alamat *IP multicast*, namun berbeda dengan tiga kelas di atas. Empat *bit* pertama di dalam IP kelas D selalu diset ke bilangan biner **1110**. 28*bit* sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host. Untuk lebih jelas mengenal alamat ini, lihat pada bagian Alamat *Multicast* IPv4

e. IP Kelas E

Alamat IP kelas D disediakan hanya untuk alamat-alamat *IP multicast*, namun berbeda dengan tiga kelas di atas. Empat *bit* pertama di dalam IP kelas D selalu diset ke bilangan biner **1110**. 28*bit* sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali host. Untuk lebih jelas mengenal alamat ini, lihat pada bagian Alamat *Multicast* IPv4

2.5.1 Jenis IP Address

Berdasarkan fungsinya, *IP Address* dibagi menjadi 2 jenis yaitu :

a. **IP *Public***

IP Public adalah IP *address* yang telah ditetapkan oleh InterNIC dan berisi beberapa buah network ID yang dijamin unik yang digunakan untuk lingkup internet, host yang menggunakan IP public dapat diakses oleh seluruh user yang tergabung diinternet baik secara langsung maupun tidak langsung (melalui proxy/NAT). IP *Addressing* juga dikelompokkan berdasarkan negara, Indonesia umumnya dimulai dengan kepala 202 & 203. Contoh : P Public adalah akses Speedy modem yang merupakan IP Public 125.126.0.1

b. IP *Private*

IP Private adalah IP address yang digunkan untuk lingkup intranet, host yang menggunakan IP Private hanya bisa diakses di linkup intranet saja. Contoh : IP private akses di LAN modem menggunakan IP Private 192.168.1.1.

2.6. Keamanan Jaringan Komputer

Perkembangan teknologi jaringan komputer menyebabkan terkaitnya satu komputer dengan komputer lainya. Hal ini membuka banyak peluang dalam pengembangan aplikasi komputer tetapi juga mebuat peluang adanya ancaman terhadap pengubahan dan pencurian data. Sebuah aplikasi yang melintasi jaringan publik seperti internet diasumsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri atau mengubah data. Oleh karena itu, untuk melindungi data terhadap akses, pengubahan dan penghalangan yang tidak dilakukan oleh pihak yang berwenang, peranti keamanan data yang melintas di jaringan komputer harus disediakan [7]

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan. Sistem jaringan komputer memberikan perlindungan terhadap data. Jaminan keamanan data tersebut diberikan melelui pengaturan hak akses para pemakai dan password, serta teknik perlindungan terhadap hardisk sehingga data mendapatkan perlindungan yang efektif. Dengan adanya pemakaian sumber daya secara bersama-sama, maka pemakai bisa mendapatkan hasil dengan maksimal dan kualitas yang tinggi. Selain itu data atau informasi yang diakses selalu terbaru, karena setiap ada perubahan yang terjadi dapat segera lengsung diketahui oleh setiap pemakai.

Prinsip keamanan jaringan dapat dibedakan menjadi :

a. Kerahasiaan

Kerahasiaan berhubungan dengan hak akses untuk membaca data atau informasi dan suatu sistem computer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya

dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal.

b. Integritas

Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem computer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat diubah oleh pihak yang telah diberi hak.

c. Ketersediaan

Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak.

d. Otentifikasi

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli. Untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature. Sedangkan untuk menguji keaslian orang atau server yang dimaksud bisa dilakukan dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

e. Akses Kontrol

Aspek kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana user dan sistem berkomunikasi dan berinteraksi dengan system dan sumberdaya yang lainnya. Akses kontrol melindungi sistem dan sumberdaya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi. Kontrol akses adalah sebuah term luas yang mencakup beberapa tipe mekanisme berbeda yang menjalankan fitur kontrol akses pada sistem komputer, jaringan, dan informasi. Kontrol akses sangatlah penting karena menjadi satu dari garis pertahanan pertama yang digunakan untuk menghadang akses yang tidak berhak ke dalam sistem dan sumberdaya jaringan.

f. Non-Repundiation

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Penggunaan digital signature, certificates, dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital signature itu jelas legal.

2.6.1 Serangan Terhadap Jaringan

Serangan keamanan jaringan yang dioperasionalkan pada jaringan publik rentan terhadap serangan oleh pihak yang tidak berwenang. Serangan terhadap sistem keamanan jaringan bertujuan untuk mengalahkan tujuan layanan keamanan jaringan . misalnya penyerang ingin mengungkap isi teks asli sehingga ia dapat mengungkap teks sandi lainya. Secara umum serangan pada sistem keamanan jaringan dapat

dikategorikan menjadi 2 jenis, yaitu serangan pasif dan serangan aktif. [7]

2.6.1.1. Serangan Pasif

Pada seragnan pasif, penyerang hanya mengumpulkan data yang melintas pada jaringan publik (jaringan yang bisa diakses oleh semua orang). Serangan pasif tidak melakukan modifikasi data yang melintas atau merusak sistem, penyerang hanya bisa membaca (read only). Berdasarkan data yang dikumpulkan tadi penyerang melakukan analisis untuk menggagalkan tujuan layanan keamanan jaringan. Karena tidak melakukan modifikasi dan mengganggu sistem, serangan pasif sulit di deteksi, tapi dapat dicegah dengan cara menggunakan sandi pada saat mengirim pesan misalnya. *Snooping* dan *Traffic Analysis* merupakan contoh dari serangan pasif

2.6.1.2. Serangan Aktif

Serangan aktif dapat mengakibatkan perubahan data yang sedang dikirimkan melaui jaringan dan mengganggu sistem. Serangan pasif memungkinkan penyerang untuk mengubah data pada lalu lintas data dijaringan. Jenis – jenis serangan aktif adalah sebagai berikut:

a. *Masquerade*

Masquerade merupakan serangan aktif yang dilakukan oleh penyerang dengan cara mengambil alih (menirukan) perilaku pengirim atau penerima. Contohnya pada saat Andi ingi membuat kunci bersama dengan Budi, disaat yang bersamaan secara tidak sadar Rani mengambil alih peran Budi sehingga Andi mengirim pesan ke Rani bukan kepada Budi.

b. *Modification*

Modification merupakan serangan dengan cara mengambil alih jalur komunikasi untuk mengubah atau menghapus pesan yang sedang dikirimkan untuk keuntungan penyerang. Misalnya pesan “kirim Rp 100.000, 00 ke nomer rekening Andi” dirubah oleh Rani menjadi “kirim Rp 100.000, 00 ke nomer rekening Rani”.

c. *Replay*

Replay merupakan serangan yang terdiri dari pencatatan secara pasif data dan transmisi ulang untuk menimbullkan efek yang diinginkan oleh penyerang. Misalnya Rani pernah meminta Budi untuk mengirim Rp 100.000, 00 ke Rani, lalu Budi mengirim pesan “kirim Rp 100.000, 00 ke Rani” ke Bank, pada saat pesan dikirimkan Rani mencatat pesan “kirim Rp 100.000, 00 ke Rani” lalu mengirim ulang pesan tersebut ke Bank sehingga Rani mendapat uang dengan jumlah dua kali lebih besar.

d. *Denial of Service*

Denial of Service merupakan jenis serangan yang bertujuan menyebabkan sistem menjadi tidak dapat bekerja sama sekali sehingga tidak bisa memeberikan pelayanan yang seharusnya kepada pengguna. Contohnya adalah penyerang membuat permintaan kosong (dummy) sehingga server menjadi overload.

Biasanya sebuah sistem keamanan jaringan dikatakan aman apabila tahan terhadap serangan aktif. Untuk mengembangkan sistem keamanan yang baik, seorang perancang keamanan jaringan harus menganalisis kemungkinan serangan-serangan terhadap layanan keamanan jaringan. [7]

2.7. Internet

Internet adalah himpunan informasi dan sumber daya komputer yang paling besar di dunia. Internet merupakan koneksi berbagai macam jaringan komputer dengan berbagai jenis hardware dan teknologi yang berbeda. Komunikasi yang dibangun pada jaringan internet menggunakan mekanisme tertentu yang disebut dengan protocol. Protocol yang digunakan untuk menjalankan komunikasi antar jaringan komputer pada internet ini adalah Transmission Control Protocol/ Internet Protocol (TCP/IP) [6].

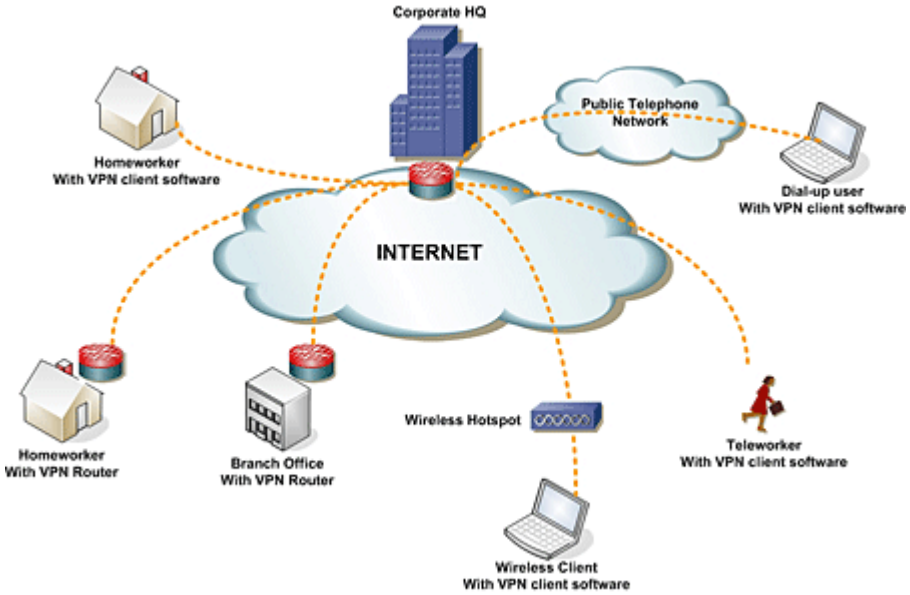
Proses yang terjadi pada internet mempunyai mekanisme yang telah diatur berdasarkan protokol standar. Proses yang terjadi di internet adalah ada satu program yang meminta kepada program yang lain untuk memberikan suatu layanan. Dua program tersebut dapat terletak dalam subnet yang sama ataupun berbeda. Komputer dengan program yang meminta layanan disebut dengan client sedangkan yang memberikan layanan disebut server.

2.8. Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan pengguna untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupaun sebenarnya menggunakan jaringan milik publik.

VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Konkesi VPN juga dapat terjadi pada semual layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. VPN dapat terjadi antara dua end-system atau dua komputer atau antara dua atau lebih jaringan yang

berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur WAN alternatif untuk mendapatkan koneksi point-to-point pribadi antara pengirim dan penerima. Dan dapat dilakukan dengan menggunakan media apa saja, tanpa perlu media leased line atau frame relay.



Gambar 2.17. Skema VPN

Dari gambar 2.16. dapat kita lihat bahwa VPN dapat terjadi pada dua end-system. Syarat yang harus terpenuhi adalah kedua system tersebut saling terhubung dengan jaringan public (Internet). Di dalam jaringan public ini kedua system membuat semacam jalur khusus yang biasa disebut tunnel untuk saling terkoneksi. Jadi tunnel inilah yang membuat seolah-olah kedua system tersebut berada dalam local area yang sama. Analogi dari gambar di atas misalkan bagan system yang kiri adalah suatu jaringan local (LAN) suatu instansi pusat kemudian

system yang kanan adalah suatu LAN anak cabang. Kedua LAN ini membangun suatu tunnel pada jaringan public untuk saling terhubung hingga membentuk suatu VPN. Dengan demikian instansi ini tidak perlu lagi membangun suatu jaringan pribadi secara leased line yang memakan banyak biaya [5].

2.5.1 Fungsi VPN

Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Ketiga fungsi utama tersebut antara lain sebagai berikut:

1. **Confidentially (Kerahasiaan)**

   Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

2. **Data Integrity (Keutuhan Data)**

   Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

3. Origin Authentication (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

2.5.2 Jenis VPN

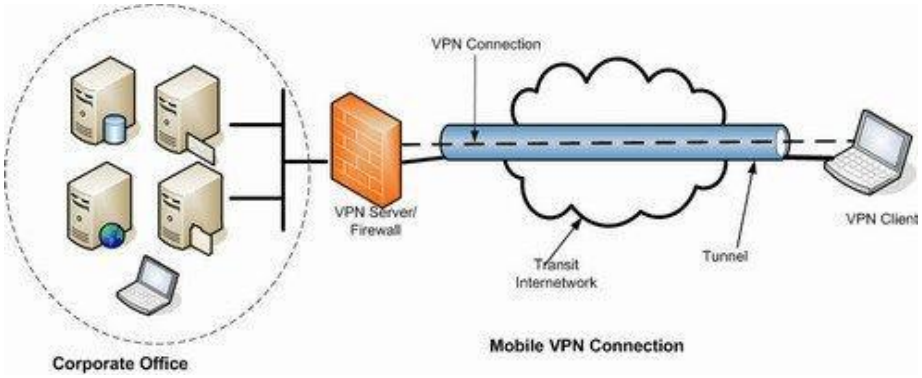
Di dalam implementasinya VPN dibagi menjadi dua jenis yaitu *remote acces* VPN dan *site-to-site VPN* :

1. *Remote Acces*

Jenis implementasi yang pertama adalah Remote access yang biasa juga disebut virtual private dial-up network (VPDN), menghubungkan antara pengguna yang mobile dengan local area network (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (remote) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan software klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut [8].

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-dial nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan sotware klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan. Perusahaan yang

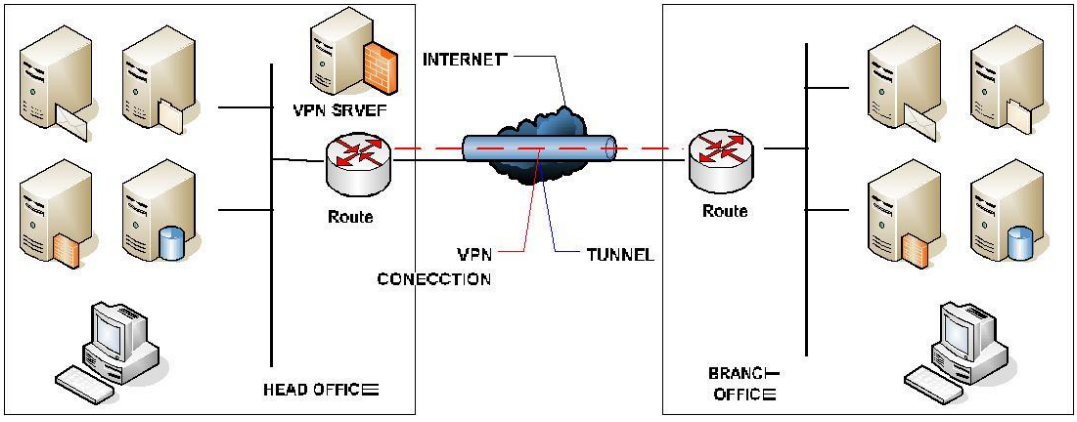
memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan remote access VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.



Gambar 2.18. *Remote Acces VPN*

2. *Site to Site*

Jenis implementasi VPN yang kedua adalah site-to-site VPN. Implementasi jenis ini menghubungkan antara dua tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet site-to-site VPN [5].

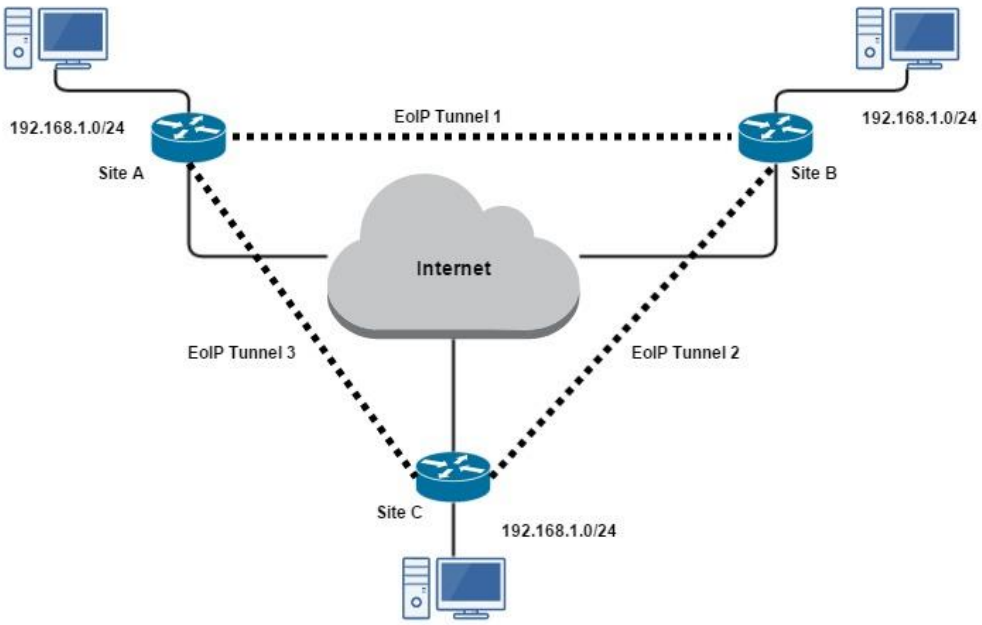


Gambar 2.19. *Site to Site VPN*

2.8.3 Ethernet over Internet Protocol (EoIP)

Ethernet over Internet Protocol (EoIP) merupakan sebuah metode yang dapat menghubungkan dua atau beberapa *route*r dengan tunneling melalui jaringan internet. EoIP merupakan *proprietary* MikroTik *Route*rOS yang artinya EoIP hanya dapat diterapkan pada MikroTik *Route*rOS saja [9]**.**

EoIP merupakan sebuah metode menghubungkan komputer melalui internet dengan membuat sebuah *tunnel* antar *route*r. Berbeda dengan VPN lainnya *tunnel* yang dibuat dengan EoIP merupakan tunnel yang bersifat *site to site* sehingga tidak memerlukan server VPN. Selain itu EoIP hanya menyediakan *tunnel* saja tanpa ada fitur keamanan. Namun, EoIP dapat dikombinasikan dengan fitur keamanan lain untuk menjaga kerahasiaan komunikasi data. EoIP yang bersifat s*ite to site* akan memerlukan lebih banyak *tunnel* jika lebih banyak jaringan yang harus terhubung.



Gambar 2.20. EoIP

2.9. IP Security (IPSec)

IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec bekerja pada lapisan IP, Paket dalam IP dibungkus dalam IPSec dengan menggunakan IKE (internet Key Exchange) [5].

IPSec bisa dipergunakan dengan beberapa cara:

a. *Transport mode*: IPSec hanya melakukan enkripsi
b. *Tunneling mode*: IPSec melakukan enkripsi dan tunneling.

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalu lintas yaitu *Authentication Header* (AH) and

Encapsulating Security Payload (ESP). Implementasi IPSec harus mendukung ESP dan juga AH.

2.9.1 *Authentification Heade*r (AH)

Autentifikasi sumber data dan proteksi terhadap pencurian data. Protocol AH dibuat dengan melakukan enkapsulasi paket IP asli kedalam paket baru yang mengandung IP header yang baru yaitu AH header disertai dengan header asli. Isi data yang dikirimkan melalui protocol AH bersifat clear text sehingga tunnel yang berdasar protocol AH ini tidak menyediakan kepastian data. Kehadiran header AH memungkinkan untuk memverifikasi integritas pesan,. Dengan demikian, AH menyediakan otentikasi tetapi tidak untuk enkripsi. AH menyediakan algoritma autentifikasi sebagai berikut :

a. SHA1

   SHA1 dikembangkan oleh Institut Nasional Standar dan Teknologi seperti yang dijelaskan di Federal Information Processing Standard (FIPS) 180-1 PUB. Proses SHA erat model setelah MD5. Hasil perhitungan dalam The SHA1 hash 160-bit yang digunakan untuk memeriksa integritas. Karena panjang hash lagi memberikan keamanan yang lebih besar, SHA lebih kuat daripada MD5 [5].

b. MD5

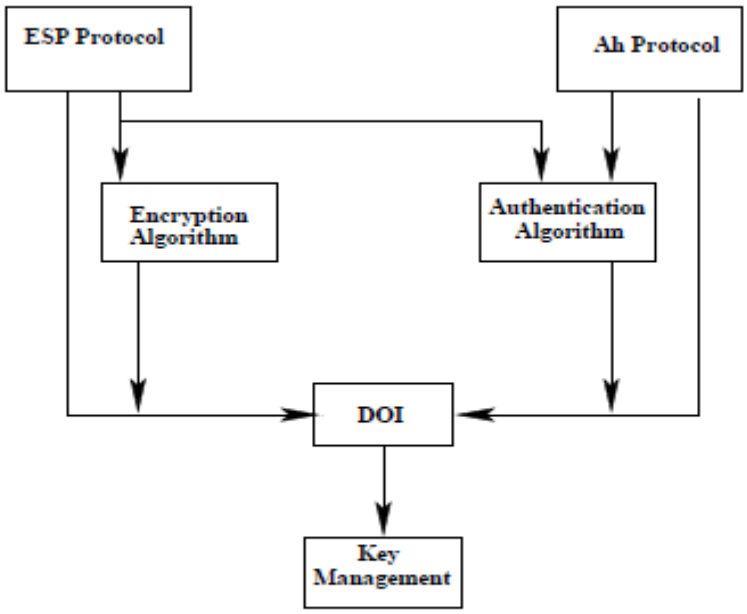
   MD5 didasarkan pada RFC 1321. MD5 melengkapi empat lewat di atas blok data, dengan menggunakan sebuah konstanta numerik yang berbeda untuk setiap kata dalam pesan pada setiap lulus. Jumlah konstanta 32-bit yang digunakan selama perhitungan MD5 akhirnya menghasilkan hash 128-bit yang digunakan untuk memeriksa integritas.

2.9.2 Encapsulating Security Payload (ESP)

Menyediakan kepastian data, autentikasi sumber data dan proteksi terhadap gangguan pada data. Protocol ESP dibuat dengan melakukan enkripsi pada paket IP dan membuat paket IP lain yang mengandung header IP asli dan header ESP. Data yang terenkripsi (yang mengandung header IP asli) dan trailer ESP, separuhnya terenkripsi dan sebagian tidak. ESP menyediakan algoritma enkripsi sebagai berikut. :

a. DES - 56-bit DES-CBC encryption algorithm;
b. 3DES - 168-bit DES encryption algorithm;
c. AES - 128, 192 and 256-bit key AES-CBC encryption algorithm;
d. Blowfish - added since v4.5
e. Twofish - added since v4.5
f. Camellia - 128, 192 and 256-bit key Camellia encryption algorithm added since v4.5

Kedua protokol ini merupakan pembawa kontrol akses berbasis distribusi, kunci kriptografi dan manajemen aliran lalu lintas relatif terhadap protokol keamanan



Gambar 2.21. Arsitektur IPSec