

Kegiatan Belajar 1 Teknologi Jaringan Berbasis Luas (WAN)

Capaian Pembelajaran Mata Kegiatan

Memahami Teknologi Jaringan Berbasis Luar (WAN)

Sub Capaian Pembelajaran Mata Kegiatan

1. Menganalisis Jaringan Berbasis Luas
2. Mengevaluasi Jaringan Nirkabel
3. Mengevaluasi Permasalahan Jaringan Nirkabel
4. Memahami Jaringan Fiber Optic
5. Mengidentifikasi jenis-jenis kabel fiber optic
6. Menerapkan Fungsi Alat Kerja Fiber Optic
7. Mengevaluasi Penyambungan Fiber Optic
8. Mengevaluasi Perangkat Pasif Jaringan Fiber Optic
9. Mengevaluasi Permasalahan Jaringan Fiber Optic

Pokok-Pokok Materi

1. Jaringan Berbasis Luas
2. Jaringan Nirkabel
3. Permasalahan Jaringan Nirkabel
4. Jaringan Fiber Optic
5. Jenis-jenis Kabel Fiber Optic
6. Fungsi Alat Kerja Fiber Optic
7. Penyambungan Fiber Optic
8. Perangkat Pasif Jaringan Fiber Optic
9. Permasalahan Jaringan Fiber Optic

Uraian Materi

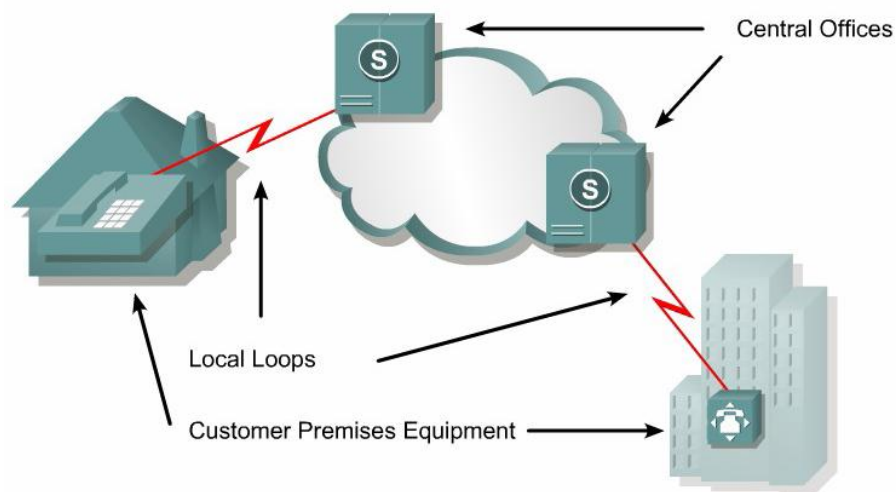
A. Jaringan Berbasis Luas

1. Pengenalan Jaringan Berbasis Luas

Terdapat begitu banyak pilihan yang tersedia untuk mengimplementasikan WAN yang bisa dibedakan berdasarkan teknologi, kecepatan dan biaya yang dibutuhkan. Satu perbedaan utama LAN dengan WAN adalah organisasi harus berlangganan kepada penyedia jaringan dari perusahaan penyedia jaringan yang ada.

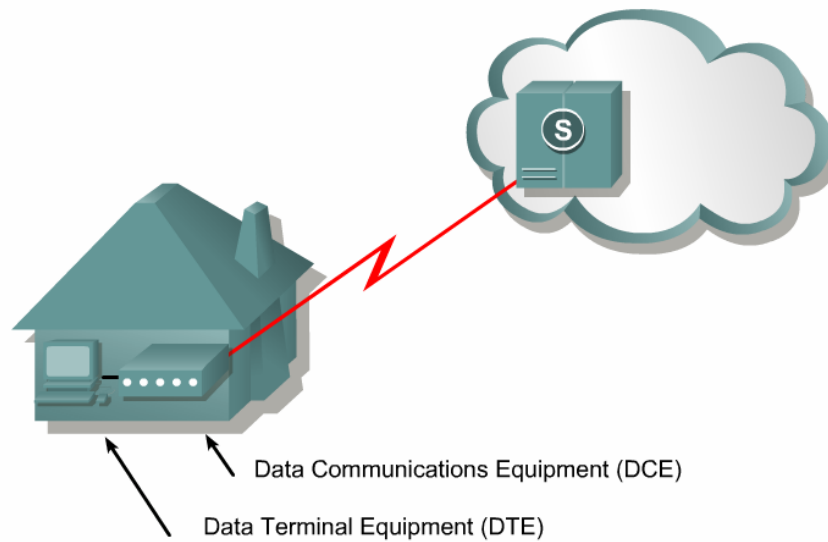
Sebuah WAN menggunakan jalur data untuk membawa data menuju ke internet dan menghubungkan lokasi lokasi perusahaan yang terpisah pisah. Telepon dan layanan data yang paling banyak digunakan pada WAN.

Perangkat pada pelanggan disebut CPE (Customer Premises Equipment). Pelanggan memiliki sendiri atau menyewa dari service provider. Kabel tembaga, serat optik atau wireless yang digunakan untuk menghubungkan CPE ke sentral provider terdekat atau ke kantor pusat dari service provider. Media ini sering disebut dengan local loop.



Gambar 1. 1 Customer Premises Equipment

Perangkat yang meletakkan data ke local loop disebut DCE (Data Circuit-terminating Equipment). Perangkat pelanggan yang melewati data ke DCE disebut dengan DTE (Data Terminal Equipment).



Gambar 1. 2 Komunikasi DCE dan DTE

Jalur WAN menyediakan berbagai macam kecepatan data yang diukur dalam satuan kilobits per second. Dibawah ini berbagai teknologi WAN dan kecepatan yang tersedia.

Line Type	Signal Standard	Bit Rate Capacity
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Gambar 1. 3 Teknologi WAN dan Kecepatannya

2. Perangkat WAN

WAN menghubungkan beberapa LAN melalui jalur komunikasi dari service provider. Karena jalur komunikasi tidak bisa langsung dimasukkan ke LAN maka diperlukan beberapa perangkat interface.

Perangkat perangkat tersebut antara lain:

a. Router

LAN mengirimkan data ke Router, kemudian Router akan menganalisa berdasarkan informasi alamat pada layer 3. Kemudian Router akan meneruskan data tersebut ke interface WAN yang sesuai berdasarkan routing table yang dimilikinya.

Router adalah perangkat jaringan yang aktif dan intelegent dan dapat berpartisipasi dalam manajemen jaringan. Router mengatur jaringan dengan menyediakan kontrol dinamis melalui sumber daya dan mendukung tugas dan tujuan dari jaringan. Beberapa tujuan tersebut antara lain konektivitas, perfomansi yang reliabel, kontrol manajemen dan fleksibilitas.

b. CSU/DSU

Jalur komunikasi membutuhkan sinyal dengan format yang sesuai. Untuk jalur digital, sebuah Channel Service Unit (CSU) dan Data Service Unit (DSU) dibutuhkan. Keduanya sering digabung menjadi sebuah perangkat yang disebut CSU/DSU.

c. Modem

Modem adalah sebuah perangkat dibutuhkan untuk mempersiapkan data untuk transmisi melalui local loop. Modem lebih dibutuhkan untuk jalur komunikasi analog dibandingkan digital. Modem mengirim data melalui jalur telepon dengan memodulasi dan demodulasi sinyal. Sinyal digital ditumpangkan ke sinyal suara analog yang dimodulasi untuk ditransmisikan. Pada sisi penerima sinyal analog dikembalikan menjadi sinyal digital atau demodulasi.

d. Communication Server

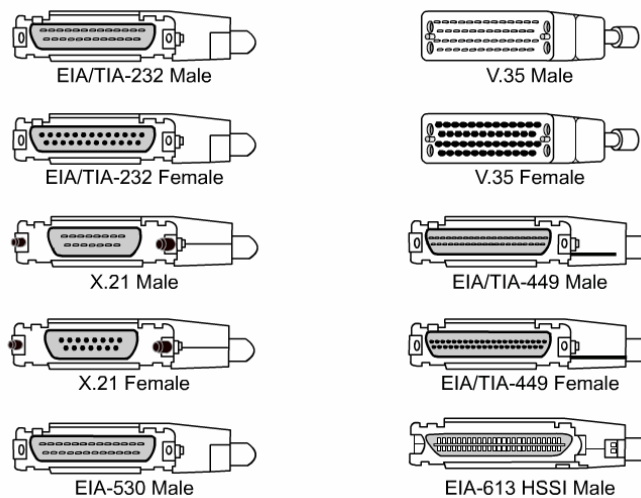
Communication Server mengkonsentrasikan komunikasi pengguna dial-in dan remote akses ke LAN. Communication Server memiliki beberapa interface analog dan digital serta mampu melayani beberapa user sekaligus.

3. Standar WAN

WAN menggunakan OSI layer tetapi hanya fokus pada layer 1 dan 2. Standar WAN pada umumnya menggambarkan baik metode pengiriman layer 1 dan kebutuhan layer 2, termasuk alamat fisik, aliran data dan enkapsulasi. Dibawah ini adalah organisasi yang mengatur standar WAN.

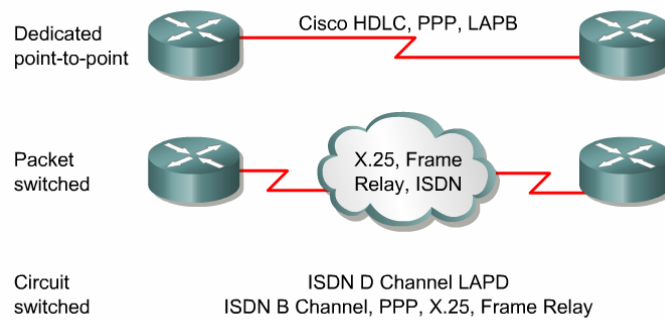
Protokol layer 1 menjelaskan bagaimana menyediakan secara elektris, mekanis, operasi dan fungsi koneksi yang disediakan oleh service provider. Beberapa standar fisik dan konektornya digambarkan dibawah ini.

Standard	Description
EIA/TIA-232	Allows signal speeds of up to 64 Kbps on a 25 pin D connector over short distances. It was formerly known as RS-232. The ITU-T V.24 specification is effectively the same.
EIA/TIA-449/530	A faster (up to 2 Mbps) version of EIA/TIA-232. It uses a 36 pin D connector and is capable of longer cable runs. There are several versions. Also known as RS-422 and RS-423.
EIA/TIA-612/613	The High Speed Serial Interface (HSSI), which provides access to services at up to 52 Mbps on a 60 pin D connector.
V.35	An ITU-T standard for synchronous communications between a network access device and a packet network at speeds up to 48 Kbps. It uses a 34 pin rectangular connector.
X.21	An ITU-T standard for synchronous digital communications. It uses a 15 pin D connector.



Gambar 1. 4 Standar Konektor

Data link layer menjelaskan bagaimana data dienkapsulasi untuk transmisi ke remote site, dan mekanisme untuk pengiriman yang menghasilkan frame. Ada bermacam macam teknologi yang digunakan seperti ISDN, Frame Relay atau Asynchronous Transfer Mode (ATM). Protokol ini menggunakan dasar mekanisme framing yang sama, yaitu High-Level Data Link Control (HDLC) atau satu dari beberapa variannya seperti Point to Point Protocol.

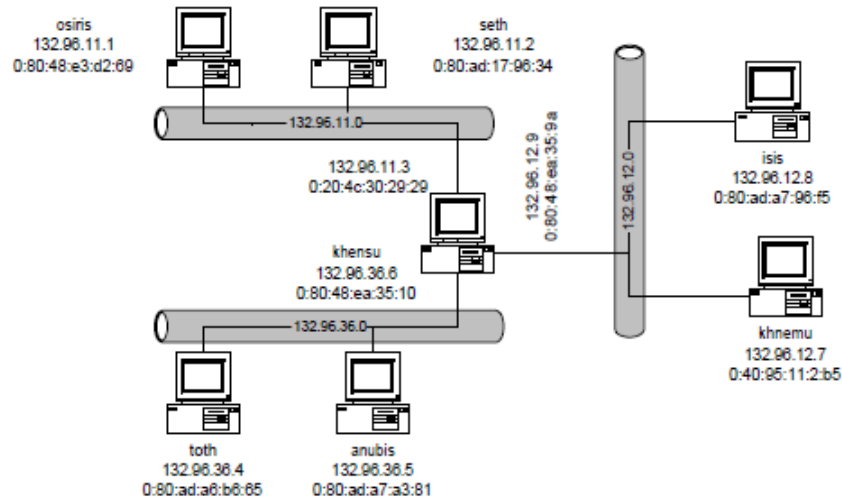


Gambar 1. 5 Data Link Layer

4. Dasar-dasar Routing

a) Routing Langsung dan Tidak Langsung

Proses pengiriman datagram IP selalu menggunakan tabel routing. Tabel routing berisi informasi yang diperlukan untuk menentukan ke mana datagram harus di kirim. Datagram dapat dikirim langsung ke host tujuan atau harus melalui host lain terlebih dahulu tergantung pada tabel routing.

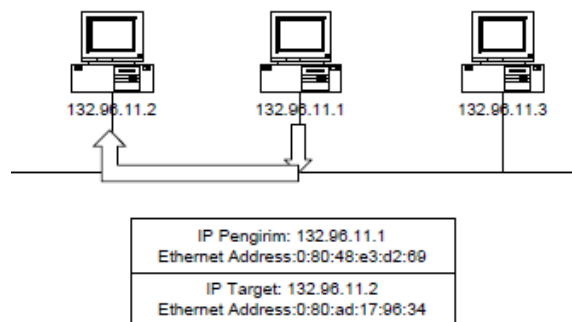


Gambar 1. 6 Jaringan TCP/IP

Gambar diatas memperlihatkan jaringan TCP/ IP yang menggunakan teknologi Ethernet. Pada jaringan tersebut host osiris mengirimkan data ke host seth, alamat tujuan datagram adalah ip address host seth dan alamat sumber datagram adalah ip address host osiris.

Frame yang dikirimkan oleh host osiris juga memiliki alamat tujuan frame MAC Address host Seth dan alamat sumbernya adalah host osiris. Pada saat host osiris mengirimkan frame, host seth membaca bahwa frame tersebut ditujukan kepada alamat ethernetnya.

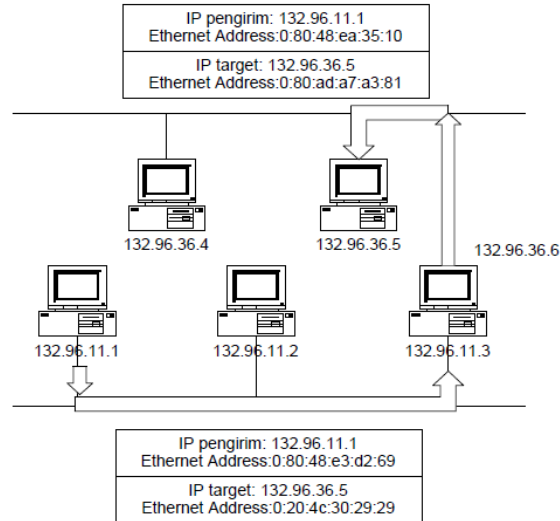
Setelah melepas header frame, host seth kemudian mengetahui bahwa IP address tujuan datagram tersebut juga adalah IP addressnya. Dengan demikian host seth meneruskan datagram ke lapisan transport untuk diproses lebih lanjut. Komunikasi model seperti ini disebut sebagai routing langsung.



Gambar 1. 7 Routing langsung

Pada gambar diatas terlihat bahwa host osiris dan host anubis terletak pada jaringan Ethernet yang berbeda. Kedua jaringan tersebut dihubungkan oleh host khensu. Host khensu memiliki lebih dari satu interface dan dapat melewati datagram dari satu interface ke interface lain (atau bertindak sebagai router).

Ketika mengirimkan data ke host anubis, osiris memeriksa tabel routing dan mengetahui bahwa data tersebut harus melewati host khensu terlebih dahulu. Dengan kondisi seperti ini datagram yang dikirim host osiris ke host anubis memiliki alamat tujuan IP Address host anubis dan alamat sumber IP Address host osiris tetapi frame ethernet yang dikirimnya diberi alamat tujuan MAC Address host khensu dan alamat sumber MAC Address host osiris.



Gambar 1. 8 Routing

Ketika host osiris mengirimkan frame ke jaringan, khensu membaca bahwa alamat ethernet yang dituju frame tersebut adalah alamat ethernetnya. Ketika host khensu melepas header frame, diketahui bahwa host yang dituju oleh datagram adalah host anubis. Host khensu kemudian memeriksa tabel routing yang dimilikinya untuk meneruskan datagram tersebut. Dari hasil pemeriksaan tabel routing, host khensu mengetahui bahwa host anubis terletak dalam satu jaringan ethernet dengannya. Dengan demikian datagram tersebut dapat langsung disampaikan oleh host khensu ke host anubis. Pada pengiriman data tersebut, alamat tujuan dan sumber datagram tetap IP Address host anubis dan host osiris tetapi alamat tujuan dan sumber frame Ethernet menjadi MAC Address host anubis dan host khensu. Komunikasi seperti ini disebut sebagai routing tak langsung karena untuk mencapai host tujuan, datagram harus melewati host lain yang bertindak sebagai router.

Pada dua kasus diatas terlihat proses yang terjadi pada lapisan internet ketika mengirimkan dan menerima datagram. Pada saat mengirimkan datagram, host harus memeriksa apakah alamat tujuan datagram terletak pada jaringan yang sama atau tidak. Jika alamat tujuan datagram terletak pada jaringan yang sama, datagram dapat langsung disampaikan. Jika ternyata alamat tujuan datagram tidak terletak pada jaringan yang sama, datagram tersebut harus disampaikan melalui host lain yang bertindak sebagai router. Pada saat menerima datagram host harus memeriksa apakah ia merupakan tujuan dari datagram tersebut. Jika memang demikian maka data diteruskan ke lapisan

transport. Jika ia bukan tujuan dari datagram tersebut, maka datagram tersebut dibuang. Jika host yang menerima datagram tersebut sebuah router, maka ia meneruskan datagram ke interface yang menuju alamat tujuan datagram.

b) Jenis Konfigurasi Routing

Konfigurasi routing secara umum terdiri dari 3 macam yaitu:

1) Minimal Routing

Dari namanya dapat diketahui bahwa ini adalah konfigurasi yang paling sederhana tapi mutlak diperlukan. Biasanya minimal routing dipasang pada network yang terisolasi dari network lain atau dengan kata lain hanya pemakaian lokal saja.

2) Static Routing

Konfigurasi routing jenis ini biasanya dibangun dalam network yang hanya mempunyai beberapa gateway, umumnya tidak lebih dari 2 atau 3. Static routing dibuat secara manual pada masing-masing gateway. Jenis ini masih memungkinkan untuk jaringan kecil dan stabil. Stabil dalam arti kata jarang down. Jaringan yang tidak stabil yang dipasang static routing dapat membuat kacau seluruh routing, karena tabel routing yang diberikan oleh gateway tidak benar sehingga paket data yang seharusnya tidak bisa diteruskan masih saja dicoba sehingga menghabiskan bandwidth. Terlebih menyusahkan lagi apabila network semakin berkembang. Setiap penambahan sebuah router, maka router yang telah ada sebelumnya harus diberikan tabel routing tambahan secara manual. Jadi jelas, static routing tidak mungkin dipakai untuk jaringan besar, karena membutuhkan effort yang besar untuk mengupdatenya.

3) *Dynamic Routing*

Dalam sebuah network dimana terdapat jalur *routing* lebih dari satu rute untuk mencapai tujuan yang sama biasanya menggunakan *dynamic routing*. Dan juga selain itu *network* besar yang terdapat lebih dari 3 *gateway*. Dengan *dynamic routing*, tinggal menjalankan *routing* protokol yang dipilih dan biarkan bekerja. Secara otomatis tabel routing yang terbaru akan didapatkan.

Seperti dua sisi uang, *dynamic routing* selain menguntungkan juga sedikit merugikan. *Dynamic routing* memerlukan routing protokol untuk membuat tabel *routing* dan *routing* protokol ini bisa memakan *resource* komputer.

1. Routing Protocol

Protokol routing merupakan aturan yang mempertukarkan informasi routing yang nantinya akan membentuk tabel routing sedangkan routing adalah aksi pengiriman-pengiriman paket data berdasarkan tabel routing tadi. Semua routing protokol bertujuan mencari rute tersingkat untuk mencapai tujuan. Dan masing-masing protokol mempunyai cara dan metodenya sendiri-sendiri. Secara garis besar, routing protokol dibagi menjadi Interior Routing Protocol dan Exterior Routing Protocol. Keduanya akan diterangkan sebagai berikut:

a. Interior Routing Protocol

Sesuai namanya, interior berarti bagian dalam. Dan interior routing protocol digunakan dalam sebuah network yang dinamakan autonomus systems (AS) . AS dapat diartikan sebagai sebuah network (bisa besar atau pun kecil) yang berada dalam satu kendali teknik. AS bisa terdiri dari beberapa sub network yang masing-masingnya mempunyai gateway untuk saling berhubungan. Interior routing protocol mempunyai beberapa macam implementasi protokol, yaitu:

1) RIP (*Routing Information Protocol*)

Merupakan protokol routing yang paling umum dijumpai karena biasanya sudah included dalam sebuah sistem operasi, biasanya unix atau novell. RIP memakai metode distance-vector algoritma. Algoritma ini bekerja dengan menambahkan satu angka metrik kepada routing apabila melewati satu gateway. Satu kali data melewati satu gateway maka angka metriknya bertambah satu (atau dengan kata lain naik satu hop). RIP hanya bisa menangani 15 hop, jika lebih maka host tujuan dianggap tidak dapat dijangkau. Oleh karena alasan tadi maka RIP tidak mungkin untuk diterapkan di sebuah AS yang besar. Selain itu RIP juga mempunyai kekurangan dalam hal network masking. Namun kabar baiknya, implementasi RIP tidak terlalu sulit jika dibandingkan dengan OSPF yang akan diterangkan berikut ini.

2) OSPF (*Open Shortest Path First*)

Merupakan protokol routing yang kompleks dan memakan resource komputer. Dengan protokol ini, route dapat dibagi menjadi beberapa jalan. Maksudnya untuk mencapai host tujuan dimungkinkan untuk mencapainya melalui dua atau lebih rute secara paralel. Lebih jauh tentang RIP akan diterangkan lebih lanjut.

b. Exterior Protocol

AS merupakan sebuah network dengan sistem policy yang pegang dalam satu pusat kendali. Internet terdiri dari ribuan AS yang saling terhubung. Untuk bisa saling berhubungan antara AS, maka tiap-tiap AS menggunakan exterior protocol untuk pertukaran informasi routingnya. Informasi routing yang dipertukarkan bernama reachability information (informasi keterjangkauan). Tidak banyak router yang menjalankan routing protokol ini. Hanya router utama dari sebuah AS yang menjalankannya. Dan untuk terhubung ke internet setiap AS harus mempunyai nomor sendiri. Protokol yang mengimplementasikan exterior:

1) EGP (*Exterior Gateway Protocol*)

Protokol ini mengumumkan ke AS lainnya tentang network yang berada di bawahnya. Pengumumannya kira-kira berbunyi: "Kalau hendak pergi ke AS nomor sekian dengan nomor network sekian, maka silahkan melewati saya".

Router utama menerima routing dari router-router AS yang lain tanpa mengevaluasinya. Maksudnya, rute untuk ke sebuah AS bisa jadi lebih dari satu rute dan EGP menerima semuanya tanpa mempertimbangkan rute terbaik.

2) BGP (*Border Gateway Protocol*)

BGP sudah mempertimbangkan rute terbaik untuk dipilih. Seperti EGP, BGP juga mempertukarkan reachability information.

2. ARP

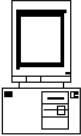
Untuk keperluan mapping IP address ke Alamat Ethernet maka di buat protokol ARP (Address Resolution Protocol). Proses mapping ini dilakukan hanya untuk datagram yang dikirim host karena pada saat inilah host menambahkan header Ethernet pada datagram. Penerjemahan dari IP address ke alamat Ethernet dilakukan dengan melihat sebuah tabel yang disebut sebagai cache ARP, lihat tabel 1. Entri cache ARP berisi IP address host beserta alamat Ethernet untuk host tersebut. Tabel ini diperlukan karena tidak ada hubungan sama sekali antara IP address dengan alamat Ethernet. IP address suatu host bergantung pada IP address jaringan tempat host tersebut berada, sementara alamat Ethernet sebuah card bergantung pada alamat yang diberikan oleh pembuatnya.

Tabel Cache ARP

IP address	Alamat Ethernet
132.96.11.1	0:80:48:e3:d2:69
132.96.11.2	0:80:ad:17:96:34
132.96.11.3	0:20:4c:30:29:29

Mekanisme penterjemahan oleh ARP dapat dijelaskan sebagai berikut. Misal suatu host A dengan IP address 132.96.11.1 baru dinyalakan, lihat Gambar 1.9. Pada saat awal, host ini hanya mengetahui informasi mengenai interface-nya sendiri, yaitu IP address, alamat network, alamat broadcast dan alamat ethernet. Dari informasi awal ini, host A tidak mengetahui alamat ethernet host lain yang terletak satu network dengannya (cache ARP hanya berisi satu entri, yaitu host A). Jika host memiliki route default, maka entri yang pertama kali dicari oleh ARP adalah router default tersebut.

Misalkan terdapat datagram IP dari host A yang ditujukan kepada host B yang memiliki IP 132.96.11.2 (host B ini terletak satu subnet dengan host A). Saat ini yang diketahui oleh host A adalah IP address host B tetapi alamat ethernet B belum diketahui.



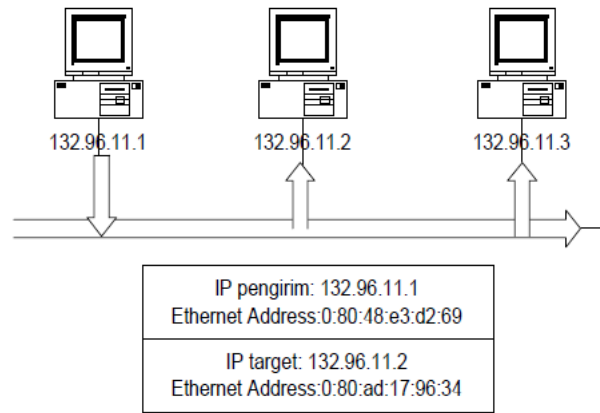
Alamat IP	Alamat Ethernet
132.96.11.1	0:80:48:e3:d2:69

132.96.11.1

Gambar 1. 9 Mekanisme Penterjemahan

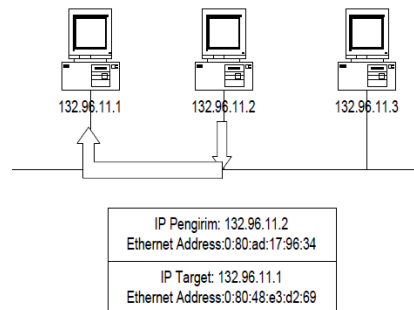
Agar dapat mengirimkan datagram ke host B, host A perlu mengisi cache ARP dengan entri host B. Karena cache ARP tidak dapat digunakan untuk menerjemahkan IP address host BB menjadi alamat Ethernet, maka host A harus melakukan dua hal yaitu: Mengirimkan paket ARP request pada seluruh host di network menggunakan alamat broadcast Ethernet (FF:FF:FF:FF:FF:FF) untuk meminta jawaban ARP dari host B, lihat gambar 1.10 Menempatkan datagram IP yang hendak dikirim dalam antrian. Paket ARP request yang dikirim host A kira-kira berbunyi Jika IP address-mu adalah 132.96.11.2, mohon beritahu alamat Ethernetmu Karena paket ARP request dikirim ke alamat broadcast Ethernet, setiap

interface Ethernet komputer yang ada dalam satu subnet (jaringan) dapat mendengarnya. Setiap host dalam jaringan tersebut kemudian memeriksa apakah IP addressnya sama dengan IP address yang diminta oleh host A.



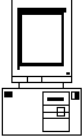
Gambar 1. 10 Menempatkan datagram IP

Host B yang mengetahui bahwa yang diminta oleh host A adalah IP address yang dimilikinya langsung memberikan jawaban dengan mengirimkan paket ARP response langsung ke alamat ethernet pengirim (host A), seperti terlihat pada gambar 1.11. Paket ARP request tersebut kira-kira berbunyi IP address 132.96.11.2 adalah milik saya, sekarang saya berikan alamat ethernet saya .



Gambar 1. 11 Respon Paket ARP

Paket ARP request dari host B tersebut diterima oleh host A dan host A kemudian menambahkan entri IP addresss host B beserta alamat Ethernet-nya ke dalam cache ARP.



Alamat IP	Alamat Ethernet
132.96.11.1	0:80:48:e3:d2:69
132.96.11.2	0:80:ad:17:96:34

132.96.11.1

Gambar 1. 12 Paket ARP diterima dari Host B ke A

Saat ini host A telah memiliki entri untuk host B di tabel cache ARP, dengan demikian datagram IP yang semula dimasukkan ke dalam antrian dapat diberi header Ethernet dan dikirim ke host B. Secara ringkas proses ARP adalah:

- Host mengirimkan paket ARP request dengan alamat broadcast Ethernet
- Datagram IP yang dikirim dimasukkan ke dalam antrian.
- Paket ARP respon diterima host dan host mengisi tabel ARP dengan entri baru.
- Datagram IP yang terletak dalam antrian diberi header Ethernet.
- Host mengirimkan frame Ethernet ke jaringan.

Setiap data ARP yang diperoleh disimpan dalam tabel cache ARP dan cache ini diberi umur. Setiap umur entri tersebut terlampaui, entri ARP dihapus dari tabel dan untuk mengisi tabel. Jika host akan mengirimkan datagram ke host yang sudah dihapus dari cache ARP, host kembali perlu melakukan langkah-langkah diatas. Dengan cara ini dimungkinkan terjadinya perubahan isi cache ARP yang dapat menunjukkan dinamika jaringan. Jika sebuah host di jaringan dimatikan, maka selang beberapa saat kemudian entri ARP untuk host tersebut dihapus karena kadaluarsa. Jika card ethernetnya diganti, maka beberapa saat kemudian entri ARP host berubah dengan informasi alamat ethernet yang baru.

c) Enkapsulasi HDLC (*High-Level Data Link Control*)

Pada umumnya, komunikasi serial berdasarkan protokol character oriented. Protokol bit oriented lebih efisien tetapi mereka juga proprietary. Pada tahun 1979, ISO menyetujui HDLC sebagai standar untuk protokol bit oriented pada data link layer yang mengenkapsulasi data pada synchronous serial data link. Sejak 1981, ITU-T telah mengembangkan berbagai seri dari pengembangan HDLC.

Beberapa contoh dari protokol tersebut adalah:

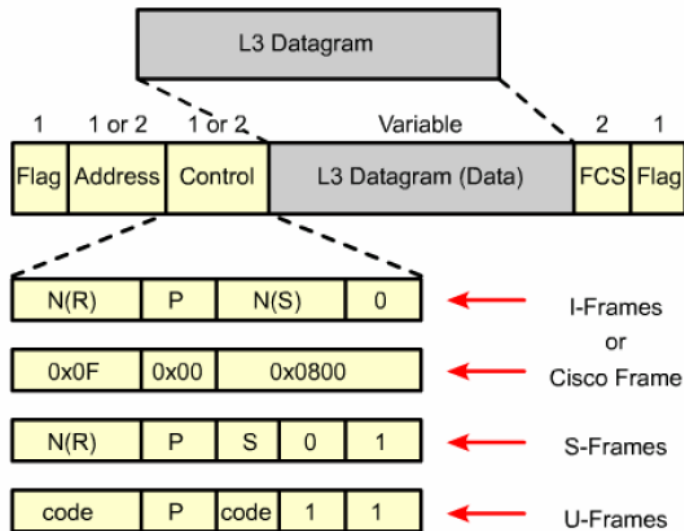
- 1) Link Access Procedure, Balanced (LAPB) untuk X.25
- 2) Link Access Procedure on the D channel (LAPD) untuk ISDN
- 3) Link Access Procedure for Modem (LAPM) dan PPP untuk modem
- 4) Link Access for Frame Relay (LAPF) untuk Frame Relay.

HDLC menggunakan transmisi serial synchronous yang menyediakan komunikasi bebas error diantara 2 titik. HDLC menjelaskan struktur frame Layer 2 yang memperbolehkan flow control dan error control menggunakan acknowledgment dan windowing scheme. Setiap frame memiliki format yang sama, baik frame data atau control. Pada router merk tertentu, HDLC yang digunakan merupakan proprietary sendiri. HDLC menggunakan sebuah field proprietary. Field ini memungkinkan beberapa network layer protocol untuk berbagi jalur serial yang sama. HDLC merupakan default Layer 2 protokol untuk interface serial.

HDLC mempunyai tiga tipe frame, dimana setiap frame memiliki format yang berbeda yaitu:

- 1) Information frame (I-frames), membawa data untuk dikirimkan.
Menambahkan flow dan error control, dimana data mungkin minta dikirimkan ulang (piggyback).
- 2) Supervisory frame (S-frames), menyediakan mekanisme request dan respond ketika piggybacking tidak digunakan.
- 3) *Unnumbered frames (U-frames)*, menyediakan tambahan fungsi pengontrolan jalur seperti setup koneksi dll.

Satu atau 2 bit pertama dari field control mengidentifikasikan tipe frame. Pada *field control* dari *I-frames*, *send-sequence number* menunjuk pada nomor frame yang dikirimkan selanjutnya. *Receive sequence number* menunjukan nomer dari frame yang diterima selanjutnya. Kedua pengirim dan penerima memelihara *send* dan *receive sequence number*.



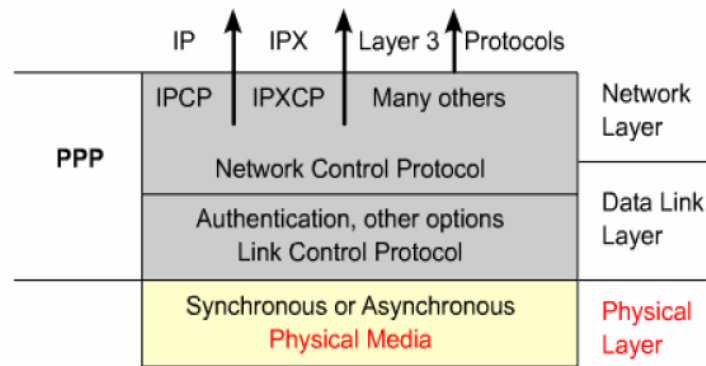
Gambar 1. 13 HLDC

HDLC dapat digunakan untuk protokol point-to-point yang dapat digunakan pada leased line diantara dua perangkat dengan merk sejenis. Ketika berkomunikasi dengan perangkat dengan merk yang berbera maka dapat menggunakan PPP.

d) Enkapsulasi PPP (*Point to Point Protocol*)

PPP menggunakan arsitektur berlapis. Arsitektur berlapis adalah model logik, desain atau cetak biru yang membantu komunikasi diantara lapisan interkoneksi. OSI model adalah arsitektur berlapis yang digunakan pada jaringan. PPP menyediakan metode untuk mengenkapsulasi multi-protocol datagram melalui jalur point-to-point dan menggunakan lapisan data link untuk mengetes koneksi. PPP terdiri dari dua sub-protocol yaitu:

- 1) Link Control Protocol (LCP), digunakan untuk membangun jalur point-to-point
- 2) Network Control Protocol (NCP), digunakan untuk mengkonfigurasi berbagai protokol network layer.



Gambar 1. 14 Point-toPoint Protocol

PPP dapat mengkonfigurasi berbagai tipe interface fisik yaitu:

- 1) Asynchronous serial
- 2) Synchronous serial
- 3) High-Speed Serial Interface (HSSI)
- 4) ISDN

PPP menggunakan LCP untuk menegosiasikan dan pilihan kontrol setup pada data link WAN. PPP menggunakan komponen NCP untuk enkapsulasi dan pilihan negosiasi untuk berbagai protokol network layer. LCP berada di atas physical layer dan digunakan untuk membangun, mengkonfigurasi dan mengetes koneksi data link.

PPP juga menggunakan LCP untuk secara otomatis menyetujui pilihan format enkapsulasi seperti dibawah ini:

- 1) Authentication, pilihan otentikasi membutuhkan sisi pemanggil untuk memasukkan informasi untuk membantu terpanggil mendapatkan ijin sesuai setting network administrator jaringan terpanggil. Ada dua pilihan otentikasi yaitu Password Authentication Protocol (PAP) dan Challenge Handshake Authentication Protocol (CHAP).
- 2) Compression, pilihan kompresi meningkatkan efektifitas throughput pada koneksi PPP dengan mengurangi sejumlah data pada frame yang harus melalui jalur. Protokol akan medekompres frame pada tujuan. Dua protokol kompresi yang tersedia adalah Stacker dan Predictor.
- 3) Error detection, mekanisme error detection dengan PPP memungkinkan proses untuk mengidentifikasi kondisi.

- 4) Multilink, CISCO IOS Release 11.1 dan sesudahnya mendukung PPP multilink. Ini alternatif yang menyediakan load balance melalui interface router dimana PPP digunakan.
- 5) PPP Callback, untuk penanganan keamanan di masa yang akan datang. Dengan pilihan LCP, sebuah router dapat berperilaku sebagai client callback atau sebagai server callback. Client melakukan inisialisasi call, meminta agar bias di callback, dan mengakhiri callback. Router callback menjawab inisialisasi call dan melakukan panggilan jawaban ke client berdasarkan konfigurasinya.

LCP juga akan melakukan:

- 1) Menangani berbagai batas dari ukuran paket
- 2) Mendeteksi kesalahan konfigurasi yang umum
- 3) Mengakhiri jalur
- 4) Memastikan ketika jalur berfungsi baik atau ketika sedang rusak

PPP mengijinkan berbagai protokol network layer untuk beroperasi pada jalur komunikasi yang sama. Untuk setiap protokol network layer yang digunakan, disediakan NCP yang berbeda. Sebagai contoh, Internet Protocol (IP) menggunakan IP Control Protocol (IPCP), dan Internetwork Packet Exchange (IPX) menggunakan Novell IPX Control Protocol (IPXCP). NCP termasuk field field functional yang berisi kode standar untuk mengidentifikasi protokol network layer yang digunakan.

Field pada frame PPP adalah sebagai berikut:

- 1) *Flag*, mengidentifikasi awal atau akhir frame dan konsisten berisi urutan biner 01111110.
- 2) *Address*, berisi broadcast address standar, dimana urutan biner 11111111. PPP tidak memberikan alamat individu untuk setiap station.
- 3) *Control*, 1 byte yang berisi urutan biner 00000011, dimana panggilan untuk transmisi data user tidak berurut.
- 4) *Protocol*, 2 byte yang mengidentifikasi protokol yang di enkapsulasi data field data pada frame.
- 5) *Data*, 0 atau lebih byte yang berisi datagram untuk protokol yang dispesifikasikan pada field protocol. Akhir field data dapat ditemukan dengan lokasi dari urutan flag penutup. Maksimum panjang field default adalah 1.500 byte.
- 6) *FCS*, normalnya 16 bit atau 2 byte yang menunjukkan karakter extra yang ditambahkan pada frame untuk fungsi error control.

Membangun sesi PPP melalui tiga fase. Fase tersebut adalah pembangunan jalur, autentikasi dan fase network layer. Frame LCP digunakan untuk memastikan kerja setiap LCP fase. Tiga kelas dari LCP frame yang digunakan untuk PPP adalah:

- 1) Frame Pembangunan Jalur digunakan untuk membangun dan mengkonfigurasi jalur.
- 2) Frame Terminasi Jalur digunakan untuk mengakhiri jalur.
- 3) Frame Pemeliharaan Jalur digunakan untuk mengatur dan melakukan debug terhadap jalur.

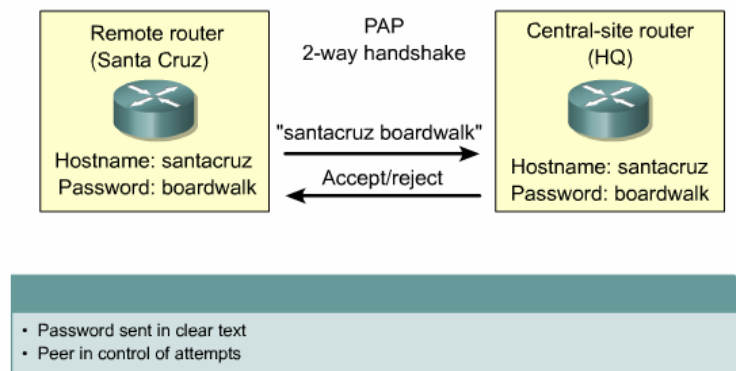
Tiga sesi pembangunan PPP adalah:

- a. Fase Pembangunan Jalur, pada fase ini perangkat PPP mengirim LCP frame untuk mengkonfigurasi dan mengetes jalur data. Frame LCP berisi configuration option field yang memungkinkan perangkat untuk menegosiasikan pilihan yang digunakan seperti maksimum transmission unit (MTU), kompresi dari beberapa field PP dan protokol otentikasi field. Jika sebuah pilihan konfigurasi tidak termasuk dalam paket LCP, nilai default untuk konfigurasi tersebut yang digunakan. Sebelum beberapa paket network layer dapat dikirimkan, LCP pertama tama harus membuka koneksi dan menegosiasikan parameter konfigurasi. Fase ini selesai ketika sebuah frame configuration acknowledgment telah dikirim dan diterima.
- b. Fase Authentication, setelah jalur dibangun dan protokol otentikasi diputuskan, maka melakukan proses otentikasi. Otentikasi jika digunakan mengambil tempat sebelum memasuki fase protokol network layer. Sebagai bagian dari fase ini, LCP juga memperbolehkan sebuah pilihan untuk memastikan kualitas jalur. Link ini di tes untuk memastikan kualitas jalur apakah cukup baik untuk membawa data protokol network layer.
- c. Fase Protokol Network Layer, pada fase ini perangkat PPP mengirim paket NCP untuk memilih dan mengkonfigurasi satu atau lebih protokol network layer seperti IP. Setiap protokol network layer yang telah dikonfigurasi, satu paket dari setiap network layer dapat dikirimkan melalui jalur. Jika LCP menutup jalur, hal tersebut diinformasikan ke protokol network layer sehingga mampu melakukan aksi yang sesuai. Perintah show interface menunjukkan kondisi LCP dan NCP dalam konfigurasi PPP. Jalur PPP meninggalkan konfigurasi untuk komunikasi jalur sampai frame LCP atau NCP menutup jalur atau sampai timer inactivity habis untuk mengintervensi pengguna.

Pilihan otentikasi membutuhkan sisi pemanggil dari jalur memasuki informasi otentikasi. Hal ini membantu untuk memastikan pengguna memiliki ijin dari network

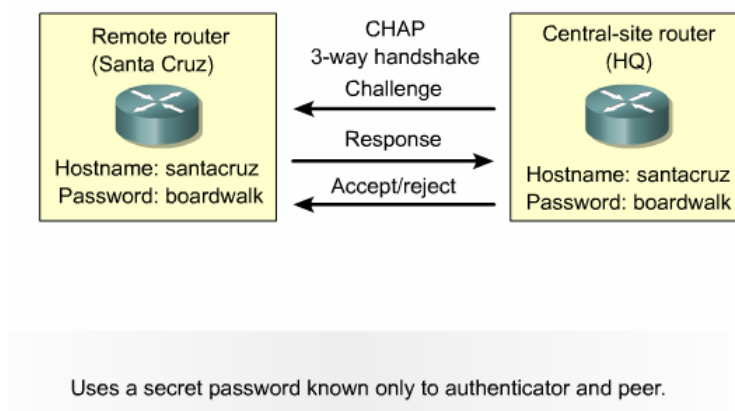
administrator untuk membuat panggilan. Ketika mengkonfigurasi otentikasi PPP, network administrator dapat memilih Password Authentication Protocol (PAP) atau Challenge Handshake Authentication Protocol (CHAP). Umumnya CHAP lebih sering digunakan.

PAP menyediakan metode sederhana untuk meremote node untuk mengidentifikasi pembangunan, menggunakan two way handshake. Setelah jalur PPP dibangun, username/password secara terus menerus dikirim dari node tujuan melalui jalur sampai otentikasi telah disetujui atau koneksi diakhiri. PAP bukan merupakan protokol yang kuat. Password dikirim melalui jalur dengan bentuk clear text dan tidak ada proteksi. Remote node yang akan mengontrol frekuensi dan waktu dari masuknya login.



Gambar 1. 15 PAP 2-way

CHAP digunakan pada startup jalur dan secara periodic di verifikasi untuk mengidentifikasi remote node menggunakan three-way handshake. CHAP menampilkan pembangunan jalur dan diulang selama jalur dibangun.



Gambar 1. 16 CAHP 3-way

Setelah fase pembangunan jalur PPP selesai, router local mengirim sebuah pesan challenge ke remote node. Remote node merespon dengan nilai yang dikalkulasi menggunakan fungsi one-way hash, dimana umumnya Message Digest 5 (MD5). Responsnya berdasarkan password dan pesan challenge. Lokal router akan mengecek respon dengan kalkulasi miliknya sendiri dengan nilai hash yang diharapkan.

Jika nilai sesuai, otentikasi di setuju, sebaliknya koneksinya akan segera diakhiri. CHAP menyediakan proteksi melawan serangan playback melalui penggunaan berbagai nilai challenge yang unik dan tidak dapat diprediksi. Jika challenge unik dan acak, maka nilai hasil hash juga akan unik dan acak. Penggunaan challenge yang diulang ulang akan meningkatkan waktu untuk sebuah serangan. Router local atau server otentikasi pihak ketiga yang akan mengontrol frekuensi dan waktu challenge.

B. Jaringan Nirkabel

Jaringan nirkabel atau yang biasa disebut dengan Wireless adalah koneksi antar satu perangkat dengan perangkat lainnya tanpa menggunakan media kabel, namun menggunakan media gelombang radio. Dalam hal ini perangkat yang dihubungkan adalah perangkat komputer, baik komputer desktop (PC), komputer jinjing (laptop) ataupun perangkat PC mobile seperti smartphone dan sebagainya.

1. Pengenalan Jaringan Nirkabel

Jaringan nirkabel atau wireless network adalah sebuah teknologi jaringan telekomunikasi dan informasi yang digunakan untuk berbagai peralatan teknologi informasi yang tidak menggunakan kabel. Jaringan nirkabel sudah umum digunakan pada jaringan komputer baik yang terkoneksi jarak dekat ataupun koneksi jarak jauh menggunakan satelit. *Jaringan nirkabel* pada umumnya menghubungkan satu sistem komputer dengan sistem telekomunikasi lainnya dengan berbagai media transmisi nirkabel, antara lain: microwave, radiowave, maupun dengan infra red.

Teknologi primer yang banyak dipakai dalam jaringan nirkabel adalah standar protokol 802.11, yang juga dikenal sebagai Wi-Fi. Protokol 802.11 merupakan protokol radio. (802.11a, 802.11b, dan 802.11g) telah menikmati kesuksesan yang luar biasa di Amerika Serikat dan Eropa. Dengan menggunakan keluarga protokol yang sama, para produsen diseluruh dunia telah membuat piranti yang saling interoperable. Keputusan ini telah terbukti menjadi ilham yang luar biasa terhadap industri dan para konsumen. Konsumen dapat menggunakan peralatan yang menggunakan 802.11 tanpa harus takut

terhadap ketergantungan terhadap suatu pedagang. Hasilnya, konsumen bisa membeli peralatan murah dalam volume yang sudah menguntungkan para produsen. Jika para produsen memilih untuk tetap memakai protokol mereka sendiri, sepertinya tidak mungkin jaringan nirkabel dapat semurah dan bisa ada dimana-mana seperti sekarang ini.

Electrical and Electronics Engineers (IEEE), telah memperkenalkan beberapa teknologi-teknologi *jaringan nirkabel* seperti WiFi (IEEE 802.11a/b/g/n) dan Fixed WiMAX (IEEE 802.16d). Dengan pengenalan teknologi nirkabel tersebut, sektor telekomunikasi mulai menyaksikan tabrakan antara dua platform jaringan yang berbeda: antara jaringan selular dan juga nirkabel. Namun, ada perbedaan antara mobilitas yang bisa ditawarkan oleh teknologi seluler dan peningkatan kecepatan data yang ditawarkan oleh jaringan nirkabel. Perbedaan kesenjangan ini dengan penggunaan teknologi WiMAX (IEEE 802.16e). Di dalam teknologi jaringan WiMAX Mobile, modul manajemen mobilitas diperkenalkan ke dalam jaringan Fixed WiMA tetap tersedia untuk mobilitas bagi pengguna. Hal ini memungkinkan sebuah proses yang dikenal sebagai sebagai 'penyerahan' (atau hand-over) antara satu menara transmisi ke menara transmisi yang lain. Proses penyerahan ini mengizinkan teknologi WiMAX sebagai jaringan 'bergerak' sepenuhnya. Mobile WiMAX juga dilihat sebagai teknologi yang potensial untuk menjembatani jurang di antara jaringan nirkabel saat ini dan juga jaringan masa depan, lebih dikenal sebagai Beyond 3G (B3G) yang distandar oleh International Telecommunications Union (ITU). Dengan spektrum kecepatan tinggi dan jaringan inti berdasarkan IP sepenuhnya, platform jaringan Mobile WiMAX dianggap sesuai dengan platform yang dipertimbangkan untuk evolusi berikutnya, yaitu jaringan Generasi Keempat (4G).

2. Perangkat Jaringan Nirkabel

Dalam membangun sebuah jaringan nirkabel, diperlukan beberapa perangkat atau device utama di antaranya adalah : antenna, access point dan wireless adapter. Pada bab ini akan dijelaskan karakteristik serta jenis-jenis dari perangkat jaringan nirkabel tersebut.

a. Antena

Antena adalah alat yang digunakan untuk menambahkan daya pancar dari sinyal analog. Dan akan menyebarkan daya pancar melalui suatu medium udara. Antena mengkonversi gelombang elektrik menjadi gelombang elektromagnetik. Kekuatan antena untuk menerima atau mengirim sinyal dikenal sebagai gain/penguatan antena.

Sedangkan satuan untuk mengukur penguatan antenna adalah dBi. Antena sendiri berfungsi untuk mengubah sinyal listrik menjadi sinyal elektromagnetik kemudian meradiasikannya. Namun antena juga dapat menerima sinyal elektromagnetik dan mengubahnya menjadi sinyal listrik. Antena Wifi juga mempunyai fungsi yang sama dengan antena pada umumnya. Secara spesifik, antena ini bertugas untuk menerima dan menyalurkan sinyal WiFi sehingga perangkat laptop maupun gadget lainnya dapat menerima sinyal tersebut. Jenis – jenis antena dapat digolongkan menjadi 2 jenis utama yaitu :

1) Antena Directional (Antena Pengarah)

Jenis antena ini digunakan pada sisi client dan mempunyai gain yang sangat tinggi yang diarahkan ke *Access point*. Jenis antena ini disebut juga dengan istilah antena narrow bandwidth, yaitu antena yang memiliki sudut pemancaran yang kecil dengan daya lebih terarah, jaraknya jauh dan tidak bisa menjangkau area yang luas, antena directional mengirim dan menerima sinyal radio hanya pada satu arah, umumnya pada fokus yang sangat sempit, dan biasanya digunakan untuk koneksi *point to point*, atau multiple point, macam antena direksional seperti antena grid, dish “parabolic”, yagi, dan antena sectoral.

a) Antena Grid, Antena WiFi jenis ini mempunyai bentuk seperti jaring. Cakupan antena grid hanya searah sehingga antena jenis ini biasanya dilengkapi dengan pasangan antena yang dipasang di tempat lain atau antena pemancar sinyal. Antena ini merupakan salah satu antena wifi yang populer. Sudut pola pancaran antena ini lebih fokus pada titik tertentu sesuai pemasangannya. Antena tersebut diarahkan ke antena pemancar sehingga sinyal yang diterima akan lebih kuat. Fungsi antena grid adalah menerima dan mengirim sinyal data melalui sistem gelombang radio 2,4 MHz.

b) Antena Parabolic, Antena jenis ini umumnya digunakan untuk jarak menengah atau jarak sedang dan mempunyai penguatan antara 18 - 28 dBi. Kelebihan antena parabola di antaranya adalah: Dapat digunakan untuk menerima 3 satellite sekaligus tanpa harus menggerakkan antenna, Dapat menampilkan gambar dari semua TV dari satelit yang ditangkap dalam sekejap, Kondisi permanen sehingga tidak gampang goyah terhadap posisi, Kualitas sinyal dapat maksimum.

- c) Antena Sectoral, Jenis antena ini mempunyai penguatan antara 10 - 19 dBi dan tingginya penguatan ini dikompensasi dengan pola radiasi yang sempit dari 45 – 1800. Bentuk antena sectoral hampir sama dengan antena omni. Antena ini mampu menampung hingga 5 klien. Biasanya antena sektoral dipasang secara horizontal maupun tegak lurus.
 - d) Antena Yagi, mempunyai bentuk menyerupai ikan teri. Sama seperti antena grid, antena ini juga mempunyai cakupan yang searah. Perbedaan utama dari antena Yagi dengan Grid adalah antena ini cukup jarang digunakan dalam jaringan. Antena Yagi umumnya digunakan untuk jarak pendek karena penguatannya rendah. Dan mempunyai penguatan antara 7 - 19 dBi. Biasanya antena ini akan diarahkan ke pemancar. Antena ini terdiri dari 3 bagian, meliputi driven, reflector, dan director. Driven merupakan titik catu dari kabel antena. Panjang fisik driven biasanya adalah setengah panjang gelombang frekuensi radio yang diterima atau dipancarkan. Reflektor merupakan bagian belakang antena yang digunakan untuk memantulkan sinyal. Panjang fisik reflector biasanya lebih panjang dari driven. Sedangkan director merupakan bagian pengarah antena. Bagian ini ukurannya lebih pendek dari driven.
 - e) Antena 8 Quad, Antena ini termasuk jenis antena sektoral. Pasalnya pola radiasi antena berada satu arah dengan sudut arah yang lebar. Antena 8 Quad cocok untuk antena access point di mana klien berada di area tertentu.
 - f) Antena Wajan Bolic, Antena ini dinamai dengan Wajan Bolic karena antena ini hampir sama dengan antena parabolic. Antena ini cukup sederhana karena bahan untuk parabolic disc menggunakan wajan atau alat dapur yang sering digunakan untuk memasak. Antena Wajan Bolic berfungsi untuk memperkuat sinyal nirkabel dari hotspot yang karena lokasinya terlalu jauh sulit diterima oleh USB Wireless Adapter jika hanya langsung terhubung dengan laptop atau PC.
- 2) Antena Omnidirectional (Omni)
- Antena WiFi ini memiliki bentuk menyerupai tongkat namun lebih kecil. Antena Omni sering digunakan pada *Access point* (AP). Antena jenis ini mempunyai pola radiasi 360 derajat. Antena ini mempunyai sudut pancaran yang besar (wide beamwidth) yaitu 3600. Cakupan antena ini menyebar ke semua arah dan membentuk seperti semacam lingkaran. Jenis antena ini biasanya digunakan pada jaringan WAN

dengan tipe konfigurasi Point to Multi Point atau P2MP. Antena Omni berfungsi untuk melayani cakupan area yang luas tetapi dengan jangkauan yang pendek. Dengan jangkauan area yang luas, kemungkinan di area ini juga akan terkumpul sinyal lain yang tidak diinginkan. Jenis antena ini sangat cocok digunakan untuk sistem koneksi point to multipoint atau koneksi hotspot. penguatan dari antena omni sangat rendah yaitu hanya sekitar 3 - 10 dBi. Berikut ini adalah gambar antena Omni :



Gambar 1. 17 Antena Omni

3. Jaringan Nirkabel Di Masa Depan

Di masa akan datang, layanan untuk jaringan nirkabel berbasis lokasi diidentifikasi sebagai kunci utama di dalam mengeksplotasi kecanggihan teknologi nirkabel. Pada masa itu, layanan berbasis lokasi akan menjadi 'tambang emas' kepada perusahaan telekomunikasi maupun perusahaan pemasaran dalam meraup keuntungan masing-masing. Saat ini, ada beberapa teknologi nirkabel berbasis lokasi yang telah mampu kita gunakan, misalnya deteksi lokasi pengguna di dalam peta Google, tanpa menggunakan bantuan sinyal dari satelit, yaitu. GPS yang sedang melejit di gunakan di dalam situs jejaring sosial seperti Facebook dan Twitter. Pengguna juga akan dari layanan berbasis lokasi ini, di mana pencarian arah, informasi dan daftar kontak bisa didapatkan melalui peta dengan menggunakan konsep direktori publik seperti Yellow Pages.

Siasat pemasaran juga akan berubah secara dinamis, di mana pemasaran berdasarkan lokasi akan menjadi sebagai katalisator pada pemasaran digital. Teknologi pemasaran ini hanya perlu mendeteksi posisi pengguna perangkat bergerak tersebut dan

akan mengirim pesan ke pengguna tentang keberadaan toko perusahaan tersebut beberapa meter di depan pengguna dan pesan juga berisi penjualan terakhir perusahaan tersebut dan mengusulkan beberapa produk lain yang bisa dimanfaatkan oleh pengguna. Bahkan, perusahaan tersebut mampu menganalisa tentang biodata pengguna tersebut dari situs sosialnya, seperti Facebook dan Twitter, dan membuat saran tentang beberapa produk yang sesuai dengan cara hidup pengguna tersebut. Di sini bisa dilihat bahwa informasi pribadi pengguna dapat digunakan dan dimanipulasi oleh perusahaan-perusahaan untuk manfaat mereka di dalam melariskan penjualan di masa depan. Jadi tidak heran pada masa depan, akan ada pengguna yang sanggup membayar pada harga yang begitu tinggi agar informasi pribadi mereka tidak diungkapkan secara umum.

Selain isu informasi pribadi, keamanan jaringan komputer dan pengguna bakal terancam di masa mendatang, terutama dari hacker dan juga virus. Pada masa depan, diharapkan semua pengguna akan berbagi informasi pribadi mereka melalui jejaring sosial. Hal ini bisa menimbulkan konflik yang serius di dalam masyarakat, di mana perlindungan identitas dan informasi pribadi menjadi salah satu tantangan utama di dalam memastikan teknologi nirkabel tidak menimbulkan masalah dan risiko pada pengguna. Salah satu solusi adalah dengan memperkenalkan identitas unik untuk setiap pengguna perangkat bergerak tersebut, atau Mobile DNA. Mobile DNA tersebut mampu menyimpan semua catatan transaksi dan juga informasi-informasi terkait pengguna. Untuk memastikan data tersebut tidak disalahgunakan, Mobile DNA hanya dapat diakses oleh pelaksana sistem hukum saja seperti polisi.

Selain bermanfaat untuk pengguna, pada skala besar, teknologi jaringan nirkabel di masa depan diperkirakan akan mengubah bentuk jaringan topografi. Diraikan hampir semua daerah kota utama akan diliputi oleh jaringan nirkabel, seperti WiMAX dan WiFi, di mana ia tersedia secara gratis atau dibiayai oleh otoritas lokal. Selain itu, perangkat bergerak diperkirakan akan menjadi sumber pemasaran terbesar, mengatasi komputer pribadi dan media massa elektronik lainnya yang berada di pasar sekarang. Pada waktu itu, diperkirakan sebanyak 50% dari seluruh populasi manusia di muka bumi akan memiliki setidaknya satu perangkat bergerak, termasuk di Afrika. Saat ini, benua tersebut memiliki nilai tembusan jaringan nirkabel yang begitu rendah. Ini disebabkan oleh masalah geografi dan juga faktor ekonomi, sampai melibatkan biaya yang begitu tinggi untuk menginstal sebuah situs transmisi. Namun, usaha ke arah membangun jaringan nirkabel masih

dilakukan di benua berikut. Dan pada masa depan, diharapkan Afrika akan menyaksikan penggunaan perangkat bergerak untuk tujuan kampanye politik.

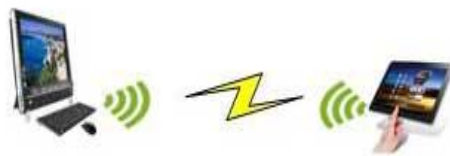
Teknologi jaringan nirkabel bergerak maju begitu cepat. Mungkin prediksi tersebut hanya tinggal menjadi khayalan semata hanya saja menentukan. Persoalan utama adalah sejauh mana kita sebelum dapat menikmati teknologi jaringan nirkabel tersebut.

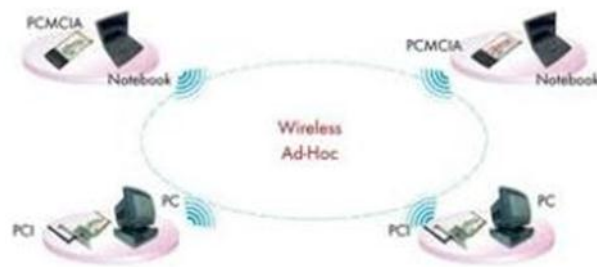
4. Klasifikasi berdasarkan topologi jaringan

Topologi dalam suatu jaringan dapat didefinisikan sebagai aturan atau cara menghubungkan komputer (device) satu dengan yang lain sehingga membentuk suatu jaringan. Dapat dikatakan pula bahwa topologi merupakan gambaran secara fisik dari pola hubungan antara komputer yang saling berkomunikasi. Kapanpun dua atau lebih komputer saling berkomunikasi satu sama lain, topologi jaringan secara otomatis akan terbentuk. Tidak seperti jaringan kabel yang memiliki banyak topologi, jaringan nirkabel hanya mempunyai dua topologi. Berdasarkan standar IEEE 802.11 yang menangani Wireless LAN (WLAN) & Mesh (Wi-Fi Certification), dua topologi jaringan nirkabel adalah topologi Ad-Hoc dan topologi infrastruktur (infrastructure).

a. Topologi Ad-Hoc

Topologi Ad-Hoc merupakan jaringan nirkabel sederhana dimana komunikasi yang terjadi antara dua atau lebih komputer dilakukan secara langsung tanpa melalui perantara berupa wireless access point. Topologi Ad-Hoc dapat pula dikatakan sebagai koneksi peer-to-peer atau computer-to-computer karena koneksi jaringan dilakukan langsung antar komputer. Kelemahan topologi ini adalah tidak bisa berkomunikasi dengan komputer yang menggunakan kabel serta jangkauan antar komputer yang terbatas. Topologi Ad-Hoc dikenal pula dengan nama Independent Basic Service Set (IBSS). Berikut ini adalah gambaran dari topologi Ad-Hoc:





Gambar 1. 18 Topologi Jaringan nirkabel Ad-Hoc

b. Topologi infrastruktur

Topologi infrastruktur merupakan jaringan nirkabel dimana komunikasi yang terjadi antara dua atau lebih komputer menggunakan perantara berupa wireless access point. Access point bertindak seperti hub atau switch pada jaringan kabel (wired networking) dan menjadi sentral atau pusat jaringan nirkabel. Pada topologi infrastruktur, perangkat wireless (wireless adapter) komputer berkomunikasi melalui access point, tidak langsung ke perangkat wireless komputer yang lain. Selain sebagai sentral atau pusat jaringan nirkabel pada topologi infrastruktur, access point juga dapat dihubungkan dengan koneksi jaringan kabel LAN. Topologi infrastruktur dikenal pula dengan nama Basic Service Set (BSS). Gambar 2.2 adalah gambar topologi infrastruktur:



Gambar 1. 19 Topologi Jaringan nirkabel Infrastruktur

Pada gambar 1.19 di atas, terlihat bahwa ketiga laptop terhubung ke Wireless AP yang sama. Karakteristik teknis termasuk kelebihan dan kelemahan dari kedua jenis topologi atau mode akses ini akan dibahas secara lebih mendalam di bab uraian materi kegiatan pembelajaran 6 tentang konfigurasi jaringan nirkabel.

Berdasarkan topologi jaringan, jaringan nirkabel yang khusus menggunakan perangkat *Access point* (AP) ataupun *Base Transceiver Station* (BTS) dikelompokkan menjadi 2 jenis topologi yaitu:

1) Point-to-point (P2P)

Jaringan point to point adalah jaringan nirkabel yang menghubungkan antar BTS atau antar *access point*. Frekuensi yang digunakan adalah 2.5 GHz, 5 GHz, 10 GHz, 15 GHz dan seterusnya. Teknologi ini harus memenuhi kriteria LOS = *Line of Sight*, yaitu suatu kondisi di antara pemancar dan penerima terlihat tanpa ada penghalang. Boleh ada penghalang di antaranya tetapi tidak boleh masuk dalam area Jari-jari pertama Fresnel Zone (Fresnel Zone 1). Daya yang digunakan untuk perangkat wireless juga harus disesuaikan, harus ada cadangan power jika terjadi hujan dan redaman atmosfer. Cadangan power untuk mengantisipasi redaman disebut Fading Margin. Fading margin merupakan ukuran level daya yang harus dicadangkan yang besarnya merupakan selisih antara daya rata-rata yang sampai di penerima dan level sensitivitas penerima. Perhitungan daya yg dibutuhkan antara 2 titik dengan jarak tertentu disebut Link Budget. Perhitungan link budget merupakan perhitungan level daya yang dilakukan untuk memastikan bahwa level daya penerimaan lebih besar atau sama dengan level daya threshold ($RSL \geq R_{th}$). Tujuannya untuk menjaga keseimbangan gain dan loss guna mencapai SNR yang diinginkan di receiver. Sehingga jarak maksimum antara transmitter dan receiver dapat bekerja dengan baik dapat ditentukan. Topologi jaringan nirkabel point-to-point biasanya digunakan untuk jaringan backbone/trunk atau jaringan akses berkecepatan tinggi. Berikut ini adalah gambar ilustrasi topologi jaringan nirkabel point-to-point.



Gambar 1. 20 Topologi Jaringan *Point to Point*

Pada gambar topologi jaringan Point to point di atas terlihat komunikasi data antara kantor pusat (Main Office) dengan kantor cabang (branch office) di sebuah instansi atau perusahaan.

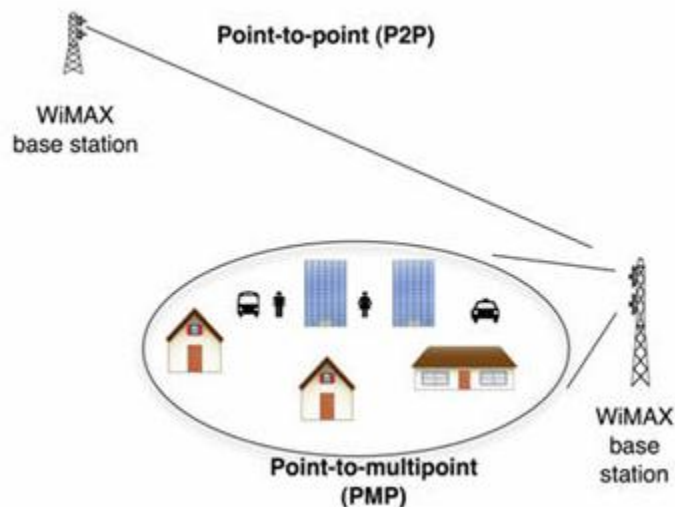
2) Point-to-Multipoint (PMP)

Topologi jaringan point to multipoint adalah topologi jaringan nirkabel yang menghubungkan satu Access point (AP) atau BTS ke banyak titik (node) perangkat wireless (WiFi). Topologi jaringan nirkabel Point to multi point (P2MP) biasanya digunakan untuk jarak jangkauan yang relatif dekat. Secara garis besar, frekuensi dan perhitungan power untuk topologi jaringan point-to-multipoint hampir sama dengan topologi jaringan point-to-point. Hanya saja jaringan point-to-multipoint ada yang mampu membentuk jaringan yang baik walaupun diantaranya terdapat penghalang (NLOS=Not Line of Sight). Hal ini karena mekanisme propagasi gelombang yang bersifat multipath atau banyak jalur yang terpancar dari sebuah access point setelah gelombang tersebut memantul pada saat membentur penghalang atau obstacle. Teknologi yang digunakan adalah OFDM (Orthogonal Frequency Division Multiplexing). Teknologi ini secara teknis memanfaatkan penghalang/obstacle sebagai media pemantul sinyal OFDM yang mempunyai banyak carrier (multi-carrier) sampai ke tujuan, sehingga sinyal yg datang dari

berbagai arah pantulan sampai di sisi penerima dibuat saling memperkuat. Jika jarak antar antenna tidak ada penghalang maka jangkauannya akan lebih jauh. Berikut ini adalah beberapa keunggulan dari topologi jaringan Point-to-Multipoint :

- a) Mampu membentuk jaringan yang baik walaupun diantaranya terdapat penghalang atau biasanya disebut NLOS (*Not Line of Sight*).
- b) 1 buah akses point dapat melayani beberapa station
- c) Dapat sebagai base station
- d) Menggunakan antenna omni atau sectoral
- e) Jika client berada pada satu area kita bisa menggunakan flat panel
- f) Menggunakan standard 802.11 b/g biar semua device bisa terkoneksi.

Dewasa ini telah berkembang teknologi wireless terbaru yaitu teknologi WiMAX (Worldwide Interoperability for Microwave Access). Teknologi nirkabel ini memungkinkan BTS atau access point (AP) dapat berkomunikasi dengan berbagai remote/client yang berbeda merk atau multivendor, dengan kecepatan yang sangat tinggi. Teknologi WiMax menggunakan standar baru nirkabel IEEE 802.16 dengan kecepatan 11 mega byte (MB) per detik. Wi-Max bisa melayani akses internet nirkabel hingga jangkauan mencapai jarak puluhan kilometer. Topologi Point to MultiPoint (PMP) ini ditujukan untuk membentuk wireless Metropolitan Area Network (MAN). Gambar berikut menjelaskan keterkaitan antara kedua topologi jaringan nirkabel tersebut :



Gambar 1. 21 Topologi Jaringan *Point to multipoint*

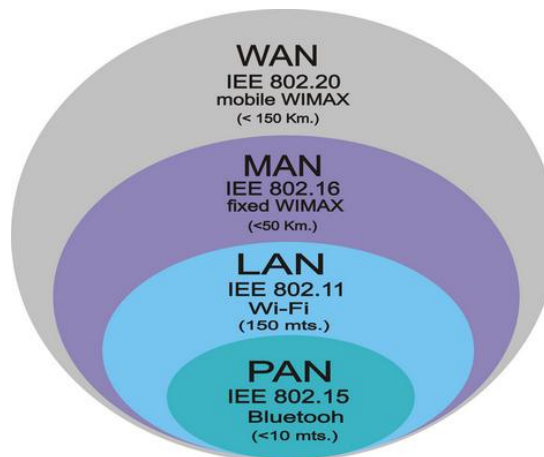
Untuk coverage area jaringan point-to-multipoint bergantung pada besar kecilnya daya pancar BTS pada saat pengaturan awal (commissioning). Secara garis besar hubungan antara jarak (coverage), Frekuensi, Kecepatan (Bandwidth) dan Harga (Cost) dari teknologi jaringan nirkabel adalah sebagai berikut :

- a) Semakin tinggi frekuensi maka : bandwidth semakin besar, harga semakin mahal dan coverage area semakin kecil.
- b) Semakin rendah frekuensi maka : bandwidth semakin kecil, harga lebih murah dan coverage area lebih jauh.

Untuk Frekuensi yang digunakan, pada umumnya perangkat wireless dapat diset di frekuensi berapa pun, tergantung regulasi pemerintah di setiap negara.

5. Klasifikasi berdasarkan jarak jangkauan

Berdasarkan jarak jangkauan jaringan dan daya sinyal nirkabel, maka teknologi nirkabel dikelompokkan menjadi 4 jenis yaitu Wide Area Network (WAN), Metropolitan Area Network (MAN), Local Area Network (LAN), Personal Area Network (PAN). Gambar berikut ini adalah ilustrasi dari ke 4 jenis jaringan nirkabel tersebut :



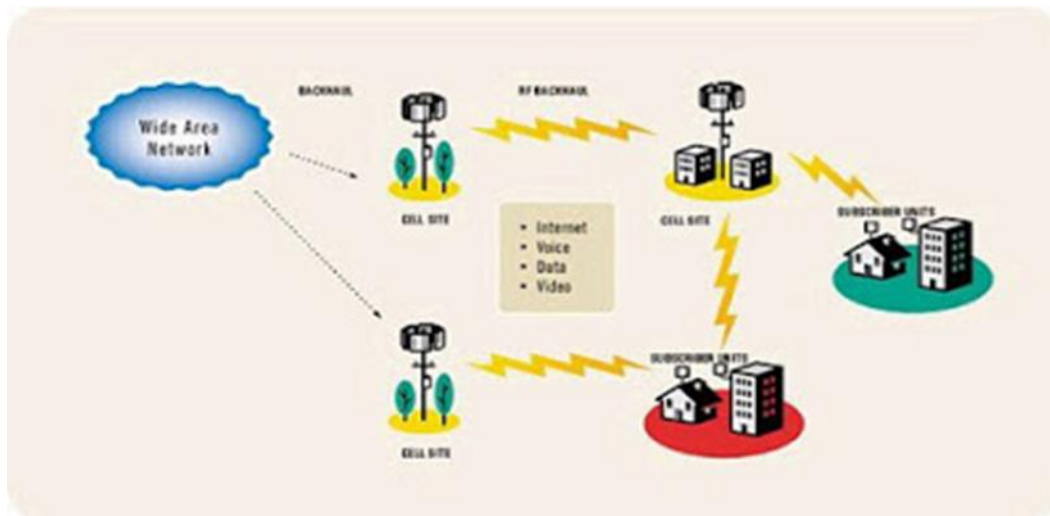
Gambar 1. 22 Klasifikasi Jaringan nirkabel berdasarkan jarak jangkauannya

Berikut ini adalah penjelasan dari masing-masing jenis jaringan berdasarkan jarak jangkauannya:

a. Wireless WAN (Wide Area Network)

Wireless Wide Area Network adalah jaringan nirkabel yang pada umumnya menjangkau area luas misalnya menghubungkan kantor pusat dan cabang antar provinsi. Untuk jarak jangkauan wireless WAN adalah dalam satuan sampai dengan puluhan kilometer, dengan daya sampai dengan ratusan mW. Jangkauan jaringan

nirkabel WAN umumnya mencakup nasional dengan infrastruktur jaringan nirkabel disediakan oleh wireless service carrier (untuk biaya pemakaian bulanan, mirip dengan langganan ponsel) Jaringan nirkabel WAN digunakan untuk menyediakan koneksi Internet bergerak dengan area jangkauan yang jauh lebih luas untuk pelaku perjalanan bisnis atau teknisi lapangan. Wireless WAN memungkinkan user untuk mengakses Internet, e-mail, dan aplikasi dan informasi perusahaan meskipun mereka jauh dari kantor. Wireless WAN menggunakan jaringan selular untuk transmisi data dan contoh sistem selular yang digunakan adalah CDMA, GSM, GPRS, EDGE, 3G, dan HSPDA. Komputer portabel dengan modem wireless WAN terhubung ke base station pada jaringan nirkabel melalui gelombang radio. Antenna yang terdapat pada tower radio kemudian membawa sinyal ke mobile switching center, di mana data dilewatkan ke jaringan yang sesuai. Koneksi ke Internet dilakukan dengan menggunakan koneksi koneksi wireless service provider. Wireless WAN menggunakan jaringan selular eksisting sehingga bisa melakukan panggilan suara melalui wireless WAN. Baik telepon selular dan kartu wireless WAN bisa melakukan panggilan suara dan juga melewatkan data pada jaringan nirkabel WAN. Berikut ini adalah gambaran dari jaringan nirkabel WAN :

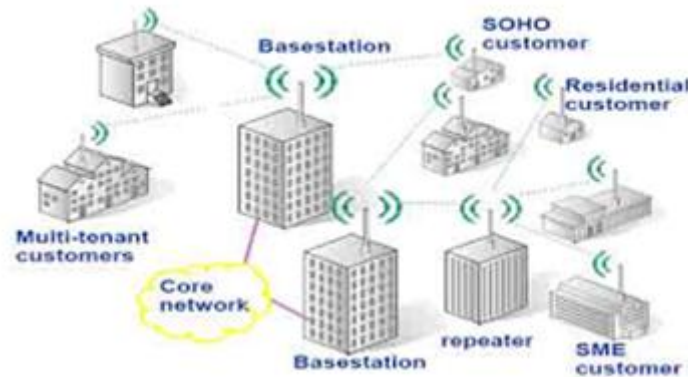


Gambar 1. 23 Jaringan nirkabel WAN

b. Wireless MAN (*Metropolitan Area Network*)

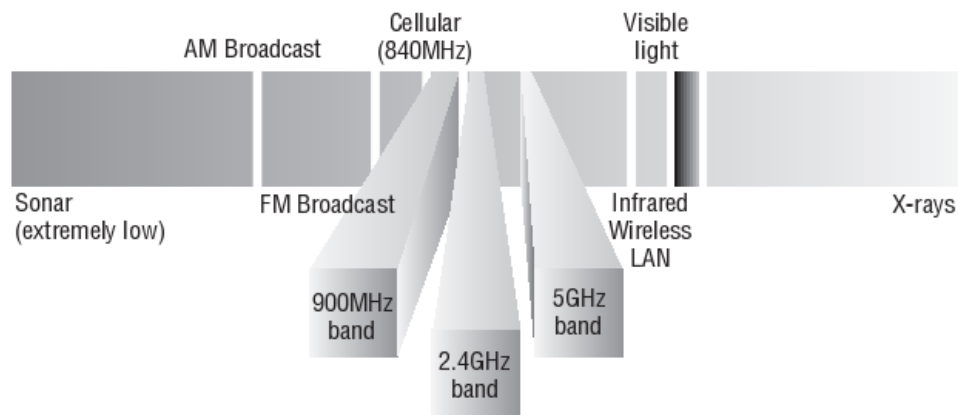
Wireless Metropolitan Area Network (WMAN) adalah jaringan nirkabel network yang menghubungkan beberapa jaringan WLAN. Jaringan MAN sendiri diartikan

sebagai suatu jaringan yang meng-cover area dari satu wilayah perkotaan. Pada awalnya rangkaian MAN dihubungkan dengan menggunakan kabel LAN untuk menghubungkan kantor yang satu ke kantor cabang yang lainnya yang jaraknya beberapa kilometer. Berikut ini adalah gambaran dari jaringan nirkabel MAN :



Gambar 1. 24 Jaringan nirkabel MAN

Contoh penerapan teknologi WMAN adalah teknologi WiMAX (Worldwide Interoperability for Microwave Access), dimana perangkat wireless dengan vendor atau merk yang berbeda-beda dapat saling berkomunikasi atau dapat dikenali satu sama lain. Kecepatan WiMax biasanya terpusat sekitar 5 mbps, meskipun terkadang bisa lebih dari itu. Pengguna WiMax dapat menyebarkan antenna WiMax untuk menutupi sebagian besar wilayah sebuah kota atau metropolitan, mirip dengan jaringan data seluler. Pelanggan membutuhkan modem WiMax khusus untuk mengakses jaringan WiMax. Dengan hadirnya teknologi WiMAX maka pengguna layanan internet semakin tertarik pada Wireless yang berskala MAN. Peralatan pre-Wimax (IEEE 802.16) merupakan suatu perangkat yang didesain khusus untuk wireless berskala MAN, contoh peralatan ini adalah Redline AN-50 AN-30, Alvarion Link Blaster. Wireless MAN dapat bekerja pada beberapa frekuensi yaitu frekuensi 900 MHz, 1.5 GHz, 2 GHz, 2.5 GHz, 3.3 GHz, 5.8 GHz. Dan Saat ini di Indonesia yang ijin pemerintah untuk dipakai oleh masyarakat umum adalah frekuensi 2.4GHz yang kemudian dibagi lagi menjadi beberapa channel. Berikut ini adalah gambar pembagian frekuensi yang digunakan diudara:



Gambar 1. 25 Pembagian frekuensi gelombang radio

Berikut ini adalah tabel daftar kanal yang dapat digunakan pada frekuensi 2.4GHz:

Tabel.2.1 Pembagian kanal pada frekuensi 2,4 GHz

Kanal	Frekuensi
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6.	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.457 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz
14	2.477 GHz

Tiap negara mempunyai aturan yang berbeda-beda dalam penggunaan channel diatas, Misalnya saja untuk beberapa daerah di Amerika, hanya dapat menggunakan Kanal 1 hingga kanal 11, di Eropa menggunakan kanal 1 hingga 13, sedangkan Jepang sendiri yang mempunyai tingkat teknologi tinggi hanya bermain pada kanal 14.

c. Wireless LAN (Lokal Area Network).

Jaringan nirkabel biasanya dikenal dengan istilah jaringan WiFi (Wireless Fidelity), untuk jarak jangkauan dalam satuan sekian ratus meter, dengan daya sekian puluh mW. Wireless LAN yang paling populer adalah jaringan 802.11b. Wireless LAN membutuhkan access point di mana semua perangkat wireless terhubung ke access point tersebut, yang kemudian menghubungkan user ke jaringan kabel. Wireless LAN digunakan di gedung perkantoran, kampus, atau rumah, supaya user bisa berbagi satu koneksi Internet. Berikut ini adalah gambaran dari jaringan nirkabel LAN :



Gambar 1. 26 Jaringan nirkabel LAN (WLAN)

Terdapat beberapa standar untuk teknologi wireless LAN, diantaranya adalah :

- 1) 802.11b, perangkat dengan standar versi ini mempunyai kecepatan transfer data sampai 11Mbps pada frekuensi 2,4 GHz.
- 2) 802.11a, perangkat dengan standar versi ini mempunyai kecepatan transfer data sampai 54 Mbps pada frekuensi 5 GHz.
- 3) 802.11g, perangkat dengan standar versi ini mempunyai kecepatan transfer data sampai 54 Mbps pada frekuensi 2,4 GHz.

Wireless LAN merupakan teknologi yang berhasil dan populer, yang menyebar luar dan diintegrasikan ke dalam laptop sebagai perangkat standar. Berikut ini adalah perbandingan antara teknologi wireless LAN dan wireless WAN:

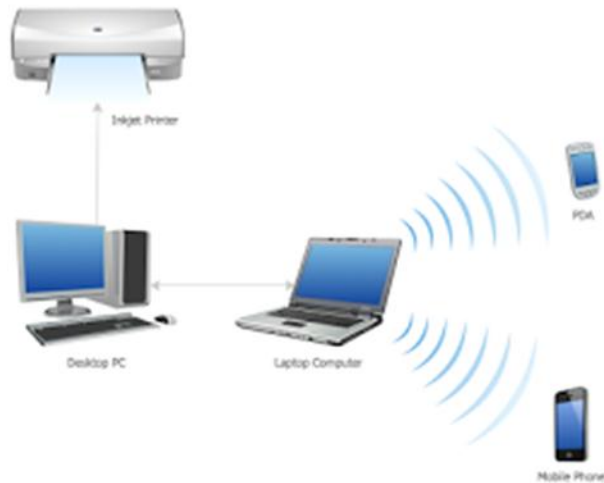
Tabel 2.2. Perbandingan wireless LAN dan wireless WAN

	WIRELESS LAN	WIRELESS WAN
Jangkauan	Gedung perkantoran atau kampus	Tersedia di manapun ada jangkauan jaringan selular; nasional dan global.
Kecepatan	<ul style="list-style-type: none"> • 11 Mbps (802.11b) • 54 Mbps (802.11a/g) 	<ul style="list-style-type: none"> • 115 kbps (GPRS) • 384 kbps (EDGE) • 3,6 Mbps (UMTS) • 153 kbps (CDMA 2000 1X) • 2,4 Mbps (CDMA 2000 1xEV-DO)
Sekuriti	Lemah	Enkripsi dan otentikasi
Biaya airtime	Biaya airtime dikenakan pada sebagian besar hotspot publik. Tidak ada airtime untuk user kantor atau rumahan (tapi tetap ada biaya bulanan layanan ISP).	Biaya bulanan dari provider jaringan wireless.
Penggunaan	Mengakses jaringan di dalam gedung atau antar kampus	<ul style="list-style-type: none"> • Remote akses ke jaringan perusahaan untuk e-mail dan aplikasi. • Akses Internet.
Voice	Tidak	Ya
Analogi Wired	Jaringan Ethernet	Remote modem access
Keuntungan	<ul style="list-style-type: none"> • Kecepatan tinggi. • Tidak ada airtime untuk membangun jaringan (tapi tetap ada biaya untuk hardware dan koneksi Internet). 	<ul style="list-style-type: none"> • Jangkauan luas. • Akses data dari mana pun dan aman.
Kerugian	<ul style="list-style-type: none"> • Jangkauannya hanya lokal. • Masalah sekuriti. 	Kecepatan data lebih cepat dari dial up, tapi belum menyamai kecepatan wireless LAN.

d. Wireless PAN (Personal Area Network)

Personal Area Network (PAN) adalah jaringan komputer personal atau pribadi yang digunakan untuk komunikasi antara komputer perangkat (termasuk telepon dan asisten pribadi digital) dekat dari satu orang. Contoh dari jaringan nirkabel PAN adalah teknologi Bluetooth, Infrared, dan ZigBee. Jangkauan dari PAN biasanya cukup pendek yaitu hanya beberapa meter (sampai dengan sekitar 10 meter). Jaringan PAN dapat digunakan untuk komunikasi antara perangkat pribadi mereka sendiri (intrapersonal komunikasi), atau untuk menghubungkan ke tingkat yang lebih tinggi dan jaringan Internet (uplink). Salah satu teknologi PAN adalah teknologi Bluetooth, yang digunakan sebagai dasar untuk sebuah standar baru, IEEE 802,15. Jaringan Bluetooth PAN juga disebut piconet, dan terdiri dari 8 sampai perangkat aktif dalam hubungan master-slave (yang sangat besar jumlah perangkat yang dapat dihubungkan pada “parkir” mode).

Perangkat Bluetooth pertama di piconet adalah master, dan semua perangkat yang berkomunikasi dengan slave master. Jaringan piconet biasanya memiliki jarak 10 meter, walaupun berkisar hingga 100 meter dapat dijangkau di bawah keadaan ideal. Gambar 1.27 berikut ini menunjukkan jaringan nirkabel PAN:



Gambar 1. 27 Jaringan Nirkabel PAN

Pada gambar 1.27 di atas terlihat bahwa terdapat komunikasi data antara laptop dengan PC atau pun perangkat-perangkat periperal dan jua perangkat mobile menggunakan teknologi bluetooth. Dalam teknologi jaringan nirkabel, setidaknya terdapat 3 hal yang mempengaruhi jarak jangkauan dari perangkat yang digunakan, yaitu :

- 1) Power, dimana semakin besar daya, semakin jauh jaraknya.
- 2) Frekuensi, dimana semakin besar frekuensi jaraknya semakin pendek.
- 3) Alat yang digunakan. Misalnya penguatan antena, loss pada kabel, sensitifitas penerima.

C. Permasalahan Jaringan Nirkabel

Jaringan nirkabel atau lebih dikenal dengan Wi-Fi banyak memiliki kelebihan jika dibandingkan dengan jaringan dengan media kabel (*wired*), terutama jika ditinjau dari sisi efisiensi desain jaringan serta efektifitas jangkauan akses penggunaanya.

Namun di sisi lain teknologi nirkabel juga memiliki kelemahan jika dibandingkan dengan jaringan kabel. Kelemahan jaringan nirkabel secara umum dapat dibagi menjadi 2 jenis, yaitu : kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang

digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi adalah kecenderungan administrator yang menerapkan konfigurasi default dari fasilitas atau tools yang disediakan oleh vendor perangkat tersebut. Fasilitas atau fitur – fitur yang umumnya dibiarkan tanpa dikonfigurasi diantaranya seperti SSID, IP Address, remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user atau password untuk administrasi ke dalam perangkat wifi tersebut. WEP (Wired Equivalent Privacy) yang menjadi teknik standar keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia secara gratis di internet. WPA – PSK dan LEAP yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode dictionaryattack secara offline.

Jika ditinjau dari lapisan-lapisan interkoneksi data pada TCP/IP, maka kelemahan dari jaringan nirkabel ini dapat diidentifikasi sebagai berikut:

1. Kelemahan nirkabel pada Lapisan Fisik (*Physical Layer*)

Wifi menggunakan gelombang radio pada frekuensi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan -batasan tertentu. Setiap wifi memiliki area jangkauan tertentu tergantung power dan antenna yang digunakan. Tidak mudah melakukan pembatasan area yang dijangkau pada wifi. Hal ini menyebabkan berbagai kemungkinan terjadi aktivitas antara lain:

a. *Interception* atau penyadapan

Penyadapan sangat mudah dilakukan, dan sudah tidak asing lagi bagi para hacker. Berbagai tools dengan mudah di peroleh di internet. Berbagai teknik kriptografi dapat di bongkar menggunakan tools-tools tersebut.

b. *Injection* atau injeksi

Pada saat transmisi melalui radio, dimungkinkan dilakukan injection karena berbagai kelemahan pada cara kerja wifi dimana tidak ada proses validasi siapa yang sedang terhubung atau siapa yang memutuskan koneksi saat itu.

c. *Jamming*

Jamming sangat dimungkinkan terjadi, baik disengaja maupun tidak disengaja karena ketidaktahuan pengguna wireless tersebut. Pengaturan penggunaan kanal frekwensi merupakan keharusan agar jamming dapat di minimalisir. Jamming terjadi karena frekwensi yang digunakan cukup sempit sehingga penggunaan kembali channel sulit dilakukan pada area yang padat jaringan nirkabelnya.

d. *Locating Mobile Node*

Dengan berbagai software, setiap orang mampu melakukan wireless site survey dan mendapatkan informasi posisi letak setiap Wifi dan beragam konfigurasi masing masing. Hal ini dapat dilakukan dengan peralatan sederhana seperti PDA atau laptop dengan di dukung GPS sebagai penanda posisi.

e. *Access Control*

Dalam membangun jaringan nirkabel perlu di design agar dapat memisahkan node atau host yang dapat dipercaya dan host yang tidak dapat dipercaya. Sehingga diperlukan access control yang baik.

f. *Hijacking*

Serangan MITM (*Man In The Middle*) yang dapat terjadi pada nirkabel karena berbagai kelemahan protokol tersebut sehingga memungkinkan terjadinya hijacking atau pengambil alihan komunikasi yang sedang terjadi dan melakukan pencurian atau modifikasi informasi.

2. Kelemahan pada Lapisan MAC (Data Layer)

Pada lapisan ini terdapat kelemahan yakni jika sudah terlalu banyak node (client) yang menggunakan channel yang sama dan terhubung pada AP yang sama, maka bandwidth yang mampu dilewatkan akan menurun. Selain itu MAC address sangat mudah di spoofing (ditiru atau di duplikasi) membuat banyak permasalahan keamanan. Lapisan data atau MAC juga digunakan dalam otentikasi dalam implementasi keamanan wifi berbasis WPA Radius (802.1x plus TKIP/AES).

3. Aspek gangguan sinyal jaringan nirkabel

Dalam daerah Fresnel zone tidak boleh ada pengganggu sinyal. Fresnel Zone dibuat beberapa lapis. Jika terdapat halangan di wilayah Fresnel Zone maka performansi jaringan nirkabel akan terganggu. Beberapa efek yang akan terjadi diantaranya adalah:

a. *Reflection (Refleksi)*

Gelombang yang menabrak merambat menjauhi bidang datar dan rata yang di tabrak. Multipath fading akan terjadi jika gelombang yang datang secara langsung menyatu di penerima dengan gelombang pantulan yang juga datang tapi dengan fasa yang berbeda.

b. Refraction (Refraksi) atau Scattering

Gelombang yang menabrak merambat melalui bidang yang dapat memudahkan (scattering) pada sudut tertentu. Pada frekuensi di bawah 10GHz kita tidak terlalu banyak terganggu oleh hujan lebat, awan, kabut dsb. Redaman pada 2.4GHz pada hujan 150mm/jam adalah sekitar 0.01dB/km.

c. Diffraction (Difraksi)

Gelombang yang menabrak melewati halangan (obstacle) dan masuk ke daerah bayangan.

Penggunaan jaringan nirkabel dalam kehidupan sehari-hari meliputi penggunaan *wi-fi*, *bluetooth*, dan inframerah. Namun banyak dari kita yang masih belum mengetahui cara memperbaiki masalah yang sering dialami oleh jaringan nirkabel.

Berikut 6 kesalahan pada jaringan nirkabel beserta cara perbaikannya:

1. Jaringan lambat

Pernahkah Anda menggunakan *wi-fi* di tempat umum/kantor, tiba-tiba koneksi menjadi lambat? hal tersebut terjadi karena jumlah pengguna sangat banyak, terutama pada jam-jam sibuk. Untuk menangkal hal tersebut, kita dapat membatasi *bandwidth* yang diterima oleh setiap *user*, dengan menggunakan *bandwidth* manajemen.

2. Lupa password

Password memiliki peran vital dalam jaringan wireless, karena dengannya kita dapat membatasi pengguna yang dapat terhubung pada jaringan kita. Namun pernahkah Anda kelupaan *password*? jika iya, lakukan peresetan modem/*access point* kepengaturan semula, sehingga kita dapat mengatur *password* baru lagi.

3. Lupa mengatur *IP address*

IP address merupakan suatu alamat pada komputer agar komputer dapat terhubung satu sama lain, *ip address* terbagi atas *DHCP (Dynamic Host Configuration Protocol)* dan *static*.

Jika kita menggunakan jaringan internet maka ada baiknya kita menggunakan *DHCP*, agar *IP address* yang kita terima tidak terjadi tabrakan (*collision*) dengan komputer lain.

Sedangkan jika kita menggunakan jaringan *ad hoc* atau *peer to peer*, maka ada baiknya kita menggunakan *ip address static*, agar *ip address* kita berada satu kelas yang sama dengan komputer lainnya.

4. Sinyal lemah

Sinyal lemah merupakan hal yang paling tidak diharapkan, hal ini terjadi akibat banyak faktor.

a) Ramainya pengguna.

Hal ini menjadi kendala bagi para pengguna jaringan terbuka, karena dengan ramainya pengguna, maka akan membuat jaringan dan sinyal melemah. Untuk mengatasi permasalahan ini, diperlukan *hotspot* tambahan, yang dapat *mengcover* jumlah pengguna yang melebihi batas.

b) Berada jauh dari *hotspot*.

Jarak merupakan hal yang mempengaruhi tingkat *device* (laptop/smartphone) dalam menjangkau sinyal *access point*. Oleh karena itu untuk menghindari hal tersebut kita bisa mencoba untuk memilih tempat duduk yang berada di dekat *access point*.

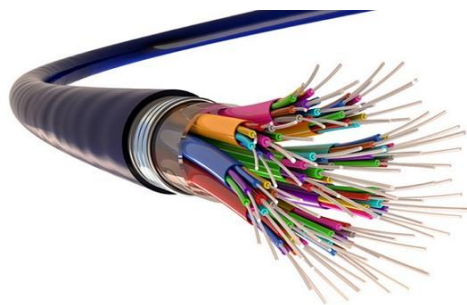
c) Wireless network adapter terdisable

Pernahkah Anda melihat tanda silang pada logo jaringan laptop Anda? padahal Anda berada pada lokasi yang memiliki akses ke internet, hal ini terjadi karena Anda mendisable wireless network adapter secara sengaja maupun tidak sengaja pada laptop anda. Agar laptop anda dapat mendeteksi jaringan yang ada, maka anda harus men-enablekan wireless network adapter.

d) Lupa membayar tagihan bulanan

Poin terakhir ini merupakan masalah klasik yang sering terjadi pada akhir bulan. Walaupun ini bukan masalah teknis, tapi kalau hal ini terjadi akan membuat kita tidak dapat terkoneksi ke internet dalam waktu yang tidak dapat diketahui (sampai kita membayar tagihan).

D. Jaringan Fiber Optic



Gambar 1. 28 Kabel Fiber Optic

Berbeda dari kabel lain yang membawa listrik, kabel Fiber Optik adalah jenis kabel yang berfungsi mengubah sinyal listrik menjadi cahaya dan mengalirkannya dari satu ke titik yang lain. Bahan utama dari kabel jenis Fiber Optik ini adalah dari serat kaca dan plastik yang sangat halus, bahkan lebih halus dari sehelai rambut manusia. Beda halnya dari kabel lain yang memakai bahan dari tembaga.

Terdapat 2 jenis mode transmisi yakni *Single Mode* yang memanfaatkan sinar laser sebagai media transmisinya dan *Multi Mode* yang menggunakan media LED. Biasanya jenis kabel Fiber Optik ini lebih sering dipakai pada suatu instalasi jaringan dengan kelas menengah hingga atas.

1. Fungsi Fiber Optik



Gambar 1. 29 Fiber Optic

Pada dasarnya fungsi dari kabel Fiber Optik sama seperti jenis kabel yang lain yakni menghubungkan antar komputer atau pengguna satu sama lain dan dalam lingkup jaringan tertentu. Yang menjadi pembeda adalah kecepatan akses yang tinggi serta kemampuan transfer data lebih cepat. Untuk kecepatan pengiriman data bisa sampai kisaran Gigabit per detiknya. Selain itu karena tidak membawa listrik kabel jenis ini juga tidak terpengaruhi gangguan elektromagnetik sehingga stabil dalam penggunaannya.

Namun tentunya dengan banyaknya kelebihan yang diperoleh tentunya harus dibayar lebih mahal, itulah sebabnya kabel jenis ini tidak dipakai oleh sembarangan orang. Biasanya perusahaan skala besar serta operator telekomunikasi yang lebih sering memilih menggunakan kabel Fiber Optik ini. Bahkan saat ini pun perusahaan pengembang Wi-Fi sudah mulai memakai Fiber Optik karena lebih cepat dan stabil.

2. Kelebihan dan Kekurangan Fiber Optik

Meskipun hadir dengan kemampuan lebih tinggi daripada jenis kabel yang terdahulu bukan berarti kabel Fiber Optik ini tidak memiliki kekurangan sama sekali. Dibawah ini kami jelaskan berbagai macam kelebihan serta kekurangan yang dapat anda peroleh jika menggunakan Fiber Optik :

a) Kelebihan Fiber Optik

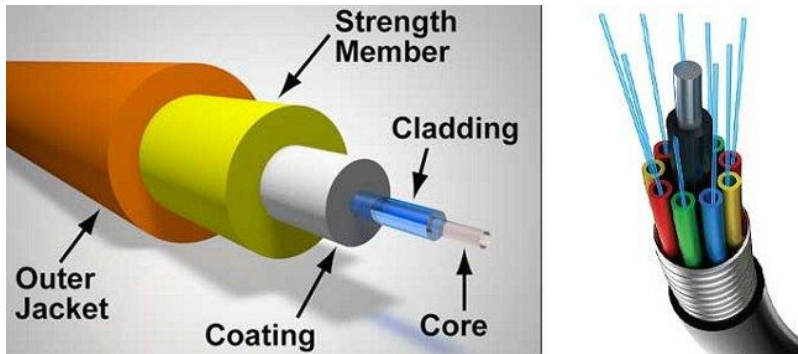
- 1) Jenis kabel Fiber Optik ini memiliki kemampuan mengantarkan data dengan kapasitas besar serta jarak transmisi yang sangat jauh. Dengan kapasitas Gigabyte per detik maka memberikan kebebasan bagi perusahaan-perusahaan internet dan telepon memilih bandwidth tinggi.
- 2) Meskipun memiliki kemampuan yang besar bentuk fisik dari kabel ini lebih kecil jika dibandingkan dengan jenis lain karena bahannya dari serat kaca dan plastik. Hal ini memungkinkan tersedianya ruang yang cukup besar.
- 3) Karena tidak menggunakan arus listrik kabel Fiber Optik ini bebas dari gangguan sinyal elektromagnetik, sinyal radio, serta mempunyai ketahanan yang cukup kuat juga sehingga banyak digunakan perusahaan – perusahaan besar.
- 4) Meskipun memiliki kecepatan akses yang tinggi namun tetap kemungkinan hilangnya data sangatlah rendah, jadi anda tidak perlu mengkhawatirkan validitas data.
- 5) Karena tidak menggunakan listrik maka kemungkinan adanya konsleting juga tidak akan terjadi, jadi dalam hal keamanan juga sangat terjamin.

b) Kekurangan Fiber Optik

- 1) Kekurangan terbesar dari kabel Fiber Optik adalah harganya yang cukup tinggi, hal ini sangatlah wajar mengingat bahan – bahan yang digunakan serta pemasangannya. Oleh sebab itu pengguna kabel jenis bukanlah sembarangan melainkan perusahaan atau penyedia jasa komunikasi yang memang menginginkan akses lebih cepat.
- 2) Selain memakan biaya besar pada saat pemasangan, untuk perawatan Fiber Optik pun juga memerlukan biaya yang tidak sedikit melihat alat – alat yang digunakan juga tidaklah murah.
- 3) Perhatikan juga penempatan kabel Fiber Optik, biasanya dipasang pada jalur yang berbelok atau yang memiliki sudut melengkung agar proses berjalannya gelombang bisa lebih lancar atau tidak terhambat.

c) Cara Kerja Fiber Optik

Karakteristik kabel jaringan fiber optik dapat dilihat seperti pada Gambar di bawah, dimana kabel fiber optik terdiri dari : Inti (Core), Jaket (Cladding), Mantel (Coating), Strength Member & Outer Jacket.



Gambar 1. 30 Karakteristik/Struktur Komponen Kabel Fiber Optik

Sebelumnya sudah dijelaskan bahwa kabel Fiber Optik tidak mengalirkan listrik namun cahaya. Listrik yang diperoleh dikonversikan menjadi sinyal cahaya dan dialirkan antar komputer yang terhubung dalam suatu jaringan skala besar. Hal ini menjadikan kabel Fiber Optik sangat cocok digunakan pada wilayah dengan banyaknya gangguan elektromagnetik.

Jika pada kabel Coaxial atau Twisted panjangnya kabel seringkali menjadi penghambat namun hal ini tidak berlaku bagi kabel Fiber Optik. Bahan baku yang terbuat dari serat kaca murni mampu membawa cahaya untuk mentransmisikan data secara terus menerus tanpa menghiraukan panjangnya kabel yang digunakan. Intinya di dalam kabel Fiber Optik menggunakan cara kerja dengan memanfaatkan cermin untuk menghasilkan total internal reflection atau bahasa umumnya adalah refleksi total pada bagian serat kaca.

Itulah pengertian Fiber Optik yang perlu anda ketahui terutama jika anda ingin melakukan instalasi jaringan. Meskipun memiliki harga yang lumayan tinggi namun dengan melihat manfaat serta keuntungan yang diperoleh maka sangatlah wajar beberapa perusahaan besar lebih memilih jenis kabel ini.

E. Jenis-jenis Kabel Fiber Optic

Kabel jaringan fiber optik terdiri dari beberapa jenis, yang biasanya dapat dengan mudah diketahui dengan melihat transmitter (media transmisi data) yang digunakannya. Berikut ini jenis-jenis kabel jaringan fiber optik :

1. Single-mode fibers

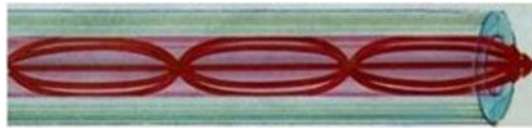
Mempunyai inti yang kecil (berdiameter 0.00035 inch atau 9 micron) dan berfungsi mengirimkan sinar laser inframerah (panjang gelombang 1300-1550 nanometer).



Gambar 1. 31 Single-mode fibers

2. Multi-mode fibers

Mempunyai inti yang lebih besar (berdiameter 0.0025 inch atau 62.5 micron) dan berfungsi mengirimkan sinar laser inframerah (panjang gelombang 850-1300 nanometer)



Gambar 1. 32 Multi-mode fibers

Jika diklasifikasikan menurut aplikasi standar, jenis-jenis kabel fiber optik dibedakan menjadi beberapa tipe. Berikut ini diantaranya :

1. *Tight Buffer (Indoor/Outdoor)*
2. *Breakout Cable (Indoor/Outdoor)*
3. *Aerial Cable/Self-Supporting*
4. *Hybrid & Composite Cable*
5. *Armored Cable*
6. *Low Smoke Zero Halogen (LSZH)*
7. *Simplex cable*
8. *Zipcord cable*

F. Fungsi Alat Kerja Fiber Optic

1. Fusion Splicer



Gambar 1. 33 Fusion Splicer

Fusion splicer atau sering dikenal sebagai alat untuk menyambungkan serat optik ini merupakan salah satu alat yang digunakan untuk menyambungkan sebuah core serat optik, dimana serat tersebut terbuat / berbasis kaca, dan mengimplementasikan suatu daya listrik yang telah dirubah menjadi sebuah media sinar berbentuk laser.

Sinar laser tersebut berfungsi untuk memanasi kaca yang terputus pada core sehingga bisa tersambung kembali dengan baik. Perlu kalian ketahui, bahwa fusion splicer ini haruslah memiliki tingkat keakuratan yang cukup tinggi, hal ini ditujukan untuk menghasilkan hasil penyambungan yang sempurna, karena pada saat penyambungan tersebut akan terjadi proses pengelasan media kaca serta peleburan kaca yang akan menghasilkan suatu media, dimana media tersebut akan tersambung dengan utuh tanpa adanya celah-celah, hal ini dikarenakan media tersebut memiliki senyawa yang sama.

2. Stripper Atau Miller



Gambar 1. 34 Stripper

Sama seperti kabel - kabel yang lain, salah satunya seperti kabel coaxial dan UTP, kabel fiber optic juga memerlukan alat ini. Alat ini berfungsi sebagai media untuk memotong dan mengupas kulit dan daging kabel.

3. Cleaver



Gambar 1. 35 Cleaver

Cleaver Tools ini mempunyai fungsi untuk memotong core yang kulit kabel optic-nya sudah dikupas, perlu kalian ketahui juga bahwa pemotongan core ini wajib menggunakan alat khusus ini, karena pada serat kacanya akan terpotong dengan rapih. Jika proses ini berhasil dilakukan dengan baik maka tahapan selanjutnya, kalian bisa teruskan ke tahap Jointing.

4. Optical Power Meter (OPM)



Gambar 1. 36 Optical Power Meter

Alat yang satu ini memiliki fungsi untuk mengetahui seberapa kuat daya dari signal cahaya yang sudah masuk, OPM ini juga mempunyai interface FC yang langsung berhubungan dengan pathcore FC. Bagi kalian yang belum mengetahui rumus yang digunakan untuk melakukan proses ini, berikut adalah rumusnya ($TX - RX = \dots \text{dB}$ dibagi jarak (Km)).

5. Optical Time Domain Reflectometer (RTDR)



Gambar 1. 37 Optical Time Domain Reflectormeter

OTDR merupakan salah satu alat yang digunakan untuk mendeteksi komunitas atau himpunan suatu kabel serat ptik dalam jarak tempuh tertentu, sehingga dengan adanya alat ini diharapkan mampu menghasilkan jarak dari dua sisi yang merupakan ukuran gangguan yang terjadi. Sehingga untuk melakukan troubleshooting dapat dilakukan dengan baik, karena akan sangat mudah menentukan suatu letak lokasi gangguan yang tengah terjadi. Alat OTDR ini sendiri biasanya digunakan untuk melakukan pendeteksian Kabel Crack, Putusnya core yang belum diketahui letaknya, Putusnya kabel atau juga untuk melakukan bending.

6. Light Source



Gambar 1. 38 Light Source

Pada dasarnya, alat yang satu ini mempunyai fungsi untuk memberikan suatu signal untuk jalur yang akan dilaluinya, misalnya untuk mengukur suatu redaman jalur atu end to end dimana Light Source ini akan berfungsi sebagai media yang memberi signal-nya.

7. Optical Fiber Identifier



Gambar 1. 39 Optical Fiber Identifier

Alat yang satu ini memiliki fungsi untuk mengetahui arah signal dengan penunjuk arah dan besar daya yang di lalunya.

8. Visual Fault Locator



Gambar 1. 40 Visual Fault Locator

Alat ini sering disebut juga Laser fiber optic atau senter fiber optic. Fungsinya untuk melakukan pengetesan pada core fiber optic. Laser akan mengikuti serat Optik pada Kabel Fiber Optik dari POP Sampai Ke User (end to end) , bila core tidak bermasalah laser akan sampai pada titik tujuan.

9. Bit Error Rate Test



Gambar 1. 41 Bit Error Rate Test

Alat ini berfungsi sebagai pengecek koneksi jaringan TDM (Time Divisio Multipleksi) yang mana jaringan TDM aplikasinya yaitu layanan Clear Channel yang sedang coba di uraikan penulis. Secara spesifiknya BER TES untuk mengecek dan mengetahui TX atau RX yang error, melalui pengiriman paket dan lup.

G. Penyambungan Fiber Optic

Penyambungan serat optik atau yang sering disebut dengan splicing serat optik dilakukan pada saat serat putus yang dikarenakan oleh faktor dari luar seperti terkena senar layangan, cangkul, jangkar, dan lain-lain atau untuk menghubungkan ujung serat optik pada saat instalasi dengan jarak yang jauh. Dengan melakukan splicing ini kita akan dapat mengurangi redaman. Hal ini disebabkan bila kita menggunakan konektor biasa untuk menghubungkan kedua ujung serat optik, maka kita akan mendapatkan redaman yang lebih besar dibandingkan melakukan teknik splicing.

1. Peralatan dan Bahan

- a) Splicer
- b) Pemotong tube
- c) Cutter
- d) Tang logam
- e) Tang pengupas serat
- f) Tang pemotong serat
- g) Kain bersih
- h) Alkohol
- i) Tissue
- j) Selotip
- k) Spidol
- l) Meteran
- m) Thinner-B
- n) Pelindung serat

2. Hal-Hal yang perlu diperhatikan dalam penyambungan Serat Optik

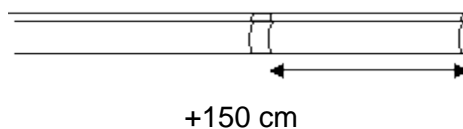
Dalam melakukan splicing ada hal-hal yang harus diperhatikan agar splicing bisa berhasil dan juga untuk keselamatan kerja. Hal-hal tersebut antara lain:

- a) Sebelum melakukan splicing usahakan agar semua peralatan dan bahan serta tangan kita sebersih mungkin sebab adanya kotoran pada serat optik dapat menyumbang redaman pada serat.
- b) Selalu letakkan tangan di belakang cutter ketika sedang melakukan pengupasan pelindung serat.
- c) Jangan menginjak tube karena akan merusak core yang ada di dalamnya sehingga bisa menyebabkan core pecah atau retak.
- d) Sebaiknya jangan mendekatkan cairan alkohol ke mata kita sebab cairan alkohol bisa menguap ke udara.
- e) Jangan menggulung core dengan diameter yang sangat kecil karena bisa membuat core putus.
- f) Jangan membuang core sembarangan sebab bila menembus kulit dikuatirkan bisa masuk ke aliran darah dan mengganggu kesehatan.
- g) Selalu perhatikan perlindungan pada kaset agar air tidak dapat masuk kedalam kaset dan bisa merusak serat tersebut.
- h) Ikuti prosedur atau langkah-langkah yang ada.

3. Langkah-Langkah Instalasi

Dalam hal ini kita menggunakan kabel serat optik untuk udara. Berikut ini adalah prosedur atau langkah-langkah dalam melakukan penyambungan atau splicing serat optik :

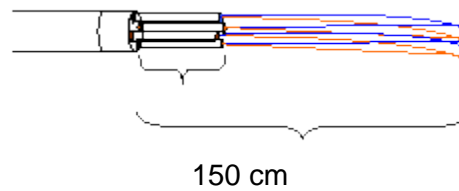
- a) Ukur dengan menggunakan meteran sepanjang ± 150 cm (dalam keadaan baik) dari ujung kabel lalu tandai dengan isolasi atau spidol.



Gambar 1. 42 Panjang kabel yang dikupas

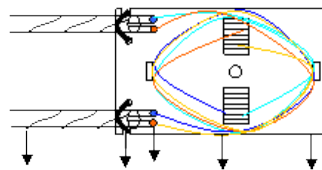
- b) Untuk kabel udara terlebih dahulu mengupas logam dalam kabel yang berfungsi sebagai penopang kabel saat berada di udara dengan menggunakan cutter sepanjang batas tersebut lalu potong dengan tang logam.
- c) Setelah itu mengupas pelindung tube yang berwarna hitam sepanjang batas tersebut. Langkah-langkah untuk membuka pelindung:

- 1) Sebaiknya dilakukan secara sedikit demi sedikit sepanjang 25 cm dengan cara digergaji dan jangan terlalu dalam karena akan mengenai tube.
- 2) Patahkan sedikit dan memutar pada bekas gergaji dan sudut patah tidak boleh 30° agar tube tidak ikut patah.
- 3) Lalu tarik sehingga yang terlihat hanya benang pelindung dan kupas benang tersebut dengan cutter sehingga yang terlihat hanya tube yang dilapisi jelly.
- d) Bersihkan tube dari jelly dengan kain yang sudah dibasahi dengan thinner-B sampai bersih.
- e) Ukur tube tersebut dari batas isolasi sepanjang ± 50 cm beri tanda dengan spidol. Lalu kupas tube pada batas tersebut dengan menggunakan pemotong tube dan sebaiknya dilakukan sedikit demi sedikit sepanjang 25 cm dengan cara memutar pemotong tube searah jarum jam sebanyak 2 kali lalu patahkan dan jangan lebih dari 30° agar serat optik tidak ikut patah, lalu tarik tube sehingga yang terlihat hanya serat optik saja yang dilindungi oleh jelly. Lakukan berulang-ulang sampai sepanjang ± 100 cm dari ujung tube.
- f) Bersihkan core tersebut dari jelly dengan kain yang sudah dibasahi dengan thinner-B sampai bersih.



Gambar 1. 43 Panjang tube yang dikupas

- g) Gulung serat optik dengan bentuk melingkar agar aman, tidak kotor dan tidak mengenai tanah.

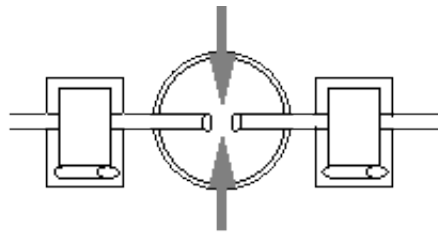


Spiral Pengikat Tube Core Kaset

Gambar 1. 44 Penempatan serat optic pada kaset

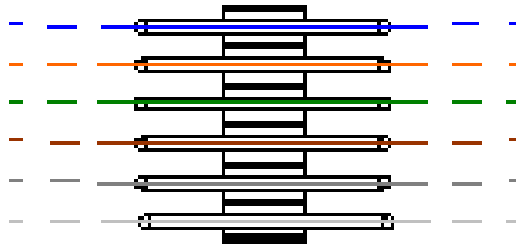
4. Langkah-Langkah Splicing

- a) Terlebih dahulu masukkan plastik khusus untuk melindungi bagian core yang telah di-splice satu persatu dengan diberi tanda dengan spidol.
- b) Kupas core dari jaketnya menggunakan tang pengupas dengan cara memposisikan tang agak miring, tahan lalu tarik ke ujung core secara perlahan.
- c) Setelah terkupas bersihkan core dengan tissue yang sudah dibasahi dengan alkohol sampai gesekannya mengeluarkan bunyi. Lakukan sebanyak 3 kali lalu keringkan dengan tissue.
- d) Lalu masukkan ke dalam pemotong core dimana kita menempatkan ujung jaket pada skala antara 15 dan 20, lalu potong. Pada saat memotong, pisau harus dijalankan dengan kecepatan yang sesuai dan konstan.
- e) Setelah itu kita masukkan ke dalam splicer yang berfungsi menyambung core dengan teknik fusion. Jangan sampai ujung core menyentuh sesuatu benda sebab akan menambah redaman.



Gambar 1. 45 Peletakan serat optik pada splicer

- f) Kemudian tekan tombol set maka secara otomatis splicer akan meleburkan kedua core dan menyambungkannya. Tunggu sampai layar menunjukkan estimasi redaman lalu tekan reset maka layar akan kembali ke tampilan awal.
- g) Setelah itu keluarkan core tersebut lalu geser plastik khusus tadi ke sisi core yang telah mengalami proses splice. Kemudian masukkan ke bagian splicer yang berfungsi untuk memanaskan plastik tersebut. Tunggu sampai splicer mengeluarkan bunyi lalu keluarkan.
- h) Kemudian letakkan core kembali ke dalam kaset tadi seperti gambar di bawah ini.



Gambar 1. 46 Peletakan protektor pada kaset

5. Rugi-Rugi Penyambungan

Rugi-rugi penyambungan dapat terjadi karena :

- a) Perbedaan struktur serat optik antara lain:
 - 1) Diameter core tidak sama.
 - 2) Letak core tidak berada di tengah.
- b) Kualitas penyambungan antara lain :
 - 1) permukaan serat tidak rata.
 - 2) Sumbu serat tidak sejajar.
 - 3) Penyimpangan sudut.
 - 4) Serat masih basah.
 - 5) Ujung serat menyentuh sesuatu.

6. Kualitas Penyambungan

Untuk mendapatkan kualitas penyambungan yang baik harus diperhatikan :

- a) Kualitas kabel yang sesuai spesifikasi
- b) Alat sambung yang baik.
- c) Lingkungan harus bersih.
- d) Joints harus berpengalaman.

Dengan melakukan penyambungan secara fusion, kita diharapkan bisa memperoleh redaman yang sekecil mungkin.

H. Perangkat Pasif Jaringan Fiber Optic

Kehadiran teknologi *Broadband* membuat dunia telekomunikasi di Indonesia menjadi lebih baik. Internet berkecepatan tinggi yang semula hanya ada di angan saja, kini bisa dirasakan oleh banyak orang. Teknologi ini mampu menerima dan mengirim banyak informasi dalam waktu yang sangat singkat. Tentu, munculnya teknologi berkecepatan tinggi ini tidak terlepas dari keberadaan fiber optik.

1. Komponen Pasif Fiber Optik: Mengenal GPON, ONT, dan OLT



Gambar 1. 47 Pasif Fiber Optik

Passive Optical Network (PON) merupakan sebuah teknologi tembaga yang digunakan baik pada *narrow-band* dan *broadband*. Teknologi ini dikatakan pasif karena memiliki elemen pembagi yang tidak memanipulasi sinyal optik. Salah satu jenis dari PON adalah GPON (*Gigabit Ethernet PON*).

a) **GPON** (*Gigabit Passive Optical Network*)

GPON merupakan sebuah teknologi node akses yang diperlukan untuk mengantarkan layanan data, suara, dan video ke tempat pelanggan. Teknologi ini berbasis FTTx, yaitu jaringan yang memanfaatkan kabel fiber optik sebagai medium transmisi.

Hingga kini, teknologi GPON bersaing ketat dengan GEPON (*Gigabit Ethernet PON*), yaitu sebuah jaringan optik pasif versi IEEE yang berbasis teknologi *Ethernet*. Namun, GPON lebih mendominasi pasar dan memiliki *roll out* yang lebih cepat dibanding dengan GEPON. Standar G.984 pada GPON memberikan dukungan keamanan lebih baik, *bit rate* yang lebih tinggi, serta pilihan protokol layer 2 (ATM, GEM, dan *Ethernet*).

Prinsip kerja dari jaringan GPON yaitu mengantarkan sinyal menuju komponen pasif fiber optik dan melanjutkannya kepada pelanggan. Teknologi ini menggunakan sebuah *splitter* untuk membagi jaringan kepada banyak pelanggan. Ketika beroperasi, GPON memanfaatkan beberapa komponen.

b) **OLT** (*Optical Line Terminal*)

Optical Line Terminal merupakan sebuah komponen pasif fiber optik yang memiliki fungsi sebagai titik akhir dari layanan jaringan. Cara kerja OLT adalah mengubah sinyal listrik menjadi sinyal optik.

OLT menyediakan sebuah tampilan tatap muka antara sistem PON dengan penyedia layanan data, video, dan jaringan telepon. Nantinya, bagian ini juga akan menjadi multiplexing, yaitu penggabungan beberapa sinyal yang dikirim secara bersamaan pada kanal transmisi.

c) **ONT** (*Optical Network Termination*)

ONT merupakan komponen pasif fiber optik berfungsi memberi tampilan tatap muka pada pengguna layanan. Sinyal optik yang ditransmisi diubah menjadi sinyal elektrik. Sinyal ini digunakan untuk menampilkan layanan pada para pelanggan. Pada penyusunan sebuah jaringan FTTH, komponen ini diletakkan di rumah pelanggan.

2. Keunggulan dan Kelemahan GPON

Berikut ini merupakan beberapa keunggulan dari GPON yang tidak dimiliki jaringan lainnya, antara lain:

- 1) Mampu menghadirkan layanan *triple play services* (suara, data, dan video) pada layanan FTTx yang dilakukan melalui satu inti FO.
- 2) Dapat membagi *bandwidth* hingga 32 ONT
- 3) GPON bisa mengurangi penggunaan kabel pada peralatan kantor
- 4) Pengalokasian *bandwidth* bisa diatur dengan mudah
- 5) Biaya perawatan lebih murah, karena memiliki komponen pasif
- 6) Lebih efisien dalam hal biaya pemasangan, pemeliharaan, dan pengembangan.

Meskipun memiliki banyak kelebihan, ada beberapa kelemahan yang terdapat pada jaringan GPON, antara lain:

- 1) Kompleksitas model *layering* dibanding jaringan lain
- 2) Jika dibandingkan dengan GPON, instalasi GPON memakan dana lebih banyak
- 3) Penerima laju data 2.4 Gbps saat ini terbilang cukup mahal
- 4) Saat ini *bandwidth upstream* hanya terbatas hingga 622 Mbps saja

I. Permasalahan Jaringan Fiber Optic

Pada Instalasi kali ini terjadi beberapa masalah, yaitu pada saat pengecekan koneksi ternyata koneksi belum sepenuhnya berjalan dengan lancar, dan loss yang

dihasilkan sangat besar atau tidak memenuhi standar loss yang direkomendasikan yaitu RX *sensitivity*-nya antara -22 s/d -24 dB, pada saat dilakukan penghitungan ternyata loss yang dihasilkan adalah -38 dB, setelah tim *troubleshooting* masalah ini mulai dari konstruksi kabel apakah ada bending atau kabel yang patah, penggunaan attenuator yang tepat, setelah beberapa tindakan tersebut dilakukan ternyata loss yang dihasilkan masih saja besar. Tim instalasi sempat mengganti atau *splice* ulang patch cord karena diasumsikan hasil *splicing*nya kurang maksimal, ternyata tindakan tersebut juga tidak merubah hasil penghitungan loss yang direkomendasikan.

Setelah tim melakukan pengecekan ulang di OTB ternyata sumber masalah ditemukan yaitu konektor FC yang masuk salah satu port di OTB tidak tertancap sebagaimana mestinya, inner dari konektor tersebut tidak masuk secara tepat. Hal inilah yang ternyata menyebabkan loss yang dihasilkan tidak sesuai dengan yang direkomendasikan.

Dari *problem* pada saat instalasi kali ini dapat diambil beberapa kesimpulan supaya hal yang sama tidak terjadi kembali, untuk meminimalisasikan terjadinya problem tersebut, tim menyimpulkan beberapa hal diantaranya:

1. Pastikan kabel fiber yang digunakan bersih dan tidak patah atau rusak.
2. Pada saat *splicing* pastikan loss yang dihasilkan seminimal mungkin. Atau mencapai RX *sensitivity* yang direkomendasikan yaitu -22 s/d -24 dB.
3. Pada saat memasukan konektor ke salah satu port di OTB pastikan inner-nya masuk secara tepat.(jika hal ini tidak diteliti dengan baik maka pada saat melakukan pengukuran dengan power meter, maka loss yang dihasilkan akan besar).
4. Pada saat pengukuran dengan power meter pastikan gelombang yang digunakan sama.

Bila terjadi beberapa masalah, maka cek beberapa keterangan konfigurasi di bawah ini diantaranya adalah :

1. *Failure of ONU to range*
 - a) Fiber yang kotor
 - b) Sinyal degradasi
 - c) Kabel fiber terlalu panjang
 - d) Kabel fiber rusak
 - e) *Bad connections/fiber plant components*
 - f) *Laser/receiver* tidak berfungsi

- g) ONU ID# *conflict*
- 2. Loss permanent pada *frame/pattern* di *TDM*
 - a) Konfigurasi kabel yang salah
 - b) Ports/Channels/Board tidak aktif
- 3. Tidak bisa telnet ke SCC management port (pada OLT)
Konfigurasi yang salah pada SCC IP parameternya.
- 4. *No IP traffic*
 - a) VLAN membership yang salah
 - b) Ports tidak di *enabled*

Rangkuman

Sebuah WAN menggunakan jalur data untuk membawa data menuju ke internet dan menghubungkan lokasi lokasi perusahaan yang terpisah pisah. Telepon dan layanan data yang paling banyak digunakan pada WAN.

WAN menghubungkan beberapa LAN melalui jalur komunikasi dari service provider. Karena jalur komunikasi tidak bisa langsung dimasukkan ke LAN maka diperlukan beberapa perangkat interface.

Perangkat perangkat tersebut antara lain:

- 1. Router
- 2. CSU/DSU
- 3. Modem
- 4. Communication Server

WAN menggunakan OSI layer tetapi hanya fokus pada layer 1 dan 2. Standar WAN pada umumnya menggambarkan baik metode pengiriman layer 1 dan kebutuhan layer 2, termasuk alamat fisik, aliran data dan enkapsulasi.

Konfigurasi routing secara umum terdiri:

- 1. Minimal Routing
- 2. Static Routing
- 3. Dynamic Routing
- 4. Routing Protocol

Permasalahan Jaringan Nirkabel

- 1. Jaringan lambat
- 2. Lupa password

3. Lupa mengatur IP address
4. Sinyal lemah
5. Wireless network adapter terdisable
6. Lupa membayar tagihan bulanan

Kabel Fiber Optik adalah jenis kabel yang berfungsi mengubah sinyal listrik menjadi cahaya dan mengalirkannya dari satu ke titik yang lain. Bahan utama dari kabel jenis Fiber Optik ini adalah dari serat kaca dan plastik yang sangat halus, bahkan lebih halus dari sehelai rambut manusia. Beda halnya dari kabel lain yang memakai bahan dari tembaga.

Kelebihan Fiber Optik:

1. Jenis kabel Fiber Optik ini memiliki kemampuan mengantarkan data dengan kapasitas besar serta jarak transmisi yang sangat jauh. Dengan kapasitas Gigabyte per detik maka memberikan kebebasan bagi perusahaan-perusahaan internet dan telepon memilih bandwidth tinggi.
2. Meskipun memiliki kemampuan yang besar bentuk fisik dari kabel ini lebih kecil jika dibandingkan dengan jenis lain karena bahannya dari serat kaca dan plastik. Hal ini memungkinkan tersedianya ruang yang cukup besar.
3. Karena tidak menggunakan arus listrik kabel Fiber Optik ini bebas dari gangguan sinyal elektromagnetik, sinyal radio, serta mempunyai ketahanan yang cukup kuat juga sehingga banyak digunakan perusahaan – perusahaan besar.
4. Meskipun memiliki kecepatan akses yang tinggi namun tetap kemungkinan hilangnya data sangatlah rendah, jadi anda tidak perlu mengkhawatirkan validitas data.
5. Karena tidak menggunakan listrik maka kemungkinan adanya korsleting juga tidak akan terjadi, jadi dalam hal keamanan juga sangat terjamin.

Kekurangan Fiber Optik

1. Kekurangan terbesar dari kabel Fiber Optik adalah harganya yang cukup tinggi, hal ini sangatlah wajar mengingat bahan – bahan yang digunakan serta pemasangannya. Oleh sebab itu pengguna kabel jenis bukanlah sembarangan melainkan perusahaan atau penyedia jasa komunikasi yang memang menginginkan akses lebih cepat.
2. Selain memakan biaya besar pada saat pemasangan, untuk perawatan Fiber Optik pun juga memerlukan biaya yang tidak sedikit melihat alat – alat yang digunakan juga tidaklah murah.

3. Perhatikan juga penempatan kabel Fiber Optik, biasanya dipasang pada jalur yang berbelok atau yang memiliki sudut melengkung agar proses berjalannya gelombang bisa lebih lancar atau tidak terhambat.

Jenis-jenis Kabel Fiber Optic:

1. Single-mode fibers
2. Multi-mode fibers

Fungsi Alat Kerja Fiber Optic

1. Fusion Splicer
2. Stripper Atau Miller
3. Cleaver
4. Optical Power Meter (OPM)
5. Optical Time Domain Reflectometer (OTDR)
6. Light Source
7. Optical Fiber Identifier
8. Visual Fault Locator
9. Bit Error Rate Test

Passive Optical Network (PON) merupakan sebuah teknologi tembaga yang digunakan baik pada *narrow-band* dan *broadband*. Teknologi ini dikatakan pasif karena memiliki elemen pembagi yang tidak memanipulasi sinyal optik. Salah satu jenis dari PON adalah GPON (*Gigabit Ethernet PON*).

Tugas

1. Pelajarilah uraian materi tentang konsep dasar jaringan WAN ini dengan baik. Buatlah rangkuman dari materi tersebut dan diskusikan
2. Peserta membuat rancangan jaringan WAN Masuklah ke LAB komputer di sekolah anda. Lakukan pengamatan terhadap jaringan LAN yang sudah ada. Amati dan catat: teknologi WAN dan tipe enkapsulasi yang digunakan. Jelaskan!

Tes Formatif

1. Perangkat yang berfungsi mengatur pemilihan jalur terbaik untuk dilewati paket data dikenal sebagai
 - a. Switch
 - b. **Router**

- c. Web server
 - d. Proxy server
 - e. Name server
2. Kumpulan dari Lan atau workgroup yang dihubungkan dengan menggunakan alat komunikasi modem atau jaringan internet adalah devinisi dari...
- a. LAN
 - b. MAN
 - c. WAN
 - d. GROUP
 - e. WORKSHEET
3. Keuntungan jaringan WAN:
- 1) Pertukaran file dapat dilakukan dengan mudah (file sharing)
 - 2) Server kantor pusat dapat berfungsi sebagai bank data dari kantor cabang
 - 3) Komunikasi antar kantor dapat menggunakan E-mail dan Chat
 - 4) Resiko kehilangan data oleh virus komputer menjadi sangat kecil sekali
 - 5) Pooling Data dan Updating Data antar kantor dapat dilakukan setiap hari pada waktu yang ditentukan.
- Dari pernyataan diatas yang sesuai dengan keuntungan jaringan WAN yang benar adalah..
- a. 1,2 dan 3
 - b. 2,3 dan 5
 - c. 1,3 dan 5
 - d. 2,3 dan 4
 - e. Semua benar
4. Konfigurasi routing yang dibangun dalam network yang hanya mempunyai beberapa gateway dan umumnya tidak lebih dari 2 atau 3 yaitu
- a. Minimal Routing
 - b. Static Routing
 - c. Dynamic Routing

- d. Routing Protocol
 - e. Interior Routing
5. Alat yang satu ini memiliki fungsi untuk mengetahui seberapa kuat daya dari signal cahaya yang sudah masuk, OPM ini juga mempunyai interface FC yang langsung berhubungan dengan pathcore FC.
- a. *Cleaver*
 - b. *Stripper Atau Miller*
 - c. *Optical Fiber Identifier*
 - d. *Bit Error Rate Test*
 - e. *Optical Power Meter (OPM)*