BAB II

LANDASAN TEORI

A. Pengertian Jaringan Komputer

Dengan berkembangnya jaringan komputer dan komunikasi suatu model komputer tunggal yang melayani seluruh tugas tugas komputasi suatu organisasi kini telah diganti dengan sekumpulan komputer yang terpisah-pisah tetapi saling berhubungan dalam melaksanakan tugasnya,sistem seperti ini disebut dengan jaringan komputer (computer network).

Sebuah jaringan komputer paling sedikit terdiri dari dua buah komputer saling terhubung dengan sebuah media sehingga komputer-komputer tersebut dapat saling berbagi *Resource* dan saling berkomunikasi. Semua *network* berbasis pada konsep pembagian (sharing)

Jaringan komputer muncul dari adanya kebutuhan untuk berbagi data diantara para pengguna, sekelompok komputer dan *device* lain saling terhubung membentuk sebuah *network*, sedangkan konsep dari komputer-komputer yang saling berbagi *resource* dikenal istilah *Networking*. Komputer-komputer yang

Pada awal perkembangannya jaringan kerap kali dihubungkan dengan menggunakan media kabel, namun seiring dengan perkembangan dunia teknologi informasi yang kian pesat penggunaan media nirkabel kini sudah banyak diterapkan. Hal ini dikarenakan semakin banyaknya pengguna yang menggunakan laptop,sehingga pengguna dapat mengakses kedalam jaringan secara mobilitas.

Berdasarkan arah tranmisinya tranmisi data dibedakan atas

- Simplex

  Sinyal hanya ditransmit satu arah saja dimana satu stasiun sebagai pemancar dan lainnya sebagai penerima, pada sistem ini aliran data hanya terjadi satu arah saja

- Half-Duplex

  Dalam operasi ini, Kedua stasiun mungkin melakukan pengiriman, tetapi tidak bisa bersamaan melainkan beroperasi bergantian. Pada sistem ini aliran informasi terjadi kedua arah tetapi tidak dapat bersamaan.

- Full-Duplex

  Dalam operasi full duplex,kedua stasiun mungkin mentranmisikan secara serentak. Pada sistem ini aliran dapat terjadi kedua arah pada saat yang bersamaan. Sistem ini dapat terjadi hanya menggunakansebuah saluran komunikasi data

B. Klasifikasi Jaringan komputer

Berdasarkan daerah jangkauannya, Dibagi 3 yaitu

- Local Area Network (LAN)

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

- Metropolitan Area Network (MAN)

  pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

- Wide Area Network (WAN)

  jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

C. Topologi

Topologi adalah istilah yang digunakan untuk mengambarkan bagaimana komputer terhubung dalam suatu jaringan. Secara umum, topologi dibedakan menjadi dua jenis yaitu topologi fisik dan topologi logika. Topologi fisik menguraikan layout aktual dari perangkat keras jaringan, sedangkan topologi

logika menguraikan perilaku komputer pada jaringan, dari sudut pandang operator manusianya.

- **Topologi Fisik**

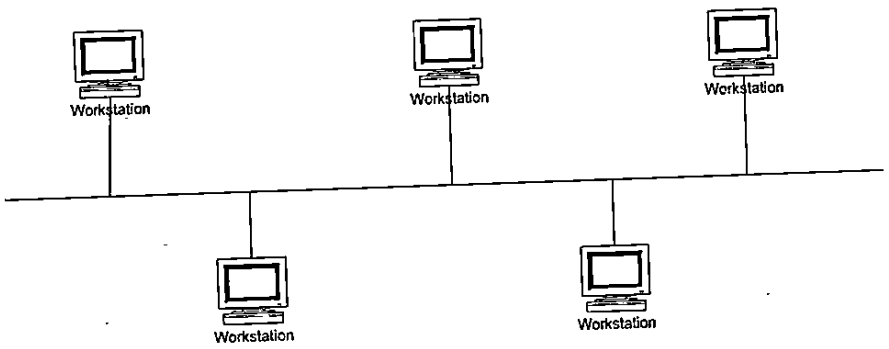
Topologi fisik jaringan komputer adalah bagaimana cara dan bentuk jaringan komputer secara fisik dalam menghubungkan antar komputer.

- **Topologi Fisik Linear Bus**

Layout ini termasuk layout yang umum. Satu kabel utama menghubungkan tiap simpul, ke saluran tunggal komputer yang mengaksesnya ujung dengan ujung. Masing-masing simpul dihubungkan ke dua simpul lainnya, kecuali mesin di salah satu ujung kabel, yang masing-masing hanya terhubung ke satu simpul lain. Topologi ini seringkali dijumpai pada sistem client/server, dimana salah satu mesin pada jaringan ditetapkan sebagai file server, yang berarti bahwa mesin tersebut dikhususkan hanya untuk penyebaran file data, dan biasanya tidak digunakan untuk pemrosesan informasi.

Topologi ini digunakan pada jaringan area lokal dan untuk jaringan banyak titik untuk jarak yang relatif pendek. Kelebihan dari model ini adalah bahwa untuk memfungsikan jaringan tidak setiap komputer perlu dijalankan dan apabila ada terminal-terminal tambahan dapat dihubungkan

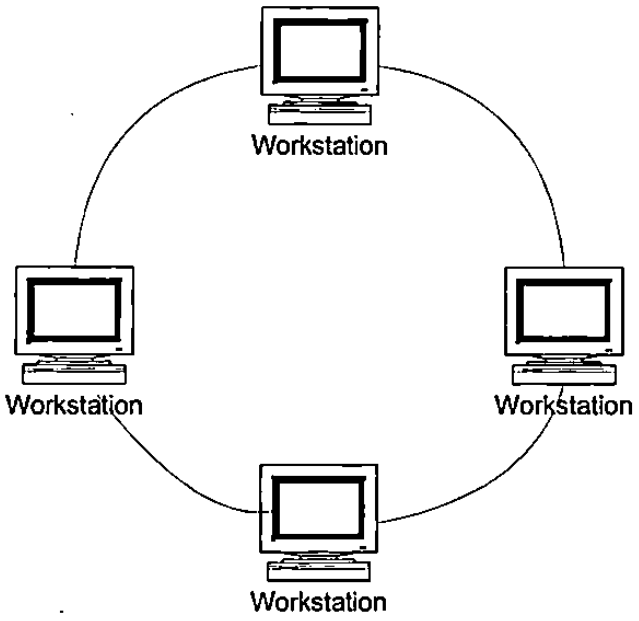
lintas informasi hanya digunakan satu kabel saja, maka kinerjanya kadang agak lambat.



Gambar 2.1 Topologi Bus

- **Topologi Fisik Ring**

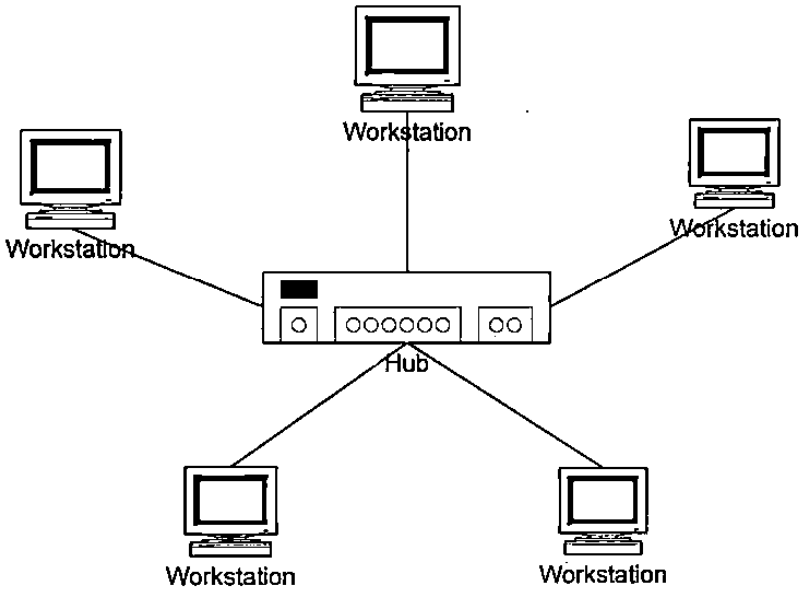
Layout ini serupa dengan linear bus, kecuali simpul terhubung dalam suatu lingkaran dengan menggunakan segmen kabel. Dalam layout ini, tiap simpul secara fisik terhubung hanya ke dua simpul lain. Masing-masing simpul mengirim informasi ke simpul berikutnya, hingga tiba di sasaran yang dituju. Kinerja pada sistem ini dapat lebih cepat sebab tiap bagian dari sistem pengkabelan hanya menangani aliran data antara dua mesin. Jenis topologi ini dapat dijumpai dalam jaringan peer-to-peer, dimana tiap mesin mengelola pemrosesan informasi maupun penyebaran file data. Kelebihan dari topologi model ring adalah kinerjanya dapat lebih cepat, sedangkan kekurangannya adalah untuk mengaktifkan jaringan, harus menghidupkan semua komputer.



Gambar 2.2 Topologi Ring

- **Topologi Fisik Star**

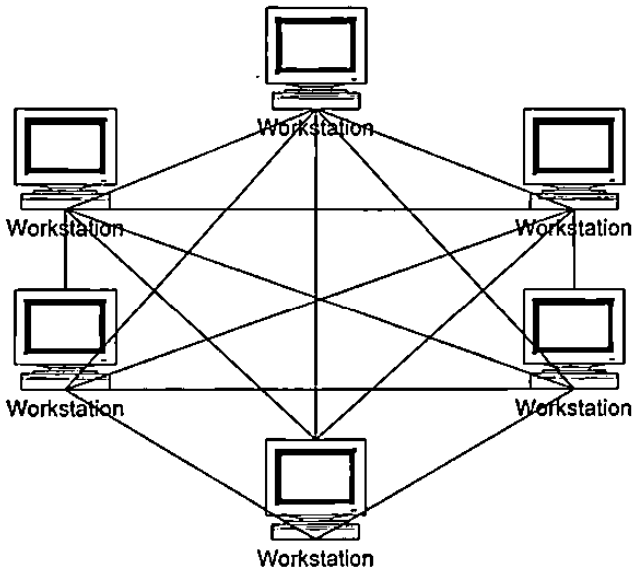
Tiap terminal terhubung ke sebuah titik pusat (server) oleh suatu sirkuit terpisah dan semua sambungan antar terminal dihubungkan oleh *hub*. Topologi ini memiliki keunggulan dalam hal minimalnya lintas data sepanjang kabel (hanya terminal ke-server), sehingga dapat dicapai kinerja yang optimal. Tetapi karena satu mesin harus mengkoordinir seluruh komunikasi data, berarti topologi ini memerlukan file server yang sangat



Gambar 2.3 Topologi Star

- **Topologi Fisik Mesh**

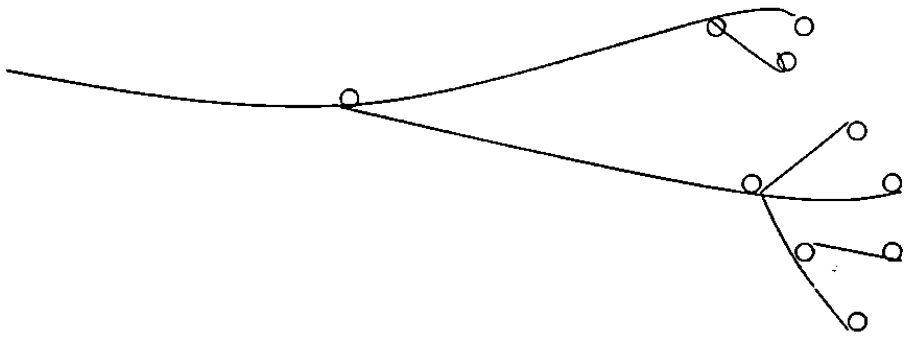
Topologi ini mempunyai sejumlah simpul dimana setiap simpulnya tersambung secara total dengan simpul-simpul yang lain, sehingga hubungan dari satu simpul ke simpul yang lain dapat melewati sejumlah jalur. Keuntungan dari model ini adlah berkurangnya efek kegagalan persambungan jalur dan kadang terjadinya *congestion* (kemacetan) sambungan ke simpul tujuan. Sedangkan kerugian dai model ini adalah munculnya tunda pengiriman, serta mahalnya biaya persambungan, sehingga simpul-simpul pada model ini tidak disambungkan secara



Gambar 2.4 Topologi Mesh

- **Topologi Fisik *Cluster* (Pohon)**

Topologi model ini menggunakan sebuah komputer yang dihubungkan oleh jalur empat kawat ke titik cabang yang disebut *cluster controller* yang sesuai untuk rangkaian pertukaran telepon. *Cluster controller* memisahkan jalur menjadi dua atau lebih cabang dan setiap cabang dipisahkan menjadi dua atau lebih cabang oleh *cluster controller* yang lain dan seterusnya sampai dicapai maksimum dua belas cabang. Diperlukan sebuah modem pada ujung komputer pada jalur utama dan



Gambar 2.5 Topologi Cluster

D. Alamat IP

Alamat IP adalah alamat *Software,* Bukan alamat Hardware pengalamatan IP ditujukan untuk memungkinkan *Host* didalam jaringan bisa berkomunikasi dengan host pada jaringan yang berbeda, tanpa memperdulikan tipe LAN yang digunakan oleh *Host* yang berparsitipasi. IP address adalah alamat khas yang harus dimiliki oleh setiap komputer yang terhubung ke dalam sebuah jaringan komputer. Tidak boleh ada dua komputer yang memiliki IP Address yang sama. IP Address ini nantinya dibutuhkan dalam pengiriman paket-paket data, karena dalam setiap paket data tersebut terdapat header yang berisi IP Address dari tujuan paket-paket data tersebut. IP address ini diberikan ke jaringan dan peralatan jaringan yang menggunakan protokol TCP/IP. IP address terdiri atas 32-bit angka biner yang dapat dituliskan sebagai empat angka desimal yang dipisahkan oleh tanda titik seperti: 192.168.0.1.

- **Kelas IP address**

Seperti telah dijelaskan sebelumnya, IP address terdiri atas 32-bit angka

oleh tanda titik. Contohnya adalah seperti dibawah ini:

11000000.00010000.00001010.00000001

Atau dapat juga ditulis dalam bentuk empat kelompok angka desimal (0-255) seperti contoh berikut:

192.16.10.1

Atau secara simbolik dapat dituliskan sebagai empat kelompok angka sebagai berikut:

w.x.y.z

IP address terdiri atas dua bagian yaitu network ID dan host ID, di mana *network* ID menentukan alamat dari jaringan, sedangkan host ID menentukan alamat dari peralatan jaringan. Oleh sebab itu IP address memberikan alamat lengkap suatu peralatan jaringan beserta alamat jaringan di mana peralatan itu berada. Ini sama ibaratnya dengan alamat rumah, yang terdiri atas nama jalan dan nomor rumah, dimana network ID merupakan nama jalan dan host ID merupakan nomor rumah.

Berapa jumlah kelompok angka yang termasuk network ID dan berapa yang termasuk host ID, bergantung pada kelas dari IP address yang dipakai. Untuk mempermudah pemakaian, bergantung pada kebutuhan pemakai. Oleh sebab itu

Kelas	A	B	C
Network ID	w.	w.x	w.x.y
Host ID	x.y.z	y.z	Z
Default Subnet Mask	255.0.0.0	255.255.0.0	255.255.255.0

Tabel 2.1 Kelas-kelas IP address dengan default subnet mask

Untuk dapat menandai kelas satu dengan kelas yang lain, maka dibuat beberapa peraturan sebagai berikut:

Oktet pertama dari kelas A harus dimulai dengan angka biner 0.

Oktet pertama dari kelas B harus dimulai dengan angka biner 10.

Oktet pertama dari kelas C harus dimulai dengan angka biner 110.

Oleh sebab itu, IP address dari masing-masing kelas harus dimulai dengan angka desimal tertentu pada oktet pertama, seperti terlihat pada Table 2.7 berikut ini.

Kelas	A	B	C
Range	1-126	128-191	192-223
Jumlah Maksimum Network	127	16384	2097152

Jumlah Maksimum Host per Network	16777214	65534	254

Tabel 2.2 Jumlah network dan host dari kelas-kelas IP address

Disamping itu ada pula beberapa aturan tambahan, yaitu:

- Angka 127 di oktet pertama digunakan untuk loopback.
- Network ID tidak boleh semuanya terdiri atas angka 0 atau 1.
- Host ID tidak boleh semuanya terdiri atas angka 0 atau 1.

E. Tipe dari Jaringan Nirkabel

Sama halnya seperti jaringan yang berbasis kabel, maka jaringan nirkabel dapat diklasifikasikan ke dalam beberapa tipe yang berbeda berdasarkan pada jarak dimana data dapat ditransmisikan.

- **Wireless Wide Area Networks (WWANs)**

Teknologi WWAN memungkinkan pengguna untuk membangun koneksi nirkabel melalui jaringan publik maupun privat. Koneksi ini dapat dibuat mencakup suatu daerah yang sangat luas, seperti kota atau negara, melalui penggunaan beberapa antena atau juga sistem satelit yang diselenggarakan oleh penyelenggara jasa telekomunikasinya. Teknologi WWAN saat ini dikenal dengan sistem 2G (second generation) Inti dari sistem 2G ini termasuk di dalamnya

Global System for Mobile Communications (GSM), Cellular Digital Packet Data (CDPD) dan juga Code Division Multiple Access (CDMA). Berbagai usaha sedang dilakukan untuk transisi dari 2G ke teknologi 3G (third generation) yang akan segera menjadi standar global dan memiliki fitur roaming yang global juga. ITU juga secara aktif dalam mempromosikan pembuatan standar global bagi teknologi 3G.

- **Wireless Metropolitan Area Networks (WMANs)**

Teknologi WMAN memungkinkan pengguna untuk membuat koneksi nirkabel antara beberapa lokasi di dalam suatu area metropolitan (contohnya, antara gedung yang berbeda-beda dalam suatu kota atau pada kampus universitas), dan ini bisa dicapai tanpa biaya fiber optic atau kabel tembaga yang terkadang sangat mahal. Sebagai tambahan, WMAN dapat bertindak sebagai backup bagi jaringan yang berbasis kabel dan dia akan aktif ketika jaringan yang berbasis kabel tadi mengalami gangguan. WMAN menggunakan gelombang radio atau cahaya infrared untuk mentransmisikan data. Jaringan akses nirkabel broadband, yang memberikan pengguna dengan akses berkecepatan tinggi, merupakan hal yang banyak diminati saat ini. Meskipun ada beberapa teknologi yang berbeda, seperti multichannel multipoint distribution service (MMDS) dan local multipoint distribution services (LMDS) digunakan saat ini, tetapi kelompok kerja IEEE 802.16 untuk standar akses nirkabel broadband masih terus membuat spesifikasi bagi teknologi-teknologi tersebut.

- **Wireless Local Area Networks (WLANs)**

Teknologi WLAN membolehkan pengguna untuk membangun jaringan nirkabel dalam suatu area yang sifatnya lokal (contohnya, dalam lingkungan gedung kantor, gedung kampus atau pada area publik, seperti bandara atau kafe). WLAN dapat digunakan pada kantor sementara atau yang mana instalasi kabel permanen tidak diperbolehkan. Atau WLAN terkadang dibangun sebagai suplemen bagi LAN yang sudah ada, sehingga pengguna dapat bekerja pada berbagai lokasi yang berbeda dalam lingkungan gedung. WLAN dapat dioperasikan dengan dua cara. Dalam infrastruktur WLAN, stasiun wireless (peranti dengan network card radio atau eksternal modem) terhubung ke access point nirkabel yang berfungsi sebagai bridge antara stasiun-stasiun dan network backbone yang ada saat itu. Dalam lingkungan WLAN yang sifatnya peer-to-peer (ad hoc), beberapa pengguna dalam area yang terbatas, seperti ruang rapat, dapat membentuk suatu jaringan sementara tanpa menggunakan access point, jika mereka tidak memerlukan akses ke sumber daya jaringan.Pada tahun 1997, IEEE meng-approve standar 802.11 untuk WLAN, yang mana menspesifikasikan suatu data transfer rate 1 sampai 2 megabits per second (Mbps). Di bawah 802.11b, yang mana menjadi standar baru yang dominan saat ini, data ditransfer pada kecepatan maksimum 11 Mbps melalui frekuensi 2.4 gigahertz (GHz). Standar yang lebih baru lainnya adalah 802.11a, yang mana menspesifikasikan data

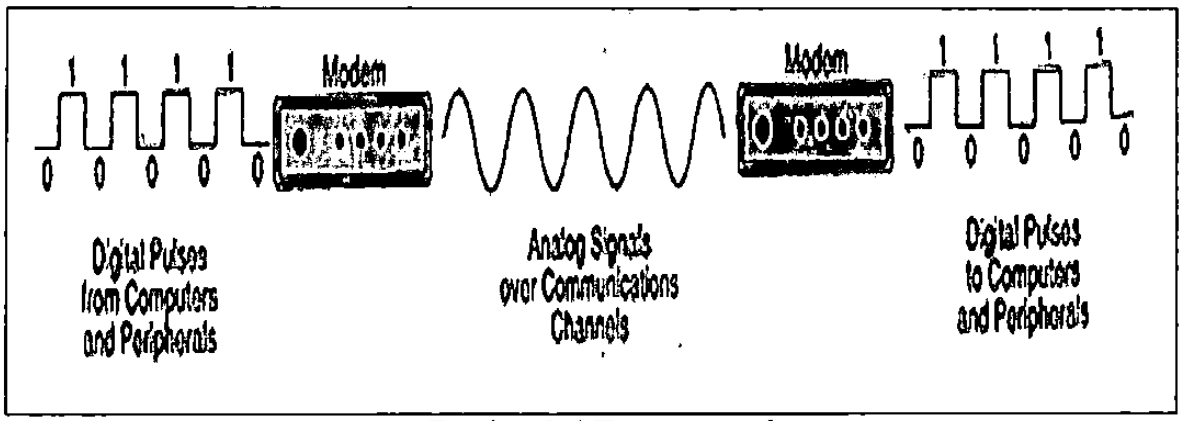
• **Wireless Personal Area Networks (WPANs)**

Teknologi WPAN membolehkan pengguna untuk membangun suatu jaringan nirkabel (ad hoc) bagi peranti sederhana, seperti PDA, telepon seluler atau laptop. Ini bisa digunakan dalam ruang operasi personal (personal operating space atau POS). Sebuah POS adalah suatu ruang yang ada disekitar orang, dan bisa mencapai jarak sekitar 10 meter. Saat ini, dua teknologi kunci dari WPAN ini adalah Bluetooth dan cahaya infra merah. Bluetooth merupakan teknologi pengganti kabel yang menggunakan gelombang radio untuk mentransmisikan data sampai dengan jarak sekitar 30 feet. Data Bluetooth dapat ditransmisikan melewati tembok, saku ataupun tas. Teknologi Bluetooth ini digerakkan oleh suatu badan yang bernama Bluetooth Special Interest Group (SIG), yang mana mempublikasikan spesifikasi Bluetooth versi 1.0 pada tahun 1999. Cara alternatif lainnya, untuk menghubungkan peranti dalam jarak sangat dekat (1 meter atau kurang), maka user bisa menggunakan cahaya infra merah.Untuk menstandarisasi pembangunan dari teknologi WPAN, IEEE telah membangun kelompok kerja 802.15 bagi WPAN. Kelompok kerja ini membuat standar WPAN, yang berbasis pada spesifikasi Bluetooth versi 1.0. Tujuan utama dari standarisasi ini adalah untuk mengurangi kompleksitas, konsumsi daya yang rendah, interoperabilitas dan bisa hidup berdampingan dengan jaringan 802.11.

F. Modem

adalah suatu processor telekomunikasi yang paling umum digunakan. Modem mengubah sinyal digital dari computer atau terminal pengirim menjadi

frekuensi analog yang dapat ditransmisikan melaui saluran telefon, dan begitu juga sebaliknya mengubah data analog menjadi data digital. Proses ini di kenal dengan modulasi dan demodulasi yang diterangkan oleh gambar berikut:



Gambar 2.6 Tentang modem

G. WiFi *(Wireless Fidelity)*

Wi-Fi (Wireless Fidelity) memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (Wireless Local Area Networks disingkat WLAN) yang didasari pada spesifikasi IEEE 802.11. Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.16 g, saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya. Awalnya Wi-Fi ditujukan untuk pengunaan perangkat nirkabel dan Jaringan Local (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinan komputer dengan kartu nirkabel (wireless card) atau personal digital assistant

Jaringan Wifi memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Saat ini,perkembangan teknologi wifi sangat signifikan sejalan dengan kebutuhan sistem informasi yang mobile. Banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan wifi pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. Hal ini membuat para hacker menjadi tertarik untuk mengexplore keamampuannya untuk melakukan berbagai aktifitas yang biasanya ilegal menggunakan wifi. Wi-Fi (Wireless Fidelity) adalah koneksi tanpa kabel seperti handphone dengan mempergunakan teknologi radio sehingga pemakainya dapat mentransfer data dengan cepat dan aman. Wi-Fi tidak hanya dapat digunakan untuk mengakses internet, Wi-Fi juga dapat digunakan untuk membuat jaringan tanpa kabel di perusahaan. Karena itu banyak orang mengasosiasikan Wi-Fi dengan "Kebebasan" karena teknologi Wi-Fi memberikan kebebasan kepada pemakainya untuk mengakses internet atau mentransfer data dari ruang meeting, kamar hotel, kampus, dan café-café yang bertanda "Wi-Fi Hot Spot". Juga salah satu kelebihan dari Wi-Fi adalah kecepatannya yang beberapa kali lebih cepat dari modem kabel yang tercepat. Jadi pemakai Wi-Fi tidak lagi harus berada di dalam ruang kantor untuk bekerja. Tapi Wi-Fi hanya dapat di akses dengan komputer, laptop, PDA atau Cellphone yang telah dikonfigurasi dengan Wi-Fi certified Radio. Untuk Laptop, pemakai dapat menginstall Wi-Fi PC Cards yang berbentuk kartu di PCMCIA Slot yang telah tersedia. Untuk PDA, pemakai dapat

pengguna yang komputer atau PDA - nya menggunakan Window XP, hanya dengan memasangkan kartu ke slot yang tersedia,

Window XP akan dengan sendirinya mendeteksi area disekitar Anda dan mencari jaringan Wi-Fi yang terdekat dengan Anda. Amatlah mudah menemukan tanda apakah peranti tersebut memiliki fasilitas Wi-Fi, yaitu dengan mencermati logo *Wi-Fi CERTIFIED* pada kemasannya. Meskipun Wi-Fi hanya dapat diakses ditempat yang bertandakan "Wi-Fi Hotspot", jumlah tempat-tempat umum yang menawarkan "Wi Fi Hotspot" meningkat secara drastis. Hal ini disebabkan karena dengan dijadikannya tempat mereka sebagai "Wi-Fi Hotspot" berarti pelanggan mereka dapat mengakses internet yang artinya memberikan nilai tambah bagi para pelanggan. Layanan Wi-Fi yang ditawarkan oleh masing-masing "*Hots Spot*" pun beragam, ada yang menawarkan akses secara gratis seperti halnya di executive lounge Bandara, ada yang mengharuskan pemakainya untuk menjadi pelanggan salah satu ISP yang menawarkan fasilitas Wi-Fi dan ada juga yang menawarkan kartu pra-bayar. Apapun pilihan Anda untuk cara mengakses Wi-Fi, yang terpenting adalah dengan adanya Wi-Fi, Anda dapat bekerja dimana saja

dan kapan saja hingga Anda tidak perlu harus selalu terkurung di ruang kerja Anda untuk menyelesaikan setiap pekerjaan.

- **Keamanan wireless hanya dengan kunci WEP**

  WEP merupakan standart keamanan & enkripsi pertama yang digunakan

- Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
- WEP menggunakan kunci yang bersifat statis
- Masalah *initialization vector* (IV) WEP
- Masalah integritas pesan *Cyclic Redundancy Check* (CRC-3 2)

WEP terdiri dari dua tingkatan, yakni kunci 64 bit, dan 128 bit. Sebenarnya kunci rahasia pada kunci WEP 64 bit hanya 40 bit, sedang 24bit merupakan Inisialisasi Vektor (IV). Demikian juga pada kunci WEP 128 bit, kunci rahasia terdiri dari 104bit.

Serangan-serangan pada kelemahan WEP antara lain :

- Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut FMS attack. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin sanyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan
- Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
- Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan *traffic*

mengumpulkan packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan *traffic injection,*diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

- **Keamanan wireless hanya dengan kunci WPA-PSK atau WPA2-PSK**

  WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS. Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline. Brute force dengan menggunakan mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang yang digunakan wireless tersebut memang terapat pada kamus kata yang digunakan si hacker. Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK

- **MAC Filtering**

  Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering. Hal ini sebenarnya tidak banyak membantu

mudah dispoofing atau bahkan dirubah. Tools *ifconfig* pada OS Linux/Unix atau beragam tools spt network utilitis, regedit, smac, machange pada OS windows dengan mudah digunakan untuk spoofing atau mengganti MAC address. Penulis masih sering menemukan wifi di perkantoran dan bahkan ISP (yang biasanya digunakan oleh warnet-warnet) yang hanya menggunakan proteksi MAC Filtering. Dengan menggunakan aplikasi wardriving seperti kismet/kisMAC atau aircrack tools, dapat diperoleh informasi MAC address tiap client yang sedang terhubung ke sebuah *Access Point*. Setelah mendapatkan informasi tersebut, kita dapat terhubung ke Access point dengan mengubah MAC sesuai dengan client tadi. Pada jaringan wireless, duplikasi MAC address tidak mengakibatkan konflik. Hanya membutuhkan IP yang berbeda dengan client yang tadi.

- **Captive Portal**

  Infrastruktur Captive Portal awalnya didesign untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (open network). Captive portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi/otentikasi. Berikut cara kerja captive portal :

  - user dengan wireless client diizinkan untuk terhubung wireless

- block semua trafik kecuali yang menuju ke captive portal (Registrasi/Otentikasi berbasis web) yang terletak pada jaringan kabel.
- *redirect* atau belokkan semua trafik web ke captive portal
- setelah user melakukan registrasi atau login, izinkan akses ke jaringan (internet)

Beberapa hal yang perlu diperhatikan, bahwa captive portal hanya melakukan tracking koneksi client berdasarkan IP dan MAC address setelah melakukan otentikasi. Hal ini membuat captive portal masih dimungkinkan digunakan tanpa otentikasi karena IP dan MAC adress dapat dispoofing. Serangan dengan melakukan spoofing IP dan MAC. Spoofing MAC adress seperti yang sudah dijelaskan pada bagian 4 diatas. Sedang untuk spoofing IP, diperlukan usaha yang lebih yakni dengan memanfaatkan ARP cache poisoning, kita dapat melakukan redirect trafik dari client yang

sudah terhubung sebelumnya. Serangan lain yang cukup mudah dilakukan adalah menggunakan Rogue AP, yaitu mensetup Access Point (biasanya menggunakan HostAP) yang menggunakan komponen informasi yang sama seperti AP target seperti SSID, BSSID hingga kanal frekwensi yang digunakan. Sehingga ketika ada client yang akan terhubung ke AP buatan kita, dapat kita membelokkan trafik ke AP sebenarnya. Tidak jarang captive portal yang dibangun pada suatu hotspot memiliki kelemahan pada konfigurasi atau design jaringannya. Misalnya, otentikasi masih menggunakan plain text (http), managemen jaringan dapat

Kelemahan lain dari captive portal adalah bahwa komunikasi data atau trafik ketika sudah melakukan otentikasi (terhubung jaringan) akan dikirimkan masih belum terenkripsi, sehingga dengan mudah dapat disadap oleh para hacker. Untuk itu perlu berhati-hati melakukan koneksi pada jaringan hotspot, agar mengusahakan menggunakan komunikasi protokol yang aman seperti https,pop3s, ssh, imaps dst.

Wi-Fi dirancang berdasarkan spesifikasi IEEE 802.11. Sekarang ini ada empat variasi dari 802.11, yaitu:

- 802.11a
- 802.11b
- 802.11g
- 802.11n

Spesifikasi *b* merupakan produk pertama Wi-Fi. Variasi *g* dan *n* merupakan salah satu produk yang memiliki penjualan terbanyak pada 2005.

Spesifikasi Wi-Fi			
Spesifikasi	**Kecepatan**	**Frekuensi Band**	**Cocok dengan**
802.11b	11 Mb/s	2.4 GHz	b
802.11a	54 Mb/s	5 GHz	a
802.11g	54 Mb/s	2.4 GHz	b, g

802.11n	100 Mb/s	2.4 GHz	b, g, n

Tabel 2.3 Spesifikasi Wi-Fi

Di banyak bagian dunia, frekuensi yang digunakan oleh Wi-Fi, pengguna tidak diperlukan untuk mendapatkan ijin dari pengatur lokal (misal, Komisi Komunikasi Federal di A.S.). 802.11a menggunakan frekuensi yang lebih tinggi dan oleh sebab itu daya jangkaunya lebih sempit, lainnya sama.

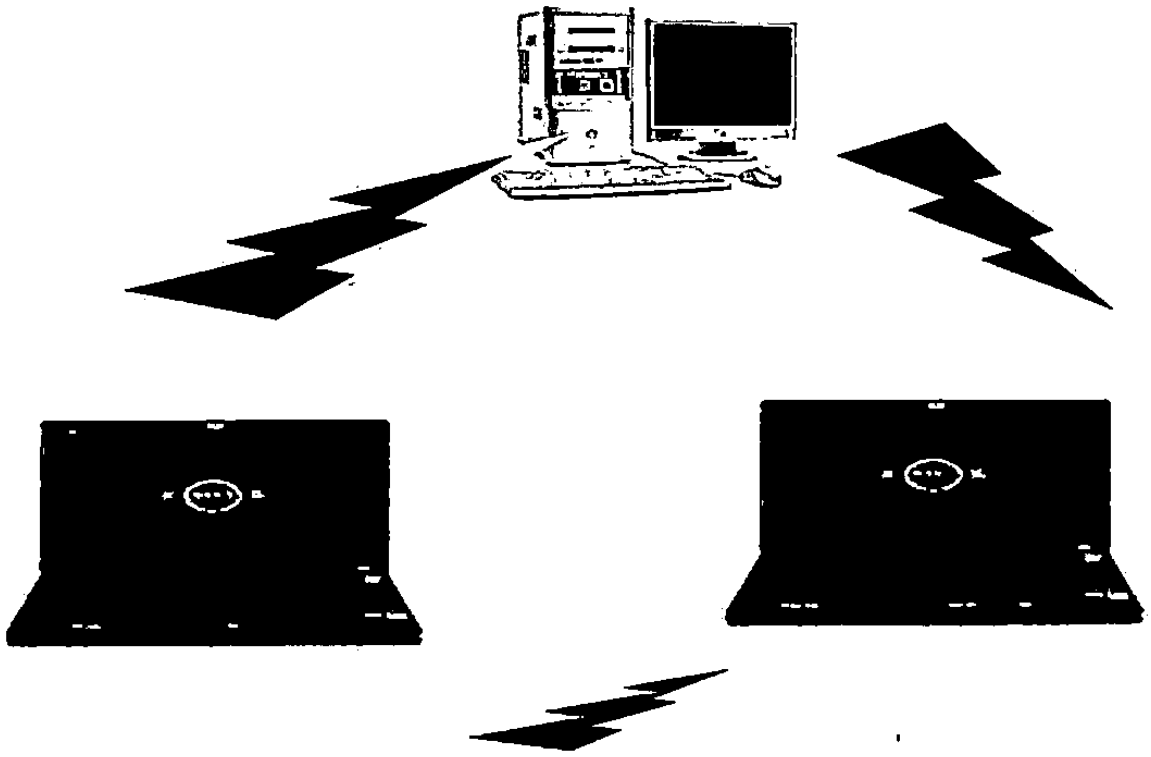
Versi Wi-Fi yang paling luas dalam pasaran AS sekarang ini (berdasarkan dalam IEEE 802.11b/g) beroperasi pada 2.400 MHz sampai 2.483,50 MHz. Dengan begitu mengijinkan operasi dalam 11 channel (masing-masing 5 MHz).

- **Tipe Jaringan WiFi**

Seperti halnya Ethernet-LAN (jaringan dengan kebel), jaringan wifi juga dikonfigurasikan ke dalam dua jenis tipe jaringan yaitu:

- **Jaringan Peer To Peer Atau Adhoc Wireless LAN**

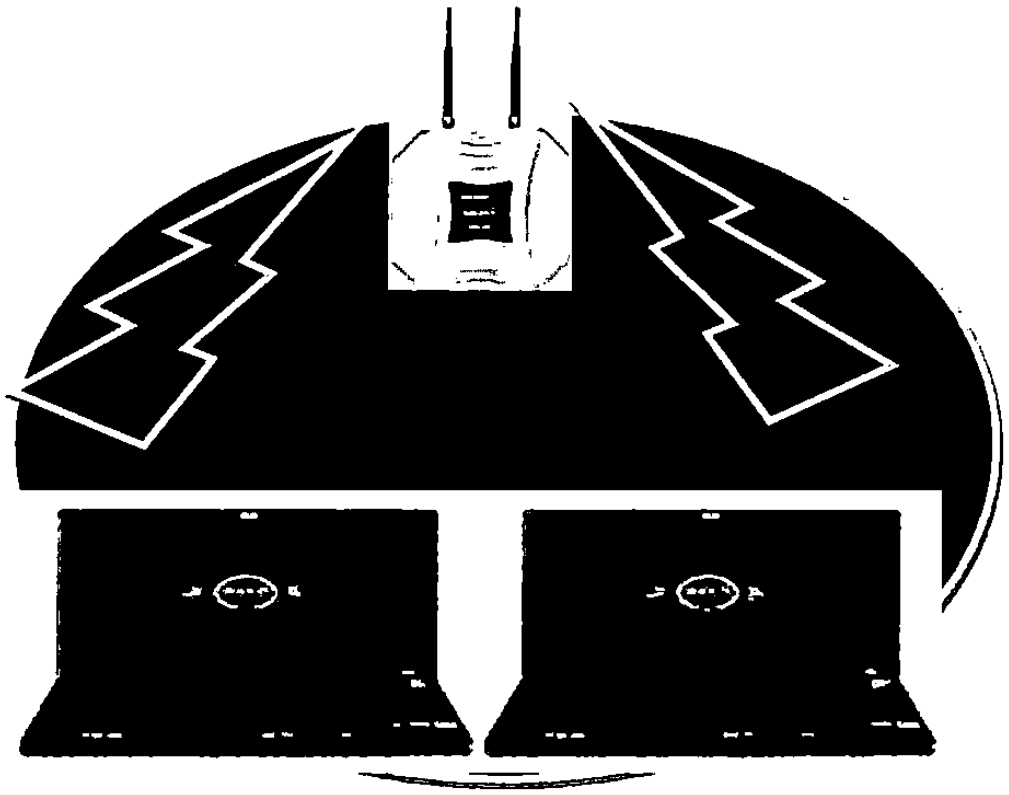
  Computer dapat saling berhubungan berdasarkan nama SSID (service



Gambar 2.7 Adhoc wireless LAN

- **Jaringan Server Based Atau Wireless Infrstruktur**

system infrastruktur membutuhkan sebuah komponen khusus yang



Gambar 2. 8 Wireless infrastruktur

- **Keamanan Jaringan WiFi**

Per alatan sinyal yang ditranmisikan oleh jaringan wifi menggunakan frekuensi secara bebas, sehingga dapat ditangkap oleh computer lain sesame user wifi. keamanan jaringan wifi secara umum terdiri dari *nonsecure* dan share key (secure):

- **non secure**: computer yang mempunyai wifi dapat menangkap transmisi pancaran dari sebuah wifi dan langsung dapat masuk kedalam jaringan tersebut
- **share key**; untuk dapat masuk ke jaringan wifi diperlukan kunci atau password, contohnya sebuah network yang menggunakan WEP

- selain menggunakan WEP, dapat ditambahkan WPA (wifi protected access).
- membatasi akses dengan mendaftarkan MAC Address dari koomputer klien yang berhak mengakses jaringan.

H. Sistem Seluler

- **FDMA**

FDMA adalah sistem multiple access yang menempatkan seorang pelanggan pada sebuah kanal berbentuk pita frekuensi (frequency band) komunikasi. Jika satu pita frekuensi dianggap sebagai satu jalan, maka FDMA merupakan teknik "satu pelanggan, satu jalan". Pada saat pelanggan A sedang menggunakan jalan itu, maka pelanggan lain tidak dapat menggunakan sebelum pelanggan A selesai. Jadi, kalau dalam waktu yang bersamaan ada 100 pelanggan yang ingin berkomunikasi dengan rekannya, maka sudah tentu diperlukan 100 pita frekuensi. Kalau setiap pita memerlukan lebar 30 Kilo Hertz (kHz) dan frekuensi yang digunakan berawal dari 890 Mega Hertz (MHz), maka:

- Pita frekuensi kanal 1 mulai dari 890 MHz hingga 890,030 Mhz
- Pita frekuensi kanal 2 mulai dari 890,030 MHz hingga 890,060 MHz
- Pita frekuensi kanal3 mulai dari 890,060 MHz hingga 890,090 MHz dan seterusnya.

Sedangkan lebar total seluruh pita yang digunakan adalah: 100 x 30.000 Hz =

bawah 890 MHz, maka batas atasnya adalah 893 MHz. Akan tetapi, frekuensi yang tersedia untuk komunikasi bergerak dibatasi oleh peraturan yang ada karena frekuensi-frekuensi lain pasti digunakan untuk jatah keperluan yang lain pula. Sementara jatah frekuensi yang ada pun harus dibagi antarpenyelenggara telepon seluler. Karena itu, untuk memperbanyak kapasitas dengan jumlah kanal yang terbatas, digunakan trik-trik tertentu sesuai dengan strategi si penyelenggara.

- **TDMA**

TDMA Berbeda dengan FDMA yang memberikan satu pita frekuensi untuk dipakai satu pelanggan, TDMA memberikan satu pita frekuensi untuk dipakai beberapa pelanggan. Jadi kanal-kanal komunikasi dirupakan dalam bentuk slot-slot waktu. Slot waktu adalah berapa lama seorang pelanggan mendapat giliran untuk memakai pita frekuensi. Satu slot waktu digunakan oleh satu pelanggan. Slot-slot waktu ini dibingkai dalam satu periode yang disebut satu frame. Jadi misalkan ada 10 pelanggan yang masing-masing adalah A, B, C, D, E, F, G, H, I, dan J, maka dalam satu frame terdapat 10 slot waktu yang merupakan giliran tiap pelanggan untuk menggunakan pita frekuensi yang sama.

Proses komunikasi multi-access dilakukan dengan menjalankan frame ini berulang- ulang sehingga akan muncul urutan giliran pemakaian saluran seperti:A –B – C – D – E – F – G – H – I – J – A – B- C – D – E – F – G – H – I – J – A – B - C-dan seterusnya. Tentu saja harus ada pembatasan jumlah pelanggan yang menggunakan satu pita frekuensi ini. Jika tidak dibatasi, periode frame akan

mengganggu pembicaraan. Karena sifatnya yang tidak kontinyu (tidak terjadi pemakaian pita frekuensi terus menerus oleh satu pelanggan dalam satu periode pembicaraan), maka teknik TDMA hanya dapat mengakomodasi data digital atau modulasi digital. Sehingga sinyal-sinyal analog yang akan dikirim, harus diubah menjadi format digital dahulu.

- **CDMA**

Teknik CDMA adalah temuan yang lebih baru dibandingkan dengan FDMA dan TDMA. Teknik CDMA berawal pada tahun 1949 ketika Claude Shannon dan Robert Pierce (yang banyak jasanya untuk kemajuan teknologi telekomunikasi saat ini) menyampaikan ide dasar CDMA. Teknik ini merupakan temuan yang brilian karena kanal yang satu dengan lainnya tidak dibedakan dari frekuensi/FDMA atau waktu/TDMA yang secara awam lebih mudah dipahami, melainkan dengan perbedaan kode. Jadi pada CDMA, seluruh pelanggan menggunakan frekuensi yang sama pada waktu yang sama. Dalam diagram blok CDMA tampak bahwa data input dari satu pelanggan dikalikan dengan salah satu dari banyak kode PN (pseudo noise). Jumlah kemungkinan kode yang dihasilkan oleh generator kode PN identik dengan jumlah kanal yang disediakan. Jika generator kode PN mampu menghasilkan 100 kode, maka sebanyak itu pula kanal yang diperoleh. Oleh modulator hasil perkalian antara input data dengan kode PN ditumpangkan pada sinyal RF (radio frequency) agar dapat dikirim lewat udara.

ditumpanginya. Sinyal pesan yang mengandung kode ini dicocokkan dengan kode PN di penerima. Sinyal pesan akan dipisahkan dari kode dan diteruskan jika kode PN pada sinyal masuk sama dengan kode PN pada penerima. CDMA (juga disebut DSSS/ direct sequence spread spectrum) merupakan salah satu dari dua jenis teknik murni spread spectrum multiple access (SSMA). Jenis lainnya dikenal sebagai FHMA (frequency hopping spread spectrum). Kedua jenis ini tergolong SSMA karena sinyalnya tersebar (spread) pada spektrum pita frekuensi yang lebar. Pada CDMA, penyebaran sinyal diperoleh akibat proses perkalian data input (yang mempunyai waktu perubahan lambat) dengan kode PN (yang mempunyai waktu perubahan cepat). Walaupun pita frekuensinya lebar, tegangan sinyal yang dihasilkan sangat kecil, menyerupai noise (bising) yang selalu menyertai gelombang radio. Sehingga apabila dimonitor oleh penerima lain, sinyal yang dipancarkan oleh pengirim berbasis CDMA hanya berupa noise (seolah-olah menunjukkan ketiadaan sinyal pancar) yang tidak mengganggu sinyal lain. Sifat CDMA yang lain adalah kemampuannya untuk tahan terhadap jamming (penutupan oleh sinyal yang lebih kuat) pada pita frekuensi sempit. Hal ini terjadi karena jamming pada pita frekuensi sempit itu tidak akan mengganggu sinyal-sinyal CDMA yang tersebar di pita frekuensi lain. Biar begitu jika diterapkan pada telepon seluler, CDMA mempunyai masalah yang disebut near-far problem. Masalah ini terjadi akibat pemakaian pita frekuensi yang sama pada waktu yang sama. Akibatnya, pelanggan yang paling dekat dengan base station (BTS) akan mendominasi BTS karena sinyalnya diterima (oleh BTS) paling besar dibandingkan dengan pelanggan lain yang jaraknya lebih jauh. Bagi pelayanan

yang baik, hal itu tidak diharapkan. Untuk mengatasinya dipakailah teknik power control. Teknik ini menyebabkan BTS memerintahkan ponsel pelanggan untuk mengurangi daya pancar (secara otomatis) ketika sinyalnya diterima paling besar. Sehingga seluruh pelanggan di areal cakupan BTS akan diterima dengan besar sinyal yang sama. CDMA dapat dikombinasikan dengan teknik lain untuk menjadi teknik hibrid semacam:

FCDMA yang merupakan kombinasi dari FDMA dan CDMA, TCDMA yang merupakan kombinasi dari TDMA dan CDMA. Juga ada DS-FHMA yang merupakan kombinasi dari CDMA/DSSS dengan FHMA. Jadi, dunia komunikasi bergerak akan terus melejit dan melahirkan teknologi terbaru. Tidak hanya fitur-fitur ponsel, tetapi juga dukungansaluran telekomunikasi.

Penelitian ini menggunakan Router TP–link MR 3420 dan penyedia layanan internet dari Smartfren dengan tehnologi CDMA dan pengujian sinyal wireless menggunakan *Software* InSSIDer2.0 yang merupakan software pemantau jaringan wireless inSSIDer menampilkan grafik real time yang menggambarkan kekuatan