DASAR-DASAR TEKNIK JARINGAN KOMPUTER DAN TELEKOMUNIKASI

BAB II

MEDIA DAN SISTEM JARINGAN TELEKOMUNIKASI

KELAS X

SMK / MAK

BAB II

Media dan Sistem Jaringan Telekomunikasi

Elemen

Media dan sistem pada bidang jaringan komputer dan dunia internet

Tujuan Pembelajaran

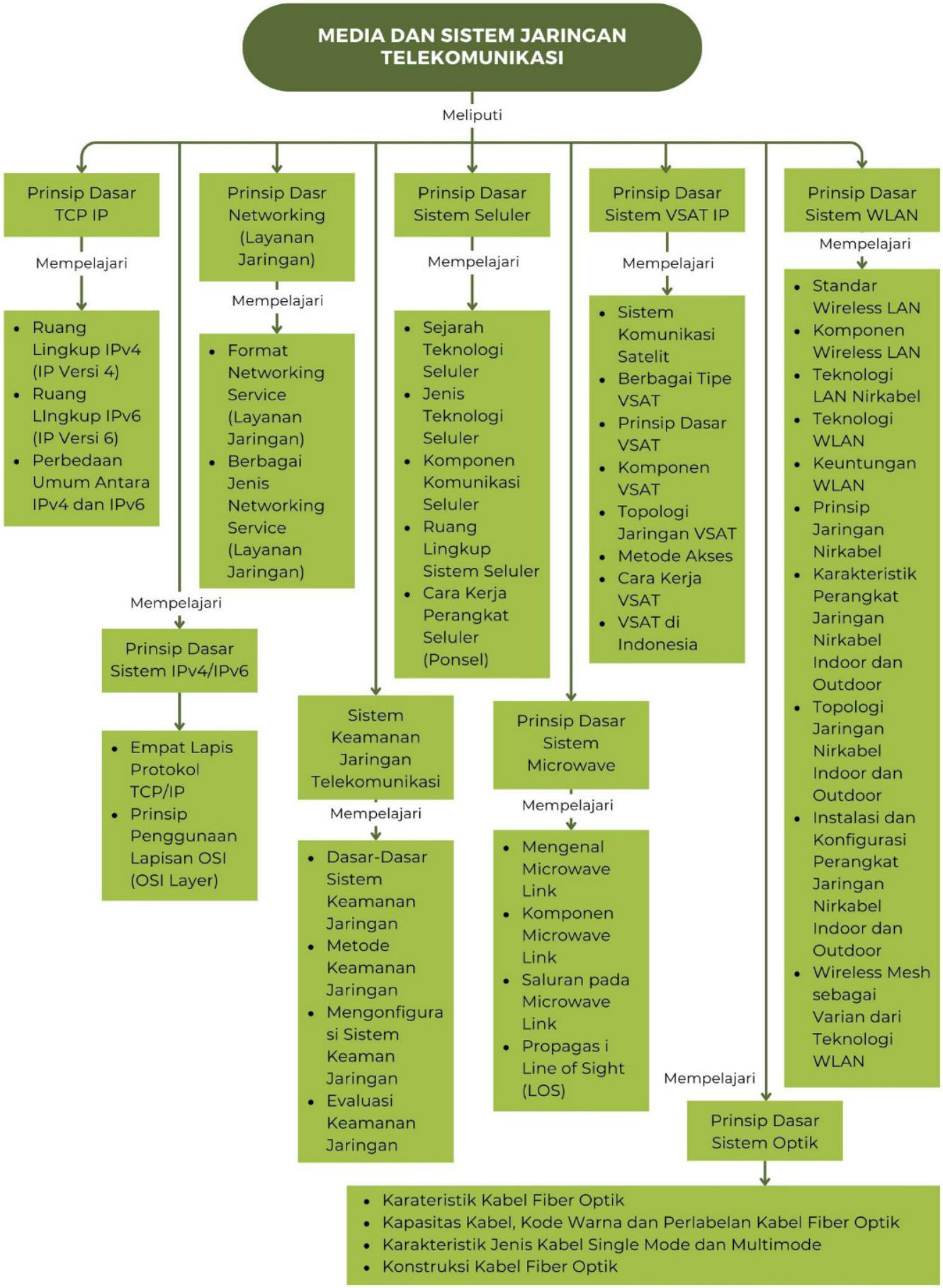
Setelah mempelajari bab ini, siswa diharapkan mampu:

1. Memahami prinsip dasar TCP/IP
2. Memahami prinsip dasar sistem IPv4/IPv6;
3. Menjelaskan prinsip dasar sistem networking service;
4. Memahami prinsip dasar sistem keamanan jaringan telekomunikasi; serta
5. Memahami prinsip dasar sistem seluler, dasar sistem microwave, sistem VSAT IP, sistem optik, dan sistem WLAN.

Kata Kunci

- Alat ukur
- IPv4
- Keamanan jaringan telekomunikasi
- IPv6
- Microwave networking service
- Optik Seluler
- TCP IP
- VSAT
- IP
- WLAN

PETA KONSEP


MEDIA DAN SISTEM JARINGAN TELEKOMUNIKASI
Meliputi
Prinsip Dasar TCP IP
Mempelajari
Ruang Lingkup IPv4 (IP Versi 4)
Ruang LIngkup IPv6 (IP Versi 6)
Perbedaan Umum Antara IPv4 dan IPv6
Prinsip Dasr Networking (Layanan Jaringan)
Mempelajari
Format Networking Service (Layanan Jaringan)
Berbagai Jenis Networking Service (Layanan Jaringan)
Prinsip Dasar Sistem Seluler
Mempelajari
Sejarah Teknologi Seluler
Jenis Teknologi Seluler
Komponen Komunikasi Seluler
Ruang Lingkup Sistem Seluler
Cara Kerja Perangkat Seluler (Ponsel)
Prinsip Dasar Sistem VSAT IP
Mempelajari
Sistem Komunikasi Satelit
Berbagai Tipe VSAT
Prinsip Dasar VSAT
Komponen VSAT
Topologi Jaringan VSAT
Metode Akses
Cara Kerja VSAT
VSAT di Indonesia
Prinsip Dasar Sistem WLAN
Mempelajari
Standar Wireless LAN
Komponen Wireless LAN
Teknologi LAN Nirkabel
Teknologi WLAN
Keuntungan WLAN
Prinsip Jaringan Nirkabel
Karakteristik Perangkat Jaringan Nirkabel Indoor dan Outdoor
Topologi Jaringan Nirkabel Indoor dan Outdoor
Instalasi dan Konfigurasi Perangkat Jaringan Nirkabel Indoor dan Outdoor
Wireless Mesh sebagai Varian dari Teknologi WLAN
Mempelajari
Prinsip Dasar Sistem IPv4/IPv6
Empat Lapis Protokol TCP/IP
Prinsip Penggunaan Lapisan OSI (OSI Layer)
Sistem Keamanan Jaringan Telekomunikasi
Mempelajari
Dasar-Dasar Sistem Keamanan Jaringan
Metode Keamanan Jaringan
Mengonfigurasi Sistem Keaman Jaringan
Evaluasi Keamanan Jaringan
Prinsip Dasar Sistem Microwave
Mempelajari
Mengenal Microwave Link
Komponen Microwave Link
Saluran pada Microwave Link
Propagas i Line of Sight (LOS)
Mempelajari
Prinsip Dasar Sistem Optik
Karateristik Kabel Fiber Optik
Kapasitas Kabel, Kode Warna dan Perlabelan Kabel Fiber Optik
Karakteristik Jenis Kabel Single Mode dan Multimode
Konstruksi Kabel Fiber Optik

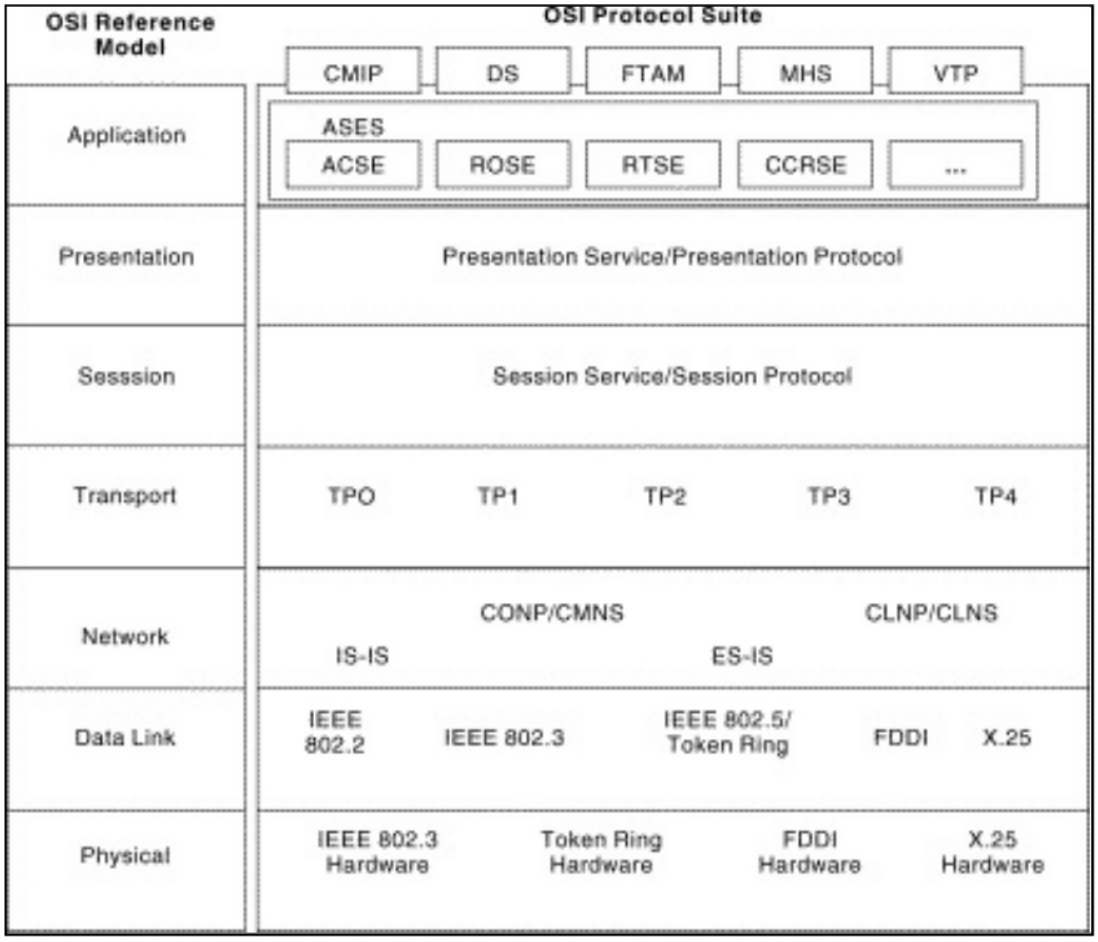
A. Prinsip Dasar TCP IP

Komunikasi data merupakan proses pengiriman data dari satu komputer ke komputer lain. Guna dapat mengirimkan data diperlukan alat khusus yang disebut network interface (interface jaringan). Jenis network interface ini bermacam-macam tergantung pada media fisik yang digunakan. Pada proses pengiriman data terdapat beberapa masalah yang harus dipecahkan. Pertama, data harus dapat dikirimkan ke komputer yang tepat sesuai tujuannya. Hal ini akan menjadi rumit jika komputer tujuan transfer data ini tidak berada pada jaringan lokal, melainkan di tempat yang jauh. Jika lokasi komputer yang saling berkomunikasi jauh (secara jaringan) maka terdapat kemungkinan data rusak atau hilang.

1. Empat Lapis Protokol TCP/IP

IP adalah singkatan dari Internet Protocol atau dalam bahasa Indonesia berarti protokol internet. Jadi, IP address atau Internet Protocol Address adalah alamat protokol internet (alamat IP) yang mengidentifikasi segala perangkat yang terhubung ke jaringan, baik jaringan internet pada umumnya maupun lokal. Saat mengunjungi sebuah website, perangkat yang digunakan perlu menemukan lokasi data website tersebut untuk kemudian mengambil datanya dan menyajikannya kepada visitor (pengunjung). Fungsi IP address adalah sebagai media komunikasi bagi suatu perangkat agar permintaan untuknya diarahkan ke tujuan yang tepat melalui jaringan.

Standar komunikasi dapat dikategorikan menjadi de facto (konvensi) dan dejure (secara hukum) yang salah satunya dalam bentuk protokol. Protokol secara umum digunakan pada komunikasi real time di mana standar digunakan untuk mengatur struktur dari informasi untuk penyimpanan jangka panjang. Protokol perlu diutamakan pada penggunaan standar teknis, untuk menspesifikasi bagaimana membangun komputer atau menghubungkan peralatan peranti keras. Protokol identik dengan sebuah aturan atau standar yang mengatur atau mengizinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada peranti keras, peranti lunak, maupun kombinasi dari keduanya.



Gambar 2. 1 OSI Protocol Suite

Dalam memecahkan masalah transfer data di atas para ahli jaringan komputer pun melakukan hal yang sama untuk setiap masalah komunikasi data, diciptakan solusi khusus berupa aturan-aturan untuk menangani masalah tersebut. Guna menangani semua masalah komunikasi data, keseluruhan aturan ini harus bekerja sama satu dengan yang lainnya. Sekumpulan aturan untuk mengatur proses pengiriman data ini disebut sebagai protokol komunikasi data. Protokol ini diterapkan dalam bentuk program komputer (software) yang terdapat pada komputer dan perlalatan komunikasi lainnya.

TCP/IP adalah sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data. TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Berkat prinsip ini, tugas masing-masing protokol menjadi sederhana. Protokol lain tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih saling mengirim dan menerima data.

TCP/IP terdiri atas empat lapis kumpulan protokol, yaitu Network Interface Layer, Internet Layer, Transport Layer, dan Application Layer. Jika suatu protokol menerima data dari protokol lain di lapisan atasnya, ia akan menambahkan informasi tambahan

miliknya ke data tersebut. Informasi ini disebut header yang berfungsi sesuai dengan fungsi protokol tersebut. Setelah itu data diteruskan ke protokol pada lapisan di bawahnya.

a. Lapisan terbawah, yaitu network interface layer yang bertanggung jawab mengirim dan menerima data ke dan dari media fisik (kabel, serat optik, dan gelombang radio).
b. Lapisan berikutnya adalah internet layer yang bertanggung jawab dalam proses pengiriman paket ke alamat yang tepat. Pada layer ini terdapat tiga macam protokol yaitu, IP, ARP, dan ICMP. IP (Internet Protokol) berfungsi untuk menyampaikan paket data ke alamat yang tepat. ARP (Address Resolution Protokol) ialah protokol yang digunakan untuk menentukan alamat hardware dari host yang terletak pada jaringan yang sama.
c. Transport layer, berisi protokol yang bertanggung jawab untuk mengadakan komunikasi antara dua host. Kedua protokol tersebut ialah TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol).
d. Lapisan teratas ialah application layer. Pada lapisan inilah terletak semua aplikasi yang menggunakan protokol TCP/IP, seperti e-mail, FTP, HTTP, dan sebagainya.

Tugas 2.1

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri atas 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetaj yang berkaitan dengan penggunaan TCP/IP!
3. Masukkan hasilnya ke dalam table berikut!

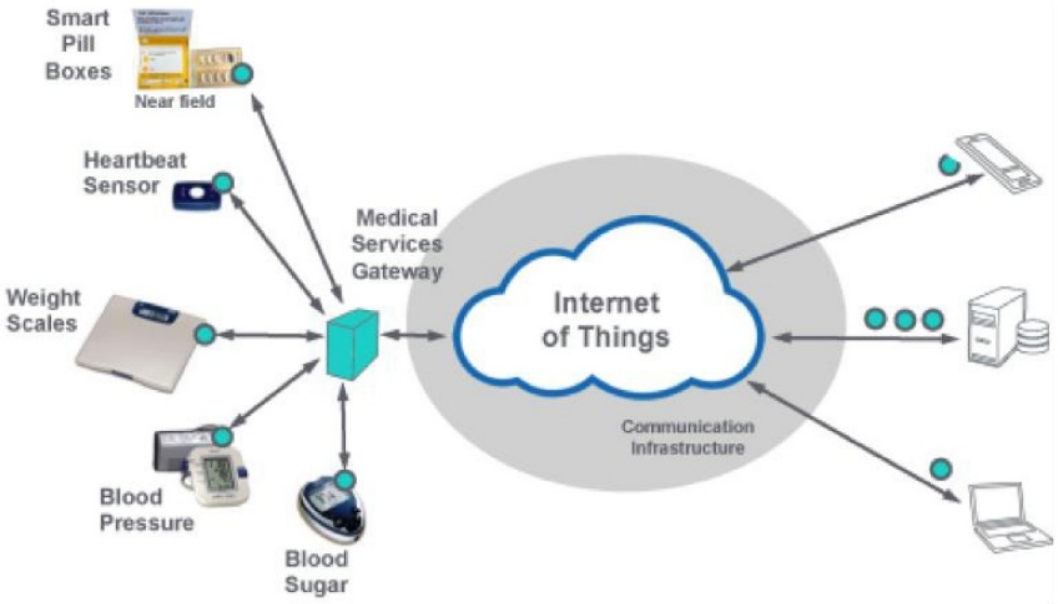
No	Penggunaan TCP/IP	Deskripsi

4. Diskusikan komponen dalam table tersebut Bersama teman kelompok Anda!
5. Presentasikan hasil diskusi kelompok Anda di depan kelas dan mintalah tanggapan dari kelompok lain!

2. Prinsip Penggunaan Lapisan OSI (OSI Layer)

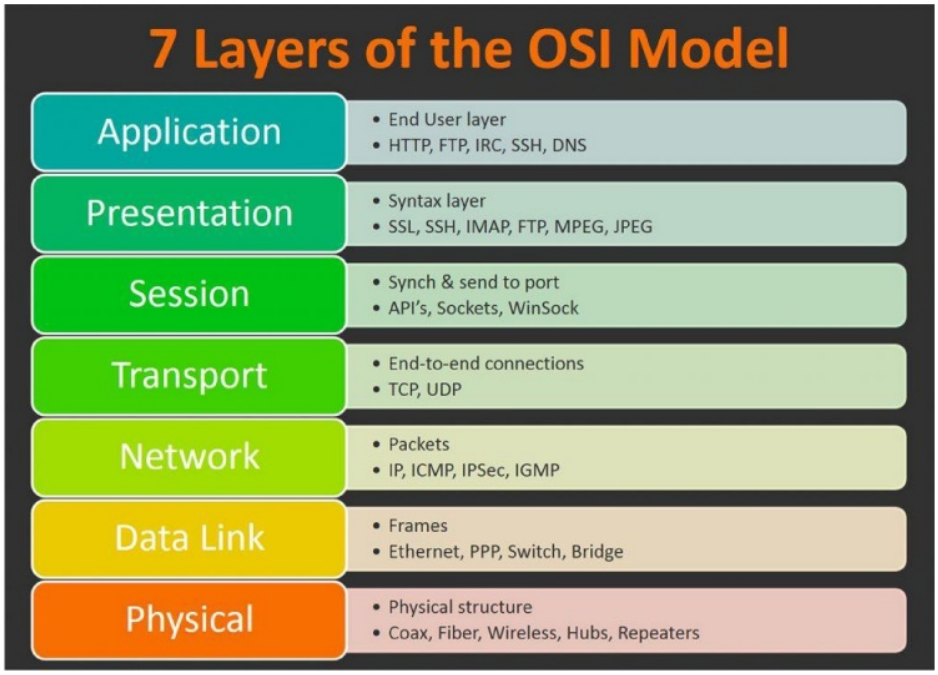
Teknologi OSI terdiri dari tujuh layer (lapisan), di mana setiap layer memiliki perannya masing-masing dengan tujuan utama user dapat berkomunikasi ke jaringan komputer lain. Model OSI di buat untuk mengatasi berbagai kendala internetworking akibat perbedaan arsitektur dan protokol jaringan. Pada arsitektur jaringan

komputer, terdapat suatu lapisan-lapisan (layer) yang memiliki tugas spesifik serta memiliki protokol tersendiri. Dalam suatu jaringan terdapat berbagai protokol jaringan yang berbeda, sehingga membuat berbagai jenis peranti tidak bisa saling berkomunikasi. Oleh sebab itu, International Organization for Standardization pada tahun 1977 membuat suatu arsitektur komunikasi yang di kenal sebagai Open System Interconection (OSI) model yang mendefinisikan standar untuk menghubungkan komputer-komputer dari vendor yang berbeda. Teknologi OSI terdiri atas physical layer (lapisan fisik), data link layer (lapisan data link), network layer (lapisan jaringan), transport layer (lapisan transport), session layer (lapisan session), presentation layer (lapisan presentasi), dan application layer (lapisan aplikasi). Dari 7 lapisan OSI Layer tersebut masih dikategorikan menjadi lower layer (meliputi physical layer, datalink layer, network layer) dan upper layer (meliputi transport layer, session layer, presentation layer, dan application layer).



Gambar 2. 2 Implementasi OSI Layer pada Diagram M2M

Model OSI menyediakan kerangka logika terstruktur tentang prosedur komunikasi data yang berinteraksi melalui jaringan. Standar ini dikembangkan untuk industri komputer agar berkomunikasi pada jaringan yang berbeda secara efisien. OSI berupaya membentuk standar umum jaringan komputer untuk menunjang interoperatibilitas antar vendor yang berbeda. Dalam mendesain suatu jaringan harus memperhatikan arsitektur standar yang telah dibuat oleh sebuah badan dunia (ISO).

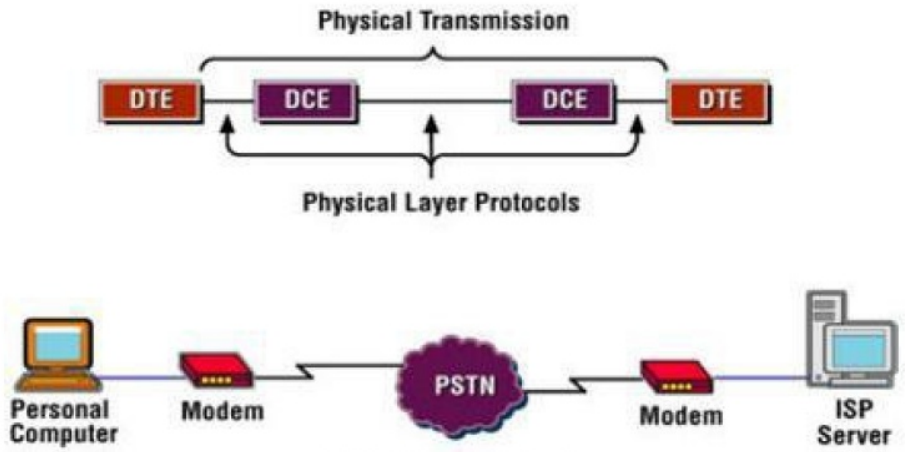


Gambar 2. 3 Pembagian pada OSI Layer

Layer-layer pada model Open Systems Interconnection (OSI) terdiri atas sebagai berikut.

a. Physical Layer (Lapisan Fisik)

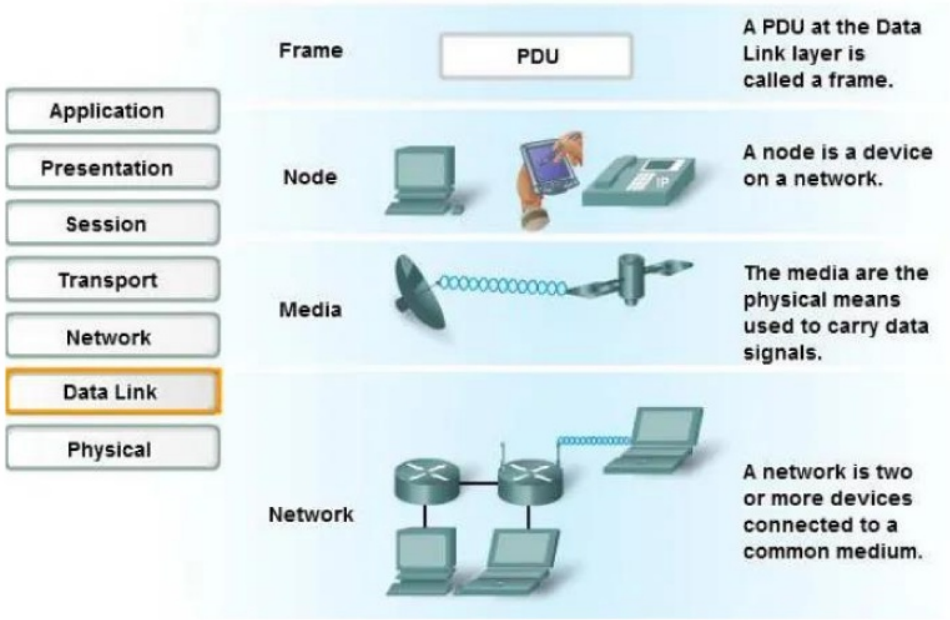
Lapisan ini dikenal sebagai lapisan yang mengatur tentang pengabelan. Physical layer adalah lapisan paling bawah di OSI layer yang berfungsi mendefinisikan media transmisi jaringan, desain jaringan, topologi jaringan, dan pengabelan. Peralatan seperti repeater, hub, dan network card berada pada layer ini. Pada dasarnya, lapisan fisik dinyatakan sebagai layer paling sederhana yang berkaitan dengan electrical dan optical koneksi antar-peralatan. Data biner dikodekan dalam bentuk yang dapat ditransmisi melalui media jaringan, misalnya kabel, transceiver, dan konektor yang berkaitan dengan physical layer.



Gambar 2. 4 Physical Layer (Lapisan Fisik)

b. Data Link Layer (Lapisan Data Link)

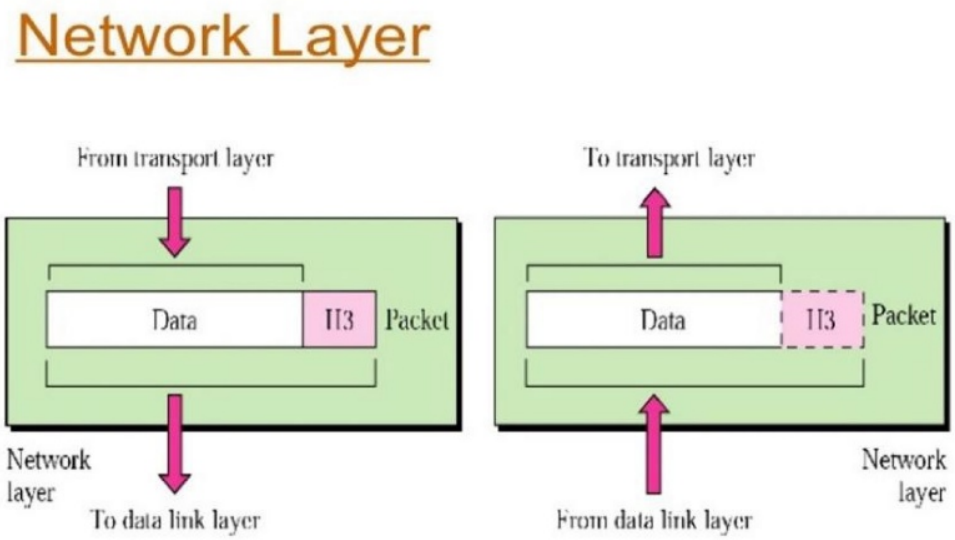
Data link layer berfungsi menentukan bagaimana bit-bit data dikelompokkan menjadi format yang sering disebut frame. Layer ini dibagi oleh IEEE 802 menjadi dua level yaitu LLC (Logical Link Control) dan MAC (Media Access Control). Beberapa protocol pada layer data-link diantaranya ethernet (802.2 dan 802.3), token bus (802.4), dan token ring (802.5). Pada layer, kedua di OSI ini terjadi koreksi kesalahan, flow control, pengalamatan hardware (MAC Address) dan menentukan prosedur penggunaan peranti-peranti jaringan seperti hub, bridge, dan repeater. Sebagai penghubung antara media network dan layer protocol yang lebih high-level, layer data link bertanggung jawab pada paket akhir dari data binari yang berasal dari level yang lebih tinggi ke paket diskrit sebelum menuju physical layer dan selanjutnya mengirimkan frame (blok dari data) melalui suatu network.



Gambar 2. 5 Data Link Layer (Lapisan Data Link)

c. Network Layer (Lapisan Jaringan)

Network layer berfungsi mendefinisikan alamat-alamat IP (Internet Protocol), membuat header untuk paket-paket kemudian melakukan routing melalui internet working dengan menggunakan router dan switch layer tiga. Tugas utama dari network layer adalah menyediakan fungsi routing sehingga paket dapat dikirim keluar dari segmen network lokal ke suatu tujuan yang berada pada suatu network lain. Protokol lainnya seperti IPX (Internet Packet eXchange), di mana perusahaan Novell telah memprogram beberapa protokol SPX (Sequence Packet Exchange) dan NCP (Netware Core Protocol) yang dimasukkan ke sistem operasi Netware. Beberapa fungsi yang dimiliki oleh layer network, yaitu mendeteksi eror, membagi aliran data biner ke paket diskrit dengan panjang tertentu, mengendalikan aliran, serta memperbaiki eror dengan mengirim ulang paket yang rusak.



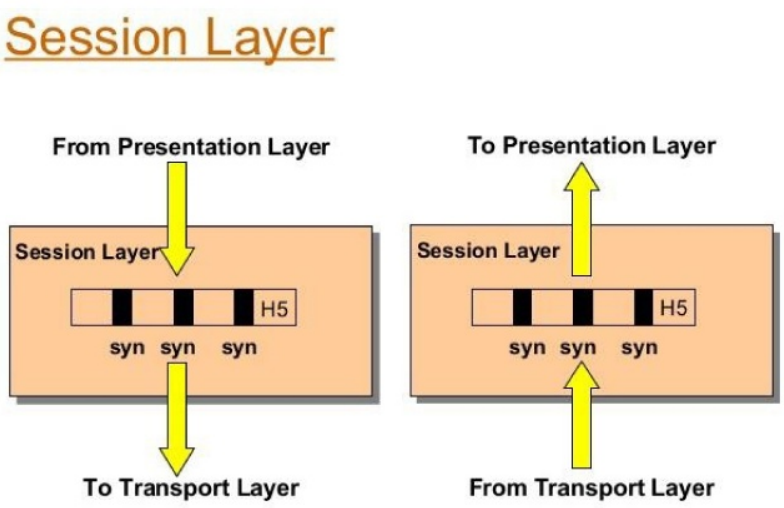
Gambar 2. 6 Network Layer (Lapisan Jaringan)

d. Transport Layer (Lapisan Transport)

Transport layer bisa dinyatakan sebagai pusat dari mode OSI yang berfungsi memecah data ke dalam beberapa paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Lapisan ini juga bertanggung jawab dalam membagi data menjadi segmen dan menyediakan penanganan eror. Layer ini menyediakan transfer yang reliable dan transparan antara kedua titik akhir, layer ini juga menyediakan multiplexing, kendali aliran dan pemeriksaan error serta memperbaikinya. Transport layer menggunakan protokol seperti UDP, TCP, dan/atau SPX (Sequence Packet eXchange) yang digunakan oleh NetWare yang dikhususkan pada koneksi berorientasi IPX.

e. Session Layer (Lapisan Session)

Session layer bertanggung jawab menentukan bagaimana dua terminal menjaga, memelihara dan mengatur koneksi. Di samping itu, juga mendefinisikan bagaimana sebuah koneksi dapat dibuat, dipelihara, atau dihilangkan. Hal mendasar yang perlu dipahami adalah layer session sering disalahartikan sebagai prosedur logon network dan berkaitan dengan keamanan (secure). Layer ini menyediakan layanan ke dua layer di atasnya dengan melakukan koordinasi komunikasi antara entitas layer yang diwakilinya.



Gambar 2. 7 Session Layer (Lapisan Session)

Beberapa protokol pada layer ini dapat dilihat pada tabel berikut.

Tabel 2. 1 Protokol pada Layer Session

No	Protokol	Keterangan
1	NETBIOS	Suatu session interface dan protokol besutan oleh IBM yang menyediakan layanan ke layer presentation dan layer application.
2	NETBEUI (NETBIOS Extended User Interface)	Suatu pengembangan dari NETBIOS yang digunakan pada produk Microsoft networking, seperti Windows NT dan LAN manager.
3	ADSP (AppleTalk Data Stream Protocol)	Digunakan untuk memeriksa aliran data dan memantau aliran data di antara komputer agar data dapat terkirim.
4	PAP (Printer Access Protocol)	Terdapat pada printer Postscript untuk akses pada jaringan Appletalk

f. Presentation Layer (Lapisan Presentasi)

Presentation layer berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Layer presentation dari model OSI melakukan fungsi tunggal dalam bentuk translasi dari berbagai tipe pada syntax sistem. Misalnya koneksi antara PC dan mainframe membutuhkan konversi dari EBCDIC character-encoding format ke ASCII. Protokol yang berada dalam level ini adalah peranti lunak director (rediktor software). Lapisan ini bekerja dalam proses data yang dikonversi dan diformat dengan tujuan transfer data.

g. Application Layer (Lapisan Aplikasi)

Layer application berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Layer jenis ini sebagai penghubung utama antara aplikasi yang berjalan pada satu komputer dan resources network yang membutuhkan akses padanya. Beberapa protokol yang berada dalam layer ini adalah HTTP, FTP, SMTP, dan NFS. Lapisan ini bekerja menyediakan jasa untuk aplikasi user, dan bertanggungjawab atas pertukaran informasi antara program komputer, seperti program e-mail dan servis lain yang berjalan di jaringan seperti server printer atau aplikasi komputer. Gateway melakukan pekerjaan yang sama seperti sebuah router, tetapi ada perbedaan di antara mereka.

Untuk lebih jelasnya mengenai 7 lapisan OSI, anda dapat melihat video berikut:

Tugas 2.2

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan empat lapis protocol TCP/IP berikut!

No	Lapisan	Langkah Penggunaan	Kendala
1	Network Interface Layer		
2	Internet Layer		
3	Transport Layer		
4	Application Layer		

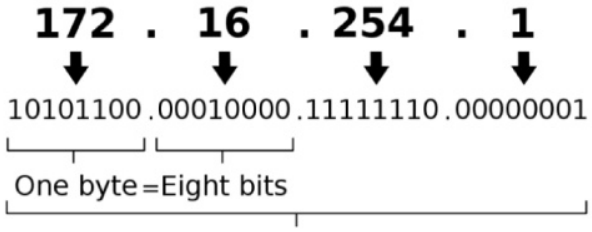
2. Rangkumlah hasil penelusuran Anda di buku tugas!
3. Kumpulkan hasilnya pada guru untuk diberi penilaian!

B. Prinsip Dasar Sistem IPv4/IPv6

Penggunaan IP address dalam hal ini adalah sebagai identitas dari masing-masing komputer baik yang bertindak sebagai server maupun sebagai client. Sama halnya dalam aktivitas internet, penggunaan IP address juga sebagai penamaan atau identitas dari masing-masing komputer host.

1. Ruang Lingkup IPv4 (IP versi 4)

Alamat IP versi 4 (sering disebut dengan Alamat IPv4) adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit dan secara teoritis dapat mengalamati hingga 4 miliar host komputer atau lebih tepatnya 4.294.967.296 host di seluruh dunia, jumlah host tersebut didapatkan dari 256 (didapatkan dari 8 bit) dipangkat 4 (karena terdapat 4 oktet) sehingga nilai maksimal dari alamat IP versi 4 tersebut adalah 255.255.255.255 di mana nilai dihitung dari nol sehingga nilai host yang dapat ditampung adalah 256 × 256 × 256 x 256 = 4.294.967.296 host, bila host yang ada di seluruh dunia melebihi kuota tersebut maka dibuatlah IP versi 6 atau IPv6. Contoh alamat IP versi 4, yaitu 192.168.100.3.



Gambar 2. 8 Contoh Alamat IPv4

a. Dasar Umum Alamat

Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik (dotted-decimal notation) yang dibagi ke dalam empat buah oktet dengan ukuran 8-bit. Pada beberapa buku referensi, format bentuknya merupakan w.x.y.z. Dikarenakan tiap oktet punya ukuran 8-bit, maka kadarnya berkisar antara 0-255 (meskipun begitu, terdapat beberapa pengecualian nilai). Alamat IP yang dipunyai oleh sebuah host bisa dibagi dengan memanfaatkan subnet mask jaringan ke dalam dua buah bidang, yaitu sebagai berikut.

1) Network Identifier/NetID
   Network Identifier/Net ID atau network address (alamat jaringan) yang dipakai khusus untuk mengidentifikasikan alamat jaringan di mana host kehadiran. Pada banyak kasus, sebuah alamat network identifier sama dengan segmen jaringan fisik dengan batasan yang dibentuk dan diberikan rumusan oleh router IP. Meskipun demikian, kehadiran beberapa kasus di mana beberapa jaringan logis terdapat di dalam sebuah segmen jaringan fisik yang sama dengan

memanfaatkan sebuah praktik yang dikata disebut sebagai multinetting. Semua sistem di dalam sebuah jaringan fisik yang sama, wajib memiliki alamat network identifier yang sama. Network identifier juga wajib bersifat unik dalam sebuah internetwork. Apabila semua node di dalam jaringan logis yang sama tidak dikonfigurasikan dengan memanfaatkan network identifier yang sama, maka terjadilah persoalan yang disebut dengan routing error. Pada umumnya, alamat network identifier tidak boleh bernilai 0 atau 255.

2) Host Identifier/HostID
   Host Identifier/HostID atau host address (alamat host) yang dipakai khusus untuk mengidentifikasikan alamat host (dapat berupa workstation, server, atau sistem yang lain yang berbasis teknologi TCP/IP) di dalam jaringan. Nilai host identifier tidak boleh bernilai 0 atau 255 dan wajib bersifat unik di dalam network identifier/ segmen jaringan di mana ia berada.

b. Jenis-jenis Alamat

Alamat IPv4 terbagi menjadi beberapa jenis, yaitu sebagai berikut.

1) Unicast Address, merupakan alamat IPv4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah internetwork IP. Unicast Address dipakai dalam komunikasi point-to-point atau one-to-one.
2) Alamat Broadcast, merupakan alamat IPv4 yang didesain agar diolah oleh setiap node IP dalam segmen jaringan yang sama. Alamat broadcast dipakai dalam komunikasi one-to-everyone.
3) Multicast Address, merupakan alamat IPv4 yang didesain agar diolah oleh satu atau beberapa node dalam segmen jaringan yang sama atau berbeda. Multicast Address dipakai dalam komunikasi one-to-many.

c. Kelas-kelas Alamat

Pada RFC 791, alamat IP versi 4 dibagi ke dalam beberapa kelas jika diperhatikan dari oktet pertamanya, seperti terlihat pada tabel. Sebenarnya yang menjadi pembeda kelas IP versi 4 merupakan pola biner yang terdapat dalam oktet pertama (utamanya merupakan bit-bit awal/high-order bit), akan tetapi untuk lebih mudah mengingatnya, bisa dengan memanfaatkan representasi desimal.

Tabel 2. 2 Kelas-kelas Alamat IP dan Penggunaannya

Kelas Alamat	Kadar Oktet Pertama	Bidang untuk Network Identifer	Bidang untuk Host Identifer	Jumlah Jaringan Maksimum	Jumlah Host dalam satu Jaringan Maksimum
Kelas A	1-126	W	X.Y.Z	126	16,777,214
Kelas B	128-191	W.X	Y.Z	16,384	65,534

Kelas C	192-223	W.X.Y	Z	1,097,152	254
Kelas D	224-239	Multicast IP address	Multicast IP address	Multicast IP address	Multicast IP address
Kelas E	240-255	Dicadangkan; eksperimen	Dicadangkan; eksperimen	Dicadangkan; eksperimen	Dicadangkan; eksperimen

1) Kelas A
   Alamat-alamat kelas A diberikan untuk jaringan skala besar. Nomor urut bit tertinggi di dalam alamat IP kelas A selalu diset dengan kadar 0 (nol). Tujuh bit berikutnya untuk melengkapi oktet pertama akan menciptakan sebuah network identifier. Adapun 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan host identifier. Hal ini mengizinkan kelas A memiliki hingga 126 jaringan dan 16,777,214 host tiap jaringannya. Alamat dengan oktet permulaan 127 tidak diizinkan, karena dipakai untuk mekanisme Inter Process Communication (IPC) di dalam mesin yang bersangkutan.
2) Kelas B
   Alamat-alamat kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diset ke bilangan biner 10. Pada 14-bit berikutnya (untuk melengkapi dua oktet pertama) akan menciptakan sebuah network identifier, adapun 16-bit sisanya (dua oktet terakhir) merepresentasikan host identifier. Kelas B bisa memiliki 16,384 network dan 65,534 host untuk setiap network.
3) Kelas C
   Alamat IP kelas C dipakai untuk jaringan berskala kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diset ke kadar biner 110. Pada 21-bit berikutnya (untuk melengkapi tiga oktet pertama) akan membuat bentuk sebuah network identifier. Kemudian 8-bit sisanya (sebagai oktet terakhir) akan merepresentasikan host identifier. Hal ini memungkinkan proses, metode, perbuatan menciptakan total 2,097,152 buah network, dan 254 host untuk setiap network.
4) Kelas D
   Alamat IP kelas D disediakan hanya untuk alamat-alamat IP multicast, dengan demikian akan berbeda dengan tiga kelas di atas. Empat bit pertama di dalam IP kelas D selalu diset ke bilangan biner 1110. Pada 28-bit sisanya dipakai menjadi alamat yang bisa dipakai untuk mengetahui host. Untuk lebih jelasnya, perhatikan bidang Multicast Address IPv4.
5) Kelas E
   Alamat IP kelas E disediakan menjadi alamat yang bersifat eksperimental atau percobaan dan dicadangkan untuk dipakai pada masa depan. Empat bit pertama

selalu diset untuk bilangan biner 1111. Pada 28-bit sisanya dipakai menjadi alamat yang bisa dipakai untuk mengetahui host.

Penggunaan kelas alamat IP kini tidak relevan lagi, mengingat alamat IP sudah tidak memanfaatkan kelas alamat lagi. Pengemban otoritas internet telah memperhatikan dengan jelas bahwa alamat yang dibagi ke dalam kelas-kelas seperti di atas sudah tidak mencukupi kebutuhan yang hadir di masa kini, di kala penggunaan internet makin meluas. Alamat IPv6 yang baru kini tidak lagi memanfaatkan kelas-kelas seperti alamat IPv4. Alamat yang dibentuk tanpa memedulikan kelas atau disebut juga dengan classless address.

d. Unicast Address

Tiap antarmuka jaringan yang memanfaatkan protokol TCP/IP wajib diidentifikasi dengan memanfaatkan sebuah alamat logis yang unik, yaitu Unicast Address. Unicast Address menjadi alamat logis karena alamat ini merupakan alamat yang dimainkan pada lapisan jaringan dalam DARPA Reference Model dan tidak memiliki relasi yang langsung dengan alamat yang dipakai pada lapisan antarmuka jaringan dalam DARPA Reference Model. Misalnya, Unicast Address bisa dikuatkan ke sebuah host dengan antarmuka jaringan dengan teknologi ethernet, yang memiliki alamat MAC sepanjang 48-bit.

Unicast Address wajib dipakai oleh semua host TCP/IP agar bisa saling terhubung. Komponen alamat ini terbagi menjadi dua jenis, yaitu alamat host (host identifier) dan alamat jaringan (network identifier). Unicast Address memanfaatkan kelas A, B, dan C dari kelas-kelas alamat IP yang telah disebutkan sebelumnya, sehingga ruang alamatnya merupakan dari 1.x.y.z hingga 223.x.y.z. Sebuah Unicast Address dibedakan dengan alamat yang lain dengan memanfaatkan skema subnet mask.

Bila kehadiran sebuah intranet tidak yang terkoneksi ke internet, semua alamat IP dalam ruangan kelas Unicast Address bisa dipakai. Bila koneksi dimainkan secara langsung (dengan memanfaatkan teknik routing) atau secara tidak langsung (dengan memanfaatkan proxy server), maka kehadiran dua jenis alamat yang bisa dipakai di dalam internet, merupakan public address (alamat publik) dan private address (alamat pribadi).

1) Alamat Publik
   Alamat publik merupakan alamat-alamat yang telah dikuatkan oleh InterNIC dan berisi beberapa buah network identifier yang telah dijamin unik (artinya, tidak kehadiran dua host yang memanfaatkan alamat yang sama) bila intranet tersebut telah terhubung ke internet. Ketika beberapa alamat publik telah dikuatkan, maka beberapa rute bisa diprogram ke dalam sebuah router sehingga lalu lintas data yang menuju alamat publik tersebut bisa mencapai lokasinya. Di internet,

lalu lintas ke sebuah alamat publik tujuan bisa dicapai, selama masih terkoneksi dengan internet.

2) Alamat Ilegal

Intranet-intranet pribadi yang tidak memiliki kemauan untuk mengoneksikan intranetnya ke internet bisa memilih alamat apa pun yang mereka bersedia, meskipun memanfaatkan alamat publik yang telah dikuatkan oleh InterNIC. Bila sebuah organisasi lalu memilihkan untuk menghubungkan intranetnya ke internet, skema alamat yang dipakainya berisi alamat-alamat yang mungkin telah dikuatkan oleh InterNIC atau organisasi yang lain. Alamat-alamat tersebut bisa menjadi konflik antara host satu dengan host yang lainnya, sehingga sering disebut juga dengan illegal address karena tidak bisa dihubungi oleh host yang lain.

3) Alamat Privat

Tiap node IP membutuhkan sebuah alamat IP yang bersifat unik terhadap Internetwork IP. Pada kasus internet, tiap node di dalam sebuah jaringan yang terhubung ke internet akan membutuhkan sebuah alamat yang unik secara global terhadap internet. Karena perkembangan internet yang sangat amat pesat, organisasi-organisasi yang menghubungkan intranet kepunyaannya ke internet membutuhkan sebuah alamat publik untuk setiap node di dalam intranet kepunyaannya tersebut. Tentu saja, hal ini akan membutuhkan sebuah alamat publik yang unik secara global.

Ketika menganalisis kebutuhan pengalamatan yang dibutuhkan oleh sebuah organisasi, para desainer internet memiliki konsep yang dibutuhkan bagi kebanyakan organisasi, kebanyakan host di dalam intranet organisasi tersebut tidak wajib terhubung secara langsung ke internet. Beberapa host yang membutuhkan sekumpulan layanan internet, seperti halnya akses terhadap web atau e-mail. Pada umumnya mengakses layanan internet tersebut melewati gateway yang berjalan di atas lapisan aplikasi, seperti proxy server atau e-mail server. Hasilnya, mayoritas organisasi hanya membutuhkan alamat publik dalam jumlah sedikit saja yang lalu dipakai oleh node-node tersebut (hanya untuk proxy, router, firewall, atau translator alamat jaringan) yang terhubung secara langsung ke internet.

Pada host-host di dalam sebuah organisasi yang tidak membutuhkan akses langsung ke internet, alamat-alamat IP yang bukan duplikat dari alamat publik yang telah dikuatkan mutlak dibutuhkan. Guna dapat mengatasi persoalan pengalamatan ini, para desainer internet mereservasikan beberapa ruangan alamat IP dan menyebut bidang tersebut menjadi ruangan alamat pribadi. Sebuah alamat IP yang hadir di dalam ruangan alamat pribadi tidak akan dipakai menjadi sebuah alamat publik. Alamat IP yang hadir di dalam ruangan alamat pribadi diketahui juga dengan alamat pribadi atau private address. Karena di antara

ruangan alamat publik dan ruangan alamat pribadi tidak saling melaksanakan overlapping, maka alamat pribadi tidak akan menduplikasi alamat publik dan sebaliknya. Sebuah jaringan yang memanfaatkan alamat IP privat sering disebut dengan jaringan privat atau private network.

Ruangan alamat pribadi yang dipilihkan di dalam RFC 1918 diberikan rumusan di dalam tiga blok alamat berupa sekumpulan kode unik, yaitu 10.0.0.0/8, 172.16.0.0/12, dan 192.168.0.0/16. Sementara itu, terdapat juga sebuah ruang alamat yang dipakai untuk alamat IP privat dalam beberapa sistem operasi seperti sebagai berikut.

a) Alamat 10.0.0.0/8
   Jaringan pribadi (private network) 10.0.0.0/8 merupakan sebuah network identifier kelas A yang mengizinkan alamat IP yang valid dari 10.0.0.1 hingga 10.255.255.254. Jaringan pribadi 10.0.0.0/8 memiliki 24-bit host yang bisa dipakai untuk skema subnetting di dalam sebuah organisasi privat.
b) Alamat 172.16.0.0/12
   Jaringan pribadi 172.16.0.0/12 bisa diinterpretasikan menjadi sebuah block dari 16 network identifier kelas B atau menjadi sebuah ruangan alamat yang memiliki 20-bit yang bisa dikuatkan menjadi host identifier, yang bisa dipakai dengan memanfaatkan skema subnetting di dalam sebuah organisasi privat. Alamat jaringan privat 172.16.0.0/12 mengizinkan alamat-alamat IP yang valid dari 172.16.0.1 hingga 172.31.255.254.
c) Alamat 192.168.0.0/16
   Jaringan pribadi 192.168.0.0/16 bisa diinterpretasikan menjadi sebuah block dari 256 network identifier kelas C atau menjadi sebuah ruangan alamat yang memiliki 16-bit yang bisa dikuatkan menjadi host identifier yang bisa dipakai dengan memanfaatkan skema subnetting apapun di dalam sebuah organisasi privat. Alamat jaringan privat 192.168.0.0/16 bisa mendukung alamat-alamat IP yang valid dari 192.168.0.1 hingga 192.168.255.254.
d) Alamat 169.254.0.0/16
   Alamat jaringan ini bisa dipakai menjadi alamat privat karena memang IANA mengalokasikan untuk tidak memanfaatkannya. Alamat IP yang kemungkinan ada di dalam ruang alamat ini merupakan 169.254.0.1 hingga 169.254.255.254, dengan alamat subnet mask 255.255.0.0. Alamat ini dipakai menjadi alamat IP privat otomatis (pada Windows, disebut dengan Automatic Private Internet Protocol Addressing (APIPA)).
   Hasil dari penggunaan alamat-alamat privat ini oleh banyak organisasi adalah untukmenghindari kehabisan dari alamat publik, mengingat pertumbuhan internet yang sangat pesat.

Tabel 2. 3 Ruang-ruang di dalam Alamat IP Privat

Ruang Alamat	Dari Alamat	Sampai Alamat	Keterangan
010.000.000.000/8	010.000.000.001	010.255.255.254	Ruang alamat privat yang sangat tinggi (mereservaskan kelas A untuk digunakan).
172.016.000.000/12	172.016.000.001	172.031.255.254	Ruang alamat privat yang tinggi (digunakan untuk jaringan menengah hingga besar).
192.168.000.000/16	192.168.000.001	192.168.255.254	Ruang alamat privat yang cukuo tinngi (digunakan untuk jaringan kecil hingga besar).
169.254.000.000/16	169.254.000.001	169.254.255.254	dipakai oleh fitur Automatic Private Internet Protocol Addressing (APIPA) dalam beberapa sitem operasi.

Karena alamat-alamat IP di dalam ruangan alamat pribadi tidak akan dikuatkan oleh Internet Network Information Center (InterNIC) atau badan yang lain yang memiliki otoritas menjadi alamat publik, maka tidak akan pernah ada rute yang menuju ke alamat-alamat pribadi tersebut di dalam router internet. Kompensasinya, alamat pribadi tidak bisa dijangkau dari internet. Oleh karena itu, semua lalu lintas dari sebuah host yang memanfaatkan sebuah alamat pribadi wajib mengirim request tersebut ke sebuah gateway (seperti halnya proxy server) yang memiliki sebuah alamat publik yang valid atau memiliki alamat pribadi yang telah ditranslasikan ke dalam sebuah alamat IP publik yang valid dengan memanfaatkan Network Address Translator (NAT) sebelum dikirimkan ke internet.

e. Multicast Address

Alamat IP Multicast (Multicast IP address) merupakan alamat yang dipakai untuk menyampaikan satu paket untuk banyak penerima. Pada sebuah intranet yang memiliki Multicast Address IPv4, sebuah paket yang ditujukan ke sebuah Multicast

Address akan diteruskan oleh router ke subjaringan di mana terdapat host-host yang sedang kehadiran dalam keadaan "listening" terhadap lalu lintas jaringan yang dikirimkan ke Multicast Address tersebut. Adapun dengan prosedur ini, Multicast Address menjadi prosedur yang efisien untuk menyampaikan paket data dari satu sumber ke beberapa tujuan untuk beberapa jenis komunikasi. Multicast Address diberikan rumusan dalam RFC 1112.

Alamat Multicast Address IPv4 diberikan rumusan dalam ruang alamat kelas D, yaitu 224.0.0.0/4 yang berkisar dari 224.0.0.0 hingga 224.255.255.255. Prefiks alamat 224.0.0.0/24 (dari alamat 224.0.0.0 hingga 224.0.0.255) tidak dapat dipakai karena dicadangkan untuk dipakai oleh lalu lintas multicast dalam subnet lokal. Daftar Multicast Address yang dikuatkan oleh IANA bisa diperhatikan pada situs IANA.

f. Alamat Broadcast

Alamat broadcast untuk IP versi 4 dipakai untuk menyampaikan paket-paket data "satu-untuk-semua". Bila sebuah host pengirim yang hendak menyampaikan paket data dengan tujuan alamat broadcast, maka semua node yang terdapat di dalam segmen jaringan tersebut akan menyatakan sepakat paket tersebut dan mengolahnya. Berbeda dengan alamat IP unicast atau alamat IP multicast, alamat IP broadcast hanya bisa dipakai menjadi alamat tujuan saja, sehingga tidak bisa dipakai menjadi alamat sumber.

Kehadiran empat buah jenis alamat IP broadcast, yaitu network broadcast, subnet broadcast, all-subnets-directed broadcast, dan limited broadcast. Pada setiap jenis alamat broadcast tersebut, paket IP broadcast akan dialamatkan untuk lapisan antarmuka jaringan dengan memanfaatkan alamat broadcast yang dimiliki oleh teknologi antarmuka jaringan yang dipakai. Contoh, pada jaringan ethernet dan token ring, semua paket broadcast IP akan dikirimkan ke alamat broadcast ethernet dan token ring, yaitu 0xFF-FF-FF-FF-FF-FF.

1) Network Broadcast
   Alamat network broadcast IPv4 merupakan alamat yang dibentuk dengan prosedur mengeset semua bit host menjadi 1 pada sebuah alamat yang memanfaatkan kelas (classful). Contohnya, dalam NetID 131.107.0.0/16, alamat broadcast-nya merupakan 131.107.255.255. Alamat network broadcast dipakai untuk menyampaikan sebuah paket untuk semua host yang terdapat di dalam sebuah jaringan yang berbasis kelas. Router tidak bisa meneruskan paket-paket yang ditujukan dengan alamat network broadcast.
2) Subnet Broadcast
   Alamat subnet broadcast merupakan alamat yang dibentuk dengan prosedur mengeset semua bit host menjadi satu dalam sebuah alamat yang tidak memanfaatkan kelas (classless). Contoh, pada NetID 131.107.26.0/24, alamat

broadcast-nya merupakan 131.107.26.255. Alamat subnet broadcast dipakai untuk menyampaikan paket ke semua host dalam sebuah jaringan yang telah dibagi dengan prosedur subnetting atau supernetting. Router tidak bisa meneruskan paket-paket yang ditujukan dengan alamat subnet broadcast. Alamat subnet broadcast tidak terdapat di dalam sebuah jaringan yang memanfaatkan kelas alamat IP. Sementara itu, alamat network broadcast tidak terdapat di dalam sebuah jaringan yang tidak memanfaatkan kelas alamat IP.

3) All-Subnets-Directed Broadcast

Alamat IP ini merupakan alamat broadcast yang dibentuk dengan mengeset semua bit-bit network identifier yang asli yang berbasis kelas menjadi satu untuk sebuah jaringan dengan alamat tidak berkelas (classless). Sebuah paket jaringan yang dialamatkan ke alamat ini akan diberikan ke semua host dalam semua subnet yang dibentuk dari network identifier berbasis kelas yang asli. Contoh alamat ini digunakan untuk sebuah network identifier 131.107.26.0/24, alamat all-subnets-directed broadcast untuknya adalah 131.107.255.255. Dengan kata lain, alamat ini merupakan alamat jaringan broadcast dari network identifier alamat berbasis kelas yang asli. Pada contoh di atas, alamat 131.107.26.0/24 yang merupakan alamat kelas B secara default memiliki network identifer 16, maka alamatnya merupakan 131.107.255.255.

Semua host dari sebuah jaringan dengan alamat tidak berkelas akan mendengarkan dan mengolah paket-paket yang dialamatkan ke alamat ini. RFC 922 mengharuskan router IP untuk meneruskan paket yang di broadcast ke alamat ini ke semua subnet dalam jaringan berkelas yang asli. Meskipun demikian, hal ini belum banyak diimplementasikan. Adapun dengan banyaknya alamat network identifier yang tidak berkelas, maka alamat ini pun di tinggalkan karena sudah tidak relevan lagi dengan perkembangan jaringan.

4) Limited Broadcast

Alamat ini merupakan alamat yang dibentuk dengan mengeset semua 32-bit alamat IP versi 4 menjadi 1 (11111111111111111111 atau 255.255.255.255). Alamat ini dipakai ketika sebuah node IP wajib melaksanakan penyampaian data secara one-to-everyone di dalam sebuah jaringan lokal, tetapi ia belum mengetahui network identifier-nya. Contoh penggunaanya, ketika proses konfigurasi alamat secara otomatis dengan memanfaatkan Boot Protocol (BOOTP) atau Dynamic Host Configuration Protocol (DHCP). Sebagai contoh, padan DHCP sebuah klien DHCP wajib memanfaatkan alamat ini untuk semua lalu lintas yang dikirimkan hingga server DHCP memberikan sewaan alamat IP untuknya.

Semua host yang berbasis kelas atau tanpa kelas akan mendengarkan dan mengolah paket jaringan yang dialamatkan ke alamat ini. Meskipun kelihatannya dengan memanfaatkan alamat ini, namun paket jaringan akan dikirimkan ke

semua node di dalam semua jaringan, ternyata hal ini hanya terjadi di dalam jaringan lokal saja dan tidak akan pernah diteruskan oleh router IP mengingat paket data dibatasi saja hanya dalam segmen jaringan lokal saja. Karenanya, alamat ini disebut sebagai limited broadcast.

Tugas 2.3

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan alamat IP privat berikut!

No	Alamat IP Privat	Sistem Operasi yang Digunakan	Kendala
1	Alamat 10.0.0.0/8		
2	Alamat 172.16.0.0/12		
3	Alamat 192.168.0.0/16		
4	Alamat 169.254.0.0/16		

2. Tulislah hasil penelitian Anda dalam bentuk rangkuman pada buku tugas!
3. Kumpulkan hasilnya pada guru untuk diberi penilaian!

2. Ruang Lingkup IPv6 (IP Versi 6)

Internet Protocol version 6 (IPv6) adalah protokol internet generasi baru yang menggantikan protokol versi sebelumnya IPv4. Tujuan utama diciptakan IPv6 karena keterbatasan ruang alamat di IPv4 yang hanya terdiri dari 32-bit. Seperti yang Anda ketahui IP versi 4 yang kini digunakan suatu saat akan habis. IP versi 6 (IPv6) yang sebelumnya sudah diimplementasikan oleh beberapa pengguna internet akan menjadi solusi untuk mengatasi keterbatasan dari IPv4 tersebut. Juni 2012 menjadi bulan bersejarah bagi perkembangan internet di dunia. Hal ini karena pada tanggal 6 Juni 2012 IPv6 telah resmi diluncurkan.

Alamat IP versi 6 (sering disebut sebagai alamat IPv6), merupakan sebuah jenis pengalamatan jaringan yang dipakai di dalam protokol jaringan TCP/IP yang memanfaatkan protokol internet versi 6. Panjang totalnya merupakan 128-bit dan secara teoritis dapat mengalamati hingga 2^{128}=3,4 x 10^{38} host komputer di seluruh dunia. Contoh alamat IPv6 adalah 21da:00d3:0000:2f3b:02aa:00ff:fe28:9c5a.

a. Dasar Umum Alamat

Berbeda dengan IPv4 yang hanya memiliki panjang 32-bit (jumlah total alamat yang dapat dicapai IPv6 mencapai 4,294,967,296 alamat), alamat IPv6 memiliki panjang 128-bit. Meskipun total alamat pada IPv4 mencapai 4 miliar, pada kenyataannya tidak sampai 4 miliar alamat. Hal ini karena kehadiran beberapa limitasi, sehingga implementasinya saat ini hanya mencapai beberapa ratus juta saja. IPv6 yang

memiliki panjang 128-bit, memiliki total alamat yang mungkin hingga 2^{128}=3,4 x 10^{38} alamat. Total alamat yang sangat besar ini bertujuan untuk mempersiapkan ruang alamat yang tidak akan tidak bersisa (hingga beberapa masa ke depan) dan membentuk prasarana routing yang ditata secara hierarkis, sehingga mengurangi kompleksitas babak routing dan tabel routing.

Sama seperti halnya IPv4, IPv6 juga mengizinkan kehadiran DHCPv6 Server sebagai pengelola alamat. Jika dalam IPv4 terdapat dynamic address dan static address, maka dalam IPv6 konfigurasi alamat dengan memanfaatkan DHCP Server disebut dengan stateful address configuration, sementara jika konfigurasi alamat IPv6 tanpa DHCP Server disebut dengan stateless address configuration.

Seperti halnya IPv4 yang memanfaatkan high-order bit sebagai alamat jaringan dengan low-order bit sebagai alamat host, pada IPv6 juga terjadi hal serupa. Pada IPv6, bit-bit pada tingkat tinggi akan dipakai sebagai tanda pengenal jenis alamat IPv6 yang disebut dengan Format Prefix (FP). Pada IPv6 tidak ada kehadiran subnet mask, yang kehadiran hanyalah Format Prefix.

b. Format Alamat

Pada IPv6, alamat 128-bit akan dibagi ke dalam 8 blok memiliki ukuran 16-bit yang dapat dikonversikan ke dalam bilangan heksadesimal memiliki ukuran 4-digit. Tiap blok bilangan heksadesimal tersebut akan dipisahkan dengan tanda titik dua (:). Karenanya, format notasi yang dipakai oleh IPv6 juga sering disebut dengan colon-hexadecimal format, berbeda dengan IPv4 yang memanfaatkan dotted-decimal format.

Contoh alamat IPv6 dalam bentuk bilangan biner, yaitu 00000010101010100000000011111111000000001101001100000000000000000010000 11101101000101111001110111001110001011010111111000101000. Guna menerjemahkannya ke dalam bentuk notasi colon-hexadecimal format, angka-angka biner di atas dibagi ke dalam 8 buah blok yang memiliki ukuran 16-bit, maka hasilnya adalah 0000001010101010 0000000011111111 0000000011010011 0000000000000000 0010000111011010 0010111100111011 1001110001011010 1111111000101000. Setiap blok memiliki ukuran 16-bit tersebut dikonversikan ke dalam bilangan heksadesimal dan setiap bilangan heksadesimal tersebut dipisahkan dengan memanfaatkan tanda titik dua. Produksi konversinya adalah 02aa:00ff:00d3:0000:21da:2f3b:9c5a:fe28.

c. Penyederhanaan Bentuk Alamat

Alamat di atas juga dapat disederhanakan lagi dengan membuang angka 0 pada permulaan setiap blok yang memiliki ukuran 16-bit di atas, dengan menyisakan satu digit terakhir. Adapun dengan membuang angka 0, alamat di atas disederhanakan menjadi 2aa:ff:d3:0:21da:2f3b:9c5a:fe28. Konvensi pengalamatan IPv6 juga mengizinkan penyederhanaan alamat bertambah jauh lagi, yaitu dengan membuang

banyak angka 0, pada sebuah alamat yang banyak angka 0-nya. Jika sebuah alamat IPv6 yang direpresentasikan dalam notasi colon-hexadecimal format mengandung beberapa blok 16-bit dengan angka 0, maka alamat tersebut dapat disederhanakan dengan memanfaatkan tanda dua buah titik dua (:). Untuk menghindari kebingungan penyederhanaan alamat IPv6 dengan prosedur ini hanya bisa dipakai sekali saja di dalam satu alamat, karena probabilitas kelak pengguna tidak dapat memilihkan berapa banyak bit 0 yang direpresentasikan oleh setiap tanda dua titik dua (:) yang terdapat dalam alamat tersebut. Prosedur penyederhanaan bentuk alamat seperti berikut.

Tabel 2. 4 Penyederhanaan Alamat IPv6

Alamat Asli	Alamat Asli yang Disederhanakan	Alamat Setelah Dikompres
da80:0000:0000:0000:076a:00hh:cb3d:9c5a	da80:0:0:0:76a:hh:cb3d:9c5a	da80::76a:hh:cb3d:9c5a
hh04:0000:0000:0000:0000:0000:0000:0004	hh04:0:0:0:0:0:0:4	hh04::4

d. Format Prefix

Pada IPv4 sebuah alamat dalam notasi dotted-decimal format dapat dipresentasikan dengan memanfaatkan angka prefiks yang merujuk untuk subnet mask. IPv6 juga memiliki angka prefiks, tapi tidak digunakan untuk merujuk untuk subnet mask, karena memang IPv6 tidak mendukung subjek mask. Prefiks merupakan sebuah bagian dari alamat IP di mana bit-bit memiliki nilai-nilai yang tetap atau bit-bit tersebut merupakan bagian dari sebuah rute atau subnet identifier. Prefiks dalam IPv6 dipresentasikan dengan prosedur yang sama seperti halnya prefiks alamat IPv4 yang merupakan alamat atau angka panjang prefiks. Panjang prefiks memiliki jumlah besar paling kiri yang menciptakan prefix subnet. Contoh grafik sebuah alamat IPv6 dapat dipresentasikan berupa 3ffe:2900:d005:f28b::/64. Pada contoh di atas, 64-bit pertama dari alamat tersebut dianggap sebagai prefiks alamat, sementara 64-bit sisanya dianggap sebagai Interface ID.

e. Jenis-Jenis Alamat IPv6

IPv6 mendukung beberapa jenis format prefix, yaitu Anycast Address, Multicast Address, dan Unicast Address. Jika diamati dari cakupan alamatnya, Multicast Address diisikan ke dalam struktur alamat. Adapun Unicast Address dan Anycast Address terbagi menjadi alamat-alamat berikut.

Tabel 2. 5 Jenis-jenis Alamat IPv6

No.	Jenis	Deskripsi
1.	Global Address	Sebuah jenis alamat yang mengizinkan sebuah komputer agar dapat menyediakan perhubungan dengan komputer ang lain dalam internet berbasis IPv6.
2.	Link-Local	Sebuah jenis alamat yang mengizinkan sebuah komputer agar dapat menyediakan perhubungan dengan komputer yang lain dalam satu subnet.
3.	Site-Local	Sebuah jenis alamat yang mengizinkan sebuah komputer agar dapat menyediakan perhubungan dengan komputer yang lain dalam sebuah internet.

1) Unicast Address

Unicast Address dipersiapkan untuk perhubungan secara point-to-point, secara langsung selang dua host dalam sebuah jaringan. Alamat IPv6 jenis Unicast Address dapat diimplementasikan dalam berbagai jenis alamat, yaitu sebagai berikut.

a) Alamat Unicast 6t04 (Unicast 6to4 Address)

Alamat unicast 6to4 merupakan alamat yang dipakai oleh dua host IPv4 dan IPv6 dalam internet IPv4 agar dapat saling menyediakan perhubungan. Alamat ini sering dipakai sebagai penukar alamat publik IPv4. Alamat ini aslinya memanfaatkan prefiks alamat 2002::/16 dengan tambahan 32-bit dari alamat publik IPv4 untuk menciptakan sebuah prefiks dengan panjang 48-bit, dengan format 2002:WWXX:YYZZ::/48, di mana WWXX dan YYZZ merupakan representasi dalam notasi colon-decimal format dari notasi dotted-decimal format w.x.y.z dari alamat publik IPv4. Sebagai contoh, alamat IPv4 157.60.91.123 diterjemahkan dan dijadikan alamat IPv6 2002:9d3c:5b7b::/48. Meskipun demikian, alamat ini sering ditulis dalam format IPv6 unicast global address, yaitu 2002:WWXX:YYZZ:SLA ID:Interface ID.

b) Alamat Unicast Global (Unicast Global Address)

Alamat unicast global IPv6 mirip dengan alamat publik dalam alamat IPv4. Diketahui juga sebagai aggregatable global unicast address. Seperti halnya alamat publik IPv4 yang dapat secara global dirujuk oleh host-host di internet dengan memanfaatkan babak routing, alamat ini juga mengimplementasikan hal serupa. Struktur alamat IPv6 unicast global dijadikan topologi tiga level (public, site, dan node).

Tabel 2. 6 Struktur Alamat IPv6 Unicast Global

Field	Panjang	keterangan
001	3-bit	Berfungsi sebagai tanda pengenal alamat, bahwa alamat ini merupakan sebuah alamat IPv6 unicast global.
Top Level Aggregation Identifier (TLA ID)	13-bit	Berffungsi sebagai level tertinggi dalam hierarki routing. TLA ID diatur oleh internet Assigned Number Authority (IANA) yang mengolakasikannya ke dalam daftar internet registry, kemudian mengolasikan sebuah TLA ID ke sebuah ISP global.
Res	8-bit	Direservasikan untuk penggunaan pada masa yang akan datang (mungkin untuk perluasan TLA ID atau NLA ID)
Next Level Aggregation Identifier (NLA ID)	24-bit	Berfungsi sebagai tanda pengenal milik situs (site) customer tertentu.
Site Level Aggregation Identifier (SLA ID)	16-bit	Mengizinkan hingga 65536 (216) subnet dalam sebuah situs individu. SLA ID ditetapkan di dalam sebuah site. ISP tidak dapat menggangti bagian alamt ini.
Interface ID	64-bit	Berfungsi sebagai alamat dari sebuah node dalam subnet yang spesifik (yang dipilihkan oleh SLA ID).

c) Alamat Unicast ISATAP (Unicast ISATAP Address)
Alamat unicast ISATAP merupakan sebuah alamat yang dipakai oleh dua host IPv4 dan IPv6 dalam sebuah intranet IPv4 agar dapat saling menyediakan perhubungan. Alamat ini menggabungkan prefiks alamat unicast link-local, alamat unicast site-local atau alamat unicast global (yang dapat berupa prefiks alamat 6to4) yang memiliki ukuran 64-bit dengan 32-bit ISATAP identifier (0000:5efe), lalu disertai dengan 32-bit alamat IPv4 yang dimiliki oleh interface atau sebuah host. Prefiks yang dipakai dalam alamat ini disebut dengan subnet prefix. Meski alamat 6to4 hanya dapat menangani alamat IPv4 publik saja, alamat ISATAP dapat menangani alamat pribadi IPv4 dan alamat publik IPv4.

d) Alamat Unicast Link-Local (Unicast Link-Local Address)
Alamat unicast link-local merupakan alamat yang dipakai oleh host-host dalam subnet yang sama. Alamat ini mirip dengan konfigurasi APIPA (Automatic Private Internet Protocol Addressing) dalam sistem operasi

Microsoft Windows XP ke atas. host-host yang kehadiran di dalam subnet yang sama akan memanfaatkan alamat-alamat ini secara otomatis agar dapat menyediakan perhubungan. Alamat ini juga memiliki fungsi resolusi alamat yang disebut dengan neighbor discovery. Prefiks alamat yang dipakai oleh jenis alamat ini merupakan fe80::/64.

Tabel 2. 7 Prefiks Alamat fe80::/64

Field	Panjang	keterangan
1111111010000000 0000000000000000 0000000000000000 0000000000000000	64-bit	Berfungsi sebagai tanda pengenal alamat unicast link-local
Interface ID	64-bit	Berfungsi sebagai alamat dari sebuah node dalam subnet yang spesifik.

e) Alamat Unicast Loopback (Unicast Loopback Address)
Alamat unicast loopback merupakan sebuah alamat yang dipakai untuk mekanisme Interprocess Communication (IPC) dalam sebuah host. Dalam IPv4, alamat yang ditetapkan merupakan 127.0.0.1, sementara dalam IPv6 merupakan 0:0:0:0:0:0:0:1, atau ::1.

f) Alamat Unicast Site-Local (Unicast Site-Local Address)
Alamat unicast site-local IPv6 mirip dengan alamat privat dalam IPv4. Ruang lingkup dari sebuah alamat terdapat pada internetwork dalam sebuah site milik sebuah organisasi. Penggunaan alamat unicast global dan unicast site-local dalam sebuah jaringan merupakan mungkin dimainkan. Prefiks yang dipakai oleh alamat ini merupakan FEC0::/48.

Tabel 2. 8 Prefiks Alamat FEC0::/48

Field	Panjang	keterangan
1111111011000000 0000000000000000 0000000000000000	48-bit	Kadar ketetapan alamat unicast site-local.
Subnet Identifier	16-bit	Mengizinkan hingga 65536 (216) subnet dalam sebuah struktur subnet datar. Administrator juga dapat membagi bit-bit yang yang memiliki kadar tinggi (high-order bit) untuk menciptakan sebuah prasarana routing hierarkis.
Interface Identifier	64-bit	Berfungsi sebagai alamat dari sebuah node dalam subnet yang spesifik.

g) Alamat unicast yang belum dipilihkan (unicast unspecified address)
Alamat unicast yang belum dipilihkan merupakan alamat yang belum dipilihkan oleh seorang administrator atau tidak menemukan sebuah DHCP

Server untuk berkeinginan alamat. Alamat ini sama dengan alamat IPv4 yang belum dipilihkan, yaitu 0.0.0.0. Kadar alamat ini dalam IPv6 merupakan 0:0:0:0:0:0:0:0 atau dapat disingkat dijadikan dua titik dua (::).

2) Multicast Address

Adapun Multicast Address dipersiapkan untuk metode untuk memberikan sebuah paket data ke banyak host yang kehadiran dalam grup yang sama. Alamat ini dipakai dalam perhubungan one-to-many. Multicast Address pada IPv6 sama seperti halnya Multicast Address pada IPv4. Paket-paket yang ditujukan ke sebuah Multicast Address akan diberikan terhadap semua interface yang dikenali oleh alamat tersebut. Prefiks alamat yang dipakai oleh Multicast Address IPv6 merupakan ff00::/8.

Tabel 2. 9 Prefiks Alamat yang Dipakai Multicast Address IPv6

Field	Panjang	keterangan
11111111	8-bit	Tanda pengenal bahwa alamat ini merupakan Multicast Address.
Flags	4-bit	Berfungsi sebagai tanda pengenal apakah alamat ini merupakan alamat transient atau bukan. Jika kadarnya 0, maka alamat ini bukan alamat transient, dan alamat ini merujuk untuk Multicast Address yang ditetapkan secara permanen. Jika kadarnya 1, maka alamat ini merupakan alamat transient.
Scope	4-bit	Berfungsi untuk mengindikasikan cakupan lalu lintas multicast, seperti halnya interface-local, link-local, site-local, dan organization-local atau global.
Group ID	112-bit	Berfungsi sebagai tanda pengenal grup multicast.

3) Anycast Address

Anycast Address dipersiapkan untuk metode penyampaian paket data untuk anggota terdekat dari sebuah grup. Alamat ini dipakai dalam perhubungan one-to-one-of-many. Alamat ini juga dipakai hanya sebagai alamat tujuan (destination address) dan diberikan hanya untuk router, bukan untuk host-host biasa.

Anycast Address dalam IPv6 mirip dengan Anycast Address dalam IPv4, tapi diimplementasikan dengan prosedur yang bertambah efisien dibandingkan dengan IPv4. Umumnya, Anycast Address dipakai oleh Internet Service Provider (ISP) yang memiliki banyak klien. Meskipun Anycast Address memanfaatkan ruang Unicast Address, tapi fungsinya berbeda daripada Unicast Address.

IPv6 memanfaatkan Anycast Address untuk mengidentifikasikan beberapa interface yang berbeda. IPv6 akan memberikan paket-paket yang dialamatkan ke sebuah Anycast Address ke interface terdekat yang dikenali oleh alamat tersebut. Hal ini sangat berbeda dengan Multicast Address, yang memberikan paket ke banyak penerima, karena Anycast Address akan memberikan paket untuk salah satu dari banyak penerima.

3. Perbedaan Umum antara IPv4 dan IPv6

IPv4 atau singkatan dari Internet Protocol version 4 merupakan sebuah protokol untuk penggunaan paket penggantian link layer networks seperti ethernet. IPv4 menawarkan alamat yang banyaknya diperkirakan hingga 4,3 milyar karena IPv4 hanya memiliki 32-bit. IPv6 atau singkatan dari Internet Protocol version 6 merupakan sebuah protokol yang lebih mutakhir dan fitur yang lebih bagus dibanding IPv4.

Ia memiliki kemampuan untuk memberikan angka alamat yang jumlahnya tidak terbatas karena IPv6 memiliki 128-bit. IPv6 menggantikan IPv4 dalam rangka untuk mengakomodir pertumbuhan angka dari jaringan di seluruh dunia dan membantu menyelesaikan masalah alamat IP yang kelelahan.

Sebelum mempelajari lebih lanjut mengenai perbedaan umum IPv4 dan IPv6, anda dapat melihat video berikut:

a. Alamat IP

Salah satu perbedaan antara IPv4 dan IPv6 adalah penampilan dari alamat IP. IPv4 menggunakan empat 1 byte angka desimal, yang dipisahkan dengan titik (contohnya, 192.168.1.1), sedangkan IPv6 menggunakan angka heksadesimal yang dipisahkan dengan titik dua (contoh: fe80::d4a8:6435:d2d8:d9f3b11).

b. Fragmentasi

Pada IPv4 dilakukan di setiap hop yang melambatkan performa router. Proses menjadi lebih lama lagi apabila ukuran paket data melampaui Maximum

Transmission Unit (MTU) paket dipecah-pecah sebelum disatukan kembali di tempat tujuan. Adapun pada IPv6 hanya dilakukan oleh host yang mengirimkan paket data. Di samping itu, terdapat fitur MTU discovery yang menentukan fragmentasi yang lebih tepat menyesuaikan dengan nilai MTU terkecil yang terdapat dalam sebuah jaringan dari ujung ke ujung.

c. IPSec (Keamanan)

Meski umum digunakan dalam mengamankan jaringan IPv4, header IPsec merupakan fitur tambahan pilihan pada standar IPv4. IPsec dikembangkan sejalan dengan IPv6. Header IPsec menjadi fitur wajib dalam standar implementasi IPv6.

d. Kapasitas

Jumlah alamat IPv4 menggunakan 32-bit sehingga jumlah alamat unik yang didukung terbatas 4.294.967.296 atau di atas 4 miliar alamat IP saja. NAT mampu untuk sekadar memperlambat habisnya jumlah alamat IPv4, namun pada dasarnya IPv4 hanya menggunakan 32-bit sehingga tidak dapat mengimbangi laju pertumbuhan internet dunia. Adapun pada IPv6 menggunakan 128-bit untuk mendukung 3.4 × 1038 alamat IP yang unik. Jumlah ini lebih dari cukup untuk menyelesaikan masalah keterbatasan jumlah alamat pada IPv4 secara permanen.

e. Konfigurasi

Ketika sebuah host terhubung ke sebuah jaringan, konfigurasi IPv4 dilakukan secara manual. Adapun IPv6 memiliki fitur stateless auto configuration di mana ketika sebuah host terhubung ke sebuah jaringan, dengan demikian konfigurasi dilakukan secara otomatis.

f. Mobilitas

Dukungan IPv4 terhadap mobilitas yang terbatas oleh kemampuan roaming saat beralih dari satu jaringan ke jaringan lain. Namun, berbeda dengan IPv6 yang memenuhi kebutuhan mobilitas tinggi melalui roaming dari satu jaringan ke jaringan lain dengan tetap terjaganya kelangsungan sambungan. Fitur ini mendukung perkembangan aplikasi-aplikasi.

g. Penggunaan Kualitas Layanan

IPv4 memakai mekanisme best effort tanpa membedakan kebutuhan, adapun IPv6 memakai mekanisme best level of effort yang memastikan kualitas layanan. Heade traffic class menentukan prioritas pengiriman paket data berdasarkan kebutuhan akan kecepatan tinggi atau tingkat latensi tinggi.

h. Routing

Performa routing IPv4 menurun seiring dengan membesarnya ukuran tabel routing. Penyebabnya pemeriksaan header MTU di tiap router dan hop switch. Berbeda

dengan IPv6 memiliki kemampuan untuk mengelola tabel routing yang besar serta proses routing yang jauh lebih efisien dari pendahulunya.

i. Ukuran Header

Ukuran header dasar IPv4 adalah 20 oktet ditambah ukuran header options yang dapat bervariasi. Di samping itu, terdapat header checksum yang diperiksa oleh tiap switch (perangkat lapis ketiga), sehingga menambah delay. Adapun ukuran header pada IPv6 tetap berjumlah 40 oktet. Sejumlah header pada IPv4, seperti Identification, Flags, Fragment Offset, Header Checksum, dan Padding telah dimodifikasi. Proses checksum pada IPv6 tidak dilakukan di tingkat header, melainkan secara end-to-end. Header IPsec telah menjamin keamanan yang memadai.

Tugas 2.4

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri dari 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan penggunaan alamat IPv6!
3. Masukkan hasilnya ke dalam table berikut!

No	Dasar Umum Alamat	Format Alamat	Penyederhanaan Bentuk Alamat	Format Prefix

4. Diskusikan komponen dalam table tersebut dengan kelompok anda!
5. Presentasikan hasil diskusi kelompok Anda di depan kelas dan mintalah tanggapan dari kelompok lain!

C. Prinsip Dasar Networking Service (Layanan Jaringan)

Network service merupakan jenis layanan yang mencakup perusahaan telekomunikasi, data carriers, ISP, wireless communication service provider, dan operator cable yang menawarkan sambungan berkecepatan tinggi. Internet saat ini merupakan kebutuhan pokok yang tidak bisa dipisahkan dari segenap sendi kehidupan. Adanya informasi-informasi praktis di internet menyebabkan masyarakat lebih suka membuka internet daripada membaca surat kabar, majalah, atau buku untuk mencari sebuah informasi. Macam-macam informasi yang disediakan oleh internet tersebut menjadikan internet sebagai pusat layanan informasi bagi masyarakat banyak.

Gambar 2. 9 Berbagai Layanan yang Ada di Internet

Melihat perkembangan saat ini, internet merupakan kebutuhan pokok bagi masyarakat luas. Bukan lagi barang mewah, internet sekarang sudah mudah diakses. Berbagai pekerjaan atau kebutuhan dapat dengan mudah selesai melalui internet Layanan-layanan yang ada di internet memang sangat membantu para penggunanya Berbagai layanan internet dapat digunakan secara gratis saat ini, semuanya memilik dampak positif maupun negatif tergantung bagaimana menggunakan semua layanan tersebut dengan bijak.

1. Format Networking Service (Layanan Jaringan)

Jaringan komputer (network) adalah sebuah sistem yang terdiri atas komputer, perangkat komputer tambahan dan perangkat jaringan lainnya seperti kabel, switch, hub, router, dan lain-lain yang saling terhubung menggunakan media tertentu dengan aturan yang sama dan bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Supaya dapat mencapai tujuan yang sama, setiap bagian dari jaringan komputer meminta dan memberikan layanan (service). Pihak yang meminta layanan disebut klien (client) dan yang memberikan layanan disebut pelayan (server). Arsitektur ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Terdapat tiga macam jenis jaringan (network), yaitu sebagai berikut.

a. Local Area Network (LAN)

LAN adalah jaringan yang dibatasi oleh area yang relatif kecil (area lokal), umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 km persegi.

b. Metropolitan Area Network (MAN)

MAN biasanya meliputi area yang lebih besar dari LAN, misalnya antarwilayah dalam satu propinsi. Pada hal ini jaringan menghubungkan beberapa buah jaringan-jaringan

kecil ke dalam lingkungan area yang lebih besar. Misalnya, jaringan bank Nusantara memiliki beberapa buah kantor cabang bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya.

c. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jaringan yang lingkupnya biasanya sudah menggunakan sarana satelit ataupun kabel bawah laut sebagai contoh keseluruhan jaringan suatu bank yang ada di Indonesia ataupun yang ada di negara-negara lain menggunakan sarana WAN untuk saling terhubung. Biasanya WAN lebih rumit dan sangat kompleks, menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN ke dalam komunikasi global seperti internet.

Akan tetapi bagaimanapun juga antara LAN, MAN, dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu dengan yang lainnya. Internet merupakan salah satu contoh jaringan nyata di dunia, internet merupakan gabungan dari jaringan-jaringan kecil yang ada di dunia yang bergabung menjadi satu jaringan yang besar di dunia. Selama terkoneksi ke jaringan besar internet, Anda bisa mengambil manfaat darinya. Beberapa aplikasi yang disediakan oleh internet, yaitu Google, Mozila, dan Firefox.

Untuk lebih jelasnya mengenai format networking service anda dapat melihat video berikut:

2. Berbagai Jenis Networking Service (Layanan Jaringan)

Semua aspek kehidupan saat ini hampir semuanya terhubung dengan layanan internet. Sekarang ini internet bukan lagi menjadi barang mewah, internet harganya sudah murah dan dapat diakses dari mana saja bahkan ada yang menyediakannya secara gratis. Layanan-layanan yang dihasilkan dari internet memang sangat membantu kehidupan masyarakat saat ini, bisa dibayangkan jika internet mati beberapa jam saja pasti banyak orang yang kebingungan. Beberapa jenis layanan yang ada di internet, di antaranya sebagai berikut.

a. Chatting

Layanan chatting saat ini menjadi salah satu layanan internet yang paling banyak digunakan untuk keperluan komunikasi antarpengguna. Chatting sekarang ini tidak hanya menggunakan media tulisan saja, akan tetapi sudah bisa menggunakan media suara, gambar, dan yang paling canggih bisa melakukan panggilan video. Aplikasi chatting yang populer saat ini, seperti WhatsApp, LINE, Facebook Messenger, Hangouts, Telegram, Skype, dan lain-lain.

b. E-Banking

Kemudahan transaksi dan transfer uang real time bisa didapatkan dengan menggunakan layanan internet e-banking. Saat ini hampir semua bank pemerintah maupun swasta menyediakan fitur e-banking ini kepada para nasabahnya. Kelebihan dari e-banking di banding dengan transaksi biasa adalah kemudahannya. Bahkan beberapa bank sudah merambah ke dunia mobile, sehingga kegiatan transfer uang bisa dilakukan di mana saja dan kapan saja, serta tidak ada jam tutup seperti bank konvensional. Pada kegiatan transfer misalkan, tidak perlu datang ke mesin ATM terdekat lagi untuk mentransfer sejumlah uang. Cukup gunakan layanan internet ini sudah bisa mentransfer uang dengan cepat.

c. E-Commerce (Electronic Commerce)

Pengertian e-commerce sebagai layanan perdagangan yang dilakukan secara elektronik. Dalam e-commerce juga terdapat promosi, pemasaran, pembelian, diskon, dan yang membedakan hanya pada medianya saja yaitu menggunakan media internet sebagai perantaranya. Pada e-commerce semuanya sudah dilakukan dengan internet mulai dari pemilihan barang, pemesanan, pembayaran, dan pengiriman. Jadi pelanggan hanya perlu menunggu di rumah saja barang sudah sampai. Contoh e-commerce di Indonesia saat ini, seperti Shopee, Tokopedia, Bukalapak, Lazada, dan Blibli.

Gambar 2. 10 Perkembangan E-commerce di Indonesia

Tugas 2.5

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan membuat situs-situs transaksi online (e-commerce) berikut!

No	Jenis Access Point	Spesifikasi
1		
2		
3		
4		

2. Rangkumlah hasil penelusuran Anda di buku tugas!
3. Kumpulkan hasilnya pada uru untuk diberi penilaian!

d. E-Government

E-government merupakan pelayanan pemerintahan kepada masyarakat yang dilakukan dengan teknologi informasi. Ada beberapa model penyampaian utama, yaitu Goverment to Citizen/Goverment to Customer (G2C) dan Goverment to Goverment (G2G). Adapun dengan menggunakan e-government masyarakat tidak perlu lagi datang ke kantor pemerintahan dengan membawa berbagai berkas yang diperlukan, tinggal lengkapi data dan unggah dokumen yang dibutuhkan saja. e-government memungkinkan untuk pelayanan publik yang lebih cepat, efisien, dan nyaman. Sudah banyak beberapa kantor pemerintahan yang menerapkan e-government ini terutama pada beberapa kota besar.

e. E-Learning

E-learning merupakan sistem pembelajaran elektronik, di mana peserta didik dan guru tidak bertatap muka secara langsung, melainkan dari jarak jauh. Komputer menjadi perantara antara pengajar dan peserta didik. Adapun dengan adanya e-learning seseorang dapat membaca materi secara berulang-ulang. Namun dapat mengurangi interaksi antara guru dengan murid secara langsung. Saat ini website e-learning di Indonesia sudah banyak bermunculan seperti Ruang Guru, Quipper, Rumah Belajar, KelasKita, Skill Academy, Pintaria, dan MauBelajar Apa. Tinggal menyesuaikan saja materi apa yang sedang dibutuhkan.

f. E-Mail (Electronic Mail)

E-mail pertama kali dikirimkan oleh Ray Tomlinson pada tahun 1971. Isi pesan pertama e-mail yang dikirimkan berupa kata QWERTYUIOP atau huruf sejenisnya. Sebagai identitas penamaan e-mail, ada tanda pemisah @ (dibaca ET) antara identitas dengan nama domain e-mail. Contoh dalam nama e-mail Google, biasanya tertulis namapengguna@gmail.com. Nama pengguna melambangkan identitas dan

gmail.com melambangkan domain e-mail yang digunakan. &E-mail sebagai jenis layanan yang paling banyak digunakan saat ini di internet, baik di Indonesia maupun di seluruh dunia. E-mail sekarang ini sudah seperti identitas pribadi, semua orang memilikinya bahkan ada yang lebih dari satu. E-mail berfungsi untuk mengirimkan pesan antarpengguna secara elektronik. Layanan e-mail dapat dikategorikan sebagai layanan e-mail gratis dan layanan e-mail berbayar. E-mail gratis yang populer, seperti AOL Mail, Gmail, Hotmail, Outlook, Pepipost, Yahoo Mail, dan Zoho Mail.

g. File Transfer Protocol (FTP)

FTP adalah layanan di internet untuk melakukan transfer antara komputer dengan banyak server di internet. FTP digunakan untuk mengirim dan menerima file di antara komputer di seluruh dunia. Cukup banyak server di internet yang menyediakan layanan ini sehingga dapat menyalin sebuah atau banyak file ke suatu komputer.

h. Gopher

Gopher adalah aplikasi perangkat lunak yang tersusun atas menu sistem pencarian informasi. Situs yang menggunakan protokol Gopher pada dasarnya berupa komputer yang menampilkan menu mewakili data dan informasi yang tersedia. Secara mendasar menu ini adalah daftar isi yang mengolah dan menunjuk informasi tertentu. Layanan ini menggunakan FTP untuk pertukaran file dan Telnet untuk terkoneksi dengan server-server tertentu. Saat ini Gopher sudah jarang sekali digunakan, bahkan hampir tidak ada.

i. Internet Relay Chat (|RC)

IRC termasuk salah suatu teknologi di mana tiap orang dapat berinteraksi dengan orang lain yang lokasinya berbeda. Adapun dengan adanya teknologi ini seseorang dapat berkenalan dengan orang baru dan memperbanyak teman atau relasi. Seseorang bisa saling melihat wajah lawan bicara dengan fitur video call, apabila komputer yang digunakan orang tersebut dilengkapi dengan WebCam.

j. Milist (Mailing List)

Milist adalah layanan yang digunakan untuk berdiskusi dalam suatu komunitas atau organisasi. Materi diskusi biasanya dilkirim ke e-mail masing-masing anggota diskusi. Penyediaan mailing list populer pada masanya adalah Yahoo Groups. Aplikasi tersebut bisa mendiskusikan berbagai macam topik diskusi dengan menjadi anggota sebuah mailing list. Setiap anggota Milist dapat membaca surat dari anggota lainnya yang berada dalam lingkaran grup diskusi dan tiap anggota juga berhak membalas surat ataupun nengabaikannya. Apabila ada salah satu anggota yang membalas pesan maka semua anggota yang berada dalam grup tersebut akan mendapat balasan pesan. Pada Milist setiap orang dapat berlangganan atau berhenti berlangganan.

Gambar 2. 11 Layanan Internet Mailing List

k. Newsgroups

Newsgroups adalah layanan di internet yang merupakan salah satu dari mailing list di internet. Pada tiap komputer terdapat beberapa newsgroup yang kemudian dibagi berdasarkan topik umum dan dibagi lagi menjadi subtopik di bawahnya. Namun tidak seperti mailing list yang menggunakan e-mail sebagai medianya, newsgroup menggunakan jaringan khusus yang disebut sebagai UseNet. UseNet sebagai sebuah sistem kelompok diskusi dengan artikel-artikel yang didistribusikan ke seluruh dunia. UseNet memiliki ribuan kelompok diskusi yang mencakup semua hal dan topik yang ada di dunia ini.

l. Tele Networking (Telnet)

Telnet merupakan program yang bisa membuat komputer menjadi pusat dari komputer lain di internet. Telnet berfungsi untuk mengakses komputer/server dari jauh. Dalam hal ini, seorang pemakai komputer (Telnet) dapat masuk ke komputer lain dan menjalankan program di komputer tersebut. Namun, pada Telnet Anda hanya dapat menjalankan program dan perintah dalam mode teks saja. Saat ini Telnet jarang digunakan karena koneksinya bisa dibajak atau dibaca. Versi Telnet yang lebih aman adalah SSH (Secure Shell) yang pada prinsipnya sama, hanya saja transfer datanya diacak dengan sistem enkripsi sehingga tidak bisa dibajak di tengah jalan.

m. Voice Over Internet Protocol (VoIP)

Voice Over Internet Protocol (VOIP) adalah layanan internet yang memungkinkan komunikasi via telepon antarpengguna dengan tanpa biaya dan hanya membutuhkan koneksi internet tanpa perlu pulsa untuk telepon. Banyak sekali layanan VOIP yang ada saat ini dan bisa digunakan dengan gratis. Salah satu contohnya, yaitu VOIP Rakyat yang bersifat open source dan hanya perlu melakukan register terlebih dahulu untuk bisa menggunakannya.

n. WAIS Server

WAIS (Wide Area Information Service) menyediakan cara lain untuk menemukan informasi yang tersebar dalam internet. WAIS mampu mengakses segala database dengan kapasitas besar, seperti dokumen, file berisi gambar, video, dan suara.

o. World Wide Web (WwW)

WWW pertama kali dikenalkan pada tahun 1989 oleh fisikawan Inggris bernama Tim Berners-Lee saat bekerja di Laboratorium Fisika Partikel Eropa. WWW adalah sebuah sistem dalam internet yang memberikan fasilitas informasi yang cepat dan menggunakan teknologi hiperteks. Layanan ini adalah layanan yang paling dikenal oleh banyak orang dan paling cepat perkembangan teknologinya. Layanan internet berupa layanan WwW sangat populer di tengah-tengah masyarakat. Layanan ini memungkinkan masyarakat bisa menjelajahi halaman website yang ada di internet. Para pencari informasi di internet memanfaatkan layanan WWW guna mencari informasi berlimpah dari internet.

Layanan ini menggunakan pranala hiperteks yang disebut hyperlink untuk merujuk pada halaman tertentu pada web server. Halaman web bisa berisi suara, gambar, animasi, teks, atau program perangkat lunak yang dapat menjadikannya dokumen yang dinamis. Pengguna mengakses world wide web dari sebuah browser sebagai program yang dapat menampilkan file HTML seperti Mozilla Firefox, Opera, dan Chrome.

Struktur sumber daya internet dalam WWW dapat dianalogikan seperti jaring laba-laba. Jika dilihat dari polanya, jaringan ini memiliki lingkaran yang terpusat pada satu titik yang sama. Dari titik tengah ini akan membentuk garis penghubung yang tegak lurus terhadap lingkaran sehingga membentuk simpul. Jika percabangan merupakan titik simpul yang mengandung data, maka tiap garis adalah penghubung yang mengkoneksikan dari tiap data. Pemilihan data ini dilakukan dengan sistem hypertext. Pada titik simpul terdapat satu atau banyak komputer yang terhubung di internet atau sebuah petunjuk yang mengarahkan ke file tertentu dalam sebuah komputer. Dalam hal ini ketika ada sebuah hyperlink maka akan ada koneksi dengan komputer lain atau berkas lainnya. Contoh WwW adalah situs yang sekarang digunakan di antaranya Facebook, Twitter, LinkedIn, dan Youtube.

Tugas 2.6

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri dari 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan berbagai jenis World Wide Web (WWW) beserta fitur-fiturnya!
3. Masukkan hasilnya ke dalam table berikut!

No	Jenis World Wide Web (WWW)	Sistem Operasi yang Digunakan	Fitur yang Dimiliki

4. Gunakan komponen dalam table di atas sebagai bahan diskusi kelompok!
5. Presentasikan hasil diskusi kelompok di depan kelas dan mintalah tanggapan dari kelompok lain!

D. Sistem Keamanan Jaringan Telekomunikasi

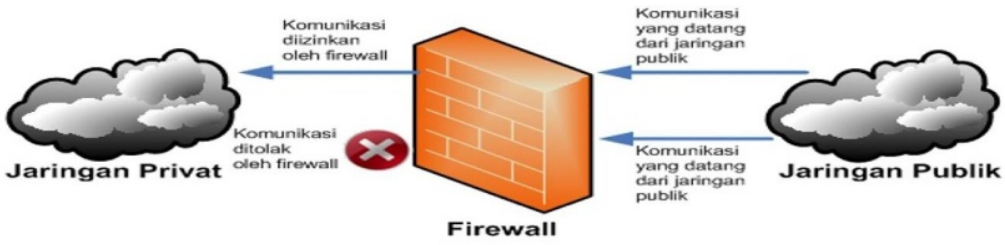
Sistem yang bersangkutan harus dilindungi dari berbagai jenis serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak bertanggung jawab. Oleh karena itu, sistem keamanan jaringan identik dengan proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer. Salah satu metode pengamanan yang umum dilakukan adalah menggunakan PIN dan password sebagaí privasi paling utama. Di samping itu, juga berfungsi untuk menjaga e-mail agar tidak jatuh kepada tangan orang-orang yang tidak bertanggung jawab.

Sebagai pengantar keamanan jaringan telekomunikasi, anda dapat melihat video berikut:

1. Dasar-Dasar Sistem Keamanan Jaringan

Satu hal mendasar yang perlu dipahami dalam penggunaan sistem keamanan jaringan (network security system) bahwa tidak ada jaringan yang antisadap maupun sistem jaringan yang benar-benar aman. Penyebab utamanya adalah sifat dasar dari jaringan Salam melakukan komunikasi dan tiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi sangat penting dalam menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Dengan demikian, hal pokok yang harus dilakukan adalah mengenal beberapa ancaman dan serangan keamanan jaringan. Security attack (serangan terhadap keamanan sistem informasi) pada dasarwarsa terakhir sering kali terjadi di dunia maya dan dilakukan oleh kelompok orang yang ingin menembus suatu keamanan sebuah sistem yang dikenal dengan kejahatan komputer (cyber crime). Adapun dengan adanya pemantauan dan pemindaian secara teratur maka penggunaan sistem oleh pihak-pihak yang tidak berhak dapat dihindari/cepat diketahui.

Penyediaan network security adalah aksi penyeimbang antara open access dengan security. Adapun dengan mengendalikan network security, risiko tersebut dapat dikurangi. Namun demikian, network security selalu bertentangan dengan network access. Jika network access makin mudah, maka akan berdampak pada network security yang makin rawan. Bila network security makin baik, justru berakibat pada network acces yang makin tidak nyaman. Oleh sebab itu, sebuah jaringan didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses ke sistem komputer, sementara Keamanan didesain untuk mengontrol akses. Guna mengetahui bentuk-bentuk aktivitas yang tidak normal, maka aktivitas yang normal pun juga perlu dipahami.



Gambar 2. 12 Arsitektur Firewalle

a. Prinsip Keamanan Jaringan

Secara mendasar, komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar dibandingkan komputer yang tidak terhubung sama sekali. Oleh sebab itu, keamanan jaringan sangatlah dibutuhkan. Metodologi keamanan informasi bertujuan untuk meminimalisasi kerusakan dan memelihara keberlangsungan sistem dengan memperhatikan berbagai kemungkinan kelemahan

dan ancaman terhadap informasi. Guna menjamin keberlangsungan sistem dengan baik, maka sebuah metodologi keamanan informasi berusaha memastikan kerahasiaan dan integritas yang ditunjang ketersediaan informasi internal.

Gambar 2. 13 Ilustrasi Prinsip Keamanan Jaringan

Berbagai aspek yang digunakan dalam prinsip keamanan jaringan dikategorikan menjadi sebagai berikut.

1) Aspek Kerahasiaan (Secrecy)
   Kerahasiaan berhubungan dengan hak akses untuk membaca data atau informasi dan suatu sistem komputer. Suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal.
2) Aspek Integritas (Integrity)
   Integrity berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem komputer. Sistem komputer dapat dinyatakan aman jika suatu data/informasi hanya dapat diubah oleh pihak yang telah diberi hak.
3) Aspek Ketersediaan (Availability)
   Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi i yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak.
4) Aspek Authentication
   Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, orang yang mengakses atau memberikan informasi adalah benar-benar orang yang dimaksud atau server yang dihubungi adalah benar-benar server yang asli. Guna membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature. Adapun untuk menguji keaslian orang atau server yang dimaksud bisa dilakukan dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.
5) Aspek Akses Kontrol
   Aspek kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana user dan sistem berkomunikasi dan berinteraksi dengan sistem dan sumber daya yang

lainnya. Akses kontrol melindungi sistem dan sumber daya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi. Kontrol akses adalah sebuah term yang mencakup beberapa tipe mekanisme berbeda yang menjalankan akses pada sistem komputer, jaringan, dan informasi. Kontrol akses sangatlah penting karena menjadi satu dari garis pertahanan pertama yang digunakan untuk menghadang akses yang tidak berhak ke dalam sistem dan sumber daya jaringan.

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

b. Identifikasi pada Gangguan, Serangan, dan Ancaman Keamanan Jaringan

Tujuan utama dalam membuat keamanan jaringan adalah untuk mengantisipasi risiko jaringan berupa bentuk ancaman fisik maupun logic secara langsung ataupun tidak langsung yang dapat mengganggu aktivitas yang sedang berlangsung dalam jaringan. Jenis-jenis gangguan, serangan, dan ancaman keamanan jaringan antara lain sebagai berikut.

1) Gangguan
Jenis-jenis gangguan keamanan jaringan dapat dillihat pada tabel berikut.

Tabel 2. 10 Jenis-jenis Gangguan Keamanan Jaringan

No.	Jenis Gangguan	Keterangan
1.	Carding	Pencurian data terhadap identitas perbankan seseorang. Misalnya, pencurian nomor kartu kredit yang digunakan untuk bertransaksi online.
2.	Phishing	Pemalsuan terhadap data resmi.
3.	Defacement	Perubahan terhadap bentuk atau tampilan website.
4.	Hacking	Perusakan pada infrastruktur jaringan komputer yang sudah ada.

2) Serangan
Serangan terhadap keamanan sistem informasi (security attack) menjadi penyebab utama terjadinya kejahatan komputer (cyber crime) pada dunia maya yang dilakukan oleh kelompok orang yang ingin menembus suatu keamanan

sebuah sistem. Beberapa tipe dari serangan yang bertujuan menerobos sistem keamaman jaringan sebagai berikut.

Tabel 2. 11 Tipe Serangan Sistem Keamanan Jaringan

No.	Tipe Serangan	Keterangan
1.	Interception	Pihak yang tidak memiliki wewenang telah berhasil mendapatkan hak akses informasi.
2.	Interruption	Penyerang yang telah dapat menguasai sistem, tetapi tidak keseluruhan. Karena admin yang asli masih bisa login.
3.	Fabrication	Penyerang telah menyisipkan objek palsu ke dalam sistem target.
4.	Modification	Penyerang telah merusak sistem dan telah mengubah secara keseluruhan

Pada dasarnya serangan terhadap suatu data dalam suatu jaringan menurut jenisnya dapat dikategorikan menjadi dua, yaitu serangan pasif dan serangan aktif.

a) Serangan Pasif

Serangan pasif diterjemahkan sebagai serangan pada sistem autentikasi dengan hanya mengamati atau memonitor pengiriman informasi ke tujuan dan tidak bertujuan menyisipkan data pada aliran data tertentu. Informasi ini dapat digunakan di lain waktu oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data kemudian menggunakannya untuk memasuki sesi autentikasi dengan berpura-pura menjadi user yang autentik (asli) disebut dengan replay attack. Beberapa informasi autentikasi seperti password atau data biometrik yang dikirim melalui transmisi elektronik dapat direkam dan digunakan untuk memalsukan data yang sesungguhnya. Serangan pasif ini sulit dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu, untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya.

b) Serangan Aktif

Serangan aktif merupakan serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket data yang salah ke dalam data stream atau dengan memodifikasi paket-paket yang melewati data stream. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitas komunikasi dan jalur-jalurnya setiap saat. Dengan demikian, hal yang dapat

dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

3) Ancaman

Bentuk-bentuk ancaman keamanan jaringan, antara lain sebagai berikut.

a) Denial of Services (DoS)

Deniel of Services (DoS) adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi terhenti, serangan yang membuat jaringan tidak bisa diakses atau serangan yang membuat sistem tidak bisa memproses/merespon terhadap traffic yang legitimasi atau permintaan layanan terhadap object dan resource jaringan. Bentuk umum dari serangan Denial of Services ini adalah dengan cara mengirim paket data dalam jumlah yang sangat besar terhadap suatu server di mana server tersebut tidak bisa memproses semuanya. Bentuk lain dari serangan keamanan jaringan Denial of Services adalah memanfaatkan celah yang rentan dari suatu operating system, layanan, atau pun aplikasi. Eksploitasi terhadap celah atau titik lemah sistem sering menyebabkan system crash atau pemakaian 100% CPU. Namun, tidak semua Denial of Services ini adalah merupakan akibat dari serangan keamanan jaringan. Eror dalam coding suatu program bisa mengakibatkan kondisi yang disebut DoS ini. Jenis-jenis DoS antara lain sebagai berikut.

- Distributed Denial of Services (DDoS)
  Distributed Denial of Services (DDoS) terjadi saat penyerang berhasil mengkompromi beberapa layanan sistem dan menggunakannya atau memanfaatkannya sebagai pusat untuk menyebarkan serangan terhadap korban lain.
- Distributed Refelective Deniel of Service (DRDoS)
  Ancaman keamanan jaringan Distributed Refelective Deniel of Service (DRDoS) memanfaatkan operasi normal dari layanan Internet, seperti protocol-2 update DNS dan router. DRDOS ini menyerang fungsi dengan mengirim update dan sesi dalam jumlah yang sangat besar kepada berbagai macam layanan server atau router dengan menggunakan address spoofing kepada target.
- Kebanjiran SYN
  Serangan keamanan jaringan dengan membanjiri sinyal SYN kepada sistem yang menggunakan protokol TCP/IP dengan melakukan inisiasi sesi komunikasi. Seperti yang diketahui, sebuah client mengirim paket SYN kepada server, server akan merespons dengan paket SYN/ACK kepada client tadi, kemudian client tadi merespons balik juga dengan paket ACK kepada server. Hal tersebut merupakan proses terbentuknya sesi komunikasi yang disebut Three-Way handshake yang dipakai untuk

transfer data sampai sesi tersebut berakhir. Kebanjiran SYN terjadi ketika melimpahnya paket SYN dikirim ke server, tetapi si pengirim tidak pernah membalas dengan paket akhir ACK.

- Smurf Attack
  Serangan keamanan jaringan dalam bentuk Smurf Attack terjadi ketika sebuah server digunakan untuk membanjiri target dengan data sampah yang tidak berguna. Server atau jaringan yang dipakai menghasilkan respons paket yang banyak seperti ICMP ECHO paket atau UDP paket dari satu paket yang dikirim. Serangan yang umum adalah dengan jalan mengirimkan broadcast kepada segmen jaringan sehingga semua node dalam jaringan akan menerima paket broadcast ini, sehingga setiap node akan merespon balik dengan satu atau lebih paket respons.
- Ping of Death
  Serangan keamanan jaringan Ping of Death adalah serangan ping yang oversize. Dengan menggunakan tool khusus, si penyerang dapat mengirimkan paket ping oversized yang banyak sekali kepada korbannya. Pada banyak kasus sistem yang diserang mencoba memproses data tersebut, eror terjadi yang menyebabkan sistem crash, freeze, atau reboot. Ping of Death ini tidak lebih dari semacam serangan buffer overflow akan tetapi karena sistem yang diserang sering jadi down, maka disebut DoS attack.
- Stream Attack
  Stream Attack terjadi saat banyak jumlah paket yang besar dikirim menuju ke port pada sistem korban menggunakan sumber nomor yang random.

b) Brute Force and Dictionary
Jenis ancaman keamanan jaringan ini lebih umum disebut sebagai Brute Force and Dictionary (memaksa masuk dan kamus password), serangan ini adalah upaya masuk ke dalam jaringan dengan menyerang database password atau menyerang login prompt yang sedang aktif. Serangan masuk paksa ini adalah suatu upaya untuk menemukan password dari akun user dengan cara yang sistematis mencoba berbagai kombinasi angka, huruf, atau simbol. Sementara serangan dengan menggunakan metode kamus password adalah upaya menemukan password dengan mencoba berbagai kemungkinan password yang biasa dipakai user secara umum dengan menggunakan daftar atau kamus password yang sudah didefinisikan sebelumnya. Guna mengatasi serangan keamanan jaringan dari jenis ini anda seharusnya memiliki suatu kebijakan tentang pemakaian password yang kuat di antaranya untuk tidak memakai password yang dekat dengan informasi pribadi misal nama, nama anak, dan tanggal lahir. Makin panjang suatu password dan kombinasinya makin sulit untuk ditemukan. Akan tetapi

dengan waktu yang cukup, semua password dapat ditemukan dengan metode brute force ini.

c) Spoofing

Spoofing adalah seni untuk menjelma menjadi sesuatu yang lain. Spoofing attack terdiri dari IP address dan node source atau tujuan yang asli atau yang valid diganti dengan IP address atau node source atau tujuan yang lain.

d) Man-in-the-middle

Serangan man-in-the-middle (serangan pembajakan) terjadi saat user perusak dapat memposisikan di antara dua titik link komunikasi. Bentuk-bentuk serangan man-in-the-middle adalah sebagai berikut.

- Para penyerang memposisikan dirinya dalam garis komunikasi di mana dia bertindak sebagai proxy atau mekanisme store-and-forwad (simpan dan lepaskan).
- Dengan jalan menggandakan atau menyusup traffic, hal ini pada dasarnya merupakan serangan penyusup.
- Para penyerang ini tidak tampak pada kedua sisi link komunikasi ini dan bisa mengubah isi dan arah traffic. Melalui cara ini para penyerang bisa menangkap logon credential atau data sensitif ataupun mampu mengubah isi pesan dari kedua titik komunikasi ini.

e) Spamming

Spam pada umumnya bukan merupakan serangan keamanan jaringan akan tetapi hampir mirip DoS. Biasanya dalam bentuk e-mail yang tidak diundang, newsgroup, atau pesan diskusi, bahkan termasuk iklan dari vendor atau bisa berisi Trojan horse.

f) Sniffer

Serangan sniffer sering difokuskan pada koneksi awal antara client dan server untuk mendapatkan logon credential, kunci rahasia, password dan lainnya. Sniffer (snooping attack) diterjemahkan sebagai kegiatan user perusak yang ingin mendapatkan informasi tentang jaringan atau traffic lewat jaringan tersebut. Sniffer sering dijumpai dalam bentuk program penangkap paket yang bisa menduplikasikan isi paket yang lewat media jaringan ke dalam file.

g) Cracker

Ancaman keamanan jaringan cracker adalah user perusak yang bermaksud menyerang suatu sistem atau seseorang. Cracker biasanya termotivasi oleh ego, power, atau ingin mendapatkan pengakuan. Akibat dari kegiatan tersebut bisa berupa pencurian (data, ide, dan lain-lain), disable system, kompromi keamanan, opini negative public, kehilangan pasar saham, mengurangi keuntungan, dan kehilangan produktivitas.

Gambar 2. 14 Kejahatan Cyber

c. Jenis-Jenis Keamanan Jaringan

Jenis-jenis keamanan jaringan, antara lain sebagai berikut.

1) Autentikasi adalah proses pengenalan peralatan, sistem operasi, aplikasi, dan identitas user yang terhubung dengan jaringan komputer. Misalnya user memasukkan username dan password pada saat login ke jaringan.
2) Kerahasiaan data (enkripsi) adalah teknik pengodean data yang dapat berguna untuk menjaga data.
3) VPN (Virtual Private Network) adalah jaringan komunikasi lokal yang dapat terhubung melalui media jaringan. Fungsi dari VPN tersendiri untuk memperoleh komunikasi yang aman melalui internet.
4) DMZ (De-Militerized Zone) berfungsi untuk melindungi sistem internal dari serangan hacker.

d. Klasifikasi Serangan ke Jaringan Komputer

Jika dilihat dari lubang keamanan yang ada pada suatu sistem, maka keamanan dapat dikategorikan sebagai berikut.

1) Keamanan Fisik (Physical Security)
   Suatu keamanan yang meliputi seluruh sistem beserta peralatan, peripheral, dan media yang digunakan. Biasanya seorang penyerang akan melakukan wiretapping (proses pengawasan dan penyadapan untuk mendapatkan password agar bisa memiliki akses).
2) Keamanan Data dan Media
   Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada software yang digunakan untuk mengolah data. Cara lainnya adalah dengan memasang backdoor atau Trojan horse pada sistem target.
3) Keamanan dari Pihak Luar
   Memanfaatkan faktor kelemahan atau kecerobohan dari orang berpengaruh (memiliki hak akses) merupakan salah satu tindakan yang diambil oleh seorang hacker maupun cracker untuk dapat masuk pada sistem yang menjadi targetnya.
4) Keamanan dalam Operasi

Merupakan salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan. Oleh karena itu, sistem tersebut dapat berjalan baik atau menjadi normal kembali.

2. Metode Keamanan Jaringan

Secara mendasar terdapat dua elemen utama pembentuk keamanan jaringan berupa tembok pengaman (firewall) dan rencana pengamanan. Tembok pengaman secara fisik maupun maya sebagai cara untuk memberikan proteksi atau perlindungan pada jaringan, baik secara fisik (kenyataan) maupun maya (menggunakan software).

Sedangkan rencana pengamanan identik dengan suatu rancangan yang nantinya akan diimplementasikan untuk melindungi jaringan agar terhindar dari berbagai ancaman dalam jaringan. Oleh sebab itu, dalam merencanakan suatu sistem keamanan jaringan terdapat beberapa metode yang dapat ditetapkan. Metode-metode tersebut, antara lain sebagai berikut.

a. Menggunakan Metode dan Mekanisme Tertentu

Beberapa metode dan mekanisme tertentu dapat dilakukan sebagai berikut.

1) Enkripsi
   Proses enkripsi merupakan salah satu pembatasan akses dengan mengodekan data dalam bentuk yang hanya dapat dibaca oleh sistem yang memiliki kunci untuk membaca data.
2) Kriptografi
   Kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga pesan agar aman.
3) Enskripsi-Deskripsi
   Proses yang digunakan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption). Ciphertext adalah sebuah pesan yang sudah tidak dapat dibaca dengan mudah.
4) Digital Signature
   Digunakan untuk menyediakan authentication, perlindungan, integritas, dan non-repudiation.
5) Algoritma Checksum (Hash)
   Digunakan untuk menyediakan perlindungan integritas, dan dapat menyediakan authentication. Satu atau lebih mekanisme dikombinasikan untuk menyediakan security service.

b. Pembatasan Akses pada Suatu Jaringan

Beberapa konsep dalam pembatasan akses jaringan, antara lain sebagai berikut.

1) Internal Password Authentication
   Password local untuk login ke sistem harus dalam bentuk password khusus serta dijaga dengan baik. Pengguna aplikasi shadow password akan sangat membantu.
2) Server Based Password Authentication
   Metode ini dapat ditemui pada sistem kerbros server atau TCP-wrapper, di mana setiap service yang disediakan oleh server tertentu dengan daftar host dan user yang boleh dan tidak boleh menggunakan service tersebut.
3) Server-Based Token Authentication
   Metode ini menggunakan authentication system yang lebih ketat menggunakan token/smart card sehingga akses-akses tertentu hanya bisa dilakukan oleh login tertentu mengggunakan token khusus.
4) Firewall dan Routing Control
   Firewall melindungi host-host pada sebuah network dari berbagai serangan, sehingga mengakses semua paket ke sistem di belakang firewall dari jaringan luar tidak dapat dilakukan langsung. Semua hubungan harus dilakukan dengan mesin firewall.

Tugas 2.7

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan pembatasan akses jaringan berikut!

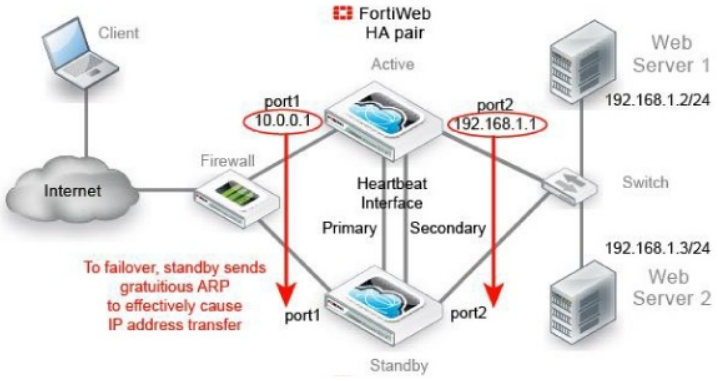
No	Jenis Pembatasan Akses Jaringan	Deskripsi

2. Rangkumlah hasil penelusuran Anda di buku tugas!
3. Kumpulkan hasilnya pada guru untuk diberi penilaian!

3. Mengonfigurasi Sistem Keamanan Jaringan

Firewall dapat didefinisikan sebagai suatu sistem peranti lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Umumnya, sebuah firewall diterapkan dalam sebuah mesin terdedikasi yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dengan jaringan internet. Firewall berfungsi untuk memfilter semua paket yang lewat pada dirinya, baik dari jaringan lokal ataupun internet. Aplikasi server jenis ini sangat penting dalam melindungi jaringan lokal dari serangan luar. Firewall digunakan untuk membatasi atau mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Supaya client bisa

mendapatkan koneksi internet dari Debian 9 Strecth yang dijadikan router harus mengatur firewall.



Gambar 2. 15 Topologi dengan Single Firewall

a. Dasar-Dasar Konfigurasi Sistem Keamanan Jaringan

Network firewall yang pertama muncul pada akhir era 1980-an, berupa perangkat router yang dipakai untuk memisahkan suatu network menjadi jaringan lokal (LAN) lebih kecil. Firewall untuk keperluan sekuriti (security firewall) pertama kali digunakan pada awal dekade 1990-an, berupa router IP dengan aturan filter tertentu. Pada kondisi ini, penggunaan firewall hanya diperuntukan untuk mengurangi masalah peluberan (spill over) data dari LAN ke seluruh jaringan. Hal ini mencegah masalah-masalah eror pada manajemen jaringan maupun aplikasi yang banyak menggunakan sumber daya ke seluruh jaringan. Aplikasi firewall yang terkenal pada Linux adalah IpTables dan Shorewall. Pada distribusi Linux jenis terbaru, Ip Tables secara default sudah terinstall. Adapun dengan catatan, bahwa kernel dari Linux OS yang digunakan minimal kernel 2.4 ke atas dengan IpTables (netfilter) aktif. Pada masa sekarang, penggunaan firewall menjadi istilah yang merujuk pada sistem yang mengatur komunikasi antar dua jenis jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke internet dan jaringan berbadan hukum di dalamnya, maka perlu adanya perlindungan terhadap peranti digital dari serangan pemata-mata, para peretas, ataupun pencuri data lainnya menjadi sebuah realita. Beberapa tools yang berhubungan dengan firewall (IpTables) antara lain sebagai berikut.

1) Ip Tables
   IpTables identik dengan tools dalam Linux OS yang berfungsi sebagai sarana dalam melakukan filter (penyaringan) terhadap (traffic) lalu lintas data. Adapun dengan Ip Tables inilah seorang administrator akan mengatur semua arus lalu lintas yang masuk mau pun keluar ke komputer, ataupun traffic yang sekedar melewati komputer client.
2) Prerouting dan Postrouting

Prerouting digunakan untuk melakukan NAT paket data yang memasuki firewall. Pada umumnya digunakan pada transparency proxy server dan membangun beberapa server dengan satu IP public. Sedangkan postrouting digunakan untuk melakukan NAT paket data yang keluar dari firewall. Pada umumnya digunakan untuk translasi alamat IP.

b. Konfigurasi Sistem Keamanan Jaringan Menggunakan Firewall

Secara mendasar, firewall digunakan sebagai sebuah mekanisme yang dapat diterapkan terhadap peranti lunak (software), peranti keras (hardware), maupun pada sistem yang bersangkutan dengan tujuan utama untuk melindungi dengan cara menyaring, membatasi atau bahkan menolak suatu atau semua kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau Local Area Network (LAN).

1) Teknik-Teknik pada Firewall

Biasanya firewall akan mengecek nomor IP address dan juga nomor port yang digunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menerjemahkan setiap permintaan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri, seperti layanan untuk web ataupun untuk mail. Teknik-teknik yang digunakan oleh sebuah firewall antara lain sebagai berikut.

a) Direction Control (Kendali Terhadap Arah)
   Aspek ini didasarkan pada arah dari berbagai permintaan (request) terhadap layanan yang akan dikenali dan diijinkan melewati firewall.
b) User Control (Kendali Terhadap User)
   Aspek ini didasarkan pada user dalam menjalankan suatu layanan. Biasanya digunakan untuk membatasi user dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.
c) Behavior Control (Kendali Terhadap Perlakuan)
   Aspek ini didasarkan pada seberapa banyak layanan itu telah digunakan. Misalnya firewall dapat memfilter e-mail untuk menanggulangi/mencegah spam.
d) Service Control (Kendali terhadap Layanan)
   Aspek ini didasarkan pada tipe-tipe layanan yang digunakan di internet dan boleh diakses baik untuk ke dalam ataupun ke luar firewall. Biasanya firewall akan mengecek nomor IP address dan juga nomor port yang digunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi software untuk proxy yang akan menerima dan menerjemahkan setiap permintaan akan suatu

layanan sebelum mengijinkannya. Bahkan bisa jadi software pada server itu sendiri, seperti layanan untuk web ataupun untuk mail.

2) Model-Model pada Firewall

Ip Tables sering disebut sebagai statefull protocol karena memiliki jenis koneksi application layer gateway (proxy firewall), packet filtering gateway, circuit level gateway, dan statefull multilayer inspection firewall.

a) Application Layer Gateway (Proxy Firewall)

Model firewall ini memiliki mekanismenya tidak hanya berdasarkan sumber, tujuan, dan atribut paket, tetapi bisa mencapai isi (content) paket tersebut.

b) Packet Filtering Gateway

Jenis firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya.

c) Circuit Level Gateway

Firewall jenis ini akan melakukan pengawasan terhadap awal hubungan TCP sehingga disebut TCP Handshaking sebagai proses dalam menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Secara mendasar, model jenis ini bekerja pada bagian lapisan transport dari model referensi TCP/IP. Bentuknya hampir sama dengan application layer gateway, hanya berbeda pada bagian yang difilter berada pada layer transport.

d) Statefull Multilayer Inspection Firewall

Adapun dengan penggabungan ketiga model firewall yaitu packet filtering gateway, application layer gateway, dan circuit level gateway dapat dikatakan sebagai firewall yang memberikan fitur terbanvak dan memberikan tingkat keamanan yang paling tinggi. Firewall jenis ini akan bekerja pada lapisan application, transport, dan internet. Aplikasi pengendalian jaringan dengan firewall dapat diimplementasikan pada seiumlah aturan (chains) pada topologi yang sudah ada. Dua faktor penting yang harus diperhatikan dalam pengendalian jaringan menggunakan IpTables yaitu koneksi paket yang menerapkan firewall yang digunakan dan konsep firewall yang diterapkan. Adapun dengan IpTables sebagai aturan guna mendefinisikan firewall agar memiliki kemampuan dalam mengenali koneksi yang terjadi berupa koneksi baru (new), koneksi yang telah ada (establish), koneksi yang memiliki relasi dengan koneksi lainnya (related) atau koneksi yang tidak valid (invalid).

4. Evaluasi Keamanan Jaringan

Penyebab masalah keamanan jaringan harus selalu dimonitor secara berkala, dengan tujuan untuk mengantipisipasi lubang keamanan (security hole) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Adakalanya lubang keamanan yang ditimbulkan oleh kecerobohan implementasi. Di samping itu, kesalahan konfigurasi karena lalai

mengakibatkan sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak. Adanya penambahan perangkat baru (hardware dan/atau software) juga bisa menyebabkan menurunnya tingkat security atau berubahnya metode untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

a. Sumber Lubang Keamanan

Beberapa sumber lubang keamanan yang paling sering terjadi sebagai berikut.

1) Salah Desain (Design Flaw)
   Salah desain (design flaw) umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat desain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada. Misalnya sebagai berikut.

   a) Kesalahan desain urutan nomor (sequence numbering) dari paket TCP/IP. Kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama "IP spoofing" (sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah mengamati urutan paket dari host yang hendak diserang).
   b) Lemah desainnya algoritma enkripsi ROT13 atau Caesar cipher, di mana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.

2) Implementasi Kurang Baik
   Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengodean hingga tidak adanya cek atau testing implementasi dari sebuah "array" tidak dicek sehingga terjadi yang disebut out-of-bound array suatu program yang baru dibuat. Misalnya tidak memperhatikan batas ("bound") atau buffer overflow yang dapat dieksploitasi (misalnya overwrite ke variable berikutnya). Di samping itu, terjadinya kelalaian memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program sehingga seseorang dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

b. Salah Konfigurasi

Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi "writeable Apabila berkas tersebut merupakan berkas yang penting, seperi

berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan. Kadangkala sebuah komputer dijual dengan konfigurasi yang sangat lemah. Di samping itu, adanya program yang secara tidak sengaja diset menjadi "setuid root" sehingga ketika dijalankan pemakai memiliki akses seperti super user (root) yang dapat melakukan apa saja.

c. Salah Menggunakan Program atau Sistem

Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal.

Tugas 2.8

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri atas 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan implementasi Windows Firewall pada Windows 10 dan Windows11!
3. Masukkan hasilnya ke dalam table berikut!

No	Windows 10		Windows 11	
	Posisi	Screenshoot	Posisi	Screenshoot

4. Selanjutnya, diskusikan komponen dalam table tersebut bersama teman kelompok Anda!
5. Presentasikan hasil diskusi kelompok Anda di depan kelas dan mintalah tanggapan dari kelompok lain!

E. Prinsip Dasar Sistem Seluler

Sistem seluler merupakan salah satu jenis komunikasi bergerak, yaitu suatu komunikasi antara dua buah terminal dengan salah satu atau kedua terminal berpindah tempat. Adapun dengan adanya perpindahan tempat ini, sistem komunikasi bergerak tidak menggunakan kabel sebagai medium transmisi. Sistem komunikasi seluler dapat melayani banyak pengguna pada cakupan area geografis yang cukup luas dalam frekuensi yang terbatas. Sistem ini juga menawarkan kualitas yang cukup tinggi dan tidak kalah jika dibandingkan dengan telepon tetap (Public Switched Telephone Network atau PSTN) yang lebih dikenal dengan istilah telepon rumah. Guna menambah kapasitas, daerah jangkauannya dibatasi dengan adanya pembagian area menjadi sel-sel. Adapun dengan adanya sel-sel ini, kanal radio dapat dipergunakan kembali (re-use) oleh base station pada jarak yang berjauhan. Ketika pengguna jasa seluer berpindah dari satu sel ke sel lain, panggilan dijaga agar tidak terinterupsi dengan menggunakan salah satu teknik switching, yaitu hand off.

1. Sejarah Teknologi Seluler

Dalam sejarahnya, telepon pertama kali ditemukan dan diciptakan oleh Alexander Graham Bell pada tahun 1876. sedangkan komunikasi tanpa kabel (wireless) ditemukan oleh Nikola Tesla pada tahun 1880 dan diperkenalkan oleh Guglielmo Marconi. Akar dari perkembangan digital wireless dan seluler dimulai sejak 1940 saat teknologi telepon mobile secara komersial diperkenalkan. Apabila dibandingkan dengan perkembangan sekarang yang begitu pesat, sebenarnya teknologi ini mengalami hambatan dalam perkembangan kurang lebih selama 60 tahun.

Hal ini di karenakan perkembangan teknologi yang murah seperti transistor atau semikonduktor belum dikembangkan dengan baik. Setelah ditemukannya transistor maka dimungkinkan perkembangan teknologi menjadi lebih pesat. Sehingga memungkinkan melahirkan teknologi ponsel yang saat ini digunakan oleh milyaran masyarakat dunia. Ide tercetusnya telepon genggam pertama kali diutarakan oleh Cooper yang merupakan salah satu tim divisi Motorolla yang ingin ada sebuah alat komunikasi yang mudah dibawa secara fleksibel untuk bepergian. Pertama kalinya telepon genggam dibuat beratnya masih 2 kilogram. Keberadaan telepon seluler atau ponsel tak luput dari jasa Amos Joel Jr yang merupakan pakar dalam bidang switching. Berkat Amos Joel Jr penggunaan ponsel menjadi nyaman.

2. Jenis Teknologi Seluler

Teknologi jaringan seluler telah sampai pada generasi ke-5 atau yang dikenal dengan nama 5G. Teknologi jaringan ini pun disebut mampu menghantarkan kecepatan data 20 kali lebih cepat dari generasi sebelumnya, yakni 4G. Huruf G merujuk pada kata "Generation" atau generasi. Masing-masing generasi memiliki standar jaringan tertentu yang disesuaikan dengan standar jaringan telepon dan sistem telepon seluler pada saat itu. Beberapa negara di kawasan Amerika Utara, Eropa, dan Asia Timur sudah menggelar teknologi 5G secara komersial. Indonesia sendiri pun saat ini sudah beberapa kali melakukan uji coba jaringan 5G. Bahkan, Kementerian Komunikasi dan Informatika (Kemenkominfo) menegaskan bahwa Indonesia telah siap mengadopsi teknologi 5G sejak tahun 2021.

a. 1G

Sesuai namanya, 1G merupakan generasi pertama pada teknologi telepon seluler. Teknologi jaringan ini pertama kali diluncurkan oleh Nippon Telegraph dan Telephone pada 1979 silam. Baru kemudian di tahun 1984, teknologi 1G menyelimuti seluruh wilayah Jepang dan menjadikannya sebagai negara pertama yang memiliki jaringan 1G secara nasional. Di Indonesia, teknologi 1G pertama kali diperkenalkan pada tahun 1984. Secara teknis, 1G beroperasi dengan menggunakan sistem analog yang umumnya dikenal dengan AMPS (Advanced Mobile Phone Service), di mana hanya memiliki kecepatan maksimum 2,4 Kbps. 1G hanya dapat dipakai untuk melakukan

panggilan telepon, itu pun dengan kualitas yang buruk, boros baterai, dan tidak terenkripsi. Sehingga, percakapan pun dapat disadap dengan menggunakan pemindai radio.

b. 2G

Teknologi jaringan seluler generasi kedua ini bisa dibilang menjadi awal kelahiran teknologi digital. Bila pada 1G menggunakan jaringan analog, maka di 2G sudah menggunakan jaringan digital. Teknologi 2G pertama kali diluncurkan secara komersial di Finlandia oleh Radiolinja pada 1991 dengan mengimplementasikan teknologi GSM (Global System for Mobile Communications) berbasis teknologi TDMA (Time Division Multiple Access). Teknologi 2G pertama kali hadir di Indonesia pada tahun 1993.

Kehadiran 2G pada saat itu menyuguhkan pengalaman baru dalam berkomunikasi. Apabila 1G hanya dapat melakukan panggilan telepon, maka di 2G terdapat beberapa fitur baru, antara lain bertukar pesan teks (SMS), pesan bergambar (MMS), dan suara panggilan yang lebih jernih. Bahkan, dalam perkembangannya 2G pun kemudian berevolusi menjadi 2,5G dengan GPRS (General Packet Radio Service) dan 2,75G dengan EDGE (Enhanced Data rates for Global Evolution), di mana kecepatan maksimal mencapai 473 Kbps. o neil

c. 3G

Hadirnya 3G membuat masyarakat di seluruh dunia sudah dapat menikmati berbagai macam layanan internet, seperti browsing, pengiriman e-mail, streaming video dan musik, berbagi data, hingga teleconference. Era 3G juga menjadi era kelahiran smartphone dengan dua nama besar pada saat itu, yakni Blackberry dan Apple. Teknologi penerus 2G ini pertama kali diluncurkan pada 2001 oleh operator asal Jepang NTT DoCoMo. Teknologi 3G hadir sebagai sebuah solusi akan kebutuhan internet yang meningkat pada masa itu dengan menggunakan standar UMTS (Universal Mobile Telecommunications System). Teknologi ini sanggup menghantarkan kecepatan data yang lebih cepat dari generasi sebelumnya dengan kecepatan mencapai 2 Mbps.

Teknologi 3G menjadi standar teknologi telepon bergerak (mobile phone), menggantikan 2.5G. Hal ini berdasarkan International Telecommunication Union (ITU) dengan standar IMT-2000. Jaringan 3G memungkinkan operator jaringan untuk menawarkan jangkauan yang lebih luas dari fasilitas tingkat lanjut ketika mencapai kapasitas jaringan yang lebih besar melalui peningkatan efisiensi penggunaan spektrum. Kemampuannya meliputi komunikasi suara nirkabel dalam jangkauan area luas (wide-area wireless voice telephony), panggilan video (video calls), dan jalur data kecepatan tinggi nirkabel (broadband wireless data), dan semuanya itu berkerja dalam perangkat bergerak (mobile).

Perangkat bergerak (mobile) termasuk teknologi komunikasi jaringan nirkabel yang memungkinkan pergerakan user untuk tetap terhubung selama komunikasi berlangsung. Tujuan komunikasi seluler untuk memudahkan konsumen dalam berkomunikasi di mana pun dan kapan pun. Prinsip dasar dari sistem komunikasi seluler yakni adanya daya pancar yang mencakup sel, menggunakan frequency reuse untuk efesiensi pemakaian frekuensi yang tinggi, dan adanya handover. Handover memungkinkan User Equipment (UE) untuk tetap terhubung walau dalam kondisi bergerak. Handover adalah proses pengalihan kanal traffic secara otomatis pada UE yang sedang digunakan untuk berkomunikasi tanpa putus sambungan. Handover pada dasarnya terdapat dua jenis yaitu soft handover dan hard handover.

Hard handover adalah tipe handover yang menggunakan metode break-before- make yaitu pemutusan hubungan dengan kanal trafik lama sebelum terjadi hubungan dengan kanal trafik baru. Masalah hard handover yakni ketika melakukan break-before-make jaringan diputus sementara untuk beberapa waktu sebelum terkoneksi kembali ke jaringan. Hal ini memungkinkan adanya pengaruh pada sisi kualitas UE saat melakukan sambungan. Jika hard handover sukses ditandai dengan tidak adanya putus sambungan atau dropping sehingga UE tetap terhubung meski dalam keadaan berpindah sel. Namun jika gagal dalam proses hard handover UE akan terputus total sehingga tidak dapat tersambung dengan UE yang lainnya dan hal menjadi kendala dalam kualitas layanan yang disediakan oleh jaringan WCDMA.

d. 4G

Kebutuhan akan layanan internet dengan menggunakan teknologi jaringan 3G dinilai tidak cukup. Maka dari itu, guna membuat penggunaan layanan internet makin nyaman, lahirlah teknologi 4G. Teknologi ini pertama kali diluncurkan secara komersial di Stockholm, Swedia dan Oslo, Norwegia pada 2009 yang menggunakan standar LTE (Long Term Evolution) berbasis teknologi OFDM (Orthogonal Frequency Division Multiplexing). Era 4G bisa dibilang sebagai lahirnya industri konten kreatif. Adapun dengan kecepatan LTE hingga 100 Mbps pada awal peluncuran dan berevolusi menjadi LTE-Advanced yang dapat mendapat kecepatan 1 Gbps, 4G menawarkan kemampuan untuk streaming video dengan kualitas HD, game online tanpa lag, dan waktu upload dan download yang lebih singkat. Tak hanya itu, 4G pun membuat proses komunikasi jadi lebih lancar dengan video conference, serta memunculkan lebih banyak startup digital.

e. 5G

5G lahir sebagai sebuah jawaban atas kebutuhan koneksi ke tahap yang lebih tinggi dalam beberapa tahun ke depan. Karenanya, sejumlah perusahaan dengan ekosistem mobile saat ini berkontribusi dan berupaya agar 5G dapat dinikmati oleh masyarakat di dunia. 5G saat ini sudah diluncurkan secara komersial di beberapa negara, seperti

Korea Selatan, Amerika Serikat, Jepang, Tiongkok, Turki, dan beberapa negara di Eropa.

Untuk lebih jelasnya mengenai prinsip dasar jaringan seluler, anda dapat melihat video berikut:

Sebagaimana halnya teknologi jaringan penerus, sudah pasti 5G memiliki kemampuan yang lebih canggih dari 4G, antara lain secara teori dapat mencapai kecepatan data hingga 20 kali lebih cepat (20 Gbps), latency 10 kali lebih rendah (1ms), dan jumlah connection density 10 kali lebih banyak dari 4G (1 juta devices/km^2), sehingga penggunaannya tidak hanya untuk pemenuhan layanan mobile broadband untuk konsumen, namun juga untuk Industry 4.0. Adapun beberapa contoh us cases untuk konsumen, seperti enhanced mobile broadband, Virtual Reality (VR), Augmented Reality (AR), dan cloud gaming.

Tugas 2.9

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan jenis teknologi seluler. Informasi yang diperoleh dimasukkan pada table berikut!

No	Jenis Teknologi Seluler	Deskripsi
1	1G	
2	2G	
3	3G	
4	4G	
5	5G	

2. Rangkumlah hasil penelusuran Anda!
3. Kumpulkan hasilnya pada guru untuk diberi penilaian!

3. Komponen Komunikasi Seluler

Sistem komunikasi seluler terdiri dari komponen-komponen berikut.

a. PSTN

PSTN tersusun atas local networks, exchange area networks, dan long-haul network. PSTN menginterkoneksikan antara telepon dengan peralatan komunikasi lain.

b. Mobile Switching Center (MSC)

Mobile Switching Center (MSC) atau Mobile Telephone Switching Office (MTSO). Dalam sistem komunikasi seluler, MSC berfungsi untuk menghubungkan antara telepon seluler dengan PSTN. Dalam sistem seluler analog, MSC berfungsi untuk mengatur agar sistem tetap beroperasi. Suatu MSC dapat menangani 100.000 pelanggan seluler dan 5.000 panggilan dalam waktu yang bersamaan.

c. Base Station

Base station sering disebut juga sebagai Base Transceiver Station (BTS) pada sistem GSM. Pada base station, terdapat beberapa pemancar (transmitter atau TX) dan penerima (receiver atau RX). TX dan RX akan menangani komunikasi full duplex secara serempak. Biasanya, TX dan RX dikombinasikan menjadi transceiver (TRX) yang diletakkan di dalam suatu Radio Base Station (RBS). Base station biasanya juga mempunyai menara untuk membantu proses pemancaran atau penerimaan sinyal pada antena.

d. Mobile Station (MS)

jasa komunikasi seluler untuk memperoleh layanan. Beberapa komponen yang ada Mobile Station (MS) merupakan suatu perangkat yang digunakan oleh pelanggan pada Mobile Station (MS) mencakup transceiver, antena, rangkaian pengontrol, dan sebagainya. Selain itu, Mobile Station (MS) juga dilengkapi dengan kartu Subscriber Identity Module (SIM) yang berisi nomor identitas pelanggan. Mobile Station (MS) biasa dikenal sebagai handphone alias HP dalam keseharian.

e. BSC (Base Stations Controler)

BSC (Base Stations Controler) yaitu suatu antena induk yang memiliki fungsi sebagai berikut.

1) Interface ke Mobile Switching Center (MSC).
2) Lokasi remote atau co-located dengan MSC.
3) Melakukan kontrol beban BTS.
4) Melakukan kontrol terhadap proses soft, softer atau hard handoff.
5) Melakukan kontrol terhadap transmit power MS.
6) Melakukan resource management, walsh code, dan trunk.
7) Mendukung kontrol terhadap call processing, dan call setup atau call release.
8) Mendukung statistic management.

4. Ruang Lingkup Sistem Seluler

Sistem seluler dewasa ini berkembang cukup pesat. Sistem seluler yang dipakai saat ini, yaitu AMPS (Advanced Mobile Phone Service) di Amerika Utara, MCS (Mobile Communications System) di Jepang, TACS (Total Access Communications System), GSM (Group Special Mobile), Spread-Spectrum CDMA (Code Division Multiple Access). Namun bila dilihat dari metode akses yang digunakan, pada dasarnya ada 3 sistem seluler, yaitu sistem seluler yang menggunakan metode akses FDMA (Frequency Division Mulltiple Access), metode akses TDMA (Time Division Multiple Access), dan metode akses CDMA (Code Division Multiple Access). Konsep awal wireless menggunakan transmitter (base station) dengan tower yang tinggi dan daya pancar yang tinggi untuk coverage yang luas. Adapun konsep seluler menggunakan beberapa transmitter (base station) daya dan ketinggian yang rendah untuk memberikan coverage yang terbatas serta sekelompok sel (cluster) untuk membagi spektrum frekuensi ke dalam kanal yang berbeda.

5. Cara Kerja Perangkat Seluler (Ponsel)

Perkembangan teknologi yang makin pesat membuat umat manusia selalu berinovasi dengan ilmu pengetahuan, termasuk salah satu di antaranya adalah telepon seluler (ponsel). Adapun dengan ponsel, pengguna dapat berbicara dan menyampaikan informasi baik dari jarak dekat maupun jauh. Hingga pada akhirnya kini, ponsel menjadi perangkat canggih dan pintar yang dilengkapi dengan tambahan fitur lainnya seperti kamera digital, radio, LCD berwarna dengan resolusi tinggi.

Pada dasarnya, ponsel merupakan alat komunikasi wireless yaitu komunikasi bergerak tanpa kabel (nirkabel) berbasiskan mobile device. Prinsip dari komunikasi wireless ini menggunakan kanal radio yang terpisah untuk berkomunikasi dengan cell site. Bisa dibilang juga, ponsel adalah perangkat telekomunikasi elektronik yang mempunyai kemampuan dasar yang sama dengan telepon fixed line konvensional, namun dapat dibawa ke mana-mana (portabel, mobile) dan tidak perlu disambungkan dengan jaringan telepon yang menggunakan kabel (nirkabel dan wireless).

Menilik dari sistem ponsel terdiri dari perangkat keras (hardware) dan perangkat lunak (software). Tanpa perangkat lunak ini hanya benda keras saja, demikian juga perangkat tanpa perangkat keras, hanya merupakan kode-kode komputer saja.

Pada dasarnya, cara kerja telepon seluler (ponsel) tidak menggunakan sistem wireline, namun menggunakan sistem wireless. Sistem wireless adalah jaringan nirkabel di mana cara kerjanya tanpa menggunakan kabel untuk berkomunikasi dengan pengguna yang lain. Antara pengirim dan penerima harus tercakup dalam Base Transceiver Station (BTS) yang memfasilitasi antar pengguna telepon seluler secara wireless. Cara kerja ponsel diawali dengan microphone menerima suara dari pengirim. Selanjutnya gelombang suara yang ditangkap microphone diubah menjadi

sinyal listrik yang kemudian dipancarkan ke BTS terdekat oleh ponsel. Berikutnya, BTS menerima sinyal tersebut untuk diteruskan ke pusat telekomunikasi dan pusat telekomunikasi meneruskan sinyal ke BTS terdekat untuk diteruskan kepada penerima. Pada akhirnya, sinyal yang sampai pada penerima diubah menjadi gelombang suara oleh speaker.

Tugas 2.10

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri dari 3-4 anggoa!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan ruang lingkup system seluler!
3. Masukkan hasilnya ke dalam table berikut!

No	Tipe Perangkat	Keterangan		
		Deskripsi	Kelebihan	Kekurangan
1	AMPS (Advanced Mobile Phone Service			
2	MCS (Mobile Communicaions System)			
3	TACS (Total Access Communications System)			
4	GSM (Group Spsecial Mobile)			
5	CDMA (Code Division Multiple Access)			

4. Gunakan komponen dalam table di atas menjadi bahan diskusi kelompok!
5. Presentasikan hasil diskusi kelompok di depan kelas dan mintalah tanggapan dari kelompok lain!

F. Prinsip Dasar Sistem Microwave

Microwave atau gelombang mikro menjadi salah satu jenis gelombang yang memiliki frekuensi dan daerah panjang gelombang tertentu. Sangat banyak gelombang elektromagnetik yang memiliki sifat berbeda karena memiliki panjang gelombang yang berbeda dan frekuensi yang juga berbeda. Adapun yang perlu diketahui secara umum ialah bagaimana peningkatan energi dari gelombang sesuai dengan panjang gelombangnya. Makin kecil panjang gelombang maka energinya makin besar, begitu pula sebaliknya, sesuai dengan rumus $E = hc/\lambda$. Energi berbanding terbalik dengan (panjang gelombang). Oleh karena itu, sinar gama memiliki energi terbesar, sedangkan gelombang radio yang memiliki energi terendah. Gelombang radio dipakai dalam komunikasi manusia di bumi, adapun untuk HP menggunakan gelombang mikro.

1. Mengenal Microwave Link

Jika Anda berjalan-jalan dan melihat menara Base Transceiver Station (BTS) dan terdapat seperti gendang itu bisa disebut dengan microwave link. Microwave link merupakan sistem komunikasi yang menggunakan gelombang radio dalam berkomunikasi. Rentang frekekuensi gelombang mikro digunakan untuk mengirimkan informasi antara dua lokasi. Microwave link banyak digunakan di dalam industri. Seperti dalam penyiaran menggunakan tautan gelombang mikro untuk mengirim informasi atau program dari studio ke lokasi pemancar yang bisa jadi jaraknya bermil-mil.

Gambar 2. 16 Microwave Link

Transmisi microwave link termasuk teknologi untuk sistem transmisi data menggunakan media nirkabel pada rentang frekuensi gelombang mikro. Transmisi microwave link terdiri atas perangkat radio microwave. Transmisi microwave link banyak diimplementasikan pada beberapa provider telekomunikasi seluler. Teknologi transmisi microwave link banyak diterapkan oleh beberapa provider telekomunikasi dikarenakan cepat dalam hal penggelaran untuk jarak jangkau yang jauh dalam mentransmisikan data lewat udara.

Adapun selain itu, dengan teknologi ini penyedia layanan internet nirkabel menggunakan tautan gelombang mikro untuk menyediakan akses internet dengan kecepatan tinggi tanpa menggunakan koneksi kabel. Perusahaan telepon juga menggunakan untuk mentransmisikan panggilan antara pusat switching melalui tautan gelombang mikro. Misalnya kartu SIM Anda mendapat sinyal atau koneksi internet di berbagai tempat. Koneksi di perangkat Anda akan mencari dan menghubungkan kartu SIM ke tower BTS terdekat dari jangkauannya, sehingga Anda mendapatkan sinyal dari BTS ke kartu SIM tersebut.

a. Fungsi Microwave Link

Antena microwave memiliki fungsi untuk menerima serta memancarkan gelombang micro/radio dari BTS ke Base Station Controller (BSC), atau juga dari Base Transceiver Station (BTS) ke Base Transceiver Station (BTS). Sedangkan dalam microwave system dibagi menjadi dua bagian yaitu indoor unit dan outdoor unit. Indoor unit berada di

dalam shelter dan outdoor unit itu berada dan melekat pada antena microwave. Tautan gelombang mikro sangat mudah beradaptasi karena tautan tersebut adalah broadband. Broadband merupakan jangkauan frekuensi yang begitu luas yang digunakan untuk mengirim data atau menerima data, selain itu merupakan koneksi internet transmisi data yang berkecepatan tinggi.

Jadi, gelombang mikro begitu mudah beradaptasi dikarenakan dapat memindahkan sejumlah besar informasi dengan kecepatan tinggi. Selain itu gelombang mikro dapat menembus hujan, kabut dan salju, diperkirakan cuaca buruk tidak mengganggu transmisi. Microwave link satu arah mencangkup empat elemen utama yaitu pemancar, penerima, saluran transmisi, dan antena. Komponen ini berada di setiap sistem komunikasi radio, termasuk telepon seluler, radio dua arah, jaringan nirkabel, dan penyiaran komersial.

b. Tujuan Microwave Link

Perencanaan link microwave sangat tidak terduga, segala faktor yang memungkinkan terjadinya redaman harus diperhitungkan dengan teliti. Oleh karena itu, dalam merencanakannya memerlukan pengetahuan tentang sifat-sifat atmosfer. Saluran (link) microwave beroperasi antara frekuensi 2 - 58 GHz. Tujuan utama dari perencanaan link microwave adalah untuk memastikan bahwa jaringan microwave dapat beroperasi dengan kinerja yang tinggi pada segala tipe kondisi atmosfer. Perencanaan link microwave mencakup 4 (empat) langkah penting.

1) Panjang lintasan merupakan jarak antara antena pemancar dengan antena penerima, panjang lintasan didapatkan dengan cara mengukur kedua titik antena pada peta.
2) Perhitungan tinggi antena harus dilakukan agar perancangan suatu jaringan microwave sesuai dengan yang diharapkan.
3) Perencanaan frekuensi ini harus sesuai dengan jarak antena pemancar dan antena penerima, di luar kota dengan jarak 30 km menggunakan frekuensi 7Ghz, sedangkan untuk BTS yang dioperasikan di kota cenderung memakai frekuensi 18 Ghz dengan jarak 500 m s.d. 2 km. Pada jarak sedang 5 s.d. 7 km menggunakan radio microwave 13 Ghz.
4) Perhitungan kinerja (performance calculations). Tujuan dari path calculation adalah untuk menentukan Receive Signal Level (RSL), menentukan besarnya Fading Margin (FM) untuk memenuhi time avaibility requirement, dan memenuhi BER (Bit Error Rate) requirement. Parameter-parameter yang dihitung meliputi daya pancar, besarnya redaman, dan besarnya penguatan.

Tugas 2.11

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan beberapa provider telekomunikasi seluluer. Informasi yang diperoleh dimasukkan table berikut!

No	Nama Provider	Jenis Layanan	Deskripsi

2. Rangkumlah hasil penelusuran Anda di buku tugas!
3. Kumpulkan hasilnya pada guru Anda untuk diberi penilaian!

2. Komponen Microwave Link

Dalam dunia telekomunikasi bergerak, antena yang bundar ini dan sering disebut sebagai antena parabola ini dipakai oleh perangkat yang dinamai perangkat transmisi radio microwave (gelombang mikro) point to point. Disebut microwave/ gelombang mikro, karena frekuensi yang dipakai cukup tinggi dimulai dari 3 GHz sampai 80 GHz. Microwave point to point mempunyai beberapa keuntungan dibandingkan jaringan optikal dan copper, yaitu cepatnya instalasi, harga perangkat dan instalasi yang lebih murah, berguna untuk daerah yang bergambut, antarpulau, pegunungan maupun pedesaan.

Di dalam microwave link terdapat beberapa komponen sebagai berikut.

a. Indoor Unit (IDU)

Indoor Unit (IDU) berfungsi sebagai modulator-demodulator sinyal. Selain itu juga berfungsi sebagai Forward Error Correction (FEC). Indoor unit biasanya diletakkan dalam gedung.

b. Outdoor Unit (ODU)

Outdoor Unit (ODU) berfungsi untuk melakukan konversi sinyal digital termodulasi yang mempunyai frekuensi dari rendah ke frekuensi tinggi. Daya Outdoor Unit (ODU) didistribusi dari indoor unit melalui kabel coaxial.

c. Antena

Antena berguna untuk mentransfer energi elektromagnetik dari ruang bebas kesaluran transmisi dan sebaliknya.

d. Waveguide

Waveguide berguna untuk meminimalisir redaman (loss) yaitu salah satu kunci dari link microwave.

e. Menara

Menara digunakan untuk menopang microwave antena, perhitungan dalam jumlah antena dan beban total harus benar agar tidak melampaui kapasitas beban maksimum dari menara.

3. Saluran pada Microwave Link

Beberapa saluran pada microwave link, saluran microwave dapat dibagi menjadi tiga kategori yaitu sebagai berikut.

a. Long Haul

Long haul memiliki frekuensi kerja 2-10 GHz dan pada kondisi iklim tiga frekuensi yang normal dapat menempuh hingga rentang 45 km-80 km. Frekuensi yang digunakan yaitu 2, 7, dan 10 GHz.

b. Medium Haul

Medium haul memiliki frekuensi kerja 11-20 GHz dengan panjang hop antara 40 km dan 20 km. Frekuensi yang digunakan adalah 13, 15, dan 18 GHz.

c. Short Haul

Short haul menjangkau jarak paling pendek, dan bekerja pada jangkauan frekuensi tinggi (23-58 GHz). Frekuensi yang digunakan adalah 23, 26, 27, 38, 55, dan 58 GHz.

4. Propagasi Line of Sight (LOS)

Propogasi mempunyai keterbatasan pada jarak pandang dengan ketinggian dari antena dan kelengkungan permukaan bumi sebagai faktor yang paling utama dari propagasi ini. Jarak jangkauannya berkisar 30-50 mil per link tergantung dari bentuk permukaan bumi. Pada kenyataannya, jarak jangkauannya adalah 4/3 dari Line of Sight (untuk K = 4/3) karena adanya faktor atmosfer bumi bagian bawah. Propagasi Line of Sight (LOS) ini bisa disebut juga dengan propagasi gelombang langsung dikarenakan gelombang yang memancar dari antena pemancar berpropagasi menuju antena penerima dan tidak merambat di atas permukaan tanah. Propagasi Line of Sight (LOS) merupakan sistem telekomunikasi masa modern karena menyediakan informasi yang lebih besar dan keandalan yang lebih tinggi.

a. Pathloss

Pathloss merupakan suatu perangkat lunak yang digunakan untuk melakukan RF planning dalam membuat suatu path-link dan link calculation (link budget), baik yang bersifat point to point (antar titik) maupun point to multipoint (banyak titik), sehingga dengan menggunakan software ini mendapatkan hasil yang diinginkan. Pathloss adalah pengurangan kepadatan daya dari sebuah gelombang elektromagnetik dalam analisis medan, lingkungan (perkotaan atau pedesaan, vegetasi, dan dedaunan), jarak antara dan desain link budget dari sistem telekomunikasi. Pathloss juga dipengaruhi oleh kontur pemancar dan penerima, serta tingginya dan lokasi antena.

Pathloss biasanya mencakup kerugian propagasi disebabkan oleh perluasan alami dari gelombang radio depan di ruang bebas (yang biasanya mengambil bentuk sebuah bola yang terus meningkat), penyerapan kerugian (kadang-kadang disebut kerugian penetrasi), ketika sinyal melewati media tidak transparan untuk gelombang elektromagnetik, difraksi kerugian ketika bagian dari gelombang radio depan terhambat dengan adanya kendala dan kerugian yang disebabkan oleh fenomena. Fitur yang terdapat di dalamnya pun bermacam-macam antara lain fitur membuat link profile, kalkulasi perfoma link, analisa reflection dan multipath, optimasi ketinggian antena, administrasi peta digital dalam format raster, administrasi geo-referentiated orthophotos, analisa interferensi, dan impor data melalui format text.

Dalam sebuah link microwave, sinyal terima harus memenuhi syarat LOS (Line of Sight). LOS adalah perambatan radio gelombang mikro dari antena pengirim ke antena penerima dengan jalur transmisi bebas. Pada penerima, sinyal yang diterima tidak hanya berasal dari sinyal LOS tetapi sinyal yang dipantulkan dari permukaan bumi. Sinyal dari beberapa pantulan ini sering disebut dengan multipath. Penerimaan sinyal di penerima memang merupakan sinyal penambahan dari sinyal LOS dan juga sinyal multipath, namun sinyal-sinyal multipath ini justru akan menimbulkan interferensi yang dapat menyebabkan fading atau perubahan gelombang elektromagnetik yang diterima.

b. Perhitungan Link Budget

Salah satu bagian yang paling penting dalam sistem jaringan microwave link adalah link budget. Dalam beberapa tahun terakhir beberapa perangkat lunak yang telah dihasilkan sangat menyederhanakan proses ini. Dalam proses perencanaan link budget ini ada beberapa tahapan.

1) Free Space Loss (FSL)
   Free space loss merupakan nilai pengurangan sinyal yang dikirim selama menempuh jarak propagasi dari stasiun bumi pengirim ke antena penerima yang ada pada satelit, redaman LOS berharga rata-rata sama dengan redaman ruang bebas. Besarnya FSL dapat dihitung dengan persamaan berikut.

   FSL = 92, 45+ 20 log f (GHz) + 20 log D (Km)

   Keterangan:

   FSL = free Space Loss (dB)

   F = frekuensi (Ghz)

   D = jarak antara antena pemancar dan penerima (km)

2) Menentukan Nilai EIRP

Effective Isotropic Radiated Power (EIRP) menunjukkan nilai efektif daya yang dipancarkan antena pemancar. Nilai ini dipengaruhi oleh level keluaran pemancar, kemungkinan rugi-rugi feeder dan gain antena dengan rumus persamaan berikut.

EIRPdBm = Ptx + Gtx - Ltx

Keterangan:

EIRP = EIRP (dBm)

Ptx = daya pancar (dBm)

Gtx = gain antena (dBi)

Ltx = transmitter loss (dB)

3) Menentukan Nilai RSL
Received Signal Level (RSL) merupakan level daya yang diterima oleh receiver. Nilai receiver ini dipengaruhi oleh rugi-rugi jalur dan gain antena penerima. RSL tersebut dapat dihitung dengan menggunakan rumus persamaan berikut.

RSL =IRL + Grx + Lrx

Keterangan:

RSL = Received Signal Level (dBm)

IRL = Isotropic Receved Leve((dBm)

Grx = gain antena (dBi)

Lrx = receiver loss (dB)

4) 4) Gain Antena
Gain antena mengukur kemampuan antena untuk mengirimkan gelombang yang diinginkan ke arah tujuan. Pada antena parabola, efisiensi tidak mencapai 100% karena beberapa daya hilang. Secara komersial, efisiensi antena parabola antara 50% hingga 70%. Besarnya nilai gain dapat dicari menggunakan persamaan berikut.

G = 20 log f+ 20 log d+ 10 log + 10,4

Keterangan:

G = gain atau penguatan antena (dBi)

d = diameter antena (m)

n = efisiensi antena (55%)

f = frekuensi antena (GHz)

5) Fading Margin (FM)
Diperlukan cadangan daya yang digunakan untuk mengatasi fading agar dapat mempertahankan level daya terima di atas level batas ambang (threshold). Cadangan daya tersebut sering disebut dengan fading margin dapat dihitung dengan persamaan berikut.

FM = 30 log D + 10 log (a. b. 2,5. f) + 10 log - 10 logUnAvpath

Tugas 2.12

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri dari 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan implementasi saluran pada microwave link dalam kehidupan sehari-hari!
3. Hasilnya dimasukkan ke dalam table berikut!

No	Tipe	Penggunaan
1	Long Haul	
2	Medium Haul	
3	Short Haul	

4. Gunakan komponen dalam table di atas menjadi bahan diskusi kelompok!
5. Presentasikan hasil diskusi kelompok Anda di depan kelas dan mintalah tanggapan dari kelompok lain!

G. Prinsip Dasar Sistem VSAT IP

VSAT IP merupakan layanan internet berbasis satelit yang dapat melayani kebutuhan komunikasi data mulai dari 2.400 bps hingga 2 Mbps dan dipastikan tidak akan terputus meski berada di lokasi terpencil sekalipun. Layanan ini dapat memenuhi kebutuhan komunikasi data/internet, voice, dan video, sehingga dapat menjadi solusi untuk industri perkebunan, pengeboran minyak, maritim, hingga masyarakat yang tinggal di daerah rural atau 3T (Terluar, Terdepan, dan Tertinggal).

Sebagai pendahuluan mengenai VSAT IP, anda dapat melihat video berikut:

Seperti halnya benda-benda yang menjadi top of mind dan nama merek yang langsung diasosiasikan dengan nama benda, VSAT awalnya adalah merek untuk stasiun bumi kecil yang dipasarkan sekitar tahun 1980 oleh Telecom General, perusahaan telekomunikasi di Amerika Serikat, Telecom General. Lazimnya, VSAT sering dianggap singkatan dari Very Small Aperture Terminal. Dalam terjemahan umumnya, VSAT dapat diartikan sebagai suatu terminal pemancar dan penerima transmisi satelit yang tersebar di banyak lokasi dan terhubung ke hub sentral melalui satelit dengan menggunakan antena parabola berdiameter tertentu. Biasanya diameternya kurang dari 3 meter. Fungsi utama dari VSAT adalah untuk menerima dan mengirim data ke satelit. Satelit berfungsi sebagai penerus sinyal untuk dikirimkan ke titik lainnya di atas bumi. Sebenarnya piringan VSAT tersebut menghadap ke sebuah satelit geostasioner (satelit yang selalu berada di tempat yang sama sejalan dengan perputaran bumi pada sumbunya).

Gambar 2. 17 VSAT IP

1. Sistem Komunikasi Satelit

Satelit adalah benda di angkasa yang bergerak mengelilingi bumi menurut orbit tertentu. Sistem komunikasi satelit dapat dikatakan sebagai sistem komunikasi

dengan menggunakan satelit sebagai repeater. Satelit berfungsi sebagai repeater aktif di mana pada satelit terjadi proses penguatan daya sinyal yang diterima dari bumi dan proses translasi frekuensi untuk kemudian memancarkannya kembali frekuensi yang berbeda ke stasiun bumi penerima.

Jalur pada setiap kanal dari antena penerima ke antena pemancar di dalam satelit disebut sebagai transponder satelit. Selain sebagai penguat sinyal, transponder juga berfungsi sebagai isolasi terhadap kanal RF (Radio Frequency) lainnya. Guna memberikan daya keluaran, transponder juga menggunakan suatu sistem penguat yang disebut TWTA (Travelling Wave Tube Amplifier) atau SSPA (Solid State Power Amplifier). Misalnya satelit BRISAT menggunakan frekuensi C-Band (4-6 GHz). Selain C-Band ada juga Ku-Band. Namun, C-Band lebih tahan terhadap cuaca dibandingkan dengan KU-Band. Satelit ini menggunakan frekuensi yang berbeda antara menerima dan mengirim data. Intinya, frekuensi yang tinggi digunakan untuk uplink (5,925 sampai 6,425 GHz), frekuensi yang lebih rendah digunakan untuk downlink (3,7 sampai 4.2 GHz).

a. Jenis Satelit Menurut Daerah Cakupannya

Jaringan VSAT menggunakan satelit geostasioner, yang memiliki orbit pada bidang ekuator dengan ketinggian ± 35.786 km di atas permukaan bumi. Ditinjau dari daerah cakupannya satelit dibagi menjadi tiga jenis, yaitu sebagai berikut.

1) LEO (Low Earth Orbit)
   Satelit ini mengorbit pada ketinggian 500-1.500 km dari permukaan bumi. Adapun dengan ketinggian ini, satelit dapat digunakan untuk komunikasi suara tanpa menimbulkan delay propagasi dan power yang digunakan juga relatif kecil.
2) MEO (Medium Earth Orbit)
   Satelit ini mengorbit pada ketinggian antara 9.000-20.000 km dari permukaan bumi. Satelit ini memiliki cakupan yang lebih sempit dan memiliki delay yang lebih kecil dibandingkan GEO.
3) GEO (Geosynchronous Earth Orbit)
   Satelit ini mengorbit pada ketinggian ± 36.000 km dari permukaan bumi. Adapun dengan ketinggian tersebut diperlukan waktu 0,25 detik untuk mentransmisikan sinyal. Satelit ini disebut juga Geosynchronous karena waktu yang dibutuhkan satelit untuk mengitari bumi sama dengan waktu bumi berotasi pada porosnya. Jangkauan satelit ini dapat mencapai 1/3 luas permukaan bumi. Kekurangan dari satelit ini adalah membutuhkan power dan delay yang besar untuk mentransmisikan sinyal.

b. Downstream dan Upstream

Downstream adalah istilah yang merujuk kepada kecepatan aliran data dari komputer lain ke komputer lokal melalui sebuah network atau bisa diartikan sebagai kecepatan

aliran data ketika pelanggan sedang melakukan download. Sedangkan upstream adalah istilah yang merujuk kepada kecepatan aliran data dari komputer lokal ke komputer lain yang terhubung melalui sebuah network, atau bisa diartikan sebagai aliran data ketika pelanggan sedang melakukan upload dengan kecepatan maksimum sampai dengan 64 Kbps.

c. Intermediate Frequency (IF) dan Radio Frequency (RF)

Intermediate Frequency (IF) pada stasiun hub terdiri dari Modulator/Transmit Master Communication Controller (mod/TMCC). Sebuah mod/TMCC diperlukan untuk setiap kanal outlink sedangkan Demod/RMCC diperlukan untuk setiap kanal returnlin. Adapun pada Radio Frequency (RF), selain antena terdapat Low Noise Amplifier (LNA) yang dipasang di antena hub stasiun, berfungsi untuk mengubah sinyal RF menjadi IF (Down Converter) untuk diproses oleh susbsistem IF. Selain itu pada susbsistem RF terdapat Up Converter (UC) yang mengubah sinyal IF menjadi sinyal RF dan High Power Amplifier (HPA) untuk memperkuat sinyal RF sehinga dapat di transmisikan. Dilihat dari penggunaanya, LNA merupakan perangkat penerima (downlink), sedangkan UC dan HPA merupakan perangkat pengirim (uplink).

Tugas 2.13

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan jenis-jenis satelit komunikasi yang pernah digunakan di Indonesia. Informasi yang diperoleh dimasukkan seperti pada table berikut!

No	Nama Satelit Komunikasi	Tahun Penggunaan	Bentuk Penggunaan

2. Rangkumlah hasil penelusuran Anda!
3. Kumpulkan hasilnya pada guru untuk diberi penilaian!

2. Berbagai Tipe VSAT

Fungsi utama dari VSAT adalah untuk menerima dan mengirim data ke satelit. Satelit berfungsi sebagai penerus sinyal untuk dikirimkan ke titik lainnya di atas bumi. Sebenarnya piringan VSAT tersebut menghadap ke sebuah satelit geostasioner. Satelit geostasioner selalu berada di tempat yang sama sejalan dengan perputaran bumi

pada sumbunya yang dimungkinkan, karena mengorbit pada titik yang sama di atas permukaan bumi dan mengikuti perputaran bumi pada sumbunya.

Sesuai dengan cara kerja frekuensi yang digunakannya, teknologi VSAT secara garis besar dapat dibagi menjadi tiga yaitu frekuensi satu arah, frekuensi Split-Two-Ways (sinyal feedback dikirimkan bukan melalui satelit), dan frekuensi dua arah. Implementasi frekuensi dua arah ini biasanya terbagi menjadi dua tipe: Star VSAT, di mana gelombang data harus melewati sebuah hub dan kedua adalah Mesh VSAT, di mana gelombang data langsung dipancarkan sesama infrastruktur VSAT. Jika dilihat berdasarkan spektrum frekuensi yang digunakan, VSAT bisa digolongkan menjadi tiga jenis yaitu VSAT C-Band, VSAT Ku-Band, dan VSAT Ka-Band.

a. VSAT C-Band banyak digunakan untuk kepentingan operasional perusahaan-perusahaan atau organisasi-organisasi besar mengingat kualitas spektrum VSAT C-Band yang relatif lebih tahan terhadap cuaca sehingga koneksinya bisa lebih stabil. Kekurangan VSAT C-Band adalah penggunaan antena atau piringan satelit yang relatif lebih besar jika dibandingkan dengan spektrum VSAT lainnya.
b. VSAT dengan spektrum frekuensi Ku-Band penggunaannya lebih luas, kerap juga digunakan untuk para penyedia ISP dan industri telekomunikasi.
c. VSAT Ka-Band banyak digunakan dari sisi terminal aplikasi pelanggan yang diterapkan oleh beberapa perusahaan dengan proyek khusus.
d. Sebenarnya ada satu jenis lagi spektrum frekuensi VSAT yang saat ini digunakan, yaitu VSAT X-Band. Tapi spektrum frekuensi VSAT ini eksklusif digunakan hanya untuk kepentingan pertahanan dan keamanan di negara-negara maju.

Adapun aplikasi jaringan VSAT antara lain sebagai berikut.

Tabel 2. 12 Alokasi Jaringan VSAT

No.	Aplikasi Jaringan	Contoh
1.	Jaringan VSAT 1 arah	a. Pelatihan/pendidikan jarak jauh. b. Pemancar luasan berita dan harga saham. c. Pengenalan produk baru untuk daerah tersebar dan sulit dijangkau. d. Penyebaran analisis keuangan. e. Penyebaran musik atau video untuk jaringan pertokoan atau fasilitas umum. f. Periklanan jarak jauh atau iklan elektronik di jaringan pertokoan. g. Update data pemasaran/pendistribusian: barang, harga dan lain-lain.
2.	Jaringan VSAT 2 arah	a. Electronic funds transfer (Visa, Master) di tempat penjualan.

		b. Enkuiri basis data. c. Internet. d. Kendali dan telemetri proses sistem terdistribusi jarak jauh. e. Kendali stok dan pemantauan penjualan. f. Komunikasi suara. g. Layanan darurat. h. Satelit News Gathering (pelaporan langsung dari tempat kejadian). i. Sistem pemesanan (tiket, hotel dan lain-lain). j. Transaksi bank atau ATM. k. Transaksi interaksi komputer. l. Transfer data medis. m. Video conference

3. Prinsip Dasar VSAT

VSAT (Very Small Aperture Terminal) pada stasiun bumi yang digunakan untuk menerima dan mengirim data, suara, dan gambar dari dan ke satelit. Disebut very small, karena stasiun ini menggunakan antena dengan ukuran yang sangat kecil, diameter piringannya antara 80 cm sampai 2,4 m. Dengan ukurannya yang kecil inilah, VSAT dapat dibawa-bawa dan diletakkan di mana saja, seperti di dalam hutan, di tengah laut, atau di atap mobil.

Ukuran yang kecil serta kemampuan menerima dan mengirim data ke satelit. membuat VSAT menjadi solusi ampuh sarana telekomunikasi untuk daerah-daerah terpencil yang belum terjangkau jaringan terestrial seperti kabel tembaga, serat optik, dan seluler. Adapun selain itu, di saat-saat darurat seperti bencana alam, ketika jaringan terestrial biasanya ikut mengalami gangguan, komunikasi data via satelit dapat menjadi solusi instan yang andal.

Apabila sebagian besar pengguna internet di tanah air tidak dapat mengakses server di luar negeri, maka ISP yang menggunakan komunikasi data via satelit sebagai cadangan masih dapat melayani para pelanggannya.

4. Komponen VSAT

Istilah VSAT dikenal sebagai Sistem Komunikasi Stasiun Bumi Mikro (SKSBM) secara sederhana dapat diartikan sebagai beberapa buah stasiun bumi dengan diameter antena kecil (1,8-3.8 m) yang letaknya secara geografis berjauhan dan mempunyai stasiun bumi utama (hub station) sebagai pengawas dan pengatur jaringan. Perangkat jaringan komunikasi VSAT yang mudah dan cepat dipasang tidak hanya dapat memberikan transmisi data yang berkualitas tinggi tetapi juga fleksibel dalam

pengembangan jaringan. Digunakannya satelit geo-stasioner menyebabkan jaringan komunikasi VSAT mempunyai daerah jangkauan yang luas dan tidak perlu melacak arah pergerakan satelit sehingga biaya operasional dan perawatan menjadi rendah.

a. Stasiun Hub

Stasiun hub berfungsi untuk mengontrol semua network di sisi stasiun hub maupun di-remote. Sinyal outroute dari hub menuju remote, sedangkan sinyal inroute dari arah remote menuju hub. Stasiun hub mempunyai satu outroute dan beberapa inroute dengan besarnya bandwidth tidak sama atau asimetris. Penentuan besarnya outroute dan jumlah inroute tergantung dari kebutuhan pelanggan. Stasiun hub terdiri dari beberapa bagian berikut.

1) Antena
   Antena berfungsi untuk memperkuat sinyal yang diterima dari arah satelit dan memperkuat sinyal yang akan dipancarkan ke arah satelit. Makin besar antena yang digunakan makin baik, karena akan mengoptimalkan sinyal yang diterima dari remote sehingga power transmit yang dibutuhkan dari remote lebih kecil.
2) Low Noise Amplifier (LNA)
   Low Noise Amplifier (LNA) terpasang pada bagian receive berfungsi untuk memperkuat sinyal yang masih lemah dari satelit.
3) Up Converter
   Up converter terpasang pada bagian transmit berfungsi untuk merubah frekuensi IF menjadi frekuensi RF dan memperkuat sinyal yang akan dipancarkan ke HPA/SSPA.
4) Down Converter
   Down converter terpasang pada bagian receive berfungsi untuk mengubah frekuensi RF menjadi frekuensi IF dan memperkuat sinyal yang diterima dari Low Noise Amplifier (LNA).
5) High Power Amplifier (HPA)
   High Power Amplifier (HPA) terpasang pada bagian transmit berfungsi untuk memperkuat sinyal yang akan dipancarkan ke arah satelit
6) Modem (Modulasi Demodulasi)
   Modem berfungsi menumpangkan sinyal digital binary ke bit sinyal carrier IF dalam bentuk perubahan sinyal carrier IF pada bagian transmit dan menumpahkan bit sinyal digital binary dari carrier IF pada bagian receive.
7) Network Operational Controller (NOC)
   Network Operational Controller (NOC) merupakan interface antara enterprice network dengan stasiun remote dan berfungsi mengontrol semua network di sisi hub dan remote. Network Operational Controller (NOC) juga memonitor kondisi dari semua remote.

b. Stasiun Remote

Stasiun remote merupakan jaringan VSAT yang berfungsi sebagai jaringan LAN pada sisi pelanggan. Modem mempunyai interface ethernet yang dapat langsung dihubungkan dengan jaringan pelanggan tanpa menggunakan router. Perangkat stasiun remote sebagai berikut.

1) Antena
   Antena pada stasiun remote berfungsi untuk memperkuat sinyal yang diterima dari satelit dan memperkuat sinyal yang akan dipancarkan ke arah satelit. Sinyal yang berasal dari BUC dipancarkan oleh feedhorn yang ditempatkan di titik fokus dari sebuah reflektor, untuk kemudian dipantulkan ke arah satelit oleh reflektor. Demikian pula sinyal yang diterima dari satelit dikumpulkan oleh feedhorn untuk kemudian disalurkan ke LNB. Stasiun remote menggunakan antena 1,8 meter jenis off-set
2) Feedhorn
   Feedhorn berfungsi untuk memfokuskan sinyal kearah reflektor sebelum dipancarkan kearah satelit, mengumpulkan sinyal yang diterima dari satelit kemudian disalurkan kearah LNB dan sebagai pemisah bagian transmit dan receive.
3) Low Noise Block (LNB)
   LNB terpasang pada bagian receive (sat in) berfungsi untuk memperkuat sinyal frekuensi RF C-band yang diterima dari arah satelit dan mengubah frekuensi RF C-Band menjadi frekuensi L-band ke arah modem. Catuan power LNB berasal dari modem sekitar 13V DC.
4) Block Up Converter (BUC)
   Block Up Converter (BUC) terpasang pada bagian transmit (sat out) berfungsi untuk mengubah frekuensi RF L-band menjafi frekuensi RF C-band dan memperkuat sinyal yang akan dipancarkan kearah satelit. Catuan power BUC berasal dari modem sekitar 18-21V DC.
5) Modem
   Modem berfungsi untuk mengubah sinyal RF menjadi data. Pada sistem VSAT IP data yang dikeluarkan bukan lagi raw-data tetapi sudah dalam bentuk paket data IP. Demikian pula sebaliknya, paket data IP yang datang diubah oleh modem ke dalam bentuk sinyal RF. Modem juga berfungsi sebagai router karena dapat terhubung langsung dengan jaringan pelanggan.
6) Kabel Coaxial
   Kabel coaxial berfungsi untuk menyalurkan sinyal RF dalam frekuensi L-band, baik dari arah modem ke BUC, maupun dari arah LNB ke modem. Jenis kabel coaxial yang digunakan kabel RG-6 dan kabel RG-8 dengan panjang kabel maksimal 30 meter.
7) Multiplexer

Multiplexer berfungsi untuk menggabungkan dan memisahkan sinyal TX dan RX, digunakan untuk modem jenis DW2000.

8) Kabel Grounding
Kabel grounding berfungsi untuk menghubungkan semua grounding perangkat dengan grounding. Grounding berfungsi sebagai tempat pembuangan lonjakan tegangan. Makin kecil nilai grounding makin bagus.

5. Topologi Jaringan VSAT

Topologi adalah suatu aturan bagaimana menghubungkan komputer (node) satu sama lain secara fisik dan pola penghubungan antara komponen-komponen yang berkomunikasi melalui media/peralatan jaringan, seperti server, workstastion, hub atau switch, dan pengabelannya (media transmisi data). Topologi juga dapat diartikan sebagai cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan.

Topologi jaringan VSAT dapat dibagi menjadi dua kategori besar, yaitu topologi fisik dan topologi kerja jaringan yang sesungguhnya. Topologi fisik berpusat pada letak dan posisi jaringan, sehingga tiap terminal dibedakan menurut letaknya saja. Sedangkan pada topologi kerja jaringan, tiap terminal di bedakan menurut kemampuan akses setiap terminalnya.

Topologi yang umum digunakan saat ini antara lain sebagai berikut.

a. Jaringan Jala (Mesh)

Pada jaringan ini tiap-tiap stasiun VSAT dapat saling berhubungan langsung melalui satelit, sistem ini dapat juga diintegraskan dengan sebuah stasiun hub yang berfungi untuk mengontrol manajemen jaringan. Jaringan mesh memiliki propagasi delay yang lebih kecil dibandingkan jaringan star, yaitu hanya 0,5 detik untuk single hop dan 0,5 detik untuk double hop. Jaringan mesh digunakan untuk komunikasi suara ataupun data.

b. Jaringan Bintang (Star)

Stasiun hub digunakan sebagai stasiun pusat yang terhubung dengan seluruh stasiun pusat. Hubungan (link) yang berasal dari stasiun hub ke stasiun VSAT disebut outbond, sedangkan link dari VSAT menuju stasiun hub disebut inbound. Jaringan bintang dapat digunakan untuk komunikasi satu arah (one-way) ataupun dua arah (two-way)

1) Jaringan Bintang Satu Arah
Jaringan bintang satu arah umumnya digunakan oleh perusahaan yang memiliki cabang-cabang yang tersebar secara geografis. Stasiun hub hanya berfungsi untuk mengirimkan informasi ke seluruh stasiun VSAT (broadcast) contoh aplikasi jaringan ini, yaitu penyiaran (broadcast) TV, pelatihan jarak jauh, dan lain-lain.
2) Jaringan Bintang Dua Arah

Jaringan bintang dua arah memungkinkan stasiun hub dapat mengirimkan dan menerima informasi dari stasiun VSAT. Tipe ini digunakan untuk traffic yang besar dan bersifat interaktif. Contoh penerapan jaringan ini antara lain pada transaksi antarbank, ATM (Automatic Teller Machine), e-mail, dan lowrate video conferencing.

6. Metode Akses

Akses antara dua buah node pada suatu jaringan komunikasi nirkabel dapat dibagi menjadi beberapa metode sebagai berikut.

a. Akses yang Selalu Tersedia (Dedicated Access)

Akses yang selalu tersedia di mana pendudukan suatu alokasi frekuensi selalu terjadi walaupun tidak ada aktivitas yang menghubungkan antara dua node. Misalnya SCPC dan microwave link.

b. Akses Menurut Kebutuhan (Demand Access)

Akses menurut kebutuhan adalah optimalisasi kebutuhan suatu alokasi frekuensi di mana frekuensi yang tersedia digunakan bersama oleh lebih dari sekedar dua node yang berhubungan, sebagai contoh: FDMA, TDMA, CDMA, point to multipoint microwave (Wi-Fi, Wimax, dan lain-lain).

1) FDMA (Frequency Division Multiple Access)
   FDMA merupakan teknologi akses di mana setiap user akan mendapatkan alokasi frekuensi tertentu selama user tersebut melakukan aktivitas dan ketika user tidak melakukan aktivitas maka frekuensi tersebut akan dialokasikan ke user lain yang membutuhkan.
2) TDMA (Time Division Multiple Access)
   TDMA merupakan teknologi untuk berbagi suatu kanal pada suatu media telekomunikasi biasanya RF, di mana setiap pengguna dibagi berdasarkan alokasi waktu. Keuntungan dari TDMA adalah penggunaan ulang frekuensi menjadi lebih efisien, tetapi juga ada kerugian dikarenakan ada kemungkinan informasi dari pengguna bertabrakan sehingga diperlukan pengiriman ulang, kerugian ini sangat berpengaruh pada komunikasi satelit yang mempunyai jarak 36.000 km dari bumi.
3) MF-TDMA (Multi Frequency Time Division Multiple Access)
   MF-TDMA (Multi Frequency Time Division Multiple Access) merupakan pengembangan dari TDMA di mana pengguna selain menggunakan alokasi frekuensi yang sama berdasarkan waktu, paket informasi dari pengguna juga bisa dilewatkan pada kanal frekuensi yang lain untuk memininalisasi kemungkinan paket data bertabrakan. Adapun dengan MF-TDMA kemungkinan tabrakan informasi bisa diminimalisasi dibandingkan dengan TDMA biasa sehingga sistem komunikasi satelit yang mempunyai delay yang tinggi banyak menerapkan sistem

MF-TDMA. Kelemahan dari MF-TDMA dibandingkan TDMA adalah pada saat terjadi perpindahan frekuensi (frekuensi hoping) akan terjadi delay tambahan yang tidak ada pada sistem TDMA.

4) RTDMA (Random Time Division Multiple Access)
   RTDMA (Random Time Division Multiple Access) merupakan pengembangan dari TDMA di mana pengguna dapat mengirimkan paket data secara acak/random, mencari slot yang kosong. Sistem "iDirect" ini menerapkan metode RTDMA untuk melakukan komunikasi datanya dengan sebuah hub dan banyak remote yang membentuk topologi jaringan star. Mekanisme komunikasinya adalah beberapa remote mengirikan data via satelit ke hub sedangkan antar-remote tidak bisa berkomunikasi.
5) TDM (Time Division Multiplexing)
   Konsep dari VSAT IP ini adalah menggunakan kombinasi dari Time Division Multiplexing (TDM) dan Time Division Multiple Access (TDMA) untuk membangun arsitektur jaringan dengan topologi star. Sedangkan pembagian datanya dengan menggunakan paket address melalui pengamatan IP di modem dan PC client.

7. Cara Kerja VSAT

Secara sederhana, sebuah stasiun bumi kecil atau VSAT hanya menerima dan mengirimkan data ke satelit komunikasi, berbeda dengan antena parabola yang digunakan hanya untuk menerima siaran televisi via satelit. Selanjutnya, data tersebut dikirimkan ke sebuah stasiun bumi lainnya. Tipe komunikasi seperti ini dikenal dengan nama point to point. Tapi, sebuah stasiun bumi juga dapat mengirimkan data satelit untuk diteruskan ke beberapa stasiun bumi lainnya sekaligus. Tipe seperti ini dikenal dengan nama point to multipoint.

Sebuah sistem VSAT bekerja dengan adanya satelit dan stasiun bumi. Satelit yang digunakan oleh VSAT adalah satelit geostasioner. Satelit ini selalu berada di tempat yang sama, sejalan dengan perputaran bumi pada sumbunya. Sampai saat ini, Indonesia telah meluncurkan lima satelit geostasioner, yakni Satelit Palapa-A, Satelit Palapa-B, Satelit Palapa-C, Satelit Telkom-1, dan Satelit Telkom-2.

VSAT menggunakan komunikasi Radio Frekuensi (RF) dua arah yaitu uplink dan downlink. RF yang dipancarkan oleh stasiun VSAT ke satelit (uplink) dan sebaliknya RF yang dipancarkan oleh satelit ke stasiun VSAT (downlink). Antena VSAT memancarkan sinyal RF ke satelit sebesar 5,925 GHz sampai dengan 6,425 GHz. Sedangkan sinyal RF yang lebih rendah diterima antena VSAT dari satelit sebesar 3,7 GHz sampai dengan 4,2 GHz.

Pendapat umum mengatakan bahwa komunikasi data dengan satelit adalah yang tercepat. Padahal, pada kenyataannya tidaklah demikian. Waktu yang dibutuhkan

dari satu titik di atas bumi ke titik lainnya melalui satelit adalah sekitar 700 milisecond, sementara leased line hanya butuh waktu sekitar 40 milisecond.

Hal ini disebabkan oleh jarak yang harus ditempuh oleh data, yaitu dari bumi ke satelit dan kembali ke bumi. Satelit geo-stasioner sendiri berketinggian sekitar 36.000 kilometer di atas permukaan bumi. Kekurangan lainnya adalah VSAT sangat rentan terhadap perubahan cuaca. Di negeri dengan curah hujan yang tinggi seperti Indonesia, komunikasi VSAT dapat mengalami gangguan atau penurunan kinerja.

Tugas 2.14

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan VSAT berdasarkan spektrum frekuensi yang digunakan dalam kehidupan sehari-hari!
3. Hasilnya dimasukkan ke dalam table berikut!

No	Jenis VSAT	Penggunaan
1	VSAT C-Band	
2	VSAT Ku-Band	
3	VSAT Ka-Band	

4. Gunakan jawaban dalam table di atas menjadi bahan diskusi kelompok!
5. Presentasikan hasil diskusi kelompok di depan kelas dan mintalah tanggapan dari kelompok lain!

8. VSAT di Indonesia

VSAT pertama kali di Indonesia digunakan untuk kalangan perbankan, sekitar tahun 1989, saat banyak bank yang membutuhkan sistem komunikasi online untuk operasional unit ATM (Automated Teller Machine). Kalangan perbankan juga memanfaatkan VSAT untuk akses komunikasi operasional kantor cabang dengan kantor pusat.

Satelit komersial VSAT pertama, sekitar tahun 1980-an, menggunakan sistem yang hanya menerima frekuensi C-band yang menggunakan teknologi spektrum lebar. Lebih dari 30.000 unit dengan antena 60 cm berhasil terjual saat itu. Mekanisme frekuensi C dua arah dikembangkan pada rentang waktu 1984-1985 dan berhasil terjual sebanyak 10.000 unit dengan menggunakan topologi star. Selain untuk sektor perbankan, teknologi VSAT ini juga banyak digunakan oleh industri eksplorasi dan pengeboran minyak; yang dikembangkan dengan menggunakan frekuensi Ku-band pada awal kemunculannya di awal 80-an. VSAT dengan frekuensi Ku-band ini akhirnya dikembangkan juga untuk keperluan kalangan perusahaan (enterprise).

Implementasi di kalangan enterprise ini lah yang memicu pesat perkembangan teknologi VSAT. Pada tahun 2005, frekuensi Ka-band mulai diaplikasikan untuk penggunaan teknologi VSAT bagi konsumen; dan sampai saat ini jutaan konsumen, khususnya di Amerika Serikat dan Eropa, telah menggunakan teknologi VSAT berfrekuensi Ka-Band untuk terhubung ke internet. Layanan VSAT juga saat ini merupakan salah satu solusi produk yang ditawarkan oleh Link Net, dengan keunggulan satelit yang dapat difokuskan di wilayah tertentu dan fungsi multi satelit yang dapat beroperasi serempak.

H. Prinsip Dasar Sistem Optik

Komunikasi fiber optik telah memberikan dampak yang besar terhadap berbagai segi pengiriman data informasi, mulai dari lingkup Local Area Networks (LAN) sampai telekomunikasi antarbenua. Fiber optik sebagai suatu media transmisi yang pemakaiannya sedang berkembang pesat. Hal ini karena media fiber optik memiliki keunggulan yang signifikan dibanding media transmisi kawat konvensional. Secara umum komunikasi fiber optik diawali dengan data yang akan dikirimkan dapat berupa analog atau digital. Dalam sistem pengiriman data dalam sistem fiber optik maka data berasal dari elektrik akan diubah dahulu ke optik oleh sumber cahaya berupa LED. Kemudian disambungkan dengan splices atau konektor dari fiber satu ke yang lain dan diterima oleh photodetector bisa berupa PIN/APD (Avalance Photodioda) yang akan mengubah dari optik ke elektrik selanjutnya akan diubah ke data semula.

Gambar 2. 18 Jaringan Komputer

1. Karakteristik Kabel Fiber Optik

Secara umum, beberapa karakteristik kabel fiber optik antara lain kecepatan dan keluaran 100 Mbps, biaya rata-rata per node cukup mahal, media, dan ukuran konektor kecil, serta panjang kabel maksimal yang diizinkan yaitu sepanjang 2 km. Membuat sebuah jaringan memerlukan media transmisi (yaitu media yang

menghubungkan antara pengirim dan penerima informasi/data. Media transmisi dibagi menjadi dua yaitu terarah (guided/wireline) dan tidak terarah (unguided/wireless) atau nirkabel. Media transmisi terarah merupakan gelombang elektromagnetik yang dipandu perambatan melalui udara, ruang hampa dan air laut. Beberapa karakteristik kabel secara fisik, sedangkan media transmisi elektromagnetik tanpa dipandu misalnya perambatan melalui udara, ruang hampa dan air laut. Beberapa karakteristik kabel serat optik secara khusus dapat dilihat pada tabel berikut.

Tabel 2. 13 Karakteristik Kabel Serat Optik

No.	Karakteristik	Keterangan
1.	Ukuran kecil	Diameter luar serat optik berkisar antara 100-250 μm. Diameter maksimum setelah dilapisi/dibungkus dengan plastik/nilon sebagai jaket menjadi ± 1 mm. Ukuran ini masih sangat kecil dibandingkan dengan konduktor kabel coaxial (1-10mm).
2.	Ringan	Dibandingkan dengan kabel transmisi biasa (spesifigravity 9,8), specifigravity bahan silika sebagai serat optik yaitu 2,2, sehingga beratnya menjadi 1/2-1/3 berat kabel transmisi biasa.
3.	Lentur	Umumnya serat optik tidak akan patah bila dilengkungkan dengan radius 5 mm. Oleh karena itu, kabel serat optik memiliki kelenturan yang sama dengan kabel transmisi biasa, sehingga teknis pemasangannya tidak jauh berbeda dengan teknik pemasangan kabel biasa.
4.	Tidak berkarat	Bahan silika sebagai bahan dasar serat optik memiliki sifat kimia yang sangat stabil, sehingga tidak mungkin berkarat.
5.	Rugi-rugi rendah	Serat optik dengan bahan silika memiliki rugi-rugi transmisi rendah, berkisar 2-8 dB/km dengan panjang gelombang 830 nm. Dibandingkan dengan kabel coaxial yang memiliki rugi-rugi transmisi sebesar 19 dB/km pada frekuensi 60 MHz.
6.	Kapasitas tinggi	Kapasitas dalam menyalurkan informasi per cross section area sangat besar, contohnya kapasitas penyaluran per cross section area 100x dibandingkan dengan multipair cable dan 10x dibandingkan dengan kabel coaxial.
7.	Bebas induksi	Serat optik menggunakan bahan dasar silika yang merupakan bahan dielektrik yang sangat baik dan kebal terhadap induksi elektromagnet dan juga terhadap kilat/petir.

8.	Cross talk rendah	Kemungkinan terjadinya kebocoran sinar antar serat optik sangat kecil, demikian pula kebocoran akibat masuknya sinar dari luar kemudian ikut merambat dalam serat optik.
9.	Tahan temperatur tinggi	Bahan silika memiliki titik leleh ± 1.900° C, ideal digunakan pada daerah yang rawan terhadap temperatur tinggi.
10.	Tidak menimbulkan bunga api	Pada titik sambung tidak mungkin terjadi bunga api (discharge), sangat ideal digunakan pada tempat-tempat yang peka terhadap ledakan/kebakaran.
11.	Tidak dapat dicabangkan	Serat optik memiliki ukuran sangat kecil/sangat tipis sehingga sulit bahkan tidak mungkin untuk dicabangkan.
12.	Bahan silika	Serat optik menggunakan bahan silika yang tidak mengandung unsur logam, kecuali pelapis pelindung pada kabel fiber optik untuk komunikasi kabel laut dan sebagai lewatnya arus DC untuk mencatu tegangan pada kumpulan repeater di bawah laut.
13.	Memiliki daya peregangan	Meskipun rapuh, masih memiliki daya peregangan kurang lebih sebesar 5% untuk menghindarkan kerusakan serat optik pada waktu pemasangan/penarikan, maka pada waktu disusun menjadi kabel optik diberi penguat.

Di samping itu, beberapa karakteristik kabel jaringan fiber optik secara umum dapat diklasifikasikan sebagai berikut.

a. Bagian dalam kabel jaringan fiber optik terdiri dari inti yang terbuat dari serat kaca dan diselubungi oleh beberapa lapisan yang bersifat sebagai pelindung pada setiap lapisan dengan fungsi masing-masing.
b. Konektor yang umum digunakan untuk kabel jaringan fiber optik adalah konektor ST. Tetapi di masa sekarang konektor tersebut telah digantikan konektor SC sebagai pasangan kabel jaringan fiber optik.
c. Kecepatan transfer data yang mampu dilakukan kabel fiber optik minimal 100 Mbps bahkan mampu mencapai 1.000 Mbps.
d. Biaya rata-rata per node cukup mahal.
e. Diameter kabel jaringan fiber optik dan dan ukuran konektornya relatif kecil sehingga fleksibel dalam proses instalasi.
f. Panjang kabel jaringan fiber optik sangat panjang hingga mencapai 2 km hingga mampu mengalahkan kabel jaringan lainnya seperti coaxial dan twisted pair.
g. Sebagai kabel yang dibuat dengan teknologi modern, kabel jaringan fiber optik punya sederet keunggulan jika dibandingkan dengan kabel jaringan lainnya seperti kabel coaxial ataupun kabel twisted pair.

a. Kelebihan Kabel Fiber Optik

Kelebihan kabel jaringan fiber optik antara lain sebagai berikut.

1) Kabel jaringan fiber optik dapat beroperasi dengan kecepatan yang sangat tinggi dalam membawa informasi atau data, bahkan lebih tinggi dibanding kabel jaringan coaxial ataupun kabel twisted pair. Kecepatan transfer datanya bahkan dapat mencapai 1.000 Mbps.
2) Bandwidth kabel jaringan fiber optik tidak perlu diragukan lagi karena mampu membawa paket-paket dengan kapasitas besar hingga 1 Gigabit per detik.
3) Kabel jaringan fiber optik dapat mengirim sinyal lebih jauh dibanding kabel jaringan jenis lainnya, bahkan tanpa memerlukan perangkat penguat sinyal seperti repeater atau lainnya. Kalaupun dibutuhkan, penguat sinyal tidak perlu dipasang setiap 5 km seperti kabel-kabel jaringan lainnya, melainkan cukup dipasang setiap 20 km saja.
4) Material yang dipakai untuk membuat kabel jaringan fiber optik memiliki keunggulan untuk bisa bertahan pada banyak gangguan seperti kelembapan udara dan cahaya (panas). Dengan begitu maka dapat disimpulkan bahwa kabel fiber optik relatif awet karena tidak gampang rusak.
5) Kemampuan kabel jaringan fiber optik yang tahan lama dan tidak gampang rusak membuatnya jadi lebih efisien dibanding kabel jaringan lainnya, karena biaya perawatan pun jadi kian murah.
6) Tak berbeda jauh dengan kabel jaringan STP, kabel jaringan fiber optik juga kuat terhadap interferensi elektromagnetik yang berasal dari sekitar kabel.
7) Kabel jaringan fiber optik terdiri dari berbagai macam jenis yang dapat menjadi opsi untuk menyesuaikan dengan lokasi instalasinya. Mulai dari instalasi di dalam gedung, di bawah tanah hingga di dalam air, semuanya tersedia dengan kriteria dan karakteristik yang berbeda-beda.
8) Oleh karena bukan mengirim sinyal listrik melainkan gelombang cahaya, maka kabel jaringan fiber optik mampu mengatasi masalah gangguan gelombang frekuensi bahan elektrik. Dengan bagitu maka kabel jaringan jenis ini sangat ideal untuk digunakan pada kawasan yang dikelilingi gelombang frekuensi cukup tinggi.
9) Diameter kabel jaringan fiber optik yang relatif kecil dan tipis, ditambah lagi dengan bobotnya yang ringan membuat proses instalasi kabel fiber optik relatif mudah karena bersifat fleksibel.
10) Berbeda dengan kabel jaringan lainnya yang berpotensi menyebabkan terjadinya korsleting atau kebakaran, khusus pada kabel fiber optik hal itu tidak akan terjadi karena menggunakan bahan dasar serat kaca yang aman dan tidak mudah terbakar karena tidak mengalirkan listrik.

11) Berbeda dengan kabel jaringan UTP dan STP yang masih menimbulkan kemungkinan terjadinya penyadapan, hal ini tidak berlaku pada kabel jaringan fiber optik karena dapat meneruskan data tanpa ada distorsi atau gangguan.
12) Kabel jaringan fiber optik mudah di-upgrade bahkan tanpa perlu mengubah sistem kabel yang ada.

b. Kekurangan Kabel Fiber Optik

Kekurangan kabel jaringan fiber optik antara lain sebagai berikut.

1) Harga kabel jaringan fiber optik masih terlalu mahal, terutama jika dibandingkan dengan kabel jaringan lainnya seperti kabel UTP yang terkenal murah meriah.
2) Dalam proses instalasi kabel jaringan fiber optik diperlukan beberapa alat khusus berupa perangkat elektronik yang untuk saat ini memang masih sangat mahal. Alhasil tidak semua orang bisa ataupun mau menggunakan kabel ini sebagai media pendukung dalam instalasi sebuah jaringan komputer.
3) Dalam proses pengiriman sinyal, karena harus dilakukan perubahan sinyal listrik ke sinyal optik terlebih dahulu maka kabel jaringan fiber optik menuntut adanya sumber cahaya yang kuat untuk melakukan persinyalan seperti alat pembangkit listrik eksternal.
4) Jika rusak, perbaikan instalasi kabel jaringan fiber optik yang kompleks memerlukan tenaga yang ahli di bidang ini.
5) Kabel jaringan fiber optik ditakutkan bisa menyerap hidrogen sehingga dapat menyebabkan loss data.
6) Mengingat kabel jaringan fiber optik menggunakan gelombang cahaya untuk mentransmisikan data, maka kabel jaringan jenis ini tidak dapat diinstal dalam jalur yang berbelok secara tajam atau menyudut. Jika terpaksa harus berbelok, maka harus dibuat belokan yang melengkung.

2. Kapasitas Kabel, Kode Warna dan Pelabelan Kabel Fiber Optik

Serat optik sebagai salah satu saluran trasmisi atau sejenis kabel terbuat dari kaca digunakan untuk mentrasmisikan sinyal cahaya dari satu tempat ke tempat lain. Dalam aplikasinya kabel serat optik biasanya diselubungi oleh lapisan resin disebut jaket yang berbahan plastik.Lapisan ini dapat menambah kekuatan untuk kabel serat optik, walaupun tidak memberikan peningkatan terhadap sifat gelombang pandu optik pada kabel tersebut. Namun lapisan resin ini dapat menyerap cahaya dan mencegah kemungkinan terjadinya kebocoran cahaya yang keluar dari selubung inti. Serta hal ini dapat juga mengurangi cakap silang (cross talk) yang mungkin terjadi.

a. Kapasitas Kabel Fiber Optik

Jangkauan dan kecepatan koneksi fiber optik yang jauh lebih unggul menjadi pilihan Utama Internet Service Provider (ISP) di Indonesia. Penggunaan fiber optik memang bukan tanpa alasan karena kabel fiber optik mampu memberikan layanan internet

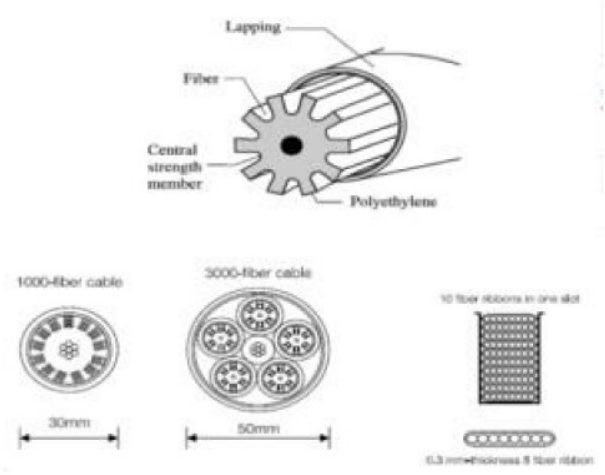
broadband tercepat secara bersamaan. Pengguna bisa mendapatkan layanan jaringan internet, telepon, bahkan video dalam waktu yang bersamaan dengan kecepatan hingga ratusan Mbps. Berbeda dengan kabel metalik, kabel serat optik memiliki ukuran ± 3 cm dan lebih ringan sehingga instalasi kabel serat optik dapat dilakukan melalui beberapa span secara sekaligus. Panjang kabel serat optik dalam satu haspel biasanya mencapai 2 s/d 4 km. Pada saat ini, untuk mengatasi keterbatasan kapasitas kabel tembaga, maka pembangunan junction menggunakan kabel serat optik jenis single mode. Dua jenis kabel fiber optik, yaitu sebagai berikut.

1) Pipa Longgar (Loose Tube)
   Serat optik ditempatkan di dalam pipa longgar (loose tube) yang terbuat dari bahan PBTP (Polybutylene Terepthalete) berisi jeli. Saat ini sebuah kabel optik maksimum memiliki kapasitas 8 loose tube, dengan setiap loose tube berisi 12 serat optik.

Tabel 2. 14 Penampang Kabel Optik Jenis Loose Tube

Cable Type	Diameter (mm)	Weight (kg)
400-fiber cable	24 (25)	0,57 (0,65)
600-fiber cable	24 (25)	0,57 (0,65)
800-fiber cable	30 (31)	0,85 (1,02)
1.000-fiber cable	30 (31)	0,85 (1,02)

2) Alur (Slot)
   Serat optik ditempatkan pada alur (slot) di dalam silinder yang terbuat dari bahan PE (Polyethylene). Salah satu negara yang menggunakan kabel jenis ini adalah Jepang yang telah membuat kabel jenis slot dengan kapasitas 1.000 serat dan 3.000 serat.



Gambar 2. 19 Penampang Kabel Optik Jenis Slot

b. Kode Warna Kabel Fiber Optik

Dalam kabel fiber optik dengan jumlah core yang banyak, maka core tersebut akan dikelompokkan dalam satu selubung (tube), di mana satu tube mengandung 12 warna kabel fiber optik core. Dengan demikian, jika kabel fiber optik 24 core akan memiliki 2 tube dengan masing-masing berisi 12 warna core serat optik yang berbeda. Warna selubung untuk pembungkus kelompok warna core serat optik juga didasarkan pada urutan-urutan tertentu. Jika mengupas kabel fober optik 96 core, maka akan memiliki 8 selubung dengan warna biru, oranye, hijau, cokelat, abu-abu, putih, dan merah.

Jika menentukan warna kabel fiber optik core ke 24 akan berada dalam selubung dan serat optik yang berwarna tosca. Beberapa tipe kabel fiber optik yang digunakan dalam instalasi kabel fiber optik, di antaranya patch cord dan kabel multi-fiber. Guna membedakan penggunaannya telah dibuatkan standar warna pelindung atau jaket pada setiap fiber optik, menggunakan standar warna sebagai berwarna oranye berikut.

1) Patch Cords

   Patch cord merupakan kabel fiber optik yang digunakan untuk kebutuhan panjang yang terbatas dalam menghubungkan 2 titik terminasi jaringan kabel optik. Terdapat dua tipe patch cord yang digunakan, yaitu single fiber optik (simplex) dan double fiber optik (duplex). Guna membedakan penggunaannya telah dibuatkan standar warna.

   Dalam standarisasinya kode warna dari selubung luar (jacket) kabel serat optik jenis patch cord adalah sebagai berikut.

Tabel 2. 15 Warna Jacket pada Kabel FIber Optik Jenis Patch Cord

No.	Warna Jacket	Keterangan
1.	Kuning	Serat optik single mode.
2.	Oranye	Serat optik multimode.
3.	Aqua	Optimal laser 10 giga 50/125 mikrometer serat optik multimode.
4.	Abu-abu	Kode warna serat optik multi mode, sekarang tidak digunakan lagi.
5.	Biru	Kadang masih digunakan dalam model perancangan.

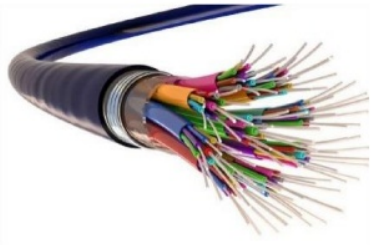
Guna keperluan terminasi, tiap ujung dari patch cord dipasang konektor. Setiap konektor yang dipasang diberi standar warna yang memiliki arti dan penggunaan berbeda-beda seperti terlihat pada tabel berikut.

Tabel 2. 16 Perbedaan Warna Konektor Kabel Patch Cord

No.	Warna Konektor	Arti Warna	Keterangan
1.	Biru	Physical Contact (PC), 0°	Umumnya digunakan pada single mode; beberapa pabrikan menggunakan untuk mengatur polarisasi fiber optik.
2.	Hijau	Angle Polished (APC), 8°	-
3.	Hitam	Physical Contact (PC), 0°	-
4.	Abu-abu, krem	Physical Contact (PC), 0°	Umumnya digunakan pada multimode

2) Kabel Multifiber

Identifikasi yang digunakan dalam Corning cable system adalah menggunakan standar EIA/TIA-598 Optical Fiber Cable Color Coding yang menjelaskan skema identifikasi fiber, jaket fiber, fiber unit dan grup dari fiber unit. Dengan menggunakan standar ini setiap fiber unit dapat diidentifikasi melalui daftar warna yang ada. Oleh sebab itu, setiap kabel fiber optik yang berada di dalam kabel multi-fiber menggunakan kode warna untuk membedakan satu dengan lainnya.



Gambar 2. 20 Multimode Kabel Fiber Optik

Kode warna-warna dapat digunakan untuk menentukan urutan kabel konektor.

Tabel 2. 17 Urutan Kode Warna Kabel Konektor

No.	Fiber Type/Class	Diameter (µm)	Jacket Color
1.	Multimode Ia	50/125	Oranye
2.	Multimode Ia	62,5/125	Abu-abu
3.	Multimode Ia	85/125	Biru
4.	Multimode Ia	100/140	Hijau
5.	Single mode IVa	Semua diameter	Kuning
6.	Single mode IVb	Semua diameter	Merah

c. Pelabelan Kabel Fiber Optik

Secara mendasar, kabel optik harus diberi tanda pengenal yang tertera pada kulit kabel di sepanjang kabel dengan tujuan tidak mudah hilang. Sedangkan tanda pengenal tersebut meliputi nama pabrik pembuat, tahun pembuatan, serta tipe serat, pemakaian, jenis dan struktur penguat kabel optik. Dalam penulisan tanda pengenal kabel optik digunakan kode-kode tertentu, yaitu sebagai berikut

Tabel 2. 18 Kode-kode Tanda Pengenal Kabel Optik

No.	Tanda Pengenal	Keterangan
1.	Tipe serat optik	SM = Single Mode GI = Graded Index SI = Step Index
2.	Jenis kabel optik	LT = Loose Tube SC = Slotted Core TB = Tight Buffered
3.	Struktur penguat	SS = Solid Steel Core WS = Standred Wire Steel GRP = Glass Reinforced Plastik
4.	Pemakaian kabel optik	D = Duct A = Aerial B = Buried S = Submarine I = Indoor
5.	Kode warna serat optik	Biru = Blue Oranye = Orange Hijau = Green Cokelat = Brown Abu-abu = Gray Putih = White Merah = Red Hitam = Black Kuning = Yellow Ungu = Purple Pink = Pink Turquoise = Turquoise
6.	Kode warna tabung (loose tube)	1 = Biru 2 = Oranye 3 = Hijau 4 = Cokelat 5 = Abu-abu

		6 = Putih 7 = Merah 8 = Hitam

3. Karakteristik Jenis Model Multimode

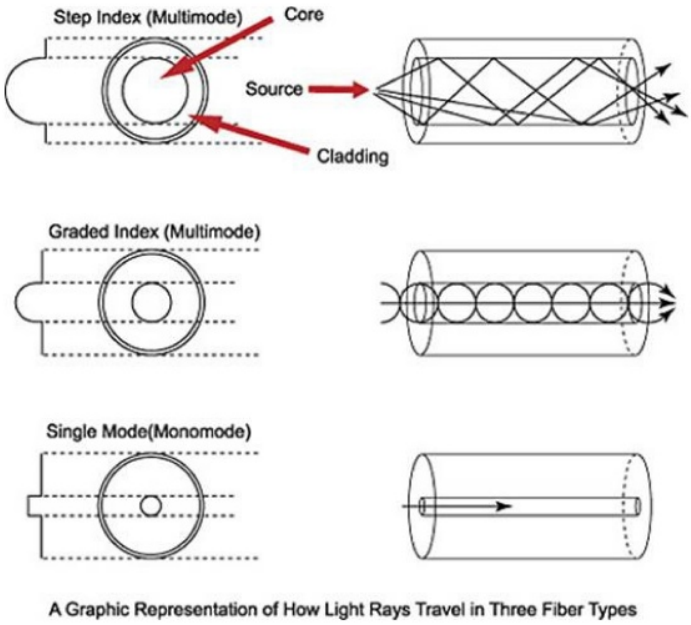
Fiber optik multimode merupakan jenis kabel fiber optik yang memiliki inti atau core yang lebih besar dengan ukuran kira-kira 62,5 mikron. Adapun dengan menggunakan kabel fiber optik berjenis multimode, maka data yang akan ditransmisikan melalui pulsa cahaya akan bekerja dengan cara saling memantul ke dinding-dinding inti atau core. Pulsa cahaya pada multimode fiber optik ini ditembakkan dengan panjang gelombang 850 hingga 1.300 nm.

Tabel 2. 19 Perbandingan Single Mode dan Multimode

Variabel	Single Mode	Multimode
Besar Diameter Core	Lebih kecil (umumnya 8-10 mikrometer)	Lebih besar (50, 62.5, atau 100 mikrometer)
Jenis Cahaya	Laser infrared	LED
Banyak Pancaran Cahaya	Satu	Beberapa
Jenis Pancaran Cahaya	1350 dan 1510nm	850 dan 1300 nm
Jarak Pancaran Cahaya	Lebih jauh (30-100 kilometer)	Lebih pendek (500 meter - 2 kilometer)
Bandwidth	Lebih tinggi (hingga 10 Gbps)	Lebih rendah (hingga 1 Gbps)

4. Karakteristik Jenis Kabel Single Mod

Fiber optik dengan single mode ini umumnya banyak digunakan pada jaringan komputer yang memiliki jarak jangkauan yang jauh, dengan kapasitas bandwidth lebih besar, dan coverage area mencapai puluhan kilometer. Single mode fiber optik memiliki inti atau core lebih kecil dengan posisi lurus tanpa terlilit satu sama lain. Fiber optik dengan single mode dapat mentransmisikan paket data melalui pulsa cahaya dengan secara langsung melewati inti secara lurus tanpa melalui proses memantul ke dinting inti atau core. Pulsa cahaya pada single mode fiber optik ini ditembakkan dengan panjang gelombang hingga 1.310 hingga 1.550 nm.



Gambar 2. 21 Kabel Fiber Optik Jenis Single Mode dan Multimode

5. Konstruksi Kabel Fiber Optik

Perkembangan teknologi serat optik makin pesat sehingga menghasilkan pelemahan (attenuation) kurang dari 20 desibel (dB)/km. Ditunjang dengan lebar jalur (bandwidth) yang makin besar sehingga kemampuan dalam mentransmisikan data menjadi lebih banyak dan cepat dibandingkan penggunaan kabel konvensional. Oleh karena itu, serat optik sangat cocok digunakan terutama dalam aplikasi sistem telekomunikasi. Pada prinsipnya serat optik memantulkan dan membiaskan sejumlah cahaya yang merambat di dalamnya. Efisiensi dari serat optik ditentukan oleh kemurnian dari bahan penyusun gelas/kaca. Makin murni bahan gelas, maka makin sedikit cahaya yang diserap oleh serat optik.

Beberapa persyaratan harus dipenuhi oleh serat optik untuk dapat digunakan, di antara- nya tidak putus saat gaya rentang (tensile force) bekerja pada serat optik, tidak menga- lami perubahan kualitas perambatan cahaya akibat tekanan dari samping seperti misalnya microbending, dan serat optik ditempatkan secara khusus didalam kabel optik dan pada sambungan serat optik harus diberi penguat.

Tugas 2.15

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan teknologi serat optik. Setelah itu, jawablah pertanyaan berikut!
   a. Apa yang tejadi jika serat optic menghasilkan pelemahan (attenuation) kurang dari 20 desibel (dB)/km?
   b. Apa yang terjadi jika sera opyik menghasilkan pelemahan (attenuation) sama dengan dari 20 desibel (dB)/km?
   c. Apa yang terjadi jika serat optic menghasilkan pelemahan (attenuation) lebih dari 20 desibel (dB)/km?
2. Tulislah jawaban Anda di buku tugas!
3. Kumpulkan hasilnya pada guru untuk diberi penilaian!

Guna memenuhi persyaratan tersebut, maka kabel optik harus memiliki beberapa konstruksi yang berbeda sesuai dengan kondisi kabel diletakkan. Secara mendasar, terdapat 6 jenis kabel fiber optik, yaitu kabel udara (aerial cables), kabel tanah tanam langsung (direct buried cables), kabel tanah dengan duct (duct cables), kabel laut/sungai (submarine cables), drop optic kabel penanggal yang ditambatkan untuk catuan user, dan indoor optic (patch cord).

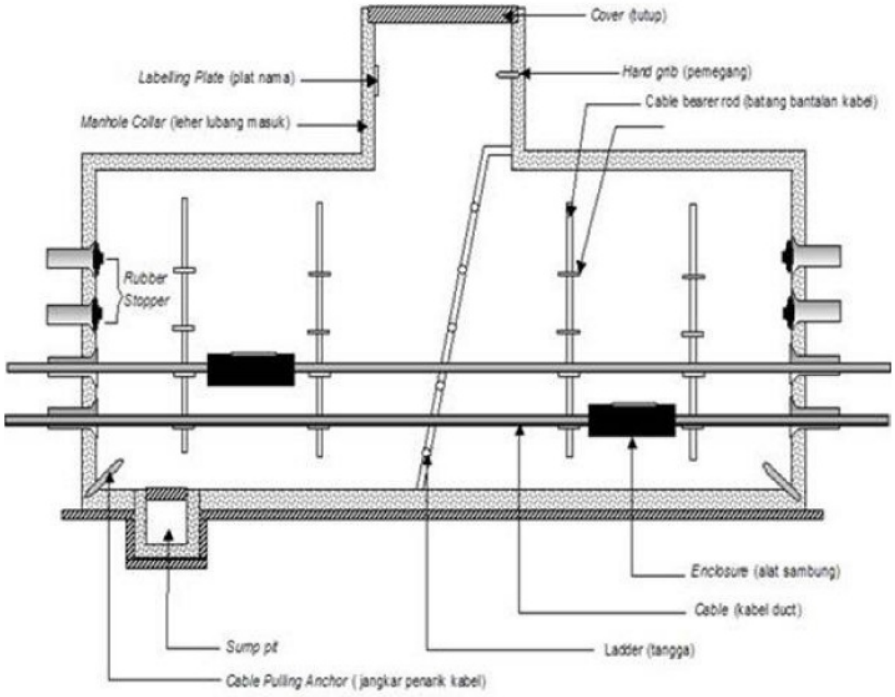
a. Jenis Konstruksi Duct Cable

Kabel tanah dengan duct (duct cables) adalah kabel yang diletakkan di bawah permukaan tanah dan harus memenuhi standar dari ITU-T seri G dan standar nasional seri STEL-K. Metode pemasangannya dengan cara galian terbuka (open trench) ataupun boring rojok (manual borring). Kabel duct pada umumnya tidak menggunakan lapisan armouring yang terbuat dari lilitan baja atau selubung aluminium karena sudah mendapat pengamanan dari pipa PVC dan lapisan cor beton. Sambungan dan penarikan dilakukan melalui manhole. Manhole sebagai salah satu sarana yang digunakan untuk instalasi kabel duct yang dipasang dengan jarak setiap 250 meter.

Fungsi dari manhole di antaranya sebagai tempat sambungan kabel duct, tempat penarikan untuk penggelaran kabel duct, tempat pemeliharaan kabel duct, dan tempat percabangan jalur pada kabel duct. Beberapa ketentuan operasional manhole antara lain sebagai berikut.

1) Pipa duct yang telah terpakai celah-celahnya diisi dengan busa seal untuk mencegah air masuk sepanjang pipa duct.
2) Lubang pipa duct di MH yang belum terpakai harus ditutup rubber stopper.

3) Jika terdapat air dalam manhole harus dikuras/dipompa keluar untuk menjaga supaya aksesoris manhole tidak mudah rusak atau sambungan kemasukan air.
4) Dinding manhole dicat antilumut agar tembok tetap terjaga dengan baik.



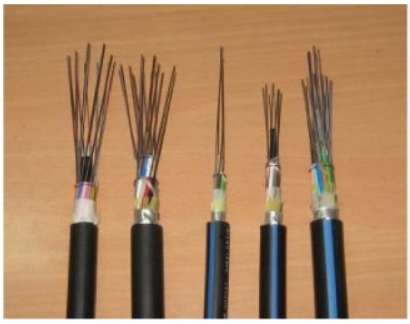
Gambar 2. 22 Manhole

Tipe duct dikategorikan menjadi sebagai berikut.

1) Menggunakan pipa PVC diameter 4 inci, ketebalan 2,2 mm, dengan selubung beton tidak bertulang campuran 2:3:5.
2) Menggunakan pipa PVC diameter 4 inci, ketebalan 5,5 mm, hanya diselubungi pasir uruk dengan pemisah (spacer).

b. Jenis Konstruksi Direct Buried Cable

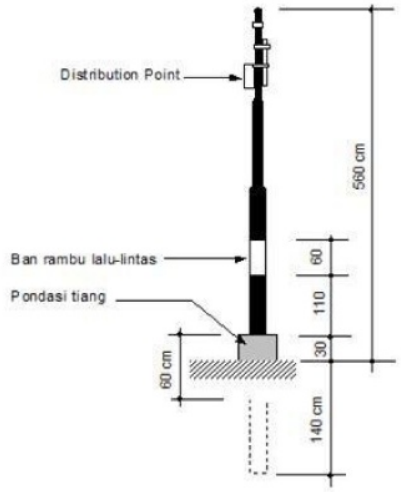
Kabel tanah tanam langsung (direct buried cables) identik dengan kabel yang digelar di bawah tanah (underground) dengan meng- gunakan pelindung pipa PVC berdiameter 4"-5" dan dilapisi dengan cor beton. Metode yang digunakan dengan sistem galian terbuka (open trench) kabel digelar langsung tanpa menggunakan duct/subduct. Jacketing kabel ini didesain lebih tebal dibandingkan kabel duct. Pemasangan penggelaran kabel tanah tanam langsung dapat dilakukan di bahu jalan dan di trotoar, melintas jalan raya, parit, sungai, bahkan pemasangan dapat melintasi rel atau jalan tol.



Gambar 2. 23 Kabel Direct Buried Cable

c. Jenis Konstruksi Aerial Cable

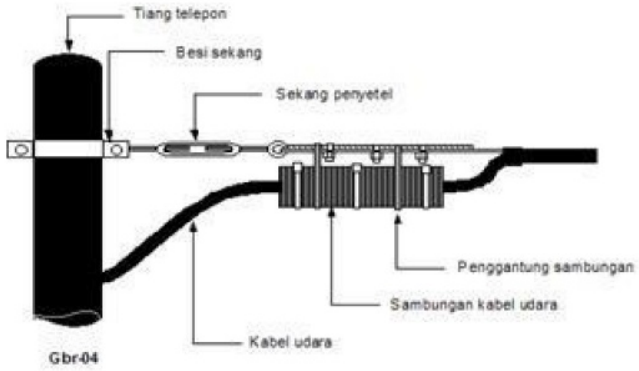
Kabel udara (aerial cables) identik dengan kabel yang ditambatkan pada tiang telepon, di mana penambatan pada bearer kabel yang terbuat dari lilitan kawat baja atau juga disebut dengan messenger wire. Jika tidak tersedia bearer, maka kabel dijepit dengan klip yang ditautkan pada tiang. Terdapat tiga jenis kabel udara yaitu Figure 8, ADSS dan OPGW. Kabel udara ditempatkan pada tiang telepon dengan ketentuan terbuat dari tiang besi dengan panjang 7 meter, 9 meter, dan 12 meter jika dipasang untuk di dalam kota. Sedangkan tiang beton dengan panjang 12 meter dipasang untuk luar kota. Pemasangan tiang dengan cara ditanam 1/5 bagian yang masuk ke dalam tanah, sedangkan untuk tiang besi di pasang pondasi penguat tiang dari adukan semen setinggi 30 cm dengan jarak antartiang antara 40-50 meter. Hal yang perlu dipahami adalah penempatan tiang jangan menutup akses jalan atau di depan pintu gerbang rumah. Sambungan kabel udara ditempatkan di dekat tiang telepon, dengan tujuan memudahkan pemasangan dan memudahkan pemeliharaan. Di dekat sambungan biasanya diberi spare cable (kabel cadangan) yang di-loop agar tidak terjadi gangguan bending. Hal ini jika terjadi gangguan masih terdapat sisa kabel yang dapat disambung dengan loop kabel ini panjangnya antara 4-6 meter.



Gambar 2. 24 Instalasi Kabel Udara

Cara pemasangan kabel udara pada tiang ada dua metode antara lain sebagai berikut.

1) Cara Gantung
   Cara gantung yaitu kabel digantung pada tiang, dengan tidak memotong bearer, digunakan untuk rute lurus dengan jarak kurang dari 50 meter. Sedangkan peralatan yang dipasang pada tiang adalah stainless steel band, suspension clamps, dan stainless steel band.
2) Cara Tambat
   Cara tambat digunakan pada jarak antara tiang lebih dari 50 meter, rute belok atau melengkung dan ujung akhir kabel, dan memotong bearer untuk ditambatkan pada tiang dengan menggunakan span wartel



Gambar 2. 25 Ditambat Karena rute Belok atau Melengkung

d. Jenis Konstruksi Indoor Cable

Kabel fiber optik yang diimplementasikan di dalam bangunan/gedung (patch cord)

Gambar 2. 26 Kabel Fiber Optik Jenis Patch Cord

e. Jenis Konektor Fiber Optik

Penggunaan kabel ini harus disesuaikan dengan jenis perangkat yang digunakan karena mereka ada kemungkinan berbeda. Pada kabel serat optik, sambungan ujung terminal dapat disebut dengan istilah konektor. Konektor kabel fiber optik terdiri dari dua jenis-konektor model ST berbentuk lingkaran dan konektor SC berbentuk persegi. Jenis-jenis dari konektor kabel fiber optik ini tersedia dalam beberapa bentuk yang berbeda-beda tergantung kebutuhan implementasinya, di mana biasanya memiliki tipe standar tertentu.

Tabel 2. 20 Tipe-tipe Konektor Kabel Fiber Optik

No.	Tipe dan Gambar	Deskripsi
1.	FC (Fiber Connector) 	Digunakan untuk model kabel single mode dengan akurasi yang sangat tinggi dalam menghubungkan kabel dengan transmitter maupun receiver. Konektor ini menggunakan sistem drat ulir dengan posisi yang dapat diatur, sehingga ketika dipasangkan ke perangkat lain, akurasinya tidak akan mudah berubah.
2.	SC (Subscriber Connector) 	Digunakan untuk model kabel single mode, dengan sistem dicabut-pasang. Konektor ini tidak terlalu mahal, simpel, dan dapat diatur secara manual serta akurasinya baik bila dipasangkan ke perangkat lain
3.	ST (Straight Tip) 	Bentuknya seperti bayonet berkunci hampir mirip dengan konektor BNC. Sangat umum digunakan baik untuk kabel multi-mode maupun single mode. Sangat mudah digunakan baik dipasang maupun dicabut.
4.	Biconic 	Salah satu konektor yang kali pertama muncul dalam komunikasi fiber optik dan sudah jarang digunakan.
5.	Konektor D4 	Konektor jenis ini hampir mirip dengan FC hanya berbeda ukurannya saja. Perbedaannya sekitar 2 mm pada bagian ferrule-nya.
6.	Konektor SMA 	Konektor jenis ini merupakan pendahulu dari konektor ST yang sama-sama menggunakan penutup dan pelindung. Namun seiring dengan berkembangnya ST konektor, maka konektor ini sudah tidak berkembang lagi penggunaannya
7.	E200	Jenis-jenis konektor tipe kecil yaitu LC, SMU, dan SC-DC.

Tugas 2.16

Kerjakan Tugas Berikut Secara kelompok!

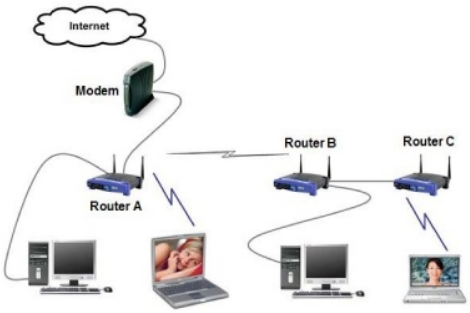
1. Bentuklah kelompok yang terdiri dari 3-4 anggota!
2. Lakukan penelusuran informasi menggunakan internet atau media cetak yang berkaitan dengan jenis kabel fiber optic yang digunakan dalam kehidupan sehari-hari!
3. Hasilnya dimasukkan seperti table berikut!

No	Jenis Kabel Fiber Optik	Penggunaan
1	Kabel drop optic kabel penanggal yang ditambatkan untuk catuan user.	
2	Kabel indoor optic (patch cord).	
3	Kabel laut/sungai (submarine cables).	
4	Kabel tanah dengan duct (duct cables).	
5	Kabel tanah tanam langsung (direct buried canbles).	
6	Kabel udara (aerial cables)	

4. Gunakan informasi dalam table di atas menjadi bahan diskusi kelompok!
5. Presentasikan hasil diskusi kelompok Anda di depan kelas dan mintalah tanggapan dari kelompok lain!

I. Prinsip Dasar Sistem WLAN

Wireless Local Area Network (Wireless LAN) adalah jaringan kompter yang memungkinkan user untuk terkoneksi tanpa menggunakan kabel jaringan. Laptop atau gadget yang dilengkapi dengan kartu wireless LAN bisa bergerak di sekitar gedung sambil membawa komputer dan tetap terhubung ke jaringan mereka tanpa perlu mencolok kabel. Jaringan wireless LAN sangat efektif digunakan dalam sebuah kawasan atau gedung. Adapun dengan performa dan keamanan yang dapat dihandalkan, pengem- bangan jaringan wireless LAN menjadi tren baru pengembangan jaringan menggantikan jaringan wired atau jaringan penuh kabel. Oleh karena wireless LAN mengirim meng- gunakan frekuensi radio, wireless LAN diatur oleh jenis hukum yang sama dan digunakan untuk mengatur hal-hal seperti AM/FM radio. Jalur WLAN Federal Communications Commission (FCC) mengatur penggunaan alat dari wireless LAN. Dalam pemasaran wireless LAN sekarang, menerima beberapa standar operasional dan syarat dalam Amerika Serikat yang diciptakan dan dirawat oleh Institute of Electrical Electronic Engineers (IEEE).



Gambar 2. 27 Jalur WLAN

1. Standar Wireless LAN

Standar wireless LAN adalah IEEE (Institute of Electrical Engineers) merupakan organisasi non-profit yang mendedikasikan kerja kerasnya demi kemajuan teknologi. Pada tahun 1980, IEEE membuat sebuah bagian yang mengurusi standarisasi LAN dan MAN (Metropolitan Area Network). Bagian ini kemudian dinamakan sebagai 802. Angka 80 menunjukkan tahun dan angka 2 menunjukkan bulan dibentuknya kelompok kerja ini.

Adapun standarisasi tersebut adalah IEEE 802.11, IEEE 802.11b, dan IEEE 802.11g.

a. IEEE 802.11: standar asli wireless LAN menetapkan tingkat perpindahan data yang paling lambat dalam teknologi transmisi light-based dan RF.
b. IEEE 802.11b: menggambarkan tentang beberapa transfer data yang lebih cepat dan lebih bersifat terbatas dalam lingkup teknologi transmisi. IEEE 802.11a-gambaran tentang pengiriman data lebih cepat dibandingkan (tetapi kurang sesuai dengan) IEEE 802.11b, dan menggunakan 5 GHZ frekuensi band UNII.
c. IEEE 802.11g: syarat yang paling terbaru berdasar pada 802.11 standar yang menguraikan transfer data sama dengan cepatnya seperti IEEE 802.11a, dan sesuai dengan 802.11b yang memungkinkan untuk lebih murah.

2. Komponen Wireless LAN

Komponen utama dalam wireless LAN antara lain sebagai berikut.

a. Access Point

Merupakan perangkat yang menjadi sentral koneksi dari pengguna (user) ke ISP, atau dari kantor cabang ke kantor pusat jika jaringannya adalah milik sebuah perusahaan. Access point berfungsi mengonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.

b. Wireless LAN Interface

Merupakan peralatan yang dipasang di Mobile/Desktop PC, peralatan yang dikembangkan secara massal adalah dalam bentuk PCMCIA (Personal Computer

Memory Card International Association) card, PCI card maupun melalui port USB (Universal Serial Bus).

c. Mobile Desktop/PC

Merupakan perangkat akses untuk pengguna, mobile PC pada umumnya sudah ter-pasang port PCMCIA sedangkan desktop PC harus ditambahkan wireless adapter melalui PCI (Peripheral Component Interconnect) card atau USB (Universal Serial Bus).

3. Teknologi LAN Nirkabel

Beberapa jenis teknologi LAN nirkabel antara lain sebagai berikut.

a. Wi-Fi

Wi-Fi (Wireless Fidelity) merupakan pe- ngembangan dari istilah Hi-Fi sebagai sebuah teknologi jaringan nirkabel yang digunakan di seluruh dunia. Wi-Fi adalah teknologi yang dirancang untuk memenuhi sistem komputasi ringan masa depan dengan mengonsumsi. daya minimal. PDA, laptop, dan berbagai aksesoris dirancang untuk Wi-Fi-kompatibel. Bahkan ada ponsel dalam pengembangan yang akan beralih dari jaringan seluler ke jaringan Wi-Fi tanpa mengabaikan panggilan masuk. Wi-Fi mengacu pada sistem yang menggunakan standar 802.11 yang dikembangkan oleh Institute of Electrical and Electronics Engineers (IEEE) dan dirilis pada tahun 1997.

Dalam jaringan Wi-Fi, komputer dengan kartu jaringan Wi-Fi terhubung tanpa kabel ke router nirkabel. Router tersambung ke internet melalui modem, biasanya kabel atau modem DSL. Setiap pengguna dalam jarak 200 kaki atau lebih (sekitar 61 meter) dari titik akses dapat terhubung ke internet, meskipun untuk kecepatan transfer yang baik berada pada jarak maksimal 100 kaki (30,5 meter). Wi-Fi jaringan dapat menjadi "open" sehingga siapa pun dapat menggunakannya atau "closed" jika dibutuhkan password. Area yang diselimuti akses nirkabel ini sering disebut area hotspot nirkabel.

b. Hotspot

Hotspot adalah definisi untuk daerah yang dilayani oleh satu access point wireless LAN standar 802.11a/b/g, pengguna (user) dapat masuk ke dalam access point secara bebas dan mobile menggunakan perangkat sejenis notebook, PDA atau lainnya.

Hal yang perlu diperhatikan dalam membangun sebuah kawasan wireless area adalah konfigurasi serta persyaratan apa yang harus dipenuhi serta untuk siapa wireless area diperuntukkan. Beberapa hal tersebut adalah ukuran lokasi cakupan, jumlah perkiraan user yang simultan, dan tipe pengguna una wireless sasaran.

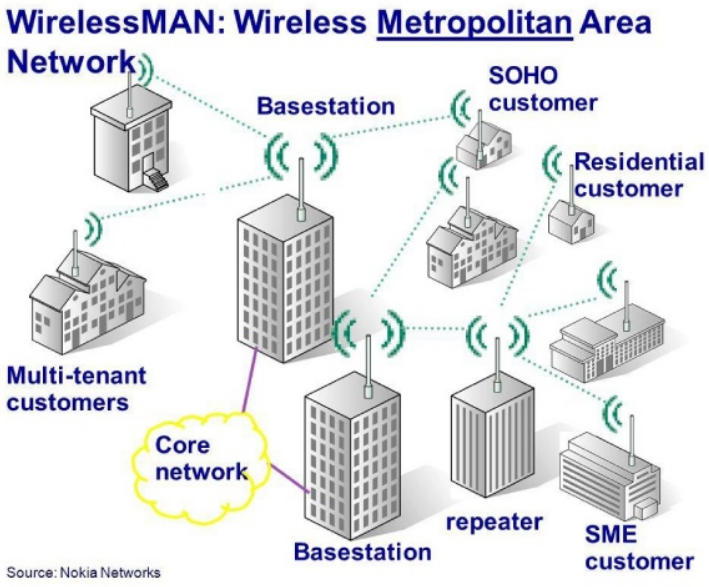
1) Ukuran lokasi cakupannya yaitu ukuran ini menjadi pertimbangan awal yang sangat menentukan dalam membangun area wireless hotspot. Adapun dengan

menentukan area cakupan, akan dapat dipilih peralatan Access Point (AP) mana yang dapat melayani. Beberapa AP diperlukan untuk menyediakan area cakupan yang lebih luas.

2) Jumlah pengguna yaitu dalam melakukan layout hotspot, jumlah user dapat digunakan untuk menentukan serta memperkirakan kepadatan pengguna pada kawasan tersebut. Kepadatan ini dapat diukur dari jumlah pengguna per kawasan. Di samping jumlah pengguna, hal yang lebih penting adalah pola pengguna sasaran yang dituju, sehingga akan dapat ditentukan pula target minimum bandwidth per user yang aktif.
3) Model penggunaan yaitu faktor ketiga adalah tipe aplikasi apa yang digunakan oleh user yang akan tersambung di hotspot tersebut. Model pada aplikasi kampus akan berbeda aplikasinya dibanding dengan di hotel, atau di kafe-kafe yang menyediakan hotspot. Kebutuhan yang dapat digunakan sebagai standar minimal bandwidth yang dibutuhkan untuk menyediakan ketersediaan resource bandwidth adalah faktor utama dalam menentukan kapasitas minimal bandwidth internet yang akan digunakan.

4. Teknologi WLAN

Teknologi wireless LAN memiliki fokus pada modulasi suara dan data. Modulasi akan mengonversi sinyal digital, sehingga dapat merepresentasikan informasi di komputer melalui sinyal digital melalui Radio Frequency (RF) atau sinyal cahaya. Wireless WAN secara eksklusif menggunakan sinyal RF yang didesain untuk mengakomodasi beberapa pengguna sekaligus. Setiap user akan memiliki channel terdedikasi. Interferensi antara pengguna wireless WAN dengan base station dapat dikurangi.

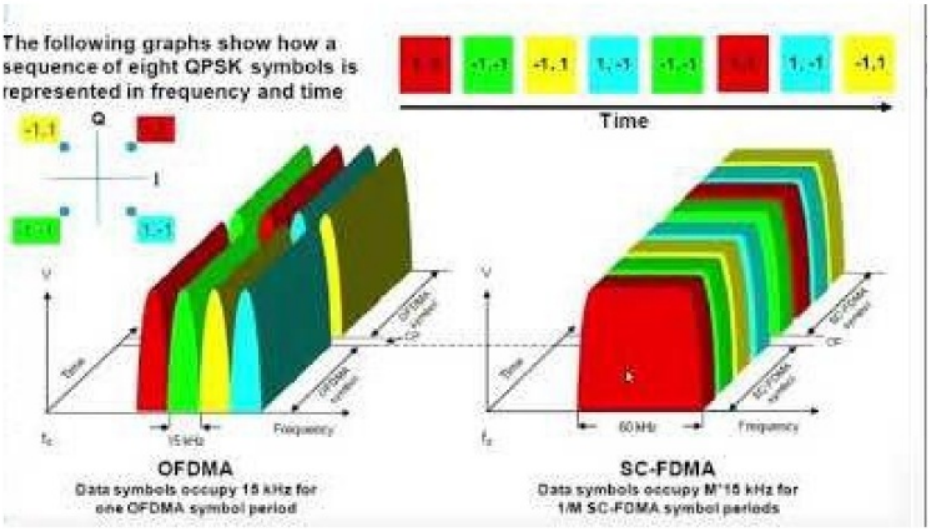


Gambar 2. 28 Gambar Topologi WWAN

Beberapa teknik modulasi pada teknologi wireless WAN antara lain sebagai berikut

a. Frequency Division Multiple Access (FDMA)

FDMA berarti banyak orang menggunakan sistem ponsel sekaligus dengan mengirimkan panggilan mereka dengan gelombang radio frekuensi yang sedikit berbeda. FDMA sendiri bisa dikatakan sebagai awal bekerjanya ponsel analog. FDMA seperti versi radio dari sistem telepon darat biasa dan masih menggunakan sistem analog. FDMA ponsel yang kadang-kadang disebut generasi pertama (1G) ponsel.



Gambar 2. 29 Skema FDMA

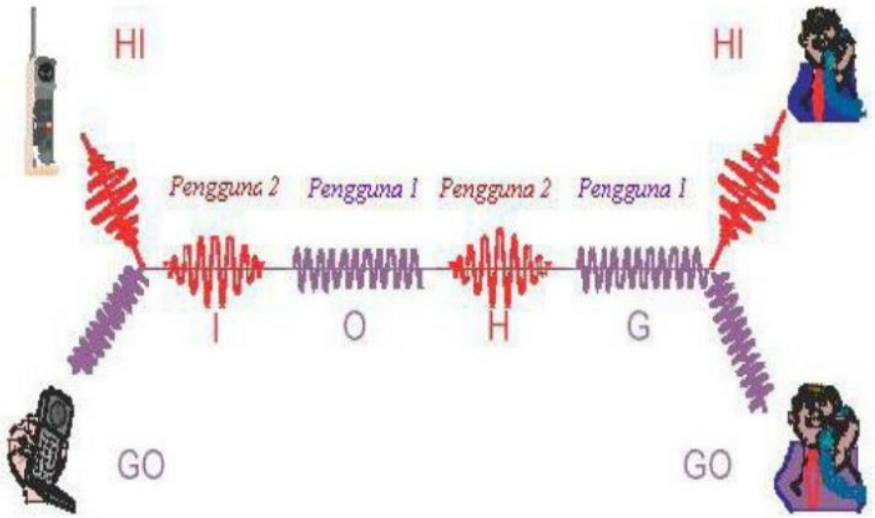
FDMA adalah sistem multiple access yang menempatkan seorang pelanggan pada sebuah kanal berbentuk pita frekuensi (frequency band) komunikasi. Jika satu pita frekuensi dianggap sebagai satu jalan, maka FDMA merupakan teknik "satu pelanggan, satu jalan. Pada saat pelanggan A sedang menggunakan jalan itu, 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. Jika setiap pita memerlukan lebar 30 Kilohertz (kHz) dan frekuensi yang digunakan berawal dari 890 Megahertz (MHz), maka:

1) pita frekuensi kanal 1 mulai dari 890 MHz hingga 890,030 MHz;
2) pita frekuensi kanal 2 mulai dari 890,030 MHz hingga 890,060 MHz; serta
3) pita frekuensi kanal 3 mulai dari 890,060 MHz hingga 890,090 MHz dan seterusnya.

Artinya, jika frekuensi yang digunakan memiliki batas 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 antar penyelenggara telepon seluler. Oleh karena itu, untuk memperbanyak kapasitas dengan jumlah kanal yang terbatas digunakan trik-trik tertentu yang sesuai dengan strategi penyedia layanan.

b. Time Division Multiple Access (TDMA)

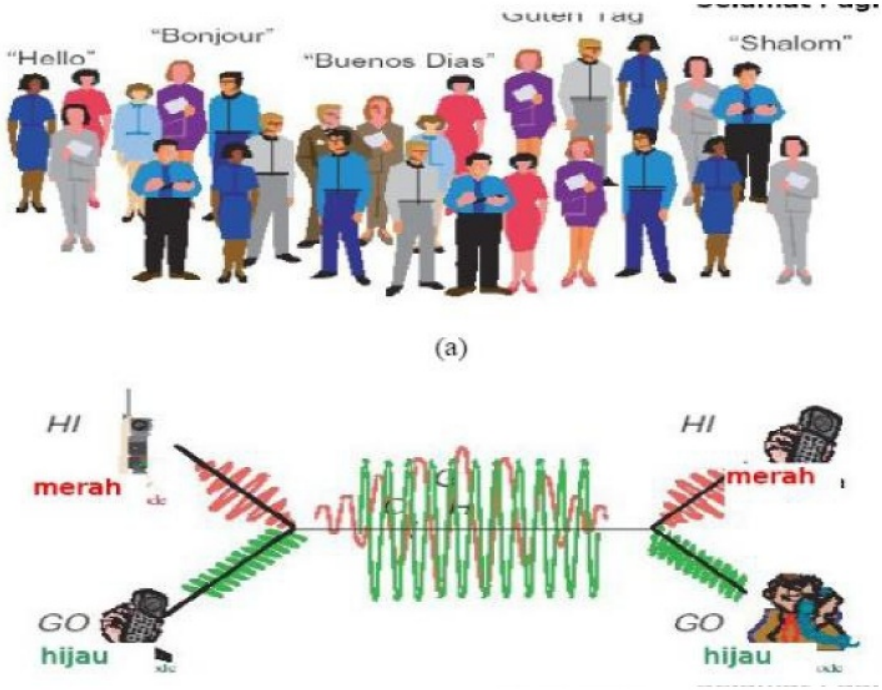
(TDMA) diperkenalkan oleh Telecommunications Industry Association (TIA) sebagai sebuah teknologi transmisi digital yang mengalokasikan slot waktu unik untuk setiap pengguna pada masing-masing saluran dan menjadi salah satu cara yang digunakan oleh jaringan digital telepon seluler untuk menghubungkan panggilan telepon. Sinyal digital dari jaringan digital dihubungkan ke user tertentu untuk berhubungan dengan sebuah kanal frekuensi digital tersendiri tanpa memutuskannya dengan mengalokasikan waktu. Keuntungannya adalah tidak berbagi dengan sistem TDMA di mana semua pemancar dan penerima harus memiliki akses pada waktu yang sama. Setiap user TDMA menggunakan pita frekuensi yang sama, tetapi domain waktu dibagi menjadi beberapa slot. Pengguna 1 dapat mengirimkan data pada slot waktu untuk pengguna 1, pengguna 2 dapat mengirimkan berupa data pada slot waktu untuk pengguna 2, dan seterusnya.



Gambar 2. 30 Sistem Kerja TDMA

c. Code Division Multiple Access (CDMA)

CDMA merupakan akses yang menggunakan prinsip komunikasi spektrum tersebar. Dalam CDMA setiap pengguna menggunakan frekuensi yang sama dalam waktu bersamaan tetapi menggunakan sandi unik yang saling ortogonal. Sandi-sandi ini membedakan antara pengguna satu dengan pengguna yang lain. Pada jumlah pengguna yang besar, dalam bidang frekuensi yang diberikan akan ada banyak sinyal dari pengguna sehingga interferensi akan meningkat. Kondisi ini akan menurunkan unjuk-kerja sistem. Hal ini berarti, kapasitas dan kualitas sistem dibatasi oleh daya interferensi yang timbul pada lebar bidang frekuensi yang digunakan.



Gambar 2. 31 Sistem Kerja CDMA

5. Keuntungan WLAN

Sebuah jaringan lokal (LAN) yang terbentuk dengan menggunakan media perantara sinyal radio frekuensi tinggi, bukan dengan menggunakan kabel. Media wireless yang tidak kasat mata menawarkan cukup banyak keuntungan bagi penggunanya, antara lain sebagai berikut.

1) Meningkatkan Produktivitas
   Jaringan WLAN sangat mudah untuk diimplementasikan, sangat rapi dalam hal fisiknya yang dapat meneruskan informasi tanpa seutas kabel pun, sangat fleksibel karena bisa diimplementasikan hampir di semua lokasi dan kapan saja, dan yang menggunakannya pun tidak terikat di satu tempat saja. Adapun dengan semua faktor yang ada ini, para penggunanya tentu dapat melakukan pekerjaan dengan lebih mudah akibatnya pekerjaan jadi cepat dilakukan, tidak membutuhkan waktu yang lama hanya karena masalah-masalah fisikal jaringan dari PC yang mereka gunakan. Berdasarkan faktor inilah, wireless LAN tentunya dapat secara tidak langsung meningkatkan produktivitas dari para penggunanya cukup banyak faktor penghambat yang ada dalam jaringan kabel yang dapat dihilangkan jika Anda menggunakan media ini. Meningkatnya produktivitas kerja para karyawannya, tentu akan sangat bermanfaat bagi perusahaan tempat mereka bekerja.
2) Cepat dan Sederhana
   Implementasinya Implementasi jaringan WLAN terbilang mudah dan sederhana. Mudah karena Anda hanya perlu memiliki sebuah perangkat penerima pemancar untuk membangun sebuah jaringan wireless. Setelah memilikinya, lakukan

konfigurasi sedikit kemudian siap untuk menggunakan sebuah jaringan komunikasi data bau dalam lokasi Anda. Namun, tidak sesederhana itu jika Anda menggunakan media kabel.

3) Fleksibel
   Media wireless LAN dapat menghubungkan Anda dengan jaringan pada tempat-tempat yang tidak bisa diwujudkan oleh media kabel. Jadi fleksibilitas media wireless ini benar-benar tinggi karena Anda bisa memasang dan menggunakannya di mana saja dan kapan saja, misalnya di taman, di ruangan rapat, dan banyak lagi.
4) Dapat Mengurangi Biaya Investasi
   Wireless LAN sangat cocok bagi Anda yang ingin menghemat biaya yang akan dikeluarkan untuk membangun sebuah jaringan komunikasi data. Tanpa kabel berarti juga tanpa biaya, termasuk biaya termasuk biaya kabelnya sendiri, biaya penarikan, biaya perawatan, dan masih banyak lagi. Apalagi jika Anda membangun LAN yang sering berubah-ubah, tentu biaya yang Anda keluarkan akan semakin tinggi jika menggunakan kabel.
5) Skalabilitas
   Adapun dengan menggunakan media wireless LAN, ekspansi jaringan dan konfigurasi ulang terhadap sebuah jaringan tidak akan rumit untuk dilakukan seperti halnya dengan jaringan kabel. Di sinilah nilai skalabilitas jaringan WLAN cukup terasa.

6. Prinsip Jaringan Nirkabel

Prinsip dasar sebuah jaringan nirkabel pada dasarnya sama dengan jaringan ethernet card, sedangkan fungsi Access Point (AP) pada sebuah jaringan nirkabel mirip dengan hub pada jaringan komputer berbasis kabel. Jika tanpa access point, komputer yang memiliki adapter nirkabel dapat berkomunikasi langsung dengan komputer lainnya, maka hal ini sama dengan hubungan komputer ke komputer (peer-to-peer) dengan menggunakan kabel metode saling-silang (cross-over). Jaringan nirkabel identik dengan teknologi yang menggunakan dua peranti untuk bertukar data tanpa media kabel. Jaringan nirkabel biasanya menghubungkan satu sistem komputer dengan sistem yang lain dengan menggunakan beberapa macam media transmisi tanpa kabel, seperti gelombang radio, gelombang mikro, maupun cahaya infrared. Data dipertukarkan melalui media gelombang cahaya tertentu seperti teknologi infrared pada remote TV atau gelombang radio seperti Bluetooth pada ponsel dan komputer dengan frekuensi tertentu.

Untuk lebih jelasnya mengenai prinsip jaringan nirkabel, anda dapat melihat video berikut:

a. Jaringan Nirkabel Berdasarkan Ukuran Fisik Area

Berdasarkan ukuran fisik area yang dapat dicakup, jaringan nirkabel terbagi menjadi beberapa kategori. Beberapa jenis jaringan nirkabel secara umum memiliki karakteristik yang hampir sama dengan jaringan kabel tradisional. Secara logika, jaringan ini sama dengan jaringan kabel tradisional, yang membedakan adalah media yang digunakan. Secara konsep dasar, layering nirkabel sama dengan wired networking, hanya cara komunikasi serta mediasinya yang berlainan.

1) WPAN (Wireless Personal Area Network)

Jaringan personal adalah jaringan nirkabel yang memiliki cakupan area yang sangat sempit, yaitu seki- tar 20 m. Jaringan ini hanya dapat digunakan sebagai jaringan per- sonal dalam ruangan kecil karena jaraknya yang sedemikian kecil. Performa jaringan wireless PAN termasuk dalam kategori sedang, dengan kecepatan datanya (date rate) mencapai 2 Mbps. Pemanfaatan jaringan personal wireless telah cukup luas, terutama pada peralatan -peralatan mobile seperti PDA, laptop, dan telepon seluler. Beberapa bentuk pemanfaatan jaringan area kecil yang paling umum adalah Aktivitas sinkronisasi antar-peralatan gadget dengan PC atau laptop. Bahkan beberapa perangkat mobile tersebut dapat melakukan koneksi ke printer atau peralatan multimedia yang lain, sehingga praktis dapat menggantikan komunikasi kabel tradisional. Beberapa peralatan mobile yang dapat memanfaatkan komunikasi area kecil hanya mengonsumsi daya cukup rendah. Konsumsi daya yang rendah mengakibatkan peralatan tersebut dapat memiliki kemampuan operasional yang relatif panjang tanpa harus kehilangan daya baterai. Implementasi wireless PAN banyak diterapkan pada peralatan gadget, seperti telepon seluler, PDA, atau PDA phone, audio headset, dan lainnya. Adapun dengan audio headset, contohnya pengguna gadget

akan dengan mudah melakukan pembicaraan dan mendengarkan musik tanpa terbebani kabel yang membelit peralatannya.

Gambar 2. 32 Jalur WPAN

Teknologi jaringan wireless PAN antara lain sebagai berikut.

a) 802.15
   Teknologi yang digunakan pada wireless PAN mencakup teknologi pemanfaatan inframerah dan radio frekuensi Bluetooth. Standar IEEE 802.15 telah memfokuskan pada pengembangan jaringan wireless personal dengan koordinasi standar yang lain, seperti standar 802.11 pada jaringan yang lebih luas. Beberapa standar 802.15 antara lain sebagai berikut.
b) 802.15.1
   Task grup 1 telah mengeluarkan standar wireless PAN pada spesifikasi Bluetooth versi 1.1 dengan menggunakan Frekuensi Hopping Spread Spectrum (FHSS) dan beroperasi hingga 1 Mbps. Standar ini dikeluarkan bulan Juni 2002 untuk memfasilitasi para pengembang yang mendukung Bluetooth.
c) 802.15.2
   Task grup 2 ini telah mendefinisikan rekomendasi terhadap 802.15 yang berdampingan dengan standar 502.11 serta beroperasi pada frekuensi yang sama, yaitu 2,4 GHz. Adapun dengan adanya koordinasi dari dua standar ini diharapkan dapat menghilangkan interferensi yang terjadi pada keduanya dan meminimalisir interferensi antar-peralatan yang mendukung standar ini.
d) 802.15.3
   Task grup 3 ini telah mengeluarkan draf standar untuk meningkatkan rate pada wireless PAN mejadi lebih tinggi. Data rate yang ditingkatkan adalah 11, 22, 33, 44, dan 55 Mbps. Kombinasi dan data rate ini sangat dibutuhkan untuk aplikasi multimedia, yaitu untuk meningkatkan Quality of Service (QoS).
e) 802.15.4

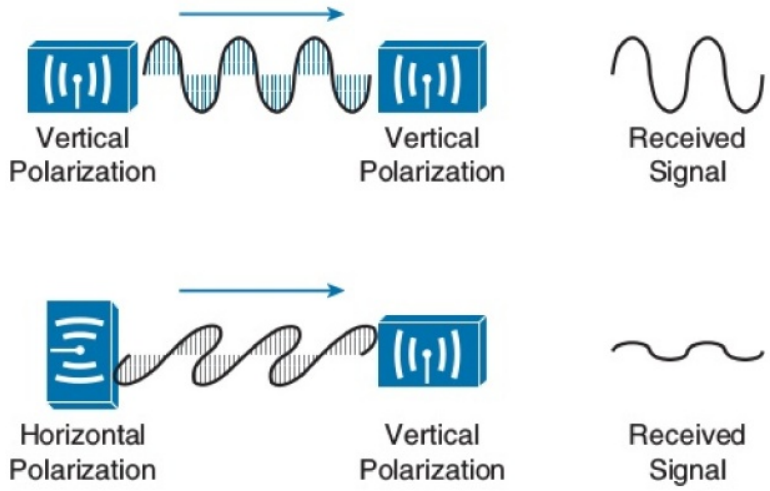
Task grup 4 ini telah mendefinisikan standar low data rate yang sangat ekstrim, sehingga menghasilkan peralatan yang memiliki konsumsi daya sangat rendah. Peralatan yang menerapkan standar ini berupa peralatan dengan bentuk yang kecil dan memiliki daya tahan baterai yang sangat panjang dari range bulanan hingga tahunan. Contoh penerapannya adalah sistem peralatan otomatisasi rumah dan lain-lain

2) Bluetooth

Bluetooth merupakan spesifikasi industri untuk jaringan wilayah pribadi nirkabel (WPAN). Bluetooth menfasilitasi koneksi dan pertukaran informasi di antara alat-alat seperti PDA, ponsel, komputer, laptop, printer, dan kamera digital melalui frekuensi radio jarak dekat. Nama Bluetooth sendiri diambil dari nama seorang raja di Denmark yang bertakhta pada abad ke 10, yakni Raja Harald Bluetooth. Pada masa hidupnya, raja tersebut aktif berdiplomasi memfasilitasi perundingan-perundingan untuk mendamaikan pihak pihak yang bersengketa. Para penemu teknologi Bluetooth menganggap nama belakang raja tersebut sesuai dengan sifat teknologi nirkabel tersebut.

b. Polarisasi

Polarisasi antena didefinisikan sebagai arah vektor medan listrik yang diradiasikan oleh antena pada arah propagasi. Jika jalur dari vektor medan listrik maju dan kembali pada suatu garis lurus dikatakan berpolarisasi linier, misalnya medan listrik dari dipole ideal. Jika vektor medan listik konstan dalam panjang tetapi berputar di sekitar jalur lingkaran, maka dapat dikatakan sedang berpolarisasi lingkaran. Umumnya karakteristik polarisasi sebuah antena relatif konstan pada main lobe. Tetapi polarisasi beberapa minor lobe berbeda jauh dengan polarisasi main lobe. Dalam teknik antena, terdapat dua macam polarisasi, yaitu vertikal dan horizontal. Antar-antena pemancar dan penerima, sebaiknya digunakan polarisasi yang sama berkaitan dengan bagaimana cara pemasangan kedua antena. Sebuah antena dapat memancarkan energi dengan polarisasi yang tidak diinginkan disebut polarisasi silang (cross polarized) yang dapat menimbulkan side lobe sehingga mengurangi gain. Polarisasi silang tegak lurus dengan polarisasi yang diinginkan pada antena polarisasi linier dan pada antena polarisasi lingkaran akan terjadi polarisasi silang berlawanan dengan arah perputarannya yang diinginkan. Hal ini biasa yang disebut dengan deviasi dari polarisasi lingkaran sempurna yang mengakibatkan polarisasinya berubah menjadi polarisasi elips.



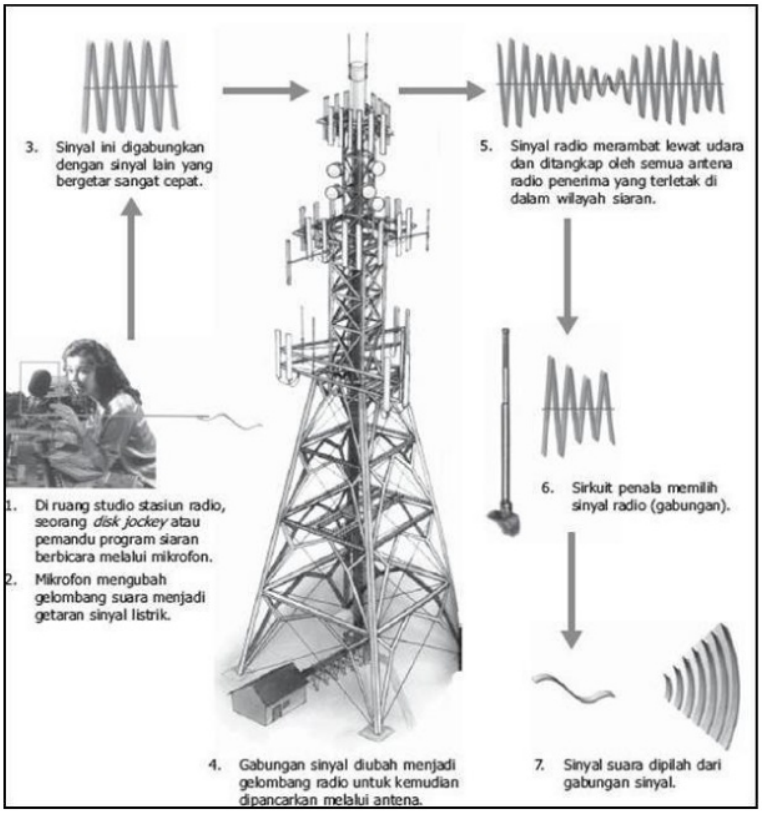
Gambar 2. 33 Polarisasi Horizontal dan Vertikal

c. Spektrum Elektromagnetik

Spektrum gelombang elektromagnetik identik dengan susunan semua bentuk gelombang berdasarkan panjang gelombang dan frekuensinya. Spektrum elektromagnetik disusun berdasarkan panjang gelombang mencakup kisaran energi yang sangat rendah, panjang gelombang tinggi, dan frekuensi rendah. Seperti gelombang radio sampai ke energi yang sangat tinggi, serta dengan panjang gelombang rendah dan frekuensi tinggi seperti radiasi sinar X-ray dan sinar gama.

1) Gelombang Radio

   Gelombang radio identik dengan gelombang elektromagnetik yang disebarkan melalui antena. Gelombang radio memiliki frekuensi yang berbeda-beda sehingga memerlukan penyetelan frekuensi tertentu yang cocok pada radio receiver (penerima radio) untuk mendapatkan sinyal tersebut. Frekuensi gelombang radio mulai dari 30 kHz ke atas dan dikelompokkan berdasarkan lebar frekuensinya. Gelombang radio dihasilkan oleh muatan-muatan listrik yang dipercepat melalui kawat-kawat penghantar. Muatan-muatan tersebut dibangkitkan oleh rangkaian elektronika (osilator) selanjutnya dipancarkan dari antena dan diterima oleh antena pula dan tidak dapat mendengar radio secara langsung, tetapi penerima radio akan mengubah terlebih dahulu energi gelombang menjadi energi bunyi. Gelombang radio berperan sebagai media transmisi pada jaringan nirkabel. Radio adalah teknologi yang digunakan untuk pengiriman sinyal dengan cara modulasi dan radiasi elektromagnetik (gelombang elektromagnetik).



Gambar 2. 34 Alur Sistem Gelombang Radio

Gelombang ini melintas dan merambat lewat udara dan bisa juga merambat lewat ruang angkasa yang hampa udara, karena gelombang ini tidak memerlukan medium pengangkut (seperti molekul udara). Gelombang radio sebagai salah satu bentuk dari radiasi elektromagnetik yang terbentuk ketika objek bermuatan listrik dimodulasi (dinaikkan frekuensinya) pada frekuensi yang terdapat dalam frekuensi gelombang radio (RF) dalam suatu spektrum elektromagnetik dan radiasi elektromagnetiknya bergerak secara osilasi elektrik maupun magnetik. Frekuensi gelombang radio mulai dari 30 kHz ke atas dan dikelompokkan berdasarkan lebar frekuensinya.

Tabel 2. 21 Pengelompokan Gelombang Radio

Lebar Frekuensi	Panjang Gelombang Tertentu	Beberapa Penggunaan
Low (LF) 30 kHz - 300 kHz	Long wave (1.500 m)	Radio gelombang panjang dan komunikasi melalui jarak jauh.
Medium (MF) 300 kHz - 3 MHz	Medium wave (300 m)	Gelombang medium lokal dan radio jarak jauh.

High (HF) 3 MHz - 30 MHz	Short wave (30 m)	Radio gelombang pendek dan komunikasi, radio amatir, dan CB.
Very High (VHF) 30 MHz - 300 MHz	Very short wave (3 m)	Radio FM, polisi, dan pelayanan darurat.
Ultra High (UHF) 300 MHz - 3 GHz	Ultra short wave (30 cm)	TV
Super High (SHF) Di atas 3 GHz	Microwaves (3 cm)	Radar, komunikasi satelit, telepon, dan saluran TV.

Secara umum simplifikasi dari perilaku gelombang radio yang dapat digunakan untuk perencanaan jaringan nirkabel adalah sebagai berikut.

a) Panjang gelombang makin panjang, makin jauh gelombang radio merambat.
b) Panjang gelombang makin panjang, makin mudah gelombang radio melalui atau mengitari penghalang.
c) Makin pendek panjang gelombang, makin banyak data yang dapat dikirim.

2) Gelombang Mikro

Gelombang mikro (microwaves) adalah gelombang radio dengan frekuensi paling tinggi diatas 3 GHz. Gelombang mikro juga dimanfaatkan pada pesawat RADAR (Radio Detection and Ranging). RADAR berarti mencari dan menentukan jejak sebuah benda dengan menggunakan gelombang mikro dengan memanfaatkan sifat pemantulan gelombang mikro. Jika gelombang mikro diserap oleh sebuah benda, maka akan muncul efek pemanasan pada benda itu. Jika makanan menyerap radiasi gelombang mikro, maka makanan menjadi panas dalam selang waktu yang sangat singkat. Proses inilah yang dimanfaatkan dalam microwave oven untuk memasak makanan dengan cepat dan ekonomis.

3) Sinar Inframerah

Sinar inframerah meliputi daerah frekuensi 1.011Hz sampai 1.014 Hz atau daerah panjang gelombang 10 cm sampai 10^{-1} cm. Jika memeriksa spektrum yang dihasilkan oleh sebuah lampu pijar dengan detektor yang dihubungkan pada miliamperemeter, maka jarum amperemeter akan berada sedikit diatas ujung spektrum merah. Sinar yang tidak dilihat tetapi dapat dideteksi di atas spektrum merah disebut radiasi inframerah. Sinar infamerah dihasilkan oleh elektron dalam molekul-molekul yang bergetar karena benda dipanaskan. Jadi setiap benda panas pasti memancarkan sinar inframerah dengan jumlah yang dipancarkan bergantung pada suhu dan warna benda.

4) Cahaya Tampak
   Cahaya tampak sebagai radiasi elektromagnetik yang paling dikenal oleh kita dapat didefinisikan sebagai bagian dari spektrum gelombang elektromagnetik yang dapat dideteksi oleh mata manusia. Panjang gelombang tampak bervariasi tergantung warnanya mulai dari panjang gelombang kira-kira 4 x 10-7 m untuk cahaya violet (ungu) sampai 7 x 10-7 m untuk cahaya merah. Kegunaan cahaya salah satunya adalah penggunaan laser dalam serat optik pada bidang telekomunikasi dan kedokteran.
5) Sinar Ultraviolet
   Sinar ultraviolet memiliki frekuensi dalam daerah 1.015 Hz sampai 1.016 Hz atau dalam daerah panjang gelombang 10-8 m-10-7 m. gelombang ini dihasilkan oleh atom dan molekul dalam nyala listrik. Matahari adalah sumber utama yang memancarkan sinar ultraviolet di permukaan bumi, lapisan ozon yang ada dalam lapisan atas atmosferlah yang berfungsi menyerap sinar ultraviolet dan meneruskan sinar ultraviolet yang tidak membahayakan kehidupan makhluk hidup di bumi.
6) Sinar X
   Sinar X memiliki frekuensi antara 10 Hz sampai 10 Hz dengan panjang gelombang sangat pendek yaitu 10 cm sampai 10 cm. meskipun seperti itu tapi sinar X memiliki daya tembus kuat, dapat menembus buku tebal, kayu tebal beberapa sentimeter dan pelat aluminium setebal 1 cm.
7) Sinar Gama
   Sinar gama memiliki frekuensi antara 10 Hz sampai 10 Hz atau panjang gelombang antara 10 cm sampai 10 cm. Daya tembus paling besar, yang menyebabkan efek yang serius jika diserap oleh jaringan tubuh.

d. Bandwidth

Pemakaian sebuah antena dalam sistem pemacar atau penerima selalu dibatasi oleh daerah frekuensi kerjanya. Pada range frekuensi kerja tersebut antena dituntut harus dapat bekerja dengan efektif agar dapat menerima atau memancarkan gelombang pada band frekuensi tertentu. Pengertian harus dapat bekerja dengan efektif adalah bahwa distribusi arus dan impedansi dari antena pada range frekuensi tersebut benar-benar belum banyak mengalami perubahan yang berarti. Sehingga pola radiasi yang sudah direncanakan serta VSWR yang dihasilkannya masih belum keluar dari batas yang diijinkan. Daerah frekuensi kerja di mana antena masih dapat bekerja dengan baik dinamakan bandwidth antena.

e. Frekuensi dan Kanal

Frekuensi adalah jumlah gelombang yang melalui suatu titik dalam satu satuan waktu. Guna mencapai suatu jarak ter- tentu, makin panjang gelombang, makin rendah frekuensinya. Sebaliknya, makin pendek gelombang, makin tinggi frekuensi yang diperlukan.

Guna menghitung frekuensi, seseorang menetapkan jarak waktu, menghitung jumlah kejadian peristiwa, dan membagi hitungan ini dengan panjang jarak waktu. Frekuensi sebesar 1 Hz menyatakan peristiwa yang terjadi satu kali per detik.

$$f = \frac{1}{T}$$

dengan *f* adalah frekuensi (hertz) dan *T* adalah periode (sekon atau detik). Selain itu frekuensi juga berhubungan dengan jumlah getaran dengan rumusan sebagai berikut.

$$f = \frac{n}{t}$$

dengan *n* adalah jumlah getaran dan *t* adalah waktu.

Guna mencari frekuensi ketika diketahui panjang gelombang, bagilah kecepatan dengan panjang gelombang.

$$f = \frac{c}{\lambda}$$

Keterangan:

f = frekuensi (Hz)

C = cepat rambat cahaya yaitu 3.000.000.000 m/detik

λ = panjang gelombang

Kanal komunikasi dapat menggunakan berbagai alat sebagai konduktor (kabel) atau serat optik atau biasa disebut komunikasi on-wire, sedangkan kanal komunikasi yang nonfisik disebut komunikasi wireless di mana medianya berupa radio atau gelombang elektromekanik (GEM). Terkadang sebuah kanal dapat membawa informasi secara langsung. Misalnya sinyal audio dapat dipindahkan secara langsung dengan sebuah twisted-pair kabel telepon. Di sisi lain, suatu sambungan/hubungan radio yang putus tidak dapat digunakan untuk menangkap sinyal secara langsung. Sebuah antena yang tinggi dapat dibuat namun itu belum tentu dapat mengirim lebih banyak sinyal yang tanpa gangguan. Ada beberapa kondisi yang membutuhkan pemakaian alat pembawa sinyal yang frekuensinya akan bergerak untuk menyebar pada kanal. Selama proses pengiriman dan penerimaan, sinyal akan mengalami gangguan sebagai akibat dari adanya beberapa distorsi di dalam sistem dan noise yang berupa energi yang tidak

diinginkan dan ada selama proses transmisi. Noise bisa berasal dari kanal (noise internal) maupun dari eksternal. Level sinyal harus lebih besar daripada level noise.

f. Line of Sight (LOS)

Line of Sight (LOS) sebagai suatu kondisi di mana pemancar dapat melihat secara jelas tanpa halangan sebuah penerima. Walaupun terjadi kondisi LOS, belum tentu tidak ada gangguan pada jalur tersebut. Dalam hal ini yang harus diperhitungkan adalah penyerapan, pemantulan, dan pemecahan sinyal. Bahkan dalam jarak yang lebih jauh bumi menjadi sebuah halangan, seperti kontur bumi, gunung, pohon, dan halangan lingkungan lainnya.

Salah satu hal yang penting dalam komunikasi radio pada frekuensi tinggi adalah kondisi line of sight antara pemancar dan penerima. Ada dua jenis line of sight, yaitu optical line of sight sebagai kondisi di mana pemancar dapat melihat secara optik posisi penerima dan radio line of sight sebagai kondisi di mana penerima bisa mendengarkan transmisi dari pemancar. LOS dipengaruhi oleh faktor-faktor sebagai berikut.

Tabel 2. 22 Folder-folder yang Memengaruhi LOS

No.	Faktor	Keterangan
1.	Panjang lintasan	Panjang antara Tx dan Rx.
2.	Faktor K	Faktor pengali jari-jari bumi. Di Indonesia, K: 1,33 atau 4/3.
3.	Kontur bumi	Kondisi permukaan dari bumi yang bisa berupa bukit, lembah, dan lainnya.
4.	Daerah fresnel	Daerah berupa lintasan elips dalam lintasan propagasi gelombang radio di mana daerah tersebut dibatasi oleh gelombang tak langsung (indirect signal) dan memiliki beda panjang lintasan dengan sinyal langsung sebesar kelipatan 1 atau 2 kali 2λ.
5.	Tinggi penghalang	Bisa berupa pohon, gedung, atau bangunan lainnya.

g. Daya

Pola daya merupakan salah satu jenis umum pola radiasi antena yang menggambarkan normalisasi daya terhadap posisi koordinat spheris (koordinat bola) dan pola medan yang menggambarkan normalisasi medan terhadap posisi koordinat spheris. Pola radiasi antena merupakan sebuah gambar grafik yang melambangkan perangkat radiasi antena sebagai sebuah fungsi posisi pada koordinat spheris.

1) Jenis-Jenis Medan Antena
   Jenis-jenis medan antena yaitu medan radiasi dan medan reaktif. Medan radiasi yang merupakan bagian karakteristik medan antena akibat radiasi gelombang (propagasi) yang melambangkan energi dipancarkan oleh antena. Adapun medan reaktif yang merupakan bagian karakteristik medan antena akibat gelombang berdiri yang melambangkan energi yang tersimpan.
2) Daerah-Daerah Medan Antena
   Adapun daerah-daerah medan antena antara lain sebagai berikut.

   a) Daerah medan dekat fresnel sebagai daerah antara medan dekat reaktif dan medan jauh dengan radiasi medan sangat dominan dan distribusi medan tergantung jarak dari antena.
   b) Daerah medan dekat reaktif yang merupakan daerah yang berada di sekitar antena dengan medan raktif sangat dominan (energi tersimpan-gelombang berdiri).
   c) Daerah medan jauh fraunhofer merupakan daerah paling terjauh dari antena dengan distribusi medan secara esensial berdiri sendiri dari jarak antena sumber (propagasi gelombang).
3) Pola Radiasi Antena Beberapa bagian dari pola radiasi antena antara lain sebagai berikut.

   a) Pola isotropis adalah pola sebuah antena didefinisikan sebagai radiasi serba sama ke segala arah, pola ini dibentuk oleh sebuah radiator isotropis (sumber titik, sebuah antena nonfisik yang tidak memiliki arah).
   b) Pola keterarahan merupakan sebuah pola dikarakterisasi oleh beberapa radiasi yang efisien dalam satu arah dibandingkan arah lainnya (secara fisik antena yang dapat direalisasikan adalah antena pengarah saja).
   c) Pola omnidirectional merupakan sebuah pola yang serba sama dalam pemberian ruang radiasinya.
   d) Pola bidang utama yaitu pola bidang E dan bidang H dari sebuah polarisasi linier antena. Bidang E adalah bidang yang terdiri vektor medan elektrik dan arah radiasinya maksimum, sedangkan bidang H adalah bidang yang terdiri vektor medan magnetik dan arah radiasinya maksimum.

Pola yang ditunjukkan menyatakan bahwa antena memiliki pengarahan yang baik, karena sebagian besar energi diradiasikan melalui batasan sempit, yang dinamakan lobe utama (main lobe). Selain itu, pola ini juga memiliki kumpulan bawah, jenis antena kawat (wire antena) dalam praktiknya sering digunakan seperti halnya antena dipole 1/21, antena monopole dengan ground plane, antena loop, antena Yagi-Uda array, antena log periodik dan sebagainya. Antena-antena jenis ini, dimensi fisiknya disesuaikan dengan panjang gelombang di mana sistem bekerja.

h. Bridge Mode

Bridge fungsinya hampir sama dengan repeater tetapi bridge lebih fleksibel dan lebih cerdas dari repeater. Dikatakan lebih fleksibel karena dapat menghubungkan jaringan yang menggunakan metode transmisi yang berbeda-beda. Misalnya bridge dapat mengubungkan antara ethernet baseband dan ethernet broadband. Bridge digunakan untuk menghubungkan antar-jaringan yang memiliki protokol sejenis dengan hasil akhirnya berupa jaringan logis tunggal. Di samping itu, bridge juga dapat digunakan jaringan jaringan yang memiliki media fisik yang berbeda. Misalnya jaringan yang menggunakan fiber optik dengan jaringan yang menggunakan coaxial. Bridge juga bisa digunakan untuk menghubungkan jaringan yang menggunakan jenis kabel berbeda atau pun topologi yang berbeda juga. Bridge dapat mengetahui alamat atau IP dari masing-masing komputer di masing-masing topologi. Bridge mempelajari alamat tujuan lalu lintas yang melewatinya dan mengarahkan ke tujuan, serta digunakan juga untuk menyekat jaringan. Jika jaringan diperlambat dengan adanya lalu lintas yang penuh maka jaringan dapat dibagi menjadi dua kesatuan yang lebih kecil.

i. Repeater Mode

Repeater identik dengan suatu alat yang ber- fungsi untuk memperkuat sinyal dengan cara menerima sinyal dari suatu segmen kabel LAN kemudian dipancarkan kembali dengan kekuatan yang sama dengan sinyal asli ke seg- men kabel yang lain. Jika repeater digunakan dalam dua segmen kabel LAN atau lebih, sebaiknya menggunakan protokol physical layer yang sama antara segmen-segmen kabel tersebut. Beberapa fungsi repeater antara lain untuk memperjauh sinyal dari server (pe- mancar), untuk mengover daerah-daerah yang lemah sinyal dari server (pemancar), dan untuk mempermudah akses sinyal Wi-Fi dari server.

7. Karakteristik Perangkat Jaringan Nirkabel Indoor dan Outdoor

Beberapa karakteristik perangkat jaringan nirkabel indoor dan outdoor diwujudkan dalam bentuk perancangan, instalasi, dan konfigurasi, perangkat jaringan nirkabel outdoor dan indoor.

Terdapat beberapa langkah untuk memulai perancangan jaringan wireless, di mana setiap langkah membutuhkan beberapa perangkat tambahan baik software, hardware, maupun strategi tertentu. Langkah-langkah perancangan jaringan wireless antara lain sebagai berikut.

a. Identifikasi Kegiatan Survei seperti Koordinat, Zona, Channel, dan Noise

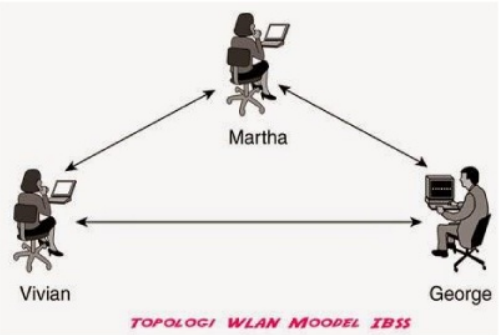
Beberapa hal yang perlu dilakukan untuk identifikasi kegiatan survei antara lain sebagai berikut.

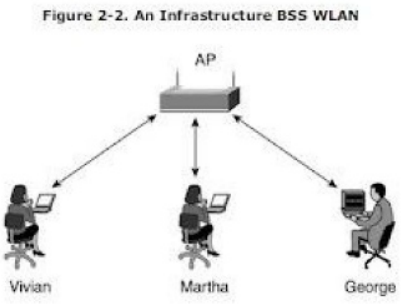
1) Menentukan koordinat letak kedudukan station, jarak udara terhadap BTS dengan GPS dan kompas pada peta.
2) Memperhatikan dan menandai titik potensial penghalang (obstructure) sepanjang path.
3) Menghitung SOM, path dan accessories loss, EIRP, freznel zone, serta ketinggian antena.
4) Memperhatikan posisi terhadap station lain, potensi hidden station, over shoot, dan test noise serta interferensi.
5) Menentukan posisi ideal tower, elevasi, panjang kabel, dan alternatif seandainya ada kesulitan dalam instalasi.
6) Merencanakan berbagai metode alternatif instalasi.

b. Penentuan Kapasitas dan Topologi Jaringan Wireless

Jenis-jenis topologi yang digunakan pada jaringan infrastruktur wireless antara lain sebagai berikut.

1) Independent Basic Service Set (IBBS)
   Jaringan jenis ini dapat terbentuk bila antara client wireless yang dilengkapi dengan wireless LAN card saling terhubung satu sama lain secara langsung. Pada jaringan ini tidak memerlukan perantara seperti access point atau perangkat lainnya. Topologi Ad-Hoc atau IBBS ini memiliki beberapa kelemahan, di antaranya jika client yang terhubung makin banyak maka proses transmisi data akan makin lambat. Selain itu, karena tidak adanya access point yang dijadikan consentrator pada topologi ini, dapat menyebabkan tidak adanya perangkat yang bisa mengatur wireless client yang terkoneksi. Dampaknya adalah collusion atau tabrakan pun sangat sering terjadi.
2) Basic Service Set (BSS)
   Koneksi antara wireless client pada topologi ini menggunakan perantara sebuah perangkat access point. Setiap wireless client yang ingin terhubung dengan client lainnya harus terhubung dahulu dengan access point yang digunakan.





Gambar 2. 35 IBBS dan BSS

3) Extended Service Set (ESS)
   Pada topologi ESS terdapat lebih dari satu access point yang digunakan dengan tujuan untuk menjangkau area yang lebih jauh lagi. Bisa dikatakan topologi ESS ini merupakan gabungan atau kumpulan dari topologi BSS. Pada topologi BSS atau ESS bisa memadukannya dengan jaringan kabel.

c. Mengidentifikasi Interkoneksi Perangkat Jaringan dan Kondisi Channel

Channel dapat diibaratkan seperti sebuah jalan. Peralatan wireless yang mendukung standar protokol 802.11a/b/g menggunakan frekuensi 2,4 GHz memiliki jumlah 14 channel. Pemasangan access point dengan menggunakan frekuensi 2,4 GHz lebih dari satu dalam satu ruangan atau area, harus memperhatikan channel agar tidak terjadi interferensi antar access point yang nanti dapat mengakibatkan kerusakan data.

d. Interferensi

Beberapa sumber noise antara lain sebagai berikut.

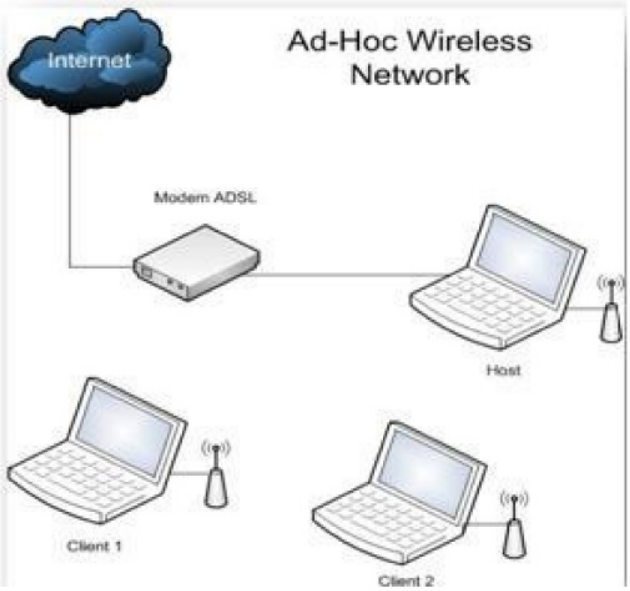
1) Natural noise adalah noise dari atmosfer dan galaksi.
2) Receiver noise adalah noise yang dihasilkan oleh rangkaian internal penerima.
3) Manmade noise adalah sinyal RF yang diambil oleh antena. Termasuk microwave oven, telepon cordless, dan indoor Wi-Fi.
4) Interferensi dari jaringan sendiri adalah terjadi jika menggunakan frekuensi yang sama lebih dari satu kali, menggunakan channel yang tidak memiliki cukup jarak/spasi antar channel-nya, atau menggunakan urusan frekuensi hopping yang tidak benar.
5) Interferensi dari jaringan lain adalah interferensi yang disebabkan oleh jaringan wireless lain yang bekerja pada band yang sama. 6) Interferensi dari sinyal out of band adalah disebabkan oleh sinyal yang kuat di luar frekuensi band yang digunakan, misalnya pemancar FM, AM, TV, pager, maupun radio CB.

8. Topologi Jaringan Nirkabel Indoor dan Outdoor

Topologi pada jaringan LAN (via kabel) tentu berbeda dengan jaringan WLAN (via wireless). Meski secara prinsip sama-sama menghubungkan komputer dengan komputer, namun media transmisi yang digunakan menyebabkan adanya perbedaan jenis topologi antara kedua jaringan ini. Teknologi yang digunakan oleh jaringan WLAN dan LAN juga berbeda, jika pada WLAN menggunakan teknologi wireless (IEEE 802.11) sedangkan jaringan LAN menggunakan teknologi ethernet (IEEE 802.3). Menurut standar IEEE untuk WLAN ada dua model topologi utama, yaitu sebagai berikut.

a. Konfigurasi Ad-Hoc

Jaringan Ad-Hoc merupakan suatu jaringan yang terdiri dari dua atau lebih peranti wireless yang berkomunikasi secara langsung satu sama lain. Sinyal yang dihasilkan oleh interface adapter jaringan Wi-Fi adalah segala arah keluar ke rentang jangkauan yang dipengaruhi oleh faktor-faktor lingkungan, dan juga sifat dari peranti yang terlibat. Jangkauan ini disebut sebagai suatu area layanan dasar (BSA-Basic Service Area). Jika terdapat satu lagi peranti wireless mendekat masuk dalam jangkauan BSA juga bisa berpartisipasi dalam jaringan. Akan tetapi jaringan Ad-Hoc tidaklah transitive, artinya jika dua peranti A dan B saling berkomunikasi dalam jangkauan peranti A, maka jika ada satu peranti C masuk dalam jangkauan peranti B tetapi tidak masuk dalam jangkauan A, maka peranti C tidak bisa berkomunikasi dengan peranti A. Berbeda dengan jaringan infrastruktur, jaringan Ad-Hoc tidak membutuhkan sebuah wireless LAN untuk menghubungkan masing-masing komputer dan topologi jaringan yang terbentuk adalah jaringan mesh.

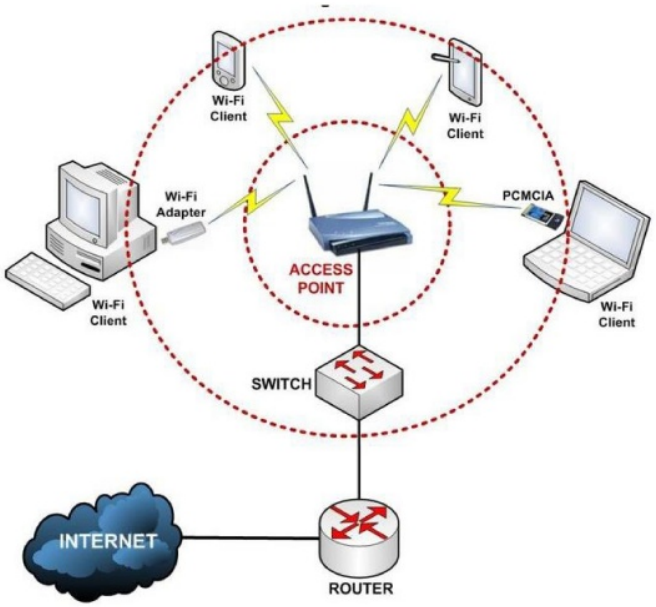


Gambar 2. 36 Jaringan Ad-Hoc

b. Konfigurasi Infrastruktur

Jaringan infrastruktur merupakan jaringan yang menggunakan suatu peranti Wi-Fi yang disebut Access Point (AP) yang berperan sebagai bridge antara peranti wireless dan jaringan kabel standar. Dalam membangun konsep jaringan infrastruktur diperlukan wireless LAN sebagai pusat. Wireless LAN memiliki SSID sebagai nama jaringan wireless tersebut, dengan adanya SSID maka wireless LAN itu dapat dikenali. Pada saat beberapa komputer terhubung dengan SSID yang sama, maka terbentuklah sebuah jaringan infrastruktur. Dengan jaringan infrastruktur dapat melakukan beberapa hal, di antaranya sebagai berikut.

1) Sebuah wireless access point dapat memperluas jaringan LAN Anda dengan kemampuan koneksi secara wireless. Komputer pada jaringan kabel dan komputer dengan koneksi wireless bisa saling berkomunikasi satu sama lain. Hal ini lah yang menjadi kekuatan utama dari topology wireless infrastruktur.
2) Memperluas jangkauan wireless dengan jalan meletakkan sebuah wireless access point di antara dua wireless adapters memperpanjang jangkauan menjadi dua kali lipat.
3) Jika menggunakan beberapa wireless access point seperti halnya dalam sebuah kantor besar atau rumah yang sangat luas, user bisa melakukan roaming antara dua cell access point yang saling terikat, tanpa harus kehilangan koneksi kepada jaringan walau melompat dari satu access point ke access point lainnya. Modus dari wireless access point dengan kemampuan roaming seperti ini disebut WDS (Wireless Distribution Sistem)
4) Dengan infrastruktur topologi bisa berbagi sambungan internet dengan perangkat yang sangat praktis. Dalam berbagi sambungan internet broadband dari sambungan ADSL adalah wireless modem-router yaitu wireless router/ gateway yang memiliki built-in modem ADSL seperti DSL-2640 dari D-Link atau Netgear DGND2000.



Gambar 2. 37 Jaringan Instruktur

Tugas 2.17

Kerjakan Tugas Berikut Secara Mandiri!

1. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan dua model topologi/konfigurasi menurut standar IEEE untuk WLAN. Informasi yang diperoleh dimasukkan table berikut!

No	Jenis Topologi	Keterangan		
		Penggunaan	Kelebihan	Kekurangan
1	Konfigurasi Ad-Hoc			
2	Konfigurasi Infrasturuktur			

2. Tulislah hasil penelusuran Anda di buku tugas!
3. Kumpulkan hasilnya pada guru Anda untuk diberi penilaian!

9. Instalasi dan Konfigurasi Perangkat Jaringan Nirkabel Outdoor dan Indoor

Instalasi wireless tidak sesulit intalasi jaringan kabel, instalasi jaringan tanpa kabel dengan menggunakan teknologi Wi-Fi jauh lebih mudah. Secara prinsip dasar, jaringan Wi-Fi terdisi atas dua komponen yaitu access point dan Wi-Fi NIC, sehingga proses instalasinya pun terdiri atas dua tahap utama sebagai berikut.

a. Proses Instalasi dan Konfigurasi Perangkat Wi-Fi Access Point

Wi-Fi access point identik dengan perangkat yang terdiri atas sebuah hardware dan dilengkapi sistem operasi khusus, fungsi dan perannya sama seperti switch yang terdapat pada jaringan kabel sebagai terminal penghubung bagi wireless klien. Ada beberapa poin yang mesti diperhatikan pada saat instalasi Wi-Fi access point adalah sebagai berikut.

1) Posisi dan Letak Access Point Harus Strategis
   Maksud dari strategis adalah posisi antenanya harus bisa terlihat dari segala sudut, hal ini bertujuan agar sinyal yang dipancarkan oleh access point bisa diterima secara maksimal oleh Wi-Fi client di manapun mereka berada dan masih dalam batas jangkauan sinyal. Hindari halangan yang berbahan material padat seperti beton dan logam karena kedua bahan tersebut sangat memengaruhi kualitas sinyal Wi-Fi jika sampai terhalang oleh kedua jenis bahan tersebut.
2) Letakkan Perangkat Wi-Fi pada Tempat yang Memiliki Sumber Listrik dan Mudah Dijangkau
   Wi-Fi access point adalah perangkat yang menggunakan sumber listrik DC yang kecil daya listriknya namun tetap membutuhkan sumber listrik tersendiri. Posisi

Wi-Fi client juga harus diletakkan sedemikian rupa agar mudah untuk dijangkau jika sesekali terjadi masalah dan membutuhkan troubleshooting.

3) Konfigurasi Wi-Fi Access Point

Setelah ditentukan lokasi yang strategis untuk menempatkan Access Point (AP), maka langkah berikutnya adalah mengatur konfigurasi dari Wi-Fi access point dengan langkah-langkah sebagai berikut.

a) Diawali dengan menyamakan segmen IP antara Wi-Fi AP dengan komputer yang dipakai untuk konfigurasi. IP address default atau bawaan dari pabrik dapat dilihat dimanualnya, biasanya adalah 192.168.1.1 dengan subnet mask 255.255.255.0, setting laptop atau komputer dengan IP address 10 pada bagian akhir dengan subnet mask 255.255.255.0 juga.

b) Sambungkan AP Wi-Fi dengan komputer menggunakan kabel data atau kabel ethernet jenis cross atau jika sudah menggunakan auto MDI/MDIX maka kabel jenis cross atau straight tidak ada masalah.

c) Buka aplikasi web browser dan ketikan alamat IP address dari Wi-Fi AP tersebut. Tekan Enter dan segera muncul tampilan user dan password. Biasanya user dan password default-nya adalah admin dengan password kosong alias tanpa password atau password-nya admin juga. Pastikan tidak ada settingan proxy server pada browser tersebut.

d) Setelah berhasil login dengan admin default maka langkah berikut yang harus dilakukan adalah mengganti password default (admin) dengan password milik sendiri.

e) Konfigurasi mode Access Point (AP) Wi-Fi dengan parameter sebagai berikut.
   - Konfigurasi jenis SSID yang akan dipakai, biasanya secara default SSID yang di-setting menggunakan nama produk tersebut.
   - Pilihan SSID broadcast atau tidak, SSID merupakan salah satu kunci pengaman, dengan tidak melakukan broadcast SSID maka clien yang tidak mengetahui SSID AP tidak bisa terkoneksi.
   - Pilih region negara Anda berada.
   - Pilih channel yang dipakai, jika menggunakan satu AP maka pilih pilihan auto.
   - Pilih mode 802.11 b, g atau n bisa memilih satu dari ketiga mode tersebut atau gabungan dari ketiganya. Sebaiknya pilih mode gabungan dari ketiganya.
   - Channel width atau lebar channel pilih auto saja.

f) Pengaman atau wireless security

Wireless security terdiri atas tiga pilihan, yaitu WEP, WEP2, WPA dan WPA2. WPA2 adalah sistem pengaman dalam dunia wireless yang paling baru dan secure. Selain itu ada pilihan untuk tidak menggunakan sistem pengaman.

g) Pengaturan Khusus
Ada jenis Wi-Fi access point yang memiliki fitur tambahan seperti router dan DHCP server. Pengaturan fungsi router digunakan untuk mengatur koneksi Wi-Fi client agar bisa terkoneksi ke internet, di antaranya memilih jenis mode koneksi internet yang digunakan 3G atau via port WAN, memilih ISP dari koneksi internet, dan mengatur konfigurasi dial sistem dari ISP tersebut. Sedangkan pengaturan DHCP server sebagai access point Wi-Fi yang bertugas untuk mengatur IP address dari Wi-Fi client secara otomatis. Pengaturan tersebut meliputi mengatur mode DHCP menjadi enable, memilih dan menentukan range IP address awal dan akhir yang akan diberikan ke klien, serta menentukan default gateway dan DNS.

h) Simpan semua konfigurasi dan restart perangkat.

Untuk lebih jelasnya, anda dapat melihat video berikut:

b. Proses Instalasi dan Konfigurasi Perangkat Wi-Fi Client

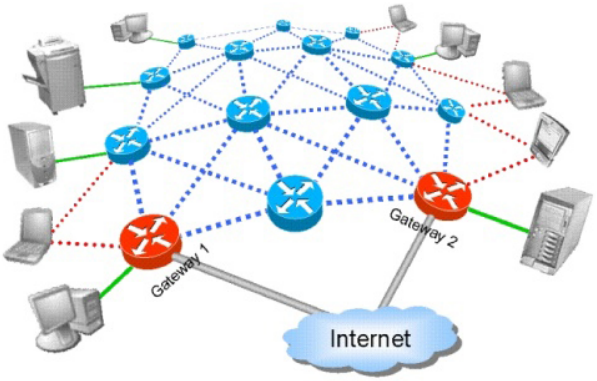
Setelah access point siap maka langkah berikutnya adalah menginstal Wi-Fi client sebagai berikut.

1) Memastikan komputer dalam keadaan mati atau off. Selanjutnya membuka casing komputer dan pasangkan Wi-Fi card ke slot PCI motherboard. Untuk laptop biasanya sudah tersedia Wi-Fi adapter dan tinggal konfigurasi saja.
2) Nyalakan komputer dan pastikan Wi-Fi NIC terdeteksi.
3) Cek pada koneksi wireless tentang SSID yang terlihat.
4) Memilih koneksi sesuai dengan SSID access point yang sudah di-setting, selanjutnya klik dan pilih connect.
5) Masukan key security yang sesuai dan tunggu sampai koneksi terbentuk
6) Setelah koneksi terbentuk maka proses selesai lanjutkan pada komputer client yang lain.

Untuk lebih jelasnya, anda dapat melihat video berikut:

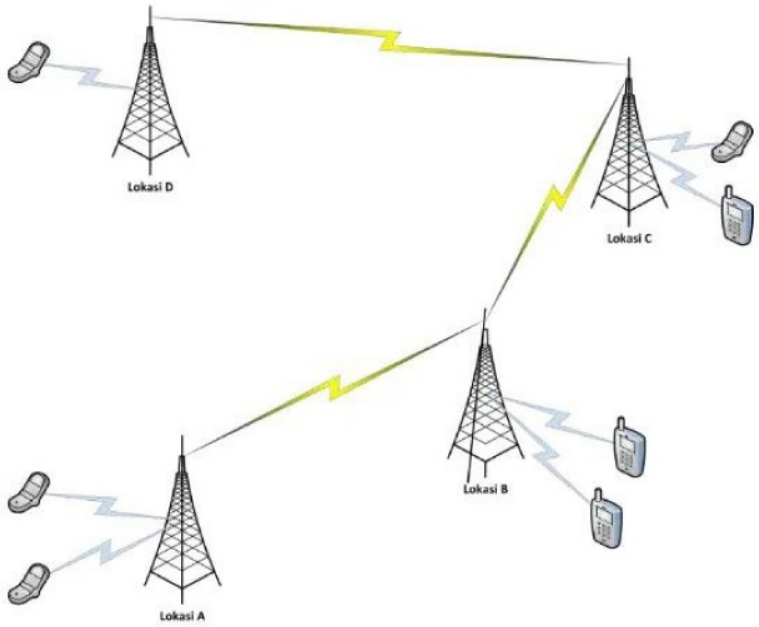
10. Wireless Mesh sebagai Varian dari Teknologi WLAN

Wireless Mesh Network (WMN) sebagai salah satu inovasi varian dari teknologi WLAN menawarkan suatu solusi yang unik karena dapat menggantikan ataupun memperkaya kemampuan infrastruktur jaringan internet yang telah ada, baik yang berbasis kabel maupun nirkabel, secara lebih efektif dan efisien karena mampu mencakup daerah layanan yang lebih luas dan sulit dijangkau tanpa mengesampingkan faktor sekuriti, mobility, dan QoS. Wireless mesh berkembang dengan memadukan antara standar wireless LAN 802.11 a/b/g. Secara teknis standar 802.11a (frekuensi 5,8 GHz) digunakan untuk menghubungkan antara AP, sedangkan standar 802.11b/g berfungsi menghubungkan device client ke AP, Wireless mesh hampir mirip dengan konfigurasi repeater mode, namun lebih diperluas lagi. AP yang digunakan tidak terbatas hanya dua AP namun sudah tergolong banyak bisa lebih dari dua AP. Hubungan antara AP tidak harus point-to-point dan menggunakan jaringan fisik namun sudah ke arah multi-point dan wirelessly.



Gambar 2. 38 Bentuk WMN

WMN merupakan suatu bentuk jaringan komunikasi di mana setiap node termasuk wireless router itu sendiri terhubung dengan menggunakan media wireless. Dalam bentuk jaringan wireless konvensional, setiap client terhubung dengan perangkat router dengan media wireless, namun perangkat wireless router tersebut terhubung ke wireless router lain menggunakan kabel. Wireless Mesh Network (WMN) memberikan solusi penghematan kabel sekaligus menjadikan tingkat mobilitas dari jaringan wireless menjadi lebih tinggi dengan mengganti penggunaan kabel sebagai penghubung antar- perangkat backbone wireless menjadi teknologi wireless yang digunakan untuk pe- nyambungan ke client. Salah satu contoh penerapan dari Wireless Mesh Network (WMN) adalah pada Base Transmission Service (BTS) operator telepon seluler yang menghubungkan satu BTS dengan BTS yang lainnya.



Gambar 2. 39 Visualisasi Topologi WMN pada BTS Telepon Seluler

Tugas 2.18

Kerjakan Tugas Berikut Secara Kelompok!

1. Bentuklah kelompok yang terdiri dari 3-4 anggota!
2. Lakukan penelusuran menggunakan internet atau media cetak yang berkaitan dengan instalasi dan konfigurasi Wi-Fi access point!
3. Praktikkan Langkah-langkah instalasi dan konfigurasi Wi-Fi access point dengan baik dan benar!
4. Hasilnya dimasukkan ke dalam table berikut!

No	Nama Perangkat	Wi-Fi Server	Wi-Fi Client

5. Gunakan informasi dalam table di atas menjadi bahan diskusi kelompok!
6. Presentasikan hasil diskusi kelompok Anda di depan kelas dan mintalah tanggapan dari kelompok lain!