



Kementerian Pendidikan dan Kebudayaan  
Republik Indonesia  
2013



# JARINGAN DASAR

# 1

UNTUK SMK / MAK KELAS X



**Penulis** : SUPRIYANTO  
**Editor Materi** : KADEK  
**Editor Bahasa** :  
**Ilustrasi Sampul** :  
**Desain & Ilustrasi Buku** : PPPPTK BOE MALANG

**Hak Cipta © 2013, Kementerian Pendidikan & Kebudayaan**

**MILIK NEGARA  
TIDAK DIPERDAGANGKAN**

Semua hak cipta dilindungi undang-undang.

Dilarang memperbanyak (merekproduksi), mendistribusikan, atau memindahkan sebagian atau seluruh isi buku teks dalam bentuk apapun atau dengan cara apapun, termasuk fotokopi, rekaman, atau melalui metode (media) elektronik atau mekanis lainnya, tanpa izin tertulis dari penerbit, kecuali dalam kasus lain, seperti diwujudkan dalam kutipan singkat atau tinjauan penulisan ilmiah dan penggunaan non-komersial tertentu lainnya diizinkan oleh perundangan hak cipta. Penggunaan untuk komersial harus mendapat izin tertulis dari Penerbit. Hak publikasi dan penerbitan dari seluruh isi buku teks dipegang oleh Kementerian Pendidikan & Kebudayaan.

Untuk permohonan izin dapat ditujukan kepada Direktorat Pembinaan Sekolah Menengah Kejuruan, melalui alamat berikut ini:

Pusat Pengembangan & Pemberdayaan Pendidik & Tenaga Kependidikan Bidang Otomotif & Elektronika:

Jl. Teluk Mandar, Arjosari Tromol Pos 5, Malang 65102, Telp. (0341) 491239, (0341) 495849, Fax. (0341) 491342, Surel: [vedcmalang@vedcmalang.or.id](mailto:vedcmalang@vedcmalang.or.id), Laman: [www.vedcmalang.com](http://www.vedcmalang.com)



## **DISKLAIMER (*DISCLAIMER*)**

Penerbit tidak menjamin kebenaran dan keakuratan isi/informasi yang tertulis di dalam buku tek ini. Kebenaran dan keakuratan isi/informasi merupakan tanggung jawab dan wewenang dari penulis.

Penerbit tidak bertanggung jawab dan tidak melayani terhadap semua komentar apapun yang ada didalam buku teks ini. Setiap komentar yang tercantum untuk tujuan perbaikan isi adalah tanggung jawab dari masing-masing penulis.

Setiap kutipan yang ada di dalam buku teks akan dicantumkan sumbernya dan penerbit tidak bertanggung jawab terhadap isi dari kutipan tersebut. Kebenaran keakuratan isi kutipan tetap menjadi tanggung jawab dan hak diberikan pada penulis dan pemilik asli. Penulis bertanggung jawab penuh terhadap setiap perawatan (perbaikan) dalam menyusun informasi dan bahan dalam buku teks ini.

Penerbit tidak bertanggung jawab atas kerugian, kerusakan atau ketidaknyamanan yang disebabkan sebagai akibat dari ketidakjelasan, ketidaktepatan atau kesalahan didalam menyusun makna kalimat didalam buku teks ini.

Kewenangan Penerbit hanya sebatas memindahkan atau menerbitkan mempublikasi, mencetak, memegang dan memproses data sesuai dengan undang-undang yang berkaitan dengan perlindungan data.

Katalog Dalam Terbitan (KDT)  
Teknik Komputer Jaringan, Edisi Pertama 2013  
Kementerian Pendidikan & Kebudayaan  
Direktorat Jenderal Peningkatan Mutu Pendidik & tenaga Kependidikan,  
Tahun 2013 : Jakarta



## KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan yang Maha Esa atas tersusunnya buku teks ini, dengan harapan dapat digunakan sebagai buku teks untuk siswa Sekolah Menengah Kejuruan (SMK) Program Keahlian Teknik Komputer Jaringan, Bidang Studi Teknik Komputer dan Informatika, Jaringan Dasar Penerapan kurikulum 2013 mengacu pada paradigma belajar kurikulum abad 21 menyebabkan terjadinya perubahan, yakni dari pengajaran (*teaching*) menjadi belajar (*learning*), dari pembelajaran yang berpusat kepada guru (*teachers-centered*) menjadi pembelajaran yang berpusat kepada peserta didik (*student-centered*), dari pembelajaran pasif (*pasive learning*) ke cara belajar peserta didik aktif (*active learning*) atau *Student Active Learning*.

Buku teks "Jaringan Dasar" ini disusun berdasarkan tuntutan paradigma pengajaran dan pembelajaran kurikulum 2013 diselaraskan berdasarkan pendekatan model pembelajaran yang sesuai dengan kebutuhan belajar kurikulum abad 21, yaitu pendekatan model pembelajaran berbasis peningkatan keterampilan proses sains.

Penyajian buku teks untuk Mata Pelajaran "Jaringan Dasar " ini disusun dengan tujuan agar supaya peserta didik dapat melakukan proses pencarian pengetahuan berkenaan dengan materi pelajaran melalui berbagai aktivitas proses sains sebagaimana dilakukan oleh para ilmuwan dalam melakukan eksperimen ilmiah (penerapan *scientific*), dengan demikian peserta didik diarahkan untuk menemukan sendiri berbagai fakta, membangun konsep, dan nilai-nilai baru secara mandiri.

Kementerian Pendidikan dan Kebudayaan, Direktorat Pembinaan Sekolah Menengah Kejuruan, dan Direktorat Jenderal Peningkatan Mutu Pendidik dan Tenaga Kependidikan menyampaikan terima kasih, sekaligus saran kritik demi kesempurnaan buku teks ini dan penghargaan kepada semua pihak yang telah berperan serta dalam membantu terselesaikannya buku teks siswa untuk Mata Pelajaran Jaringan Dasar Kelas X / Semester 1 Sekolah Menengah Kejuruan (SMK).

Jakarta, 12 Desember 2013

Menteri Pendidikan dan Kebudayaan

Prof. Dr. Mohammad Nuh, DEA



## Daftar Isi

Disklaimer.....	ii
Kata Pengantar.....	iv
Daftar Isi .....	v

### A.Kegiatan Belajar 1: Mengenal Jaringan Komputer

a.Tujuan Pembelajaran .....	1
b.Uraian Materi .....	1
c.Tes Formatif.....	11
d.Lembar Tes Formatif.....	12
e.Lembar Kerja Siswa .....	12

### B.Kegiatan Belajar 2:Mengenal Referensi OSI

a.Tujuan Pembelajaran .....	13
b.Uraian Materi .....	13
c.Tes Formatif.....	23
d.Lembar Jawaban Siswa .....	24
e.Lembar kerja siswa .....	24

### C.Kegiatan Belajar 3:Topologi Jaringan

a.Tujuan Pembelajaran .....	25
b. Uraian Materi .....	25
c. Tes Formatif.....	33
d. Lembar Tes Formatif.....	35
e. Lembar Kerja Siswa .....	35

### D.Kegiatan Belajar 4:Media Jaringan

a.Tujuan Pembelajaran .....	36
b.Uraian Materi .....	36
c.Tes Formati.....	54
d.Lembar Jawab Siswa .....	55
e.Lembar Kerja Siswa .....	55



**E. Kegiatan Belajar 5: Sejarah TCP/IP**

a. Tujuan Pembelajaran .....	56
b. Uraian Materi .....	56
c. Tes Formatif .....	78
d. Lembar Jawab Siswa .....	79
e. Lembar Kerja Siswa .....	79

**F. Kegiatan Belajar 6: Pengalamatan IPV6**

a. Tujuan Pembelajaran .....	80
b. Uraian Materi .....	80
c. Tes Formatif .....	86
d. Lembar Jawaban Kerja Siswa .....	87
e. Lembar kerja Siswa .....	87

**G. Kegiatan Belajar 7: Protokol Pengalamatan**

a. Tujuan Pembelajaran .....	88
b. Uraian Materi .....	88
c. Tes Formatif .....	93
d. Lembar Jawab Siswa .....	94
e. Lembar Kerja Siswa .....	94



## Kegiatan Belajar 1 : Mengenal Jaringan Komputer (PAN, LAN, MAN dan WAN)

### a. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 1 ini siswa diharapkan dapat :

- 1) Memahami Jaringan Komputer (PAN, LAN, MAN dan WAN)
- 2) Menganalisis Jaringan Komputer (PAN, LAN, MAN dan WAN)

### b. Uraian Materi

#### 1. Mengenal Jaringan Komputer (PAN, LAN, MAN dan WAN)

Saat ini hampir setiap komputer yang kita temui merupakan bagian dari sebuah jaringan komputer yang kompleks. Misalkan saja ketika sebuah laptop atau komputer yang tadinya berdiri sendiri (stand alone) kemudian kita tambahkan sebuah USB Modem sehingga terhubung ke internet, maka komputer kita telah terhubung dan merupakan bagian dari sebuah jaringan yang sangat luas yaitu WAN (Wide Area Network). Dalam artikel berikut ini kita akan mencoba mengenal pengertian dari jaringan komputer, manfaat dan resiko dari jaringan komputer dan pembagian jaringan komputer berdasarkan luas areanya yaitu PAN, LAN, MAN dan WAN.

#### **Apakah yang dimaksud dengan jaringan computer ?**

Secara sederhana pengertian dari jaringan komputer adalah hubungan antara dua atau lebih sistem komputer melalui media komunikasi untuk melakukan komunikasi data satu dengan yang lainnya.

#### **Manfaat jaringan computer :**

Manfaat utama yang dapat kita rasakan dari terbentuknya jaringan komputer adalah :

1. Dapat saling berbagi (*sharing*) sumber daya peralatan (devices) secara bersama seperti harddisk, printer, modem, dan lain sebagainya. Dengan demikian terjadi peningkatan efisiensi waktu dalam operasi dan biaya pembelian *hardware*.



2. Dapat saling berbagai (*sharing*) penggunaan *file* yang ada pada *server* atau pada masing-masing *workstation*.
3. Aplikasi dapat dipakai bersama-sama (multiuser)
4. Akses ke jaringan memakai nama, kata sandi, dan pengaturan hak untuk data-data rahasia, sehingga masing-masing pengguna memiliki otorisasi.
5. Komunikasi antar pemakai melalui *email* atau *LAN Conference*.
6. Pengontrolan para pemakai ataupun pemakaian data secara terpusat dan oleh orang-orang tertentu, sehingga meningkatkan keamanan dan dapat melakukan pendelegasian pekerjaan yang sesuai.
7. Mudah dalam melakukan *backup data*, karena manajemen yang tersentralisasi.
8. Tidak tergantung kepada orang yang menyimpan data (apabila orangnya tidak ada) karena penyimpanan data tersentralisasi
9. Data yang selalu *up to date* karena *server* senantiasa memutakhirkan data begitu ada *input (data entry)* diterima.
10. Seorang supervisor/ administrator dapat melakukan pengontrolan pemakai berdasarkan waktu akses, tempat akses, kapasitas pemakaian *hard disk*, mendeteksi pemakai yang tidak berhak, monitor pekerjaan setiap pemakai.

### **Kerugian Jaringan Komputer:**

Sebenarnya istilah tepatnya mungkin bukan kerugian tetapi konsekuensi dari terhubungnya sistem komputer kita ke jaringan komputer ini diantaranya adalah masalah keamanan (*security*) baik pada pengaksesan berbagai sumberdaya dari pihak-pihak yang tidak berwenang maupun masalah keamanan (*ancaman virus*) pada data yang dipertukarkan. Berikut beberapa kerugian dari implementasi jaringan :

1. Biaya yang tinggi kemudian semakin tinggi lagi. pembangunan jaringan meliputi berbagai aspek: pembelian hardware, software, biaya untuk konsultasi perencanaan jaringan, kemudian biaya untuk jasa pembangunan jaringan itu sendiri. Infestasi yang tinggi ini



tentunya untuk perusahaan yang besar dengan kebutuhan akan jaringan yang tinggi. Sedangkan untuk pengguna rumahan biaya ini relatif kecil dan dapat ditekan. Tetapi dari awal juga network harus dirancang sedemikian rupa sehingga tidak ada biaya overhead yang semakin membengkak karena misi untuk pemenuhan kebutuhan akan jaringan komputer ini.

2. Manajemen Perangkat keras Dan Administrasi sistem : Di suatu organisasi perusahaan yang telah memiliki sistem, administrasi ini dirasakan merupakan hal yang kecil, paling tidak apabila dibandingkan dengan besarnya biaya pekerjaan dan biaya yang dikeluarkan pada tahap implementasi. Akan tetapi hal ini merupakan tahapan yang paling penting. Karena Kesalahan pada point ini dapat mengakibatkan peninjauan ulang bahkan konstruksi ulang jaringan. Manajemen pemeliharaan ini bersifat berkelanjutan dan memerlukan seorang IT profesional, yang telah mengerti benar akan tugasnya. Atau paling tidak telah mengikuti training dan pelatihan jaringan yang bersifat khusus untuk kebutuhan kantornya.
3. Sharing file yang tidak diinginkan : *With the good comes the bad*, ini selalu merupakan hal yang umum berlaku (ambigu), kemudahan sharing file dalam jaringan yang ditujukan untuk dipakai oleh orang-orang tertentu, seringkali mengakibatkan bocornya sharing folder dan dapat dibaca pula oleh orang lain yang tidak berhak. Hal ini akan selalu terjadi apabila tidak diatur oleh administrator jaringan.
4. Aplikasi virus dan metode hacking : hal-hal ini selalu menjadi momok yang menakutkan bagi semua orang, mengakibatkan network down dan berhentinya pekerjaan. Permasalahan ini bersifat klasik karena system yang direncanakan secara tidak baik. Masalah ini akan dijelaskan lebih lanjut dalam bab keamanan jaringan.

Terlepas dari berbagai resiko yang harus kita hadapi, rasanya untuk komputer saat ini terhubung atau merupakan bagian dari jaringan komputer merupakan hal yang tidak bisa dihindari.



### Jenis-Jenis Jaringan Komputer

Jenis-jenis jaringan komputer berdasarkan cakupannya dapat dibedakan menjadi beberapa jenis yaitu PAN, LAN, MAN dan WAN.

#### 1. PAN (Personal Area Network)



**Personal Area Network (PAN)** adalah jaringan komputer yang digunakan untuk komunikasi antara komputer perangkat (termasuk telepon dan asisten pribadi digital) dekat dari satu orang. Perangkat mungkin atau tidak milik orang tersebut. Jangkauan dari PAN biasanya beberapa meter. PANs dapat digunakan untuk komunikasi antara perangkat pribadi mereka sendiri (intrapersonal komunikasi), atau untuk menghubungkan ke tingkat yang lebih tinggi dan jaringan Internet (an uplink). Personal area jaringan kabel mungkin dengan komputer bus seperti USB dan FireWire. A wireless personal area network (WPAN) juga dapat dimungkinkan dengan teknologi jaringan seperti IrDA, Bluetooth, UWB, Z-Wave dan ZigBee.

#### Teknologi

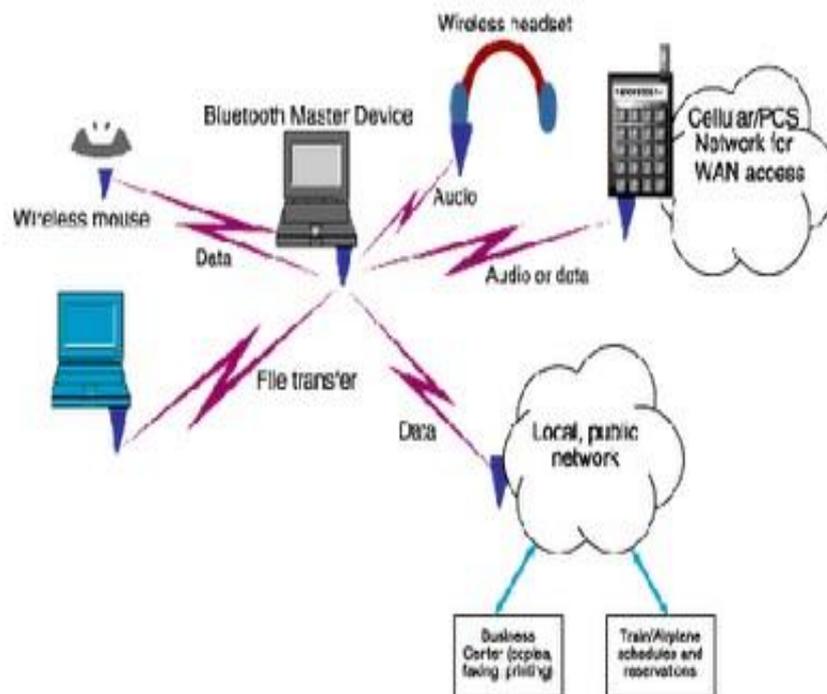
J Bluetooth PAN juga disebut piconet, dan terdiri dari 8 sampai perangkat aktif dalam hubungan tuan-budak (yang sangat besar jumlah perangkat yang dapat dihubungkan pada “parkir” mode). Perangkat



Bluetooth pertama di piconet adalah master, dan semua perangkat yang berkomunikasi dengan slave master. J piconet biasanya memiliki jarak 10 meter, walaupun berkisar hingga 100 meter dapat dijangkau di bawah keadaan ideal.

Inovasi baru dalam Bluetooth antenna ada diizinkan untuk perangkat ini sangat melebihi jangkauan untuk mereka yang pada awalnya dirancang. Pada DEF CON 12, sekelompok hacker yang dikenal sebagai "Flexilis" berhasil tersambung dua perangkat Bluetooth lebih dari setengah mil (800 m) itu. Mereka menggunakan antenna dengan lingkup dan antenna Yagi, semua terpasang ke senapan saham. J terpasang kabel antenna ke Bluetooth kartu di komputer. Mereka kemudian dinamakan antenna "The BlueSniper.". Skinplex, PAN teknologi lain, transmit melalui capacitive dekat bidang kulit manusia. Skinplex dapat mendeteksi dan berkomunikasi hingga satu meter dari tubuh manusia. Sudah digunakan untuk kontrol akses untuk mengunci pintu dan kemacetan perlindungan mobil di atap mobil.

**Wireless PAN**





WPAN (wireless personal area network) adalah jaringan area pribadi – untuk jaringan yang terpusat di sekitar perangkat interconnecting perorangan dari kerja – di mana sambungan nirkabel. Umumnya, personal area jaringan nirkabel menggunakan beberapa teknologi yang memungkinkan komunikasi dalam waktu sekitar 10 meter – dengan kata lain, yang sangat jarak dekat. Salah satu teknologi Bluetooth, yang digunakan sebagai dasar untuk sebuah standar baru, IEEE 802,15.

J WPAN dapat melayani semua interkoneksi ke komputer dan berkomunikasi biasa pada perangkat yang memiliki banyak orang di meja mereka atau membawa mereka dengan hari ini – atau bisa melayani tujuan yang lebih khusus seperti mengizinkan ahli bedah dan anggota tim lainnya untuk berkomunikasi selama suatu operasi. Kunci konsep dalam teknologi WPAN dikenal sebagai “plugging dalam”. Dalam skenario yang ideal, jika dua-WPAN dilengkapi perangkat menjadi dekat (dalam beberapa meter dari satu sama lain) atau dalam waktu beberapa kilometer dari server pusat, mereka dapat berkomunikasi seakan-akan terhubung dengan kabel. Fitur penting lain adalah kemampuan masing-masing untuk mengunci perangkat dari perangkat lain yang selektif, perlu mencegah gangguan yang tidak sah atau akses informasi.

Pada saat kita saling menghubungkan komputer atau perangkat lain seperti handphone, PDA, keyboard, mouse, headset wireless, camera dan peralatan lain yang jaraknya cukup dekat (4-6 meter) maka kita telah membentuk suatu Personal Area Network. Hal yang paling penting bahwa dalam PAN ini kita sendiri yang mengendalikan (authoritas) pada semua peralatan tersebut. Selain dihubungkan langsung ke komputer lewat port USB atau FireWire, PAN juga sering dibentuk dengan teknologi wireless seperti bluetooth, Infrared atau WIFI.



## 2. LAN (Local Area Network)



Local Area Network biasa disingkat LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi Ethernet, saat ini teknologi 802.11b (atau biasa disebut *Wi-fi*) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi *Wi-fi* biasa disebut *hotspot*. Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep *dump terminal*. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti printer. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai. Berbeda dengan Jaringan Area Luas atau Wide Area Network (WAN), maka LAN mempunyai karakteristik sebagai berikut :

1. Mempunyai pesat data yang lebih tinggi
2. Meliputi wilayah geografi yang lebih sempit
3. Tidak membutuhkan jalur telekomunikasi yang disewa dari operator telekomunikasi

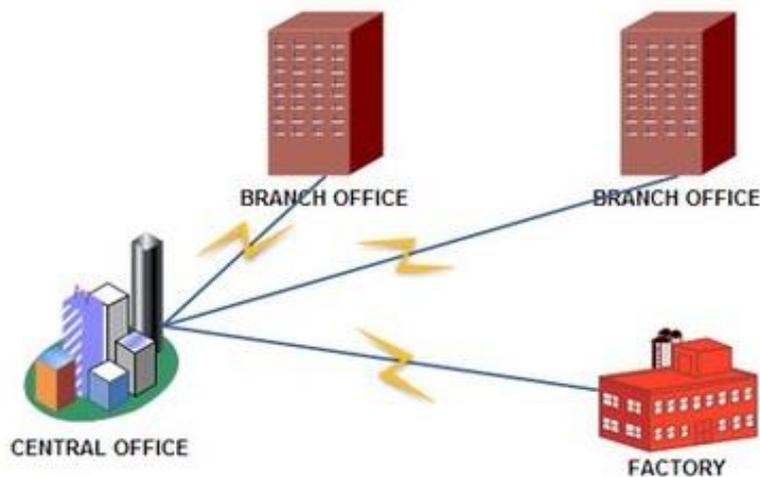


Biasanya salah satu komputer di antara jaringan komputer itu akan digunakan menjadi server yang mengatur semua sistem di dalam jaringan tersebut.

### Prinsip kerja Local Area Network

Prinsip Kerja LAN dapat didefinisikan sebagai network atau jaringan sejumlah system komputer yang lokasinya terbatas didalam satu gedung, satu kompleks gedung atau suatu kampus dan tidak menggunakan media fasilitas komunikasi umum seperti telepon, melainkan pemilik dan pengelola media komunikasinya adalah pemilik LAN itu sendiri. Dari definisi diatas dapat kita ketahui bahwa sebuah LAN dibatasi oleh lokasi secara fisik. Adapun penggunaan LAN itu sendiri mengakibatkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama. LAN yang umumnya menggunakan hub/switch, akan mengikuti prinsip kerja hub itu sendiri. Dalam hal ini adalah bahwa hub tidak memiliki pengetahuan tentang alamat tujuan sehingga penyampaian data secara broadcast, dan juga karena hub hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu. Itulah diantara kelebihan dan kekurangan jaringan LAN

### 3. MAN (Metropolitan Area Network)

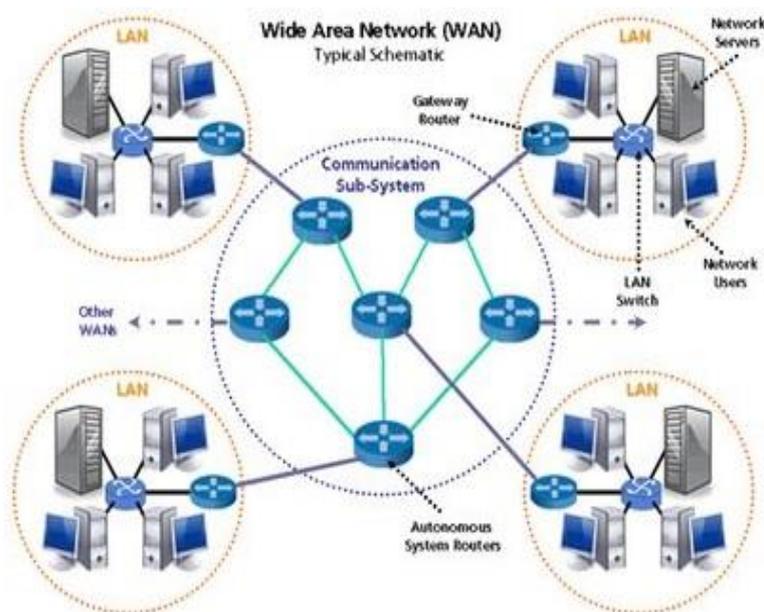




Metropolitan Area Network (MAN) adalah suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi yang menghubungkan berbagai lokasi seperti kampus, perkantoran, pemerintahan, dan sebagainya. Berikut adalah karakteristik MAN yaitu:

1. Meliputi area seluas antara 5 dan 50 kisaran km. Banyak MAN mencakup area perkotaan.
2. Sebuah MAN (seperti WAN) umumnya tidak dimiliki oleh satu organisasi. MAN, komunikasi linknya dan peralatan, umumnya dimiliki oleh salah satu konsorsium pengguna atau oleh penyedia layanan jaringan yang menjual pelayanan kepada pengguna.
3. MAN sering bertindak sebagai jaringan kecepatan tinggi untuk memungkinkan berbagi sumber daya daerah. Hal ini juga sering digunakan untuk menyediakan koneksi bersama untuk jaringan lain dengan menggunakan link ke WAN.
4. MAN berukuran lebih besar dan biasanya memakai teknologi yang sama dengan LAN.
5. Hanya memiliki sebuah atau dua buah kabel dan tidak memiliki elemen switching, yang berfungsi untuk mengatur paket melalui beberapa output kabel . Adanya elemen switching membuat rancangan menjadi lebih sederhana

#### 4. WAN (Wide Area Network)





WAN (Wide Area Network) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. Internet merupakan contoh dari jaringan WAN ini. Jika Wide Area Network sudah mencakup area intercontinental maka disebut jaringan informasi global atau internet.

Disamping pengiriman paket secara datagram, dalam jaringan IP juga dikenal pengiriman paket secara connection oriented dimana sebelum paket dikirim, dilakukan setup koneksi logika dari tempat asal ke tujuan oleh proses packet control dengan request logical connection agar paket suatu informasi menempuh rute yang sama. Mode koneksi ini disebut virtual circuit, tetapi tidak seperti pada jaringan circuit switched yang menduduki kanal (bandwidth/resources) secara monopoli, dalam virtual circuit penggunaan resources masih dalam pola sharing. Dengan cara demikian urutan paket bisa dijamin, tetapi tingkat kontinuitas real time tidak dijamin, sangat bergantung pada kapasitas dan tingkat kepadatan trafik dalam jaringan. Dengan mode virtual circuit ini memungkinkan suatu kelompok organisasi/perusahaan memiliki jaringan privat (semacam jaringan PBX) secara virtual (disebut IP VPN / Virtual Private Network), atau semacam jaringan PBX (Private Branch Exchange) tetapi lingkup area tidak terbatas seperti PABX karena jaringan yang dibangun dalam IP VPN bukan secara fisik melainkan secara logika dan pembentukan jaringan hanya saat diperlukan saja sehingga lingkup jaringan pribadi IP VPN dapat mencakup area nasional bahkan internasional.

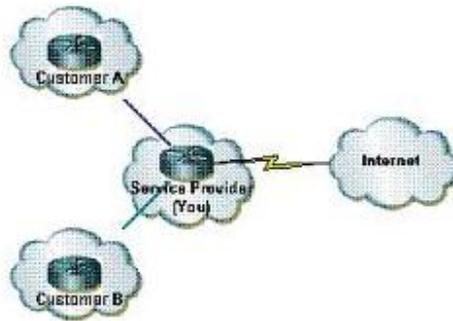
Jaringan berbasis packet switched lain yang banyak dikembangkan di AS adalah jaringan ATM (Asynchronous Transfer Mode). Perbedaannya dengan jaringan IP, bahwa pada jaringan ATM mode koneksi secara keseluruhan menggunakan virtual circuit, sedangkan pada jaringan IP, virtual circuit hanya bersifat option. Perbedaan lain, paket pada jaringan ATM disebut cell selalu tetap yakni 53 oktet (Byte) yang terdiri dari 48 oktet payload, 5 oktet header. Sedangkan dalam jaringan IP, ukuran paket tidak tetap. Teknologi ATM banyak dikembangkan di Amerika Serikat (tidak



dibahas disini). Satu hal lagi, bahwa jaringan ATM dirancang berbasis layanan broadband dan dapat mengakomodasi layanan VBR (Variable Bit Rate) selain CBR (Constant Bit Rate). Sedangkan rancangan awal jaringan IP berbasis Narrow Band dan layanan CBR.

### c. Tes Formatif

1. Tipe jaringan computer yang memiliki ciri: bandwidth yang tinggi dan latency yang rendah, adalah jaringan ...
  - a. LAN
  - b. WAN
  - c. Hybrid
  - d. MAN
  - e. Ring
2. Gambar di bawah ini merupakan komunikasi bridge dengan



konfigurasi ...

- a. Point to point
  - b. Multipoint to Point
  - c. Point to multipoint
  - d. Multipoint to multipoint
  - e. Point to point multipoint
3. Perangkat jaringan yang berfungsi sebagai penghubung / concentrator dalam jaringan wireless adalah ...
  - a. Hub
  - b. Access point
  - c. Bridge
  - d. Switch
  - e. Modem



4. Perintah berbasis teks yang berfungsi untuk memantau koneksi jaringan pada suatu computer, baik itu jaringan local (LAN) maupun jaringan internet adalah ...
  - a. Ping
  - b. Netstat
  - c. Tracert
  - d. Looklan
  - e. Host
  
5. Untuk melihat indikasi pada konfigurasi IP yang terpasang pada computer dengan system operasi windows adalah dengan perintah ...
  - a. ifconfig
  - b. ipconfig
  - c. isconfig
  - d. cpconfig
  - e. isconfig

### **d. Lembar Jawaban Tes Formatif**

1. B. Wan
2. A. Poin to multipoint
3. B. Access point
4. A. PING
5. B. ipconfig

### **e. Lembar Kerja Siswa**



## Kegiatan Belajar 2 : Model Referensi OSI

### a. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 2 ini siswa diharapkan dapat :

- 1). Memahami **Model Referensi OSI**
- 2). Menganalisis **Model Referensi OSI**

### b. Uraian Materi

#### 1. Model Referensi OSI

##### Apa itu OSI?

Mengirim pesan dari satu jaringan ke jaringan yang lain merupakan proses yang sangat kompleks. Sedikit cerita terbentuknya OSI, pada tahun 1977 suatu subcommittee dari International Organization for Standardization (ISO) mulai bekerja untuk membuat beberapa set standard untuk memfasilitasi komunikasi jaringan. Pekerjaan ini selesai pada tahun 1984 dan dikenal sebagai model referensi OSI – Open System Interconnection. Model OSI ini merupakan metoda yang paling luas digunakan untuk menjelaskan komunikasi jaringan. Seksi berikut mencakup topic-topik:

##### 7 Layer model OSI

OSI yang merupakan model referensi dan bukan suatu model fisik membagi tugas-tugas jaringan kedalam 7 layer yang akan dijelaskan lebih detail berikut ini:



1. Layer 7: Application Layer
2. Layer 6: Presentation Layer
3. Layer 5: Session Layer
4. Layer 4: Transport layer
5. Layer 3: Network layer
6. Layer 2: Data link layer
7. Layer 1: Physical layer

Model OSI



Physical layer merupakan layer pertama, akan tetapi biasa dalam model referensi ini ditumpuk pada layer paling bawah untuk menekankan bagaimana suatu pesan di kirim melalui jaringan.

Untuk lebih jelasnya berikut akan dijelaskan secara singkat masing-masing layer OSI dan gue coba analogikan dengan konsep sederhana dari kehidupan kita.

### **Layer 7: Layer Application**

Layer 7 adalah layer Aplikasi mendefinisikan interface antara software-software atau aplikasi yang berkomunikasi keluar dari komputer dimana aplikasi tersebut berada. Layer ini menjelaskan aturan-aturan untuk yang berikut:

1. Penyediaan layanan jaringan
2. Penawaran – pengiklanan layanan jaringan
3. Pengaksesan layanan jaringan

Contoh berikut adalah protocol-protocol yang mengimplementasikan aturan layer Application.

1. Netware's services advertising protocol (SAP)
2. TCP/IP Network File System (NFS)
3. TCP/IP Simple Mail Transfer Protocol (SMTP); Telnet; HTTP; FTP; WWW browser
4. Termasuk dalam contoh ini adalah file; print; aplikasi database; message.

### **Layer 6: Layer Presentasi**

Layer 6 adalah layer presentation dimana tujuan utamanya adalah mendefinisikan format data seperti text ASCII, text EBCDIC, binary, BCD dan juga jpeg. Enkripsi juga didefinisikan dalam layer 6 ini. Layer Presentation menspesifikasikan aturan-2 untuk yang berikut:

1. Penterjemahan Data
2. Enkripsi dan kompresi data

Protocol-2 berikut adalah contoh yang mengimplementasikan aturan layer Presentation

1. Netware Core Protocol (NCP)
2. AppleTalk Filing Protocol (AFP)



3. JPEG; ASCII; EBCDIC; TIFF; GIF; PICT; encryption; MPEG; MIDI  
Misal mainframe mempunyai format EBCDIC; sementara Windows mempunyai format data ASCII. Tugas layer Presentation adalah menterjemahkan format yang berbeda ini sehingga bisa saling nyambung.

#### **Layer 5: Layer Session**

Session layer ini mendefinisikan bagaimana memulai, mengontrol, dan mengakhiri suatu percakapan (disebut session). Hal ini termasuk dalam kendali dan manajemen dari berbagai pesan bidirectional sehingga aplikasi bisa menyertakan suatu sinyal pemberitahuan atau notifikasi jika beberapa pesan telah lengkap. Layer ke lima Session menspesifikasikan aturan-2 berikut:

1. Pengendalian sesi komunikasi antara dua piranti
2. Membuat; mengelola; dan melepas koneksi

Yang berikut adalah protocol yang menimplementasikan layer session model OSI:

1. Netware's Service Advertising Protocol (SAP)
2. TCP/IP remote procedure call (RPC)
3. SQL; NFS; NetBIOS names; AppleTalk ASP; DECnet SCP

Contoh sederhana analoginya adalah operator telpon. Jika anda mau menelpon suatu nomor sementara anda tidak tahu nomornya, maka anda bisa nanya ke operator. Layer session ini analoginya yach kayak operator telpon getu.

#### **Layer 4: layer Transport**

Layer 4 (Transport layer) lebih fokus pada masalah yang berhubungan dengan pengiriman data kepada komputer lain seperti proses memperbaiki suatu kesalahan atau error recovery, segmentasi dari blok data dari aplikasi yang besar kedalam potongan kecil-2 untuk di kirim, dan pada sisi komputer penerima potongan-2 tersebut disusun kembali.

Layer OSI ke 4 ini menspesifikasikan aturan-2 untuk yang berikut:

1. Menyembunyikan struktur jaringan dari layer di atasnya
2. Pemberitahuan kalau data pesan telah diterima
3. Menjamin kehandalan, pengiriman pesan bebas kesalahan



Contoh-2 berikut adalah protocol-2 yg mengimplementasikan aturan layer transport

1. Netware's Sequence Packet Exchange (SPX) protocol
2. TCP/IP's Transmission Control Protocol (TCP)
3. TCP/IP's Domain Name System (DNS)

Analogi dari layer transport ini kayak penyedia jasa pengiriman paket, missal Tiki, POS atau Fedex. Tiki atau Fedex bertanggung jawab penuh untuk sampainya paket ke alamat tujuan dan paket dalam keadaan utuh tanpa cacat. Seperti juga ISP, kalau kita ketikkan WWW.dotkom.com maka ISP akan menterjemahkan kedalam address tujuan.

### **Layer ke 3: Layer Network**

Layer Network dari model OSI ini mendefinisikan pengiriman paket dari ujung-ke-ujung. Untuk melengkapinya pekerjaan ini, Network layer mendefinisikan logical address sehingga setiap titik ujung perangkat yang berkomunikasi bisa diidentifikasi. Layer ini juga mendefinisikan bagaimana routing bekerja dan bagaimana jalur dipelajari sehingga semua paket bisa dikirim.

Layer Network menspesifikasikan aturan-2 untuk yang berikut:

1. Data routing antar banyak jaringan
2. Frakmentasi dan membentuk ulang data
3. Identifikasi segmen kabel jaringan

Protocol-2 berikut menerapkan aturan layer Network

1. Netware's Internetwork Packet Exchange (IPX) Protocol
2. TCP/IP's Internet Protocol (IP); AppleTalk DDP

Analogi dari layer ini tugasnya mengirim surat atau paket ke kota atau kode pos tertentu, tidak langsung di kirim ke alamat tujuan. Layer ini sangat penting dalam jaringan yang kompleks, dimana layer Network mengirim data paket ke jaringan logical. Router berfungsi pada layer ini.

### **Layer ke 2: Data link layer**

Layer Data link menspesifikasikan aturan berikut:

1. Koordinasi bits kedalam kelompok-2 logical dari suatu informasi
2. Mendeteksi dan terkadang juga memperbaiki kesalahan
3. Mengendalikan aliran data



#### 4. Identifikasi piranti jaringan

Protocol-2 berikut mengimplementasikan Data link layer:

1. Ntware's Link Support layer (LSL)
2. Asynchrone Transfer Mode (ATM)
3. IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, IEEE 802.5/802.2

Analogi data link ini seperti surat tercatat yang dikirm pada alamat rumah dan dijamin sampai dengan adanya resi yang ditandatangani penerima. Layer ini mengidentifikasi address yang sesungguhnya dari suatu piranti.

#### **Layer ke 1: Layer Physical**

Layer Physical dari model OSI ini berhubungan dengan karakteristik dari media transmisi. Contoh-2 spesifikasi dari konektor, pin, pemakaian pin, arus listrik, encoding dan modulasi cahaya. Biasanya dalam menyelesaikan semua detail dari layer Physical ini melibatkan banyak spesifikasi. Layer ini menspesifikasikan aturan-2 berikut:

1. Struktur fisik suatu jaringan missal bentuk konektor dan aturan pin pada konektor kabel RJ-45. Ethernet dan standard 802.3 mendefinisikan pemakaian dari kabel pin ke 1,2,3 dan 6 yang dipakai dalam kabel Cat 5 dengan konektor Rj-45 untuk koneksi Ethernet.
2. Aturan mekanis dan elektris dalam pemakaian medium transmisi
3. Protocol Ethernet seperti IBM Token ring; AppleTalk
4. Fiber Distributed Data Interface (FDDI) EIA / TIA-232; V.35, EIA/TIA-449, RJ-45, Ethernet, 802.3, 802.5, B8ZS
5. Sinkronisasi sinyal-2 elektrik melalui jaringan
6. Encoding data secara electronic

Untuk memudahkan anda mengingat model OSI ini gunakan kalimat berikut:

Aku (Application)

Punya (Presentation)

Susu (Session)

Telor (Transport)

MiNum (Network)

Dalam (Data)



Plastik (Physical)

Weleh kok malah gak nyambung ...dah dech pake boso kromo aja biar gampang ngingetnye:

### **Implementasi Protocol**

Perlu diingat bahwa model OSI hanyalah sebuah teori tentang cara melihat komunikasi dalam jaringan. Setiap layer menspesifikasikan standard untuk diikuti saat mengimplementasikan suatu jaringan. Akan tetapi perlu diingat bahwa layer-layer OSI tidak melakukan tugas-tugas yang real, OSI hanyalah model. Bahasan berikut meringkas keuntungan dan kerugian dari penggunaan model OSI dalam mendeskripsikan komunikasi jaringan.

### **Keuntungan dan kerugian model OSI**

Anda mesti faham betul dengan model OSI ini karena ini sangat luas digunakan jika bicara soal komunikasi jaringan. Akan tetapi perlu diingat bahwa ini hanyalah sebuah model teori yang mendefinisikan standards bagi programmer dan system administrator jaringan, jadi bukanlah model layer fisik yang sesungguhnya.

Menggunakan model OSI dalam diskusi konseps jaringan mempunyai beberapa keuntungan:

1. Memberikan bahasa dan referensi yang sama antar sesama professional jaringan
2. Membagi tugas-2 jaringan ke dalam layer-2 logis demi kemudahan dalam pemahaman
3. Memberikan keleluasaan fitur-2 khusus pada level-2 yang berbeda
4. Memudahkan dalam troubleshooting
5. Mendorong standard interoperability antar jaringan dan piranti
6. Memberikan modularity dalam fitur-2 jaringan (developer dapat mengubah fitur-2 tanpa mengubah dengan cara pendekatan keseluruhan), jadi bisa main comot antar modul getu lho

Akan tetapi anda perlu mengetahui beberapa batasan:

1. Layer-2 OSI adalah teoritis dan tidak melakukan fungsi-2 yang sesungguhnya
2. Dalam implementasi industry jarang sekali mempunyai hubungan layer-ke-layer



3. Protocol-2 yang berbeda dalam stack melakukan fungsi-2 yang berbeda yang membantu menerima dan mengirim data pesan secara keseluruhan
4. Implementasi suatu protocol tertentu bisa tidak mewakili setiap layer OSI (atau bisa tersebar di beberapa layer)

Dalam prakteknya, tugas-2 komunikasi jaringan komputer dilaksanakan dengan cara implementasi protocol. Apa sich protocol itu ...nich protocol itu kayak standard industri piranti software khusus vendor yang dipakai dalam proses komunikasi dalam tugas-2 nya melakukan komunikasi jaringan. Berikut ini menjelaskan beberapa konsep penting untuk diketahui mengenai protocol-2 yang sebenarnya.

Kebanyakan vendor dan implementasi standard industry menggunakan suatu pendekatan layer-2. Suatu kumpulan dari standard-2 yang dimaksudkan untuk digunakan secara bersamaan disebut suatu protocol suite atau protocol stack.

Protocol-2 dalam suatu suite mempunyai cirri-2 berikut:

1. Setiap protocol melaksanakan satu atau beberapa tugas komunikasi jaringan
2. Protocol-2 dapat melaksanakan tugas-2 dalam beberapa layer OSI yang berbeda
3. Beberapa protocol dalam suatu suite yang sama dapat melaksanakan tugas yang sama
4. Beberapa protocol suite membolehkan suatu pilihan dari protocol khusus dalam suite untuk melaksanakan suatu tugas khusus atau meng-enable fitur tertentu.
5. Protocol-2 harus bekerja-sama, mengirim dan mnerima data kepada protocol-2 yang lain.

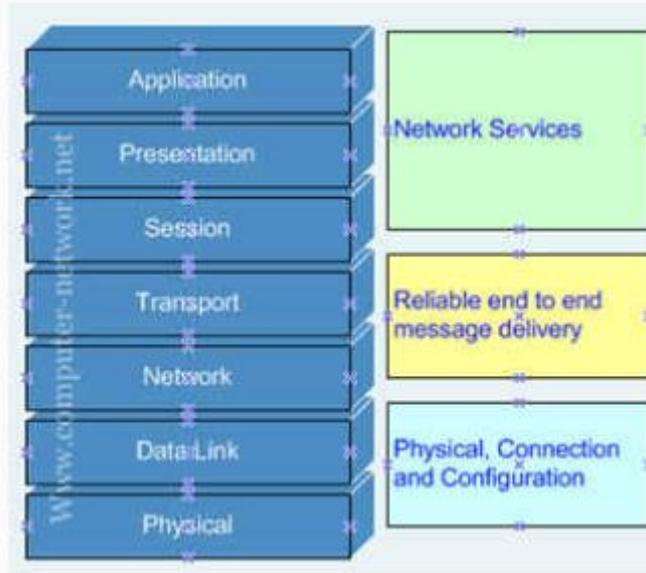
Protocol-2 dapat juga dibagi kedalam satu dari tiga katagori menurut fungsi-2 yang mereka lakukan. Pembagian antar protocol sering jatuh pada tiga macam divisi.

1. Services
2. Transportasi data
3. Koneksi phisik



### Protocol Jaringan

Protocol pada level application bekerja pada layer bagian atas dari model OSI, yaitu: Application; Presentation; Session. Protocol-2 ini melakukan pertukaran data dan komunikasi aplikasi-to-aplikasi.



Model OSI – Network Protocol

Protocol-2 pada level transport (yaitu transport dan network layer) menjalin sesi komunikasi antar komputer; menjamin bahwa data ditransmisikan dengan handal; dan menghadirkan routing antar jaringan.

Protocol-2 pada level physical membentuk hubungan dengan layer bagian bawah dari model OSI (Data link dan Physical layer). Protocol-2 ini menangani informasi; melakukan error-checking; dan mengirim permintaan kirim ulang – (retransmit request).

Catatan:

Beberapa protocol berada pada lebih dari satu level protocol, sehingga protocol-2 bisa jadi tidak klop secara tepat dengan model-2 jaringan. Hal ini dikarenakan suatu protocol dimaksudkan untuk memenuhi suatu tugas tertentu dalam komunikasi, yang mana tidak selalu berhubungan dengan suatu bentuk model.

### Komunikasi antar piranti jaringan

Piranti-2 jaringan bisa berkomunikasi antar sesama dikarenakan bahwa piranti-2 tersebut menjalankan protocol stack yang sama, walaupun mereka menggunakan system operasi yang berbeda. Data yang dikirim dari satu piranti berjalan turun ke protocol stack dibawahnya melalui media



transmisi, dan kemudian naik ke protocol stack pada sisi piranti lawan komunikasinya.

Kedua belah piranti yang saling berkomunikasi harus menggunakan protocol stack yang sama. Suatu pesan data yang dikirim dari satu piranti ke piranti yang lain berjalan melalui proses seperti berikut:

1. Pesan data dipecah kedalam paket-2
2. Setiap protocol didalam stack menambahkan informasi control kedalam paket, meng-enable fitur-2 seperti enkripsi dan error check. Setiap paket biasanya mempunyai komponen berikut: Header , Data , dan Trailer.
3. Pada layer physical, paket-paket dikonversikan kedalam format electrical yang tepat untuk ditransmisikan.
4. Protocol pada masing-2 layer yang berhubungan pada sisi piranti lawannya (pada sisi penerima) akan menghapus header dan trailer yang ditambahkan saat pengiriman. Paket-2 tersebut kemudian disusun kembali seperti data aslinya.

**Catatan:**

Informasi header dan trailer yang ditambahkan pada masing-2 layer OSI dimaksudkan untuk bisa dibaca oleh komputer penerima. Missal, informasi yang ditambahkan pada layer transport pada sisi komputer pengirim akan diterjemahkan oleh layer transport juga pada sisi komputer penerima. Makanya interaksi komunikasi layer OSI ini sering dijelaskan sebagai komunikasi antar peer layer.

Header – Header paket mengandung informasi berikut:

1. Address asal dari komputer pengirim
2. Address tujuan dari pesan yang dikirim
3. Informasi untuk mensinkronkan clock

Data – Setiap paket mengandung data yang merupakan:

1. Data real dari aplikasi, seperti bagian dari file yang dikirim
2. Ukuran data bisa sekitaran 48 bytes sampai 4 kilobytes

Trailer – Trailer paket bisa meliputi:

1. Informasi error-checking
2. Informasi control yang lain yang membantu pengiriman data

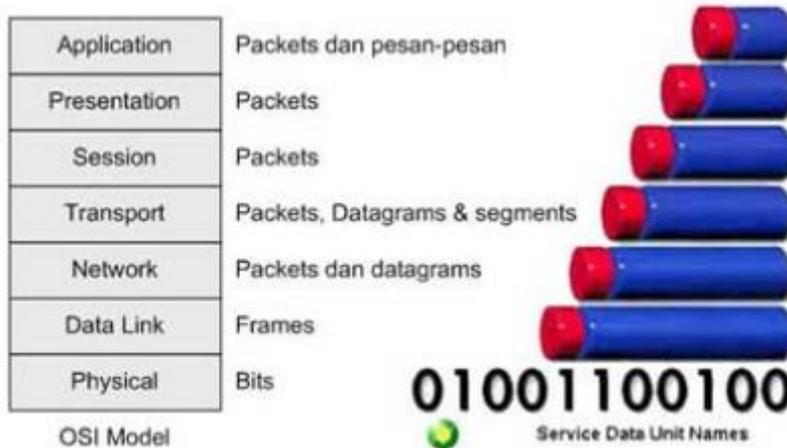


### Process Encapsulation

Adalah process pemecahan suatu pesan kedalam paket-2, penambahan control dan informasi lainnya, dan kemudian mentransmisikan pesan tersebut melalui media transmisi. Anda harus faham betul proses pengiriman pesan ini.

Ada 5 macam step pada proses data encapsulation:

1. Layer bagian atas menyiapkan data yang akan dikirim melalui jaringan
2. Layer transport memecah data kedalam potongan-2 yang disebut segmen, menambah informasi urutan dan juga informasi control.
3. Layer network mengkonversikan segmen kedalam paket-2, menambah logical jaringan, dan menambah address piranti.
4. Layer Data link mengkonversikan paket-2 kedalam frame-2, menambahkan informasi address phisik dari piranti.
5. Layer physical mengkonversikan frame-2 kedalam bit-2 untuk ditransmisikan melalui media transmisi.



Proses encapsulation data pada model OSI

Gunakan ringkasan berikut:

1. Layer bagian atas – Data
2. Layer Transport – Segment
3. Layer Network – paket yang mengandung address logical
4. Layer Data link – frame yang mengandung address physical
5. Layer Physical – bits



**c. Tes Formatif**

1. Model yang mendefinisikan standart untuk menghubungkan komputer-komputer dari vendor-vendor yang berbeda disebut dengan.....
  - A. MODEL OSI 7 LAYER
  - B. TOPOLOGI
  - C. NETWORK SERVICE
  - D. NOS
  
2. Layer yang bertanggung jawab bagaimana data di konversi dan di format untuk transfer data merupakan tanggung jawab dari layer.....
  - A. NETWORK
  - B. PRESENTATION
  - C. TRANSPORT
  - D. SESSION
  - E. PHYSICAL
  
3. Berikut adalah Jenis-Jenis Protocol Jaringan computer kecuali .....
  - A. Ethernet
  - B. NETWORK
  - C. Token Ring
  - D. FDDI
  - E. ATM
  
4. Yang termasuk dalam protocol-protokol pada layer physical yaitu ....
  - A. IEEE 802 (Ethernet standard), repeater, ISDN, TDR
  - B. IEEE 802.2 (Ethernet standard), media access control, logical link control, controls the type of media
  - C. IEEE 802, IEEE 802.2, ISO 2110, ISDN
  - D. ISO 2110, ISDN, media access control, repeater
  
5. Fungsi yang mungkin dilakukan oleh layer network adalah ....
  - A. Mendeteksi error, mendeteksi virus, mengendalikan aliran, koneksi antar peralatan
  - B. Peralatan yang terdapat pada layer network adalah router , memperbaiki error dengan mengirim, menyediakan transfer data yang lebih nyata



- C. Membagi aliran data biner ke paket diskrit panjang tertentu, mendeteksi error, memperbaiki error, memperbaiki error dengan mengirim, mengendalikan aliran, peralatan yang terdapat pada layer ini adalah router
- D. Mendeteksi virus, menyediakan transfer data yang lebih nyata, mengendalikan aliran, koneksi antar peralatan

### **d. Lembar Jawaban Tes Formatif**

1. A. MODEL OSI 7 LAYER
2. B. PRESENTATION
3. B. NETWORK
4. C. IEEE 802, IEEE 802.2, ISO 2110, ISDN
5. C. Membagi aliran data biner ke paket diskrit panjang tertentu, mendeteksi error, memperbaiki error, memperbaiki error dengan mengirim, mengendalikan aliran, peralatan yang terdapat pada layer ini adalah router

### **e. Lembar Kerja Siswa**



## Kegiatan Belajar 3 : TOPOLOGI JARINGAN

### f. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 3 ini siswa diharapkan dapat :

- 1) Memahami Topologi jaringan
- 2) Menganalisis Topologi jaringan

### g. Uraian Materi

#### 1. TOPOLOGI JARINGAN

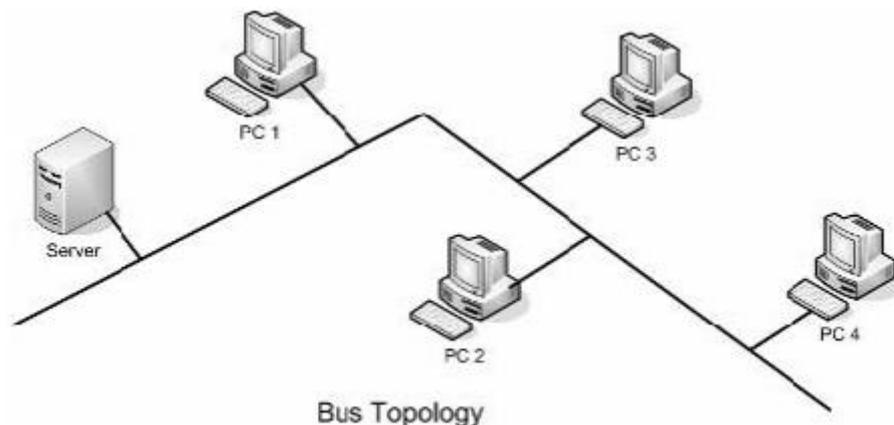
##### Pengertian Topologi Jaringan

Topologi jaringan dalam telekomunikasi adalah suatu cara menghubungkan perangkat telekomunikasi yang satu dengan yang lainnya sehingga membentuk jaringan. Dalam suatu jaringan telekomunikasi, jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan/kerugian dari masing - masing topologi berdasarkan karak teristiknya.

##### Jenis Topologi :

1. Topologi BUS
2. Topologi Star
3. Topologi Ring
4. Topologi Mesh
5. Topologi Extended Star
6. Topologi Hierarchical

##### Topologi BUS





### Karakteristik Topologi BUS

- Node – node dihubungkan secara serial sepanjang kabel, dan pada kedua ujung kabel ditutup dengan terminator.
- Sangat sederhana dalam instalasi
- Sangat ekonomis dalam biaya.
- Paket-paket data saling bersimpangan pada suatu kabel
- Tidak diperlukan hub, yang banyak diperlukan adalah Tconnector pada setiap Ethernet card.
- Problem yang sering terjadi adalah jika salah satu node rusak, maka jaringan keseluruhan dapat down, sehingga seluruh node tidak bisa berkomunikasi dalam jaringan tersebut.

### Keuntungan Topologi BUS

- Topologi yang sederhana
- Kabel yang digunakan sedikit untuk menghubungkan komputer-komputer atau peralatan-peralatan yang lain
- Biayanya lebih murah dibandingkan dengan susunan pengkabelan yang lain.
- Cukup mudah apabila kita ingin memperluas jaringan pada topologi bus.

### Kerugian Topologi BUS

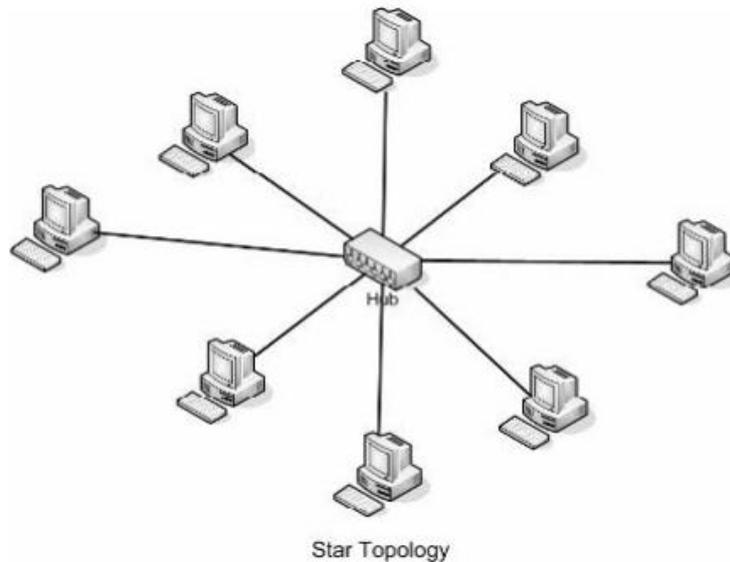
- Traffic (lalu lintas) yang padat akan sangat memperlambat bus.
- Setiap barrel connector yang digunakan sebagai penghubung memperlambat sinyal elektrik yang dikirimkan, dan kebanyakan akan menghalangi sinyal untuk dapat diterima dengan benar.
- Sangat sulit untuk melakukan troubleshoot pada bus.
- Lebih lambat dibandingkan dengan topologi yang lain.

Pada topologi bus 2 ujung jaringan harus diakhiri dgn sebuah **terminator**. **Barel connector** dpt digunakan ukt memperluasnya. Jaringan hanya terdiri dari satu saluran kabel yg menggunakan kabel BNC. Komputer yg ingin terhubung ke jaringan dpt mengkaitkan dirinya dgn men tap Ethernetnya sepanjang kabel.



**Instalasi jaringan Bus** sangat sederhana, murah & maksimal terdiri atas 5-7 komputer. Kesulitan yg sering dihadapi adl kemungkinan terjadinya tabrakan data karena mekanisme jaringan relatif sederhana & jika salah satu node putus maka akan mengganggu kinerja & trafik seluruh jaringan.

### Topologi STAR



Pada topologi star tidak langsung terhubung satu sama lain, tetapi melalui perangkat pusat pengendali (*central controller*) yang biasa disebut dengan HUB.

Pada topologi star, HUB berfungsi layaknya seperti pengatur lalu lintas. Jika satu komputer ingin mengirimkan data ke komputer lainnya maka data tersebut dikirimkan ke HUB terlebih dahulu, yang kemudian meneruskannya ke komputer tujuan (lihat gambar).

Dengan bentuk hubungan seperti itu, kabel yang diperlukan hanyalah sebanyak komputer dalam jaringan dan port I/O juga cukup hanya satu di setiap komputer. Sehingga banyaknya kabel link dan port I/O menjadi lebih sedikit yang berarti bahwa biaya yang dibutuhkan menjadi tidak semahal seperti pada topologi mesh.

### Karakteristik Topologi STAR

- Setiap node berkomunikasi langsung dengan konsentrator (HUB)



- Bila setiap paket data yang masuk ke concentrator (HUB) kemudian di broadcast ke seluruh node yang terhubung sangat banyak (misalnya memakai hub 32 port), maka kinerja jaringan akan semakin turun.
- Sangat mudah dikembangkan
- Jika salah satu ethernet card rusak, atau salah satu kabel pada terminal putus, maka keseluruhan jaringan masih tetap bisa berkomunikasi atau tidak terjadi down pada jaringan keseluruhan tersebut.
- Tipe kabel yang digunakan biasanya jenis UTP.

### **Keuntungan Topologi STAR**

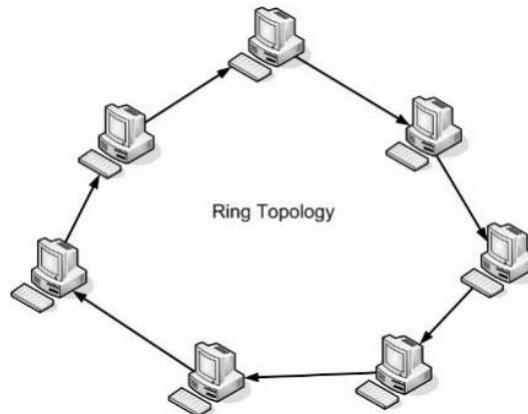
- Cukup mudah untuk mengubah dan menambah komputer ke dalam jaringan yang menggunakan topologi star tanpa mengganggu aktivitas jaringan yang sedang berlangsung.
- Apabila satu komputer yang mengalami kerusakan dalam jaringan maka komputer tersebut tidak akan membuat mati seluruh jaringan star.
- Kita dapat menggunakan beberapa tipe kabel di dalam jaringan yang sama dengan hub yang dapat mengakomodasi tipe kabel yang berbeda.

### **Kerugian Topologi STAR**

- Memiliki satu titik kesalahan, terletak pada hub. Jika hub pusat mengalami kegagalan, maka seluruh jaringan akan gagal untuk beroperasi.
- Membutuhkan lebih banyak kabel karena semua kabel jaringan harus ditarik ke satu central point, jadi lebih banyak membutuhkan lebih banyak kabel daripada topologi jaringan yang lain.
- Jumlah terminal terbatas, tergantung dari port yang ada pada hub.
- Lalulintas data yang padat dapat menyebabkan jaringan bekerja lebih lambat.



## Topologi RING



Topologi Ring hanya menghubungkan secara langsung dua perangkat dalam jaringan (lihat gambar).

Seperti terlihat pada gambar, dengan bentuk topologi yang menyerupai cincin (ring) ini maka sinyal data akan bergerak searah dari satu perangkat ke perangkat lainnya sampai pada akhirnya berhenti di perangkat tujuan. Dengan kata lain, untuk mencapai perangkat D maka sinyal yang dikirimkan dari perangkat A harus melalui perangkat B dan C.

Permasalahannya adalah sinyal akan semakin melemah apabila jarak yang harus ditempuh untuk mencapai tujuan semakin jauh. Karenanya untuk mengatasi lemahnya sinyal data karena kemungkinan menempuh jarak di luar batasan yang dibolehkan, maka setiap perangkat pada topologi ini dilengkapi dengan sebuah repeater. Dengan adanya Repeater, maka sinyal data yang melalui sebuah perangkat akan langsung diperkuat kembali sehingga dapat 'berjalan' terus ke perangkat lainnya, demikian seterusnya sampai pada akhirnya sinyal data tersebut tiba di perangkat tujuan.

### Karakteristik Topologi RING

- Node-node dihubungkan secara serial di sepanjang kabel, dengan bentuk jaringan seperti lingkaran.
- Sangat sederhana dalam layout seperti jenis topologi bus.
- Paket-paket data dapat mengalir dalam satu arah (kekiri atau kekanan) sehingga collision dapat dihindarkan.



- Problem yang dihadapi sama dengan topologi bus, yaitu: jika salah satu node rusak maka seluruh node tidak bisa berkomunikasi dalam jaringan tersebut.
- Tipe kabel yang digunakan biasanya kabel UTP atau Patch Cable (IBM tipe 6).

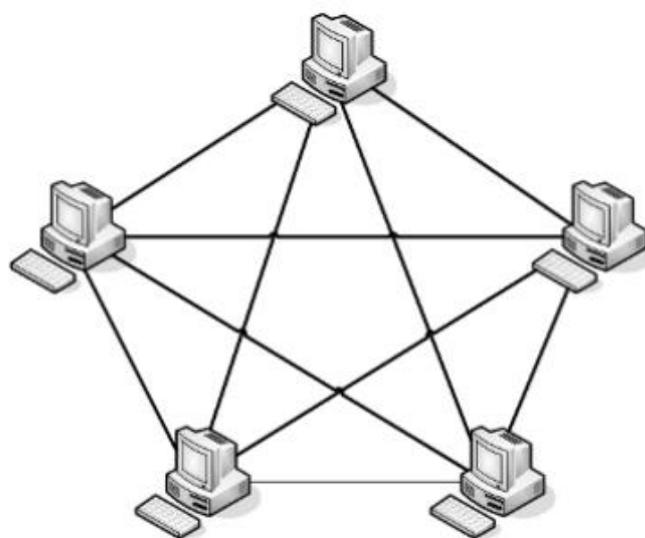
### **Keuntungan Topologi RING**

- Data mengalir dalam satu arah sehingga terjadinya collision dapat dihindarkan.
- Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari server.
- Dapat melayani aliran lalulintas data yang padat, karena data dapat bergerak kekiri atau kekanan.
- Waktu untuk mengakses data lebih optimal.

### **Kerugian Topologi RING**

- Apabila ada satu komputer dalam ring yang gagal berfungsi, maka akan mempengaruhi keseluruhan jaringan.
- Menambah atau mengurangi computer akan mengacaukan jaringan.
- Sulit untuk melakukan konfigurasi ulang.

### **Topologi MESH**



Mesh Topology



### Komponen Pembentuk Utama Topologi Jaringan Mesh

Komponen utama yang biasanya dipakai dalam topologi jaringan mesh ini adalah *Digital Cross Connect* (DXC) dengan satu atau lebih dari dua sinyal *aggregate*, dan tingkat *cross connect* (koneksi persilangan) yang bermacam pada level sinyal SDH.

Topologi jaringan mesh ini menerapkan hubungan antar sentral secara penuh. Banyaknya saluran ini harus disiapkan guna membentuk suatu jaringan topologi mesh yaitu jumlah sentral dikurangi 1 ( $n-1$ , dengan  $n$  adalah jumlah sentral).

Tingkat kesulitan yang terdapat pada topologi jaringan mesh ini sebanding dengan meningkatnya jumlah sentral yang terpasang. Jadi dapat kita ketahui bahwa disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.

### Ciri-ciri dari topologi jaringan mesh

1. Konsep Internet
2. Tidak ada client server, semuanya bisa bertindak sebagai *client dan server*
3. *Peer to peer*
4. Bentuk mesh yang paling sederhana adalah array dua dimensi tempat masing-masing simpul saling terhubung dengan keempat tetangganya.
5. Diameter komunikasi sebuah mesh yang sederhana adalah  $2(n-1)$
6. Koneksi wraparound pada bagian-bagian ujung akan mengurangi ukuran diameter menjadi  $2(n/s)$ .
7. Topologi Mesh ini cocok untuk hal-hal yang berkaitan dengan algoritma yang berorientasi matriks.

### Karakteristik Topologi MESH

- Topologi mesh memiliki hubungan yang berlebihan antara peralatan-peralatan yang ada.
- Susunannya pada setiap peralatan yang ada didalam jaringan saling terhubung satu sama lain.
- jika jumlah peralatan yang terhubung sangat banyak, tentunya ini akan sangat sulit sekali untuk dikendalikan dibandingkan hanya sedikit peralatan saja yang terhubung.



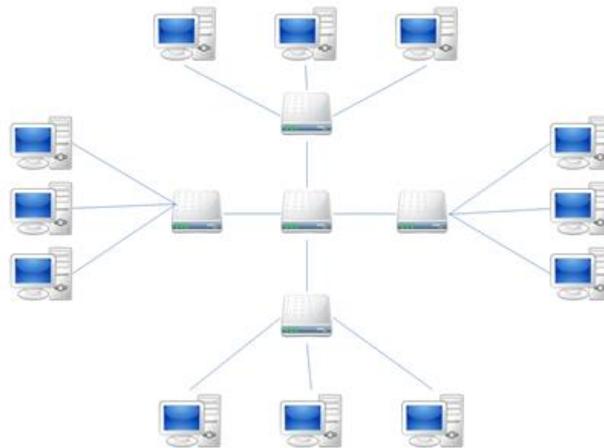
### Keuntungan Topologi MESH

- Keuntungan utama dari penggunaan topologi mesh adalah fault tolerance.
- Terjaminnya kapasitas channel komunikasi, karena memiliki hubungan yang berlebih.
- Relatif lebih mudah untuk dilakukan troubleshooting.

### Kerugian Topologi MESH

- Sulitnya pada saat melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya.
- Biaya yang besar untuk memelihara hubungan yang berlebih.

### Topologi Extended Star



Merupakan topologi yang sama dengan topologi star. Tetapi dalam extended star, memiliki satu atau lebih repeater dalam satu node pusat dan jangkauannya lebih panjang dibandingkan topologi star.

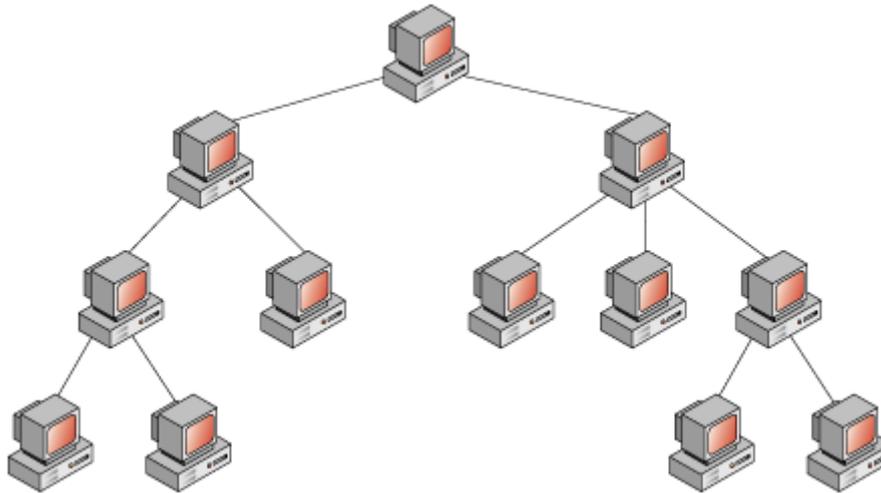
Topologi Extended Star merupakan perkembangan lanjutan dari topologi star dimana karakteristiknya tidak jauh berbeda dengan topologi star yaitu :

1. Setiap node berkomunikasi langsung dengan sub node, sedangkan sub node berkomunikasi dengan central node. traffic data mengalir dari node ke sub node lalu diteruskan ke central node dan kembali lagi.



2. Digunakan pada jaringan yang besar dan membutuhkan penghubung yang banyak atau melebihi dari kapasitas maksimal penghubung.

### Topologi Hierarchy



Topologi hierarchy atau tree ini mempunyai susunan jaringan yang bisa dibayangkan hampir mirip dengan pohon yang bercabang. Topologi ini juga sebenarnya “versi luas” topologi star. Pada topologi ini setiap node memiliki tingkat masing – masing. Node yang memiliki tingkat tinggi diletakkan di atas sedangkan untuk yang memiliki tingkat rendah diletakkan di bawah. Dalam topologi ini sebuah node bisa mempunyai cabang layaknya pohon yang memiliki cabang yang mempunyai cabang lagi.

Data yang dikirim oleh node tertentu harus melewati node pusat (node pusat cabang) untuk sampai pada tujuan. Jadi pada suatu kesempatan, jika node pusat tersebut rusak, maka node tertentu akan kesulitan untuk mengirim data ke node yang letaknya lebih jauh.

### Kelebihan

1. Topologi ini mudah dimanajemen karena adanya pusat node dalam tingkatan masing – masing.
2. Dapat menjangkau jarak yang jauh dengan adanya sifat repeater yang dimiliki hub.

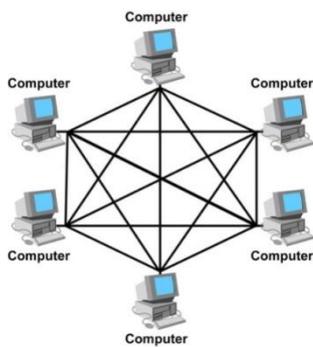


### Kekurangan

1. Jika ada node yang rusak, maka node yang berada di bawahnya akan susah untuk mengirim node yang jauh atau tetangganya.
2. Harus memikirkan secara matang dalam mendesainnya. Karena kabel yang dibutuhkan banyak untuk membuat topologi ini.
3. Sering terjadinya collision.

### c. Tes Formatif

1. Topologi jaringan dibawah ini termasuk topologi ...



- A. Star
  - B. Bus
  - C. Ring
  - D. Tree
  - E. Mesh
2. Tingkat keamanannya tinggi,tidak terjadi tabrakan dalam pengiriman data,merupakan kelebihan dari topologi.....
    - A.Topologi mesh
    - B. Topologi bintang
    - C. Topologi bus
    - D. Topologi pohon
    - E. Topologi cincin
  3. Pada topologi Star, digunakan :
    - A. Repeater
    - B. Hub
    - C. Terminator
    - D. Amplifier
    - E. Tang crimping



4. Berikut ini adalah Topologi jaringan yang menggunakan Hub sebagai pusat transmisi Data, yaitu :
- A. Topologi Star
  - B. Topologi Bus
  - C. Peer To Peer
  - D. Topologi Ring
  - E. Topologi WAN
5. Untuk Menguatkan Sinyal pada kabel jaringan local diperlukan alat :
- A. Bridge
  - B. Repeater
  - C. Gateway
  - D. Amplifier
  - E. Router

#### **d. Lembar Jawaban Tes Formatif**

1. Mesh
2. Topologi cincin
3. Hub
4. Topologi star
5. Repeater

#### **e. Lembar Kerja Siswa**



## Kegiatan Belajar 4 : Media Jaringan

### a. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 4 ini siswa diharapkan dapat :

- a. Memahami **Media Jaringan**
- b. Menganalisis **Media Jaringan**

### b. Uraian Materi

#### 1. Media Jaringan

Perangkat keras yang dibutuhkan untuk membangun sebuah komputer baik hardware maupun software, yaitu minimal dua buah komputer, Network interface card, serta perangkat lain seperti hub, repeater, router, bridge, file server, dan media transmisi.

**Media transmisi** yang digunakan jaringan komputer sebagai sarana penghubung ada dua macam, yaitu sebagai berikut.

#### A. Media Transmisi menggunakan Kabel (Wired Network)

Hampir semua jaringan komputer yang ada saat ini menggunakan kabel sebagai media transmisi. Media transmisi ini memiliki keterbatasan jangkauan dan tidak efisien karena banyak memakai tempat untuk jaringan kabel. Jaringan kabel ini biasanya digunakan dalam area lokal, misalnya dalam satu gedung atau antar gedung dalam satu lembaga pendidikan. Bila sumber data dan penerima memiliki jarak yang tidak terlalu jauh, kabel memang dapat digunakan sebagai media transmisi. Kabel yang sering digunakan sebagai media transmisi antara lain sebagai berikut.

1. Twisted Pair
2. Coaxial
3. Serat optic, dll

#### B. Media Transmisi tanpa Kabel (Wireless Network)

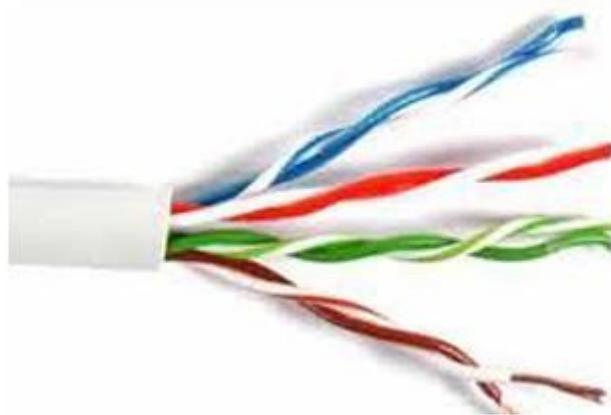
**Media transmisi** tanpa kabel merupakan komunikasi data dalam jaringan komputer yang tidak memanfaatkan kabel sebagai media transmisi, melainkan berupa gelombang elektromagnetik. Jaringan tanpa kabel ini memberikan keunggulan kepada pemakai untuk dapat



mengakses setiap saat di manapun berada. Sedangkan kekurangan media transmisi ini adalah kemampuan transfer data lebih kecil dibandingkan dengan jaringan kabel. Pada media transmisi ini, masih sering terjadi gangguan sehingga memungkinkan terjadinya kehilangan data. Jika sumber data dan penerima data jaraknya cukup jauh atau medannya sulit, maka dapat digunakan media transmisi radiasi elektromagnetik yang dipancarkan melalui udara terbuka berupa:

1. Gelombang Mikro
2. Gelombang radio,dll

### 1. Kabel Unshielded Twisted Pair (UTP)



Gambar kabel UTP

Kabel Unshielded Twisted Pair (UTP) merupakan sepasang kabel yang di-twist/dililit satu sama lain dengan tujuan untuk mengurangi interferensi listrik yang dapat terdiri dari dua, empat atau lebih pasangan kabel (umumnya yang dipakai dalam jaringan komputer terdiri dari 4 pasang kabel / 8kabel). UTP dapat mempunyai transfer rate 10 Mbps sampai dengan 100 Mbps tetapi mempunyai jarak yang pendek yaitu maximum 100m.



**Terdapat 5 kategori kabel UTP :**

1. Category (CAT) 1

Digunakan untuk telekomunikasi telepon dan tidak sesuai untuk transmisi data.

2. Category (CAT) 2

Jenis UTP ini dapat melakukan transmisi data sampai kecepatan 4 Mbps.

3. Category (CAT) 3

Digunakan untuk mengakomodasikan transmisi dengan kecepatan sampai dengan 10 Mbps.

4. Category (CAT) 4

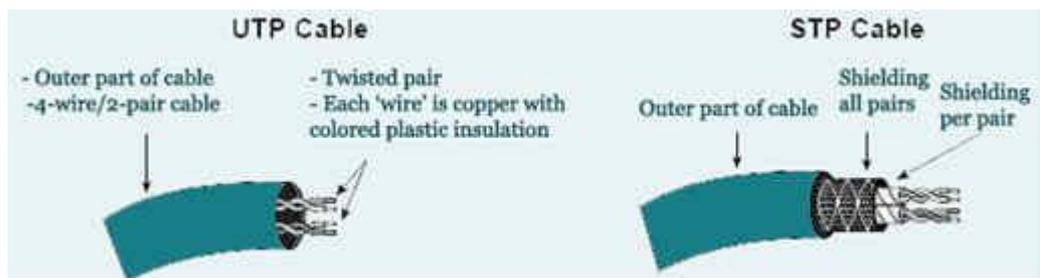
Digunakan untuk mengakomodasikan transmisi dengan kecepatan sampai dengan 16 Mbps.

5. Category (CAT) 5

Merupakan jenis yang paling populer dipakai dalam jaringan komputer di dunia pada saat ini. Digunakan untuk mengakomodasikan transmisi dengan kecepatan sampai dengan 100 Mbps.

**UTP (Unshielded Twisted Pair) dan STP (Shielded twisted pair)**

Ada dua jenis kabel dengan kawat tembaga ini yaitu STP dan UTP, akan tetapi yang paling populer adalah kabel lan UTP.



Gambar diatas ini menunjukkan detail komponen dari kabel lan UTP dan STP.

Kabel lan UTP adalah yang paling populer yang terdiri dari 4 pasang kabel yang saling melilit dengan kode warna khusus yang standard dan diisolasi dengan plastic. Tingkatan dari kabel UTP ini diindikasikan oleh banyak nya lilitan atau pumtiran per inchi, tingkat rendahnya attenuasi, kurang nya tingkat interferensi dan gejala crosstalk. Panjang maksimum per segmen dari kabel lan ini adalah 100 meter saja, jika lebih panjang dari



100 meter maka anda tidak bisa menjamin tingginya tingkat attenuasi. Kecepatan yang bisa dicapai adalah sampai 1 Gigabit yaitu dari jenis kabel lan UTP Cat5e, yang mana jumlah puntiran atau lilitan dari pasangan kabel sedikit lebih banyak per inchi dan ditambah lagi adanya jaket kabel nilon tunggal sebagai insulasi. Jadi sekali lagi grade dari UTP kabel ini ditentukan oleh banyaknya puntiran per inchi.

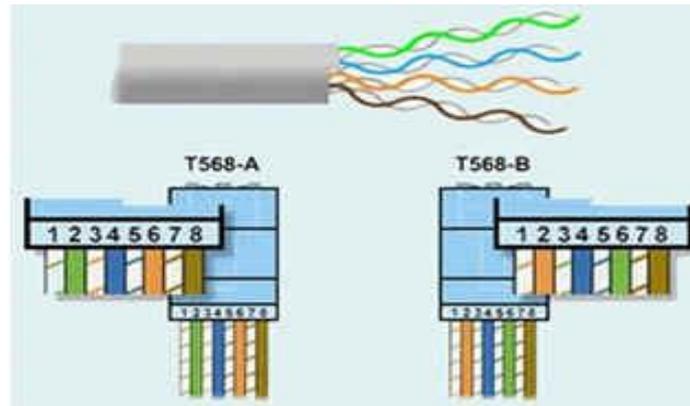
### Standard UTP

1. Kabel lan UTP Cat 1, dipakai untuk jaringan telpon.
2. Kabel lan UTP Cat 2, kecepatan maksimum 4 Mbps, aslinya dimaksudkan untuk mendukung Token Ring lewat UTP.
3. Kabel lan Cat 3, dengan kecepatan maksimum 10 Mbps. Kabel lan ini bisa dipakai untuk jaringan telpon dan merupakan pilihan kabel lan UTP masa silam.
4. Kabel lan UTP Cat 4, kecepatan maksimum adalah 16 Mbps, umum dipakai jaringan versi cepat Token Ring.
5. Kabel lan Cat 5, kecepatan maksimum 1 Gigabps, sangat populer untuk kabel lan desktop.
6. Kabel lan UTP Cat 5e, dengan kecepatan maksimum 1 Gigabps, tingkat emisi lebih rendah, lebih mahal dari Cat 5 akan tetapi lebih bagus untuk jaringan Gigabit.
7. Kabel lan UTP Cat 6, kecepatan maksimum adalah 1 Gigabps+, dimaksudkan sebagai pengganti Cat 5e dengan kemampuan mendukung kecepatan-2 multigigabit.

### Identifikasi UTP

Anda harus terbiasa dengan baik untuk bisa mengidentifikasi cabling ini dengan memeriksa pin-nya. Sebenarnya ada dua macam standard yaitu:

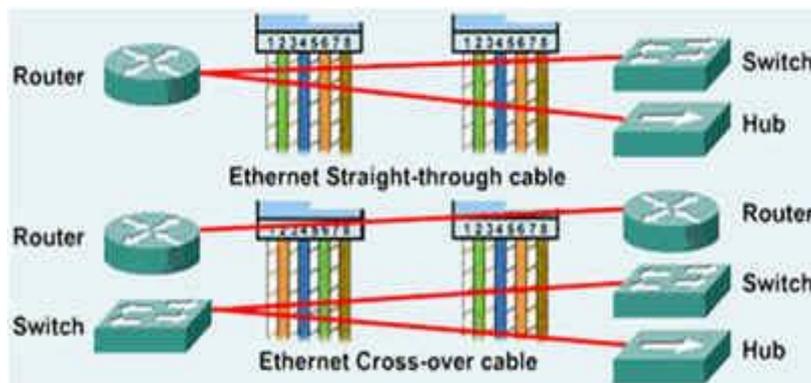
1. T568-A adalah kabel lan UTP jenis straight through, kedua ujung penempatan kabel pada pin-2 konektor RJ-45 adalah sama.
2. T568-B adalah kabel lan UTP jenis cross-over. Anda bisa perhatikan dengan seksama pada kabel cross-over ini, pasangan pin 2 dan 6 dan pasangan pin 1 dan 3 bertukar tempat.



Gambar standard kabel UTPT568-A dan T568-B

### Meghubungkan piranti

Aturan main dari pemakaian kabel ini adalah sebagai berikut, jika untuk menghubungkan dua jenis piranti yang berbeda, gunakan kabel lan UTP straight-through. Sementara jika anda menghubungkan dua piranti yang sejenis, gunakanlah kabel lan cross-over.



Penggunaan cross atau straight UTP cable ke piranti jaringan Kabel UTP (Unshielded Twisted Pair) juga memiliki kelebihan serta kekurangan antara lain

#### Kelebihan :

- a. Murah
- b. mudah diinstalasi
- c. ukurannya kecil

#### Kekurangan :

- a. rentan terhadap interferensi gelombang elektromagnetik
- b. jarak jangkauannya hanya 100m



## 2. Kabel Shielded Twisted Pair (STP)



Gambar 2 kabel STP

Secara fisik kabel shielded sama dengan unshielded tetapi perbedaannya sangat besar dimulai dari konstruksi kabel shielded mempunyai selubung tembaga atau aluminium foil yang khusus dirancang untuk mengurangi gangguan elektrik. Kekurangan kabel STP lainnya adalah tidak samanya standar antar perusahaan yang memproduksi dan lebih mahal dan lebih tebal sehingga lebih susah dalam penanganan fisiknya

Kabel ini terdiri dari 4 pasang kabel yang dipilin (twisted pair), instalasinya mudah, harganya relatif murah dan cukup handal. Kelebihan dan kekurangan dari kabel STP (Shielded Twisted Pair) antara lain :

### **Kelebihan :**

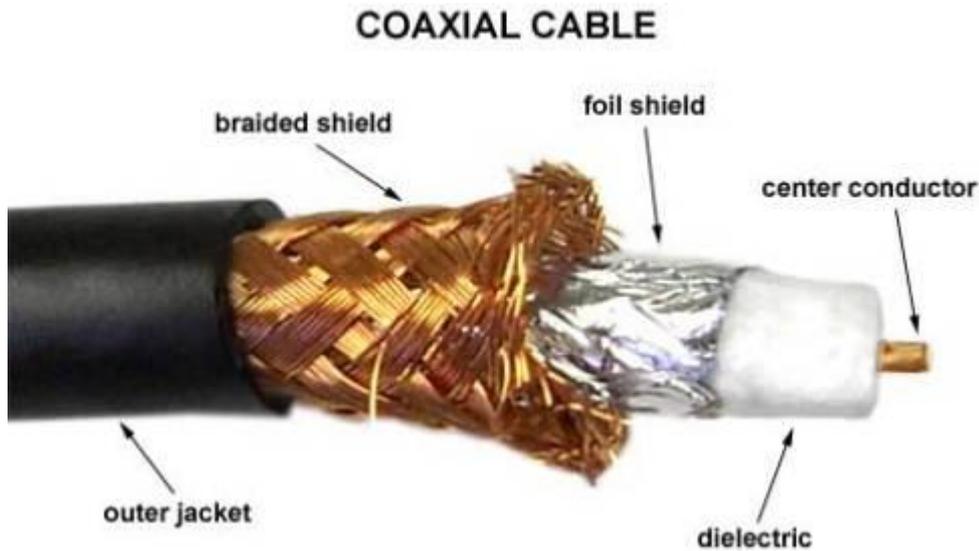
- a. lebih tahan terhadap interferensi gelombang elektromagnetik baik dari dalam maupun dari luar
- b. memiliki perlindungan dan antisipasi tekukan kabel

### **Kekurangan :**

- a. mahal
- b. attenuasi meningkat pada frekuensi tinggi
- c. pada frekuensi tinggi, keseimbangan menurun sehingga tidak dapat mengkompensasi timbulnya "crosstalk" dan sinyal "noise"
- d. susah pada saat instalasi (terutama masalah grounding)
- e. jarak jangkauannya hanya 100m



### 3. Kabel Coaxial

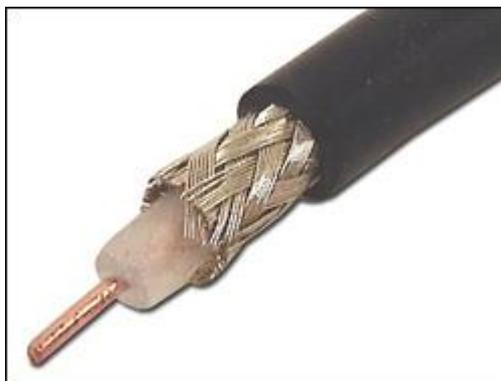


Gambar 3 kabel coaxial

Kabel coaxial terdiri atas dua kabel yang diselubungi oleh dua tingkat isolasi. Tingkat isolasi pertama adalah yang paling dekat dengan kawat konduktor tembaga. Tingkat pertama ini dilindungi oleh serabut konduktor yang menutup bagian atasnya yang melindungi dari pengaruh elektromagnetik. Sedangkan bagian inti yang digunakan untuk transfer data adalah bagian tengahnya yang selanjutnya ditutup atau dilindungi dengan plastik sebagai pelindung akhir untuk menghindari dari goresan kabel. Beberapa jenis kabel coaxial lebih besar dari pada yang lain. Makin besar kabel, makin besar kapasitas datanya, lebih jauh jarak jangkauannya dan tidak begitu sensitif terhadap interferensi listrik.

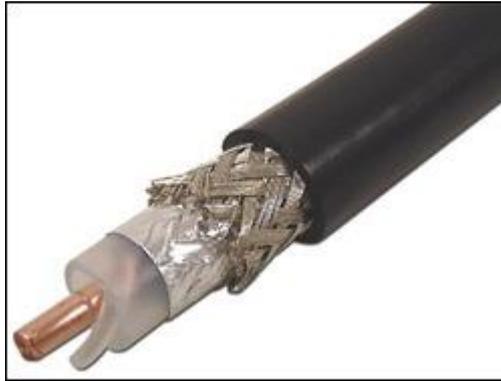
Ada 4 jenis kabel coaxial, yaitu :

- Thinnet atau RG-58 (10Base2)

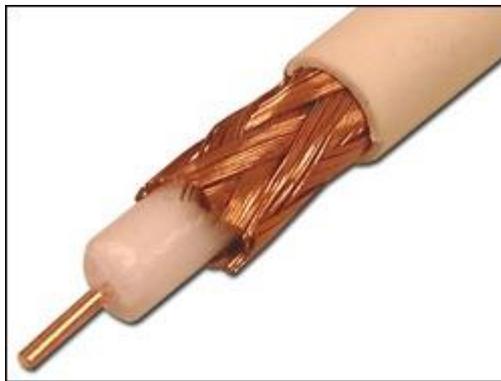




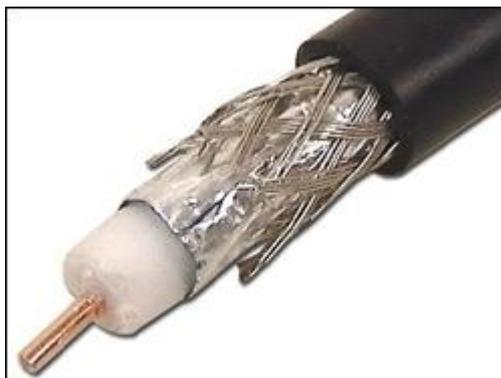
- Thicknet atau RG-8 (10Base5).



- RG-59



- RG-6



**Karakteristik kabel coaxial :**

1. Kecepatan dan keluaran 10 - 100 MBps
2. Biaya Rata-rata per node murah
3. Media dan ukuran konektor medium
4. Panjang kabel maksimal yang di izinkan yaitu 500 meter (medium)



Berikut ini adalah kelebihan serta kekurangan dari penggunaan kabel koaksial :

**Kelebihan :**

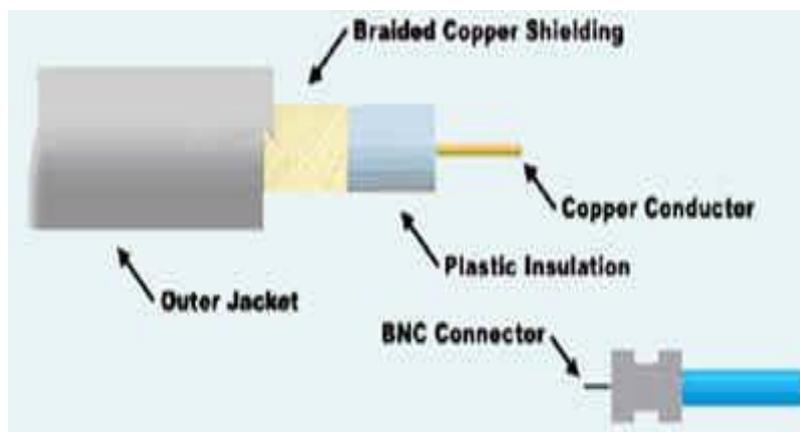
- a. Murah
- b. jarak jangkauannya cukup jauh.
- c. Dapat digunakan untuk menyalurkan informasi sampai dengan 900 kanal telepon
- d. Karena menggunakan penutup isolasi maka kecil kemungkinan terjadi interferensi dengan system lain.

**Kekurangan:**

- a. susah pada saat instalasi
- b. mempunyai redaman yang relative besar, sehingga untuk hubungan jauh harus dipasang repeater-repeater
- c. jika kabel dipasang di atas tanah, rawan terhadap gangguan-gangguan fisik yang dapat berakibat putusnya hubungan

Jaringan yang menggunakan kabel coaxial merupakan jaringan dengan biaya rendah, tetapi jangkauannya sangat terbatas dan keandalannya juga sangat terbatas. Kabel coaxial pada umumnya digunakan pada topologi bus dan ring.

Kabel lan coaxial digunakan pada Ethernet 10Base2 dan 10Base5 beberapa tahun yang lalu. 10Base5 mengacu pada thicknet sementara 10Base2 mengacu pada thinnet sebab 10Base5 dulu menggunakan kabel lan coaxial yang lebih tebal.



Gambar 4 Coaxial cable



Awalnya Ethernet mendasakan jaringannya pada Kabel lan coaxial yang mana bisa membentang sampai 500 meter dalam satu segmen. Kabel lan coaxial ini mahal, dan maksimum hanya sampai kecepatan 10Mbps saja. Kabel lan coaxial ini sekarang sudah tidak populer.

#### 4. Wireless

Jaringan Wireless atau jaringan Wifi memungkinkan kita melakukan komunikasi tanpa melalui kabel jaringan. Akan tetapi piranti jaringan pada Jaringan ini masih perlu berkomunikasi dengan piranti lainnya yang ada pada jaringan kabel LAN. Jaringan wifi menawarkan banyak keuntungan yang tampak (yaitu tanpa kabel) dan juga beberapa hal lain yang mungkin tidak pernah kita pertimbangkan. Yang paling nyata adalah sifat praktisnya mudah dibawa-bawa. Anda bahkan bisa browsing disisi kolam renang anda, di teras rumah, di gazebo anda, di pendopo anda (wah ini kayak rumah di sinetron aja ...?, jika memang ada Jaringan Wireless atau Wifi di rumah anda. Atau bahkan dengan laptop, anda bisa browsing internet di café, di airport, dan banyak lagi tempat-2 yang menyediakan hot-spot layanan Internet gratis demi kenyamanan anda.

Dalam wireless sendiripun tentunya memiliki kelebihan serta kekurangan. Adapun kelebihan serta kekurangannya adalah sebagai berikut:



Gambar wireless

#### Kelebihan:

- a) Dapat dipergunakan untuk komunikasi data dengan jarak yang jauh sekali. Tergantung LOS (Line of Sight) dan kemampuan perangkat wireless dalam memancarkan gelombang.
- b) Sangat baik digunakan pada gedung yang sangat sulit menginstall kabel



### **Kekurangan:**

- a) Sulit diperoleh karena spectrum frekuensi terbatas
- b) Biaya instalasi, operasional dan pemeliharaan sangat mahal  
Keamanan data kurang terjamin
- c) Pengaruh gangguan (derau) cukup besar  
Transfer data lebih lambat dibandingkan dengan penggunaan kabel

### **Menggunakan gelombang radio**

Komunikasi wifi terjadi di-mana-2 disekitar kita, seperti telpon rumah tanpa kabel (cordless) yang memungkinkan terjadinya komunikasi antara telpon cordless anda dengan base unit telpon adalah karena menggunakan gelombang radio. Mirip juga yang terjadi antara telpon cellular GSM anda yang juga menggunakan gelombang radio untuk berkomunikasi kepada jaringan tower transmitter dan receiver disekitarnya. Bahkan remote control TV anda juga memperagakan dasar komunikasi wireless dengan menggunakan gelombang infra merah.

Komunikasi Jaringan Wireless atau Wifi menggunakan bentuk energy elektromagnetik yang merambat melewati ruang. Energy merambat melalui udara pada berbagai panjang gelombang. Tergantung dari panjang gelombang itu sendiri, gelombang energy bisa kelihatan kasat mata ataupun tidak kelihatan. Pada dasarnya energy elektromagnetik dapat menembus melalui materi, akan tetapi tidak jarang materi memantulkan energy pada beberapa derajat dan menyerap sebagian energy juga. Beberapa panjang gelombang energy memerlukan suatu komunikasi untuk bisa terjadi jika berada pada satu garis saling lihat karena panjang gelombang tersebut tidak bisa menembus atau melalui materi itu dengan baik. Sebagai contoh, sebuah remote control televisi anda yang menggunakan gelombang infra merah pada umumnya memerlukan komunikasi segaris lurus, tidak terhalang.

### **Halangan bisa melemahkan gelombang**

Tidak seperti gelombang inframerah, gelombang radio lainnya yang dipakai pada telpon cellular tidak memerlukan komunikasi segaris dengan Tower BTS disekitarnya, akan tetapi berpengaruh juga terhadap ketebalan materi penghalang. Di suatu daerah yang penerimaan sinyal cellular ini



kurang, terkadang kita akan mencari-cari tempat yang agak tinggi atau bahkan disamping bangunan untuk mendapatkan sinyal yang bagus – karena dalam kenyataannya bagian dari bangunan tersebut menyerap sebagian energy dan ada juga yang memantulkannya.

Jaringan Wireless menjadi begitu sangat populer untuk dipasang dirumah-rumah atau di kantor-2. Keuntungan dari komunikasi wireless adalah kurang memerlukan perkabelan dalam jaringan. Kekurangannya adalah dalam hal kecepatan yang biasanya lebih rendah dari kecepatan jaringan kabel, resiko keamanan karena setiap orang disekitar jaringan Wifi ini akan bisa berusaha nguping komunikasi anda, dan juga memerlukan technology extra untuk bisa mendapatkan sinyal yang bagus dalam area yang bisa di jangkau seperti Teknology MIMO.

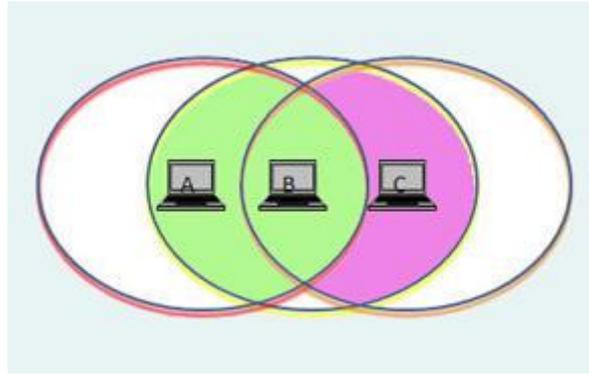
### **Topology Jaringan Wireless**

Dalam jaringan komputer, istilah topology umumnya merujuk pada pola kabel yang digunakan untuk menghubungkan komputer-2. Jaringan Wifi tidak menggunakan kabel, akan tetapi masih mempunyai topology, yang mendefinisikan bagaimana piranti wireless berinteraksi pada layer physical pada model OSI. Pada layer Physical, Jaringan berbasis wireless standard 802.11 menggunakan komunikasi spectrum yang menyebar secara berurutan pada frequency 2.4 GHz, dan piranti-2 tersebut berkomunikasi satu sama lain menggunakan dua dasar topology: ad hoc dan infrastructure.

#### ***Jaringan Ad Hoc***

Suatu jaringan Ad Hoc terdiri dari dua atau lebih piranti wireless yang berkomunikasi secara langsung satu sama lain. Sinyal yang dihasilkan oleh interface adapter Jaringan Wifi adalah berarah Omni keluar ke rentang jangkauan yang dipengaruhi oleh faktor-2 lingkungan, dan juga sifat dari piranti yang terlibat. Jangkauan ini disebut sebagai suatu area layanan dasar (BSA – basic service area).

Jika dua piranti berdelatan pada jangkauan satu sama lain, mereka bisa berkomunikasi satu sama lain, dan segera membentuk 2 node jaringan. Piranti jaringan yang berada pada area layanan dasar disebut suatu set layanan dasar (BSS – basic service set).



Gambar 5 Jaringan Ad-Hoc tidak transitif

### **Jaringan Wireless Ad Hoc**

Jika ada satu lagi piranti wireless mendekat masuk dalam jangkauan BSA ini juga bisa berpartisipasi dalam jaringan. Akan tetapi jaringan Ad Hoc tidaklah transitive, artinya jika dua piranti A dan B saling berkomunikasi dalam jangkauan piranti A, maka jika ada satu piranti C masuk dalam jangkauan piranti B tetapi tidak masuk dalam jangkauan A, maka piranti C tidak bisa berkomunikasi dengan piranti A.

### **Jaringan infrastructure**

Suatu jaringan infrastructure menggunakan suatu piranti Wifi yang disebut Access Point (AP) sebagai suatu bridge antara piranti wireless dan jaringan kabel standard. Suatu Access Point (yang berisi transceiver wireless compliant) adalah suatu unit yang menghubungkan ke jaringan Ethernet (atau jaringan kabel lain) oleh suatu kabel. Jika ada piranti Wifi lain masuk dalam jangkauan wireless Access Point ini maka ia bisa saling komunikasi dengan jaringan kabel, layaknya mereka terhubung dengan kabel saja. Fungsi dari Access Point adalah seperti bridge transparan, yang secara efektif memperpanjang kabel jaringan dengan memasukkan piranti wireless didalamnya.

### **Client berkomunikasi dengan AP**

Dalam jaringan Infrastructure ini, piranti Wifi berkomunikasi dengan access point; mereka tidak berkomunikasi satu sama lain secara langsung. Makanya walaupun jika kedua piranti wireless berada satu jangkauan mereka masih harus menggunakan Access Point untuk bisa saling berkomunikasi.



**Jaringan Wireless / Wireless Network IEEE 802.11**

Jenis yang paling populer dari Jaringan Wireless alias wifi network sekarang ini adalah yang berdasarkan standard 802.11, yang disebut secara informal sebagai jaringan Wifi. Spesifikasi 802.11 mendefinisikan bagaimana dua piranti atau lebih bisa saling mengirim dan menerima data.

**Wifi adalah shared LAN**

Komunikasi Jaringan Wireless adalah merupakan shared LAN – berbagi satu jalur LAN yang sama karena hanya ada satu station saja yang secara efektif dapat mentransmit data pada satu waktu. Standard 802.11 secara effective bisa menjangkau areal sejauh 100 meter saja. Akan tetapi dengan beberapa teknologi khusus sinyal ini juga bisa menjangkau areal lebih luas sampai 300-400 meteran.

Jaringan wifi pada umumnya terdiri dari satu atau beberapa komputer yang dilengkapi adapter wireless, plus satu atau lebih wireless access point (WAP). Fungsi dari WAP ini adalah menjebatani atau mengarahkan traffic dari Jaringan wifi ke jaringan kabel LAN dan sebaliknya. Gambar dibawah ini adalah diagram dari komunikasi computer dengan adapter wireless dan access point.



Gambar 6 contoh wireless

Access point dilengkapi dengan dua buah antenna, yang merupakan komponen dari wireless yang digunakan untuk men-transmit dan receive sinyal radio wireless. Sementara dua laptop juga dilengkapi dengan adapter wifi yang juga mempunyai antenna internal yang memancarkan gelombang radio.

Catatan bahwa 802.11 tidak lagi menggunakan IEEE 802.2 LLC ataupun format address yang didefinisikan 802.3; 802.11 menggunakan



header MAC yang berbeda dari 802.3. Sehingga untuk melewati traffic, access point cukup menukar header 802.11 dengan header 802.3 dan sebaliknya menggunakan address MAC yang sama. Access point mengarahkan traffic dari Wifi network ke jaringan kabel.

### **Standard wireless 802.11**

Ada banyak standard wireless 802.11 yang digunakan secara industri yaitu:

#### **1. Standard wireless-B 802.11b**

- mentransmit pada rate kecepatan sampai 11 Mbps menggunakan frequency band 2.4 GHz, berbagi jaringan dengan keluaran maksimum biasanya secara real terpatok sekitaran 7 Mbps.
- 802.11b mempunyai range yang bagus akan tetapi bisa dipengaruhi oleh interferensi sinyal radio. Banyak dipakai untuk jaringan dirumahan dan banyak kelemahan disisi keamanan.

#### **2. Standard wireless 802.11a,**

- beroperasi pada frequency band 5 GHz dengan transmisi sampai maksimum 54 Mbps.
- Sangat cocok dan bagus pada aplikasi konferensi dan video.
- Bekerja dengan bagus pada populasi yang padat
- Tidak bisa beroperasi pada standard 802.11b/g

#### **3. Standard wireless-G 802.11g**

- Pengembangan dari bersi 802.11b dengan rate kecepatan sampai 54 Mbps
- Jangkauan yang lebih pendek (beberapa jenis piranti wireless-G dikuatkan dengan technology yang bisa mencakup area yang lebih luas seperti technology MIMO)

#### **4. Standard wireless-N 802.11n**

- Bisa mencapai speed sampai 450 Mbps dengan tiga spatial data streams secara teoritis dengan kondisi ideal
- Dengan teknologi MIMO bisa mencakup area sampai 300-400 meteran.

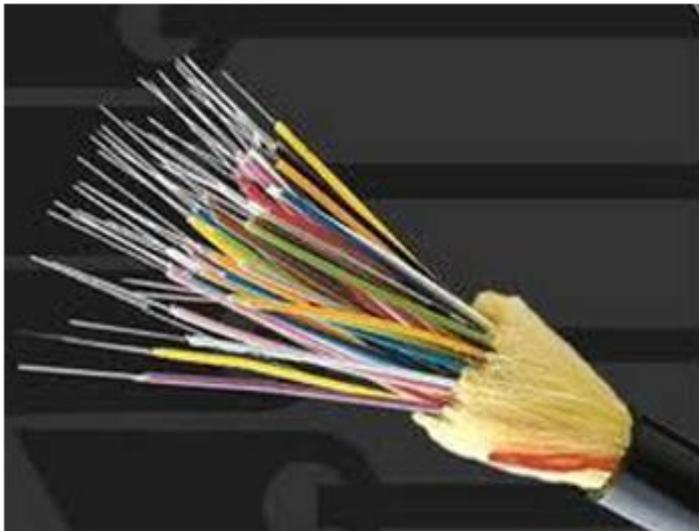
Disamping kecepatannya jauh lebih tinggi dan juga jangkauannya lebih luas, wireless-N ini dilengkapi dengan standard keamanan wireless terkini yaitu Wi-Fi Protected Access (WPA dan WPA2).



### 5. *Standard wireless AC 802.11ac*

802.11ac adalah standard (masih draft) teknologi wifi generasi kelima yang bisa menembus kecepatan sampai 1300Mbps. Banyak sudah diproduksi perangkat wifi dengan teknologi wireless ac ini diantaranya Netgear dengan R6300 wireless ac dual band, Asus RT-AC66, TP-link Archer dan lain-lain.

### 5. Kabel Serat Optik (Fiber Optik)



Gambar7 fiber optic

Jenis kabel fiber optic merupakan kabel jaringan yang jarang digunakan pada instalasi jaringan tingkat menengah ke atas. Pada umumnya, kabel jenis ini digunakan pada instalasi jaringan yang besar dan pada perusahaan multinasional serta digunakan untuk antar lantai atau antar gedung. Kabel fiber optic merupakan media networking medium yang digunakan untuk transmisi-transmisi modulasi.

Fiber Optik harganya lebih mahal di bandingkan media lain. Fiber Optik mempunyai dua mode transmisi, yaitu single mode dan multi mode. Single mode menggunakan sinar laser sebagai media transmisi data sehingga mempunyai jangkauan yang lebih jauh.

Sedangkan multimode menggunakan LED sebagai media transmisi.

#### **Karakteristik kabel fiber optik :**

1. Beroperasi pada kecepatan tinggi (gigabit per detik)
2. Mampu membawa paket-paket dengan kapasitas besar

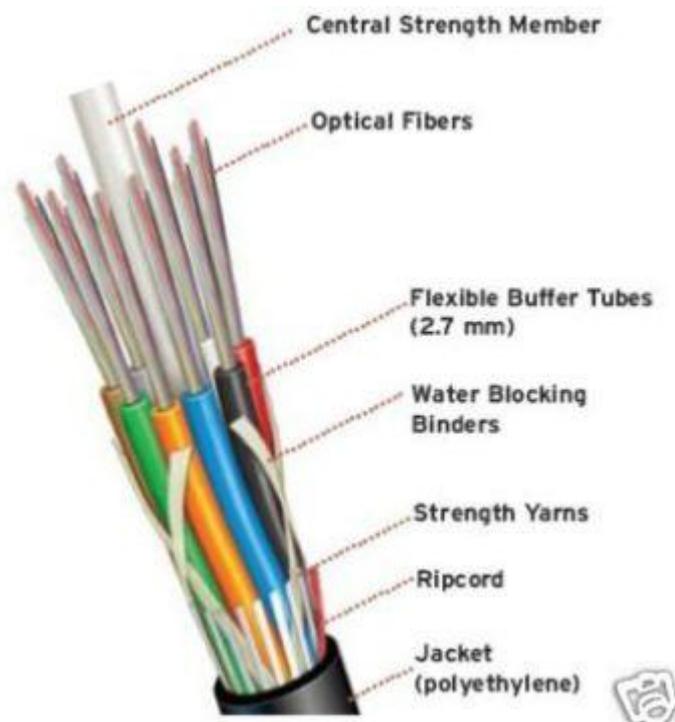


3. Biaya rata-rata pernode cukup mahal
4. Media dan ukuran konektor kecil
5. Kebal terhadap interferensi elektromagnetik
6. Jarak transmisi yang lebih jauh ( 2 - 60 kilometer)

Teknologi fiber optic atau serat cahaya memungkinkan menjangkau jarak yang besar dan menyediakan perlindungan total terhadap gangguan elektrik. Kecepatan transfer data dapat mencapai 1000 mbps serta jarak dalam satu segment dapat lebih dari 3.5 km. kabel serat cahaya tidak terganggu oleh lingkungan cuaca dan panas.

Fiber optic merupakan media transmisi terkini untuk standard Ethernet dalam kabel lan. Perbedaan utama dalam hal fungsi antara kabel fiber optic dan kabel electric adalah sebagai berikut:

- Jarak lebih jauh
- Jauh lebih mahal
- Kurang interferensi magnetic, membuatnya lebih aman
- Dapat menunjang kecepatan sampai 10Gigabits



Gambar 8 Penampang kabel fiber optic



Ada dua macam kabel lan dalam piranti optic ini:

- Multimode (MM), menggunakan ukuran diameter fiber optic lebih luas
- Single mode (SM), menggunakan diameter fiber optic sangat kecil. Jenis ini sangat mahal dikarenakan proses fabrikasinya lebih presisi. Kabel optic ini bisa mencapai jauh lebih panjang dari pada jenis optic MM.

**Konektor optic**

Untuk mentransmisikan data lewat kabel lan optic ini anda memerlukan sebuah strand optic tunggal untuk satu arah. Anda memerlukan dua strand optic untuk kedua arah masing-2 untuk kirim dan terima. Konektor untuk masing ujung dari fiber optic ini umumnya seperti gambar berikut:



Gambar 9 Konektor optic



Di bawah ini merupakan kelebihan serta kekurangan dari fiber optic :

### **Kelebihan:**

- a) kemampuannya yang baik dalam mengantarkan data dengan kapasitas yang lebih besar dalam jarak transmisi yang cukup jauh
- b) kecepatan transmisi yang tinggi hingga mencapai ukuran gigabits, serta tingkat kemungkinan hilangnya data yang sangat rendah.
- c) tingkat keamanan fiber optic yang tinggi, aman dari pengaruh interferensi sinyal radio, motor, maupun kabelkabel yang berada di sekitarnya, membuat fiber optic lebih banyak digunakan dalam infrastruktur perbankan atau perusahaan yang membutuhkan jaringan dengan tingkat keamanan yang tinggi.
- d) aman digunakan dalam lingkungan yang mudah terbakar dan panas.
- e) fiber optic juga jauh lebih kecil dibandingkan dengan kabel tembaga, sehingga lebih menghemat tempat dalam ruangan network data center di mana pun

### **Kekurangan:**

- a) harganya yang cukup mahal jika dibandingkan dengan teknologi kabel tembaga. Hal ini dikarenakan fiber optic dapat mengantarkan data dengan kapasitas yang lebih besar dan jarak transmisi yang lebih jauh
- b) Kekurangan lainnya adalah cukup besarnya investasi yang diperlukan untuk pengadaan sumber daya manusia yang andal, karena tingkat kesulitan implementasi dan deployment fiber optic yang cukup tinggi.

### **c. Tes Formatif**

1. Media Transmisi dapat digolongkan menjadi dua, yaitu :
  - a. Unguided dan Guided
  - b. Guided unplug
  - c. unplug dan Unguided
  - d. Plug dan unplug
2. Dibawah ini merupakan contoh dari Unguided, kecuali :
  - a. Twisted pair



- b. Vacuum
  - c. Propagasi udara
  - d. Air laut
3. Media transmisi yang biasa digunakan untuk jaringan komputer ialah, kecuali :
- a. Kabel tunggal
  - b. Kabel coaxial
  - c. Kabel UTP/STP
  - d. Kabel fiber optic
4. Data rate yang dihasilkan bisa mencapai 20Gbps dengan jarak 10 Km adalah karakteristik dari media transmisi berbentuk :
- a. UTP
  - b. STP
  - c. Fiber Optik
  - d. Coaxial
5. Dibawah ini media transmisi hardware, kecuali :
- a. Udara
  - b. Kabel
  - c. Serat Optik
  - d. Microwave
6. Berikut ini merupakan media transmisi Guided, kecuali :
- a. Kabel Coaxial
  - b. Serat Optik
  - c. Twisted Pair
  - d. Vacuum

#### **d. Lembar Jawaban Tes Formatif**

1. Unguided dan Guided
2. Twisted pair
3. Kabel tunggal
4. Fiber Optik
5. Udara
6. Vacuum

#### **e. Lembar Kerja Siswa**



## Kegiatan Belajar 5 : Sejarah TCP / IP

### a. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 5 ini siswa diharapkan dapat :

1. Memahami **Sejarah TCP / IP**
2. Menganalisis **Sejarah TCP / IP**

### b. Uraian Materi

#### TCP / IP

##### 1. Sejarah TCP/IP

Sejarah TCP/IP dimulainya dari lahirnya ARPANET yaitu jaringan paket switching digital yang didanai oleh DARPA (Defence Advanced Research Projects Agency) pada tahun 1969. Sementara itu ARPANET terus bertambah besar sehingga protokol yang digunakan pada waktu itu tidak mampu lagi menampung jumlah node yang semakin banyak. Oleh karena itu DARPA mendanai pembuatan protokol komunikasi yang lebih umum, yakni TCP/IP. Ia diadopsi menjadi standard ARPANET pada tahun 1983.

Untuk memudahkan proses konversi, DARPA juga mendanai suatu proyek yang mengimplementasikan protokol ini ke dalam BSD UNIX, sehingga dimulailah perkawinan antara UNIX dan TCP/IP. Pada awalnya internet digunakan untuk menunjukan jaringan yang menggunakan internet protocol (IP) tapi dengan semakin berkembangnya jaringan, istilah ini sekarang sudah berupa istilah generik yang digunakan untuk semua kelas jaringan. Internet digunakan untuk menunjuk pada komunitas jaringan komputer worldwide yang saling dihubungkan dengan protokol TCP/IP.

Perkembangan TCP/IP yang diterima luas dan praktis menjadi standar de-facto jaringan komputer berkaitan dengan ciri-ciri yang terdapat pada protokol itu sendiri yang merupakan keunggulan dari TCP/IP, yaitu :

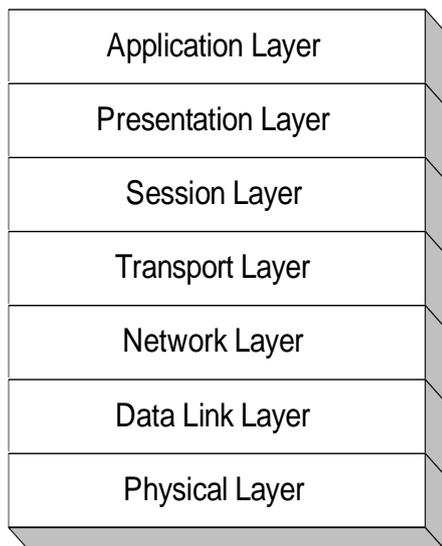
- **Perkembangan protokol TCP/IP menggunakan standar protokol terbuka** sehingga tersedia secara luas. Semua orang bisa mengembangkan perangkat lunak untuk dapat berkomunikasi menggunakan protokol ini. Hal ini membuat pemakaian TCP/IP meluas dengan sangat cepat, terutama dari sisi pengadopsian oleh berbagai sistem operasi dan aplikasi jaringan.



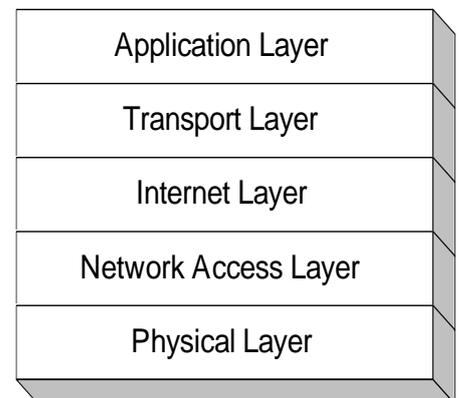
- **Tidak tergantung pada perangkat keras atau sistem operasi jaringan tertentu** sehingga TCP/IP cocok untuk menyatukan bermacam macam network, misalnya Ethernet, token ring, dial-up line, X-25 net dan lain lain.
- **Cara pengalamatan bersifat unik dalam skala global**, memungkinkan komputer dapat mengidentifikasi secara unik komputer yang lain dalam seluruh jaringan, walaupun jaringannya sebesar jaringan *worldwide* Internet. Setiap komputer yang tersambung dengan jaringan TCP/IP (Internet) akan memiliki address yang hanya dimiliki olehnya.
- **TCP/IP memiliki fasilitas routing** dan jenis-jenis layanan lainnya yang memungkinkan diterapkan pada internetwork.

**1.1. Arsitektur dan Protokol Jaringan TCP/IP**

Dalam arsitektur jaringan komputer, terdapat suatu lapisan-lapisan ( *layer* ) yang memiliki tugas spesifik serta memiliki protokol tersendiri. ISO (International Standard Organization) telah mengeluarkan suatu standard untuk arsitektur jaringan komputer yang dikenal dengan nama *Open System Interconnection* ( *OSI* ). Standard ini terdiri dari 7 lapisan protokol yang menjalankan fungsi komunikasi antara 2 komputer. Dalam TCP/IP hanya terdapat 5 lapisan sbb :



Arsitektur OSI



Arsitektur TCP/IP

Gambar 14. Perbandingan Arsitektur OSI dan TCP/IP



Walaupun jumlahnya berbeda, namun semua fungsi dari lapisan-lapisan arsitektur OSI telah tercakup oleh arsitektur TCP/IP. Adapun rincian fungsi masing-masing layer arsitektur TCP/IP adalah sbb :

**Physical Layer** (lapisan fisik) merupakan lapisan terbawah yang mendefinisikan besaran fisik seperti media komunikasi, tegangan, arus, dsb. Lapisan ini dapat bervariasi bergantung pada media komunikasi pada jaringan yang bersangkutan. TCP/IP bersifat fleksibel sehingga dapat mengintegrasikan berbagai jaringan dengan media fisik yang berbeda-beda.

**NetworkAccessLayer** mempunyai fungsi yang mirip dengan *Data Link layer* pada OSI. Lapisan ini mengatur penyaluran data frame-frame data pada media fisik yang digunakan secara handal. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan. Beberapa contoh protokol yang digunakan pada lapisan ini adalah X.25 jaringan publik, Ethernet untuk jaringan Etehernet, AX.25 untuk jaringan Paket Radio dsb.

**InternetLayer** mendefinisikan bagaimana hubungan dapat terjadi antara dua pihak yang berada pada jaringan yang berbeda seperti *Network Layer* pada OSI. Pada jaringan Internet yang terdiri atas puluhan juta host dan ratusan ribu jaringan lokal, lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya dimana pun berada. Oleh karena itu, lapisan ini memiliki peranan penting terutama dalam mewujudkan internetworking yang meliputi wilayah luas (worldwide Internet). Beberapa tugas penting pada lapisan ini adalah:

- **Addressing**, yakni melengkapi setiap datagram dengan alamat Internet dari tujuan. Alamat pada protokol inilah yang dikenal dengan Internet Protocol Address ( IP Address). Karena pengalamatan (*addressing*) pada jaringan TCP/IP berada pada level ini (*software*), maka jaringan TCP/IP independen dari jenis media dan komputer yang digunakan.
- **Routing**, yakni menentukan ke mana datagram akan dikirim agar mencapai tujuan yang diinginkan. Fungsi ini merupakan fungsi terpenting dari Internet Protocol (IP). Sebagai protokol yang bersifat *connectionless*, proses routing sepenuhnya ditentukan oleh jaringan. Pengirim tidak memiliki kendali terhadap paket yang dikirimkannya



untuk bisa mencapai tujuan. Router-router pada jaringan TCP/IP lah yang sangat menentukan dalam penyampaian datagram dari penerima ke tujuan.

**TransportLayer** mendefinisikan cara-cara untuk melakukan pengiriman data antara *end to end host* secara handal. Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima adalah sama dengan informasi yang dikirimkan pada pengirim. Untuk itu, lapisan ini memiliki beberapa fungsi penting antara lain :

- **FlowControl.** Pengiriman data yang telah dipecah menjadi paket-paket tersebut harus diatur sedemikian rupa agar pengirim tidak sampai mengirimkan data dengan kecepatan yang melebihi kemampuan penerima dalam menerima data.
- **Error Detection.** Pengirim dan penerima juga melengkapi data dengan sejumlah informasi yang bisa digunakan untuk memeriksa data yang dikirimkan bebas dari kesalahan. Jika ditemukan kesalahan pada paket data yang diterima, maka penerima tidak akan menerima data tersebut. Pengirim akan mengirim ulang paket data yang mengandung kesalahan tadi. Namun hal ini dapat menimbulkan *delay* yang cukup berarti.

Pada TCP/IP, protokol yang dipergunakan adalah *Transmission Control Protocol* (TCP) atau *User Datagram Protocol* (UDP). TCP dipakai untuk aplikasi-aplikasi yang membutuhkan keandalan data, sedangkan UDP digunakan untuk aplikasi yang membutuhkan panjang paket yang pendek dan tidak menuntut keandalan yang tinggi. TCP memiliki fungsi *flow control* dan *error detection* dan bersifat *connection oriented*. Sebaliknya pada UDP yang bersifat *connectionless* tidak ada mekanisme pemeriksaan data dan *flow control*, sehingga UDP disebut juga *unreliable protocol*. Untuk beberapa hal yang menyangkut efisiensi dan penyederhanaan, beberapa aplikasi memilih menggunakan UDP sebagai protokol transport. Contohnya adalah aplikasi database yang hanya bersifat *query* dan *response*, atau aplikasi lain yang sangat sensitif terhadap delay seperti *video conference*. Aplikasi seperti ini dapat mentolerir sedikit kesalahan (gambar atau suara masih bisa dimengerti), namun akan tidak nyaman untuk dilihat jika terdapat delay yang cukup berarti.

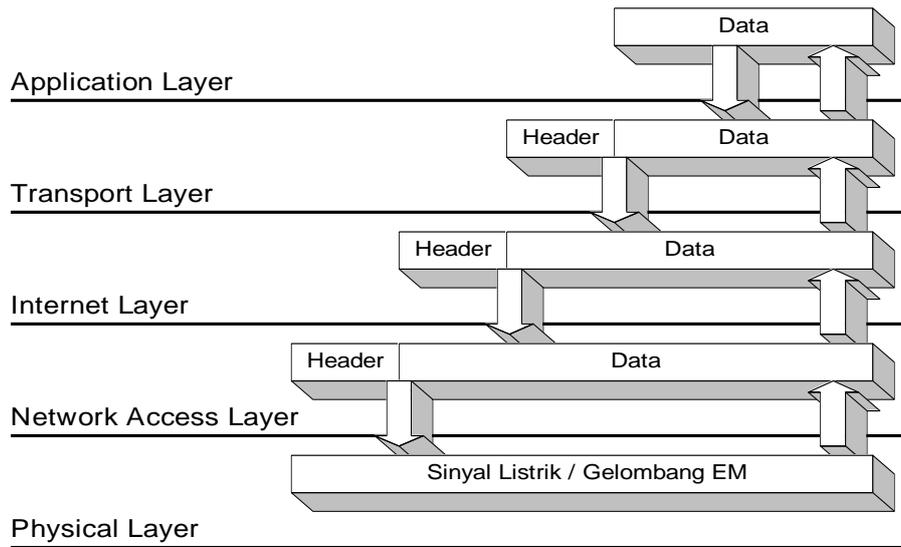


**Application Layer** merupakan lapisan terakhir dalam arsitektur TCP/IP yang berfungsi mendefinisikan aplikasi-aplikasi yang dijalankan pada jaringan. Karena itu, terdapat banyak protokol pada lapisan ini, sesuai dengan banyaknya aplikasi TCP/IP yang dapat dijalankan. Contohnya adalah SMTP ( *Simple Mail Transfer Protocol* ) untuk pengiriman *e-mail*, FTP ( *File Transfer Protocol* ) untuk transfer file, HTTP ( *Hyper Text Transfer Protocol* ) untuk aplikasi web, NNTP ( *Network News Transfer Protocol* ) untuk distribusi *news group* dan lain-lain. Setiap aplikasi pada umumnya menggunakan protokol TCP dan IP, sehingga keseluruhan keluarga protokol ini dinamai dengan TCP/IP.

### 1.2. Pengiriman dan Penerimaan Paket Data

Layer-layer dan protokol yang terdapat dalam arsitektur jaringan TCP/IP menggambarkan fungsi-fungsi dalam komunikasi antara dua buah komputer. Setiap lapisan menerima data dari lapisan di atas atau dibawahnya, kemudian memproses data tersebut sesuai fungsi protokol yang dimilikinya dan meneruskannya ke lapisan berikutnya. Ketika dua komputer berkomunikasi, terjadi aliran data antara pengirim dan penerima melalui lapisan-lapisan di atas. Pada pengirim, aliran data adalah dari atas ke bawah. Data dari user maupun suatu aplikasi dikirimkan ke Lapisan Transport dalam bentuk paket-paket dengan panjang tertentu. Protokol menambahkan sejumlah bit pada setiap paket sebagai header yang berisi informasi mengenai urutan segmentasi untuk menjaga integritas data dan bit-bit pariti untuk deteksi dan koreksi kesalahan.

Dari Lapisan Transport, data yang telah diberi header tersebut diteruskan ke Lapisan Network / Internet. Pada lapisan ini terjadi penambahan header oleh protokol yang berisi informasi alamat tujuan, alamat pengirim dan informasi lain yang dibutuhkan untuk melakukan routing. Kemudian terjadi pengarahan routing data, yakni ke network dan interface yang mana data akan dikirimkan, jika terdapat lebih dari satu interface pada host. Pada lapisan ini juga dapat terjadi segmentasi data, karena panjang paket yang akan dikirimkan harus disesuaikan dengan kondisi media komunikasi pada network yang akan dilalui. Proses komunikasi data di atas dapat dijelaskan seperti pada gambar berikut ini :



Gambar 15. Proses Enkapsulasi Data

Selanjutnya data menuju Network Access Layer (Data Link) dimana data akan diolah menjadi frame-frame, menambahkan informasi keandalan dan address pada level link. Protokol pada lapisan ini menyiapkan data dalam bentuk yang paling sesuai untuk dikirimkan melalui media komunikasi tertentu.

Terakhir data akan sampai pada Physical Layer yang akan mengirimkan data dalam bentuk besaran-besaran listrik/fisik seperti tegangan, arus, gelombang radio maupun cahaya, sesuai media yang digunakan.

Di bagian penerima, proses pengolahan data mirip seperti di atas hanya dalam urutan yang berlawanan (dari bawah ke atas). Sinyal yang diterima pada physical layer akan diubah dalam ke dalam data. Protokol akan memeriksa integritasnya dan jika tidak ditemukan error t header yang ditambahkan akan dilepas.

Selanjutnya data diteruskan ke lapisan network. Pada lapisan ini, address tujuan dari paket data yang diterima akan diperiksa. Jika address tujuan merupakan address host yang bersangkutan, maka header lapisan network akan dicopot dan data akan diteruskan ke lapisan yang di atasnya. Namun jika tidak, data akan di forward ke network tujuannya, sesuai dengan informasi routing yang dimiliki.

Pada lapisan Transport, kebenaran data akan diperiksa kembali, menggunakan informasi header yang dikirimkan oleh pengirim. Jika tidak



ada kesalahan, paket-paket data yang diterima akan disusun kembali sesuai urutannya pada saat akan dikirim dan diteruskan ke lapisan aplikasi pada penerima.

Proses yang dilakukan tiap lapisan tersebut dikenal dengan istilah enkapsulasi data. Enkapsulasi ini sifatnya transparan. Maksudnya, suatu lapisan tidak perlu mengetahui ada berapa lapisan yang ada di atasnya maupun di bawahnya. Masing-masing hanya mengerjakan tugasnya. Pada pengirim, tugas ini adalah menerima data dari lapisan di atasnya, mengolah data tersebut sesuai dengan fungsi protokol, menambahkan header protokol dan meneruskan ke lapisan di bawahnya.

Pada penerima, tugas ini adalah menerima data dari lapisan di bawahnya, mengolah data sesuai fungsi protokol, mencopot header protokol tersebut dan meneruskan ke lapisan di atasnya.

### **Internet Protocol**

Internet Protocol (IP) berfungsi menyampaikan paket data ke alamat yang tepat. Oleh karena itu Internet Protokol memegang peranan yang sangat penting dari jaringan TCP/IP. Karena semua aplikasi jaringan TCP/IP pasti bertumpu kepada Internet Protocol agar dapat berjalan dengan baik.

IP merupakan protokol pada network layer yang bersifat :

- **Connectionless**, yakni setiap paket data yang dikirim pada suatu saat akan melalui rute secara independen. Paket IP (datagram) akan melalui rute yang ditentukan oleh setiap router yang dilalui oleh datagram tersebut. Hal ini memungkinkan keseluruhan datagram tiba di tempat tujuan dalam urutan yang berbeda karena menempuh rute yang berbeda pula.
- **Unreliable** atau ketidakandalan yakni Protokol IP tidak menjamin datagram yang dikirim pasti sampai ke tempat tujuan. Ia hanya akan melakukan *best effort delivery* yakni melakukan usaha sebaik-baiknya agar paket yang dikirim tersebut sampai ke tujuan.

Suatu datagram bisa saja tidak sampai dengan selamat ke tujuan karena beberapa hal berikut:

- Adanya *bit error* pada saat penransmisian datagram pada suatu medium



- *Router* yang dilewati *discard* datagram karena terjadinya kongesti dan kekurangan ruang memori *buffer*
- Putusnya rute ke tujuan untuk sementara waktu akibat adanya *router* yang *down*

Terjadinya kekacauan *routing*, sehingga datagram mengalami *looping*

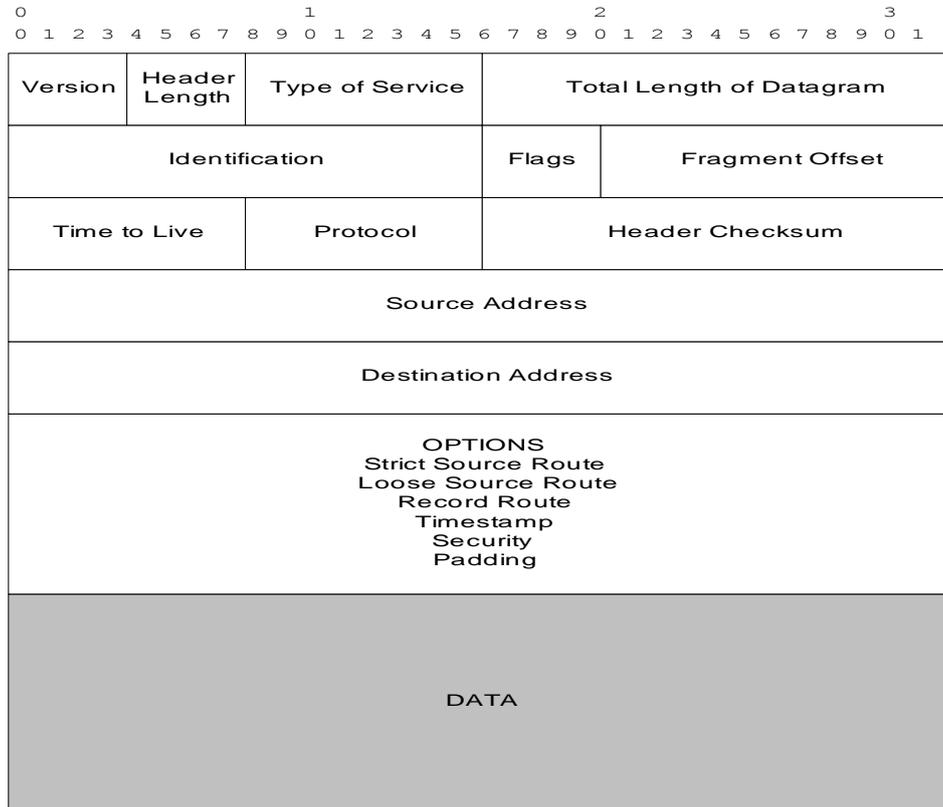
IP juga didesain untuk dapat melewati berbagai media komunikasi yang memiliki karakteristik dan kecepatan yang berbeda-beda. Pada jaringan *Ethernet*, panjang satu datagram akan lebih besar dari panjang datagram pada jaringan publik yang menggunakan media jaringan telepon, atau pada jaringan *wireless*. Perbedaan ini semata-mata untuk mencapai *throughput* yang baik pada setiap media. Pada umumnya, semakin cepat kemampuan transfer data pada media tersebut, semakin besar panjang datagram maksimum yang digunakan. Akibat dari perbedaan ini, datagram IP dapat mengalami fragmentasi ketika berpindah dari media kecepatan tinggi ke kecepatan rendah (misalnya dari LAN *Ethernet* 10 Mbps ke leased line menggunakan *Point-to-Point Protocol* dengan kecepatan 64 kbps). Pada *router/host* penerima, datagram yang ter-fragmen ini harus disatukan kembali sebelum diteruskan ke *router* berikutnya, atau ke lapisan transport pada *host* tujuan. Hal ini menambah waktu pemrosesan pada *router* dan menyebabkan *delay*.

Seluruh sifat yang diuraikan pada di atas adalah akibat adanya sisi efisiensi protokol yang dikorbankan sebagai konsekuensi dari keunggulan protokol IP. Keunggulan ini berupa kemampuan menggabungkan berbagai media komunikasi dengan karakteristik yang berbeda-beda, fleksibel dengan perkembangan jaringan, dapat merubah *routing* secara otomatis jika suatu rute mengalami kegagalan, dsb. Misalnya, untuk dapat merubah *routing* secara dinamis, dipilih mekanisme *routing* yang ditentukan oleh kondisi jaringan dan elemen-elemen jaringan (*router*). Selain itu, proses *routing* juga harus dilakukan untuk setiap datagram, tidak hanya pada permulaan hubungan. Marilah kita perhatikan struktur *header* dari protokol IP beserta fungsinya masing-masing.

Setiap protokol memiliki bit-bit ekstra diluar informasi/data yang dibawanya. Selain informasi, bit-bit ini juga berfungsi sebagai alat kontrol. Dari sisi efisiensi, semakin besar jumlah bit ekstra ini, maka semakin kecil efisiensi komunikasi yang berjalan. Sebaliknya semakin kecil jumlah bit



ekstra ini, semakin tinggi efisiensi komunikasi yang berjalan. Disinilah dilakukan *trade-off* antara keandalan datagram dan efisiensi. Sebagai contoh, agar datagram IP dapat menemukan tujuannya, diperlukan informasi tambahan yang harus dicantumkan pada *header* ini. Struktur *header* datagram protokol IP dapat dilihat pada gambar berikut.



Gambar 16.Format datagram IP

Setiap paket IP membawa data yang terdiri atas :

- Version, yaitu versi dari protokol IP yang dipakai.
- Header Length, berisi panjang dari header paket IP dalam hitungan 32 bit word.
- Type of Service, berisi kualitas service yang dapat mempengaruhi cara penanganan paket IP.
- Total length Of Datagram, panjang IP datagram total dalam ukuran byte.
- Identification, Flags, dan Fragment Offset, berisi data yang berhubungan fragmentasi paket.
- Time to Live, berisi jumlah router/hop maksimal yang dilewati paket IP (datagram). Nilai maksimum field ini adalah 255. Setiap kali paket IP



lewat satu router, isi dari field ini dikurangi satu. Jika TTL telah habis dan paket tetap belum sampai ke tujuan, paket ini akan dibuang dan router terakhir akan mengirimkan paket ICMP time exceeded. Hal ini dilakukan untuk mencegah paket IP terus menerus berada dalam network.

- Protocol, mengandung angka yang mengidentifikasi protokol layer atas pengguna isi data dari paket IP ini.
- Header Checksum, berisi nilai checksum yang dihitung dari jumlah seluruh field dari header paket IP. Sebelum dikirimkan, protokol IP terlebih dahulu menghitung checksum dari header paket IP tersebut untuk nantinya dihitung kembali di sisi penerima. Jika terjadi perbedaan, maka paket ini dianggap rusak dan dibuang.
- Source Address dan Destination Address, isi dari masing-masing *field* ini cukup jelas, yakni alamat pengirim dan alamat penerima dari datagram. Masing-masing *field* terdiri dari 32 bit, sesuai panjang IP Address yang digunakan dalam Internet. Destination address merupakan field yang akan dibaca oleh setiap router untuk menentukan kemana paket IP tersebut akan diteruskan untuk mencapai destination address tersebut. Struktur IP Address ini secara lebih jelas akan diuraikan pada bagian selanjutnya.

### 1.3. Pembagian Kelas IP Address

#### Pengertian

IP address digunakan sebagai alamat dalam hubungan antar host di internet sehingga merupakan sebuah sistem komunikasi yang universal karena merupakan metode pengalamatan yang telah diterima di seluruh dunia. Dengan menentukan IP address berarti kita telah memberikan identitas yang universal bagi setiap interadce komputer. Jika suatu komputer memiliki lebih dari satu interface (misalkan menggunakan dua ethernet) maka kita harus memberi dua IP address untuk komputer tersebut masing-masing untuk setiap interfacenya.



□ **Format Penulisan IP Address**

IP address terdiri dari bilangan biner 32 bit yang dipisahkan oleh tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai oktet. Bentuk IP address dapat dituliskan sebagai berikut :

xxxxxxxx.xxxxxxxxx.xxxxxxxxx.xxxxxxxxx

Jadi IP address ini mempunyai range dari 00000000.00000000.00000000.00000000 sampai 11111111.11111111.11111111.11111111. Notasi IP address dengan bilangan biner seperti ini susah untuk digunakan, sehingga sering ditulis dalam 4 bilangan desimal yang masing-masing dipisahkan oleh 4 buah titik yang lebih dikenal dengan “notasi desimal bertitik”. Setiap bilangan desimal merupakan nilai dari satu oktet IP address. Contoh hubungan suatu IP address dalam format biner dan desimal :

Desimal	167	205	206	100
Biner	10100111	11001101	11001110	01100100

Gambar 17.Format IP Address

**1.4. Pembagian Kelas IP Address**

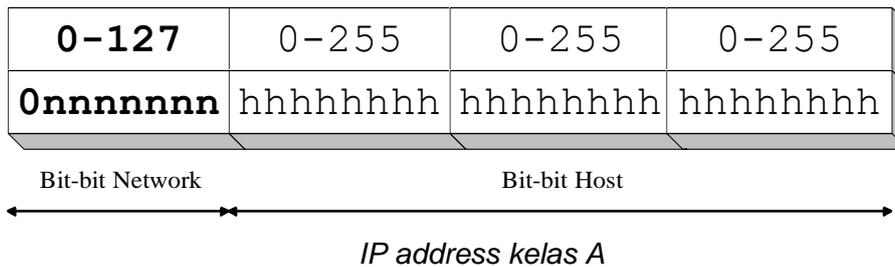
Jumlah IP address yang tersedia secara teoritis adalah 255x255x255x255 atau sekitar 4 milyar lebih yang harus dibagikan ke seluruh pengguna jaringan internet di seluruh dunia. Pembagian kelas-kelas ini ditujukan untuk mempermudah alokasi IP Address, baik untuk host/jaringan tertentu atau untuk keperluan tertentu.

IP Address dapat dipisahkan menjadi 2 bagian, yakni bagian *network* (net ID) dan bagian *host* (host ID). Net ID berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan host ID berperan untuk identifikasi *host* dalam suatu *network*. Jadi, seluruh *host* yang tersambung dalam jaringan yang sama memiliki net ID yang sama. Sebagian dari bit-bit bagian awal dari IP Address merupakan *network bit/network number*, sedangkan sisanya untuk *host*. Garis pemisah antara bagian *network* dan *host* tidak tetap, bergantung kepada kelas *network*. IP address dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D



dan kelas E. Perbedaan tiap kelas adalah pada ukuran dan jumlahnya. Contohnya IP kelas A dipakai oleh sedikit jaringan namun jumlah host yang dapat ditampung oleh tiap jaringan sangat besar. Kelas D dan E tidak digunakan secara umum, kelas D digunakan bagi jaringan multicast dan kelas E untuk keperluan eksperimental. Perangkat lunak *Internet Protocol* menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari IP Address. Penentuan kelas ini dilakukan dengan cara berikut :

Bit pertama IP address kelas A adalah 0, dengan panjang net ID 8 bit dan panjang host ID 24 bit. Jadi byte pertama IP address kelas A mempunyai range dari 0-127. Jadi pada kelas A terdapat 127 network dengan tiap network dapat menampung sekitar 16 juta host (255x255x255). IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar, IP kelas ini dapat dilukiskan pada gambar berikut ini:

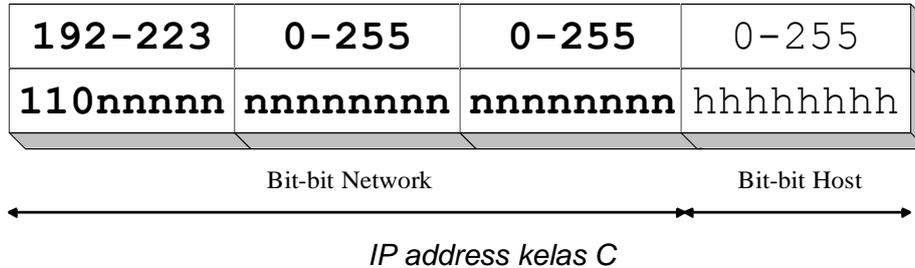


- Dua bit IP address kelas B selalu diset 10 sehingga byte pertamanya selalu bernilai antara 128-191. Network ID adalah 16 bit pertama dan 16 bit sisanya adalah host ID sehingga kalau ada komputer mempunyai IP address 192.168.26.161, network ID = 192.168 dan host ID = 26.161. Pada IP address kelas B ini mempunyai range IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx, yakni berjumlah 65.255 network dengan jumlah host tiap network 255 x 255 host atau sekitar 65 ribu host.





- IP address kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP address kelas C selalu diset 111. Network ID terdiri dari 24 bit dan host ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta network dengan masing-masing network memiliki 256 host.



- IP address kelas D digunakan untuk keperluan multicasting. 4 bit pertama IP address kelas D selalu diset 1110 sehingga byte pertamanya berkisar antara 224-247, sedangkan bit-bit berikutnya diatur sesuai keperluan multicast group yang menggunakan IP address ini. Dalam multicasting tidak dikenal istilah network ID dan host ID.
- IP address kelas E tidak diperuntukkan untuk keperluan umum. 4 bit pertama IP address kelas ini diset 1111 sehingga byte pertamanya berkisar antara 248-255.

Sebagai tambahan dikenal juga istilah *Network Prefix*, yang digunakan untuk IP address yang menunjuk bagian jaringan. Penulisan network prefix adalah dengan tanda slash “/” yang diikuti angka yang menunjukkan panjang network prefix ini dalam bit. Misal untuk menunjuk satu network kelas B 192.168.xxx.xxx digunakan penulisan 192.168/16. Angka 16 ini merupakan panjang bit untuk network prefix kelas B.

### 1.5. Address Khusus

Selain address yang dipergunakan untuk pengenalan *host*, ada beberapa jenis address yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk pengenalan *host*. Address tersebut adalah:

**Network Address.** Address ini digunakan untuk mengenali suatu network pada jaringan Internet. Misalkan untuk *host* dengan IP Address kelas B 192.168.9.35. Tanpa memakai subnet (akan diterangkan kemudian), *network address* dari *host* ini adalah 192.168.0.0. Address ini didapat dengan membuat seluruh bit *host* pada 2 segmen terakhir menjadi 0. Tujuannya adalah untuk menyederhanakan informasi *routing* pada Internet.



*Router* cukup melihat *network address* (192.168) untuk menentukan ke *router* mana *datagram* tersebut harus dikirimkan. Analoginya mirip dengan dalam proses pengantaran surat, petugas penyortir pada kantor pos cukup melihat kota tujuan pada alamat surat (tidak perlu membaca seluruh alamat) untuk menentukan jalur mana yang harus ditempuh surat tersebut.

**Broadcast Address.** Address ini digunakan untuk mengirim/menerima informasi yang harus diketahui oleh seluruh *host* yang ada pada suatu *network*. Seperti diketahui, setiap *datagram* IP memiliki *header* alamat tujuan berupa IP Address dari *host* yang akan dituju oleh *datagram* tersebut. Dengan adanya alamat ini, maka hanya *host* tujuan saja yang memproses *datagram* tersebut, sedangkan *host* lain akan mengabaikannya. Bagaimana jika suatu *host* ingin mengirim *datagram* kepada seluruh *host* yang ada pada *network*nya ? Tidak efisien jika ia harus membuat replikasi *datagram* sebanyak jumlah *host* tujuan. Pemakaian *bandwidth* akan meningkat dan beban kerja *host* pengirim bertambah, padahal isi *datagram*-*datagram* tersebut sama. Oleh karena itu, dibuat konsep *broadcast address*. *Host* cukup mengirim ke alamat *broadcast*, maka seluruh *host* yang ada pada *network* akan menerima *datagram* tersebut. Konsekuensinya, seluruh *host* pada *network* yang sama harus memiliki *broadcast address* yang sama dan address tersebut tidak boleh digunakan sebagai IP Address untuk *host* tertentu.

Jadi, sebenarnya setiap *host* memiliki 2 address untuk menerima *datagram* : pertama adalah IP Addressnya yang bersifat unik dan kedua adalah *broadcast address* pada *network* tempat *host* tersebut berada.

*Broadcast address* diperoleh dengan membuat bit-bit *host* pada IP Address menjadi 1. Jadi, untuk *host* dengan IP address 192.168.9.35 atau 192.168.240.2, *broadcast address*nya adalah 192.168.255.255 (2 segmen terakhir dari IP Address tersebut dibuat berharga 11111111.11111111, sehingga secara desimal terbaca 255.255). Jenis informasi yang *broadcast* biasanya adalah informasi *routing*.

**Multicast Address.** Kelas address A, B dan C adalah address yang digunakan untuk komunikasi antar *host*, yang menggunakan *datagram*-*datagram* *unicast*. Artinya, *datagram*/paket memiliki address tujuan berupa satu *host* tertentu. Hanya *host* yang memiliki IP address sama dengan *destination address* pada *datagram* yang akan menerima *datagram*



tersebut, sedangkan *host* lain akan mengabaikannya. Jika datagram ditujukan untuk seluruh *host* pada suatu jaringan, maka *field* address tujuan ini akan berisi alamat *broadcast* dari jaringan yang bersangkutan. Dari dua mode pengiriman ini (*unicast* dan *broadcast*), muncul pula mode ke tiga. Diperlukan suatu mode khusus jika suatu *host* ingin berkomunikasi dengan beberapa *host* sekaligus (*host group*), dengan hanya mengirimkan satu datagram saja. Namun berbeda dengan mode *broadcast*, hanya *host-host* yang tergabung dalam suatu group saja yang akan menerima datagram ini, sedangkan *host* lain tidak akan terpengaruh. Oleh karena itu, dikenalkan konsep *multicast*. Pada konsep ini, setiap *group* yang menjalankan aplikasi bersama mendapatkan satu *multicastaddress*. Struktur kelas *multicastaddress* dapat dilihat pada Gambar berikut.

<b>224-239</b>	0-255	0-255	0-255
<b>1110xxxx</b>	xxxxxxxx	xxxxxxxx	xxxxxxxx

Struktur IP Address Kelas Multicast Address

Untuk keperluan *multicast*, sejumlah IP Address dialokasikan sebagai *multicastaddress*. Jika struktur IP Address mengikuti bentuk 1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx (bentuk desimal 224.0.0.0 sampai 239.255.255.255), maka IP Address merupakan *multicastaddress*. Alokasi ini ditujukan untuk keperluan *group*, bukan untuk *host* seperti pada kelas A, B dan C. Anggota *group* adalah *host-host* yang ingin bergabung dalam *group* tersebut. Anggota ini juga tidak terbatas pada jaringan di satu *subnet*, namun bisa mencapai seluruh dunia. Karena menyerupai suatu *backbone*, maka jaringan *muticast* ini dikenal pula sebagai **Multicast Backbone (Mbone)**.

❑ **Aturan Dasar Pemilihan network ID dan host ID**

Berikut adalah aturan-aturan dasar dalam menentukan network ID dan host ID yang digunakan :

- Network ID tidak boleh sama dengan 127  
 Network ID 127 secara default digunakan sebagai alamat loopback yakni IP address yang digunakan oleh suatu komputer untuk menunjuk dirinya sendiri.



- Network ID dan host ID tidak boleh sama dengan 255  
Network ID atau host ID 255 akan diartikan sebagai alamat broadcast. ID ini merupakan alamat yang mewakili seluruh jaringan.
- Network ID dan host ID tidak boleh sama dengan 0  
IP address dengan host ID 0 diartikan sebagai alamat network. Alamat network digunakan untuk menunjuk suatu jaringan bukan suatu host.
- Host ID harus unik dalam suatu network.  
Dalam suatu network tidak boleh ada dua host yang memiliki host ID yang sama.

### 1.6. Subnetting

Untuk beberapa alasan yang menyangkut efisiensi IP Address, mengatasi masalah topologi network dan organisasi, network administrator biasanya melakukan subnetting. Esensi dari subnetting adalah “memindahkan” garis pemisah antara bagian network dan bagian host dari suatu IP Address. Beberapa bit dari bagian host dialokasikan menjadi bit tambahan pada bagian network. Address satu network menurut struktur baku dipecah menjadi beberapa subnetwork. Cara ini menciptakan sejumlah network tambahan, tetapi mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.

Subnetting juga dilakukan untuk mengatasi perbedaan hardware dan media fisik yang digunakan dalam suatu network. Router IP dapat mengintegrasikan berbagai network dengan media fisik yang berbeda hanya jika setiap network memiliki address network yang unik. Selain itu, dengan subnetting, seorang Network Administrator dapat mendelegasikan pengaturan host address seluruh departemen dari suatu perusahaan besar kepada setiap departemen, untuk memudahkannya dalam mengatur keseluruhan network.

Suatu subnet didefinisikan dengan mengimplementasikan masking bit (subnet mask) kepada IP Address. Struktur subnet mask sama dengan struktur IP Address, yakni terdiri dari 32 bit yang dibagi atas 4 segmen. Bit-bit dari IP Address yang “ditutupi” (masking) oleh bit-bit subnet mask yang aktif dan bersesuaian akan diinterpretasikan sebagai network bit. Bit 1 pada subnet mask berarti mengaktifkan masking ( on ), sedangkan bit 0



tidak aktif ( off ). Sebagai contoh kasus, mari kita ambil satu IP Address kelas A dengan nomor 44.132.1.20. Ilustrasinya dapat dilihat Tabel berikut :

44	132	1	20
00101100	10000100	00000001	00010100
IP Address			
255	255	0	0
11111111	11111111	00000000	00000000
Subnet Mask			
44	132	0	0
00101100	10000100	00000000	00000000
Network Address			
44	132	255	255
00101100	10000100	11111111	11111111
Broadcast Address			

Gambar 17. Subnetting 16 bit pada IP Address kelas A

Dengan aturan standard, nomor network IP Address ini adalah 44 dan nomor host adalah 132.1.20. Network tersebut dapat menampung maksimum lebih dari 16 juta host yang terhubung langsung. Misalkan pada address ini akan diimplementasikan subnet mask sebanyak 16 bit 255.255.0.0. ( Hexa = FF.FF.00.00 atau Biner = 11111111.11111111.00000000.00000000 ). Perhatikan bahwa pada 16 bit pertama dari subnet mask tersebut berharga 1, sedangkan 16 bit berikutnya 0. Dengan demikian, 16 bit pertama dari suatu IP Address yang dikenakan subnet mask tersebut akan dianggap sebagai network bit. Nomor network akan berubah menjadi 44.132 dan nomor host menjadi 1.20. Kapasitas maksimum host yang langsung terhubung pada network menjadi sekitar 65 ribu host.

Subnet mask di atas identik dengan standard IP Address kelas B. Dengan menerapkan subnet mask tersebut pada satu network kelas A, dapat dibuat 256 network baru dengan kapasitas masing-masing subnet setara network kelas B. Penerapan subnet yang lebih jauh seperti 255.255.255.0 ( 24 bit ) pada kelas A akan menghasilkan jumlah network yang lebih besar ( lebih dari 65 ribu network ) dengan kapasitas masing-masing subnet sebesar 256 host. Network kelas C juga dapat dibagi-bagi lagi menjadi beberapa subnet dengan menerapkan subnet mask yang lebih



tinggi seperti untuk 25 bit (255.255.255.128), 26 bit (255.255.255.192), 27 bit (255.255.255.224) dan seterusnya.

Subnetting dilakukan pada saat konfigurasi interface. Penerapan subnet mask pada IP Address akan mendefinisikan 2 buah address baru, yakni Network Address dan Broadcast Address. Network address didefinisikan dengan menset seluruh bit host berharga 0, sedangkan broadcast address dengan menset bit host berharga 1. Seperti yang telah dijelaskan pada bagian sebelumnya, network address adalah alamat network yang berguna pada informasi routing. Suatu host yang tidak perlu mengetahui address seluruh host yang ada pada network yang lain. Informasi yang dibutuhkannya hanyalah address dari network yang akan dihubungi serta gateway untuk mencapai network tersebut. Ilustrasi mengenai subnetting, network address dan broadcast address dapat dilihat pada Tabel di bawah. Dari tabel dapat disimpulkan bagaimana nomor network standard dari suatu IP Address diubah menjadi nomor subnet / subnet address melalui subnetting.

IP Address	Network Address Standard	Subnet Mask	Interpretasi	Broadcast Address
44.132.1.20	44.0.0.0	255.255.0.0(16 bit)	Host 1.20 pada subnet 44.132.0.0	44.132.255.255
81.150.2.3	81.0.0.0	255.255.255.0 (24 bit)	Host 3 pada subnet 81.50.2.0	81.50.2.255
192.168.2.100	192.168.0.0	255.255.255.128 (25 bit)	Host 100 pada Subnet 192.168.2.0	192.168.2.127
192.168.2. 130	192.168.0.0	255.255.255.192 (26 bit)	Host 130 pada subnet 192.168.2.128	192.168.2.191

Table 1. Beberapa kombinasi IP Address, Netmask dan network number

Subnetting hanya berlaku pada network lokal. Bagi network di luar network lokal, nomor network yang dikenali tetap nomor network standard menurut kelas IP Address.



### 1.7. Desain LAN

#### □ Metode Perencanaan LAN

Sekarang kita akan membahas bagaimana merencanakan suatu LAN yang baik. Tujuan utamanya untuk merancang LAN yang memenuhi kebutuhan pengguna saat ini dan dapat dikembangkan di masa yang akan datang sejalan dengan peningkatan kebutuhan jaringan yang lebih besar.

Desain sebuah LAN meliputi perencanaan secara fisik dan logic . Perencanaan fisik meliputi media yang digunakan bersama dan infrastruktur LAN yakni pengkabelan sebagai jalur fisik komunikasi setiap devais jaringan. Infrastruktur yang dirancang dengan baik cukup fleksibel untuk memenuhi kebutuhan sekarang dan masa datang.

Metode perencanaan LAN meliputi :

- Seorang administrator network yang bertanggung jawab terhadap jaringan.
- Pengalokasian IP address dengan subnetting.
- Peta letak komputer dari LAN dan topologi yang hendak kita gunakan.
- Persiapan fisik yang meliputi pengkabelan dan peralatan lainnya.

Di antara hal-hal yang perlu diperhatikan dalam perancangan LAN adalah lokasi fisik itu sendiri. Peta atau cetak biru bangunan-bangunan yang akan dihubungkan serta informasi jalur kabel (*conduit*) yang ada dan menghubungkan bangunan-bangunan tersebut sangat diperlukan. Jika peta seperti ini tidak ada maka perlu digambarkan peta dengan cara merunut kabel-kabel yang ada. Secara umum dapat diasumsikan bahwa pengkabelan yang menghubungkan bangunan-bangunan atau yang melewati tempat terbuka harus terdapat di dalam conduit. Seorang manajer jaringan harus menghubungi manajer bangunan untuk mengetahui aturan-aturan pengkabelan ini sebab manajer bangunan yang mengetahui dan bertanggung jawab atas bangunan tersebut. Pada setiap lokasi (yang dapat terdiri dari beberapa bangunan) harus ditunjuk seorang manajer jaringan. Manajer jaringan harus mengetahui semua konfigurasi jaringan dan pengkabelan pada lokasi yang menjadi tanggung jawabnya. Pada awalnya tugas ini hanya memakan waktu sedikit. Namun sejalan dengan perkembangan jaringan menjadi lebih kompleks, tugas ini berubah menjadi



tugas yang berat. Jadi sebaiknya dipilih orang yang betul-betul berminat dan mau terlibat dalam perkembangan jaringan.

#### □ Pengalokasian IP Address

Bagian ini memegang peranan yang sangat penting karena meliputi perencanaan jumlah network yang akan dibuat dan alokasi IP address untuk tiap network. Kita harus membuat subnetting yang tepat untuk keseluruhan jaringan dengan mempertimbangkan kemungkinan perkembangan jaringan di masa yang akan datang. Sebagai contoh, sebuah kantor memasang jaringan internet via V-SAT mendapat alokasi IP address dari INTERNIC (<http://www.internic.net>) untuk kelas B yaitu 192.168.xxx.xxx. Jika diimplementasikan dalam suatu jaringan saja (flat), maka dengan IP Address ini kita hanya dapat membuat satu network dengan kapasitas lebih dari 65.000 host. Karena letak fisik jaringan tersebar (dalam beberapa departemen dan laboratorium) dan tingkat kongesti yang akan sangat tinggi, tidak mungkin menghubungkan seluruh komputer dalam kantor tersebut hanya dengan menggunakan satu buah jaringan saja (flat). Maka dilakukan pembagian jaringan sesuai letak fisiknya. Pembagian ini tidak hanya pada level fisik (media) saja, namun juga pada level logik (network layer), yakni pada tingkat IP address. Pembagian pada level network membutuhkan segmentasi pada IP Address yang akan digunakan. Untuk itu, dilakukan proses pendelegasian IP Address kepada masing-masing jurusan, laboratorium dan lembaga lain yang memiliki LAN dan akan diintegrasikan dalam suatu jaringan kampus yang besar. Misalkan dilakukan pembagian IP kelas B sebagai berikut :

- IP address 192.168.1.xxx dialokasikan untuk cadangan
- IP address 192.168.2.xxx dialokasikan untuk departemen **A**
- IP address 192.168.3.xxx dialokasikan untuk departemen **B**
- IP address 192.168.4.xxx dialokasikan untuk unit **X**
- dsb.

Pembagian ini didasari oleh jumlah komputer yang terdapat pada suatu jurusan dan prediksi peningkatan populasinya untuk beberapa tahun kemudian. Hal ini dilakukan semata-mata karena IP Address bersifat terbatas, sehingga pemanfaatannya harus diusahakan seefisien mungkin.



Jika seorang administrator di salah satu departemen mendapat alokasi IP address 192.168.48.xxx, maka alokasi ini akan setara dengan sebuah IP address kelas C karena dengan IP ini kita hanya dapat membentuk satu jaringan berkapasitas 256 host yakni dari 192.168.9.0 sampai 192.168.9.255.

Dalam pembagian ini, seorang network administrator di suatu lembaga mendapat alokasi IP Address 192.168.9.xxx. Alokasi ini setara dengan satu buah kelas C karena sama-sama memiliki kapasitas 256 IP Address, yakni dari 192.168.9.0 sampai dengan 192.168.9.255. Misalkan dalam melakukan instalasi jaringan, ia dihadapkan pada permasalahan-permasalahan sebagai berikut :

- Dibutuhkan kira-kira 7 buah LAN.
- Setiap LAN memiliki kurang dari 30 komputer.

Berdasarkan fakta tersebut, ia membagi 256 buah IP address itu menjadi 8 segmen. Karena pembagian ini berbasis bilangan biner, pembagian hanya dapat dilakukan untuk kelipatan pangkat 2, yakni dibagi 2, dibagi 4, 8, 16, 32 dst. Jika kita tinjau secara biner, maka kita mendapatkan :

Jumlah bit host dari subnet 192.168.9.xxx adalah 8 bit (segmen terakhir). Jika hanya akan diimplementasikan menjadi satu jaringan, maka jaringan tersebut dapat menampung sekitar 256 host.

Jika ia ingin membagi menjadi 2 segmen, maka bit pertama dari 8 bit segmen terakhir IP Address di tutup (mask) menjadi bit network, sehingga masking keseluruhan menjadi  $24 + 1 = 25$  bit. Bit untuk host menjadi 7 bit. Ia memperoleh 2 buah sub network, dengan kapasitas masing-masing subnet 128 host. Subnet pertama akan menggunakan IP Address dari 192.168.9.(**0-127**), sedangkan subnet kedua akan menggunakan IP Address 192.168.9.(**128-255**).



<b>167</b>	<b>205</b>	<b>9</b>	<b>xxx</b>	
10100111	11001101	00001001	xxxxxxxx	
11111111	11111111	11111111	1xxxxxxxx	<b>Byte terakhir</b>
10100111	11001101	00001001	0xxxxxxxx	0 - 127
10100111	11001101	00001001	1xxxxxxxx	128 - 255

Tabel 2. Pembagian 256 IP Address menjadi 2 segmen

Karena ia ingin membagi menjadi 8 segmen, maka ia harus mengambil 3 bit pertama ( $2^3 = 8$ ) dari 8 bit segmen terakhir IP Address untuk di tutup (mask) menjadi bit network, sehingga masking keseluruhan menjadi  $24 + 3 = 27$  bit. Bit untuk host menjadi 5 bit. Dengan masking ini, ia memperoleh 8 buah sub network, dengan kapasitas masing-masing subnet  $32 (=2^5)$  host. Ilustrasinya dapat dilihat pada Tabel 3 berikut :

167	205	9	xxx	
10100111	11001101	00001001	xxxxxxxx	
11111111	11111111	11111111	11100000	Byte Akhir
10100111	11001101	00001001	000xxxxx	0-31
10100111	11001101	00001001	001xxxxx	32-63
10100111	11001101	00001001	010xxxxx	64-95
10100111	11001101	00001001	011xxxxx	96-127
10100111	11001101	00001001	100xxxxx	128-159
10100111	11001101	00001001	101xxxxx	160-191
10100111	11001101	00001001	110xxxxx	192-223
10100111	11001101	00001001	111xxxxx	224-255

Tabel 3. Ilustrasi subnetting



### c. Tes Formatif

#### Studi Kasus :

Anda sebagai penanggungjawab jaringan di suatu kantor yang mempunyai 3 buah departemen mendapat alokasi IP dari suatu ISP (Internet Service Provider) 192.168.9.10xxxxxx (8 bit terakhir adalah biner). Jika jumlah host tiap-tiap departemen diperkirakan tidak lebih dari 13 buah dan masing masing departemen akan dibuat jaringan lokal (LAN) tersendiri, coba anda tentukan :(semua host mendapat alokasi IP asli)

- Subnet yang harus dibuat
  - Network address
1. Penulisan IP Address 10.208.15.240 dalam bentuk binary ditulis sebagai berikut
    - A. 00001010.11010000.00001111.11010000
    - B. 00001010.11010000.00001111.11100000
    - C. 00001010.11010000.00001111.11111000
    - D. 00001010.11010000.00001111.10110000
    - E. 00001010.11010000.00001111.11110000
  2. File Server is different with FTP Server. because..
    - a. File Server is Sharing file, FTP is Transfer File
    - b. File Server use explorer, FTP use Browser
    - c. File server better than FTP Server
    - d. File server store files, FTP Server Share Applications
    - e. File server use port 22, FTP use port 33
  3. Bridges operate at the \_\_\_\_\_ OSI level.
    - a. The Transport Layer
    - b. The Data-Link Layer
    - c. The Network Layer
    - d. The Session Layer
    - e. Top Layer
  4. Domain Name System (DNS) adalah suatu sistem yang memungkinkan nama suatu host pada jaringan komputer atau internet ditranslasikan menjadi.....
    - a. IP address
    - b. home ID
    - c. host ID



- d. broadcast address
  - e. Protocol
5. Berapa jumlah maksimum ID host yang tersedia pada alamat kelas C?
- a. 65,534
  - b. 192
  - c. 16,384
  - d. 126
  - e. 254

#### **d. Lembar Jawaban Tes Formatif**

##### **Penyelesaian :**

- Subnet yang harus dibuat adalah :  
11111111.11111111.11111111.11110000 atau 255.255.255.240.  
Terdapat network address sbb :  
192.168.9.10000000  
192.168.9.10010000  
192.168.9.10100000  
192.168.9.10110000
  - Terdapat broadcast address sbb:
    - 192.168.9.10001111 = 192.168.9.143
    - 192.168.9.10011111 = 192.168.9.159
    - 192.168.9.10101111 = 192.168.9.175
1. E. 00001010.11010000.00001111.11110000
  2. B. File Server use explorer, FTP use Browser
  3. C. The Network Layer
  4. A. IP address
  5. E. 254

#### **e. Lembar Kerja Siswa**



## Kegiatan Belajar 6 : Pengalamatan IP v6

### a. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 6 ini siswa diharapkan dapat :

- 1).Memahami **Pengalamatan IP v6**
- 2).Menganalisis **Pengalamatan IP v6**

### b. Uraian Materi

#### Pengalamatan IP v6

IPv6 ini merupakan perkembangan dari IPv4 yang dapat menyediakan lebih banyak IP address karena IPv6 ini panjangnya adalah 128 bit tidak seperti IPv4 yang panjangnya hanya 32 bit saja. selain itu, masih banyak kelebihan lain dari IPv6 ini bila dibandingkan dengan IPv4.

#### Keunggulan IPv6

##### 1. Jumlah IP Address yang sangat banyak

Seperti yang telah diketahui, pada IPv4 panjang satu alamat IP-nya adalah 32 bit yang berarti dapat menyediakan alamat IP sebanyak 4.294.967.296.mungkin jika dilihat sepintas jumlah tersebut sudah banyak, tetapi karena implementasi tertentu dalam penggunaannya pada kenyataanya jumlah IP tersebut masih kurang jika digunakan untuk membuat jaringan pada seluruh dunia ini. Berbeda dengan IPv6, IPv6 pada satu alamat IP-nya panjangnya 128 bit atau dengan kata lain dapat menyediakan alamat IP sebanyak  $3.4 \times 10^{38}$ . Jumlah tersebut sangatlah besar sehingga dapat mengatasi masalah kekurangan IP pada beberapa tahun mendatang.

##### 2. Autoconfiguration

IPv6 dirancang agar penggunaanya tidak dipusingkan dengan konfigurasi Ip address. Komputer pengguna yang terhubung dengan jaringan IPv6 akan mendapatkan IP address langsung dari router, sehingga nantinya DHCP server tidak diperlukan lagi. Autoconfiguration nantinya sangat berguna bagi peralatan mobile internet karena



pengguna tidak direpotkan dengan konfigurasi sewaktu berpindah tempat dan jaringan.

### 3. Security

IPv6 telah dilengkapi dengan protokol IPSec, sehingga semua aplikasi telah memiliki security yang optimal bagi berbagai aplikasi yang membutuhkan keamanan, misalnya saja transaksi e-banking. Disamping itu, IPSec dalam Ipv6 merupakan protokol keamanan yang paling andal saat ini. Dimana ia menggunakan teknik enkripsi yang rumit sehingga sulit ditebak oleh hacker yang akan membaca data yang dilewatkan.

### 4. Quality of Service.

IPv6 memiliki protokol QoS yang terintegrasi dengan baik, sehingga semua aplikasi yang berjalan diatas Ipv6 memiliki jaminan QoS, terutama bagi aplikasi yang sensitive terhadap delay seperti VoIP dan streaming video.

### Penulisan IPv6

Tidak seperti IPv4, IPv4 dituliskan dengan bilangan hexadecimal yaitu 0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f. pada IPv6 ini terdapat delapan blok dimana tiap blok tersebut terdapat empat digit bilangan hexadecimal. Berbeda dengan IPv4 hanya terdiri dari empat blok saja. selain itu, untuk memisahkan tiap bloknnya pada IPv6 digunakan titik dua, tidak titik seperti pada IPv4. Berikut merupakan contoh penulisan IPv6

```
2001:0db8:0000:0000:5a55:0302:fef6:0012
```

Karena pada IPv6 alamat yang digunakan panjang dalam penulisanya, maka telah dibuat ketentuan tertentu untuk penyederhanaan untuk alamat IPv6, yaitu:

- Angka 0 didepan bisa dihilangkan
- 0000 yang berurutan bisa dihilangkan dan diganti dengan titik dua

Dengan begitu penulisan alamat IPv6

```
2001:0db8:0000:0000:5a55:0302:fef6:0012 diatas menjadi
```

```
2001:db8::5a55:302:fef6:12
```



### **Jenis Pengalamatan IPv6**

Seperti yang telah diketahui, pada IPv4 terdapat suatu pengalamatan IP yang dibagi menjadi lima kelas yaitu kelas a, b, c, d, dan e. dimana diantara kelima kelas tersebut hanya kelas a, b, dan c yang bisa digunakan karena kelas D digunakan untuk keperluan multicasting dan kelas E untuk keperluan eksperimental. Berbeda dengan IPv6, pada IPv6 tidak dikenal system pengkelasan seperti pada IPv4 melainkan pada IPv6 hanya menyediakan tiga jenis pengalamatan yaitu Unicast, Anycast, dan Multicast

#### **1. Unicast**

Pengalamatan unicast mirip dengan IPv4 yaitu dengan sekumpulan alamat dengan sejumlah bit kontinyu yang sama sesuai dengan alamat subnet-nya dan Class-less Interdomain Routing (CIDR). Ada banyak jenis pengalamatan unicast pada IPv6 sesuai dengan tipenya seperti :

- Alamat Link Local : alamat yang digunakan di dalam satu link yaitu jaringan local yang saling tersambung dalam satu level
- Alamat Site Local : setara dengan alamat privat, yang dipakai terbatas dalam satu site sehingga terbatas penggunaannya hanya didalam satu site sehingga tidak dapat digunakan untuk mengirimkan alamat diluar site ini
- Alamat Global : alamat yang dipakai misalnya untuk ISP (Internet Service Provider)

#### **2. Anycast**

Pengalamatan anycast digunakan untuk mengirimkan packet ke salah satu anggota dari anycast yang terdekat. Jadi sebuah alamat anycast digunakan oleh beberapa interface dan setiap packet anycast akan terkirim ke interface anggota yang terdekat. Model pengalamatan pada anycast hampir sama dengan model unicast. Jadi secara sintaksis alamat anycast sama saja dengan unicast, hanya saja sebuah alamat anycast digunakan oleh lebih dari 1 host. Syarat dari pengalamatan anycast:

- a. Sebuah alamat anycast tidak boleh digunakan sebagai alamat sumber dari sebuah packet IPv6.



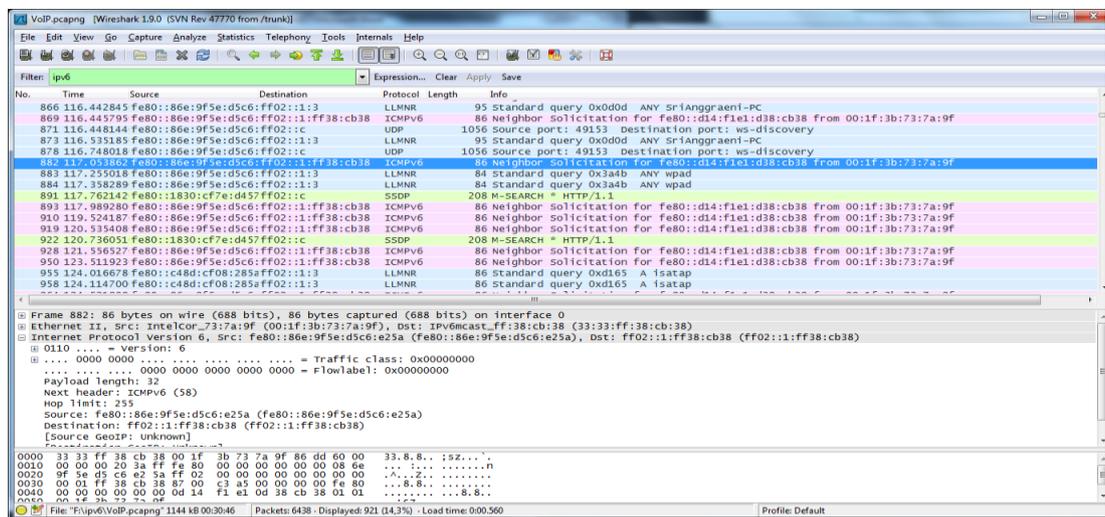
b. Sebuah alamat anycast tidak boleh digunakan sebagai alamat interface pada router.

### 3. Multicast

Alamat multicast IPv6 digunakan sebagai identitas sebuah group node. Jika packet dikirim ke alamat multicast, maka packet tersebut akan diterima oleh semua node anggota dari group tersebut. Sebuah node dapat menjadi anggota banyak group multicast

### 4. Capturing IPv6

Berikut merupakan contoh hasil capture IPv6 dengan menggunakan wireshark :



Pada gambar tersebut terlihat jika pada filter wireshark telah diterapkan filter untuk IPv6. Pada kolom hasil pencarian terlihat jika protocol-protocol yang telah ter-capture menggunakan IPv6 pada layer tiga/network-nya. Dapat dilihat pada source dan destination dari setiap paket yang telah ter-capture tersebut semuanya menggunakan bilangan hexadesimal dan dibatasi dengan titik dua untuk setiap blok-nya, tidak ada IP yang berbentuk seperti IPv4. Berikut merupakan detail dari salah satu paket yang menggunakan IPv6 tersebut.



```
882.117.053862000 fe80::86e:9f5e:d5c6:e25a ff02::1:ff38:cb38 ICMPv6 86 Neighbor Solicitation for fe80::d14:f1e1:d38:cb38 from 00:1f:3b:73:7a:9f
Frame 882: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: IntelCor_73:7a:9f (00:1f:3b:73:7a:9f), Dst: IPv6mcast_ff:38:cb:38 (33:33:ff:38:cb:38)
Internet Protocol Version 6, Src: fe80::86e:9f5e:d5c6:e25a (fe80::86e:9f5e:d5c6:e25a), Dst: ff02::1:ff38:cb38 (ff02::1:ff38:cb38)
  0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  .... 0000 0000 .... = Traffic class: 0x00000000
  .... 0000 00.. .... = Differentiated Services Field: Default (0x00000000)
  .... ..0. .... = ECN-Capable Transport (ECT): Not set
  .... ..0. .... = ECN-CE: Not set
  .... ..0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 32
Next header: ICMPv6 (58)
Hop limit: 255
Source: fe80::86e:9f5e:d5c6:e25a (fe80::86e:9f5e:d5c6:e25a)
Destination: ff02::1:ff38:cb38 (ff02::1:ff38:cb38)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol v6
Type: Neighbor solicitation (135)
Code: 0
Checksum: 0xc3a5 [correct]
Reserved: 00000000
Target Address: fe80::d14:f1e1:d38:cb38 (fe80::d14:f1e1:d38:cb38)
ICMPv6 Option (source link-layer address : 00:1f:3b:73:7a:9f)
Type: source link-layer address (1)
Length: 1 (8 bytes)
Link-layer address: IntelCor_73:7a:9f (00:1f:3b:73:7a:9f)
```

Pada gambar tersebut terlihat beberapa detail dari IPv6 seperti payload, next header, hop limit, source, dan destination.

Payload Length merupakan panjangnya data user yang dibawa dalam paket tersebut. Pada gambar tersebut terlihat jika payload length-nya adalah 32.

Next header merupakan 8-bit selector yang berfungsi untuk mengidentifikasi dengan cepat header selanjutnya setelah header IPv6. Pada gambar tersebut terlihat jika header selanjutnya merupakan header untuk layer di atasnya yaitu header dari ICMPv6.

Hop limit terdiri dari 8-bit unsigned integer. Nilai dari hop limit ini terus berkurang satu persatu setiap melewati node saat paket dikirim. Paket akan dihilangkan apabila hop limit terus berkurang hingga nol. Pada gambar tersebut terlihat jika node limit-nya 255. Hal itu berarti paket yang dikirim tersebut langsung dikirim ke destination tanpa melewati node tertentu.

Source address merupakan alamat sumber dari pengirim. Seperti yang telah dijelaskan di atas, alamat dari IPv6 panjangnya 128-bit dimana pada gambar hasil capture ditunjukkan dengan alamat Fe80::86e:9f5e:d5c6:e25a.

Destination address merupakan alamat tujuan kemana paket tersebut akan dikirim. Sama dengan source address, alamat dari destination ini juga terdiri dari 128 bit data alamat dari destination ini juga terdiri dari 128 bit data dimana pada gambar di atas ditunjukkan dengan nilai ff02::1:ff38:cb38

(Sumber: *ilmuKomputer.com*)



## 5.Subnetting Classfull

**Classfull** adalah alamat IP yang dibagi berdasarkan dalam kelas. Ada 5 kelas yang berbeda dan itu adalah kelas yang memutuskan ukuran jaringan. Empat bit pertama dari alamat IP yang digunakan untuk mengidentifikasi kelas. Dari lima kelas A, B, C, D dan E. kelas A, B dan C digunakan untuk jaringan **unicast**, D untuk jaringan **multicast** dan E disediakan untuk penggunaan "**masa depan**".

Bit yang digunakan untuk mengidentifikasi kelas adalah sebagai berikut:

A = 0

B = 10

C = 110

D = 1.110

E = 1.111

Tetapi permasalahan muncul dengan adanya arsitektur ini, bahwa ukuran jaringan tersebut terlalu besar. ini mengurangi tingkat fleksibilitasnya ini menyebabkan pemborosan beberapa alamat.

Untuk mengatasi ini, CIDR atau Routing Inter-Domain Classless diperkenalkan pada tahun 1993. Berikut alamat IP dibagi menjadi dua bagian: bagian paling penting adalah alamat jaringan yang digunakan untuk mengidentifikasi jaringan dan bagian yang paling signifikan adalah host identifier.

Contoh :

IP Kelas C mempunyai range host 0 – 255 192.168.1.0 – 192.168.1.255, Bagaimana jika komputer dikantor cuma ada 10 ? klo kita menggunakan default netmask ip kelas C 255.255.255.0 maka akan ada banyak IP yang tidak digunakan karena yang kita butuhkan hanya 10 IP saja, memang tidak ada masalah dengan mengkoneksikan IP /24 itu tetapi jika akan mengatur dan mengelola pasti akan susah karena kita bingung IP mana yang telah digunakan karena terlalu banyak. maka dari itu digunakan CIDR yang biasanya dinotasikan dengan " / " atau Slash. sehingga notasi yang digunakan **/28** (pelajari teknik subnetting ip)



jadi :

192.168.1.0 /28 = range ip 192.168.1.0 – 192.168.1.15

ip 192.168.1.0 = Net ID

ip 192.168.1.15 = Broadcast

ip 192.168.1.1 – 192.168.1.14 adalah **IP Available**

### c. Tes Formatif

1. Yang termasuk jenis-jenis alamat IPV6 adalah ....
  - A. Unicast, Anycast, Global Address
  - B. Multicast, Unicast Address, Anycast
  - C. Global Address, Site-Local, Link-Local
  - D. Unicast, Anycast, Multicast
  
2. Perubahan dari IPV4 ke IPV6 terutama pada .....
  - A. Memperluas kemampuan pengalamatan, meningkatnya alamat public, mengalirkan kemampuan Labeling
  - B. Penyederhanaan format header, memperluas kemampuan pengalamatan, pengesahan dan kemampuan privasi, meningkatkan support untuk memperluas dan pilihan, penyederhanaan format header.
  - C. Kemampuan pengalamatan, memisahkan header, meningkatnya alamat public.
  - D. Meningkatnya alamat public, memisahkan header, meningkatkan support untuk perluasan dan pilihan.
  
3. Alamat Unicast global IPV6 mirip dengan alamat public dalam alamat IPV4, dikenal juga sebagai .....
  - A. Unicast Site-Local IPV6
  - B. Aggregatable Global Unicast Address
  - C. Neighbor Discovery
  - D. Automatic Private Internet Protocol Addressing



4. Sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan **TCP/IP** yang menggunakan protokol Internet versi 6 Disebut Dengan.....

- A. IPV.4
- B. IPV.6
- C. STATING ROUTING
- D. DINAMIK ROUTING
- E. KOMPUTER

5. Alamat IPv6 *unicast* dapat diimplementasikan dalam berbagai jenis alamat. *kecuali*....

- A. Alamat unicast global
- B. Alamat unicast link-local
- C. Alamat unicast 6to4
- D. Alamat unicast loopback
- E. Alamat multicast

#### **d. Lembar Jawaban Tes Formatif**

1. **D.** Unicast, Anycast, Multicast
2. **B.** Penyederhanaan format header, memperluas kemampuan pengalamatan, pengesahan dan kemampuan privasi, meningkatkan support untuk memperluas dan pilihan, penyederhanaan format header.
3. **B.** Aggregatable Global Unicast Address
4. **B.** IPV.6
5. **E.** Alamat multicast

#### **e. Lembar Kerja Siswa**



## Kegiatan Belajar 7 :Protokol Pengalamatan

### a. Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 1 ini siswa diharapkan dapat :

- 1).Memahami paradigma pemrograman berorientasi obyek
- 2).Menganalisis perbandingan pemrograman procedural dan pemrograman berorientasi obyek

### b. Uraian Materi

#### Protokol Pengalamatan

##### Protokol

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer.Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya.Pada tingkatan yang terendah, protokol mendefinisikan koneksi perangkat keras. Protocol digunakan untuk menentukan jenis layanan yang akan dilakukan pada internet.

##### 1.Pengalamatan IP v4

Dalam jaringan komputer pengalamatan IP merupakan hal yang sangat penting karena pengalamatan ini merupakan pengidentifikasian suatu komputer pada jaringan sehingga memiliki identitas yang unik. Dengan adanya IP address maka dapat diketahui sumber ataupun tujuan dari pengiriman paket. Ipv4 menggunakan notasi biner yang memiliki panjang 32 bit. Pada dasarnya, arsitektur IPv4 menganut konsep *classful addressing*, yaitu pembagian ruang alokasi alamat ke dalam 5 kelas (50% A, 25% B, 12.5% C, 6.25% D,dan6.25% E). Bila direpresentasikan dengan notasi desimal, pembagian kelas ini dapat dilihat dari *byte*/oktet pertama seperti pada Tabel 1.

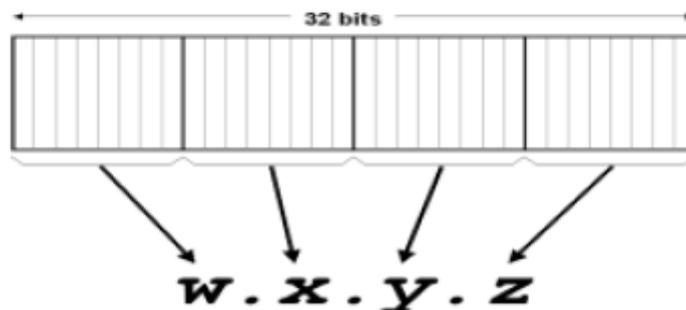


Kelas IP	Byte pertama
A	0 – 127
B	128 – 191
C	192 – 223
D	224 – 247
E	248 – 255

dari kelima kelas diatas, jenis alamat yang sering dipakai adalah alamat kelas A,B, dan C, sedangkan alamat kelas D biasanya digunakan untuk keperluan multicasting dan kelas E untuk keperluan Experimental. Pada IPv4 dikenal juga istilah subnet mask yaitu angka biner 32 bit yang digunakan untuk membedakan network ID dan host ID.

### IPv4 Address Syntax

Sistem pengalamatan pada IPv4 menggunakan notasi biner sebesar 32 *bit* yang dibagi atas 4 kelompok (setiap kelompok terdiri dari 8 bit atau oktet) dan tiap kelompok dipisahkan oleh sebuah tanda titik. IPv4 juga sering disebut sebagai sistem pengalamatan 4- oktet atau pengalamatan 4-*bytes* (1*byte*= 8*bit*).Untuk memudahkan pembacaan, penulisan alamat dilakukan dengan angka decimal dan diberi pemisah menggunakan tanda titik(dot). Dibawah ini contoh pengelompokkan IPv4 menggunakan notasi w, x, y, z.



Gambar.1 IPv4 address dalam notasi titik desimal

Sebagai contoh misalnya 100.3.1.100 yang jika dinyatakan dalam binary menjadi 01100100.00000011.00000001.01100100. Dari 32 bit ini berarti banyaknya jumlahmaksimum alamat yang dapat dituliskan adalah 2



pangkat 32, atau 4.294.967.296 alamat. Format alamat ini terdiri dari 2 bagian, netid dan hostid. Netid sendiri menyatakan alamat jaringan sedangkan hostid menyatakan alamat lokal (host/router). Dari 32 bit ini, tidak boleh semuanya angka 0 atau 1 (0.0.0.0 digunakan untuk jaringan yang tidak dikenal dan 255.255.255.255 digunakan untuk broadcast). Dalam penerapannya, alamat internet ini diklasifikasikan ke dalam kelas (A-E). Alasan klasifikasi ini antara lain :

- Memudahkan sistem pengelolaan dan pengaturan alamat-alamat.
- Memanfaatkan jumlah alamat yang ada secara optimum (tidak ada alamat yang terlewat).
- Memudahkan pengorganisasian jaringan di seluruh dunia dengan membedakan jaringan tersebut termasuk kategori besar, menengah, atau kecil.
- Membedakan antara alamat untuk jaringan dan alamat untuk host/router.

Dengan perkembangan internet dan jaringan akhir akhir ini telah membuat internet protocol (IP) yang merupakan tulang punggung jaringan berbasis TCP/IP dengan cepat menjadi ketinggalan zaman, dan alamat IPv4 pun juga akan habis terpakai.

### **IPv4 Address Prefixes**

Representasi prefix dari alamat IPv4 adalah menunjukkan banyaknya jumlah alamat pada IPv4. Untuk menentukan panjang notasi dari alamat prefix, kamu bisa memulainya dengan cara merubah seluruh variable bit menjadi 0, kemudian konversi ke notasi decimal, dan tambahkan potongan bit yang telah ditentukan (panjang prefix) di awal pengalamatan. Sebagai contoh misalnya alamat IPv4 adalah 131.107.0.0/16 memiliki 16 bit yang telah ditentukan (100000011 01101011). Awali pengalamatan dengan 16 bit sebelumnya yang telah ditentukan, kemudian merubah 16 bit terakhir menjadi bit 0, sehingga hasilnya menjadi 1000000111 01101011 00000000 00000000 atau 131.107.0.0. Kemudian tinggal menambahkan potongan bit yang telah ditentukan (/16) untuk merepresentasikan alamat prefix dari 131.107.0.0/16.



## Types of IPv4 Addresses

Ada 3 model pengalamatan standar dari pengalamtan IPv4, yaitu;

1. Unicast
2. Multicast
3. Broadcast

### 1. IPv4 Unicast Addresses

Penugasan terhadap sebuah interface jaringan yang menempatkan subnet khusus; digunakan untuk komunikasi point to point. Setiap antarmuka jaringan yang menggunakan protokol TCP/IP harus diidentifikasi dengan menggunakan sebuah alamat logis yang unik, yang disebut dengan alamat unicast (*unicast address*). Alamat unicast disebut sebagai alamat logis karena alamat ini merupakan alamat yang diterapkan pada lapisan jaringan dalam DARPA Reference Model dan tidak memiliki relasi yang langsung dengan alamat yang digunakan pada lapisan antarmuka jaringan dalam DARPA Reference Model. Sebagai contoh, alamat *unicast* dapat ditetapkan ke sebuah *host* dengan antarmuka jaringan dengan teknologi Ethernet, yang memiliki alamat MAC sepanjang 48-bit. Alamat *unicast* inilah yang harus digunakan oleh semua *host* TCP/IP agar dapat saling terhubung. Komponen alamat ini terbagi menjadi dua jenis, yakni alamat host (*host identifier*) dan alamat jaringan (*network identifier*). Alamat *unicast* menggunakan kelas A, B, dan C dari kelas-kelas alamat IP yang telah disebutkan sebelumnya, sehingga ruang alamatnya adalah dari 1.x.y.z hingga 223.x.y.z. Sebuah alamat *unicast* dibedakan dengan alamat lainnya dengan menggunakan skema *subnet mask*.

### 2. IPv4 Multicast Addresses

Penugasan terhadap satu atau lebih interface jaringan dengan subnet yang berbeda; digunakan untuk komunikasi satu ke banyak komputer. Alamat IP Multicast (*Multicast IP Address*) adalah alamat yang digunakan untuk menyampaikan satu paket kepada banyak penerima. Dalam sebuah intranet yang memiliki alamat multicast paket yang ditujukan ke sebuah alamat *multicast* akan diteruskan oleh router ke subjaringan di mana terdapat host-host yang sedang berada dalam



kondisi "*listening*" terhadap lalu lintas jaringan yang dikirimkan ke alamat *multicast* tersebut. Dengan cara ini, alamat *multicast* pun menjadi cara yang efisien untuk mengirimkan paket data dari satu sumber ke beberapa tujuan untuk beberapa jenis komunikasi. Alamat *multicast* didefinisikan dalam RFC 1112. Alamat-alamat *multicast* IPv4 didefinisikan dalam ruang alamat **kelas D**, yakni **224.0.0.0/4**, yang berkisar dari 224.0.0.0 hingga 239.255.255.255. Prefiks alamat 224.0.0.0/24 (dari alamat 224.0.0.0 hingga 224.0.0.255) tidak dapat digunakan karena dicadangkan untuk digunakan oleh lalu lintas *multicast* dalam subnet lokal.

### 3. IPv4 Broadcast Addresses

Penugasan terhadap seluruh interface jaringan dalam suatu subnet; digunakan untuk komunikasi satu computer ke semuanya dalam suatu subnet. Alamat *broadcast* untuk IP versi 4 digunakan untuk menyampaikan paket-paket data "satu-untuk-semua". Jika sebuah *host* pengirim yang hendak mengirimkan paket data dengan tujuan alamat *broadcast*, maka semua *node* yang terdapat di dalam segmen jaringan tersebut akan menerima paket tersebut dan memprosesnya. Berbeda dengan alamat *IP unicast* atau alamat *IP multicast*, alamat *IP broadcast* hanya dapat digunakan sebagai alamat tujuan saja, sehingga tidak dapat digunakan sebagai alamat sumber.

Ada empat buah jenis alamat IP *broadcast*, yakni *network broadcast*, *subnet broadcast*, *all subnets-directed broadcast*, dan *Limited Broadcast*. Untuk setiap jenis alamat *broadcast* tersebut, paket IP *broadcast* akan dialamatkan kepada lapisan antarmuka jaringan dengan menggunakan alamat *broadcast* yang dimiliki oleh teknologi antarmuka jaringan yang digunakan. Sebagai contoh, untuk jaringan Ethernet dan Token Ring, semua paket *broadcast* IP akan dikirimkan ke alamat *broadcast* Ethernet dan Token Ring, yakni 0xFF-FF-FF-FF-FF-FF.



**c. Tes Formatif**

1. Kunci pokok suatu protocol adalah.....
  - A. Syntax, Simantic, Timing
  - B. Semantic, Timing, Working
  - C. Timing, Working, Semantic
  - D. Working, Syntax, Semantic
  
2. Macam-macam protocol antara lain, kecuali.....
  - A. Ethernet
  - B. Token Ring
  - C. Local Disk
  - D. Internet
  
3. 192.168.0.10 merupakan contoh pemberian alamat pada sebuah komputer yang akan dihubungkan dalam sebuah jaringan. Angka-angka tersebut dikenal dengan.....
  - A. Protokol
  - B. IP Address
  - C. Konfigurasi
  - D. Domain
  - E. TCP/IP
  
4. Nilai angka digital dan bit adalah.....
  - A. 0 dan 1
  - B. 5 dan 6
  - C. 1 dan 3
  - D. 4 dan 7
  
5. Berapa jumlah maksimum Dhost yang tersedia pada alamat kelas C.....
  - A. 65,534
  - B. 192
  - C. 16,384
  - D. 126
  - E. 254



**d. Lembar Jawaban Tes Formatif**

1. A. Syntax, Semantic, Timing
2. D. Internet
3. B. IP Address
4. A. 0 dan 1
5. E. 254

**e. Lembar Kerja Siswa**

