

Agung supriyono
250209007
D4 MPLM
ALPHA

Soal ;

1. Pengertian jaringan komputer
2. Macam-macam topologi jaringan komputer (kelebihan, kekurangan, karakteristik, gambar)
3. Bagaimana internet bekerja ?
4. Bagaimana internet bekerja ?

Jawab ;

1. Pengertian jaringan komputer;

Secara sederhana, jaringan komputer (atau *computer network*) adalah sekelompok dua atau lebih perangkat komputer yang saling terhubung satu sama lain melalui media komunikasi, dengan tujuan utama untuk berbagi data, informasi, dan sumber daya (seperti *printer*, *server*, atau koneksi internet).

2. Macam-macam topologi ;

1. Topologi Bus



Foto Ini oleh Penulis Tidak Diketahui dilisensikan atas nama CC BY

Topologi Bus menggunakan satu kabel utama (disebut *backbone*) yang menjadi pusat koneksi bagi semua *node* (komputer atau perangkat).

☐ Karakteristik

Semua perangkat terhubung secara linear ke satu kabel panjang tunggal.

Di kedua ujung kabel utama dipasang **terminator** untuk mencegah sinyal memantul.

☐ Kelebihan

- a) **Sederhana:** Pemasangan kabel relatif mudah dan hemat.

- b) **Murah:** Biaya instalasi rendah karena menggunakan kabel yang sedikit.
- **Kekurangan**
- a) **Sulit Troubleshooting:** Sulit mendeteksi masalah pada kabel utama.
- b) **Kepadatan Tinggi (Congestion):** Kinerja jaringan sangat menurun jika banyak perangkat menggunakan jaringan secara bersamaan.
- c) **Gagal Total:** Jika kabel utama putus, seluruh jaringan akan lumpuh.

2. Topologi Ring (Cincin)

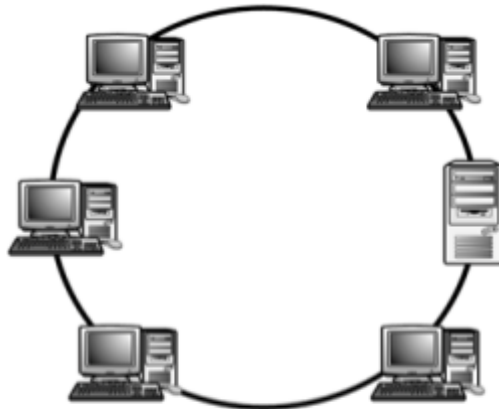


Foto Ini oleh Penulis Tidak Diketahui
dilisensikan atas nama [CC BY-SA](#)

Topologi Ring menghubungkan setiap perangkat ke dua perangkat lainnya, membentuk jalur melingkar (cincin). Data bergerak dalam satu arah, mengelilingi cincin.

Karakteristik

Setiap *node* terhubung langsung ke *node* tetangga di kedua sisi.

Transmisi data terjadi dalam satu arah saja (*unidirectional*).

- **Kelebihan**
- a) **Kinerja Stabil:** Aliran data teratur dan stabil karena tidak ada tabrakan data (kolisi).
- b) **Sederhana:** Kabel yang digunakan tidak rumit.
- **Kekurangan**
- a) **Lambat:** Penambahan atau pemindahan satu perangkat sangat mengganggu jaringan.
- b) **Gagal Sebagian:** Jika satu *node* atau kabel putus, seluruh jaringan bisa terhenti karena jalur terputus.

- c) **Sulit Ekspansi:** Memperluas jaringan sulit karena memerlukan pemutusan sementara koneksi.

3. Topologi Star (Bintang)

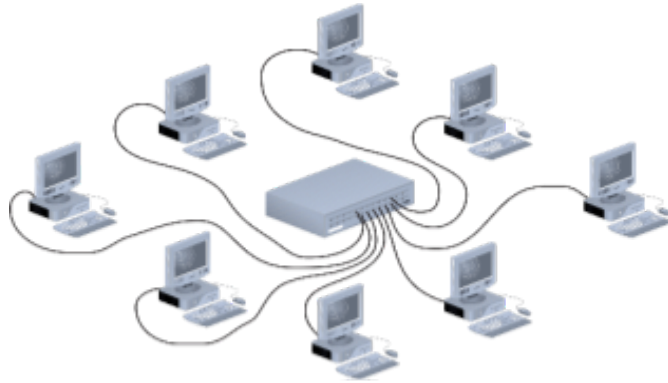


Foto Ini oleh Penulis Tidak Diketahui dilisensikan atas nama [CC BY-SA-NC](#)

Topologi Star menghubungkan semua perangkat secara terpisah ke satu perangkat pusat, seperti **Hub** atau **Switch**. Ini adalah topologi yang paling umum digunakan saat ini.

☐ **Karakteristik**

- a) Semua *node* berkomunikasi melalui perangkat pusat (Hub/Switch).
- b) Setiap *node* memiliki kabel khusus ke perangkat pusat.

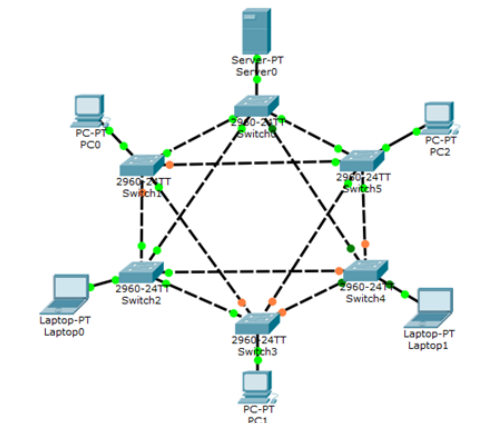
☐ **Kelebihan**

- a) **Mudah:** Kerusakan pada satu kabel hanya memengaruhi *node* tersebut, dan mudah **Fleksibel:** Penambahan atau pemindahan perangkat sangat mudah tanpa mengganggu jaringan lain.
- b) **Troubleshooting** dideteksi.
- c) **Kinerja Baik:** Jika menggunakan *Switch*, kinerja jaringan akan sangat baik.

☐ **Kekurangan**

- a) **Mahal:** Membutuhkan lebih banyak kabel daripada Bus atau Ring.
- b) **Ketergantungan Pusat:** Jika perangkat pusat (Hub/Switch) rusak, seluruh jaringan akan lumpuh.

4. Topologi Mesh



Topologi Mesh menghubungkan setiap *node* ke *node* lainnya dalam jaringan. Ini menciptakan banyak jalur redundan untuk transmisi data.

□ Karakteristik

Terdapat koneksi langsung (titik-ke-titik) antara setiap pasangan perangkat.

Jumlah koneksi yang dibutuhkan pada topologi *Mesh* penuh dapat dihitung dengan rumus $\frac{N(N-1)}{2}$, di mana N adalah jumlah *node*.

□ Kelebihan

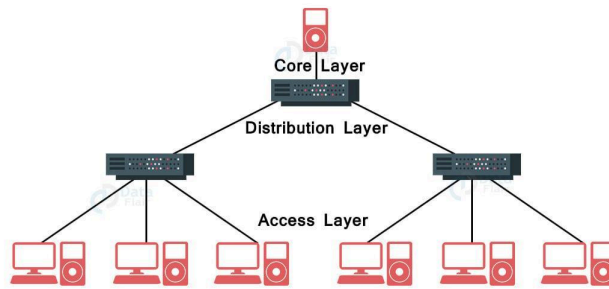
- Sangat *Fault-Tolerant* (Tahan Kegagalan):** Kegagalan satu jalur tidak akan mengganggu komunikasi karena ada banyak jalur alternatif.
- Keamanan Tinggi:** Jalur komunikasi antar perangkat bersifat khusus.
- Beban Terdistribusi:** Lalu lintas data dapat didistribusikan ke banyak jalur.

□ Kekurangan

- Sangat Mahal & Kompleks:** Membutuhkan jumlah kabel dan *port* I/O yang sangat banyak, menjadikannya mahal dan sulit diinstalasi.
- Sulit Diatur:** Pengelolaan kabel dan konfigurasi menjadi sangat rumit.

5. Topologi Tree (Pohon)

Tree Topology



Topologi Tree adalah gabungan dari topologi **Star** yang dihubungkan satu sama lain menggunakan topologi **Bus**. Ini sering disebut *Hierarchical Topology*.

☐ **Karakteristik**

- a) Terdapat *Hub* pusat (*root*) dan *Hub* sekunder yang berfungsi sebagai cabang.
- b) Jaringan diorganisasi secara hierarkis (bertingkat).

☐ **Kelebihan**

- a) **Mudah Diperluas:** Penambahan *node* baru sangat mudah.
- b) **Pengelolaan Terpusat:** Pengelolaan jaringan dilakukan pada pusat *root*.
- c) **Cocok untuk Jaringan Besar:** Ideal untuk jaringan skala besar seperti antar gedung atau lantai.

☐ **Kekurangan**

- a) **Ketergantungan Root:** Jika *Hub* utama (*root*) rusak, seluruh jaringan akan terpengaruh.
- b) **Mahal:** Membutuhkan banyak kabel dan *Hub*.

3. Cara Kerja Internet (Secara Sederhana)

data antar miliaran perangkat. Proses ini diatur oleh serangkaian aturan universal yang dikenal Internet adalah jaringan global raksasa yang bekerja berdasarkan prinsip pengiriman dan penerimaan sebagai **Protokol TCP/IP**.

1. Protokol: Bahasa Universal Internet

Internet menggunakan bahasa standar, yaitu:

- **TCP (*Transmission Control Protocol*):** Bertugas memecah data besar (seperti halaman web atau video) menjadi **paket-paket kecil** sebelum dikirim, dan

memastikan paket-paket tersebut tiba di tujuan **secara utuh dan dalam urutan yang benar**.

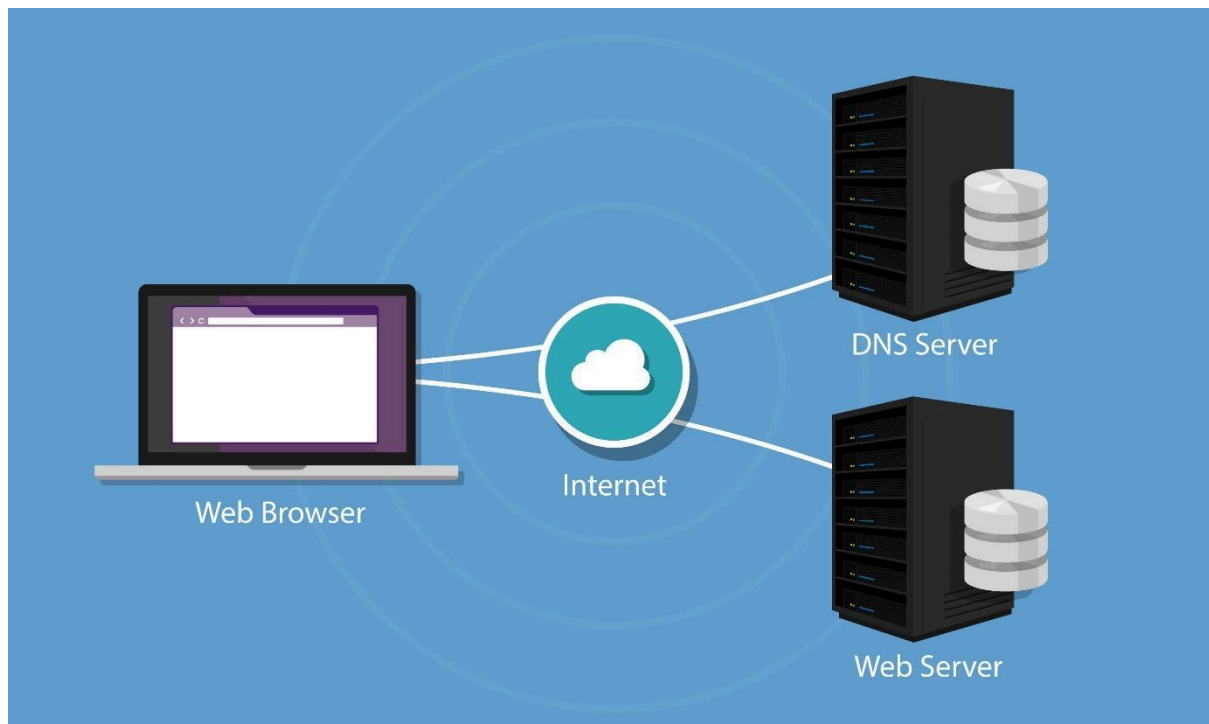
- **IP (*Internet Protocol*)**: Bertugas memberikan **alamat unik (Alamat IP)** kepada setiap perangkat di jaringan, dan berfungsi sebagai "tukang pos" yang memastikan setiap paket data diarahkan melalui jalur yang benar ke alamat IP tujuannya.

2. Tahapan Utama Saat Anda Mengakses Sesuatu

Anggaplah Anda mengetik `www.contoh.com` di *browser*:

Langkah 1: Permintaan DNS (Pencarian Alamat)

- Ketika Anda mengetik nama situs web, perangkat Anda tidak tahu lokasi fisiknya (alamat IP).
- Perangkat Anda segera mengirimkan permintaan ke **Server DNS (*Domain Name System*)**



Shutterstock

- Server DNS bertindak seperti buku telepon internet, menerjemahkan nama domain yang mudah diingat (`www.contoh.com`) menjadi **Alamat IP numerik** (misalnya, `203.0.113.45`).

Langkah 2: Pengiriman Permintaan (Melalui Router)

- Setelah alamat IP server tujuan diketahui, perangkat Anda (sebagai *Client*) membuat koneksi menggunakan TCP/IP.
- Permintaan Anda dikemas menjadi paket data dan dikirimkan keluar.
- Paket ini melewati serangkaian **Router** di sepanjang jalan. Setiap router di jaringan bertugas mengarahkan paket ke rute terbaik berikutnya menuju alamat IP tujuan.

Langkah 3: Server Merespons

- Permintaan tiba di **Server** tujuan (komputer yang menyimpan data www.contoh.com).
- Server memproses permintaan dan mulai mengirimkan data halaman web (teks, gambar, kode) kembali ke perangkat Anda. Data ini juga dipecah menjadi paket-paket kecil.

Langkah 4: Penyusunan Kembali dan Tampilan

- Paket-paket data dari server mungkin mengambil rute yang berbeda-beda.
- Ketika paket-paket ini tiba di perangkat Anda, **TCP memastikan semua paket diterima dan disusun kembali** dalam urutan yang benar.
- *Browser* Anda kemudian membaca dan menerjemahkan data yang telah disusun kembali menjadi halaman web yang utuh, yang Anda lihat di layar.

3. Infrastruktur Fisik

Seluruh proses ini dimungkinkan oleh infrastruktur fisik yang masif, yaitu:

- **ISP (*Internet Service Provider*):** Perusahaan seperti Telkomsel atau Indosat yang menyediakan gerbang bagi perangkat Anda untuk terhubung ke jaringan global.
- **Kabel Serat Optik:** Media transmisi utama yang membentang di bawah tanah dan dasar laut (kabel bawah laut) yang memungkinkan data bergerak cepat antar benua.
- **Peralatan Jaringan:** Modem, *router*, dan *switch* yang bekerja non-stop untuk memodulasi sinyal dan mengarahkan lalu lintas data.

4. Ancaman keamanan internet

1. Malware (Perangkat Lunak Berbahaya)

Ini adalah istilah umum untuk perangkat lunak yang dirancang untuk merusak, melumpuhkan, atau mendapatkan akses tidak sah ke sistem komputer.

- a) **Virus:** Program yang menyebar dengan menempelkan dirinya pada *file* yang sah.

- b) **Worm:** Mirip virus tetapi dapat mereplikasi diri dan menyebar ke seluruh jaringan tanpa memerlukan interaksi pengguna.
- c) **Trojan (*Trojan Horse*):** Program jahat yang menyamar sebagai *software* legal dan berguna untuk mencuri informasi.
- d) **Spyware:** Program yang diam-diam memantau aktivitas Anda (*keyboard strokes*, *browser history*) dan mengirimkannya ke pihak ketiga.

2. Ransomware

- Jenis *malware* yang mengenkripsi (mengunci) *file* atau seluruh sistem komputer korban dan menuntut tebusan (*ransom*)—biasanya dalam bentuk *cryptocurrency*—agar korban bisa mendapatkan kembali aksesnya. Ini adalah ancaman yang sangat merusak bagi individu maupun perusahaan.

3. Phishing dan Social Engineering

Ini adalah taktik manipulasi psikologis untuk menipu pengguna agar mengungkapkan informasi sensitif.

- a) **Phishing:** Upaya penipuan melalui email, SMS, atau pesan palsu yang menyamar sebagai entitas tepercaya (bank, layanan *online*, atau perusahaan) untuk mencuri kredensial (*username* dan *password*).
- b) **Social Engineering:** Teknik yang memanfaatkan kelemahan manusia (rasa ingin tahu, ketakutan, atau keinginan membantu) untuk mendapatkan akses ke sistem atau informasi.

4. Serangan DDoS (*Distributed Denial of Service*)

- a) Upaya untuk **membanjiri server**, situs web, atau sumber daya jaringan dengan lalu lintas yang sangat besar dari banyak komputer yang terinfeksi (*botnet*).
- b) Tujuannya adalah membuat *server* tersebut kewalahan dan **tidak dapat diakses** oleh pengguna yang sah.

5. SQL Injection dan Cross-Site Scripting (XSS)

Ini adalah ancaman yang menargetkan **aplikasi web** (situs *e-commerce*, portal, dll.).

- a) **SQL Injection:** Penyerang menyisipkan kode berbahaya ke dalam *input* formulir web untuk mengakses, mengubah, atau menghapus data sensitif di *database* aplikasi.
- b) **XSS:** Penyerang menyuntikkan *script* berbahaya ke dalam situs web yang kemudian dijalankan di *browser* pengguna lain.

6. Man-in-the-Middle (MITM) Attack

Penyerang secara diam-diam mencegat dan mungkin mengubah komunikasi antara dua pihak yang percaya bahwa mereka sedang berkomunikasi secara langsung.

Ini sering terjadi di jaringan Wi-Fi publik yang tidak aman, di mana penyerang dapat mencuri data yang tidak dienkripsi.

7. Kerentanan Perangkat Lunak (*Software Vulnerabilities*)

Celah atau kesalahan dalam kode perangkat lunak (sistem operasi, *browser*, aplikasi) yang belum diperbaiki.

Penyerang dapat mengeksploitasi kerentanan ini (*zero-day exploit*) untuk mendapatkan akses tidak sah ke sistem.