



Kurikulum
Merdeka

SMK Kelas X TJKT

PRINSIP DASAR TCP/IP DAN ALAMAT IP



Disusun oleh : Ferju Prihamdani

Teknologi adalah salah satu unsur pokok dalam pembangunan yang terencana. Tanpa adanya perkembangan teknologi, maka perubahan zaman tidak akan secepat Tanpa adanya perkembangan teknologi, maka perubahan zaman tidak akan secepat dan secanggih seperti sekarang. Adapun kecanggihan teknologi informasi yang kita dan secanggih seperti sekarang. Adapun kecanggihan teknologi informasi yang kita nikmati saat ini merupakan buah hasil yang dimulai dari proses panjang puluhan nikmati saat ini merupakan buah hasil yang dimulai dari proses panjang puluhan atau bahkan ratusan tahun kebelakang.

Terlepas dari pesatnya evolusi teknologi, dampak positif maupun negatif di Terlepas dari pesatnya evolusi teknologi, dampak positif maupun negatif di lingkungan pun tidak bisa dihindarkan. Tidak hanya berdampak ke sektor komunikasi, lingkungan pun tidak bisa dihindarkan. Tidak hanya berdampak ke sektor komunikasi, namun juga terasa hingga sektor pendidikan, manufaktur, kesehatan, hingga sistem namun juga terasa hingga sektor pendidikan, manufaktur, kesehatan, hingga sistem pertahanan.



1. Prinsip Dasar TCP/IP

A. Model OSI vs Model TCP/IP

- 1) Model OSI (Open Systems Interconnection): Model referensi 7 lapisan yang digunakan untuk standarisasi komunikasi jaringan. Lapisan-lapisan tersebut adalah:
 - a. Physical – Media fisik komunikasi (kabel, sinyal, konektor).
 - b. Data Link – Pengalamatan MAC, pengendalian akses media.
 - c. Network – Routing dan pengalamatan IP.
 - d. Transport – Pengendalian aliran data (TCP, UDP).
 - e. Session – Pengelolaan sesi komunikasi antar aplikasi.
 - f. Presentation – Enkripsi, kompresi, encoding data.
 - g. Application – Antarmuka aplikasi pengguna (HTTP, FTP, SMTP).

Tabel 1. Model OSI dan Model TCP/IP

Lapisan (Layer)	Model OSI	Lapisan (Layer)	Model TCP/IP Update
7	<i>Application</i>	5	<i>Application</i>
6	<i>Presentation</i>		
5	<i>Session</i>		
4	<i>Transport</i>	4	<i>Transport</i>
3	<i>Network</i>	3	<i>Network</i>
2	<i>Data Link</i>	2	<i>Data Link</i>
1	<i>Physical</i>	1	<i>Physical</i>

Pada Tabel 1 terlihat bahwa model OSI memiliki tujuh lapisan. Pada model tersebut, lapisan Application, Presentation, dan Session digabungkan menjadi satu lapisan saja (lapisan ke-5) pada model TCP/ IP, yaitu Application. Adapun keempat lapisan lainnya sama, yaitu pada lapisan ke-1 hingga lapisan ke-4.

2) Model TCP/IP: Model 4 lapisan yang digunakan secara praktis dalam komunikasi internet.

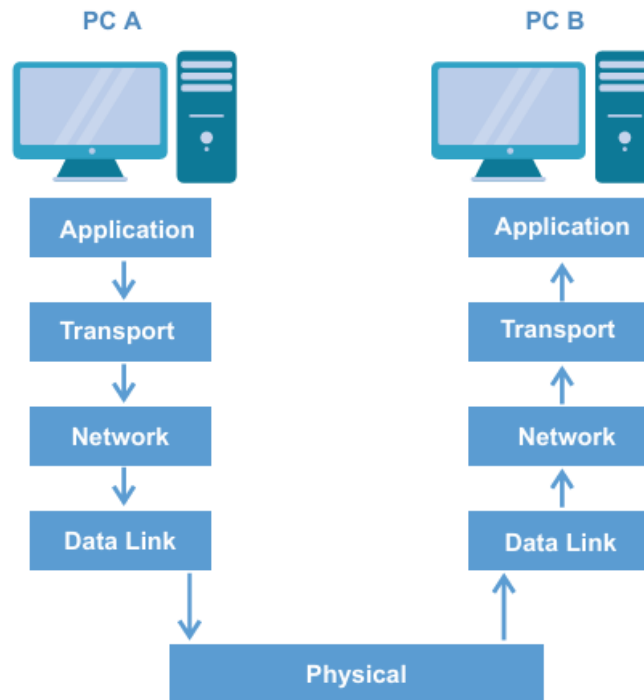
Lapisan-lapisan tersebut adalah:

- a. Network Interface (Link Layer) – Lapisan fisik dan data link.
- b. Internet Layer – Bertanggung jawab atas pengalamatan dan routing data (IP, ICMP, ARP).
- c. Transport Layer – Protokol komunikasi antar host (TCP, UDP).
- d. Application Layer – Protokol aplikasi seperti HTTP, FTP, DNS.

Tabel 2. Fungsi Lapisan pada Model TCP/IP

Lapisan	Nama Lapisan	Fungsi
5	<i>Application</i>	Menyediakan akses pengguna dengan aplikasi perangkat lunak, seperti HTTP, FTP, dan SMTP.
4	<i>Transport</i>	Memecahkan paket menjadi lebih kecil, memberikan <i>sequence number</i> , memberikan ACK, <i>error recovery</i> , serta mentransmisikan data melalui TCP dan UDP.
3	<i>Network</i>	Memberikan <i>header</i> , seperti alamat IP sumber dan tujuan, <i>port</i> sumber dan tujuan, serta informasi <i>routing</i> protokol.
2	<i>Data Link</i>	Lapisan ini berisi aturan media koneksi. Sinyal data dialirkan melalui media koneksi, alamat MAC, dan ethernet standar.
1	<i>Physical</i>	Berisi segala hal tentang komponen fisik jaringan, seperti media kabel dan <i>network interface</i> .

Berdasarkan fungsi-fungsi dari lapisan TCP/IP, transmisi data dari komputer sumber ke komputer tujuan dapat diilustrasikan seperti pada gambar berikut.



Gambar 1. Konsep Data Transmisi Model TCP/IP

Prinsip kerja model lapisan TCP/IP adalah sebagai berikut:


- 1) Pada PC A, pengguna dimisalkan menggunakan aplikasi HTTP untuk mengirimkan berkas (file) ke PC B. Pada saat ini, pengguna berada pada lapisan paling atas atau lapisan ke-5 dari model TCP/IP terbaru (update), yaitu Application. Pada tahap ini akan ditambahkan header application.
- 2) Selanjutnya, data dari lapisan Application diturunkan ke lapisan Transport. Dua layanan yang diberikan dalam lapisan ini, yaitu TCP (transmission control protocol) dan UDP (user data protocol).
- 3) Setelah mendapatkan header dari lapisan Transport, data diturunkan ke lapisan Network/Internet. Dalam lapisan ini akan ditambahkan header yang berisi alamat IP tujuan, routing protokol, dan hal lain yang berhubungan dengan pengalaman jaringan.
- 4) Setelah mendapatkan header dari lapisan Network, data diturunkan ke lapisan Data Link untuk diberikan header dan trailer. Pada bagian ini, data akan berurusan dengan aturan media koneksi, sinyal data dialirkan melalui media koneksi alamat MAC. Selanjutnya, data diteruskan ke lapisan terakhir.
- 5) Lapisan terakhir dari PC A berupa perangkat fisik jaringan, yaitu kartu jaringan dan media koneksi. Lapisan tersebut menjadi lapisan pertama dari PC B. Data yang dikirim PC A akan diterima di lapisan fisik dan diteruskan ke lapisan di atasnya, dari PC B, kemudian diteruskan hingga lapisan terakhir, yaitu lapisan ke-5 (Application). Pada lapisan ini, dilakukan decapsulation pada data.

3) Perbedaan utama OSI vs TCP/IP:

- a. OSI lebih konseptual dan detail, sedangkan TCP/IP lebih praktis dan digunakan dalam jaringan modern.
- b. TCP/IP menggabungkan beberapa lapisan OSI menjadi satu, misalnya sesi dan presentasi digabung ke dalam lapisan aplikasi.

B. Pengalamatan IP (IPv4 & IPv6)

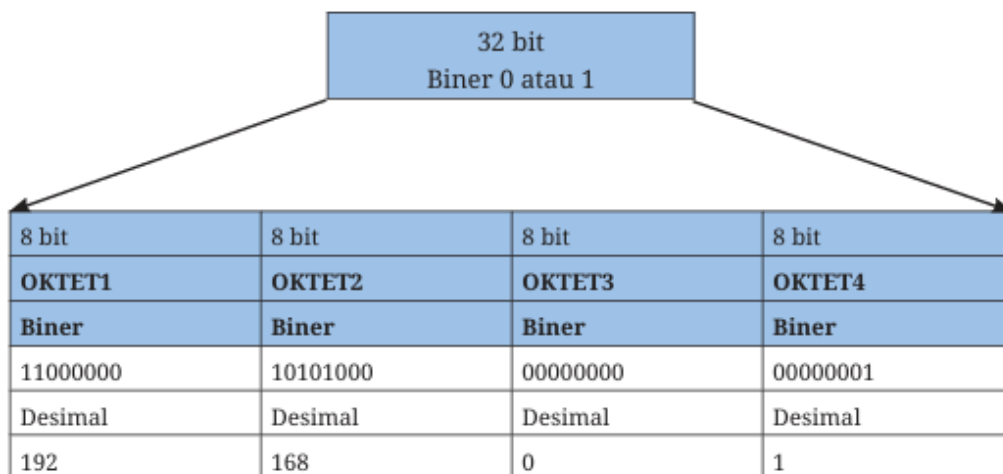
Internet Protocol menempati lapisan model TCP/IP terbaru pada lapisan ketiga, yaitu Network, yang berfungsi menyediakan informasi alamat IP sumber, alamat IP tujuan, dan routing protokol. Setiap perangkat akhir pengguna pasti memiliki alamat yang disebut alamat IP (IP address) dan setiap paket yang dikirim akan diperiksa alamat IP tujuannya. Jika berada di luar jaringan, routing jaringannya akan diperiksa. Dengan demikian, jika kalian berpikir tentang alamat IP, hal itu adalah bagian dari protokol TCP/IP pada lapisan ketiga.

**Apakah Kalian Tahu?**

- Bit adalah bilangan biner dengan nilai 0 dan 1.
- 1 *byte* sama dengan 8 bit. Berapa *byte* 32 bit?
- 1 *oktet* sama dengan 8 bit. Jika alamat IP terdiri dari bilangan 32 bit, berapa oktet alamat IP tersebut?

1) IPv4

- a. Format: 32-bit, terdiri dari 4 oktet (contoh: 192.168.1.1).



Gambar 2. Format Penulisan Alamat IPv4

b. Kelas Alamat IP

Untuk mempermudah penggunaan alamat IPv4 sehingga dapat disesuaikan dengan kebutuhan jaringan seperti jumlah pengguna atau host, alamat IPv4 dikelompokkan berdasarkan kelas alamat IP. Pengelompokan mengacu pada jumlah network dan jumlah host. Dengan demikian, dalam penggunaannya akan terdapat jumlah ruang network yang sedikit, namun jumlah ruang host (dapat berupa perangkat akhir pengguna) yang banyak; atau kebutuhan ruang network yang banyak, namun kebutuhan ruang host sedikit

Kelas A				
8 bit	8 bit	8 bit	8 bit	Total 32 bit dapat ditulis /8
Network	Host	Host	Host	
Kelas B				
8 bit	8 bit	8 bit	8 bit	Total 32 bit dapat ditulis /16
Network	Network	Host	Host	
Kelas C				
8 bit	8 bit	8 bit	8 bit	Total 32 bit dapat ditulis /24
Network	Network	Network	Host	
Kelas D				
Multicast Network				
Kelas E				
Research				

Gambar 3. Kelas Alamat IPv4

- c. Jenis alamat: Public, Private, Loopback, Multicast.
- d. Masalah keterbatasan jumlah alamat mendorong peralihan ke IPv6.

2) IPv6

- a. Format: 128-bit, ditulis dalam bentuk heksadesimal (contoh: 2001:db8::1).
- b. Keunggulan: Lebih banyak alamat, keamanan lebih baik, mendukung auto-configuration.

C. Subnetting dan Routing

- 1) Subnetting: Teknik membagi jaringan besar menjadi jaringan-jaringan lebih kecil untuk efisiensi penggunaan IP.
 - a. Contoh: Dari jaringan **192.168.1.0/24**, bisa dibuat subnet lebih kecil seperti **192.168.1.0/26**.
 - b. Menggunakan **Subnet Mask** untuk menentukan jumlah host dalam suatu subnet.
- 2) Routing: Proses meneruskan paket data dari satu jaringan ke jaringan lain melalui router.
 - a. Static Routing – Konfigurasi manual oleh administrator jaringan.
 - b. Dynamic Routing – Menggunakan protokol seperti RIP, OSPF, dan BGP untuk pembaruan otomatis jalur terbaik.

2. Sistem Layanan Jaringan

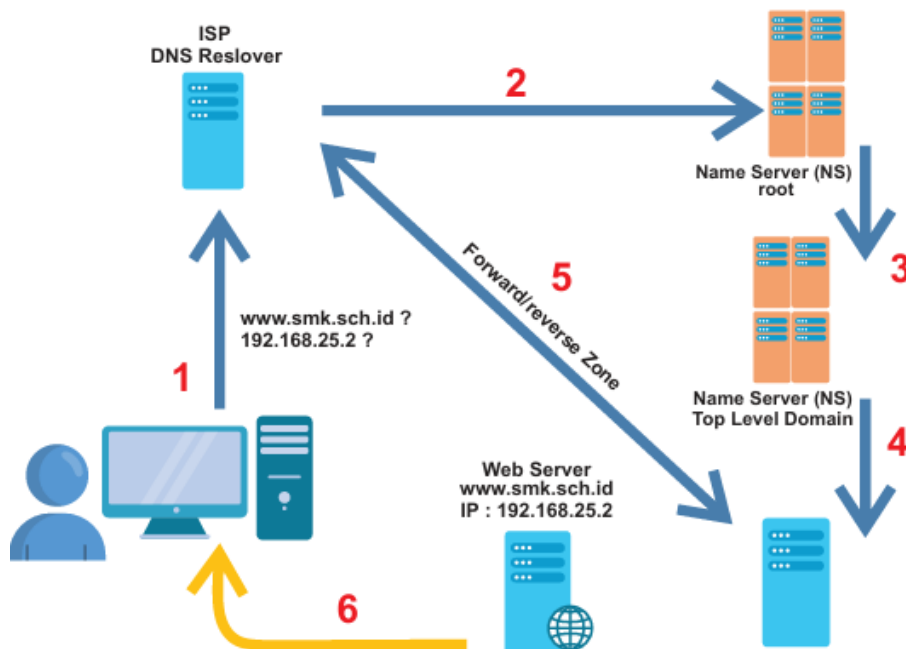
A. DNS, DHCP, Web Server

1) DNS (Domain Name System)

DNS server digunakan untuk menerjemahkan nama domain atau situs web menjadi alamat IP web server, atau sebaliknya, menerjemahkan alamat IP menjadi nama domain. Terdapat tingkatan dalam sebuah DNS. Urutan tertinggi adalah DNS root server yang disebut Top Level Domain (TLD)—di bawah domain root server, terdapat beberapa domain. TLD merupakan ranah tingkat teratas dari sebuah domain. Beberapa TLD yang cukup dikenal luas, antara lain:

- “.com” (commercial organizations). Contoh domain yang digunakan: www.detik.com dan kompas.com
 - “.edu” (educational institutions). Contoh domain yang digunakan: www.upi.edu
 - “.gov” (government institutions). Contoh domain yang digunakan: www.usa.gov
 - “.org” (nonprofit organizations). Contoh domain yang digunakan: en.wikipedia.org
- Mengubah nama domain menjadi alamat IP.

Contoh: www.google.com diterjemahkan menjadi 142.250.180.14.



Gambar 4. Prinsip Kerja Layanan DNS

Prinsip Kerja Layanan DNS

- (1) Jika kalian membutuhkan informasi laman situs web dan mengetikkan **www.smk.sch.id**, kalian tidak mengetahui berapa alamat IP dari server tersebut. Informasi tersebut akan dikirim ke sebuah DNS *Resolver* milik ISP.
- (2) Selanjutnya, informasi diteruskan pada DNS *Root* untuk mencari informasi tentang alamat IP yang dimiliki domain tersebut.
- (3) DNS *Root* tidak memiliki informasi keberadaan nama domain tersebut, kemudian meneruskan pada *Name Server* dari *Top Level Domain* di bawahnya, seperti “.com”, “.edu”, dan “.org”. *Top Level Domain* akan menyarankan pencarian pada sebuah *Name Server* dari zona tertentu yang dimiliki, yaitu *Name Server* MyTelco.com.
- (4) Informasi yang dimiliki oleh NS.MyTelco.com mengatakan bahwa domain www.smk.sch.id menggunakan alamat IP 192.168.25.2. Menerjemahkan nama domain menjadi informasi alamat IP adalah fungsi *forward zone* dalam sebuah DNS Server. Adapun untuk mengembalikannya (menerjemahkan alamat IP menjadi nama domain) adalah fungsi *reverse zone* dalam sebuah DNS Server.
- (5) Selanjutnya, informasi tersebut dikirim ke DNS *Resolver* di ISP untuk diteruskan kepada pengguna, yaitu kalian.
- (6) Setelah informasi tentang alamat server didapat, komputer kalian secara otomatis akan berkomunikasi melalui internet dan *router* ke server www.smk.sch.id.

2) DHCP (Dynamic Host Configuration Protocol)

Untuk memberikan pengalamatan IP satu per satu pada seluruh komputer di sekolah kalian, tentunya itu adalah pekerjaan yang berat. Untungnya, terdapat sebuah layanan yang dapat memberikan alamat IP secara otomatis sesuai dengan network yang dimiliki. Layanan tersebut disebut DHCP Server—DHCP singkatan dari Dynamic Host Configuration Protocol. Protokol ini memiliki prinsip kerja seperti pada Gambar berikut:



Gambar 5. Prinsip Kerja Layanan DHCP

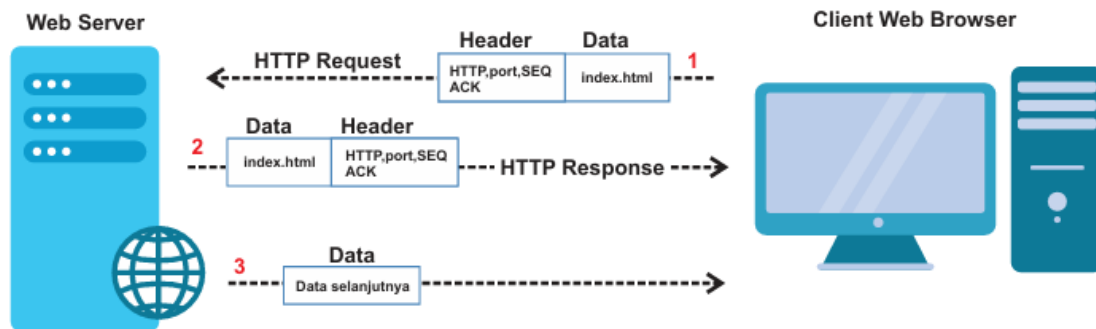
Prinsip Kerja Layanan DHCP

- (1) Sebuah komputer atau perangkat akhir pengguna—yang telah dikonfigurasi untuk mendapatkan alamat IP otomatis atau sebagai *DHCP Client*—akan mencari layanan DHCP dalam jaringan. Proses ini disebut **DHCP Discover**, yaitu komputer klien akan memberikan pesan *broadcast* pada jaringan untuk mencari layanan DHCP Server.
- (2) Server yang mendengar *broadcast* dari klien akan mengirimkan pesan *DHCP Offering*, yaitu penawaran tentang peminjaman alamat IP sementara pada klien. *DHCP Offering* berisi alamat IP dan batas waktu penggunaan alamat IP atau sering disebut **DHCP Lease**.
- (3) Setelah server mengirimkan pesan *DHCP Offering*, komputer klien membalas pesan tersebut dengan mengirimkan *DHCP Request*, yang berisi bahwa klien telah menerima *DHCP Offering* dan meminjam alamat IP berikut jangka waktu yang diberikan.
- (4) Selanjutnya, setelah *DHCP Request* diterima oleh server, server akan membalas dengan *DHCP Acknowledge*. Pesan ini memberikan hak penggunaan alamat IP yang ditawarkan. Jika server tidak dapat memenuhi *DHCP Request* dari klien, server akan mengirimkan pesan *DHCP Negative Acknowledgement*.

- a. Mengotomatiskan pemberian alamat IP ke perangkat dalam jaringan.
- b. Mempermudah administrasi jaringan dengan mencegah konflik IP.

3) Web Server

a. Prinsip Kerja Layanan HTTP (Web Server)



Gambar 6. Prinsip Kerja Layanan Web

Prinsip Kerja Layanan Web

- (1) *Web Browser* dari klien (*client*) mengirimkan *HTTP Request*. Data tersebut dapat berupa permintaan informasi *file* default.html atau index.html.
- (2) Web Server memberikan *HTTP Response* berupa data yang dilampiri oleh *header*. Data tersebut dapat berupa informasi *file* default.html atau index.html dan akan ditampilkan dalam *Web Browser* klien, namun jika index.html tidak ditemukan, Web Server akan mengirimkan kode “HTTP reply 404”.



Gambar 6.16 Tangkapan Layar “HTTP Reply 404” dari Mesin Pencari Google

Sumber: Agung Puspita Bantala (2022)

- (3) Langkah selanjutnya menunjukkan pesan dari Web Server ke *Web Browser* klien, mengirimkan beberapa pesan HTTP dengan bagian *file* masing-masing.

- b. Layanan yang meng-hosting situs web (contoh: Apache, Nginx).
- c. Menggunakan protokol **HTTP/HTTPS** untuk komunikasi dengan klien.

B. Konfigurasi Dasar Layanan Jaringan

1) Konfigurasi DNS Server

- a. Instalasi DNS server (misal: Bind9 pada Linux).
- b. Menambahkan A Record, CNAME, MX Record untuk domain.

C. Konfigurasi DHCP Server

- a. Menentukan rentang IP yang dialokasikan (192.168.1.100 - 192.168.1.200).

- b. Mengatur lease time dan opsi tambahan (Gateway, DNS).

D. Konfigurasi Web Server

- a. Instalasi web server (Apache/Nginx).
- b. Menentukan Virtual Host untuk menangani banyak domain.

3. Keamanan Jaringan

A. Firewall, Enkripsi, Serangan MITM

- 1) Firewall
 - a. Mengontrol lalu lintas jaringan berdasarkan aturan yang ditentukan.
 - b. Jenis: Packet Filtering, Stateful Inspection, Application Gateway.
- 2) Enkripsi
 - a. Mengamankan data dengan algoritma seperti AES, RSA, SSL/TLS.
 - b. Digunakan dalam VPN, HTTPS, SSH.
- 3) Serangan MITM (Man-In-The-Middle)
 - a. Teknik penyadapan komunikasi antara dua pihak tanpa sepengetahuan mereka.
 - b. Pencegahan: SSL/TLS, VPN, DNSSEC, Two-Factor Authentication.

B. Keamanan Jaringan Nirkabel

- 1) Metode Keamanan Wi-Fi
 - a. WPA2/WPA3 untuk enkripsi jaringan nirkabel.
 - b. Penggunaan MAC Filtering untuk membatasi akses perangkat tertentu.
- 2) Serangan pada Jaringan Nirkabel:
 - a. Evil Twin Attack – Membuat jaringan palsu untuk mencuri data pengguna.
 - b. Deauthentication Attack – Memutuskan koneksi pengguna dari jaringan asli.
- 3) Solusi Keamanan:
 - a. Menyembunyikan SSID, menggunakan VPN, dan menerapkan Intrusion Detection System (IDS).

4. Sistem Telekomunikasi

A. Jaringan Seluler (3G, 4G, 5G)

- 1) 3G: Kecepatan hingga 2 Mbps, mendukung panggilan video dan internet dasar.
- 2) 4G (LTE): Kecepatan lebih tinggi (100 Mbps - 1 Gbps), mendukung streaming HD dan VoLTE.
- 3) 5G: Kecepatan hingga 10 Gbps, latensi rendah, mendukung IoT dan kendaraan otonom.

B. Teknologi Microwave, VSAT IP, Fiber Optik, WLAN

- 1) Microwave
 - a. Komunikasi nirkabel dengan frekuensi tinggi (6 GHz - 38 GHz).
 - b. Digunakan untuk Backhaul Network dan komunikasi antar tower BTS.

- 2) VSAT IP (Very Small Aperture Terminal)
 - a. Teknologi satelit yang memungkinkan komunikasi di daerah terpencil.
 - b. Digunakan untuk perbankan, militer, dan jaringan bisnis global.
- 3) Fiber Optik
 - a. Media transmisi berbasis cahaya dengan kecepatan tinggi dan latensi rendah.
 - b. Digunakan dalam backbone internet dan jaringan metropolitan (MAN).
- 4) WLAN (Wireless Local Area Network)
 - a. Teknologi jaringan nirkabel berbasis standar **IEEE 802.11 (Wi-Fi)**.
 - b. Mendukung jaringan lokal tanpa kabel dengan cakupan terbatas.