

## **1 FTP (File Transfer Protocol)**

### ◆ Pengertian FTP

FTP adalah **protokol jaringan** yang digunakan untuk **mengirim dan mengambil file** antara:

- **client** (komputer kita)
- **server** (komputer penyedia file)

Contoh gampang:

👉 kamu upload file ke server / download file dari server kampus.

---

### ◆ Cara Kerja FTP (PENTING)

FTP menggunakan **2 koneksi**, ini sering keluar di ujian:

#### 1. Control Connection

- Untuk perintah (login, ls, get, put)
- **Port: 21**

#### 2. Data Connection

- Untuk transfer file
- Port tergantung mode (ini yang sering bikin bingung)

📌 Jadi ingat:

FTP ≠ satu koneksi, tapi **dua koneksi**

---

### ◆ Mode FTP

Ada **2 mode**, ini WAJIB kamu tahu:

#### 1. Active Mode

- Client → Server lewat **port 21** (control)
- Server → Client lewat **port 20** (data)

📌 Kekurangan:

- Client harus buka port → **sering diblok firewall**

#### 2. Passive Mode

- Client → Server (control **dan** data)

- Server kasih port random (>1023)

📌 Kelebihan:

- Lebih aman
- Lebih sering dipakai sekarang

🧠 Tips hafalan:

**Passive = client yang aktif semua**

---

#### ◆ Port FTP (INI SERING DITANYA)

**Fungsi                      Port**

FTP Control        **21**

FTP Data (Active) **20**

Kalau soal pilihan ganda:

“FTP berjalan pada port?”

Jawaban aman: **21**

---

#### ◆ Kelemahan FTP

✗ Username & password **tidak terenkripsi**

✗ Data dikirim dalam bentuk **plain text**

Makanya FTP jarang dipakai di jaringan modern tanpa pengamanan tambahan.

---

#### ◆ Perbandingan FTP vs SFTP vs FTPS

Protokol	Aman?	Keterangan
FTP	✗	Tidak terenkripsi
FTPS	✓	FTP + SSL/TLS
SFTP	✓	Lewat SSH (port 22)

📌 Jangan ketukar:

- **SFTP ≠ Secure FTP**
- SFTP itu **SSH File Transfer Protocol**

## 2 Telnet & Port Telnet

### ◆ Pengertian Telnet

Telnet adalah **protokol jaringan** yang digunakan untuk:

- remote login
- mengakses komputer / server **jarak jauh** melalui **command line (teks)**.

Contoh gampang:

👉 kamu login ke server dari komputer lain dan ngetik perintah langsung.

---

### ◆ Port Telnet (WAJIB HAFAL)

#### 📌 Telnet berjalan pada port: 23

Kalau ada soal:

“Port default Telnet adalah ...”

Jawaban: **23**

---

### ◆ Cara Kerja Telnet (Sederhana)

1. Client membuka koneksi ke server
2. Client login (username & password)
3. Semua perintah diketik via teks
4. Server menjalankan perintah

#### 📌 Masalah besar Telnet:

Semua data (termasuk password) dikirim **TANPA enkripsi** 😱

---

### ◆ Kelemahan Telnet (INI SERING DITANYA)

- ✗ Tidak aman
- ✗ Password dikirim dalam **plain text**
- ✗ Mudah disadap (sniffing)

Makanya:

**Telnet jarang dipakai di jaringan modern**

---

#### ◆ Telnet vs SSH (PERBANDINGAN)

Ini favorit soal teori 🍦

Aspek	Telnet	SSH
Port	23	22
Enkripsi	✗ Tidak ada	✓ Ada
Keamanan	Rendah	Tinggi
Penggunaan	Lama	Modern

💡 Tips hafalan:

**Telnet = Tua & Tidak Aman**

**SSH = Secure**

---

#### ◆ Kapan Telnet Masih Dipakai?

- Simulasi jaringan (Cisco Packet Tracer)
- Pembelajaran
- Jaringan internal (terbatas)

### 3 Network Layer → Physical Layer

(OSI Layer 3, 2, dan 1)

Model OSI punya **7 layer**, tapi di sini kita fokus ke **Layer 3 sampai Layer 1**.

💡 Urutan dari atas ke bawah:

**Network → Data Link → Physical**

---

#### ◆ Layer 3 – Network Layer

##### 📌 Fungsi Utama

- Pengalamatan logis (IP Address)
- Routing (menentukan jalur paket)
- Mengirim data **antar jaringan** (beda network)

📌 Kalau ada IP → pasti Network Layer

---

### 📌 Contoh di Network Layer

- IP Address (IPv4, IPv6)
- Router
- Protokol: **IP, ICMP**

📌 Router kerja di **Layer 3**, ini wajib ingat.

---

### 📌 Contoh Kasus

Kalau komputer kamu kirim data ke server **beda jaringan**, yang menentukan jalurnya adalah **Network Layer**.

---

## ◆ Layer 2 – Data Link Layer

### 📌 Fungsi Utama

- Pengalamatan fisik (**MAC Address**)
- Framing (memecah data jadi frame)
- Error detection
- Mengatur komunikasi **dalam satu jaringan**

📌 Kalau MAC Address → **Data Link Layer**

---

### 📌 Sub-layer di Data Link

1. **LLC (Logical Link Control)**
  2. **MAC (Media Access Control)**
- 

### 📌 Contoh di Data Link Layer

- MAC Address (contoh: 00:1A:2B:3C:4D:5E)
- Switch
- Protokol: Ethernet, ARP

📌 **Switch bekerja di Layer 2**

---

### Contoh Kasus

- Komputer A kirim data ke komputer B **dalam satu LAN**  
→ Data Link Layer yang mengatur.
- 

### Layer 1 – Physical Layer

#### Fungsi Utama

- Mengirim **bit (0 dan 1)**
- Media fisik
- Sinyal listrik / cahaya / gelombang radio

 Layer ini **tidak peduli data isinya apa**, yang penting terkirim.

---

#### Contoh di Physical Layer

- Kabel UTP
- Fiber Optic
- Wireless signal
- Repeater, Hub

 Repeater & Hub = **Layer 1**

---

### Perbandingan Singkat

Layer	Fokus	Contoh
Layer 3	IP & routing	Router, IP
Layer 2	MAC & frame	Switch, MAC
Layer 1	Sinyal fisik	Kabel, Hub

---

### Tips Hafalan Cepat

- IP → Layer 3
- MAC → Layer 2

- **Kabel** → Layer 1
- **Router** → L3
- **Switch** → L2
- **Hub** → L1

## 4 IPv4 & IPv6

### ◆ Apa itu IP Address?

**IP Address** = alamat unik sebuah device di jaringan.  
Fungsinya biar data **tahu ke mana harus dikirim**.

Ibarat:

- Nama orang 
  - **Alamat rumah** 
- 

## ◆ IPv4

### 📌 Bentuk IPv4

IPv4 terdiri dari **32 bit**, ditulis jadi **4 oktet**.

Contoh:

192.168.1.10

 Setiap oktet nilainya **0 – 255**

Kenapa 255?

Karena 1 oktet = **8 bit**

11111111 (biner) = 255 (desimal)

---

### 📌 Struktur IPv4

[ Network ID ] [ Host ID ]

- **Network ID** → alamat jaringannya
- **Host ID** → alamat device di jaringan itu

 Ini penting banget buat **class IP & subnetting** nanti.

---

## (Sedikit) Dasar Hitungan Biner (PELAAAAN YA)

1 bit cuma punya 2 nilai:

0 atau 1

8 bit (1 oktet):

128 64 32 16 8 4 2 1

Contoh:

$$11000000 = 128 + 64 = 192$$

 Ini keapek nanti buat subnet, tapi **kita ulang terus**, santai.

---

## IPv6

### Kenapa IPv6 Dibuat?

Karena **IPv4 hampir habis** 😱

- IPv4: ±4,3 miliar alamat
  - IPv6: **sangat banyak** ( $2^{128}$ )
- 

### Bentuk IPv6

IPv6 = **128 bit**, ditulis heksadesimal.

Contoh:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Boleh disingkat jadi:

2001:db8:85a3::8a2e:370:7334

 Aturan singkat IPv6:

- Nol berturut-turut → :: (hanya boleh **sekali**)
- 

## Perbandingan IPv4 vs IPv6

Aspek	IPv4	IPv6
Panjang	32 bit	128 bit
Bentuk	Desimal	Heksadesimal

Contoh	192.168.1.1	2001:db8::1
NAT	Perlu	Tidak perlu
Keamanan	Optional	Built-in

## 5 Data Modelling Language (DML)

### ◆ Apa itu DML?

DML (Data Manipulation Language) adalah **bahasa** yang digunakan untuk:

👉 mengolah data di database

Biasanya dipakai di:

- Server
- Sistem informasi
- Aplikasi jaringan (server login, data user, log, dll)

📌 DML adalah **bagian dari SQL**.

---

### ◆ Fungsi Utama DML

DML dipakai untuk:

- Menambah data
  - Mengubah data
  - Menghapus data
  - Menampilkan data
- 

### ◆ Perintah-perintah DML (WAJIB HAFAL)

#### 1 INSERT

Menambahkan data

```
INSERT INTO user VALUES ('001', 'Andi');
```

---

#### 2 SELECT

Menampilkan data

```
SELECT * FROM user;
```

📌 Ini yang **paling sering dipakai**

---

### 3 UPDATE

Mengubah data

```
UPDATE user SET nama='Budi' WHERE id='001';
```

---

### 4 DELETE

Menghapus data

```
DELETE FROM user WHERE id='001';
```

---

#### ◆ DML vs DDL (JANGAN KETUKER)

Ini sering jadi soal jebakan ⚡

**DML**      **DDL**

Mengolah data Mengatur struktur

INSERT      CREATE

SELECT      ALTER

UPDATE      DROP

DELETE      TRUNCATE

🧠 Tips hafalan:

**DML = Data-nya**

**DDL = Tabel-nya**

---

#### ◆ Hubungan DML dengan Jaringan

Kenapa DML masuk materi **Jaringan Komputer?**

Contoh:

- Server DHCP simpan data client
- Server AAA simpan data user

- Server login pakai database
- 📌 Semua itu pakai **DML di sisi server.**

## 6 Repeater & Routing

### ♦ A. Repeater

#### 📌 Pengertian Repeater

**Repeater** adalah **perangkat jaringan** yang berfungsi untuk:

👉 memperkuat / meneruskan sinyal yang melemah

📌 Repeater **TIDAK mengolah data**, cuma meneruskan sinyal.

---

#### 📌 Layer OSI Repeater

#### 👉 Layer 1 – Physical Layer

🧠 Ingat:

- Repeater = fisik
  - Bit 0 dan 1
  - Tidak tahu IP / MAC
- 

#### 📌 Fungsi Repeater

- Memperpanjang jarak kabel
  - Mengatasi sinyal lemah
  - Mengurangi noise
- 

#### 📌 Contoh Repeater

- WiFi extender
  - Repeater jaringan kabel
- 

## ■ Contoh Soal

**Soal:**

Perangkat yang bekerja pada Physical Layer untuk memperkuat sinyal adalah?

**Jawaban:**

- Repeater
- 

◆ **B. Routing**

Sekarang yang **lebih konsep**.

📌 **Pengertian Routing**

**Routing** adalah proses:

👉 menentukan jalur terbaik untuk mengirim paket data dari sumber ke tujuan.

Routing dilakukan oleh:

👉 **Router**

---

📌 **Routing Bekerja di Layer?**

👉 **Layer 3 – Network Layer**

Karena routing berhubungan dengan:

- IP Address
  - Network ID
  - Jalur antar jaringan
- 

📌 **Jenis Routing**

**1 Static Routing**

- Jalur ditentukan manual
- Tidak berubah otomatis

📌 Kelebihan: simpel

📌 Kekurangan: tidak fleksibel

---

**2 Dynamic Routing**

- Jalur ditentukan otomatis

- Pakai protokol routing

Contoh protokol:

- RIP
  - OSPF
  - EIGRP
  - BGP
- 

### 📌 Perbandingan Static vs Dynamic Routing

Static	Dynamic
Manual	Otomatis
Simpel	Kompleks
Cocok jaringan kecil	Jaringan besar

## 7 VPN (Virtual Private Network)

### ◆ Pengertian VPN

VPN adalah teknologi jaringan yang digunakan untuk:

👉 membuat koneksi aman (**private**) melalui jaringan publik (internet).

Ibaratnya:

- Internet = jalan umum
  - VPN = **terowongan pribadi** 
- 

### ◆ Fungsi VPN

VPN digunakan untuk:

- Mengamankan data (enkripsi)
  - Mengakses jaringan kantor dari luar
  - Menyembunyikan IP asli
  - Menghubungkan dua jaringan berbeda secara aman
- 

### ◆ Cara Kerja VPN (Sederhana)

1. User terkoneksi ke internet
2. User membuat koneksi VPN ke server VPN
3. Data **dienkripsi**
4. Data dikirim lewat “terowongan” VPN
5. Server VPN mendekripsi data

📌 Walaupun lewat internet, **orang lain tidak bisa membaca datanya.**

---

#### ◆ Istilah Penting di VPN

- **Tunneling** → proses membuat jalur aman
  - **Encryption** → pengamanan data
  - **Authentication** → verifikasi user
- 

#### ◆ Jenis VPN

##### 1 Remote Access VPN

- User → kantor
  - Contoh: WFH, akses server kampus
- 

##### 2 Site-to-Site VPN

- Kantor pusat ↔ cabang
  - Jaringan ↔ jaringan
- 

#### ◆ Protokol VPN (Sering Ditanya)

##### Protokol Keterangan

PPTP      Lama, kurang aman

L2TP      Biasanya dengan IPSec

IPSec      Aman, populer

SSL VPN Berbasis web

📌 Jawaban aman kalau bingung: **IPSec**

---

#### ◆ VPN vs Proxy (Jebakan Soal)

VPN	Proxy
Enkripsi data	Tidak selalu
Layer jaringan	Aplikasi
Lebih aman	Kurang aman

---

## 8 DHCP (Dynamic Host Configuration Protocol)

#### ◆ Pengertian DHCP

DHCP adalah protokol jaringan yang berfungsi untuk:

👉 memberikan IP Address secara otomatis ke client.

Tanpa DHCP:

- Kita harus setting IP **manual** satu-satu 😕

Dengan DHCP:

- IP otomatis ✓
- Lebih cepat ✓
- Lebih minim error ✓

---

#### ◆ Informasi yang Diberikan DHCP

DHCP tidak cuma kasih IP, tapi juga:

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server

---

#### ◆ Proses DHCP (WAJIB HAFAL)

Namanya **DORA** 👉

⌚ **DORA**

## **1 Discover**

Client mencari DHCP Server  
(broadcast)

## **2 Offer**

Server menawarkan IP Address

## **3 Request**

Client meminta IP tersebut

## **4 Acknowledge**

Server menyetujui & mengikat IP

 Tips hafalan:

**DORA = Discover → Offer → Request → Acknowledge**

---

### ◆ **DHCP Server & Client**

- **DHCP Server** → pemberi IP
- **DHCP Client** → penerima IP

Contoh DHCP Server:

- Router
  - Windows Server
  - Linux Server
- 

### ◆ **Lease Time**

 **Lease Time** = lama IP dipinjamkan

- Kalau habis → IP bisa diperpanjang
  - Atau dikembalikan ke pool IP
- 

### ◆ **DHCP vs Static IP**

<b>DHCP</b>	<b>Static</b>
Otomatis	Manual
Fleksibel	Tetap

Cocok user banyak	Cocok server
-------------------	--------------

📌 Server biasanya pakai **Static IP**.

## 9 **AAA (Authentication, Authorization, Accounting)**

### ◆ **Apa itu AAA?**

**AAA** adalah konsep untuk **mengatur akses user ke jaringan**.

AAA memastikan:

- Siapa kamu?
  - Boleh ngapain?
  - Ngapain aja tadi?
- 

### ◆ **A pertama – Authentication**

👉 **Siapa kamu?**

Proses **verifikasi identitas user**.

Contoh:

- Username & password
- PIN
- Biometrik
- OTP

📌 Kalau belum lolos authentication → **tidak bisa masuk jaringan**

---

### ◆ **A kedua – Authorization**

👉 **Kamu boleh ngapain?**

Menentukan **hak akses user** setelah login.

Contoh:

- User biasa: hanya baca data
- Admin: tambah, hapus, konfigurasi

📌 Authorization terjadi **SETELAH authentication**

---

◆ A ketiga – Accounting

👉 Kamu ngapain aja?

Mencatat aktivitas user.

Contoh:

- Jam login & logout
- IP yang dipakai
- Aktivitas jaringan

📌 Biasanya buat:

- Audit
- Billing
- Monitoring

---

◆ Urutan AAA (PENTING)

🧠 Urutannya TIDAK BOLEH KETUKER:

- 1 Authentication
- 2 Authorization
- 3 Accounting

Kalau ada soal urutan → ini jawabannya

---

◆ Contoh Implementasi AAA

- Login WiFi kampus
- VPN kantor
- Akses router / server

Protokol yang sering dipakai:

- RADIUS
- TACACS+

10 NAT (Network Address Translation)

◆ Pengertian NAT

**NAT** adalah teknik jaringan untuk:

👉 **mengubah IP Address** saat paket melewati router.

Biasanya dipakai untuk:

- Menghemat IP publik
  - Menghubungkan jaringan lokal ke internet
- 

#### ◆ **Kenapa NAT Dibutuhkan?**

Karena:

- **IPv4 terbatas**
- Banyak device, IP publik sedikit

📌 Solusinya:

Banyak IP private → **1 IP public** (pakai NAT)

---

#### ◆ **IP Private vs IP Public**

##### **IP Private (TIDAK bisa ke internet langsung)**

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

##### **IP Public**

- Bisa diakses internet
  - Diberikan oleh ISP
- 

#### ◆ **Cara Kerja NAT (Sederhana)**

1. Client (IP private) kirim data
2. Router NAT **mengganti IP sumber**
3. Router simpan tabel NAT
4. Data dikirim ke internet
5. Balasan dikembalikan ke client

📌 Router yang melakukan NAT.

---

- ◆ Jenis-jenis NAT (WAJIB TAHU)

### 1 Static NAT

- 1 IP private ↔ 1 IP public
- Tetap

📌 Cocok untuk server

---

### 2 Dynamic NAT

- Banyak IP private ↔ banyak IP public
- IP public dipilih dari pool

---

### 3 PAT (Port Address Translation) ⭐

- Banyak IP private ↔ **1 IP public**
- Dibedakan lewat **port**

📌 Ini yang paling sering dipakai

💡 Tips:

PAT sering disebut **NAT Overload**

---

- ◆ Contoh Alur PAT (PENTING)

IP Private	Port	IP Public	Port
192.168.1.2	5000	203.0.113.1	30001
192.168.1.3	5001	203.0.113.1	30002

📌 Router tahu balikin ke siapa lewat port.

---

### 1 1 NAP – Access Point – Access Protocol

- ◆ A. NAP (Network Access Point)

📌 Pengertian NAP

**NAP (Network Access Point)** adalah:

👉 titik akses tempat user / jaringan **masuk ke jaringan lain** (biasanya internet atau backbone).

📌 Dulu:

- NAP dipakai untuk menghubungkan ISP satu dengan lainnya.

📌 Sekarang (konsep modern):

- Tempat kontrol **siapa yang boleh masuk jaringan**.
- 

### 📌 **Fungsi NAP**

- Mengatur akses jaringan
  - Titik pertemuan jaringan
  - Penghubung ke jaringan lebih besar
- 

### ◆ **B. Access Point (AP)**

#### 📌 **Pengertian Access Point**

**Access Point** adalah perangkat jaringan yang:

👉 menghubungkan **perangkat wireless** ke jaringan kabel (LAN).

Contoh:

- WiFi kampus
- WiFi rumah
- Hotspot cafe

📌 Access Point bekerja di:

- **Layer 2 (Data Link)**
  - kadang Layer 3 (kalau AP canggih)
- 

### 📌 **Fungsi Access Point**

- Memancarkan sinyal WiFi
- Mengatur koneksi client wireless
- Jembatan LAN ↔ WLAN

---

### 📌 Access Point ≠ Router

Access Point	Router
Fokus WiFi	Routing
Tidak NAT	Ada NAT
Layer 2	Layer 3

---

#### ◆ C. Access Protocol

### 📌 Pengertian Access Protocol

**Access Protocol** adalah protokol yang:

👉 digunakan user untuk **mengakses layanan jaringan**.

---

### 📌 Contoh Access Protocol

Protokol	Fungsi	Port
HTTP	Akses web	80
HTTPS	Web aman	443
FTP	Transfer file	21
Telnet	Remote login	23
SSH	Remote aman	22

📌 Ini sering keluar dalam bentuk **cocokkan fungsi & port**.

---

### 🧠 Hubungan Ketiganya (PENTING)

Contoh kasus di kampus:

1. User connect ke **Access Point**
2. User masuk jaringan lewat **NAP**
3. User akses layanan pakai **Access Protocol** (HTTP, FTP, dll)

### 1 2 LACP (Link Aggregation Control Protocol)

#### ◆ Pengertian LACP

**LACP** adalah protokol yang digunakan untuk:

👉 menggabungkan beberapa link fisik menjadi **satu link logis**.

Tujuannya:

- **Menambah bandwidth**
  - **Redundancy** (backup link)
- 

◆ **Contoh Sederhana**

Misalnya:

- Ada **2 kabel LAN**, masing-masing 1 Gbps
  - ➡ Digabung pakai LACP
  - ➡ Jadi **1 link logis 2 Gbps**

📌 Kalau satu kabel putus, link masih jalan 👍

---

◆ **LACP Bekerja di Layer Berapa?**

👉 **Layer 2 (Data Link Layer)**

📌 Biasanya dipakai di:

- Switch ↔ Switch
  - Switch ↔ Server
- 

◆ **Fungsi Utama LACP**

- Load balancing
  - High availability
  - Menghindari single point of failure
- 

◆ **Syarat Menggunakan LACP**

- Perangkat **harus mendukung LACP**
- Port harus:
  - Speed sama
  - Duplex sama

❖ Kalau beda → LACP gagal.

---

#### ◆ Mode LACP

Biasanya ada:

- **Active** → aktif negosiasi
- **Passive** → menunggu

❖ Minimal satu sisi **Active**.

---

#### ◆ LACP vs Trunk (Jebakan)

LACP	Trunk
Gabung link	Gabung VLAN
Fokus bandwidth	Fokus segmentasi
Layer 2	Layer 2

### 1 3 ACL (Access Control List)

#### ◆ Pengertian ACL

**ACL (Access Control List)** adalah:

👉 daftar aturan untuk **mengizinkan (permit)** atau **menolak (deny)** lalu lintas jaringan.

Biasanya diterapkan di:

- Router
- Switch Layer 3
- Firewall

---

#### ◆ Fungsi ACL

- Membatasi akses jaringan
  - Meningkatkan keamanan
  - Mengontrol trafik masuk & keluar
-

#### ◆ Cara Kerja ACL (PENTING)

ACL bekerja dengan prinsip:

**dibaca dari atas ke bawah**

- Kalau aturan cocok → **langsung dieksekusi**
- Kalau tidak cocok → lanjut ke aturan berikutnya
- Di akhir selalu ada:

**implicit deny** (ditolak semua)

📌 Ini sering jadi jebakan soal.

---

#### ◆ Jenis ACL

##### 1 Standard ACL

- Berdasarkan **IP sumber saja**
- Lebih sederhana
- Ditempatkan **dekat tujuan**

Contoh logika:

“Blokir semua trafik dari IP tertentu”

---

##### 2 Extended ACL ⭐

- Berdasarkan:
  - IP sumber
  - IP tujuan
  - Protokol (TCP/UDP)
  - Port
- Lebih detail
- Ditempatkan **dekat sumber**

📌 Extended ACL lebih sering dipakai.

---

#### ◆ Inbound vs Outbound

Inbound	Outbound
Masuk ke interface	Keluar dari interface
Disaring saat masuk	Disaring saat keluar

📌 Salah pilih arah → ACL tidak bekerja.

---

#### ◆ Contoh Logika ACL (PELAAAN)

Misal:

Izinkan hanya IP 192.168.1.10 mengakses server

Logika:

- Permit IP 192.168.1.10
- Deny lainnya

📌 Urutan sangat penting.

---

#### 🔑 Ringkasan Wajib Ingat

- ACL = aturan izin & tolak
- Dibaca dari atas ke bawah
- Ada **implicit deny**
- Standard vs Extended
- Inbound ≠ Outbound

## 1 4 TCP dan UDP

TCP dan UDP adalah **protokol Layer 4 (Transport Layer)** pada model OSI.

📌 Fungsinya:

👉 Mengirim data **end-to-end** dari aplikasi ke aplikasi.

---

#### ◆ A. TCP (Transmission Control Protocol)

##### 📌 Ciri Utama TCP

- **Connection-oriented**

- **Reliable** (data dijamin sampai)
- Data berurutan
- Ada kontrol error & flow control

📌 TCP cocok untuk data yang **tidak boleh hilang**.

---

### 📌 **Cara Kerja TCP – 3 Way Handshake (WAJIB HAFAL)**

Ini **materi ujian klasik**.

#### 1 SYN

Client minta koneksi

#### 2 SYN-ACK

Server setuju

#### 3 ACK

Client konfirmasi

📌 Setelah ini → koneksi terbentuk.

💡 Tips hafalan:

**SYN → SYN-ACK → ACK**

---

### 📌 **Contoh Penggunaan TCP**

- HTTP / HTTPS
- FTP
- SMTP
- SSH

## ◆ **B. UDP (User Datagram Protocol)**

### 📌 **Ciri Utama UDP**

- **Connectionless**
- **Tidak reliable**
- Tidak ada jaminan sampai
- Lebih **cepat**

- ❖ UDP cocok untuk data **real-time**.
- 

### ❖ **Contoh Penggunaan UDP**

- Video streaming
  - Voice call
  - Online gaming
  - DNS
- 

### ◆ **TCP vs UDP (WAJIB PAHAM)**

Aspek	TCP	UDP
Koneksi	Ada	Tidak
Keandalan	Tinggi	Rendah
Urutan data	Dijaga	Tidak
Kecepatan	Lebih lambat	Lebih cepat
Contoh	FTP, HTTP	Streaming, DNS

---

### ◆ **Port & TCP/UDP (SERING KELUAR)**

#### ❖ Port bekerja di Layer 4

Contoh:

- HTTP → TCP 80
- HTTPS → TCP 443
- FTP → TCP 21
- DNS → UDP 53

#### ❖ Kalau soal:

“Protokol transport yang digunakan DNS?”

Jawaban aman: **UDP**

### **1 5 SNMP (Simple Network Management Protocol)**

#### ◆ **Pengertian SNMP**

**SNMP** adalah protokol jaringan yang digunakan untuk:

👉 **memantau, mengelola, dan memonitor perangkat jaringan.**

Contoh perangkat:

- Router
  - Switch
  - Server
  - Access Point
- 

#### ◆ **Fungsi SNMP**

Dengan SNMP, admin bisa:

- Melihat status perangkat
  - Mengecek trafik
  - Mengetahui error
  - Monitoring jaringan jarak jauh
- 

#### ◆ **Komponen Utama SNMP (WAJIB HAFAL)**

##### 1 **SNMP Manager**

- Pusat pengelolaan
  - Mengirim permintaan
  - Menerima laporan
- 

##### 2 **SNMP Agent**

- Ada di perangkat jaringan
  - Mengumpulkan informasi
  - Menjawab permintaan manager
- 

##### 3 **MIB (Management Information Base)**

- Database informasi perangkat
- Berisi parameter (CPU, RAM, interface)

❖ MIB itu bukan perangkat, tapi database.

---

◆ **Cara Kerja SNMP (Sederhana)**

1. Manager kirim request
  2. Agent ambil data dari MIB
  3. Agent kirim response
  4. Manager tampilkan data
- 

◆ **SNMP Trap (SERING KELUAR)**

**Trap** = notifikasi otomatis

❖ Agent mengirim pesan sendiri ke Manager jika:

- Ada error
- Link down
- Perangkat bermasalah

🧠 Trap ≠ request

---

◆ **Versi SNMP**

Versi	Keterangan
SNMPv1	Lama
SNMPv2	Lebih baik
SNMPv3	<b>Paling aman</b> (auth & enkripsi)

❖ Kalau soal keamanan → **SNMPv3**

---

◆ **Port SNMP (WAJIB HAFAL)**

- SNMP → **UDP 161**
- SNMP Trap → **UDP 162**

## ◆ Pengertian WLAN

**WLAN (Wireless Local Area Network)** adalah:

👉 jaringan lokal yang menggunakan **gelombang radio** (tanpa kabel).

Contoh:

- WiFi rumah
- WiFi kampus
- Hotspot café

📌 WLAN = LAN versi **wireless**

---

## ◆ Komponen WLAN (WAJIB TAHU)

### 1 Access Point (AP)

- Memancarkan sinyal WiFi
- Penghubung LAN ↔ WLAN

### 2 Wireless Client

- Laptop
- HP
- Tablet

### 3 Wireless NIC (Network Interface Card)

- Adapter WiFi pada perangkat
- 

## ◆ Cara Kerja WLAN (Sederhana)

1. Access Point memancarkan SSID
  2. Client menangkap sinyal
  3. Client melakukan authentication
  4. Client terhubung ke jaringan
- 

## ◆ Mode WLAN

### 1 Infrastructure Mode

- Pakai Access Point
- Client ↔ AP ↔ jaringan

📌 **Paling umum digunakan**

---

## 2 Ad-hoc Mode

- Client ↔ client langsung
- Tanpa Access Point

📌 Jarang dipakai

---

### ♦ Standar WLAN (IEEE 802.11) ⭐

Ini sering keluar di ujian.

Standar	Frekuensi	Kecepatan
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 / 5 GHz	Hingga 600 Mbps
802.11ac	5 GHz	>1 Gbps
802.11ax (WiFi 6)	2.4 / 5 GHz	Lebih cepat & stabil

📌 Tips ujian:

- **2.4 GHz → jarak jauh, interferensi**
  - **5 GHz → cepat, jarak lebih pendek**
- 

### ♦ Keamanan WLAN (WAJIB PAHAM)

Metode	Keamanan
WEP	✗ Lemah
WPA	⚠ Lebih baik
WPA2	✓ Aman

WPA3	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Paling aman
------	---	-------------

📌 Kalau soal:

“Keamanan WLAN yang direkomendasikan?”

Jawaban: **WPA2 / WPA3**

---

#### ◆ Masalah Umum WLAN

- Interferensi
- Jarak
- Banyak user
- Channel overlap

### 1 7 Class IP IPv4 & NFP (Full Dasar + Hitungan)

#### ◆ Apa itu Class IP?

Class IP adalah **pengelompokan IPv4** berdasarkan:

- nilai oktet pertama
- jumlah network & host

📌 Ini dipakai untuk:

- menentukan **network ID**
  - menentukan **jumlah host**
  - dasar subnetting
- 

### 3 Struktur IPv4 (ingat lagi)

IPv4 = **32 bit** = 4 oktet.

Setiap oktet = 8 bit

xxx.xxx.xxx.xxx ->  $8 * 4 = 32$

**1 oktet = 8 bit**

Nilai bit:

128 64 32 16 8 4 2 1

$$128+64+32+16+8+4+2+1 = 255$$

---

◆ Class IP IPv4 (WAJIB HAFAL TABEL INI)

Class	Oktet Pertama	Range IP	Default Subnet Mask	Jumlah Host
A	1 – 126	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)	16 juta
B	128 – 191	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	65 ribu
C	192 – 223	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	254
D	224 – 239	Multicast	–	–
E	240 – 255	Experimental	–	–

📌 Ujian hampir selalu fokus ke Class A, B, C

---

🧠 Cara Cepat Menentukan Class IP

👉 Lihat angka pertama

Contoh:

- 10.1.2.3 → **Class A**
  - 172.16.5.1 → **Class B**
  - 192.168.1.10 → **Class C**
- 

◆ Default Subnet Mask (WAJIB HAFAL)

Class	Subnet Mask	Ket
A	255.0.0.0	1 network + 3 host
B	255.255.0.0	2 network + 2 host
C	255.255.255.0	3 network + 1 host

---

◆ Network ID & Host ID (INI PENTING)

**Contoh 1 (PELAAAAAN)**

IP:

192.168.1.10

Langkah 1 : Tentukan class

→ 192 = **Class C**

Langkah 2 : Subnet mask default

→ 255.255.255.0

Langkah 3 :

- Network ID = **192.168.1.0** -> 3 oktet pertama
- Host ID = **10** -> 1 oktet terakhir

❖ Di Class C: [ Network ][ Network ][ Network ][ Host ]

- Network = 3 oktet pertama
- Host = 1 oktet terakhir

---

#### ◆ Jumlah Host (ADA HITUNGAN)

Rumus:

Jumlah host =  $2^n - 2$

(n = jumlah bit host)

Kenapa -2?

- 1 untuk **network ID**
- 1 untuk **broadcast**

---

#### Contoh Class C

Subnet mask: /24

→ Host bit =  $32 - 24 = 8$  bit

$2^8 - 2 = 256 - 2 = 254$  host

❖ Makanya Class C = **254 host**

#### Bentuk biner subnet mask /24

1111111.1111111.1111111.00000000

Ubah ke desimal:

255.255.255.0

💡 Jadi:

$/24 = 255.255.255.0$

---

◆ **NFP (yang kemungkinan dimaksud dosen)**

Biasanya **NFP** = **Network Prefix** (CIDR)

Contoh:

- 192.168.1.0/24
- /24 = jumlah bit network

CIDR	Subnet Mask	Ket
/8	255.0.0.0	8 bit untuk network,, 24 bit untuk host
/16	255.255.0.0	16 bit untuk network, 16 bit untuk host
/24	255.255.255.0	24 bit untuk network, 8 bit untuk host

💡 /24 = Class C default

---

📘 **Contoh Soal Ujian (FULL)**

**Soal 1**

Tentukan class dan subnet mask IP berikut:

172.16.10.5

**Jawab:**

- 172 → Class B
  - Subnet mask → 255.255.0.0
- 

**Soal 2**

Berapa jumlah host maksimal pada Class C?

**Jawab:**

$2^8 - 2 = 254$  host

---

### Soal 3

Network ID dari IP 192.168.10.25?

Jawab:

192.168.10.0 (3 oktet pertama)

---

### 1 Apa itu Subnetting?

Subnetting = membagi **1 jaringan besar** menjadi **beberapa jaringan kecil**.

Kenapa dilakukan?

- Menghemat IP
  - Mengatur jaringan
  - Keamanan & performa
- 

### 2 Contoh Kasus (yang SERING keluar ujian)

Misal:

192.168.1.0/24

Lalu diminta:

👉 dibagi jadi beberapa subnet

---

### 3 Subnetting /24 → /26 (CONTOH UTAMA)

◆ Artinya apa?

- Awalnya: /24
- Dipinjam **2 bit** dari host

/24 → /26

---

### 4 Hitungan WAJIB (INI INTI)

◆ Bit host awal

$32 - 24 = 8$  bit host

◆ Bit host baru

$32 - 26 = 6$  bit host

---

## 5 Jumlah Subnet

Rumus:

Jumlah subnet =  $2^n$

n = bit yang dipinjam

$2^2 = 4$  subnet

---

## 6 Jumlah Host per Subnet

$2^6 - 2 = 64 - 2 = 62$  host

📌 Dikurangi 2:

- Network ID
  - Broadcast
- 

## 7 Tentukan Block Size (INI KUNCI)

Subnet mask /26 =

255.255.255.192

Kenapa 192?

Bit terakhir:

$11000000 = 128 + 64 = 192$

Subnet mask = **26 bit 1**, lalu **6 bit 0**

Kita susun per oktet (8 bit):

**Oktet 1–3 (24 bit):**

11111111 . 11111111 . 11111111

→ ini pasti **255.255.255**

**Oktet ke-4 (sisa 2 bit network)**

Karena total network = 26 bit

Sudah kepakai 24 bit → sisa **2 bit di oktet ke-4**

Bentuknya: 11000000

### 🔑 Block size:

$$256 - 192 = 64$$

---

### 8 Tabel Subnet (PALING PENTING)

Subnet	Network ID	Host Range	Broadcast
1	192.168.1.0	.1 – .62	.63
2	192.168.1.64	.65 – .126	.127
3	192.168.1.128	.129 – .190	.191
4	192.168.1.192	.193 – .254	.255

📌 Polanya naik **64**

---

### Cara CEPAT (tanpa mikir lama)

1. Cari subnet mask
  2. Hitung block size
  3. Naikkan IP sesuai block
- 

### 9 Contoh Soal Ujian

#### Soal:

IP 192.168.1.70/26 berada di subnet mana?

#### Jawab:

- Block size = 64
- 70 masuk range **64–127**

#### → Network ID:

192.168.1.64

CARA :

Block size = 256 – nilai subnet mask oktet terakhir

Subnet mask:255.255.255.192

Jadi:

$$256 - 192 = 64$$

➡ **Subnet naik per 64**

Karena block size = 64, maka network ID-nya:

0

64

128

192

Jadi subnet-subnetnya:

Subnet	Network ID
1	192.168.1.0
2	192.168.1.64
3	192.168.1.128
4	192.168.1.192

---

3 Sekarang masukkan IP 70

IP:

192.168.1.70

Fokus ke oktet terakhir:

70

Bandingkan dengan daftar:

- 0 – 63 ✗
- 64 – 127 ✓
- 128 – 191 ✗

➡ **70 masuk ke range 64–127**

---

4 Maka Network ID-nya adalah:

192.168.1.64

## 1 8 ACL (Access Control List)

### ◆ Apa itu ACL?

ACL (Access Control List) adalah:

👉 aturan (rule) untuk mengizinkan atau menolak trafik jaringan

Dipakai di:

- Router
- Switch Layer 3
- Firewall

📌 Intinya: filter paket data

---

### ◆ Fungsi ACL (WAJIB HAFAL)

- Mengontrol akses jaringan
  - Meningkatkan keamanan
  - Membatasi trafik tertentu
  - Mengatur siapa boleh akses apa
- 

### ◆ Cara Kerja ACL (INI PENTING BANGET)

ACL bekerja dengan prinsip:

**Dibaca dari atas ke bawah, berhenti di rule pertama yang cocok**

Kalau **tidak cocok semua** →

🚫 **implicit deny** (DITOLAK otomatis)

⚠ **Implicit deny** = soal favorit ujian

---

### ◆ Jenis ACL (SERING KELUAR)

#### 1 Standard ACL

- Filter berdasarkan **IP sumber**
- **Sederhana**

Contoh konsep:

permit 192.168.1.0

deny 192.168.2.0

📌 Tidak peduli port & tujuan

---

## 2 Extended ACL ⭐

- Filter berdasarkan:
  - IP sumber
  - IP tujuan
  - Protocol (TCP/UDP/ICMP)
  - Port

## 📌 PALING SERING KELUAR

---

### ◆ Wildcard Mask (INI BIKIN BINGUNG, TENANG)

Wildcard mask = kebalikan subnet mask

**Contoh:**

Subnet mask:

255.255.255.0

Wildcard:

0.0.0.255

📌 Aturan:

- 0 → harus sama
  - 255 → bebas
- 

### ◆ Contoh ACL Standard (PELAAAAAN)

**Soal:**

Blokir jaringan 192.168.1.0/24

Subnet mask:

255.255.255.0

Wildcard:

0.0.0.255

ACL:

```
access-list 1 deny 192.168.1.0 0.0.0.255
```

```
access-list 1 permit any
```

---

◆ **Contoh ACL Extended (WAJIB LIHAT)**

**Soal:**

Blokir HTTP dari 192.168.1.0/24 ke server 10.1.1.1

ACL:

```
access-list 100 deny tcp 192.168.1.0 0.0.0.255 host 10.1.1.1 eq 80
```

```
access-list 100 permit ip any any
```

---

◆ **Penempatan ACL (SERING DITANYA)**

- **Standard ACL** → dekat **tujuan**
- **Extended ACL** → dekat **sumber**

📌 Ini sering jadi soal teori jebakan

---

**1 9 NETCONF**

◆ **Apa itu NETCONF?**

**NETCONF (Network Configuration Protocol)** adalah:

👉 **protokol untuk mengelola dan mengonfigurasi perangkat jaringan secara terprogram (programmatic)**

Dipakai untuk:

- Router
- Switch
- Network device modern

📌 NETCONF = **cara modern** mengatur jaringan

📌 Lawannya konfigurasi manual via CLI

---

#### ◆ Tujuan NETCONF

- Otomatisasi jaringan
  - Konfigurasi lebih aman
  - Mengurangi human error
  - Konsisten antar device
- 

#### ◆ Cara Kerja NETCONF

NETCONF bekerja dengan model:

Client ↔ Server

- Client: admin / aplikasi / controller
- Server: perangkat jaringan

Transport protocol:

👉 SSH (port 830) ⭐ sering ditanya

---

#### ◆ Perbedaan NETCONF vs CLI (SERING KELUAR)

**NETCONF    CLI**

Terstruktur    Manual

Berbasis XML    Text command

Bisa rollback    Sulit rollback

Aman (SSH)    Tergantung user

---

#### ◆ Konsep Data Store (INI PENTING)

NETCONF punya **datastore**:

**1 running**

- Konfigurasi aktif

**2 candidate**

- Konfigurasi sementara (bisa diuji)

**3 startup**

- Konfigurasi saat boot

📌 Banyak soal tanya:

“Konfigurasi yang sedang berjalan?”

Jawab: **running**

---

#### ◆ Operasi NETCONF (WAJIB TAHU)

- <get>
- <get-config>
- <edit-config>
- <commit>
- <lock> / <unlock>

📌 <commit> = menerapkan konfigurasi

---

#### ◆ NETCONF + YANG

NETCONF sering dipasangkan dengan:

👉 YANG (data modeling language)

YANG:

- Mendefinisikan struktur data
- Schema konfigurasi

📌 Ini nyambung ke nomor 5 (Data Modeling Language)

## 2 0 Bangun Jaringan (Network Design & Implementation)

#### ◆ Apa itu “Bangun Jaringan”?

Bangun jaringan adalah proses:

👉 merancang, mengimplementasikan, dan mengelola jaringan komputer agar:

- stabil
- aman
- sesuai kebutuhan

---

## ◆ Tahapan Bangun Jaringan (WAJIB HAFAL URUTANNYA)

Biasanya dosen suka tanya urutan 

### 1 Analisis Kebutuhan

- Jumlah user
- Jenis layanan (internet, server, WiFi)
- Skala jaringan (kecil / besar)

 Contoh:

- 50 PC
- 3 access point
- 1 server

---

### 2 Desain Jaringan

Menentukan:

- Topologi
- IP addressing
- Perangkat

 Ini sering muncul sebagai soal kasus

---

### 3 Pemilihan Perangkat

- Router
- Switch
- Access Point
- Kabel (UTP, fiber)

---

### 4 Implementasi

- Pemasangan fisik
- Konfigurasi IP

- Setting DHCP, NAT, VLAN
- 

## 5 Pengujian (Testing)

- Ping
- Traceroute
- Uji akses internet

📌 Soal sering: "Langkah untuk memastikan jaringan berjalan?"

---

## 6 Dokumentasi & Maintenance

- Diagram jaringan
  - Backup konfigurasi
  - Monitoring
- 

### ◆ Topologi Jaringan (SERING KELUAR)

#### Topologi Ciri

Star      Pusat di switch

Bus      Kabel utama

Ring      Melingkar

Mesh      Redundant ("anti mati")

📌 Star paling umum

---

### ◆ IP Addressing Plan

Ini nyambung ke nomor 17:

- Tentukan subnet
- Tentukan range IP
- Tentukan gateway

📌 Contoh:

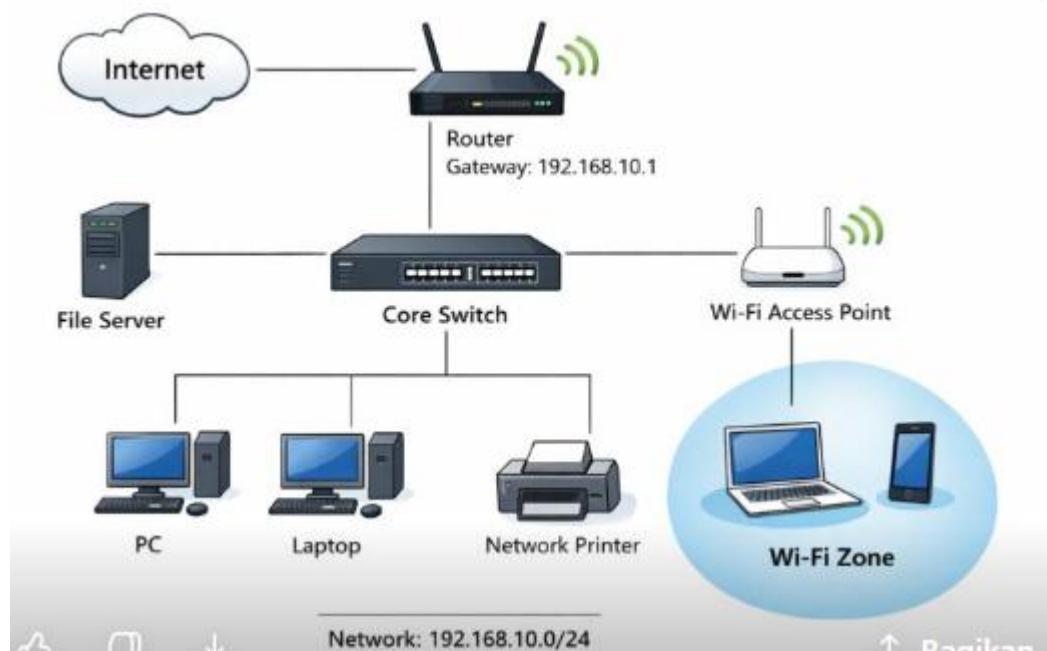
192.168.10.0/24

Gateway: 192.168.10.1

---

◆ Keamanan Jaringan

- ACL
- Firewall
- WPA2/WPA3
- Segmentasi jaringan



**2 1 FIT (Thin Client) & FAT (Fat Client)**

◆ Apa itu FAT (Fat Client)?

**Fat Client** adalah:

👉 komputer/client yang melakukan sebagian besar proses sendiri

Artinya:

- Aplikasi jalan di client
- Proses berat di client
- Server cuma bantu data

📌 Contoh:

- PC/laptop biasa
  - Aplikasi desktop (MS Office, Photoshop)
  - Game offline
- 

#### ◆ Ciri-ciri FAT Client

- Spesifikasi client **tinggi**
  - Butuh storage lokal
  - Update aplikasi di tiap client
  - Lebih mandiri
- 

#### ◆ Apa itu FIT (Thin Client)?

**FIT / Thin Client** adalah:

👉 client yang **hampir semua prosesnya dilakukan di server**

Client cuma:

- input (keyboard, mouse)
- output (layar)

📌 Contoh:

- Komputer lab berbasis server
  - VDI (Virtual Desktop Infrastructure)
  - Terminal di bank / kampus
- 

#### ◆ Ciri-ciri FIT (Thin Client)

- Spesifikasi client **rendah**
  - Tidak butuh storage besar
  - Aplikasi di server
  - Sangat tergantung jaringan
- 

⌚ **Perbandingan FAT vs FIT (WAJIB HAFAL TABEL)**

Aspek	FAT Client	FIT / Thin Client
Proses	Di client	Di server
Spesifikasi client	Tinggi	Rendah
Ketergantungan server	Rendah	Tinggi
Maintenance	Sulit	Mudah
Kinerja jaringan	Normal	Sangat penting

---

#### ◆ Kelebihan & Kekurangan

##### FAT Client

- Tidak tergantung server
  - Maintenance berat
  - Biaya hardware tinggi
- 

##### FIT (Thin Client)

- Hemat biaya client
- Mudah dikelola
- Sangat tergantung jaringan
- Server harus kuat

Network : 192.168.10.0

Subnetmask : 255.255.255.192/26

$$2^6 - 2 = 62$$

Host range : 192.168.10.1 – 192.168.10.62

Broadcast : 192.168.10.63