
WEEK 1 – NETWORKING FOUNDATIONS

DAY 2 – PHYSICAL & DATA LINK LAYER (FULL EXPLANATION)

---

1. Where Day 2 Fits in Networking

In **Day 1**, you learned:

- OSI model
- How data flows layer by layer

Now, **Day 2 zooms into the lowest layers**, where:

- Devices physically connect
- Frames are created
- MAC addresses are used
- Attacks like **MAC flooding** happen

This is **very important for networking + cybersecurity interviews**.

---

2. Physical Layer (Layer 1) – Very Detailed

What Is the Physical Layer?

The Physical layer is responsible for:

- **Sending raw bits (0s and 1s)**
- Over a **physical medium**

It does NOT care about:

- IP address
- MAC address
- Who is sending data

It only cares about:

- Signals
- Speed
- Media

What Comes Under Physical Layer?

- Ethernet cables (Cat5, Cat6)

- Fiber optics
- Wireless signals
- Voltage levels
- Data rates (10 Mbps, 100 Mbps, 1 Gbps)

Example:
When you plug in a LAN cable:

- Physical layer becomes active

Interview sentence:

“Physical layer transmits raw bits over physical media such as cables or wireless signals.”

---

3. Data Link Layer (Layer 2) – Core Focus

The Data Link layer ensures **local delivery**.

Think of it as:

“How devices talk inside the same network.”

It has **two sublayers**:

1. **LLC (Logical Link Control)** – Flow & error control
2. **MAC (Media Access Control)** – Addressing & access

---

4. Ethernet – Explained Very Clearly

What Is Ethernet?

Ethernet is:

- A **Layer 2 technology**
- Used in **LAN networks**
- Defines:
    - How devices access the network
    - Frame format
    - MAC addressing

Example:

- Office LAN
- Home Wi-Fi (Ethernet standards underneath)

Interview line:

“Ethernet is a data link layer technology used for communication within LANs.”

---

5. MAC Addressing – Deep Explanation

What Is a MAC Address?

MAC = **Media Access Control address**

It is:

- A **unique hardware address**
- Assigned to network interfaces
- Usually **48 bits**

Format:

- 6 bytes (e.g., 00:1A:2B:3C:4D:5E)

Why MAC Address Is Needed?

- IP changes (dynamic)
- MAC address is **permanent**
- Used for **local delivery**

Example:

- Inside an office network, switches use MAC addresses to forward frames

Interview sentence:

“MAC address uniquely identifies a network interface at the Data Link layer.”

---

6. ARP (Address Resolution Protocol) – Very Important

Why ARP Exists?

Computers know:

- Destination **IP address**
  But to send data:
- They need **MAC address**

ARP solves:

“Which MAC address belongs to this IP?”

How ARP Works (Step-by-Step)

Example:
PC A wants to send data to PC B.

1. PC A checks ARP table
2. If MAC not found:
    - Sends **ARP broadcast**
3. All devices receive it
4. PC B replies with its MAC
5. PC A stores mapping

This is called **ARP resolution**.

Interview sentence:

“ARP maps IP addresses to MAC addresses within a local network.”

---

7. RARP (Reverse ARP) – Explained

RARP does the **opposite** of ARP.

- Given MAC address
- Finds IP address

Used when:

- Device does not know its IP
- Common in older systems

Now replaced by:

- DHCP

Interview line:

“RARP maps MAC addresses to IP addresses but is mostly obsolete.”

---

8. Collision Domain vs Broadcast Domain (High-Probability Interview Topic)

Collision Domain

A collision happens when:

- Two devices send data at the same time

Collision domain:

- Area where collisions can occur

Devices:

- Hub → one collision domain
- Switch → each port is a separate collision domain

Broadcast Domain

Broadcast domain:

- Area where broadcast packets are forwarded

Devices:

- Switch → one broadcast domain
- Router → separates broadcast domains

Simple Comparison

Concept	Collision Domain	Broadcast Domain
What	Data collision area	Broadcast reach
Reduced by	Switch	Router
Example	Hub	LAN network

Interview sentence:

"A switch separates collision domains, while a router separates broadcast domains."

---

9. Hub vs Switch – Explained Simply

Hub (Layer 1)

- Works at Physical layer
- Sends data to **all ports**
- No MAC learning
- Slow and insecure

Example:

- Old networks

Switch (Layer 2)

- Works at Data Link layer
- Uses MAC address table

- Sends data only to intended device
- Fast and secure

Example:

- Modern LANs

Interview Comparison Table

Feature	Hub	Switch
OSI Layer	Layer 1	Layer 2
Data Forwarding	Broadcast	MAC-based
Security	Poor	Better
Collision Domain	Single	Multiple

---

10. Security Topic – MAC Flooding Attack (Very Important)

What Is MAC Flooding?

MAC flooding is a **Layer 2 attack**.

Attack idea:

- Flood switch with fake MAC addresses
- Overload MAC table
- Switch behaves like a hub

Result:

- Attacker can sniff traffic

Why It Is Dangerous?

- Confidential data exposed
- Man-in-the-middle possible

How to Prevent MAC Flooding?

- Port security
- MAC address limits
- Static MAC entries

Interview sentence:

“MAC flooding attack overflows the switch MAC table, forcing it to broadcast traffic like a hub.”