
WEEK 2 – SWITCHING, ROUTING & CORE DEVICES

DAY 8 – SWITCHING CONCEPTS (DETAILED EXPLANATION)

---

1. What a Switch Really Does (Big Picture)

A **switch** is a **Layer-2 (Data Link Layer) device** whose main job is:

Forward Ethernet frames intelligently using MAC addresses

Unlike hubs, switches:

- Learn which device is connected to which port
- Send traffic **only where it is needed**
- Reduce collisions
- Improve performance and security

Interview one-liner:
"A switch is a Layer-2 device that forwards frames based on MAC addresses using a CAM table."

---

2. Switch Architecture (Internal Working)

2.1 Main Components of a Switch

1. **Ports**
    - Physical interfaces where devices connect
    - Each port belongs to a collision domain
2. **Switch Fabric / Backplane**
    - High-speed internal pathway
    - Allows simultaneous communication between multiple ports
3. **ASICs (Application-Specific Integrated Circuits)**
    - Specialized hardware for fast packet processing
    - Enables wire-speed switching (very low latency)
4. **Memory**
    - Stores CAM table
    - Buffers frames during congestion

2.2 How a Switch Processes a Frame (Step-by-Step)

1. Frame arrives on a port
2. Switch reads **source MAC** → learns it
3. Switch checks **destination MAC** in CAM table
4. If found → forwards frame to correct port
5. If not found → floods frame to all ports (except incoming port)

Important:
Flooding happens **only when destination MAC is unknown**.

---

3. CAM Table (Content Addressable Memory)

3.1 What is CAM Table?

CAM table is a table inside a switch that maps:

MAC Address → Switch Port

Example:

MAC Address	Port
AA:BB:CC	Fa0/1
DD:EE:FF	Fa0/3

3.2 How CAM Table Learns

- Switch learns MAC addresses **dynamically**
- Based on **source MAC address** of incoming frames

Key points:

- Entries age out (default ~300 seconds)
- Table size is limited
- CAM table is critical for efficient switching

Interview line:
"A switch learns MAC addresses dynamically by reading the source MAC of incoming frames and storing them in the CAM table."

---

4. VLAN Basics (Virtual LAN)

4.1 What is a VLAN?

A **VLAN** is a **logical separation of devices** on the same physical switch.

VLANs divide one physical network into multiple **logical broadcast domains**.

4.2 Why VLANs Are Used

1. **Reduce broadcast traffic**
2. **Improve security**
3. **Logical grouping of users**
4. **Better network management**

Example:

- VLAN 10 → HR Department
- VLAN 20 → Finance Department
- VLAN 30 → IT Department

Devices in different VLANs **cannot communicate directly** without routing.

4.3 Access Port vs Trunk Port

Access Port

- Carries traffic for **one VLAN only**
- Used for end devices (PC, printer)

Trunk Port

- Carries traffic for **multiple VLANs**
- Used between switches
- Uses **802.1Q tagging**

802.1Q Tag:

- Adds VLAN ID to Ethernet frame
- Allows switch to identify VLAN membership

---

5. Security Focus – VLAN Hopping Attack (VERY IMPORTANT)

5.1 What is VLAN Hopping?

A **VLAN hopping attack** allows an attacker to:

Send traffic from one VLAN into another VLAN without authorization

This breaks **network segmentation**, which is a core security principle.

5.2 Why VLAN Hopping Is Dangerous

- Attacker bypasses VLAN isolation
- Can sniff sensitive traffic
- Can access restricted departments
- Violates trust boundaries

---

6. Types of VLAN Hopping Attacks

6.1 Switch Spoofing Attack

How It Works

1. Attacker connects a device to a switch port
2. Attacker pretends to be a **switch**
3. Initiates **Dynamic Trunking Protocol (DTP)**
4. Switch forms a **trunk link**
5. Attacker gains access to **all VLANs**

Key weakness:
Switch port is left in **dynamic mode**

Real-World Analogy

Attacker pretends to be a building manager and gets master key access to all rooms.

Prevention

- Disable DTP
- Set ports manually

switchport mode access

switchport nonegotiate

6.2 Double Tagging Attack

How It Works (Step-by-Step)

1. Attacker is in VLAN 10
2. Attacker sends frame with **two VLAN tags**
    - Outer tag → native VLAN

    - Inner tag → target VLAN
3. First switch removes outer tag
4. Second switch forwards frame into target VLAN

Important:
This works only when:

- Native VLAN is same on trunk
- Attacker is on native VLAN

Why It's Hard to Detect

- No DTP involved
- Appears as legitimate traffic
- Happens at Layer 2

Prevention

- Do not use VLAN 1 as native VLAN
- Use unused VLAN as native VLAN
- Tag native VLAN

vlan dot1q tag native

---

7. VLAN Hopping – Interview Explanation (Perfect Answer)

"VLAN hopping is a Layer-2 attack where an attacker gains access to traffic in another VLAN. It mainly occurs via switch spoofing using DTP or double-tagging attacks. This can be prevented by disabling DTP, using access mode on ports, avoiding VLAN 1 as native VLAN, and tagging the native VLAN."

---

8. Summary Table

Concept	**Key Point**
Switch	Layer-2 device
CAM Table	MAC → Port mapping
VLAN	Logical broadcast domain
Trunk	Carries multiple VLANs
VLAN Hopping	Breaks VLAN isolation

Concept	Key Point
Prevention	Disable DTP, secure native VLAN

---

9. Day 8 Revision Checklist

You should be able to:

1. Explain switch internal architecture
2. Explain CAM table learning process
3. Explain VLAN purpose and benefits
4. Explain access vs trunk ports
5. Explain VLAN hopping attacks clearly
6. List VLAN hopping prevention techniques