
WEEK 2 – SWITCHING, ROUTING & CORE DEVICES

DAY 9 – VLANS & TRUNKING (DETAILED EXPLANATION)

---

1. VLAN Configuration Logic – What You Need to Know

What is VLAN?

- **VLAN (Virtual LAN)** is a **logical segmentation** of a physical switch into multiple broadcast domains.
- Devices on different VLANs **cannot communicate directly** without routing.

Why VLANs?

- Reduce broadcast traffic
- Improve security
- Group users logically (by department, function, or project)
- Simplify network management

Interview line:

"VLANs are logical broadcast domains that segment a network to improve performance and security."

VLAN Configuration Steps (Conceptual)

1. **Create VLAN** on switch
2. vlan 10
3. name HR
4. **Assign switch ports to VLAN**
5. interface fa0/1
6. switchport mode access
7. switchport access vlan 10
8. **Verify VLAN assignment**
9. show vlan brief
10. **Optional:** Assign VLAN name (for clarity)

Interview tip: Explain **why access ports are assigned to VLANs**: each device is placed in the correct logical group.

---

2. Access vs Trunk Ports

Feature	Access Port	Trunk Port
Purpose	Connects **end devices** (PCs, printers)	Connects **switches or routers**
VLANs	Single VLAN only	Multiple VLANs simultaneously
Tagging	No tagging	VLAN ID added (802.1Q)
Mode Command	switchport mode access	switchport mode trunk
Example	PC in HR VLAN 10	Link between Switch1 & Switch2 carrying VLAN 10, 20, 30

Key Idea:

- **Access ports = user ports**
- **Trunk ports = link multiple VLANs between switches**

---

3. 802.1Q VLAN Tagging

Why Tagging is Needed

- When multiple VLANs share a **single physical link**, the switch needs to know which frame belongs to which VLAN.
- **802.1Q** adds a **4-byte VLAN tag** in the Ethernet frame.

How 802.1Q Works

1. Frame arrives at **trunk port**
2. Switch inserts **VLAN ID tag**
3. Frame travels across trunk
4. Receiving switch reads tag → forwards frame to the correct VLAN

Native VLAN Exception:

- Frames from **native VLAN** are **untagged**
- Default is usually **VLAN 1**

Interview line:

"802.1Q tagging allows multiple VLANs to share a trunk link by adding a VLAN ID to Ethernet frames."

---

4. Inter-VLAN Routing

Problem

- Devices in **different VLANs cannot communicate directly**
- For example: HR VLAN 10 → IT VLAN 20

Solution

- **Router or Layer-3 switch** routes traffic between VLANs
- Called **Inter-VLAN routing**

Methods

1. **Router-on-a-stick**
    - Single physical router interface
    - Subinterfaces created for each VLAN
    - Each subinterface has an IP in that VLAN
    - Trunk link connects router to switch

Example:

interface g0/0.10

encapsulation dot1Q 10

ip address 192.168.10.1 255.255.255.0

interface g0/0.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

2. **Layer-3 Switch**
    - Switch itself routes between VLANs
    - Avoids need for external router
    - Use **SVI (Switch Virtual Interface)** for each VLAN

Example:

interface vlan 10

ip address 192.168.10.1 255.255.255.0

interface vlan 20

ip address 192.168.20.1 255.255.255.0

Interview line:

“Inter-VLAN routing allows communication between VLANs using either a router-on-a-stick or Layer-3 switch with SVIs.”

---

5. Common Best Practices for VLANs

1. **Avoid VLAN 1 for production**
    - Default VLAN, commonly targeted in attacks
2. **Use meaningful VLAN names**
    - Example: HR, Finance, IT
3. **Limit trunk ports**
    - Only between switches
4. **Tag native VLAN**
    - Prevent double-tagging attacks
5. **Document VLAN assignments**
    - Helps in troubleshooting

---

6. Security Considerations

- **VLAN Hopping Attack** (Day 8)
    - Switch spoofing or double tagging
- **Mitigation:**
    - Disable DTP on access ports
    - Avoid native VLAN 1
    - Use explicit VLAN tagging
    - Assign unused VLAN as native for trunks

---

7. Quick Reference Table – Day 9

Concept	Key Points
Access Port	Single VLAN, connects end devices
Trunk Port	Multiple VLANs, connects switches

Concept	Key Points
802.1Q Tagging	Adds VLAN ID for frames across trunk
Inter-VLAN Routing	Router-on-a-stick or Layer-3 switch
Security	Avoid VLAN 1, disable DTP, tag native VLAN

---

8. Day 9 Revision Checklist

You should be able to:

1. Explain **VLAN logic and configuration**
2. Differentiate **access vs trunk ports** clearly
3. Explain **802.1Q tagging** with native VLAN exception
4. Explain **Inter-VLAN routing** and configuration options
5. Relate **VLANs to security attacks and mitigations**
6. Draw **switch + VLAN + trunk + router setup**