
WEEK 2 – SWITCHING, ROUTING & CORE DEVICES

DAY 11 – ROUTING FUNDAMENTALS

---

1. Router vs Switch – Core Differences

Feature	Switch	Router
Layer	Layer 2 (Data Link)	Layer 3 (Network)
Function	Forward frames based on MAC addresses	Forward packets based on IP addresses
Broadcast Domains	VLANs (can divide network)	Each interface = separate broadcast domain
Routing	No	Yes (static/dynamic)
Example	Connect multiple PCs in same office	Connect LAN to Internet or other LANs

Interview line:

"Switches operate at Layer 2 using MAC addresses, while routers operate at Layer 3 using IP addresses to forward traffic between networks."

---

2. Static Routing

What is Static Routing?

- Administrator manually configures routing table
- Example:

ip route 192.168.2.0 255.255.255.0 10.0.0.2

- Meaning: To reach **192.168.2.0/24**, forward packets to **next-hop 10.0.0.2**

Pros:

- Simple, predictable
- No CPU overhead
- Useful for small networks

Cons:

- Not scalable
- Manual updates if network changes

Interview line:

“Static routing is manually configured by the admin and is suitable for small or stable networks.”

---

3. Default Routes

What is a Default Route?

- Router sends packets **to a catch-all path** when no specific route exists
- Often used to send traffic to the Internet

Example:

ip route 0.0.0.0 0.0.0.0 192.168.1.1

- 0.0.0.0/0 → matches **any destination** not in routing table

Interview line:

“A default route is a route used when no specific match is found in the routing table, commonly pointing to the ISP gateway for Internet traffic.”

---

4. Routing Table Basics

- Each router has a **routing table**
- Contains:
    1. Destination network
    2. Subnet mask
    3. Next-hop IP
    4. Outgoing interface
    5. Metric / administrative distance

Static vs Dynamic:

- Static → manually added
- Dynamic → updated automatically using protocols (e.g., RIP, OSPF)

---

5. Security Focus – Route Poisoning

What is Route Poisoning?

- Attackers **inject false routing updates** to manipulate network traffic
- Common in dynamic routing protocols (RIP, OSPF, EIGRP)

Attack Types:

1. **Blackhole Attack**

- Advertise a network exists via attacker → all traffic sent there → dropped

2. **Man-in-the-Middle Attack**
    - Advertise fake routes → traffic flows through attacker → sniff or modify data

---

How Route Poisoning Works (Example)

- Attacker sends **routing update claiming network 10.0.0.0/24** is reachable via attacker's IP
- Legitimate routers update their tables → traffic flows through attacker

---

Mitigation

- Use **authentication in routing protocols**
    - Example: RIP password, OSPF MD5
- Implement **prefix filtering** to block unexpected updates
- Monitor routing table changes regularly
- Use **route validation / route maps**

Interview line:

"Route poisoning is a type of attack where false routing information is advertised to manipulate traffic. It can be mitigated with routing protocol authentication, filtering, and monitoring."

---

6. Example – Static & Default Routing

Topology:

- LAN A → Router → LAN B → Internet

Static Route Example:

RouterA(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

Default Route Example:

RouterA(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

- **Packets to LAN B** → use static route
- **Packets to Internet** → use default route

---

7. Day 11 Revision Checklist

You should be able to:

1. Differentiate **router vs switch** clearly

2. Explain **static routing** with examples
3. Explain **default routes and when they are used**
4. Understand **routing tables** (destination, next-hop, metric)
5. Explain **route poisoning attacks** and mitigation strategies
6. Draw **small routing topology** showing static/default routes