---

**WEEK 2 – SWITCHING, ROUTING & CORE DEVICES**

**DAY 10 – SPANNING TREE PROTOCOL (STP)**

---

**1. Why STP is Required**

**The Problem: Loops in Layer-2 Networks**

- Switches forward broadcast frames to all ports except incoming
- **If a loop exists**, frames can circulate endlessly → **broadcast storm**
- Consequences:
    - Network congestion
    - CPU exhaustion on switches
    - Packet loss

**Solution:** Spanning Tree Protocol (STP)

STP creates a **loop-free logical topology** while still keeping redundant paths for fault tolerance.

**Interview line:**

"STP prevents Layer-2 loops by selectively blocking certain redundant paths while maintaining network redundancy."

---

**2. Root Bridge Election**

**Step 1: Election Process**

1. Each switch has a **Bridge ID (BID)**:
2. BID = Bridge Priority + MAC Address
3. Switches exchange **BPDU (Bridge Protocol Data Units)**
4. **Lowest BID becomes Root Bridge**
    - All decisions in STP are based on root bridge

**Step 2: Port Roles Relative to Root Bridge**

| Port Role | Description |
|---|---|
| Root Port (RP) | Closest port to root bridge |
| Designated Port (DP) | Forwarding port for a segment |
| Blocked Port | Prevents loops, does not forward |

---

**Step 2: Election Rules (Simple)**

- Compare **Bridge Priority** first (default 32768)
- If tie → lowest MAC Address wins

**Interview tip:**

Always mention **BPDU exchange**, **Bridge ID**, and **lowest BID = root bridge**.

---

**3. Port States**

STP uses **port states** to prevent loops during convergence:

| Port State | Function | Time (default) |
|---|---|---|
| Blocking | Does not forward frames | 20 sec (max age) |
| Listening | Listens to BPDUs, no learning | 15 sec (forward delay) |
| Learning | Learns MAC addresses, still not forwarding | 15 sec |
| Forwarding | Normal operation, forwards frames | N/A |
| Disabled | Administratively shut down | N/A |

**Visual:**

- Blocking → Listening → Learning → Forwarding
- Blocks loops during network changes

---

**4. Security Focus – BPDU Attack**

**What is a BPDU Attack?**

- **BPDU (Bridge Protocol Data Unit)** is the STP message that switches exchange
- Attacker **sends fake BPDU packets** to manipulate STP

**Attack Consequences:**

1. Attacker can **become the root bridge**
2. Redirect traffic through attacker's switch → potential MITM
3. Cause network instability (loops or outages)

---

**Types of BPDU Attack**

1. **Root Bridge Takeover**
    - Attacker advertises **lower BID**

- Network selects attacker as root
- Traffic may pass through attacker

2. **BPDU Flood**
    - Attacker floods fake BPDUs
    - Overloads switches, prevents convergence

---

**Mitigation**

- **BPDU Guard** → shuts down port if BPDU received on access port
- **Root Guard** → prevents a port from becoming root
- Use **PortFast** for access ports
- Network monitoring and alerts

**Interview line:**

"A BPDU attack manipulates STP by sending fake BPDUs to become the root bridge or disrupt the network. Mitigation includes BPDU Guard, Root Guard, and PortFast on access ports."

---

**5. Summary Table – Day 10**

| Concept | Key Points |
|---|---|
| STP Purpose | Prevent Layer-2 loops while keeping redundancy |
| Root Bridge | Switch with lowest BID (priority + MAC) |
| Port Roles | Root Port, Designated Port, Blocked Port |
| Port States | Blocking, Listening, Learning, Forwarding, Disabled |
| Security | BPDU attacks (takeover/flood), mitigated by BPDU Guard, Root Guard, PortFast |

---

**6. Day 10 Revision Checklist**

You should be able to:

1. Explain **why loops are dangerous** and why STP exists
2. Explain **root bridge election** process and BID composition
3. Explain **port roles and port states**
4. Explain **BPDU attacks** with examples
5. List **mitigation strategies**

6. Draw a **small network with STP, ports, root bridge, and blocked ports**