Tóm tắt Kiến thức VLAN, Trunking, QoS, VXLAN, VRF CHO CỘNG ĐỒNG VNPRO

1. Tổng quan về VLAN (Virtual LAN)

- VLAN là một mạng logic tách biệt trong cùng một hạ tầng vật lý, giúp phân chia broadcast domain.
- Mỗi VLAN có một VLAN ID (VID), từ 1 đến 4094.
- Thiết bị trong cùng VLAN có thể giao tiếp trực tiếp, khác VLAN phải đi qua router hoặc Layer 3 switch.

2. Chuẩn trunk 802.1Q và Giao thức VLAN Trunking

- 802.1Q là chuẩn trunking cho phép truyền lưu lượng nhiều VLAN trên một kết nối vật lý giữa các switch.
- Header 802.1Q chèn thêm 4 byte vào giữa địa chỉ MAC nguồn và Type trong frame Ethernet.
- Tag gồm: TPID (0x8100), Priority (3 bits cho QoS), CFI (1 bit), VLAN ID (12 bits).
- Lệnh Cisco: `switchport trunk encapsulation dot1q`, `switchport mode trunk`, `switchport trunk allowed vlan`.

3. Giới hạn và kiểm soát lưu lượng VLAN trên trunk

- Dùng `switchport trunk allowed vlan` để cho phép hoặc chặn VLAN cụ thể trên trunk.
- VTP (VLAN Trunking Protocol) giúp đồng bộ VLAN giữa các switch trong domain.
- `show interface trunk` giúp kiểm tra các VLAN đang chạy trên trunk.

4. QoS trong môi trường VLAN và Voice VLAN

- QoS (Quality of Service) phân loại và ưu tiên lưu lượng.
- Voice VLAN là VLAN riêng cho IP Phone, đảm bảo độ trễ thấp.

- Thường gán CoS (Class of Service) = 5 cho thoại (ưu tiên cao).
- Các kỹ thuật: marking (CoS/DSCP), policing, shaping, queuing.

5. VXLAN (Virtual Extensible LAN)

- VXLAN mở rộng VLAN qua hạ tầng mạng Layer 3 bằng cách encapsulate frame Layer 2 trong UDP/IP.
- Dùng VNI (VXLAN Network Identifier) 24-bit, hỗ trợ tới 16 triệu mạng ảo.
- Cấu trúc gói VXLAN gồm: Outer MAC + Outer IP + UDP (port 4789) + VXLAN Header + Ethernet gốc.
- Cho phép tạo mạng Layer 2 mở rộng giữa các Data Center.

6. VRF (Virtual Routing and Forwarding) và phân tách mạng

- VRF tách bảng định tuyến logic, tạo nhiều instance mạng riêng biệt trên cùng thiết bị.
- Tương tự như VLAN ở Layer 3 – cho phép nhiều tenant hoạt động độc lập.
- Ứng dụng trong MPLS VPN, bảo mật multi-tenant.
- Có thể kết hợp VXLAN + VRF để xây kiến trúc mạng phân tán và scalable.

7. Các cơ chế bảo mật và kiểm soát VLAN

- Port Security: giới hạn MAC được phép truy cập.
- Private VLAN: tách biệt máy trong cùng VLAN.
- VLAN Hopping attack: tấn công vượt VLAN qua switch misconfiguration hoặc gắn tag giả.
- Giải pháp: disable DTP, dùng trunk allowed cụ thể, kiểm soát native VLAN.