

Triển khai VLAN, STP & Định tuyến Mạng

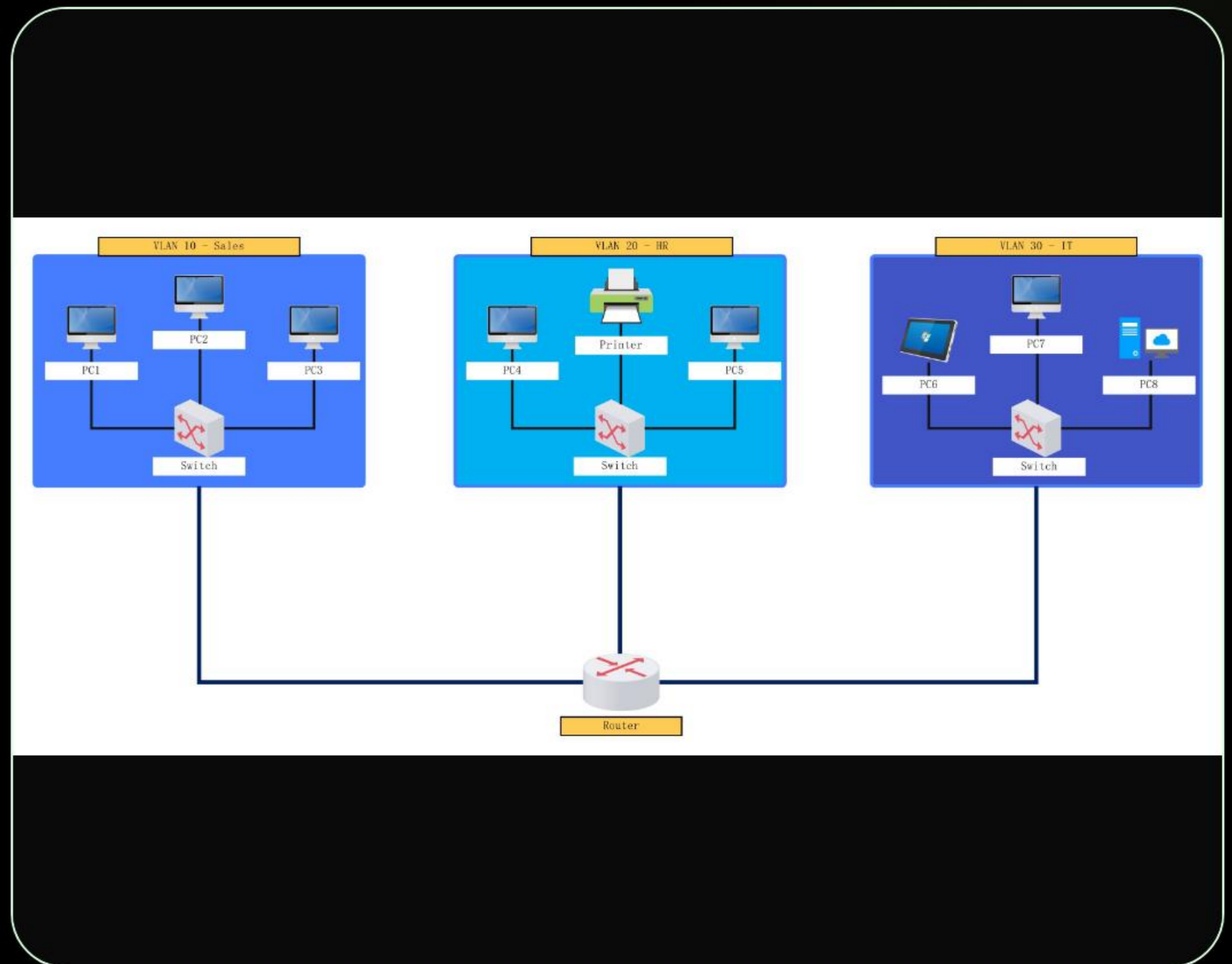
Hướng dẫn chi tiết về cấu hình hạ tầng mạng Layer 2 và các giải pháp định tuyến Inter-VLAN chuyên nghiệp.

Phần 1: Tổng quan về VLAN

Cơ sở hạ tầng mạng logic và phân đoạn người dùng.

Khái niệm Mạng LAN ảo (VLAN)

- ☰ Phân chia mạng vật lý thành các mạng logic riêng biệt.
- 🛡 Tăng cường bảo mật bằng cách cách ly lưu lượng giữa các phòng ban.
- ⚡ Giảm kích thước miền quảng bá (Broadcast Domain), tối ưu hiệu suất.
- 🔧 Quản lý linh hoạt: Người dùng có thể ở bất kỳ vị trí vật lý nào.



Các dải VLAN ID tiêu chuẩn

Dải VLAN	Mục đích sử dụng	Ghi chú
0, 4095	Dự phòng hệ thống	Không thể chỉnh sửa
1	Mặc định (Cisco Default)	Không thể xóa
2 - 1001	VLAN thông dụng	Dành cho Ethernet
1002 - 1005	Cisco Defaults	FDDI và Token Ring
1006 - 4094	Mở rộng (Extended)	Dùng cho Service Provider

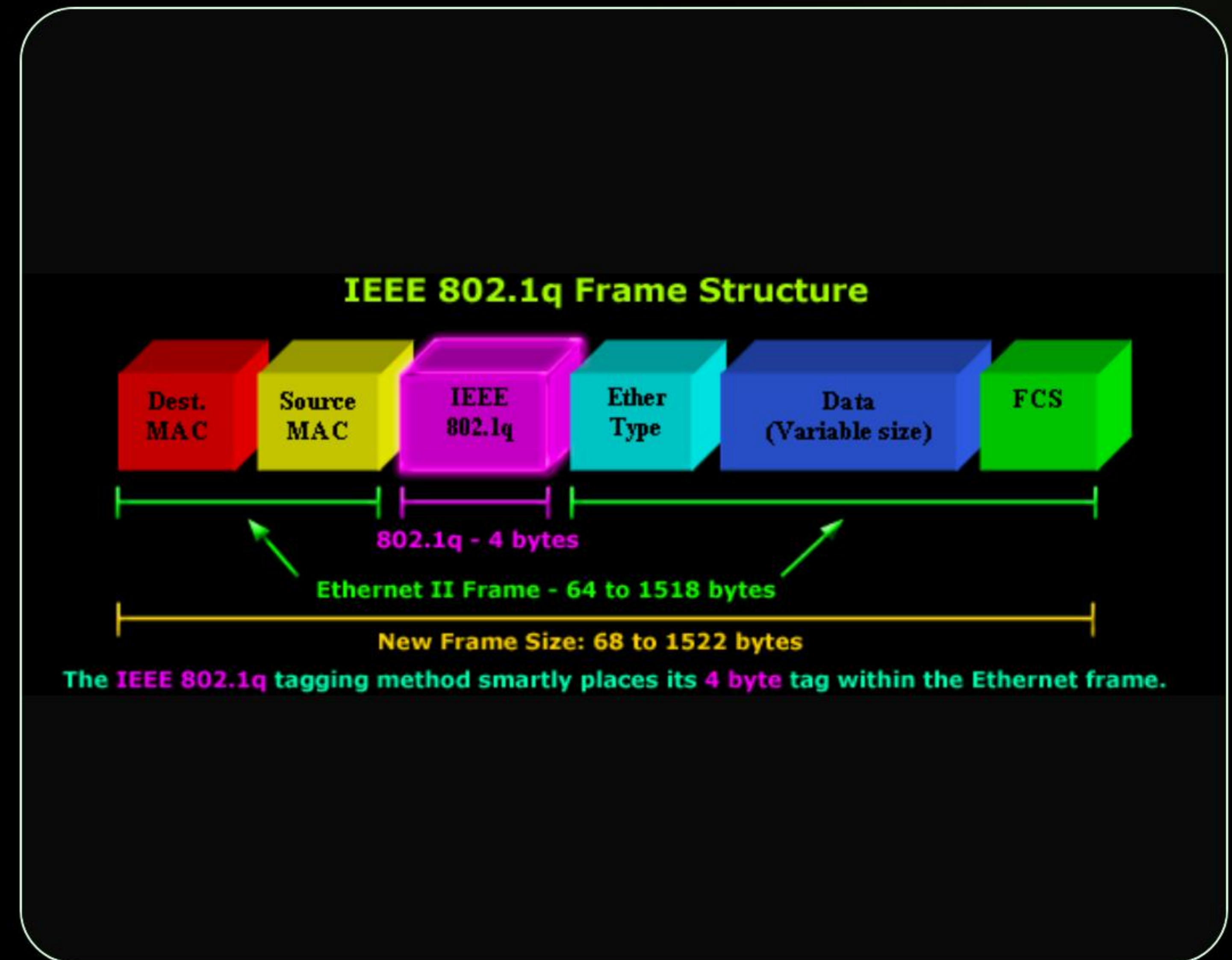
Phần 2: Trunking & Giao thức VTP

Truyền tải đa VLAN và đồng bộ hóa cấu hình tự động.

Giao thức 802.1Q Trunking

Cổng Trunk cho phép truyền tải dữ liệu của nhiều VLAN trên một kết nối vật lý duy nhất giữa các Switch.

- 🏷️ **Tagging:** Chèn thêm 4-byte header để định danh VLAN ID.
- 🌿 **Native VLAN:** Lưu lượng của VLAN này sẽ không được gắn tag khi truyền qua Trunk.
- </> **Lệnh cấu hình:** `switchport mode trunk.`



Các chế độ hoạt động của VTP



Server

Chế độ mặc định. Cho phép tạo, sửa, xóa VLAN và quảng bá thông tin cho toàn bộ Domain.



Client

Không thể thay đổi cấu hình VLAN. Chỉ nhận và đồng bộ hóa từ Server.



Transparent




Chỉ cho phép quản lý VLAN cục bộ. Chuyển tiếp quảng bá VTP nhưng không đồng bộ vào database.

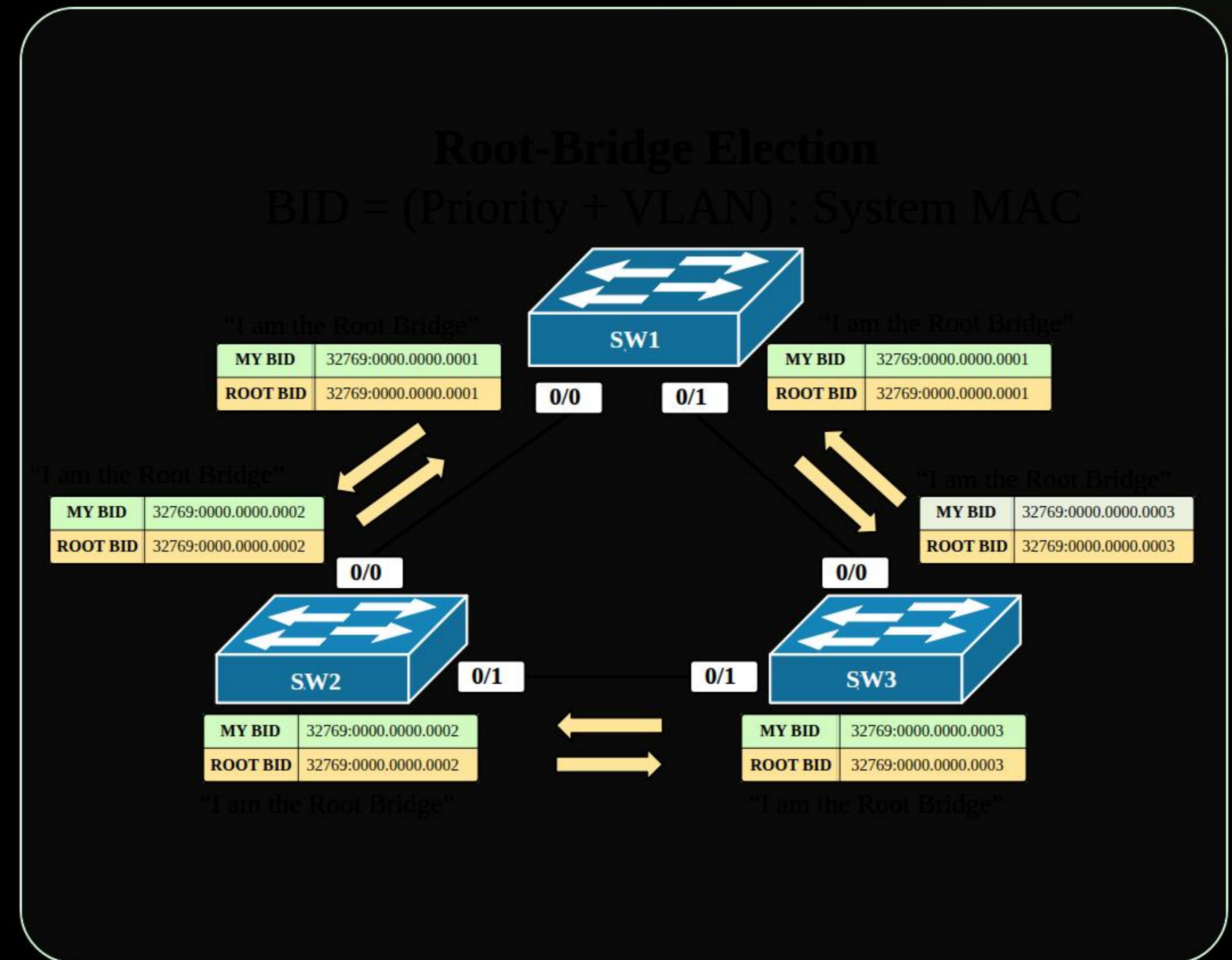
Phần 3: Spanning Tree (STP)

Cơ chế chống Loop và đảm bảo tính dự phòng cho mạng lớp 2.





Bầu chọn Root Bridge

STP bầu chọn một Root Bridge làm "gốc" để xây dựng sơ đồ mạng không có vòng lặp.

-  **Bridge ID:** Gồm Priority (mặc định 32768) và MAC Address.
-  Thiết bị có Bridge ID thấp nhất sẽ trở thành Root Bridge.
-  **Path Cost:** Chi phí đường truyền dựa trên băng thông (10Gbps=2, 1Gbps=4, 100Mbps=19).



Cơ chế Bảo mật STP

-  **BPDU Guard:** Ngắt ngay lập tức cổng Access nếu nhận được gói tin BPDU, ngăn chặn Switch lạ kết nối vào.
-  **Root Guard:** Ngăn chặn một Switch mới tham gia vào mạng chiếm quyền làm Root Bridge.
-  **Loop Guard:** Ngăn chặn loop xảy ra khi một cổng đáng lẽ phải ở trạng thái Blocking lại chuyển sang Forwarding do lỗi vật lý.
-  **PortFast:** Cho phép cổng Access chuyển thẳng sang trạng thái Forwarding mà không cần đợi 30 giây hội tụ.

Gộp liên kết với EtherChannel

EtherChannel cho phép gộp tới 8 liên kết vật lý thành một liên kết logic duy nhất.

- + Tăng băng thông tổng thể giữa các Switch.
- ❤️ Cung cấp khả năng dự phòng: Nếu một link chết, traffic vẫn chạy trên các link còn lại.
- 👉 Giao thức: LACP (Chuẩn mở IEEE) hoặc PAgP (Cisco).

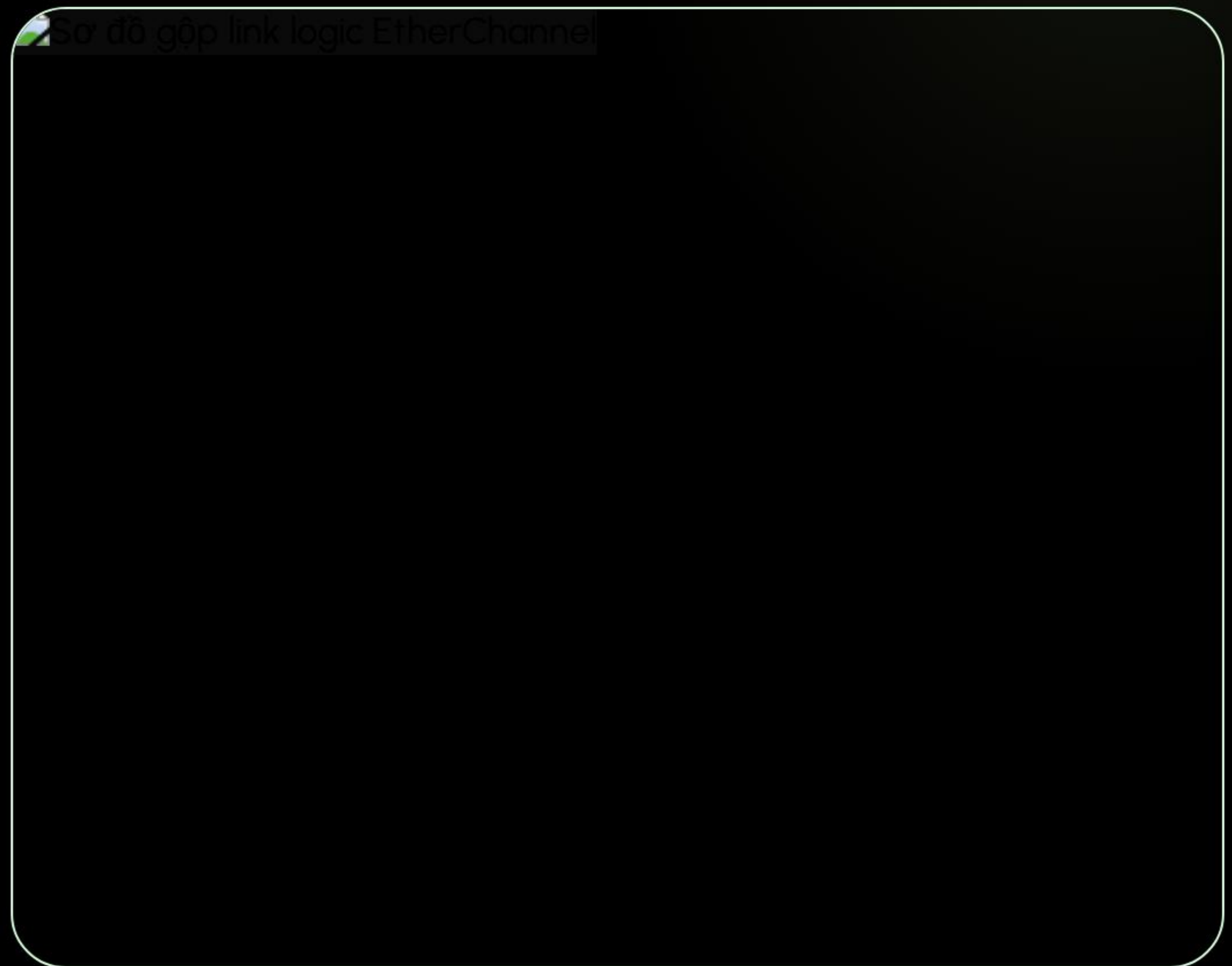
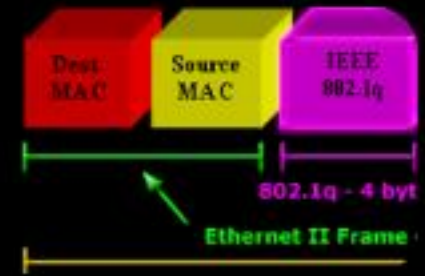


Image Sources



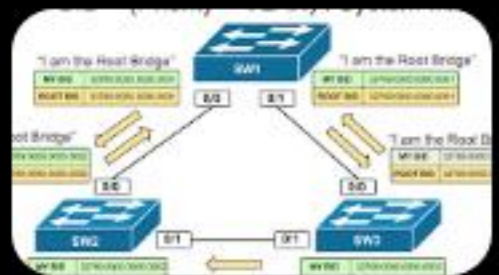
<https://edrawmax.wondershare.com/templates/Network/vlan-network-diagram.jpg>

Source: edrawmax.wondershare.com



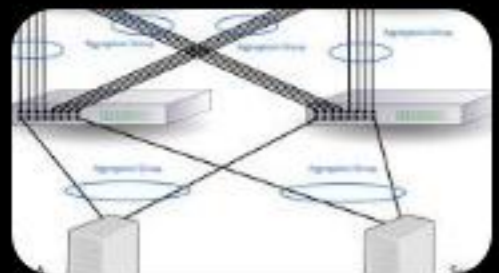
<https://www.firewall.cx/images/stories/vlans-8021q-analysis-1.gif>

Source: www.firewall.cx



<https://www.networkacademy.io/sites/default/files/inline-images/root-bridge-election-process-step-1.svg>

Source: www.networkacademy.io



<https://cciedump.spoto.net/static/upload/images/common/a43ae0c0450d9a3d0374b21b4b57283a.png>

Source: cciedump.spoto.net
