CANTHO UNIVERSITY

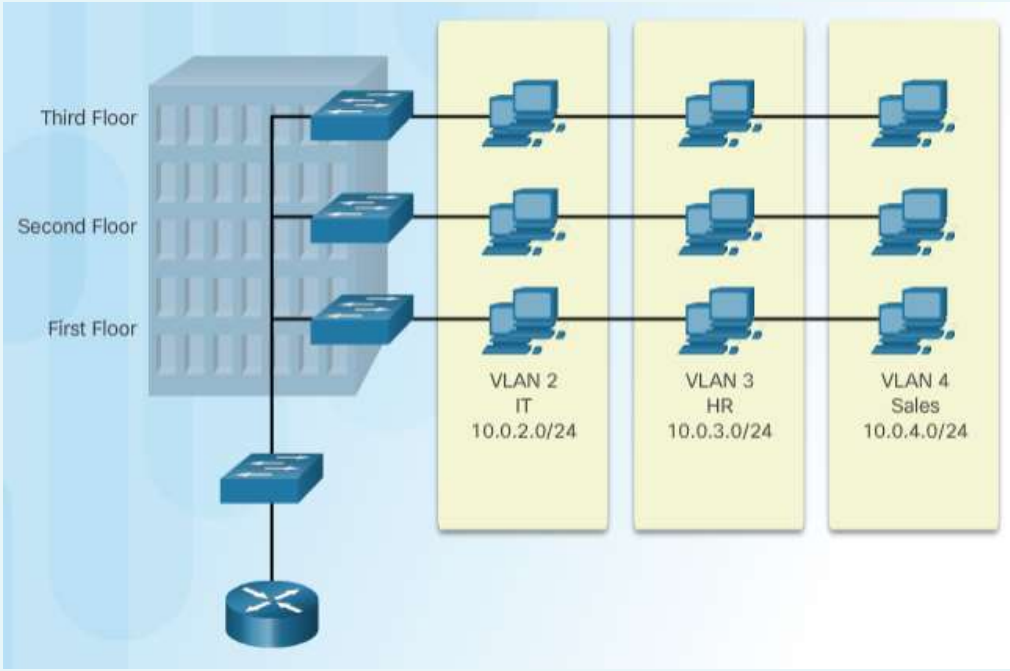
THIẾT KẾ CÀI ĐẶT MẠNG MÁY TÍNH

MÃ SỐ HỌC PHẦN: CT335

CHƯƠNG 7: MẠNG CỤC BỘ ẢO VIRTUAL LAN

GIỚI THIỆU VLAN

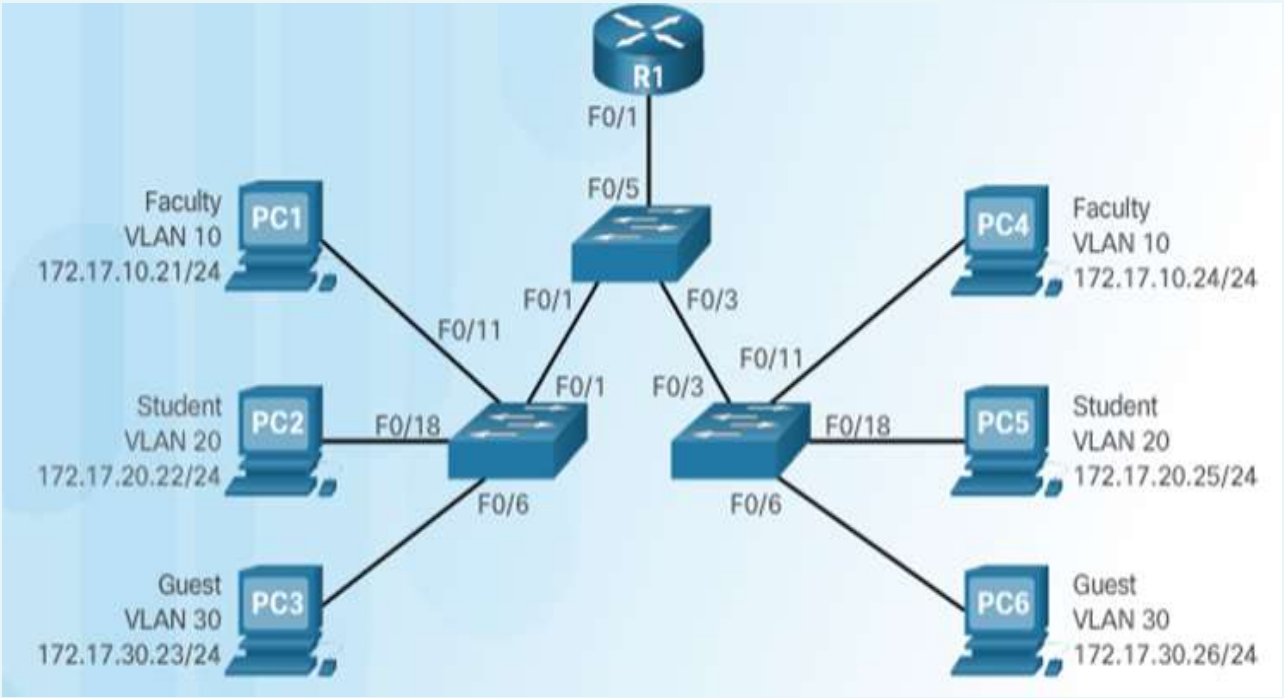
- VLAN cho phép phân đoạn các LAN mà không cần quan tâm đến vị trí thực của người dùng hoặc thiết bị
- Có thể tạo nhiều phân vùng và nhiều VLAN cùng tồn tại
- Mỗi VLAN là một miền quảng bá
- Việc phân vùng logic của mạng được thực hiện trên thiết bị tầng 2, thường dùng là bộ chuyển mạch
- Các thiết bị trên cùng một VLAN không biết về sự tồn tại của VLAN
- Các VLAN được cách ly lẫn nhau và các gói tin chỉ có thể truyền giữa các VLAN thông qua một bộ định tuyến (router)



CANTHO UNIVERSITY

THUẬN LỢI CỦA VLAN

- Tăng cường độ an ninh
- Giảm chi phí
- Cải thiện hiệu suất mạng
- Giảm kích thước miền quảng bá
- Quản trị hệ thống đơn giản hơn, hiệu quả hơn



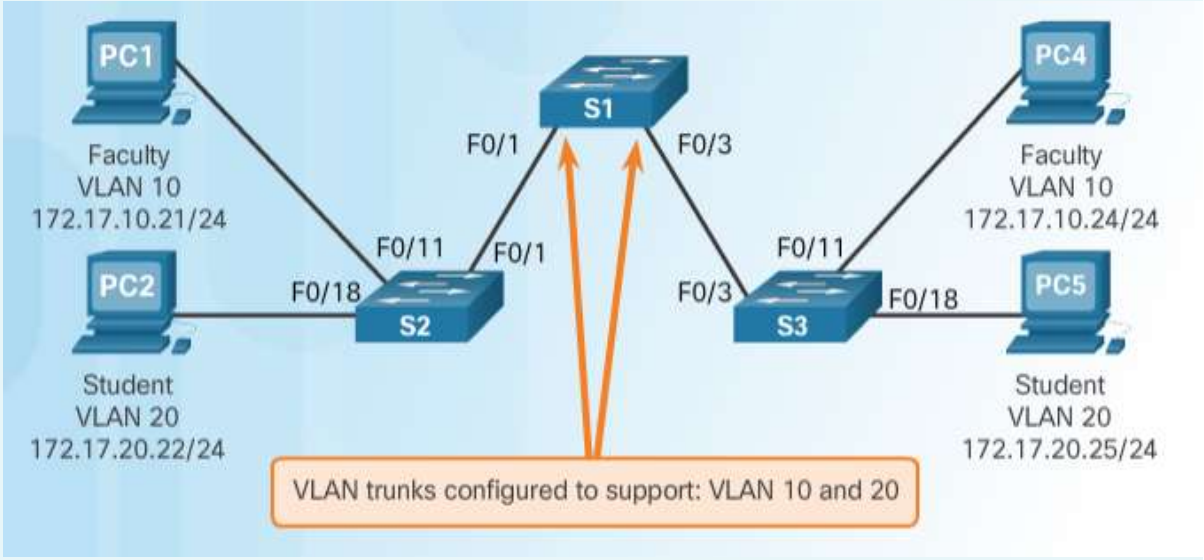
CANTHO UNIVERSITY

KIỂM SOÁT MIỀN QUẢNG BÁ

- Nếu một cổng của switch nhận một khung quảng bá, switch sẽ chuyển ra tất cả các cổng trừ cổng khung đi vào
  - Toàn bộ các thiết bị nhận được khung quảng bá đó do cùng một miền quảng bá
- VLAN được xem như giới hạn được sự quảng bá các khung ra toàn bộ các thiết bị kết nối vì mỗi VLAN là một miền quảng bá riêng biệt cho dù trong cùng một switch
  - VLAN giúp điều khiển sự ảnh hưởng của các khung quảng bá

Trong hình minh họa, PC1 thuộc VLAN 10 gửi một khung quảng bá

- Đường kết nối giữa S1 – S2 và S1 - S3 được cấu hình kiểu trunk nên có thể mang khung lan truyền khung quảng bá tới các thiết bị khác trong cùng VLAN 10
- Chỉ những thiết bị cùng VLAN mới nhận được các khung quảng bá đó, do vậy, chỉ có PC4 đang kết nối với S3 nhận được khung quảng bá do cùng VLAN 10 với PC1
- Các máy còn lại không nhận được khung quảng bá từ PC1



CANTHO UNIVERSITY

CÁC KIỂU VLAN

- Một số kiểu VLAN phổ biến:

– **Default VLAN**: mặc định là VLAN 1. Tất cả các cổng của switch được khởi tạo thuộc VLAN 1

– **Data VLAN**: là VLAN được tạo cho các dữ liệu thông thường trong thiết bị của người dùng trong mạng.

– **Native VLAN:** đây là một VLAN đặc biệt mang những dữ liệu không gán thẻ lưu thông khi qua đường trunk. Dữ liệu thường không được phát ra từ các cổng thuộc VLAN (vd như STP BPDU trao đổi giữa các switch)

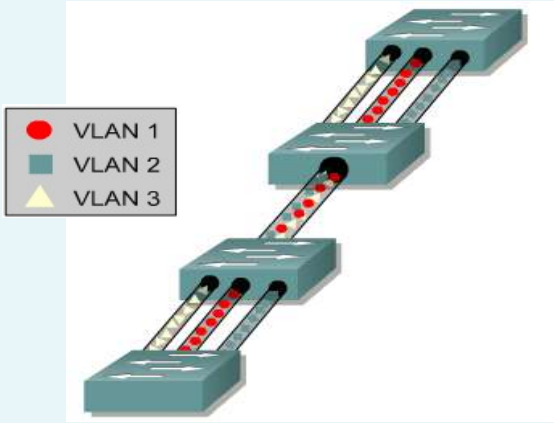
– **Management VLAN:** đây là VLAN được quản trị mạng tạo ra để mang các lưu thông của các dịch vụ quản trị như Telnet, SSH, SNMP, Syslog...

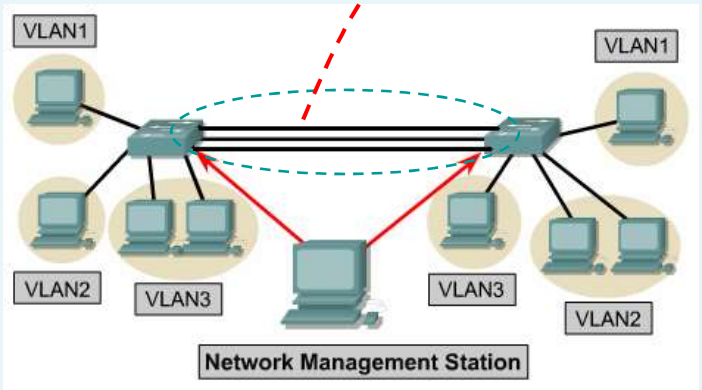
```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1, Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

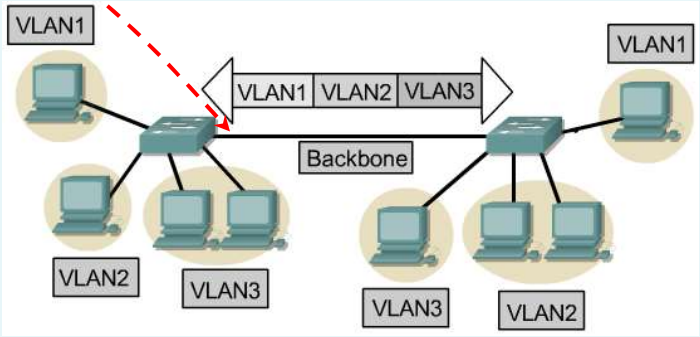
Một số VLAN mặc định trên Switch của Cisco
VLAN 1 dùng cho mạng Fast Ethernet, tất cả các cổng mặc định đều thuộc VLAN 1

CANTHO UNIVERSITY

KẾT NỐI GIỮA CÁC VLAN







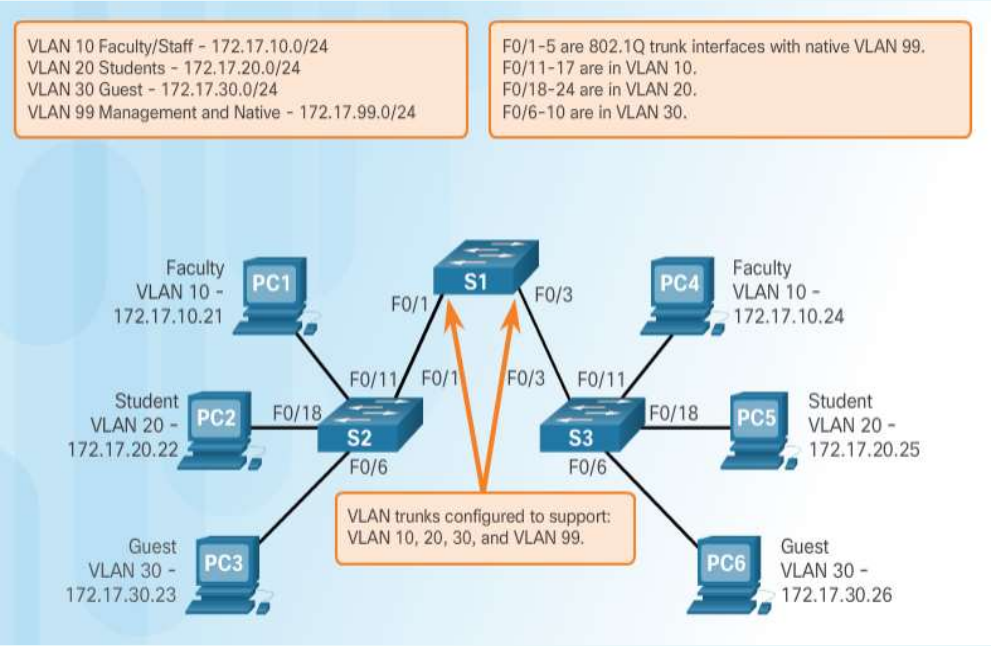
CANTHO UNIVERSITY

VLAN TRUNK

- Đường trunk là một liên kết point-to-point mang lưu thông của *nhiều hơn một* VLAN

– *Thường được thiết lập giữa các switch để hỗ trợ truyền dữ liệu của các VLAN*

– *Một cổng được cấu hình kiểu trunk thì cổng đó không thuộc một VLAN nào*



Đường kết nối giữa S1 và S2, S1 và S3 được cấu hình kiểu trunk để mang lưu thông của các VLANs 10, 20, 30 và 99

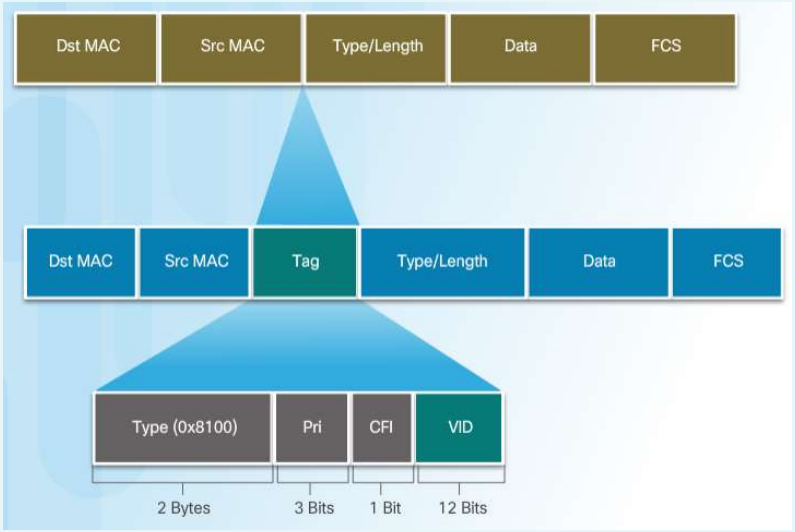
- Giao thức dùng trên đường trunk được chuẩn hóa trong chuẩn IEEE 802.1q

CANTHO UNIVERSITY

GẮN THẺ QUẢN LÝ KHUNG QUA ĐƯỜNG TRUNK

- Trước khi khung được chuyển ra khỏi giao diện của switch được cấu hình kiểu Trunk, khung phải được gắn thẻ để quản lý thông tin VLAN
  - Một thẻ được thêm vào header của khung để nhận diện VLAN
  - Trong đường trunk có nhiều khung thuộc các VLAN khác nhau lưu thông đồng thời
- IEEE 802.1Q là một giao thức đường trunk phổ biến

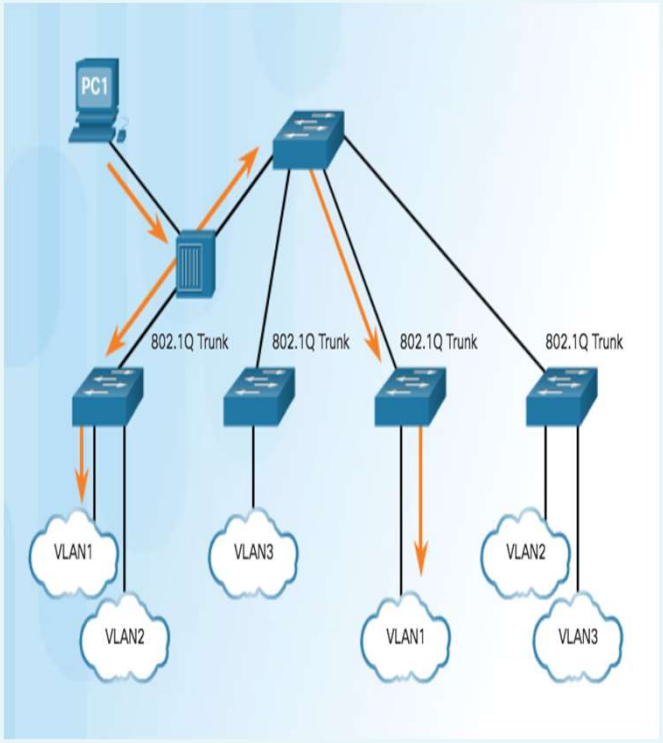
- ✓ Switch thêm thẻ thông tin VLAN sau trường địa chỉ MAC nguồn
- ✓ Một trường trong thẻ 802.1Q chứa thông tin VLAN ID (VID).
- ✓ Đường trunk thêm thẻ thông tin trước khi gửi khung vào đường trunk
- ✓ Ở phía đối diện, khung sẽ được kiểm tra thông tin trên thẻ để xác định thuộc VLAN nào thì sẽ chuyển sang các cổng thuộc VLAN phù hợp. Thẻ sẽ được gỡ bỏ khi ra khỏi đường trunk



CANTHO UNIVERSITY

NATIVE VLAN VÀ THẺ 802.1Q

- ***Native VLAN*** là VLAN mang dữ liệu liên lạc giữa các switch, không mang dữ liệu người dùng
- Điều khiển lưu thông trên switch sẽ không gắn thẻ các khung thuộc ***native VLAN***
- Phía đối diện, switch nhận diện các khung không có gắn thẻ sẽ chuyển vào ***native VLAN***
- Nếu cổng trunk không có khai báo cổng nào liên quan đến *native VLAN* và khi một khung đến giao diện kiểu trunk mà không có gắn thẻ thì khung sẽ bị bỏ đi



CANTHO UNIVERSITY

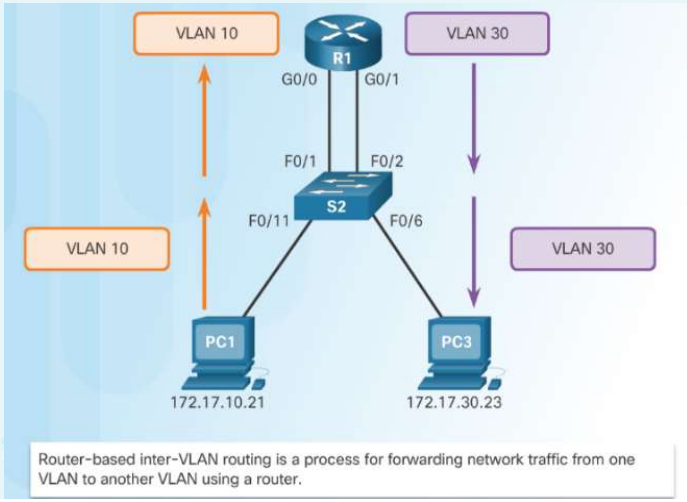
KẾT NỐI GIỮA CÁC VLAN

- Switch tầng 2 không thể chuyển mạch lưu thông (định tuyến) các khung thuộc các VLAN khác nhau
- Các VLAN khác nhau thuộc các miền quảng bá khác nhau chỉ trao đổi được lưu thông thông qua router
- Định tuyến giữa các VLAN là một quá trình chuyển tiếp lưu thông mạng từ VLAN này sang VLAN khác thông qua router
- Có 3 cách thức để kết nối giữa các VLAN:

➢ Định tuyến theo cách truyền thống (dùng router, mỗi VLAN gắn vào một giao diện)

➢ Router-on-a-Stick (đường trunk IEEE 802.1q)

➢ Dùng MultiLayer Switch cấu hình giao diện theo kiểu SVI



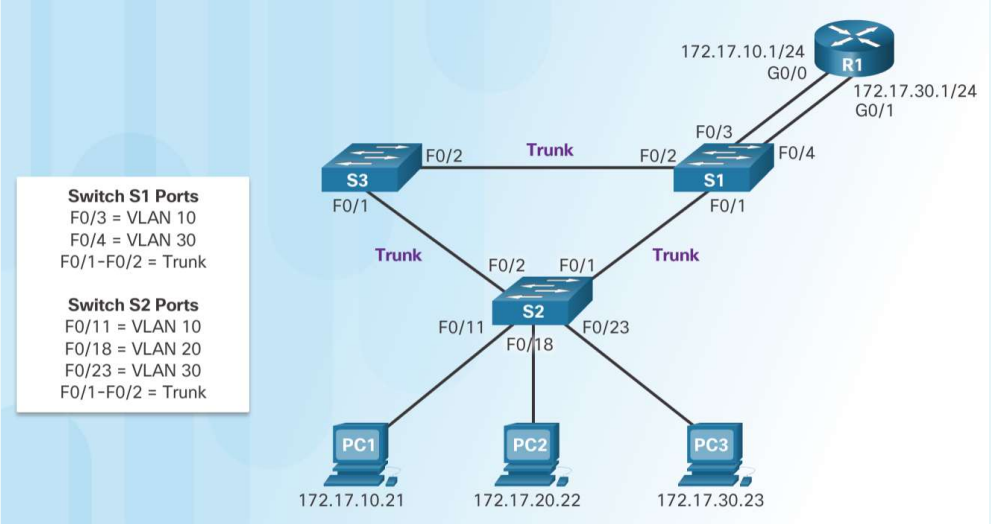
Router-based inter-VLAN routing is a process for forwarding network traffic from one VLAN to another VLAN using a router.

ĐỊNH TUYẾN KIỂU TRUYỀN THỐNG

Kiểu truyền thống:

- Router được sử dụng để định tuyến giữa các VLAN
- Mỗi VLAN được kết nối với một giao diện vật lý khác nhau của router
- Các gói tin sẽ đến router thông qua một giao diện, được định tuyến và đi đến mạng đích qua một giao diện khác
- Các mạng có số lượng VLAN lớn thì yêu cầu nhiều giao diện trên router

Trong hình, router R1 được cấu hình để kết nối 02 giao diện với 02 VLAN riêng biệt.



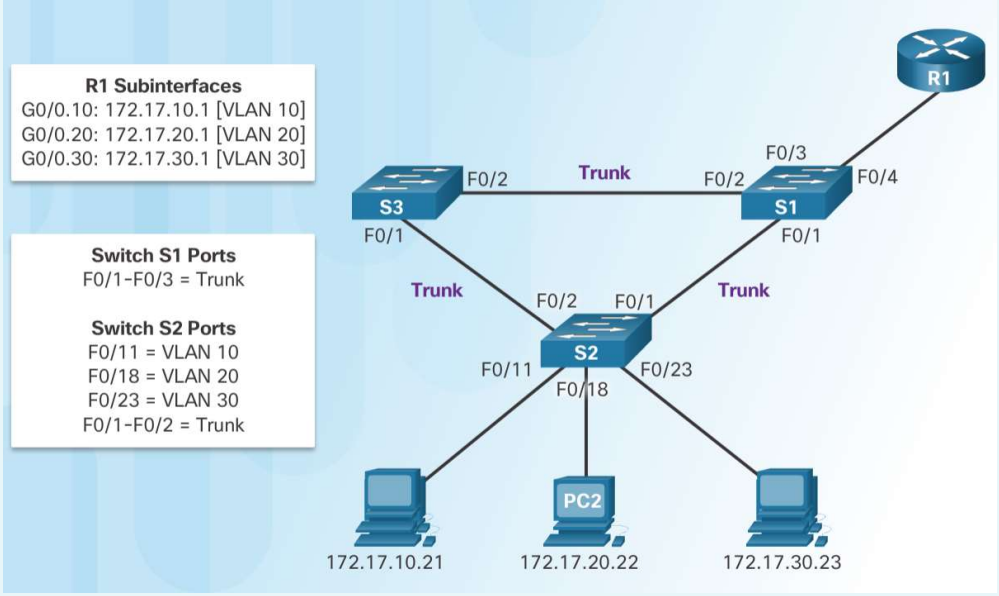
ĐỊNH TUYẾN KIỂU ROUTER-ON-A-STICK

CANTHO UNIVERSITY

- **Router-on-a-Stick** là cách thức định tuyến nhiều VLAN trên 1 giao diện vật lý của router
  - Một giao diện vật lý của router được cấu hình với giao thức IEEE 802.1Q (trunk) để nó có thể hiểu các thẻ gắn vào mỗi VLAN
  - Các giao diện con (sub-interface) logic được tạo ra và mỗi sub-interface được gán để thuộc về một VLAN
  - Mỗi sub-interface được cấu hình với một địa chỉ IP thuộc VLAN. Đây chính là địa chỉ gateway của VLAN đó
  - Các máy tính hay thiết bị thuộc VLAN được cấu hình sẻ khai báo địa chỉ của sub-interface làm *default gateway*

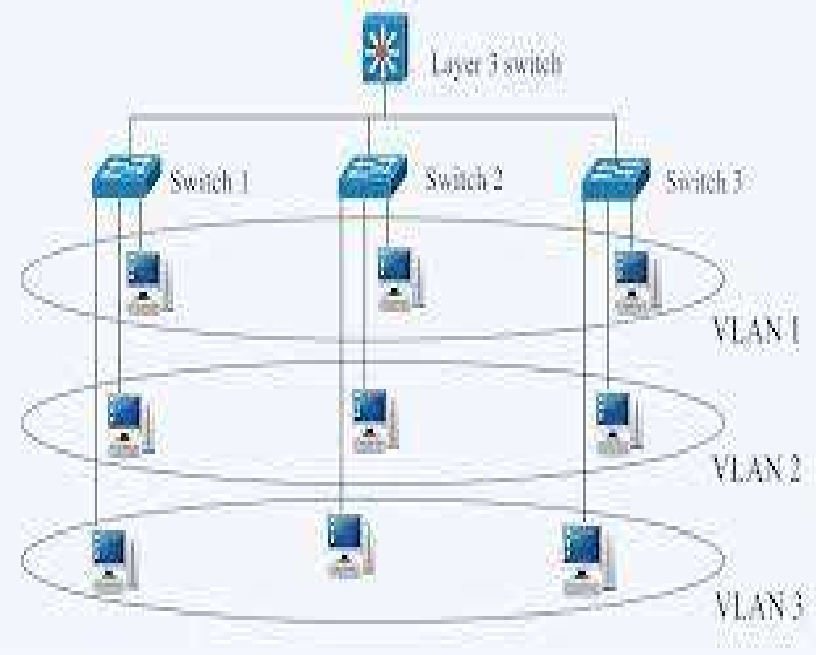
Trong hình bên dưới, giao diện trên router R1 được cấu hình theo chuẩn IEEE 802.1Q (trunk) đang kết nối với cổng F0/4 của switch S1 (cũng phải khai báo kiểu trunk)

- Router nhận các lưu thông có gắn thẻ VLAN trên giao diện
- Router chuyển mạch lưu thông giữa các sub-interface trong giao diện vật lý đó



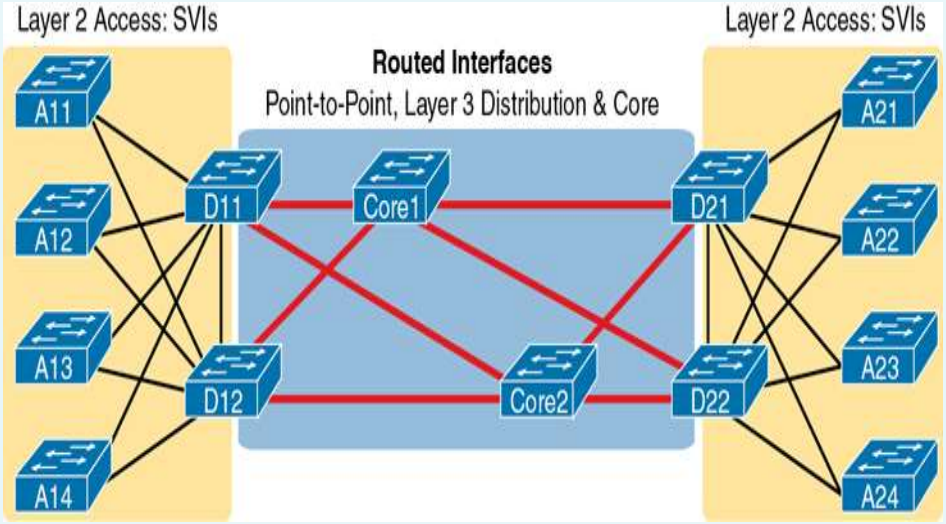
SỬ DỤNG SWITCH LAYER 3 TRIỂN KHAI SWITCH VIRTUAL INTERFACE (SVI)

- Switch layer 3 có đầy đủ chức năng của switch layer 2, bên cạnh đó switch layer 3 là những router tốc độ cao nhưng lại không có cổng kết nối WAN
- Với đặc điểm được gắn thêm bảng định tuyến IP ở bên trong, nó được sử dụng để nối kết các mạng con LAN hoặc VLAN
- Hệ thống hoạt động ổn định hơn mà không cần đến router, switch layer 3 có năng lực xử lý vượt trội hơn so với switch layer 2



SỬ DỤNG SWITCH LAYER3 TRIỂN KHAI SWITCH VIRTUAL INTERFACE (SVI)

- Triển khai SVI là việc tạo ra các interface VLAN trên multilayer switch, các interface này sẽ là default gateway cho các VLAN tương ứng. Lúc này, các cổng SVI trên switch hoạt động tương đương với một cổng của router
- Nhờ năng lực chuyển mạch lớp 3 mạnh mẽ, phương pháp này gần như là tốt nhất, vượt xa các phương pháp khác, tốc độ chuyển khung nhanh nhất, bảo đảm việc định tuyến nhanh, đáng tin cậy



CANTHO UNIVERSITY

CÁC CÁCH CÀI ĐẶT VLAN

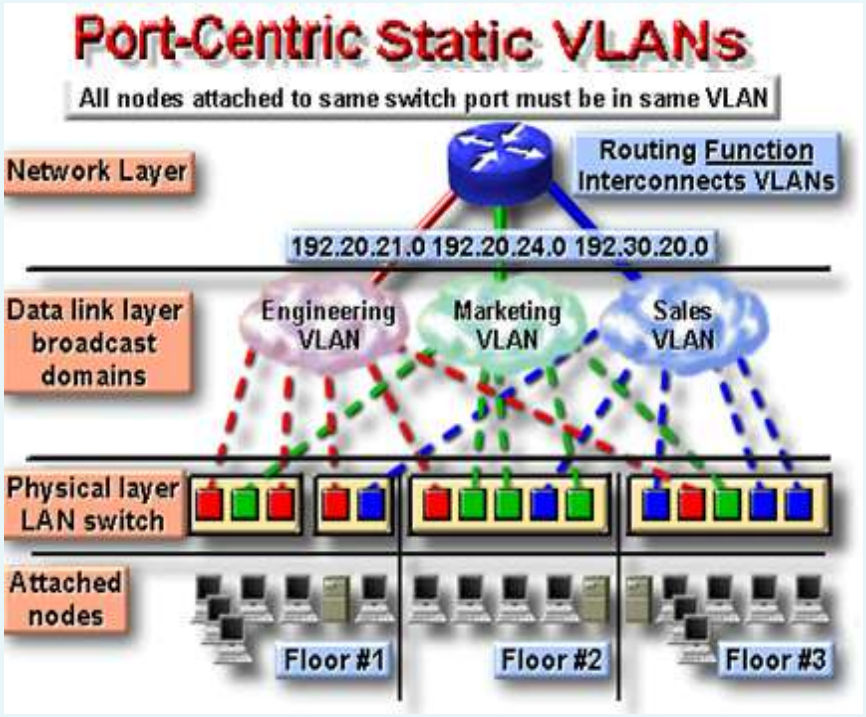
- **Mô hình cài đặt VLAN tĩnh**

➢ Cài đặt VLAN tĩnh là một nhóm các cổng trên một switch được nhà quản trị mạng gán vào một VLAN

➢ Mỗi thiết bị được gán thuộc một VLAN dựa trên cổng mà thiết bị đó đang kết nối

➢ Các VLAN được quản lý một cách dễ dàng

➢ Tăng cường tối đa tính an toàn của VLAN



CANTHO UNIVERSITY

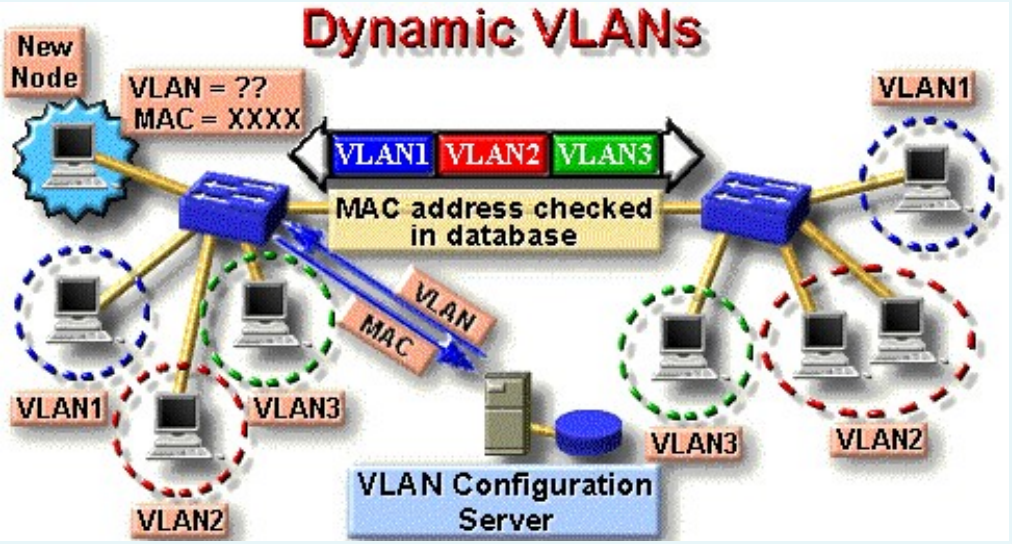
CÁC CÁCH CÀI ĐẶT VLAN

- **Mô hình cài đặt VLAN động**

➢ Cấu hình VLAN động là thực hiện nhóm các cổng trên một switch thuộc một VLAN nào đó một cách tự động thông qua *phần mềm quản lý VLAN động*

➢ Phần mềm quản lý VLAN động có thể thực hiện trên máy chủ chuyên dụng hay được cài đặt sẵn trên switch

➢ Việc quản lý VLAN động và các thiết bị được dựa trên địa chỉ vật lý MAC hay trên thông tin xác thực của người dùng



HẾT CHƯƠNG 7