VLAN

**I. Khái niệm**

+ Là kết nối ảo hóa kết nối nhiều thiết bị và nút mạng từ các mạng LAN khác nhau vào một mạng logic.

+ VLAN range:

* **VLAN 0, 4095:** Đây là VLAN được dành riêng, không thể nhìn thấy hoặc sử dụng.
* **VLAN 1:** Đây là VLAN mặc định của các switch. Theo mặc định, tất cả các cổng switch đều nằm trong VLAN. VLAN này không thể xóa hoặc chỉnh sửa nhưng có thể sử dụng.
* **VLAN 2-1001:** Đây là phạm vi VLAN bình thường. Chúng ta có thể tạo, chỉnh sửa và xóa các VLAN này.
* **VLAN 1002-1005:** Đây là mặc định của CISCO cho fddi và token rings. Không thể xóa các VLAN này.
* **Vlan 1006-4094:** Đây là phạm vi mở rộng của Vlan.

+ Các loại kết nối trong VLAN:

* Trunk link:

+ Tất cả các thiết bị được kết nối đến trunk link phải nhận biết VLAN. Tất cả các frame trên đó phải có một header đặc biệt được gắn vào gọi là tagged frame.

* Liên kết truy cập:

+ Kết nối các thiết bị không nhận biết VLAN với cầu nối nhận biết VLAN. Tất cả các khung trên liên kết truy cập phải không được gắn thẻ.

* Liên kết lai:

+ Đây là sự kết hợp của liên kết Trunk và liên kết Access. Ở đây, cả thiết bị không nhận biết VLAN và thiết bị nhận biết VLAN đều được kết nối và có thể có cả khung được gắn thẻ và không được gắn thẻ

**II. Cách hoạt động:**

+ VLAN được nhận diện trên switch thông qua VLAN ID. Mỗi cổng trên Switch có thể có 1 hoặc nhiều VLAN ID được gán cho nó và sẽ nằm trong VLAN mặc định nếu không có cổng nào được gán.

+ VLAN ID được dịch sang VLAN tag, là một trường 12 bit trong header của mỗi khung Ethernet (Ethernet Frame) được gửi tới VLAN đó. Vì tag dài 12 bit nên có thể xác định tối đa 4096 Vlan trên mỗi miền switch. VLAN tag được xác định bởi IEEE trong tiêu chuẩn 802.1Q

+ Khi khung Ethernet được nhận từ máy chủ đính kèm, nó không có VLAN tag. Switch sẽ thêm VLAN tag. Trong VLAN tĩnh, Switch sẽ chèn VLAN tag được liên kết với VLAN ID của cổng vào. Trong VLAN động, nó chèn tag được liên kết với ID của thiết đó bị hoặc loại lưu lượng mà nó tạo ra.

+ Chuyển tiếp các frame được gắn tag tới các địa chỉ kiểm soát truy cập phương tiện đích của chúng, chỉ chuyển tiếp đến các cổng mà VLAN được liên kết. Broadcast, unknow unicast, multicast traffic sẽ được chuyển tiếp tới toàn bộ port trong VLAN. Các liên kết **Trunk** giữa các switch biết VLAN nào trải rộng trên các switch, chấp nhận và chuyển tất cả lưu lượng truy cập cho bất kỳ VLAN nào được sử dụng ở 2 phía của trunk. Khi frame đến switch port đích, VLAN tag sẽ bị xóa trước khi khung được truyền đến thiết bị đích

+ Giao thức Spanning Tree (Spanning Tree Protocol) được sử dụng để tạo cấu trúc liên kết (topology) không có vòng lặp giữa các Switch Layer 2. Có thể sử dụng phiên bản STP trên mỗi VLAN, cho phép các cấu trúc liên kết Lớp 2 khác nhau. STP đa phiên bản cũng có thể được sử dụng để giảm chi phí STP nếu cấu trúc liên kết giống nhau giữa nhiều VLANs.

**III. Phân loại VLAN**

1. Management VLAN

+ VLAN quản lý được cấu hình để truy cập vào các khả năng quản lý của một bộ chuyển mạch (lưu lượng như ghi nhật ký hệ thống, giám sát). VLAN 1 là VLAN quản lý theo mặc định (VLAN 1 sẽ là lựa chọn tồi cho VLAN quản lý). Bất kỳ VLAN nào của bộ chuyển mạch cũng có thể được định nghĩa là VLAN quản lý nếu quản trị viên chưa cấu hình một VLAN duy nhất để làm VLAN quản lý. VLAN này đảm bảo rằng băng thông để quản lý sẽ khả dụng ngay cả khi lưu lượng người dùng cao.

A diagram of a network

Description automatically generated

1. Data VLAN

+ Data VLAN được sử dụng để chia toàn bộ mạng thành 2 nhóm. Một nhóm người dùng và nhóm thiết bị khác. VLAN này còn được gọi là VLAN người dùng, VLAN dữ liệu chỉ được sử dụng cho dữ liệu do người dùng tạo ra. VLAN này chỉ mang dữ liệu. Nó không được sử dụng để mang lưu lượng quản lý hoặc giọng nói.A diagram of a network

Description automatically generated

1. Voice VLAN:

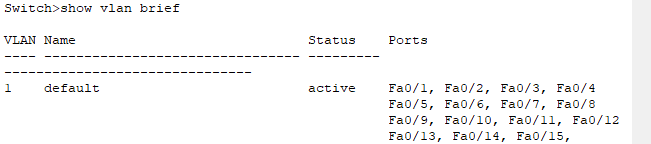
+ Voice VLAN được cấu hình để truyền lưu lượng thoại. Voice VLAN thường được ưu tiên truyền tải cao hơn các loại lưu lượng mạng khác. Để đảm bảo chất lượng thoại qua IP (VoIP) (độ trễ dưới 150 mili giây (ms) trên toàn mạng), chúng ta phải có voice VLAN riêng vì điều này sẽ bảo toàn băng thông cho các ứng dụng khác.

A diagram of a telephone

Description automatically generated

1. Default VLAN

+ Khi switch khởi động lần đầu, tất cả các cổng switch đều trở thành thành viên của VLAN mặc định (nói chung tất cả các switch đều có VLAN mặc định được đặt tên là **VLAN 1** ), khiến chúng trở thành một phần của cùng một miền phát sóng. Sử dụng VLAN mặc định cho phép bất kỳ thiết bị mạng nào được kết nối với bất kỳ cổng switch nào kết nối với các thiết bị khác trên các cổng switch khác. Một tính năng độc đáo của VLAN mặc định là không thể đổi tên hoặc xóa.



A diagram of a router

Description automatically generated

1. Native VLAN

+ VLAN này xác định lưu lượng đến từ mỗi đầu của liên kết trunk. Một native VLAN chỉ được phân bổ cho một cổng trunk 802.1Q. Cổng trunk 802.1Q đặt lưu lượng không được gắn thẻ (lưu lượng không đến từ bất kỳ VLAN nào) trên native VLAN. Tốt nhất là cấu hình native VLAN thành một VLAN chưa sử dụng.

A diagram of a network

Description automatically generated

1. VLAN dựa trên cổng

+ Trong VLAN dựa trên cổng, mỗi cổng trên một công tắc tổ chức được chuyển đến một VLAN cụ thể. Tất cả lưu lượng trên cổng đó sau đó được chỉ định tự nhiên đến VLAN liên quan đến cổng đó.

1. VLAN được gắn thẻ (tag)

+ VLAN được gắn thẻ được sử dụng để hỗ trợ các VLAN khác nhau trên một cổng thực tế duy nhất. Trong loại VLAN này, mỗi bưu kiện được gắn nhãn với một ID VLAN, nhận dạng VLAN mà nó có một vị trí. Điều này cho phép các VLAN khác nhau được duy trì trong một cổng thực tế duy nhất.

1. VLAN dựa trên giao thức

+ VLAN dựa trên giao thức sử dụng dữ liệu quy ước Lớp 3 để phân phối các gói cho một VLAN. Ví dụ, tất cả lưu lượng truy cập cho một quy ước cụ thể, như IPX, có thể được chuyển đến một VLAN cụ thể. Loại VLAN này ít được sử dụng hơn so với VLAN dựa trên cổng và có nhãn.

**IV. So sánh VLAN và Subnet:**

A screenshot of a computer

Description automatically generated

**V. Định tuyến VLAN (Inter VLAN Routing - IVR):**

1. Định tuyến VLAN bằng Switch Layer 3:

+ Sử dụng một loại Switch đặc biệt gọi là Multiplayer Switch hoặc Switch Layer 3 để thực hiện định tuyến VLAN mà không cần sử dụng Router chuyên dụng. Switch Layer 3 là loại bộ chuyển mạch kết hợp tính năng định tuyến của router và hoạt động cả 2 tầng 2 và 3 của mô hình OSI. Nó có thể sử dụng các giao thức định tuyến như RIP, OSPF để thực hiện định tuyến giữa các VLAN và [mạng con](https://thietbimanggiare.com/subnetting-mang-con/).

+ Switch L3 sẽ sử dụng các giao diện logic ảo hay còn được gọi là SVI để liên kết cho mỗi VLAN. Một SVI sẽ định tuyến kết nối với 1 VLAN. Nó cũng được cấu hình với địa chỉ IP tương ứng với các VLAN trên Switch. Các SVI đảm bảo chuyển tiếp thông tin giữa các VLAN mà ko cần Router hay liên kết Trunk phức tạp.

+ Ví dụ:

A diagram of a firewall

Description automatically generated

* Quy trình:

+ A gửi gói tin dưới dạng Unicast đến Switch L2

+ Switch L2 nhận được gói tin và gắn thẻ TAG VLAN 10 rồi chuyển tiếp tới Switch L3 qua đường liên kết Trunk

+ Switch L3 nhận được gói tin và loại bỏ thẻ TAG rồi chuyển tiếp sang giao diện SVI tương ứng với VLAN 10

+ Switch L3 tiếp tục định tuyến lưu lượng đến SVI tương ứng của VLAN 20 và gắn thẻ TAG VLAN 20 gửi tới Switch L2

+ Switch L2 loại bỏ thẻ TAG và chuyển tiếp đến máy chủ B qua cổng Fa0/3

* Cấu hình:

+ Switch Layer 2:

A screenshot of a computer

Description automatically generated

+ Switch Layer 3:

A screenshot of a computer

Description automatically generated

A screenshot of a computer code

Description automatically generated

2. Định tuyến VLAN theo truyền thống:

+ Sẽ sử dụng một Router và kết nối với Switch qua nhiều cổng. Mỗi cổng cấu hình cho một VLAN cụ thể. Các cổng trên Router sẽ được thiết lập là các cổng mặc định cho các VLAN tương ứng được cấu hình trên Switch.

+ Khi một thiết bị từ VLAN này kết nối với VLAN khác, gói tin chuyển từ thiết bị đến cổng truy cập kết nối với Router tương ứng VLAN mà thiết bị kết nối. Router nhận được gói tin, nó kiểm tra [địa chỉ IP](https://thietbimanggiare.com/dia-chi-ip/) đích của gói tin và chuyển tiếp đến mạng đích bằng cổng truy cập tương ứng của VLAN đích.

+ Switch nhận được gói tin sẽ chuyến tiếp khung tới thiết bị đích vì Router đã đổi thông tin VLAN từ VLAN nguồn sang VLAN đích.

* Cách này rất đơn giản nhưng yêu cầu Router phải có số cổng bằng với số lượng VLAN cấu hình trên Switch. Do đó, nếu Switch có 10 VLAN thì Router cũng cần 10 cổng để thực hiện kết nối định tuyến dữ liệu. Do đó, cách này thường không được sử dụng.

+ Ví dụ minh họa:

A computer network diagram with a cable

Description automatically generated with medium confidence

+ Theo cách truyền thống, ta sẽ sử dụng 2 kết nối giữa Router và Switch để đặt định tuyến cho từng VLAN một. (Thông số như trên)

+ Khi đó A muốn gửi tin nhắn đến B thì quá trình sẽ diễn ra:

* Máy chủ A kiểm tra địa chỉ IP của gói tin xem có nằm trong VLAN 10 (VLAN của máy chủ A). Nếu không, gói tin chuyển tiếp đến cổng mặc định trên Router (cổng Fa0/0).
* Máy chủ A gửi yêu cầu ARP đến Switch để tìm [địa chỉ MAC](https://thietbimanggiare.com/dia-chi-mac/) của giao diện Fa0/0 trên Router. Đợi Router trả lời, máy chủ A gửi khung đến Router dưới dạng tin nhắn [Unicast](https://thietbimanggiare.com/unicast-la-gi/).
* Máy chủ A kiểm tra xem địa chỉ IP đích có nằm trong VLAN của nó hay không; nếu không, lưu lượng sẽ được chuyển tiếp đến cổng mặc định của nó trên giao diện Fa0/0 trên bộ định tuyến.
* Khi Router nhận được Frame nó xác định địa chỉ IP và cổng tương ứng từ bảng định tuyến.
* Sau đó, Router gửi yêu cầu [ARP](https://thietbimanggiare.com/address-resolution-protocol-arp/) đến giao diện được kết nối với VLAN đích (VLAN 20), tương ứng Fa0/1 trên Router.
* Switch nhận được yêu cầu ARP nó chuyển tiếp đến các cổng và ghi nhận địa chỉ máy chủ B bằng địa chỉ MAC của nó.
* Sau đó, Router nhận được thông tin về máy chủ B và chuyển tiếp gói tin đến máy chủ B trên VLAN 20 dưới dạng tin nhắn Unicast qua bộ chuyển mạch.

+ Cấu hình:

- Switch:

A screenshot of a computer program

Description automatically generated

- Router:

A screenshot of a computer code

Description automatically generated

3. Định tuyến VLAN theo Router on stick:

+  router được kết nối với switch thông qua một cổng và cổng này được cấu hình để hoạt động như một [**cổng trunk**](https://thietbimanggiare.com/cong-trunk/), có khả năng truyền thông tin của nhiều VLAN qua cùng một kết nối.

+ Phần mềm Router sẽ cho phép cấu hình nhiều cổng ảo trên cùng một cổng vật lý, mỗi cổng phụ ảo được kết nối để liên kết với một VLAN trên Switch và được cấu hình địa chỉ IP riêng. Bảng [giao thức](https://thietbimanggiare.com/protocol-giao-thuc-la-gi/) 802.1Q, lưu lượng qua cổng Trunk trên Router sẽ được gắn thẻ TAG để cho phép truyền lưu lượng từ nhiều VLAN trên cùng 1 cổng kết nối vật lý.

+ Ví dụ:

A diagram of a network connection

Description automatically generated

Theo cách Router-on-a-stick, ta sẽ cấu hình một đường Trunk giữa Router và Switch, trên Router ta sẽ tiến hành cấu hình 2 giao diện phụ ảo tương ứng với VLAN 10 và 20 để định tuyến giữ liệu. Theo đó, nếu Máy chủ A gửi tin tới máy chủ B thì quá trình sẽ diễn ra như sau:

* Máy chủ A gửi tin nhắn dưới dạng Unicast tới Switch.
* Switch gắn thẻ TAG VLAN 10 và truyền tiếp theo đường Trunk tới Router.
* Router nhận lưu lượng với thẻ TAG VLAN 10 và định tuyến đến VLAN 20 bằng giao diện con đã cấu hình tương ứng.
* Gói tin sẽ được gắn thẻ TAG VLAN 20 và gửi từ giao diện phụ tương ứng tới Switch.
* Switch nhận gói tin và loại bỏ thẻ TAG và tiếp tục chuyển đến máy chủ B qua cổng Fa0/3.

Cấu hình:

+ Switch:

A screenshot of a computer

Description automatically generated

+ Router

A screenshot of a computer code

Description automatically generated