Shape, square

Description automatically generated

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA ĐIỆN TỬ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_**🙠**🕮**🙢**\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Logo

Description automatically generated

**MẠNG MÁY TÍNH**

**TÌM HIỂU VÀ TRÌNH BÀY CHIA MẠNG CON VLSM. TÌM HIỂU ACL, VLAN VÀ CẤU HÌNH ỨNG DỤNG**

Giảng viên: T.S Bồ Quốc Bảo

Nhóm: 2

Thành viên: Nguyễn Văn Dũng

Trần Ngọc Chính

Lê Đức Sáng

Đào Duy Phương

Đồng Văn Ngữ

*Hà Nội, 12/2021*

MỤC LỤC

[CHƯƠNG I: CHIA MẠNG CON VLSM 4](#_Toc91182494)

[CHƯƠNG 2: Danh sách kiểm soát tru nhập ACL 5](#_Toc91182495)

[2.1. Khái niệm 5](#_Toc91182496)

[2.2. Phân loại 6](#_Toc91182497)

[2.3. Cách thức hoạt động của Access Control List (ACL) 6](#_Toc91182498)

[2.4. Câu lệnh cấu hình Access Control list (ACL) 7](#_Toc91182499)

[2.4.1. Các thuật ngữ cơ bản 7](#_Toc91182500)

[2.4.2. Cấu hình của standard ACL 8](#_Toc91182501)

[2.4.3. Cấu hình của Extended ACL 9](#_Toc91182502)

[CHƯƠNG 3: VLAN ? 10](#_Toc91182503)

[3.1. VLAN là gì ? 10](#_Toc91182504)

[3.2. Lịch sử của VLAN 11](#_Toc91182505)

[3.3. Giao thức VLAN 11](#_Toc91182506)

[3.4. Làm việc với VLAN 12](#_Toc91182507)

[3.4.1. Phân bổ 12](#_Toc91182508)

[3.4.2. Gửi thông tin đến mục tiêu 12](#_Toc91182509)

[3.4.3. Nguyên tắc cấu hình VLAN 13](#_Toc91182510)

[3.4.4. Nhận tin nhắn không xác định 13](#_Toc91182511)

[3.4.5. Cập nhật bảng 13](#_Toc91182512)

[3.4.6. STP (Giao thức cây kéo dài) 13](#_Toc91182513)

[3.5. Phân loại VLAN 14](#_Toc91182514)

[3.5.1. VLAN dựa trên giao thức 14](#_Toc91182515)

[3.5.2. VLAN tĩnh 14](#_Toc91182516)

[3.5.3. VLAN động 14](#_Toc91182517)

[3.6. Các chế độ VLAN 14](#_Toc91182518)

[3.6.1. Trunking mode 14](#_Toc91182519)

[3.6.2. Access mode 15](#_Toc91182520)

[3.7. Ưu điểm và nhược điểm của VLAN 15](#_Toc91182521)

[3.7.1. Ưu điểm của VLAN 15](#_Toc91182522)

[3.7.2. Nhược điểm 16](#_Toc91182523)

[3.8. VLAN cung cấp những gì? 16](#_Toc91182524)

[3.9. Ứng dụng của VLAN 16](#_Toc91182525)

# CHƯƠNG I: CHIA MẠNG CON VLSM

## 1.1. Bài toán chia mạng con VLSM (Variable length subnet masking)

Trường đại học công nghiệp Hà Nội được cấp 1 dải địa chỉ ip là 203.200.1.0 / 24. Trường có 3 cơ sở vói 3 yêu cầu về số lượng địa chỉ host khác nhau:

Cơ sở 1 cần 68 địa chỉ Ip

Cơ sở 2 cần 28 địa chỉ Ip

Cơ sở 3 cần 55 địa chỉ ip

Mỗi cơ sở đều được có nối 1 mạng với 1 cơ sở còn lại như hình

Chart

Description automatically generated

27 -2= 128-2 >= 68 => m =7

23 -2= 8-2 >= 3 => n = 3

Lớp C có 8bit host => ko đủ để chia

Nếu ta chia mạng con như bình sẽ đáp ứng được yêu cầu như có chỗ sẽ dư thừa hoặc thiếu địa chỉ nên không thể chia được.

* Ta cần chia theo VLSM

Ta cần chia thỏa mãn đk: Số lượng host của 1 subnet >= số lượng host yêu cầu của mỗi mạng

2m – 2 >= số lượng host cần

Ta nên chia subnet theo thứ tự yêu cầu số lượng giảm dần, bắt đầu là Cơ sở 1 với 68 host

2m – 2 >= 68 => m = 7

=> n = 8 – 7 = 1;

Bước nhảy 27 = 128;

=> 203.200.1.0 – 203.200.1.127 – subnet mask 255.255.255.128

Tiếp đến là Cơ sở 3 vói 55 host

2m – 2 >= 55 => m = 6

=> n = 8 – 6 = 2;

Bước nhảy 26 = 64;

=> 203.200.1.128 – 203.200.1.191 – subnet mask 255.255.255.192

Cuối cùng là cơ sở 2 với 28 host

2m – 2 >= 28 => m = 5

=> n = 8 – 5 = 3;

Bước nhảy 25 = 32;

=> 203.200.1.192 – 203.200.1.223 – subnet mask 255.255.255.224

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Subnet Address | Subnet mask | Dải địa chỉ | Broadcast Address |
| Cơ sở 1 | 203.200.1.0 | 255.255.255.128 | 203.200.1.1-203.200.1.126 | 203.200.1.127 |
| Cơ sở 3 | 203.200.1.128 | 255.255.255.192 | 203.200.1.129-203.200.1.190 | 203.200.1.191 |
| Cơ sở 2 | 203.200.1.192 | 255.255.255.224 | 203.200.1.193-203.200.1.222 | 203.200.1.223 |

# CHƯƠNG 2: DANH SÁCH KIỂM SOÁT TRU NHẬP ACL

* 1. Khái niệm
* Access control List (ACL) hay còn được gọi là kiểm soát truy cập. Là một danh sách các điều kiện được áp đặt vào các cổng của router để lọc các gói tin đi qua nó.Danh sách này chỉ ra cho router biết loại dữ liệu nào được cho phép (allow) và loại dữ liệu nào bị hủy bỏ (deny) . Sự cho phép và hủy bỏ này có thể được kiểm tra dựa vào địa chỉ nguồn, địa chỉ đích, giao thức hoặc chỉ số cổng.
* Thông qua sự bảo mật cho các thiết bị ở tầng 3 (layer 3) mà nó kiểm soát khả năng kết nối từ thiết bị định tuyến đến các thiết bị khác.
  1. Phân loại

\*Standard Acl:

- Dải số cho standard ACL từ 1 – 99.

- Có thể chặn được NetWork, Host và subnet.

- Chặn toàn bộ các dịch vụ.

- Thực hiện tại điểm gần nhất với đích.

- Có chế lọc được thực hiện dựa trên địa chỉ IP nguồn .

\*Extended ACL:

- Dải số cho Extended ACL từ 100 – 999.

- Có thể đồng ý hoặc chặn bất cứ một Network, Host, subnet, hoặc cả dịch vụ.

- Được lựa chọn các dịch vụ muốn chặn.

- Cơ chế được dựa trên địa chỉ IP nguồn, IP đích, giao thưc(protocol), cổng.

* 1. Cách thức hoạt động của Access Control List (ACL)

- Access Control List (ACL) sẽ thực hiện việc kiểm tra theo trình tự của các điều khiển trong danh sách cấu hình. Nếu có một điều kiện được so khớp trong danh sách thì nó sẽ thực hiện hành động tương ứng trong điều kiện đó, và các điều kiện còn lại sẽ không được kiểm tra nữa. Trường hợp tất cả các điều kiện trong danh sách đều không khớp thì một câu lệnh mặc định “deny any’ được thực hiện, nó có nghĩa là điều kiện cuối cùng ngầm định trong một ACL mặc định sẽ là cấm tất cả, Vì vậy, trong cấu hình ACL cần phải có ít nhất một câu lệnh có hành động là “permit’.

- Khi có gói tin vào một cổng, router sẽ kiểm tra xem có ACL nào được đặt trên cổng đó hay không để kiểm tra, nếu có thì các gói tin sẽ được kiểm tra với những phải có điều kiện trong danh sách. Nếu gói tin đó được cho phép bỏi ACL, nó sẽ tiếp tục được kiểmt tra trong bảng định tuyên để quyết định chọn cổng ra để đi đến đích.

- Tiếp đó, router sẽ kiểm tra xem trên cổng dữ liệu chuyển ra có đặt ACL hay không. Nếu không thì gói tin đó có thể sẽ được gửi tới mạng đích. Nếu có ACL thì nó sẽ kiểm tra với những điều kiện trong danh sách ACL đó.

- Danh sách điều khiển truy cập (ACL – Access Control List) cho phép khai báo những địa chỉ nào được chuyển đổi. Bạn nên nhớ là kết thúc một ACL luôn có câu lệnh ẩn cấm tuyệt đói để tránh những kết quả không dự tính được khi một ACL có quá nhiều điều kiện cho phép.

- lưu ý: Không nên dùng điều kiện cho phép tất cả “ permit any” trong ACL sử dụng cho NAT vì câu lệnh này làm hao tốn quá nhiều tài nguyên của Router và do đó có thể gây ra các sự cố mạng.

* 1. Câu lệnh cấu hình Access Control list (ACL)
     1. Các thuật ngữ cơ bản

\*Để hiểu cách cấu hình cho ACL, Cần phải hiểu một số thuật ngữ sau:

- “Wildcard mask” có 32 bit (0 và 1), chia thành 4 phần, mỗi phần có 8 bit, là tham số được dùng để xác định các bit nào sẽ được bỏ qua hay buộc phải so trùng trong việc kiểm tra điều kiện.Bit “1” có nghĩa là bỏ qua vị trí bit đó khi so sánh và bit “0” xác định vị trí đó phải giống nhau. Mặc dù cấu trúc giống subnet mask nhung chúng hoạt động khác nhau (xem lại phần địa chỉ IP).

- Với standard ACL, nếu không thêm” wildcard- mask” trong câu lệnh ACL thì mặc định sẽ là 0.0.0.0.

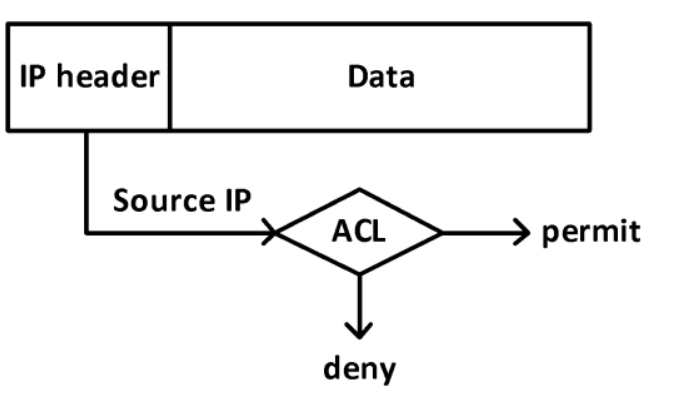
- “wildcard mask” dùng cho một thiết bị hay còn gọi là “wildcard-host” có dạng: 0.0.0.0 (kiểm tra tất cả các bit). Khi kiểm tra ACL, nó sẽ kiểm tra tất cả các bit trong địa chỉ dùng để so khớp. Từ khóa “host” được thay thê cho thuật ngữ này.

- wildcard mask cho tất cả các thiết bị được gọi là wildcard ”card” có dạng: 255.2555.255.255 (không kiểm tra tất cả các bit ). Từ khóa “any” được thay thế cho thuật ngữ.

- Lưu ý: khi áp dụng Access Control List (ACL) trên một cổng, phải xác định ACL đó được dùng cho luồng dữ liệu vào (inbound) hay ra ( outbound). Chiều của luồng dữ liệu được xác định trên cổng của Router.

* + 1. Cấu hình của standard ACL

- “Standard CL” kiểm tra điều kiện dựa vào địa chỉ nguồn trong các gói tin và thực hiện hành động cấm hoặc cho phép tất cả các lưu lượng từ một thiết bị hay một mạng xác định nào đó.



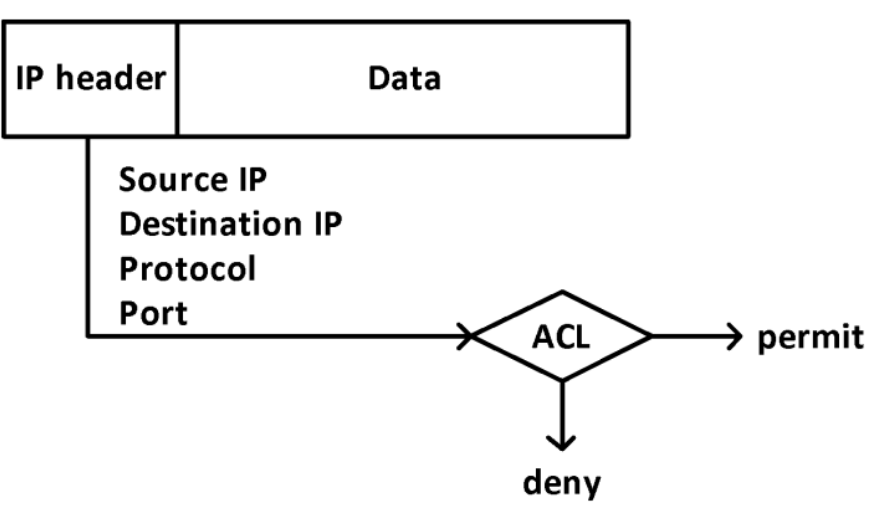
Router(config)# access-list <ACL-number> {permit|deny} source [wildcast-mask]

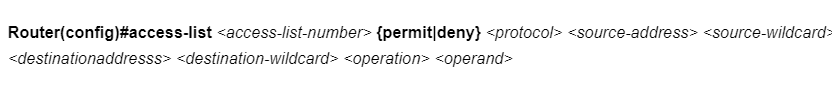
* Để gán ACL vào một cổng và đặt chế độ kiểm tra cho luồng dữ liệu đi vào hay đi ra khỏi cổng của router, ta sử dụng câu lệnh sau:

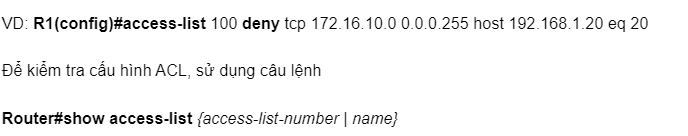


* + 1. Cấu hình của Extended ACL

- “Extended ACL” cung cấp sự điều khiển linh hoạt hơn “standard ACL”. Nó kiểm tra địa chỉ nguồn, địa chỉ đích, giao thức(protocol), chỉ số cổng ứng dụng. “Extended ACL” thực hiện hành động cấm hay cho phép ở một số ứng dụng xác định.







\*\*Tóm Lại:

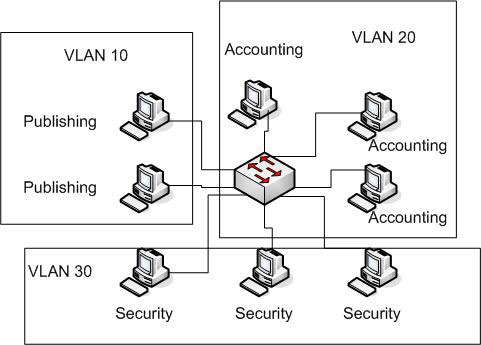
* Access Control List (ACL) có thể xem như là mọt tưởng lửa nhỏ định ra một tập luật để chặn các truy cập bất hợp pháp được cấu hình trên các router.
* ACL được chia làm hai loại:

+> standard ACL

+> Extended ACL

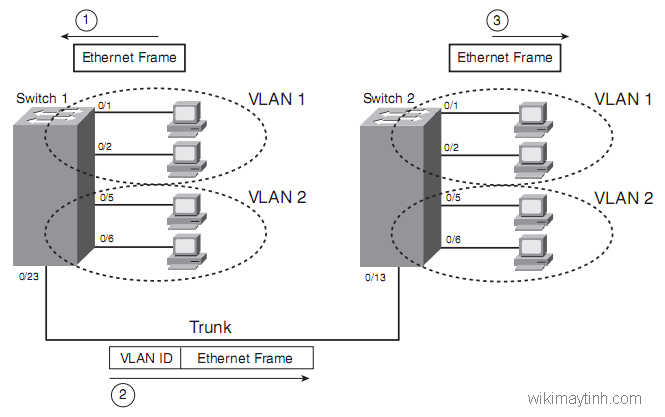
* Trong đó, Standard ACL thường được đặt ở gần đích, còn Extended ACL thường đặt ở gần nguồn cần cấm luồng dữ liệu.

# CHƯƠNG 3: VLAN ?

* 1. VLAN là gì ?
* VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Một VLAN được định nghĩa là một nhóm logic các thiết bị mạng và được thiết lập dựa trên các yếu tố như chức năng, bộ phận, ứng dụng… của công ty. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Bình thường thì router đóng vai trò tạo ra miền quảng bá. Đối với VLAN, switch có thể tạo ra miền quảng bá.

Ảnh minh họa

* Việc này được thực hiện khi bạn - quản trị viên - đặt một số cổng switch trong VLAN ngoại trừ VLAN 1 - VLAN mặc định. Tất cả các cổng trong một mạng VLAN đơn đều thuộc một miền quảng bá duy nhất.
* Vì các switch có thể giao tiếp với nhau nên một số cổng trên switch A có thể nằm trong VLAN 10 và một số cổng trên switch B cũng có thể trong VLAN 10. Các bản tin quảng bá giữa những máy tính này sẽ không bị lộ trên các cổng thuộc bất kỳ VLAN nào ngoại trừ VLAN 10. Tuy nhiên, tất cả các máy tính này đều có thể giao tiếp với nhau vì chúng thuộc cùng một VLAN. Nếu không được cấu hình bổ sung, chúng sẽ không thể giao tiếp với các máy tính khác nằm ngoài VLAN này.
  1. Lịch sử của VLAN
* Với mạng LAN thông thường, các máy tính trong cùng một địa điểm (cùng phòng...) có thể được kết nối với nhau thành một mạng LAN, chỉ sử dụng một thiết bị tập trung như hub hoặc switch. Có nhiều mạng LAN khác nhau cần rất nhiều bộ [hub](https://vi.wikipedia.org/w/index.php?title=Hub&action=edit&redlink=1), [switch](https://vi.wikipedia.org/wiki/Switch). Tuy nhiên thực tế số lượng máy tính trong một LAN thường không nhiều, ngoài ra nhiều máy tính cùng một địa điểm (cùng phòng) có thể thuộc nhiều LAN khác nhau vì vậy càng tốn nhiều bộ hub, switch khác nhau. Do đó vừa tốn tài nguyên số lượng hub, switch và lãng phí số lượng port [Ethernet](https://vi.wikipedia.org/wiki/Ethernet).
* Với nhu cầu tiết kiệm tài nguyên, đồng thời đáp ứng nhu cầu sử dụng nhiều LAN trong cùng một địa điểm, giải pháp đưa ra là nhóm các máy tính thuộc các LAN khác nhau vào cùng một bộ tập trung switch. Giải pháp này gọi là mạng LAN ảo hay VLAN.
  1. Giao thức VLAN
* Vì lưu lượng truy cập từ nhiều VLAN có thể đi qua cùng một mạng vật lý, nên dữ liệu phải được ánh xạ tới một mạng cụ thể. Điều này được thực hiện bằng giao thức VLAN (VLAN Protocols), chẳng hạn như IEEE 802.1Q, ISL của Cisco hoặc VLT của 3Com. Hầu hết các VLAN hiện đại sử dụng giao thức IEEE 802.1Q, giao thức này chèn thêm một header hoặc “tag” vào mỗi khung Ethernet. Thẻ này xác định VLAN mà thiết bị gửi thuộc về, ngăn không cho dữ liệu được định tuyến đến các hệ thống bên ngoài mạng ảo. Dữ liệu được gửi giữa các thiết bị chuyển mạch bằng cách sử dụng một liên kết vật lý được gọi là “trung kế” kết nối các thiết bị chuyển mạch với nhau. Trunking phải được bật để một công tắc chuyển thông tin VLAN sang một công tắc khác.



Trunking trong VLAN

4,904 VLAN có thể được tạo trong mạng Ethernet bằng giao thức 802.1Q, nhưng trong hầu hết các cấu hình mạng chỉ cần một số VLAN. Các thiết bị không dây có thể được bao gồm trong một VLAN, nhưng chúng phải được định tuyến thông qua bộ định tuyến không dây được kết nối với mạng LAN.

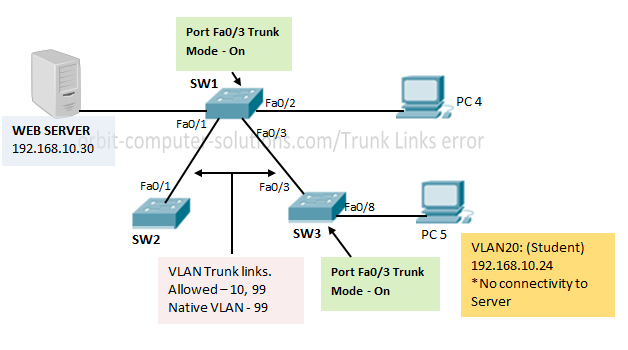
* 1. Làm việc với VLAN
     1. Phân bổ
* VLAN có thể được cấp phát bằng cách sử dụng một hoặc nhiều cổng ( giao diện ) và được nhóm thành các lớp logic tùy thuộc vào kết nối hoặc kiểu điều khiển và sự tương tác của chúng với chính chúng. Cùng một ID VLAN được sử dụng để quản lý các cổng kết nối với thiết bị chuyển mạch cho tất cả các máy chủ sử dụng liên kết dữ liệu do VLAN cung cấp. Trong tiêu đề Ethernet, các thẻ VLAN (Tag) là một trường 12 bit. IEEE chuẩn hóa VLAN là 802.1Q. Nó còn được gọi là Dot1Q.
  + 1. Gửi thông tin đến mục tiêu
* Khi máy chủ kết nối nhận được một khung không an toàn bằng cách sử dụng định dạng 802.1Q được đính kèm với tiêu đề khung liên kết dữ liệu, thẻ VLAN ID được cài đặt trên một cổng giao tiếp. Khung 802.1Q sau đó được gửi đến đích. Một VLAN được cấu hình sao cho nó phải giữ lưu lượng riêng biệt với các VLAN khác; mỗi công tắc sử dụng tên và chỉ truyền điều này. Kết nối đường trục giữa các thiết bị chuyển mạch vận hành nhiều VLAN, được phân chia bằng cách sử dụng thẻ hoặc tên. Khi khung chạm vào công tắc đích, thẻ VLAN sẽ bị loại bỏ trước khi khung được gửi đến máy tính đích.
  + 1. Nguyên tắc cấu hình VLAN
* Cấu hình trung kế của mỗi khung VLAN được gửi qua cổng (đã đề cập ở trên) có thể cấu hình nhiều VLAN trên một cổng duy nhất. Để gửi và chấp nhận các khung được gắn thẻ, bạn cần có giao diện hệ thống lân cận trên máy chủ, hệ thống hoặc bộ chuyển mạch khác chấp nhận gắn thẻ 802.1Q. Mọi khung Ethernet không được lên lịch đều được cấp phát cho một VLAN mặc định trong quá trình thiết lập bộ chuyển mạch.
  + 1. Nhận tin nhắn không xác định
* Khi một khung Ethernet không được gắn thẻ từ một máy chủ kết nối đến công tắc VLAN, thẻ VLAN được phân bổ cho giao diện đầu vào sẽ được áp dụng. Khung được gắn với địa chỉ MAC và được gửi đến cổng máy chủ. Broadcast unicast và multicast không xác định được gửi đến tất cả các cổng VLAN. Nếu một máy chủ không xác định giải quyết một hệ thống unicast ẩn danh, các nút chuyển sẽ tìm hiểu vị trí máy chủ. Sau đó, họ không gửi khung đến máy chủ đó.
  + 1. Cập nhật bảng
* Hai hệ thống sau giữ bảng truyền tải được cập nhật.
* Sau khoảng thời gian chờ có thể định cấu hình, các mục truyền tải cũ thường xuyên bị xóa khỏi bảng truyền.
* Bất kỳ thay đổi nào trong cấu trúc liên kết sẽ làm giảm bộ đếm thời gian làm mới của bảng chuyển tiếp, điều này gây ra việc làm mới.
  + 1. STP (Giao thức cây kéo dài)
* Nó được sử dụng để thiết lập cấu trúc liên kết không có vòng lặp trong mỗi miền của lớp 2 giữa các thiết bị chuyển mạch. Per-VLAN STP có thể được sử dụng để giảm thiểu tổng STP nếu cấu trúc liên kết giống nhau giữa các cấu trúc liên kết lớp 2 khác nhau hoặc MISTP (STP đa trường hợp). STP chặn các kết nối có thể kích hoạt vòng lặp truyền và tạo cây bao trùm từ công tắc đã chọn sang gốc. Khối này không cho phép STP là một phần của tuyến chuyển tiếp đang hoạt động cho đến khi xảy ra sự cố trong một phần khác của mạng.
  1. Phân loại VLAN

Có ba loại VLAN cơ bản:

* + 1. VLAN dựa trên giao thức
* Một VLAN dựa trên giao thức xử lý lưu lượng giao thức. VLAN dựa trên giao thức có thể chỉ định các tham số lọc gói không được gắn thẻ. Các gói không được gắn thẻ được gán cho VLAN 1 bằng công tắc thông minh nếu thiết lập cổng không được thay đổi hoặc định cấu hình như một VLAN dựa trên giao thức. Bằng cách chỉ định VLAN dựa trên cổng, VLAN dựa trên giao thức hoặc cả hai, bạn có thể ghi đè hành vi mặc định này. Tuân theo tiêu chuẩn 802.1q, công tắc thông minh chỉ xử lý các gói được gắn thẻ và không chuyển tiếp chúng vào các VLAN dựa trên giao thức.
  + 1. VLAN tĩnh
* VLAN tĩnh là một tập hợp các cổng được xác định là một phần của cùng một miền quảng bá bởi một bộ chuyển mạch. Nói cách khác, tất cả các cổng có lưu lượng truy cập cho một địa chỉ mạng con nhất định thuộc cùng một VLAN. Với một VLAN, có thể nhóm người dùng theo một phương pháp logic thay vì theo vị trí, giúp xử lý việc tiêu thụ băng thông và sắp xếp người dùng theo nhu cầu của họ.
  + 1. VLAN động
* Một bộ chuyển mạch chỉ định một VLAN cho một cổng sử dụng dữ liệu từ hệ thống người dùng hoặc các thiết bị như địa chỉ IP và địa chỉ MAC tự động trong một VLAN động. Khi máy tính được kết nối với ổ cắm công tắc, công tắc yêu cầu thiết lập tư cách thành viên VLAN cho cơ sở dữ liệu. Các VLAN động cung cấp khả năng kích hoạt ngay lập tức các thiết bị đầu cuối. Các VLAN động có thể cấu hình động thành viên VLAN nếu hệ thống được chuyển từ cổng này sang cổng khác trên bộ chuyển mạch khác.
  1. Các chế độ VLAN

Các cổng (port) của switch có thể hoạt động ở 2 chế độ: Chế độ trung kế (trunking mode) và chế độ truy nhập (access mode).

* + 1. Trunking mode
* Trunking mode cho phép tập hợp lưu lượng từ nhiều VLAN qua cùng một cổng vật lý đơn như hình vẽ:



* Các kết nối trung kế thường được sử dụng kết nối giữa các switch với nhau, như hình vẽ:
  + 1. Access mode
* Giao diện này thuộc về một và chỉ một VLAN. Thông thường một cổng của switch gắn tới một thiết bị của người dùng đầu cuối hoặc một server.
  1. Ưu điểm và nhược điểm của VLAN
     1. Ưu điểm của VLAN
* Tiết kiệm băng thông của hệ thống mạng: VLAN chia mạng LAN thành nhiều đoạn (segment) nhỏ, mỗi đoạn đó là một vùng quảng bá (broadcast domain). Khi có gói tin quảng bá (broadcast), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng.
* Tăng khả năng bảo mật: Do các thiết bị ở các VLAN khác nhau không thể truy nhập vào nhau (trừ khi ta sử dụng router nối giữa các VLAN). Như trong ví dụ trên, các máy tính trong VLAN kế toán (Accounting) chỉ có thể liên lạc được với nhau. Máy ở VLAN kế toán không thể kết nối được với máy tính ở VLAN kỹ sư (Engineering).
* Dễ dàng thêm hay bớt máy tính vào VLAN: Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn.
* Giúp mạng có tính linh động cao: VLAN có thể dễ dàng di chuyển các thiết bị. Giả sử trong ví dụ trên, sau một thời gian sử dụng công ty quyết định để mỗi bộ phận ở một tầng riêng biệt. Với VLAN, ta chỉ cần cấu hình lại các cổng switch rồi đặt chúng vào các VLAN theo yêu cầu. VLAN có thể được cấu hình tĩnh hay động. Trong cấu hình tĩnh, người quản trị mạng phải cấu hình cho từng cổng của mỗi switch. Sau đó, gán cho nó vào một VLAN nào đó. Trong cấu hình động mỗi cổng của switch có thể tự cấu hình VLAN cho mình dựa vào địa chỉ MAC của thiết bị được kết nối vào.
  + 1. Nhược điểm
* Một gói tin có thể bị rò rỉ từ VLAN này sang VLAN khác.
* Cần có một bộ định tuyến mạnh để kiểm soát khối lượng công việc trong các mạng lớn.
* Một VLAN không thể chuyển tiếp lưu lượng mạng tới các VLAN khác.
  1. VLAN cung cấp những gì?
* VLAN giúp tăng hiệu suất mạng LAN cỡ trung bình và lớn vì nó hạn chế bản tin quảng bá. Khi số lượng máy tính và lưu lượng truyền tải tăng cao, số lượng gói tin quảng bá cũng gia tăng. Bằng cách sử dụng VLAN, bạn sẽ hạn chế được bản tin quảng bá.
* VLAN cũng tăng cường tính bảo mật bởi vì thực chất bạn đặt một nhóm máy tính trong một VLAN vào mạng riêng của chúng.
  1. Ứng dụng của VLAN
* Sử dụng VLAN để tạo các mạng LAN khác nhau của nhiều máy tính cùng văn phòng:
* Sử dụng VLAN để tạo mạng dữ liệu ảo (Virtual Data Network - VAN):