Công ty An ninh mạng Viettel

Báo cáo về Switching

Sinh viên: Nguyễn Đan Trường

*MỤC LỤC*

[Chương 1. Basic Networking 4](#_Toc154412363)

[1. Mô hình OSI và TCP/IP 4](#_Toc154412364)

[2. Encapsulation 7](#_Toc154412365)

[3. Application Layer Service and Protocol 9](#_Toc154412366)

[a. DNS 9](#_Toc154412367)

[b. FTP 10](#_Toc154412368)

[c. Mail 10](#_Toc154412369)

[d. HTTP 10](#_Toc154412370)

[e. TELNET 10](#_Toc154412371)

[f. SSH 11](#_Toc154412372)

[4. Client – Server Model 11](#_Toc154412373)

[5. Connection-oriented và connectionless 12](#_Toc154412374)

[a. Giao thức hướng kết nối (connection-oriented) 12](#_Toc154412375)

[b. Giao thức không hướng kết nối (Connectionless) 14](#_Toc154412376)

[Chương 2. Basic Switching 16](#_Toc154412377)

[1. Công nghệ Ethernet 16](#_Toc154412378)

[2. Ethernet frame 17](#_Toc154412379)

[3. CSMA/CD 18](#_Toc154412380)

[4. Collision domain và broadcast domain 19](#_Toc154412381)

[5. Simplex và Duplex 21](#_Toc154412382)

[6. Switch 22](#_Toc154412383)

[7. STP – Spanning tree protocol 23](#_Toc154412384)

[8. VLAN 25](#_Toc154412385)

[9. VTP – Virtual Trunking Protocol 28](#_Toc154412386)

[10. Inter-Vlan 31](#_Toc154412387)

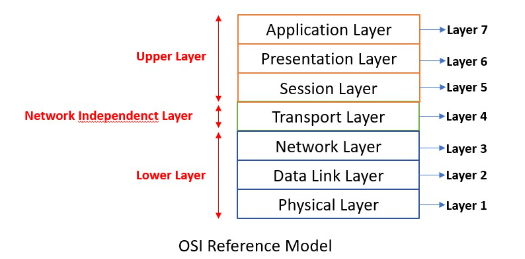
# Basic Networking

## Mô hình OSI và TCP/IP

OSI và TCP/IP là hai mô hình tham chiếu được sử dụng để mô tả cách một hệ thống mạng hoạt động. Để dữ liệu có thể được trao đổi giữa hai hay nhiều người dùng trong mạng máy tính, chúng ta cần một phương pháp có tính hệ thống. Phương pháp này cho phép dữ liệu được trao đổi một cách hiệu quả và được sắp đặt sẵn. Những mô hình mạng này chịu trách nhiệm cung cấp những quy tác, giao thức để vận chuyển dữ liệu giữa người nhận và người gửi.

**Mô hình OSI**

Mô hình OSI hay Open Systems Interconnection có nhiệm vụ thiết lập kết nối giữa các thiết bị giao tiếp trên toàn cầu. OSI được coi là mã nguồn mở vì khả năng phù hợp với mọi hệ thống mạng của nó. Mô hình cung cấp một tiêu chuẩn dưới dạng kiến trúc phân tầng cho phép các hệ thống khác nhau có thể giao tiếp được với nhau, trong đó gồm có 7 tầng với những cấu trúc và chức năng riêng đã được định nghĩa sẵn.



Mỗi tầng có một chức năng riêng và chỉ giao tiếp với tầng tiếp giáp nó:

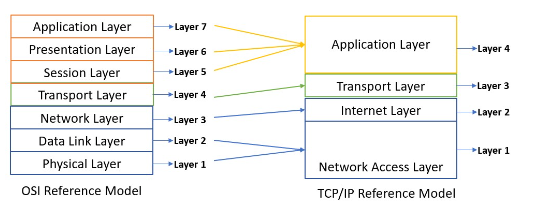
* **Tầng ứng dụng (Application Layer)**: là tâng tương tác trực tiếp với tiến trình ứng dụng, có trách nhiệp cung cấp giao diện cũng như các thao tác dữ liệu giúp người dùng và phần mềm ứng dụng tương tác với nhau. Một số giao thức tầng ứng dụng như: HTTP, FTP, DHCP, DNS ….
* **Tầng trình diễn (Presentation Layer)**: là tầng ngay dưới tầng ứng dụng, nó đáp ứng các nhu cầu của tầng ứng dụng như phiên dịch, mã hóa, giải mã, nén dữ liệu. Phiên dịch dữ liệu theo cú pháp mà ứng dụng có thể hiểu, mã hóa dữ liệu gửi đi cũng như giải mã dữ liệu nhận, nén dữ liệu trước khi truyền xuống tầng phiên.
* **Tầng phiên (Session Layer)**: là tầng ngay dưới tầng trình diễn, cung cấp các nhu cầu dịch vụ cho tầng trình diễn. Tầng phiên chịu trách nhiệm đóng và mở luồng giao tiếp giữa hai thiết bị, thời gian giữa mở và đóng được gọi là phiên, nó đảm bảo phiên mở đủ lâu để dữ liệu có thể gửi đi và đóng đủ nhanh để tránh lãng phí tài nguyên.
* **Tầng giao vận (Transport Layer):** là tầng ngay dưới tầng phiên, nó đáp ứng các nhu cầu của tầng phiên. Tầng giao vận chịu trách nhiệm thiết lập kết nối giữa hai thiết bị, nó nhận dữ liệu từ tầng phiên rồi xử lý để gửi xuống tầng dưới cũng như nhận dữ liệu từ tầng dưới xử lý để chuyển lên tầng phiên.

Tầng giao vận có thể cung cấp dịch vụ kiểm soát luồng và kiểm soát lỗi để đảm bảo dữ liệu được chuyển đi được chính xác và không quá tải bên nhận.

* **Tầng mạng (Network Layer):** đáp ứng các nhu cầu của tầng giao vận, chịu trách nhiệm giúp dữ liệu có thể truyền giữa các thiết bị ở các mạng khác nhau, nếu 2 thiết bị cùng trong một mạng thì ta không cần thiết phải có tầng này. Tầng mạng còn cung cấp các thuật toán dò đường cho các bộ định tuyến để xác định đường truyền vật lý tốt nhất cho dữ liệu.
* **Tầng liên kết dữ liệu (Data Link Layer):** đáp ứng các nhu cầu của tầng mạng, về cơ bản tầng này giống với tầng mạng nhưng nó hỗ trợ dữ liệu có thể được tuyền đi giữa các thiết bị trong cùng một mạng.
* **Tầng vật lý (Physical Layer):** bao gồm các thiết bị phần cứng giúp truyển tải dữ liệu như cáp, bộ định tuyến, …Ở tầng này dữ kiệu được truyền tải dưới dạng bit 0 và 1.

**Mô hình TCP/IP**

Giống với OSI, mô hình TCP/IP cũng có kiến trúc phân tầng cho phép dữ liệu được truyền tải thông qua các giao thức được tích hợp sẵn. TCP/IP chỉ có 4 tầng so với 7 tầng của OSI, thực chất 4 tầng đó là sự kết hợp của các tầng trong mô hình OSI nhưng chức năng cũng như tính chất của các tầng trong TCP/IP có sự thay đổi so với OSI.



Trong mô hình TCP/IP mỗi tầng được phân một chức năng riêng và có thể giao tiếp với các tầng kề bên nó, việc thay đổi vị trí các tầng cũng không được chấp nhận trong mô hình này.

* **Tầng ứng dụng(Application)**: có nhiệm vụ tương tác trực tiếp với tiến trình ứng dụng, cung cấp giao diện giữa người dùng và ứng dụng. Vì không có tầng nào giữa tầng ứng dụng và tầng giao vận như mô hình OSI nên đôi khi tầng ứng dụng của TCP/IP bao gồm các chức năng của tầng phiên, tầng trình diễn bên mô hình OSI.
* **Tầng giao vận(Transport)**: đáp ứng nhu cầu của tầng ứng dụng, cung cấp các giao thức giúp dữ liệu được vận chuyển từ tiến trình ứng dụng ở hệ thống nguồn đến tiến trình ứng dụng ở hệ thống đích. Ngoài ra, còn cung cấp các dịch vụ kiểm soát luồng, kiểm tra lỗi gói tin, gửi xác nhận khi vận chuyển thành công. Một vài giao thức thông dụng nhất hiện nay trong tầng giao vận là TCP và UDP.
* **Tầng mạng(Internet)**: đáp ứng nhu cầu của tầng giao vận, có nhiệm vụ dẫn đường cho dữ liệu có thể được vận chuyển từ điểm đầu đến điểm đích an toàn, nó tìm kiếm đường truyền dữ liệu tốt nhất thông qua các giao thức cũng như các thuật toán dò đường được tích hợp trên các bộ định tuyến (Routing). Một vài giao thức có trong tầng mạng: IP, ICMP,
* **Tầng liên kết** (**Network Access Layer**): đáp ứng nhu cầu của tầng mạng, nó đóng vai trò như tầng liên kết dữ liệu và tầng vật lý của mô hình OSI. Tầng liên kết nhận dữ liệu dưới dạng bit sau đó đưa dữ liệu vào trong 1 gói dữ liệu rồi gửi lên mạng lưới máy tính để truyền đến điểm đích.

**So sáng mô hình OSI và TCP/IP**

**Giống nhau**

* Cả 2 mô hình đều chia thành nhiều layer giúp hiểu rõ hơn và quản lý dễ dàng hơn
* Cả 2 mô hình đều có lớp Network và lớp Transport. Lớp Network chịu trách nhiệm định tuyến dữ liệu qua mạng còn lớp Transport chịu trách nhiệm đảm bảo tính toàn vẹn và thứ tự của dữ liệu

**Khác nhau**

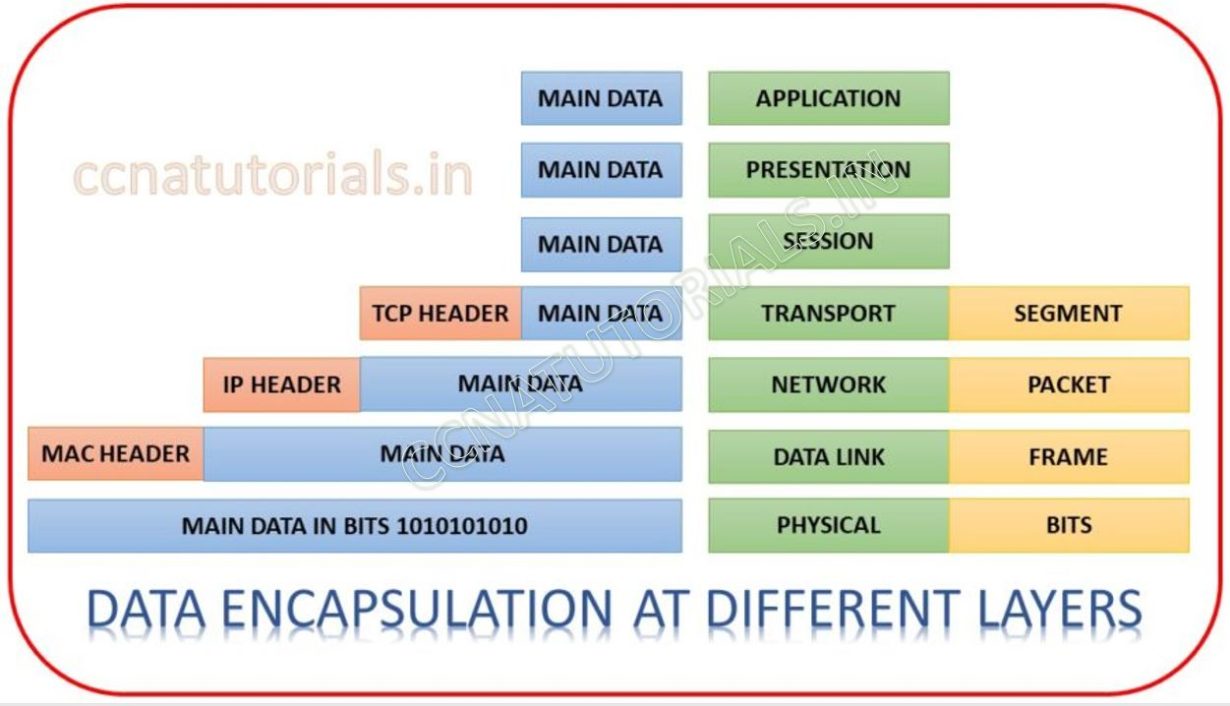
* Số lượng tầng: OSI có 7 tầng, TCP/IP có 4 tầng
* Mô hình OSI mang tính chất học tập nghiên cứu, còn mô hình TCP/IP mạng tính thực tế được sử dụng nhiều hơn.

## Encapsulation

Tất cả các giao dịch mạng đều bắt đầu tại lớp ứng dụng, nó sẽ khởi tạo một yêu cầu dịch vụ đến một máy tính khác và yêu cầu này không thể truyền trực tiếp trên đường mạng mà nó cẩn được xử lý từ lớp 7 xuống lớp 1 rồi mới được truyền đi.

Quá trình này được gọi là đóng gói dữ liệu (encapsulation) – là việc dùng các thông tin về giao thức để bao quanh dữ liệu sao cho mỗi lần dữ liệu đến từng layer thì mỗi layer sẽ hiểu và xử lý thông tin tốt nhất.

Để truyền tải và trao đổi dữ liệu thì mỗi layer sẽ sử dụng Protocal Data Unit. Mỗi khi data xuống một layer nào đó sẽ được thêm thông tin cảu layer đó và layer tương ứng ở phía host nhận dữ liệu sẽ được được thông tin này. Sau khi đọc xong thì thông tin đó sẽ được gỡ bỏ để đưa lên layer trên.



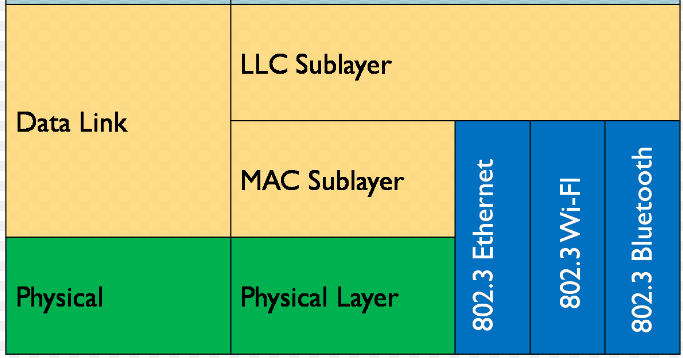
Trong hình ta thấy được đơn vị dữ liệu cho từng layer là:

* Transport: Segments
* Network: Packets
* Data link: Frames
* Physical: Bits

Các segments sẽ đc đưa xuống Network layer để thêm vào IP header, mục đích của Network layers là đánh địa chỉ mạng và chỉ đường đi cho gói tin trên mạng. Địa chỉ mạng(ví dụ IP) có mục đích là đưa Segments đến đúng nơi nhận/ Segments sau khi đc thêm IP header của Network layer thì đc gọi là Packets hay datagram.

Khi packet xuống đến Datalink layer thì sẽ đc đóng gói thành các frame. Frame header mang theo thông tin về địa chỉ vật lý của host nguồn và host đích.

Ở trên ta thấy các packet đc đóng gói thành các frame sẽ đc đưa thêm vào 2 thông tin là LLC header và MAC header. Tại sao trong Datalink layer lại có tới 2 thông tin đc thêm vào?



Điều đó là do trong Datalink layer có 2 sublayer(layer con) là Logical Link Control(LLC) và Media Access Control(MAC)

* Lớp LLC liên kết với Network layer để xác định loại địa chỉ logic đang dùng là gì và sẽ đóng gói frame theo kiểu tương ứng.
* Lớp MAC lại kết hợp với lớp cuối cùng là Physical l để biết môi trường truyền dẫn bên dưới là gì để có cách thức sử dụng phù hợp.

Để đưa các frame này lên mạng thì các thông tin phải đc chuyển sang dạng tín hiệu digital. Physical layer có trách nhiệm sẽ mã hóa các thông tin thành các chuỗi bit 0 1 để các thiết bị có thể đọc được.

**De-encapsulation**

Sau khi nhận đc các bit 0 1 thì bên nhận sẽ đồng bộ các tín hiệu digital và sau đó sẽ decode các tín hiệu digital. Bên gửi sẽ tiến hành việc xây dựng lại các frames từ các thông tin ở Physical layer đưa lên.

Khi các thiết bị bắt đầu việc xây dựng lại frames thì sẽ check các thông tin từ FCS(Frame Check Sequence) để xác định đúng thứ tự các frame và check, nếu sai bất kỳ một thông tin nào đó hoặc trong quá trình vận chuyển xảy ra lỗi thì sẽ bị loại bỏ. Các thông tin sau khi đc kiểm tra, nếu vẫn ổn thì sẽ đc đưa vào các frame.

Sau khi đã rebuild lại Frame thì frame sẽ đc đưa lên Network layer, ở đây frame header sẽ đc gỡ bỏ và thông tin đc kiểm tra đó là IP header. Thông tin về địa chỉ Logic(IP) sẽ đc kiểm tra ở đây, sau khi kiểm tra xong thì IP header sẽ đc gỡ bỏ để đưa lên layer tiếp theo phía trên.

….

Cứ như vậy quá trình de-encapsulation sẽ đc diễn ra thông qua các layers và sau đó sẽ đc biểu diễn thành các dữ liệu cho người dùng.

## Application Layer Service and Protocol

### DNS

**Mô hình hoạt động**

Dịch vụ DNS hoạt động theo mô hình client-server. Máy tính client sử dụng DNS để dịch tên miền thành địa chỉ IP. Để thực hiện điều này, máy tính client sẽ gửi yêu cầu đến máy chủ DNS. Máy chủ DNS sẽ trả về địa chỉ IP của máy chủ mà tên miền đó trỏ tới.

**Các thành phần cơ bản**

* Máy chủ DNS: Máy chủ DNS là máy tính chịu trách nhiệm lưu trữ thông tin về tên miền và địa chỉ IP.
* Tên miền: Tên miền là một chuỗi ký tự được sử dụng để xác định một máy tính hoặc một dịch vụ trên Internet.
* Địa chỉ IP: Địa chỉ IP là một dãy số được sử dụng để xác định vị trí của một máy tính trên mạng.

### FTP

Mô hình hoạt động

Dịch vụ FTP hoạt động theo mô hình client-server. Máy tính client sử dụng FTP để truyền tải tập tin giữa các máy tính trên mạng.

Các thành phần cơ bản

* Máy chủ FTP: Máy chủ FTP là máy tính cung cấp dịch vụ FTP.
* Máy tính client: Máy tính client là máy tính sử dụng dịch vụ FTP.
* Tập tin: Tập tin là một tập hợp dữ liệu được lưu trữ trên máy tính.

### Mail

**Mô hình hoạt động**

Dịch vụ MAIL hoạt động theo mô hình client-server. Máy tính client sử dụng MAIL để gửi và nhận email.

**Các thành phần cơ bản**

* Máy chủ MAIL: Máy chủ MAIL là máy tính cung cấp dịch vụ MAIL.
* Máy tính client: Máy tính client là máy tính sử dụng dịch vụ MAIL.
* Email: Email là một phương thức giao tiếp điện tử.

### HTTP

**Mô hình hoạt động**

Dịch vụ HTTP hoạt động theo mô hình client-server. Máy tính client sử dụng HTTP để truy cập các trang web.

**Các thành phần cơ bản**

* Máy chủ web: Máy chủ web là máy tính cung cấp các trang web.
* Máy tính client: Máy tính client là máy tính sử dụng các trang web.
* Trang web: Trang web là một tập hợp các trang web liên kết với nhau.

### TELNET

**Mô hình hoạt động**

Dịch vụ TELNET hoạt động theo mô hình client-server. Máy tính client sử dụng TELNET để kết nối với một máy tính khác và thực hiện các tác vụ trên máy tính đó.

**Các thành phần cơ bản**

* Máy chủ TELNET: Máy chủ TELNET là máy tính cung cấp dịch vụ TELNET.
* Máy tính client: Máy tính client là máy tính sử dụng dịch vụ TELNET.

### SSH

**Mô hình hoạt động**

Dịch vụ SSH hoạt động theo mô hình client-server. Máy tính client sử dụng SSH để kết nối với một máy tính khác và thực hiện các tác vụ trên máy tính đó. SSH sử dụng mã hóa để bảo vệ dữ liệu được truyền tải

**Các thành phần cơ bản**

* Máy chủ SSH: Máy chủ SSH là máy tính cung cấp dịch vụ SSH.
* Máy tính client: Máy tính client là máy tính sử dụng dịch vụ SSH.

## Client – Server Model

Mô hình Client – Server là một mô hình phân tians trong đó các ứng dụng được chia thành 2 thành phần chính: Client và server. Trong mô hình này, client và server tương tác với nhau thông qua mạng.

Các thành phần

* Máy chủ: Máy chủ là máy tính cung cấp các dịch vụ và tài nguyên cho các client.
* Client: Client là máy tính yêu cầu sử dụng các dịch vụ và tài nguyên từ máy chủ.

**Mô hình hoạt động**

Trong mô hình client-server, client gửi yêu cầu đến máy chủ. Máy chủ nhận được yêu cầu và xử lý nó. Sau khi xử lý xong, máy chủ trả lại kết quả cho client.

**Lấy ví dụ**

Một ví dụ đơn giản về mô hình client-server là khi bạn truy cập một trang web. Máy tính của bạn (client) gửi yêu cầu đến máy chủ web (server). Máy chủ web nhận được yêu cầu và trả về cho bạn trang web.

Một ví dụ khác là khi bạn gửi email. Máy tính của bạn (client) gửi yêu cầu đến máy chủ email (server). Máy chủ email nhận được yêu cầu và gửi email đến người nhận.

**Ưu điểm**

* Tính hiệu quả: Máy chủ có thể cung cấp dịch vụ cho nhiều client cùng một lúc.
* Tính bảo mật: Máy chủ có thể kiểm soát truy cập vào các tài nguyên.
* Tính mở rộng: Mô hình client-server có thể được mở rộng để đáp ứng nhu cầu của người dùng.

**Nhược điểm**

* Tính phụ thuộc: Client phụ thuộc vào máy chủ để cung cấp dịch vụ.
* Tính phức tạp: Mô hình client-server có thể phức tạp để triển khai và quản lý.

**Ứng dụng**

Mô hình client-server được sử dụng trong nhiều ứng dụng khác nhau, bao gồm:

* Internet: Các ứng dụng Internet như web, email, FTP,... đều sử dụng mô hình client-server.
* Mạng nội bộ: Các ứng dụng mạng nội bộ như chia sẻ file, in ấn,... cũng sử dụng mô hình client-server.
* Mạng doanh nghiệp: Các ứng dụng doanh nghiệp như ERP, CRM,... cũng sử dụng mô hình client-server.

## Connection-oriented và connectionless

### Giao thức hướng kết nối (connection-oriented)

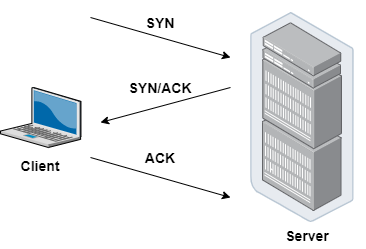
Trước khi gói tin được truyền đi trong mạng, 2 host sẽ cần thỏa thuận các tham số kích thước gói, chất lượng dịch vụ, cơ chế kiểm tra lỗi…

Sau khi thiết lập, hai thiết bị duy trì kết nối và theo dõi thứ tự các gói tin được gửi và nhận, đảm báo tính toàn vẹn và thứ tự của dữ liệu.

**Giao thức TCP**

TCP là giao thức hướng kết nối cũng cấp truyền thông tin cậy đảm bảo dữ liệu được gửi đến đích.

TCP hoạt động theo trình bắt tay 3 bước:

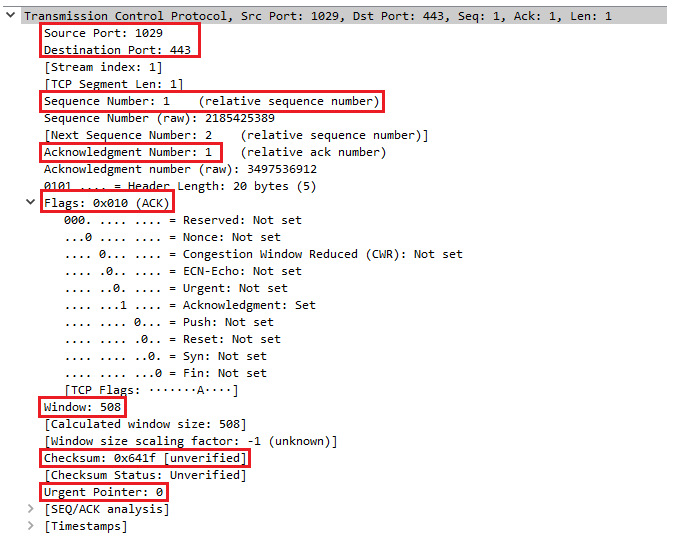


* Máy client gửi gói tin SYN – yêu cầu kết nối
* Máy Server phản hồi bằng gói SYN/ACK, xác nhận yêu cầu kết nối.
* Máy Client nhận gói SYN/ACK và trả lời bằng gói ACK

Sau khi kết nối được thiết lập, TCP hoạt đông bằng cách chia nhỏ dữ liệu thành từng segments.

**Cấu trúc TCP Header**

* Source port (16 bit): Số cổng của thiết bị gửi.
* Destination port (16 bit): Số cổng của thiết bị nhận.
* Sequence number (32 bit): Dùng để đánh số thứ tự gói tin ( từ số sequense nó sẽ tính ra được số byte đã được truyền)
* Acknowledgment number (32 bit): Dùng để báo đã nhận được gói tin nào và mong nhận được byte mang số thứ tự nào tiếp theo.
* DO (4 bit): Cho biết toàn bộ header dài bao nhiêu tính theo đơn vị word (1 Word = 4 byte).
* RSV (4 bit): Đều được thiết lập bằng 0.
* Flags (9 bit): Được sử dụng để thiết lập kết nối, gửi dữ liệu và chấm dứt kêt nối.
  + URG: Ưu tiên dữ liệu này hơn các dữ liệu khác.
  + ACK: Được sử dụng để xác nhận.
  + PSH: Segment yêu cầu chức năng push.
  + RST: Thiết lập lại kết nối.
  + SYN: Được sử dụng để đặt số thứ tự ban đầu.
  + FIN: Kết thúc kết nối TCP.
* Windows (16 bit): Số lượng byte được thiết bị sẵn sàng tiếp nhận.
* Checksum (16 bit): Kiểm tra lỗi của toàn bộ TCP segment.
* Urgent pointer (16 bit): Sử dụng trong trường hợp cần ưu tiên dữ liệu.
* Options (tối đa 32 bit): Cho phép thêm vào TCP các tính năng khác.



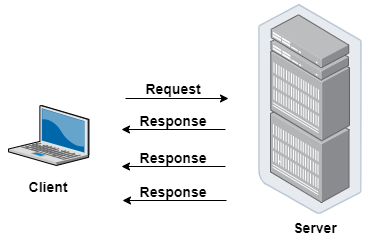
### Giao thức không hướng kết nối (Connectionless)

Mỗi gói tin chứa đầy đủ thông tin định tuyến (như địa chỉ nguồn và đích) để được định tuyến độc lập trên mạng. Không có cơ chế theo dõi thứ tự các gói tin, các gói có thể đến theo thứ tự khác nhau hoặc bị mất.

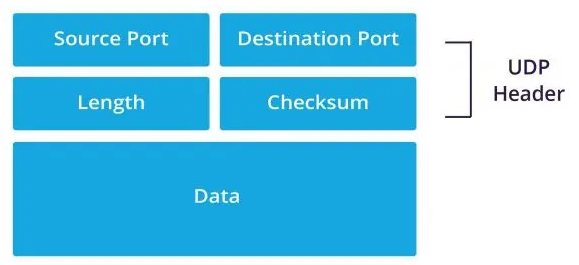
**Giao thức UDP**

UDP (User Datagram Protocol) là một trong những giao thức cốt lõi của giao thức TCP/IP. Dùng UDP, chương trình trên mạng máy tính có thể gửi những dữ liệu ngắn được gọi là datagram tới máy khác. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP làm; các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái của nó nên nó hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu.

Khi một ứng dụng sử dụng giao thức UDP, các gói tin được gửi cho bên nhận và bên gửi không phải chờ để đảm bảo bên nhận đã nhận được gói tin, do đó nó lại tiếp tục gửi gói tin tiếp theo. Nếu bên nhận bỏ lỡ một vài gói tin UDP, họ sẽ mất vì bên gửi không gửi lại chúng. Do đó thiết bị có thể giao tiếp nhanh hơn.



**Cấu trúc UDP Header**

****

* Source port: Số cổng của thiết bị gửi. Trường này có thể đặt là 0 nếu máy tính đích đến không cần trả lời người gửi.
* Destination port: Số cổng của thiết bị nhận.
* Length: Xác định chiều dài của toàn bộ datagram: phần header và dữ liệu. Chiều dài tối thiểu là 8 byte khi gói tin không có dữ liệu, chỉ có header.

# Basic Switching

## Công nghệ Ethernet

Ethernet là một dạng công nghệ truyền thống dùng để kết nối các mạng LAN cục bộ, cho phép các thiết bị có thể giao tiếp với nhau thông qua một giao thức - một bộ quy tắc hoặc ngôn ngữ mạng chung.

Ethernet cung cấp các chức năng sau:

* Giao tiếp giữa các thiết bị trên cùng một mạng: Ethernet cho phép các thiết bị trên cùng một mạng giao tiếp với nhau bằng cách sử dụng một phương thức truy cập phương tiện (MAC) được gọi là CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
* Cung cấp địa chỉ vật lý cho các thiết bị: Ethernet sử dụng địa chỉ MAC (Media Access Control) để xác định các thiết bị trên mạng. Địa chỉ MAC là một số duy nhất được gán cho mỗi thiết bị Ethernet khi nó được sản xuất.
* Cung cấp tính bảo mật: Ethernet có thể được sử dụng để cung cấp tính bảo mật cho dữ liệu được truyền trên mạng bằng cách sử dụng các giao thức bảo mật như IPsec.

**Lớp Physical và Datalink trong Ethernet**

Lớp Physical (Lớp vật lý) trong Ethernet chịu trách nhiệm giao tiếp dữ liệu ở dạng bit trên phương tiện truyền dẫn. Lớp này định nghĩa các đặc điểm vật lý của mạng, chẳng hạn như loại cáp được sử dụng, tốc độ truyền dữ liệu và phương thức ghép kênh.

Lớp Datalink (Lớp liên kết dữ liệu) trong Ethernet chịu trách nhiệm cung cấp các dịch vụ giao tiếp giữa các thiết bị trên mạng. Lớp này bao gồm các chức năng sau:

* Giao tiếp dữ liệu giữa các thiết bị: Lớp Datalink chịu trách nhiệm truyền dữ liệu từ một thiết bị đến thiết bị khác trên mạng.
* Quản lý truy cập phương tiện: Lớp Datalink sử dụng phương thức CSMA/CD để quản lý truy cập phương tiện.
* Cung cấp địa chỉ vật lý: Lớp Datalink sử dụng địa chỉ MAC để xác định các thiết bị trên mạng.

**LLC và MAC**

Lớp Datalink trong Ethernet thường được chia thành hai lớp phụ:

* Lớp Kiểm soát truy cập phương tiện (MAC): Lớp MAC chịu trách nhiệm quản lý truy cập phương tiện và cung cấp địa chỉ vật lý cho các thiết bị.
* Lớp Điều khiển liên kết logic (LLC): Lớp LLC cung cấp các dịch vụ giao tiếp giữa các thiết bị trên mạng.

Lớp MAC là một lớp quan trọng trong Ethernet vì nó chịu trách nhiệm quản lý truy cập phương tiện. Phương thức CSMA/CD được sử dụng để đảm bảo rằng chỉ một thiết bị tại một thời điểm có thể truyền dữ liệu trên mạng.

Lớp LLC cung cấp các dịch vụ giao tiếp giữa các thiết bị trên mạng. Lớp này có thể được sử dụng để cung cấp các dịch vụ như xác thực, kiểm soát luồng và phân đoạn dữ liệu.

## Ethernet frame

Một packet data (gói dữ liệu) trên một link Ethernet được gọi là một packet Ethernet. Frame Ethernet là payload (phần tải mang theo) do packet này vận chuyển. Một frame Ethernet có một preamble và một start frame delimiter (SFD) đi đầu, cả hai đều là một phần của packet Ethernet ở tầng vật lý.

Mỗi frame Ethernet bắt đầu bởi một header Ethernet. Header này chứa địa chỉ MAC nguồn và đích ở hai trường đầu tiên. Phần ở giữa frame là data payload chứa các header bất kì của các protocol khác (ví dụ, Internet Protocol) được mang trong frame này. Frame kết thúc bởi một frame check sequence (FCS, chuỗi kiểm tra frame).Đây là một cyclic redundancy check 32 bit được dùng để phát hiện bất kì hư hỏng dữ liệu nào trong lúc truyền.



* **Preamble**: Preamble là một chuỗi 7 bytes được sử dụng để đồng bộ hóa các thiết bị nhận và truyền. Preamble bao gồm các bit 1 và 0 được sắp xếp theo một mẫu nhất định.
* **Start Frame Delimiter (SFD):** SFD là một byte được sử dụng để xác định bắt đầu của Ethernet Frame. SFD là một chuỗi 1 byte có giá trị 10101010.
* **Destination Address**: Destination Address là 6 bytes chứa địa chỉ MAC của thiết bị nhận. Địa chỉ MAC là một số duy nhất được gán cho mỗi thiết bị Ethernet khi nó được sản xuất.
* **Source Address**: Source Address là 6 bytes chứa địa chỉ MAC của thiết bị truyền.
* **Type**: Type là 2 bytes xác định loại dữ liệu được truyền trong Ethernet Frame. Type được sử dụng bởi các thiết bị nhận để xác định cách xử lý dữ liệu trong Ethernet Frame.
* **Data**: Data là dữ liệu được truyền giữa các thiết bị. Data có thể là bất kỳ loại dữ liệu nào, chẳng hạn như dữ liệu IP, dữ liệu TCP, dữ liệu UDP, v.v.
* **Frame Check Sequence (FCS**): FCS là 4 bytes được sử dụng để phát hiện lỗi trong Ethernet Frame. FCS được tính toán dựa trên tất cả các byte trong Ethernet Frame. Nếu FCS không hợp lệ, thì Ethernet Frame bị lỗi và sẽ bị bỏ qua bởi thiết bị nhận.

**Encapsulation Ethernet Frame**

Encapsulation Ethernet Frame là quá trình bao bọc dữ liệu trong một Ethernet Frame. Quá trình này được thực hiện bởi các thiết bị Ethernet, chẳng hạn như switch, router, và máy tính.

Encapsulation Ethernet Frame bao gồm các bước sau:

* Thêm preamble và SFD vào đầu dữ liệu.
* Thêm địa chỉ MAC của thiết bị nhận vào header của Ethernet Frame.
* Thêm địa chỉ MAC của thiết bị truyền vào header của Ethernet Frame.
* Thêm Type vào header của Ethernet Frame.
* Thêm dữ liệu vào Ethernet Frame.
* Tính toán FCS.

Sau khi hoàn thành các bước trên, dữ liệu sẽ được bao bọc trong một Ethernet Frame và có thể được truyền trên mạng Ethernet.

## CSMA/CD

CSMA/CD là viết tắt của Carrier Sense Multiple Access with Collision Detection, là một phương thức truy cập phương tiện (MAC) được sử dụng trong mạng Ethernet. CSMA/CD cho phép các thiết bị trên cùng một mạng chia sẻ phương tiện truyền dẫn (chẳng hạn như cáp Ethernet) một cách hiệu quả và tránh xung đột.

**Cách thức hoạt động của CSMA/CD**

CSMA/CD hoạt động theo các bước sau:

* Thiết bị muốn truyền dữ liệu sẽ lắng nghe kênh truyền dẫn để xem có thiết bị nào khác đang truyền dữ liệu hay không.
* Nếu kênh truyền dẫn đang trống, thì thiết bị sẽ bắt đầu truyền dữ liệu.
* Nếu kênh truyền dẫn đang bận, thì thiết bị sẽ tạm dừng việc truyền dữ liệu và lắng nghe kênh truyền dẫn trong một khoảng thời gian ngẫu nhiên.
* Nếu sau khi lắng nghe kênh truyền dẫn trong một khoảng thời gian ngẫu nhiên mà vẫn không có thiết bị nào khác đang truyền dữ liệu, thì thiết bị sẽ bắt đầu truyền dữ liệu.

**Cách phát hiện xung đột**

Nếu hai thiết bị trên cùng một mạng bắt đầu truyền dữ liệu cùng một lúc, thì sẽ xảy ra xung đột. Khi xảy ra xung đột, các thiết bị sẽ phát hiện ra xung đột bằng cách lắng nghe kênh truyền dẫn.

Khi phát hiện ra xung đột, các thiết bị sẽ dừng việc truyền dữ liệu và bắt đầu một khoảng thời gian ngẫu nhiên. Sau khoảng thời gian ngẫu nhiên, các thiết bị sẽ thử lại việc truyền dữ liệu.

**Ưu điểm của CSMA/CD**

* Đơn giản và hiệu quả
* Không cần sử dụng bộ định thời gian hoặc bộ đếm
* Có thể hoạt động trên nhiều loại phương tiện truyền dẫn

**Nhược điểm của CSMA/CD**

* Có thể dẫn đến lãng phí băng thông
* Không thể đảm bảo rằng dữ liệu sẽ được truyền thành công trong mọi trường hợp

## Collision domain và broadcast domain

Collision domain là một khu vực trong mạng nơi các thiết bị có thể gửi dữ liệu cùng một lúc và có thể xảy ra xung đột. Các thiết bị trong cùng một collision domain được kết nối trực tiếp với nhau, chẳng hạn như các thiết bị được kết nối với cùng một hub.

Broadcast domain là một khu vực trong mạng nơi các thiết bị có thể gửi dữ liệu broadcast đến tất cả các thiết bị khác trong miền. Các thiết bị trong cùng một broadcast domain được kết nối với nhau thông qua một bộ định tuyến hoặc switch.

Sự khác biệt giữa collision domain và broadcast domain:

|  |  |  |
| --- | --- | --- |
| Tính năng | Collision domain | Broadcast domain |
| Định nghĩa | Khu vực trong mạng nơi các thiết bị có thể gửi dữ liệu cùng một lúc và có thể xảy ra xung đột | Khu vực trong mạng nơi các thiết bị có thể gửi dữ liệu broadcast đến tất cả các thiết bị khác trong miền |
| Kết nối | Các thiết bị trong cùng một collision domain được kết nối trực tiếp với nhau | Các thiết bị trong cùng một broadcast domain được kết nối với nhau thông qua một bộ định tuyến hoặc switch |
| Xung đột | Có thể xảy ra xung đột | Không thể xảy ra xung đột |
| Broadcast | Không thể gửi broadcast | Có thể gửi broadcast |

**Tác động của collision domain và broadcast domain**

Collision domain và broadcast domain có thể ảnh hưởng đến hiệu suất của mạng.

* Collision domain: Collision domain càng lớn thì khả năng xảy ra xung đột càng cao. Điều này có thể dẫn đến lãng phí băng thông và giảm hiệu suất mạng.
* Broadcast domain: Broadcast domain càng lớn thì càng nhiều dữ liệu broadcast được gửi trên mạng. Điều này có thể dẫn đến tắc nghẽn mạng và giảm hiệu suất mạng.

**Cách giảm thiểu collision domain và broadcast domain**

Để giảm thiểu collision domain và broadcast domain, có thể sử dụng các thiết bị mạng như switch và router.

* Switch: Switch có thể chia một collision domain lớn thành nhiều collision domain nhỏ hơn. Điều này có thể giúp giảm khả năng xảy ra xung đột và cải thiện hiệu suất mạng.
* Router: Router có thể phân tách các broadcast domain. Điều này có thể giúp giảm lượng dữ liệu broadcast được gửi trên mạng và cải thiện hiệu suất mạng.

Ví dụ

Giả sử có một mạng Ethernet với 10 máy tính được kết nối với một hub. Trong trường hợp này, tất cả 10 máy tính đều nằm trong cùng một collision domain. Nếu

hai máy tính trên cùng một collision domain bắt đầu truyền dữ liệu cùng một lúc, thì sẽ xảy ra xung đột.

Nếu một bộ định tuyến được thêm vào mạng, thì bộ định tuyến sẽ phân tách các máy tính thành hai collision domain. Máy tính 1, 2, 3 và 4 sẽ nằm trong collision domain 1, và máy tính 5, 6, 7, 8, 9 và 10 sẽ nằm trong collision domain 2. Điều này sẽ giúp giảm khả năng xảy ra xung đột và cải thiện hiệu suất mạng.

## Simplex và Duplex

Có 3 chế độ truyền, cụ thể là: Simplex (đơn công), half duplex (bán song công) và full duplex (song công toàn phần). Chế độ truyền xác định hướng của luồng tín hiệu giữa hai thiết bị được kết nối.

Sự khác biệt chính giữa 3 chế độ truyền là ở chế độ truyền đơn công, tín hiệu được truyền theo một hướng. Trong khi ở chế độ truyền bán song công, việc truyền tín hiệu có thể diễn ra theo cả 2 hướng, nhưng hai thiết bị được kết nối sử dụng luân phiên kênh (nghĩa là tín hiệu chỉ được truyền theo một chiều tại một thời điểm).

Mặt khác, trong chế độ truyền song công toàn phần, việc truyền tín hiệu diễn ra theo hai hướng cùng một lúc và kênh được sử dụng đồng thời bởi cả hai thiết bị đã kết nối.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiêu chí so sánh** | **Simplex** | **Half Duplex** | **Full Duplex** |
| Hướng truyền tín hiệu | Đơn hướng | Hai chiều, mỗi lần theo một hướng | Hai chiều, đồng thời theo hai hướng |
| Gửi/Nhận | Bên gửi chỉ có thể gửi dữ liệu | Bên gửi có thể gửi và nhận dữ liệu, nhưng chỉ thực hiện được một hành động vào một thời điểm | Bên gửi có thể gửi và nhận dữ liệu cùng một lúc |
| Hiệu suất | Chế độ truyền kém nhất | Tốt hơn chế độ Simplex | Chế độ truyền tốt nhất |
| Ví dụ | Bàn phím và màn hình | Bộ đàm | Điện thoại |

**Simplex**

Trong chế độ truyền đơn công, việc giao tiếp giữa bên gửi và bên nhận chỉ xảy ra theo một hướng. Bên gửi chỉ có thể gửi dữ liệu và bên nhận chỉ có thể nhận dữ liệu. Bên nhận không thể trả lời bên gửi.

**Half Duplex**

Việc giao tiếp giữa bên gửi và bên nhận diễn ra theo cả hai hướng trong truyền dẫn bán song công, nhưng mỗi lần chỉ được theo một hướng. Bên gửi và bên nhận có thể gửi cũng như nhận thông tin, nhưng chỉ một bên được phép gửi tại một thời điểm cụ thể.

**Full duplex**

Trong chế độ truyền song công toàn phần, việc giao tiếp giữa bên gửi và bên nhận có thể diễn ra đồng thời. Bên gửi và bên nhận có thể truyền và nhận tín hiệu cùng một lúc. Chế độ truyền song công toàn phần giống như con đường hai chiều, trong đó các phương tiện có thể lưu chuyển theo cả hai hướng cùng một lúc.

## Switch

Switch là một thiết bị mạng được sử dụng để kết nối các thiết bị khác nhau trong một mạng LAN. Switch hoạt động theo phương thức chuyển mạch (switching) để chuyển tiếp dữ liệu từ một cổng đến một cổng khác.

**Vai trò chính của Switch trong mạng LAN là:**

* Kết nối các thiết bị trong mạng LAN: Switch cung cấp một cách để kết nối các máy tính, máy in, thiết bị lưu trữ và các thiết bị mạng khác trong cùng một mạng LAN.
* Cải thiện hiệu suất mạng: Switch sử dụng phương thức chuyển mạch để chuyển tiếp dữ liệu từ một cổng đến một cổng khác. Điều này giúp cải thiện hiệu suất mạng bằng cách giảm thiểu xung đột và lãng phí băng thông.
* Tăng cường bảo mật mạng: Switch có thể được sử dụng để phân tách các miền mạng và áp dụng các chính sách bảo mật.

**Nguyên tắc chuyển mạch trong Switch**

Nguyên tắc chuyển mạch của switch dựa trên việc sử dụng bảng ánh xạ địa chỉ MAC (MAC address table). Bảng ánh xạ địa chỉ MAC là một bảng lưu trữ các địa chỉ MAC của các thiết bị được kết nối với switch.

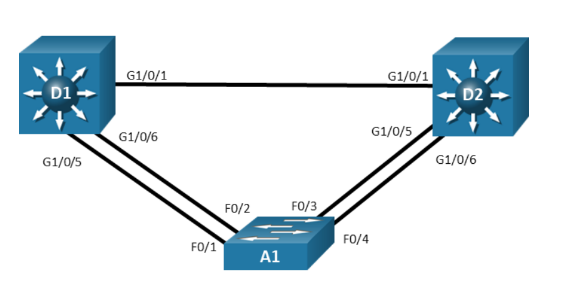
Khi một thiết bị gửi dữ liệu, switch sẽ sử dụng bảng ánh xạ địa chỉ MAC để xác định cổng kết nối với thiết bị nhận. Switch sẽ chỉ chuyển tiếp dữ liệu đến cổng đó.

**Quá trình chuyển mạch của switch được thực hiện theo các bước sau:**

* Switch nhận dữ liệu từ cổng đầu vào.
* Switch xác định địa chỉ MAC của thiết bị gửi.
* Switch tìm kiếm địa chỉ MAC của thiết bị nhận trong bảng ánh xạ địa chỉ MAC.
* Nếu tìm thấy địa chỉ MAC của thiết bị nhận trong bảng ánh xạ địa chỉ MAC, thì switch sẽ xác định cổng kết nối với thiết bị nhận.
* Switch sẽ chuyển tiếp dữ liệu đến cổng đó.
* Nếu không tìm thấy địa chỉ MAC của thiết bị nhận trong bảng ánh xạ địa chỉ MAC, thì switch sẽ chuyển tiếp dữ liệu đến tất cả các cổng. (Trừ cổng nhận vào)

## STP – Spanning tree protocol

STP là một giao thức chống loop tại layer 2 và giúp tăng tính dự phòng



Nếu switch không được cấu hình gì thì cũng sẽ chạy pvst

Các trạng thái Port trong STP:

* **Disabled**: Port bị shutdowm
* **Blocking**: Port được mở nhưng không chuyển tiếp các gói tin. Port này chỉ lắng nghe các bản tin BPDU
* **Listening**: Port lắng nghe các gói tin BPDU và chuẩn bị cho quá trình chuyển tiếp gói tin. Trong trạng thái này port không chuyển tiếp dữ liệu người dùng
* **Learning**: Port lắng nghe và học thông tin từ gói tin BPDU nhận được. Switch bắt đầu học địa chỉ MAC của các thiết bị. Ở trạng thái này, port vẫn không chuyển tiếp dữ liệu.
* **Forwarding**: Port đã hoàn tất quá trình học và đã chuyển sang chế độ chuyển tiếp.

Các loại Port trong STP:

* **Root port**: là port có hướng gần nhất về root brigde, có cost thấp nhất, chỉ có 1 root port , port ở trạng thái chuyển tiếp dữ liệu.
* **Designated port**: ở trạng thái chuyển tiếp dữ liệu, gửi các BPDU frame. Tất cả các port trên Root switch đều thuộc loại này.
* **Bloking port**: Port ở trạng thái khóa, không gửi và nhận dữ liệu những vẫn gửi và nhận BPDU frame
  + - * Quá trình bình bầu Blocking port:
* Bình bầu root brigde:

*Brigde-ID = Priority (2byte) + MAC(6byte) - giá trị định danh cho switch*

Switch nào có Priority nhỏ nhất sẽ được bầu làm root brigde. Nếu Priority bằng nhau thì switch nào có địa chỉ MAC nhỏ hơn thì sẽ làm root brigde.

Sau khi đã bầu được Root – Bridge thì chỉ có Switch làm root mới gửi BPDU ra khỏi cổng để duy trì tiến trình STP (gửi 2s/lần). Các Switch con chỉ nhận, bổ xung thông tin BPDU và Forward thông tin BPDU này

* Chọn ra root port :

Sau khi đã bầu Root – bridge thì sẽ sang các Switch bầu chọn Root-Port. Root-Port là port có đường về Root – bridge có tổng cost tích lũy nhỏ nhất.

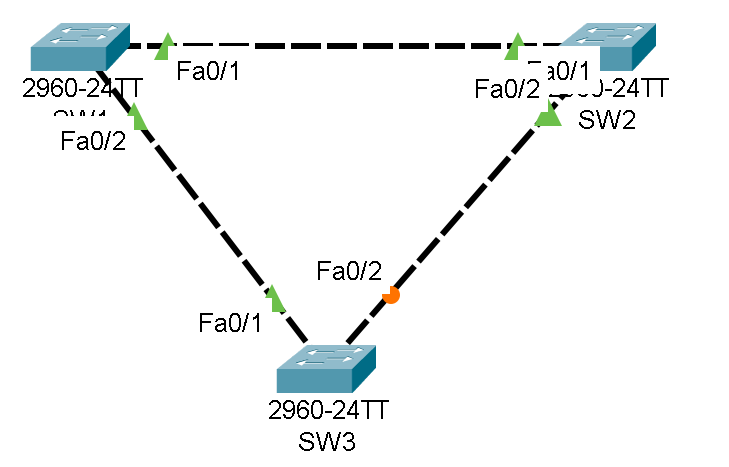
Mỗi interface của Ethernet LAN đều được gán cho một giá trị. Giá trị đó gọi là cost dùng để thực hiện tính toán của STP.

Để xác định được cost tích lũy của một port đến Switch làm Root-bridge bạn thực hiện tính ngược từ Root về cổng đó dựa theo chiều lan truyền BPDU theo quy tắc “vào cộng ra không cộng”.

* Chọn ra designated port:

Tiếp theo STP ta thực hiện bầu Designated Port. Designated Port là Port cung cấp đường về root-bridge có tổng cost nhỏ nhất trên phân đoạn mạng bạn đang xét. Chỉ có một Designated port ứng với một link kết nối.

* Chọn ra blocking port : Port còn lại là blocking port
  + - * Kiểm tra thông tin spanning tree:
* Pvst (pervlan spanning tree): để tối ưu spanning tree trên đường trunk có nhiều vlan thì mỗi vlan sẽ chạy một cây spanning tree độc lập và tối ưu root switch trên nhiều vlan
* Câu hình:



*SW(config)#spanning-tree mode pvst*

*SW1(config)#spanning-tree vlan 10 root primary*

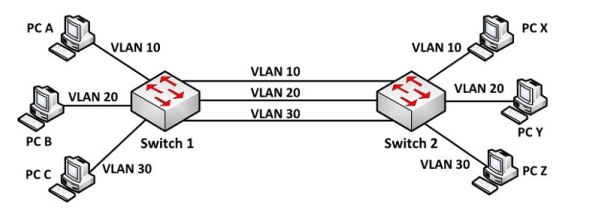
*SW1(config)#spanning-tree vlan 20 root secondary*

*SW2(config)#spanning-tree vlan 10 root secondary*

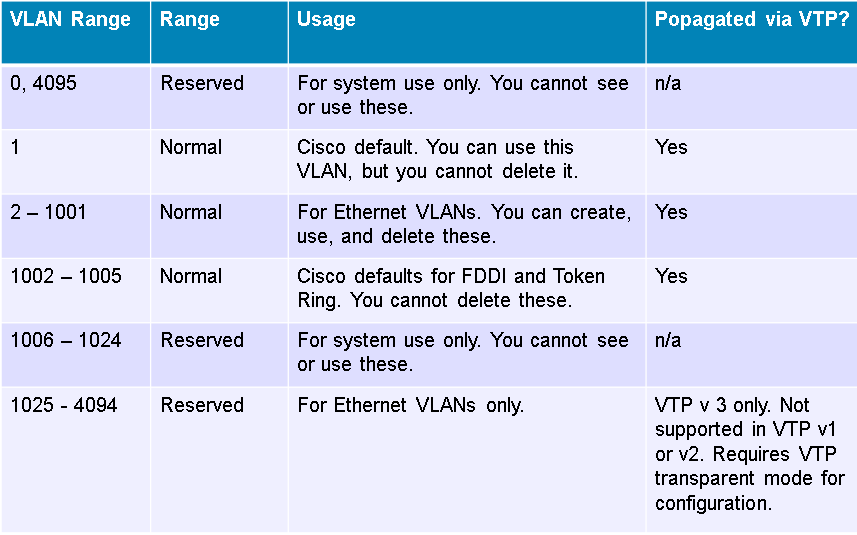
*SW2(config)#spanning-tree vlan 20 root primary*

## VLAN

Vlan là khái niệm mạng LAN ảo, hệ thống mạng LAN độc lập với nhau về mặt logic nhưng sử dụng chung 1 hạ tầng SW vật lý



Ưu điểm: Tiết kiệm tài nguyên, số lượng switch



Vlan 1 là default vlan luôn tồn tại tên switch, nó được tự động tạo và mặc định được cấu hình để kết nối tất cả các cổng vật lý của switch

* + - * Cấu hình Vlan:

*SW(config)#vlan 10*

*SW(config-vlan)#name IT*

*SW(config-vlan)#vlan 20*

*SW(config-vlan)#name HR*

* + - * Gán port vào vlan

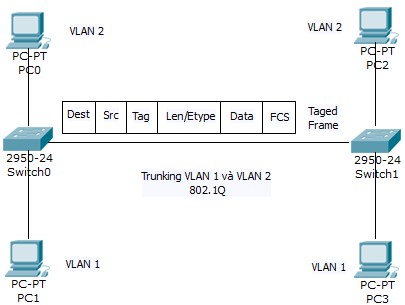
*SW(config)#int e0/2*

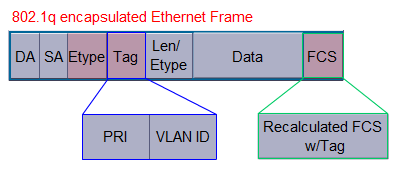
*SW(config-if)#switchport mode access*

*SW(config-if)#switchport access vlan 10*

Trunk là đường link kết nối giữa các switch cho phép gói tin từ nhiểu Vlan khác nhau cùn đi qua

Mỗi một gói tin của từng vlan khi đi qua đường trunk sẽ được đánh dấu tagging để có thể phân biệt với nhau





* + - * Cấu hình trunking:

*SW(config)#int e0/1*

*SW(config-if)#switchport trunk encapsulation dot1q*

*SW(config-if)#switchport mode trunk*

*SW(config-if)#switchport trunk allowed vlan 10,20*

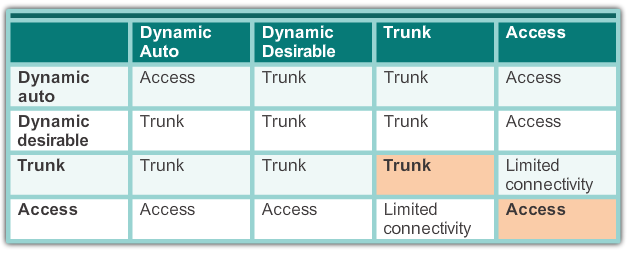
*SW(config-if)#switchport trunk allowed vlan add 30*

*SW(config-if)#switchport trunk allowed vlan remove 30*

* Native Vlan: khi frame của native vlan đi qua đường trunk thì không được tagging. Điều kiện là 2 đầu của switch phải cấu hinh chung một native vlan.   
  Mặc định native vlan là vlan 1
* DTP – Dynamic Trunking Protocol : là giao thức tự động cấu hình liên kết trunk trên các thiết bị switch của Cisco.

Có 4 chế độ port trong giao thức DTP:

* + Dynamic auto: tự động, mặc định port sẽ được đặt ở mode này
  + Dynamic desirable: chủ động
  + Trunk: Cấu hình thủ công
  + Access: ở mode này frame sẽ không được tagging, phù hợp với kết nối với PC



Để bảo mật thì nên cấu hình: *switchport nonegotiate .* Cấu hình này các port sẽ không chủ động thương lượng thiết lập đường trunk và nếu muốn thiết lập đường trunk thì sẽ phải cấu hình thủ công.

## VTP – Virtual Trunking Protocol

VTP là giao thức giúp đồng bộ thông tin VLAN trên hạ tầng Switch

VTP domain bao gồm tất cả các SW có cùng chính sách cấu hình về vlan

VTP server là SW có thể tạo chỉnh sửa , xóa vlan trong vtp domain

VTP client đóng vai trò thực hiện theo hướng dẫn của vtp server, không thể tự tạo, chỉnh sửa và xóa các cấu hình vlan

VTP transparent nhận và chuyển tiếp các bản tin VTP và không thể modify được database vlan. Có thể tạo thông tin vlan nhưng sẽ không đồng bộ với các SW khác

* Cấu hình:

*Server(config)# vtp domain \_\_\_\_*

*#vtp version 2*

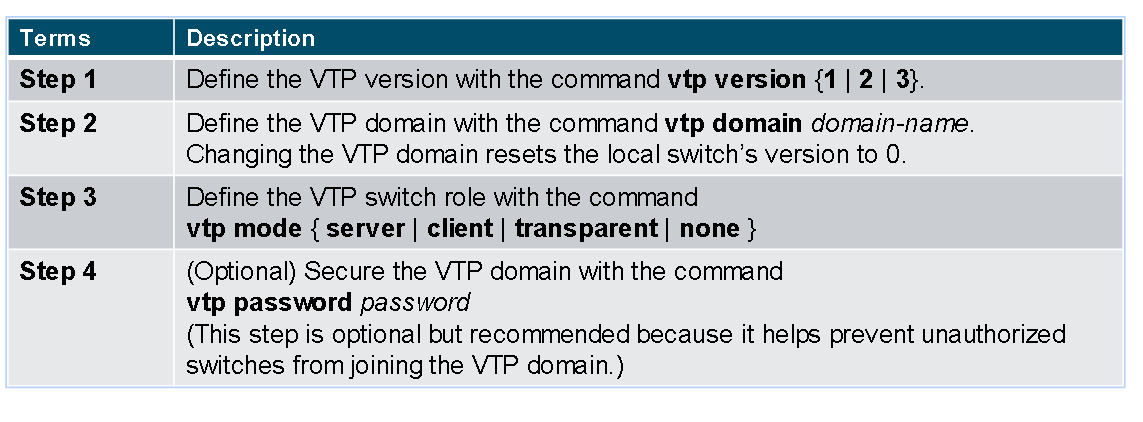
*#vtp mode server*

*Client(Config)#vtp version 2*

*#vtp domain \_\_\_\_\_*

*#vtp mode client*

*Client(#)#show vtp status*



VTP – Transparent: là switch có vai trò chuyển tiếp bản tin VTP nhận được, không nhận những cấu hình trong bản tin VTP đó

VTP – Off: Không chuyển tiếp bản tin VTP đi

Nếu switch không cấu hình gì cả:

* + Khi nhận được bản tin VTP thì switch sẽ tự động cấu hình với domain giống với bản tin VTP nhận được

Khi cấu hình: VTP enable => switch ở mode server

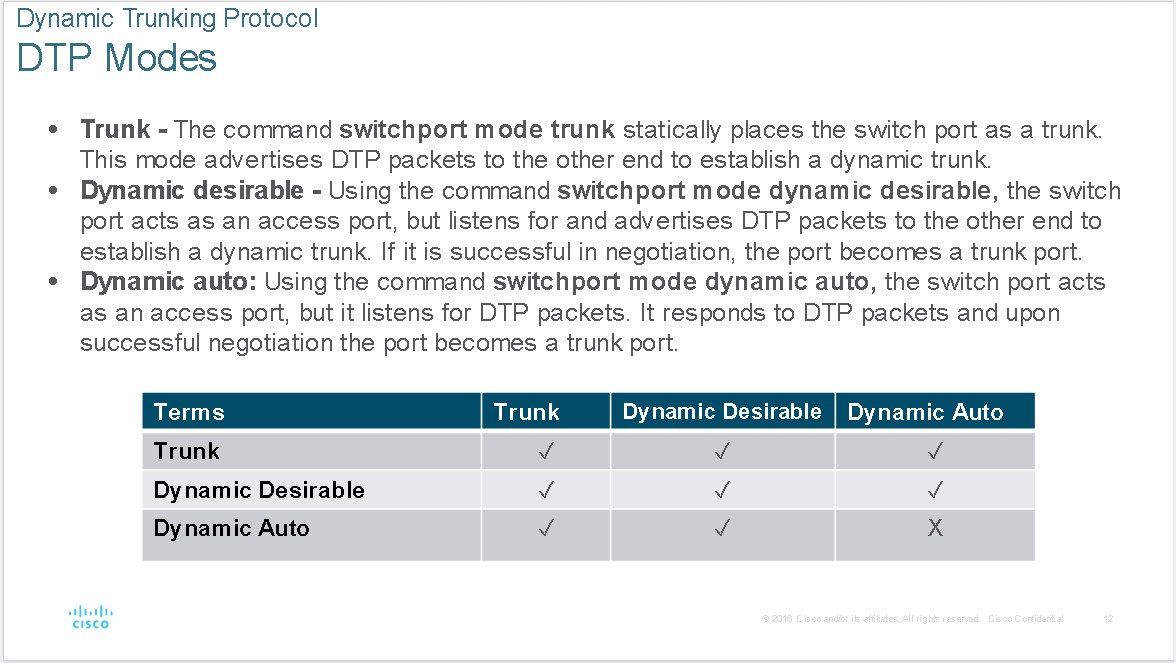
Tham số ***Revisons***: thể hiện sự thay đổi trong domain, có thay đổi tham số sẽ được tăng lên 1

* + Nếu bản tin VTP nhận được có trường Revisons lớn hơn giá trị Revisions trên client thì client mới chấp nhận thay đổi và cật nhật vào cơ sở dữ liệu của mình.
  + Vì vậy, cứ bản tin có Revisions lớn hơn sẽ khiến cho các switch khác cùng domain chấp nhận và cật nhật vào cơ sở dữ liệu vlan (kể cả trường hợp client cật nhật cho server)
  + Khi cắm 1 switch cũ đã được cấu hình VTP và có database sẵn, các switch mới chưa được cấu hình VTP sẽ nhận bảng data của switch cũ đó. Điều này có thể dẫn tới những sai sót không mong muốn

**DTP – dynamic trunking protocol**

Là giao thức thiết lập cổng trunk một cách tự động.

Chúng ta nên tắt tính năng này nhằm bảo mật hệ thống mạng



Tắt giao thức dtp:

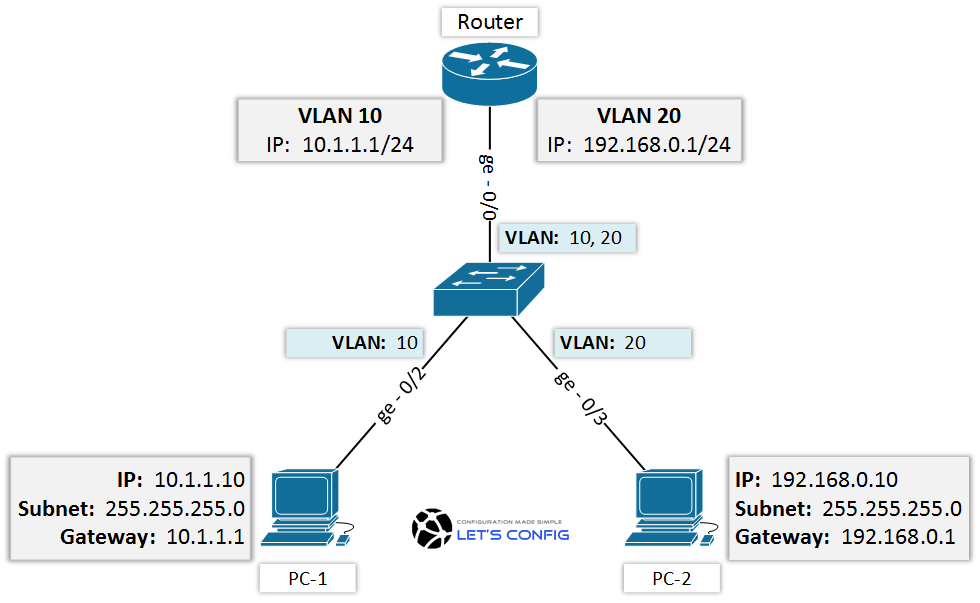
*#int e0/0*

*#switchport nonegotiated*

## Inter-Vlan

Inter-VLAN là phương pháp được thiết lập có hiệu quả nhất bằng cách cung cấp một liên kết trunk duy nhất giữa Switch và Router mà có thể mang lưu lượng truy cập của nhiều VLAN và trong đó các lưu lượng ấy lần lượt có thể được định tuyến bởi Router.

Với Inter-VLAN Routing, Router nhận frame từ Switch với gói tin xuất phát từ một VLAN đã được tag. Nó liên kết các frame với các subinterface thích hợp và sau đó giải mã nội dung của frame (phần IP packet). Router sau đó thực hiện chức năng của Layer 3 dựa trên địa chỉ mạng đích có trong gói tin IP để xác định subinterface cần chuyển tiếp gói IP. Các IP packet bây giờ được đóng gói thành frame theo chuẩn dot1Q (hoặc ISL) để nhận dạng VLAN của subinterface chuyển tiếp và truyền đi trên đường trunk vào Switch.



**Cấu hình Inter-VLAN**

a. Trên Switch

SW0(config)#vlan 10

SW0(config-vlan)#name IT

SW0(config-vlan)#vlan 20

SW0(config-vlan)#name sale

SW0(config-vlan)#exit

SW0(config)#interface range f0/1-10

SW0(config-if-range)#switchport access vlan 10

SW0(config-if-range)#exit

SW0(config)#interface range f0/11-20

SW0(config-if-range)#switchport access vlan 20

SW0(config-if-range)#exit

SW0(config)#interface range g1/1-2

SW0(config-if-range)#switchport mode trunk

SW0(config)#interface vlan 1

SW0(config)#no shutdown

SW0(config-if)#ip add 10.0.0.101 255.255.255.0

SW0(config-if)#end

SW0#writ

b. Cấu hình định tuyến VLAN trên Router

R1(config)#int f0/0

R1(config-if)#no shut

R1(config)#int f0/0.10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip add 192.168.1.1 255.255.255.0

R1(config-subif)#exit

R1(config)#int f0/0.20

R1(config-subif)#encapsulation dot1Q 20

R1(config-subif)#ip add 192.168.2.1 255.255.255.0

R1(config-subif)#exit