Hệ thống mạng

- Thiết bị: Firewall, Core Switch, Access Switch, Modem, Router, Gateway, Bridge, Repeater, Wireless, Module quang, bộ chuyển đổi quang điện: Chức năng và vị trí của mỗi thiết bị trong sơ đồ cấu trúc Hệ thống mạng.

- Các vấn đề liên quan đến địa chỉ IP

- Tổng hợp sơ đồ kết nối 1 sợi nếu như một hệ thống sử dụng full các thiết và các thành phần đấu nối.

**Mục lục**

[CHƯƠNG 1. TÌM HIỂU VỀ MÔ HÌNH OSI 4](#_Toc90319207)

[1. Mô hình OSI 4](#_Toc90319208)

[2. Các thiết bị phần cứng mạng 6](#_Toc90319209)

[CHƯƠNG 2. FIREWALL 8](#_Toc90319210)

[1. Tường lửa Firewall là gì? 8](#_Toc90319211)

[2. Firewall hoạt động như thế nào? 8](#_Toc90319212)

[3. Ưu điểm của Firewall 9](#_Toc90319213)

[4. Các loại Firewall 9](#_Toc90319214)

[CHƯƠNG 3. CORE SWITCH (SWITCH LAYER 3) 10](#_Toc90319215)

[CHƯƠNG 4. ACCESS SWITCH (SWITCH LAYER 2) 11](#_Toc90319216)

[1. Access Switch là gì? 11](#_Toc90319217)

[Điểm khác biệt giữa Core Switch và Switch Access 11](#_Toc90319218)

[CHƯƠNG 5. MODEM 12](#_Toc90319219)

[1. Modem là gì? 12](#_Toc90319220)

[2. Chức năng Modem 12](#_Toc90319221)

[3. Cách hoạt động và chức năng của Modem 12](#_Toc90319222)

[CHƯƠNG 6. ROUTER 13](#_Toc90319223)

[1. Router là gì? 13](#_Toc90319224)

[2. Chức năng của router 13](#_Toc90319225)

[3. Ưu và nhược điểm của Router 14](#_Toc90319226)

[Modem và Router (Bộ định tuyến) khác gì nhau? 14](#_Toc90319227)

[CHƯƠNG 7. GATEWAY 18](#_Toc90319228)

[1. Gateway là gì? 18](#_Toc90319229)

[2. gateway hoạt động 18](#_Toc90319230)

[3. Các loại gateway 19](#_Toc90319231)

[CHƯƠNG 8. BRIDGE 19](#_Toc90319232)

[Bridge là gì? 19](#_Toc90319233)

[Đặc điểm 20](#_Toc90319234)

[Ưu điểm của Bridge 20](#_Toc90319235)

[Nhược điểm của cầu 20](#_Toc90319236)

[Sự khác biệt giữa Bridge và Switch 21](#_Toc90319237)

[CHƯƠNG 9. REPETER 21](#_Toc90319238)

[1. Repeater là gì 21](#_Toc90319239)

[2. Ưu điểm của Repeater 22](#_Toc90319240)

[3. Nhược điểm Repeater 22](#_Toc90319241)

[Sự khác nhau giữa hub và repeater 22](#_Toc90319242)

[CHƯƠNG 10. WIRELESS 22](#_Toc90319243)

[1. Wireless là gì? 22](#_Toc90319244)

[2. Mạng không dây là gì? 23](#_Toc90319245)

[3. Phân loại mạng không dây 23](#_Toc90319246)

[CHƯƠNG 11. MODULE QUANG 25](#_Toc90319247)

[1. SFP Module là gì ? 25](#_Toc90319248)

[2. Chuẩn SFP là gì? 25](#_Toc90319249)

[3. SFP Module có những loại nào? 25](#_Toc90319250)

[4. Tìm hiểu về chức năng DDM 26](#_Toc90319251)

[5. Module quang dùng để làm gì? 26](#_Toc90319252)

[CHƯƠNG 12. BỘ CHUYỂN ĐỔI QUANG ĐIỆN 26](#_Toc90319253)

[1. Module quang là gì? 26](#_Toc90319254)

[2. Sự hình thành và phát triển 26](#_Toc90319255)

[3. Phải chăng SFP nào cũng như nhau? 27](#_Toc90319256)

[CHƯƠNG 13. CÁC VẤN ĐỀ LIÊN QUAN ĐÉN IP 27](#_Toc90319257)

[1. IP là gì? 27](#_Toc90319258)

[2. IP dùng để làm gì? 28](#_Toc90319259)

[3. Ưu và nhược điểm của địa chỉ IP là gì? 28](#_Toc90319260)

[4. Phân loại IP 28](#_Toc90319261)

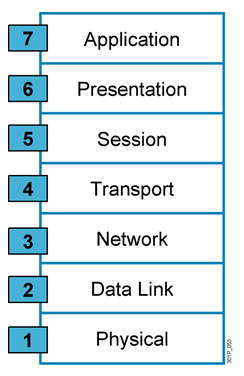
[5. Subnet Mask là gì? 29](#_Toc90319262)

[6. IPv4 là gì? 30](#_Toc90319263)

[7. IPv6 là gì? 30](#_Toc90319264)

# CHƯƠNG 1. TÌM HIỂU VỀ MÔ HÌNH OSI

## Mô hình OSI



Tầng ứng dụng (Application layer – lớp 7): tầng ứng dụng quy định giao diện giữa người sử dụng và môi trường OSI, nó cung cấp các phương tiện cho người sử dụng truy cập vả sử dụng các dịch vụ của mô hình OSI. Các ứng dụng cung được cấp như các chương trình xử lý kí tự, bảng biểu, thư tín … và lớp 7 đưa ra các giao thức HTTP, FTP, SMTP, POP3, Telnet.

Tầng trình bày (Presentation layer – lớp 6): chuyển đổi các thông tin từ cú pháp người sử dụng sang cú pháp để truyền dữ liệu, ngoài ra nó có thể nén dữ liệu truyền và mã hóa chúng trước khi truyền đễ bảo mật. Tầng này sẽ định dạng dữ liệu từ lớp 7 đưa xuống rồi gửi đi đảm bảo sao cho bên thu có thể đọc được dữ liệu của bên phát. Các chuẩn định dạng dữ liệu của lớp 6 là GIF, JPEG, PICT, MP3, MPEG …

Tầng giao dịch (Session layer – lớp 5): thực hiện thiết lập, duy trì và kết thúc các phiên làm việc giữa hai hệ thống. Tầng giao dịch quy định một giao diện ứng dụng cho tầng vận chuyển sử dụng. Nó xác lập ánh xạ giữa các tên đặt địa chỉ, tạo ra các tiếp xúc ban đầu giữa các máy tính khác nhau trên cơ sở các giao dịch truyền thông. Nó đặt tên nhất quán cho mọi thành phần muốn đối thoại riêng với nhau. Các giao thức trong lớp 5 sử dụng là NFS, X- Window System, ASP.

Tầng vận chuyển (Transport layer – lớp 4): tầng vận chuyển xác định địa chỉ trên mạng, cách thức chuyển giao gói tin trên cơ sở trực tiếp giữa hai đầu mút, đảm bảo truyền dữ liệu tin cậy giữa hai đầu cuối (end-to-end). Các giao thức phổ biến tại đây là TCP, UDP, SPX.

Tầng mạng (Network layer – lớp 3): tầng mạng có nhiệm vụ xác định việc chuyển hướng, vạch đường các gói tin trong mạng (chức năng định tuyến), các gói tin này có thể phải đi qua nhiều chặng trước khi đến được đích cuối cùng. Lớp 3 là lớp có liên quan đến các địa chỉ logic trong mạng Các giao thức hay sử dụng ở đây là IP, RIP, IPX, OSPF, AppleTalk.

Tầng liên kết dữ liệu (Data link layer – lớp 2): tầng liên kết dữ liệu có nhiệm vụ xác định cơ chế truy nhập thông tin trên mạng, các dạng thức chung trong các gói tin, đóng gói và phân phát các gói tin.Lớp 2 có liên quan đến địa chỉ vật lý của các thiết bị mạng, topo mạng, truy nhập mạng, các cơ chế sửa lỗi và điều khiển luồng.

Tầng vật lý (Phisical layer – lớp 1): tầng vật lý cung cấp phương thức truy cập vào đường truyền vật lý để truyền các dòng Bit không cấu trúc, ngoài ra nó cung cấp các chuẩn về điện, dây cáp, đầu nối, kỹ thuật nối mạch điện, điện áp, tốc độ cáp truyền dẫn, giao diện nối kết và các mức nối kết.

## Các thiết bị phần cứng mạng

1. Card mạng – NIC (Network Interface Card)

Thiết bị này còn được biết đến với nhiều tên khác nhau như network card (card mạng), Network Interface Card (card giao diện mạng) là một tấm mạch in được cắm vào trong máy tính dùng để cung cấp cổng kết nối vào mạng. Card mạng được coi là một thiết bị hoạt động ở lớp 2 của mô hình OSI. Mỗi card mạng có chứa một địa chỉ duy nhất là địa chỉ MAC - Media Access Control. Card mạng điều khiển việc kết nối máy tính vào các phương tiện truyền dẫn trên mạng.

Nói đến card mạng chúng ta cũng nói đến phương thức truyền tải thông tin trên mạng, đó chính là kiểu cap dùng để kết nối, có thể dùng dây hay không dây còn tùy thuộc vào card mạng. Chẳng hạn, trước khi xây dựng một mạng và bắt đầu mua card mạng, dây cáp, bạn phải quyết định xem nên dùng Ethernet, Ethernet đồng trục, Token Ring hay một tiêu chuẩn mạng nào khác. Mỗi tiêu chuẩn mạng có độ dài và nhược điểm riêng. Thiết kế một mô hình mạng là một bước quan trong.

Các mạng Ethernet hiện đại đều sử dụng cáp đôi xoắn vòng 8 dây. Các dây này được sắp xếp theo thứ tự đặc biệt và đầu nối RJ-45 được gắn vào phần cuối cáp. Đầu nối RJ-45 trông giống như bộ kết nối ở phần cuối dây điện thoại, nhưng lớn hơn. Các dây điện thoại dùng bộ kết nối RJ-11, tương phản với bộ kết nối RJ-45 dùng trong cáp Ethernet.

2. Repeater - Bộ lặp

Repeater là một thiết bị hoạt động ở lớp 1 (Physical) của mô hình OSI khuyếch đại và định thời lại tín hiệu. Repeater khuyếch đại và gửi mọi tín hiệu mà nó nhận được từ một port ra tất cả các port còn lại. Mục đích của repeater là phục hồi lại các tín hiệu đã bị suy yếu đi trên đường truyền mà không sửa đổi gì.

3. Hub

Còn được gọi là multiport repeater, nó có chức năng hoàn toàn giống như Repeater nhưng có nhiều port để kết nối với các thiết bị khác. Mỗi máy tính trong mạng sẽ được kết nối tới một hub thông qua cáp Ethernet. Hub thông thường có 4, 8, 12 và 24 port và là trung tâm của mạng hình sao. Khi một máy tính gửi yêu cầu đến một máy khác, thì nó sẽ gửi đến Hub rồi gửi ra tất cả các máy tính có trong mạng. Mỗi card Ethernet đều được cung cấp một địa chỉ vật lý MAC (Media Access Control) duy nhất. Tất cả máy tính đều nhận dữ liệu, sau đó so sánh địa chỉ đích với địa chỉ vật lý MAC của nó. Nếu khớp, máy tính sẽ biết rằng nó chính là người nhận dữ liệu, nếu không nó sẽ lờ dữ liệu đi. Việc truyền dữ liệu trên Hub thường gây ra xung đột, khi một máy truyền dữ liệu trên dây cùng thời điểm máy khác cũng truyền thì nó sẽ gây ra xung đột, các gói tin sẽ bị phá hủy, sau một thời gian nó sẽ truyền lại, việc này sẽ làm chậm hệ thống rất nhiều và với hệ thống càng lớn thì việc xảy ra xung đột càng lớn., do đó ngày nay vai trò của Hub dần được thay thế bởi các thiết bị cấp cao hơn như switch. Hub họat động ở mức 1 của mô hình OSI.

4. Bridge - Cầu nối

Bridge là một thiết bị hoạt động ở lớp 2 của mô hình OSI dùng để kết nối các phân đoạn mạng nhỏ có cùng cách đánh địa chỉ và công nghệ mạng lại với nhau và gửi các gói dữ liệu giữa chúng. Việc trao đổi dữ liệu giữa hai phân đoạn mạng được tổ chức một cách thông minh cho phép giảm các tắc nghẽn cổ chai tại các điểm kết nối. Các dữ liệu chỉ trao đổi trong một phân đoạn mạng sẽ không được truyền qua phân đoạn khác, giúp làm giảm lưu lượng trao đổi giữa hai phân đoạn. Bridge có thể nối nhiều hub lại với nhau như hình dưới đây.

5. Switch

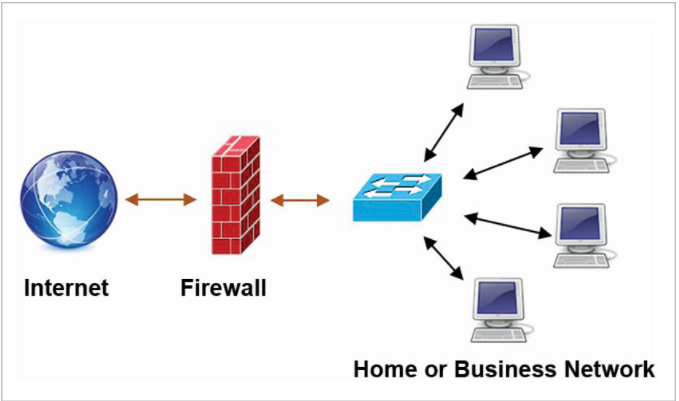
Công nghệ chuyển mạch là một công nghệ mới giúp làm giảm bớt lưu thông trên mạng và làm gia tăng băng thông. Bộ chuyển mạch cho LAN (LAN switch) được sử dụng để thay thế các Hub và làm việc được với hệ thống cáp sẵn có. Giống như bridges, switches kết nối các phân đoạn mạng và xác định được phân đoạn mà gói dữ liệu cần được gửi tới và làm giảm bớt lưu thông trên mạng. Switch có tốc độ nhanh hơn bridge và có hỗ trợ các chức năng mới như VLAN (Vitural LAN). Vlan có một chức năng quan trọng trong switch, đóng vai trò như một mutiswitch. Switch được coi là thiết bị hoạt động ở lớp 2 của mô hình OSI. Ngày nay có những thiết bị switch hoạt động ở lớp 3 chức năng giống như một router.

6. Router

Chức năng của Router là định tuyến, chuyển các gói dữ liệu từ mạng này sang mạng khác. Router hoạt động ở lớp 3 trong mô hình OSI. Có nhiều loại router từ rẽ đến các loại đắt tiền, tùy từng mô hình hệ thống mạng mà yêu cầu thiết bị router tương ứng. Router rất cần thiết cho hệ thống mạng.

# CHƯƠNG 2. FIREWALL

## Tường lửa Firewall là gì?



Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Nó kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Nghĩa là, chỉ những traffic phù hợp với chính sách được định nghĩa trong tường lửa mới được truy cập vào mạng, mọi traffic khác đều bị từ chối.

Bất kì máy tính nào kết nối tới Internet cũng cần có firewall, giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng. Việc có một “người gác cổng” như vậy để giám sát mọi việc xảy ra rất quan trọng bởi 2 lý do:

Thứ nhất, bất kì máy tính kết nối mạng nào thường kết nối vĩnh viễn với Internet.

Thứ hai, mỗi máy tính trực tuyến lại có một chữ ký điện tử riêng, được gọi là Internet Protocol address (hay còn gọi là địa chỉ IP): Nếu không có firewall hỗ trợ, nó chẳng khác gì chuyện bạn bật tất cả đèn lên và mở rộng cửa để đón trộm vào.

Một firewall được cấu hình chính xác sẽ ngăn chặn điều này xảy ra và giúp máy tính “ẩn” một cách hiệu quả, cho phép người dùng thoải mái thưởng thức những gì thế giới trực tuyến mang lại. Firewall không giống chương trình diệt virus. Thay vào đó, nó làm việc cùng với những công cụ này nhằm đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến.

## Firewall hoạt động như thế nào?

Firewall phân tích cẩn thận lưu lượng đến dựa trên các quy tắc được thiết lập trước và lọc lưu lượng đến từ các nguồn không an toàn hoặc đáng ngờ để ngăn chặn các cuộc tấn công. Firewall bảo vệ lưu lượng truy cập tại điểm vào của máy tính, được gọi là cổng, nơi thông tin được trao đổi với các thiết bị bên ngoài. Ví dụ: “Địa chỉ nguồn 192.168.1.1 được phép đến đích 192.168.2.1 qua cổng 22.”

Hãy coi địa chỉ IP là nhà và số cổng là phòng trong nhà. Chỉ những người đáng tin cậy (địa chỉ nguồn) mới được phép vào nhà (địa chỉ đích) sau đó nó được lọc thêm để những người trong nhà chỉ được phép truy cập vào một số phòng nhất định (cổng đích), tùy thuộc vào việc họ có phải là chủ sở hữu hay không , một đứa trẻ, hoặc một vị khách. Chủ sở hữu được phép vào bất kỳ phòng nào (bất kỳ cổng nào), trong khi trẻ em và khách được phép vào một nhóm phòng nhất định (cổng cụ thể).

## Ưu điểm của Firewall

Các chương trình Firewall đôi khi có thể được sử dụng làm máy chủ proxy. Bất cứ khi nào bạn truy cập một trang web, máy chủ proxy trước tiên sẽ nhận dữ liệu trước khi gửi đến máy tính của bạn. Thiết lập này có một số ưu điểm:

• Vì máy chủ giữ trang web không tương tác trực tiếp với máy tính của bạn nên nó làm giảm nguy cơ lây nhiễm vào máy tính của bạn bởi các trang web độc hại.

• Địa chỉ mạng trực tuyến của máy tính của bạn được ẩn đi.

• Phiên bản của trang web được lưu trữ trong bộ nhớ đệm của máy chủ proxy, vì vậy nó có thể tải nhanh hơn trong lần truy cập trang tiếp theo.

## Các loại Firewall

Firewall có thể là phần mềm hoặc phần cứng, tuy nhiên tốt nhất là bạn nên có cả hai. Firewall phần mềm là một chương trình được cài đặt trên mỗi máy tính và điều chỉnh lưu lượng truy cập thông qua số cổng và ứng dụng, trong khi Firewall vật lý là một phần thiết bị được cài đặt giữa mạng và cổng của bạn.

– Firewall tầng mạng • Bộ lọc gói tin

Firewall lọc gói, loại Firewall phổ biến nhất, kiểm tra các gói và cấm chúng đi qua nếu chúng không khớp với bộ quy tắc bảo mật đã thiết lập. Loại Firewall này kiểm tra địa chỉ IP nguồn và đích của gói tin. Nếu các gói phù hợp với quy tắc “được phép” trên Firewall, thì nó được tin cậy để vào mạng.

Firewall lọc gói có 2 loại:

• Firewall không trạng thái: Kiểm tra các gói độc lập với nhau và thiếu ngữ cảnh, khiến chúng trở thành mục tiêu dễ dàng cho tin tặc.

• Firewall giữ trạng thái: Ghi nhớ thông tin về các gói đã truyền trước đó và được coi là an toàn hơn nhiều.

– Firewall proxy

Lọc lưu lượng mạng ở cấp ứng dụng. Không giống như tường lửa cơ bản, proxy đóng vai trò trung gian giữa hai hệ thống đầu cuối. Máy khách phải gửi một yêu cầu tới tường lửa, nơi nó sau đó được đánh giá dựa trên một bộ quy tắc bảo mật và sau đó được phép hoặc bị chặn. Đáng chú ý nhất, tường lửa proxy giám sát lưu lượng truy cập cho các giao thức lớp 7 như HTTP và FTP, đồng thời sử dụng cả kiểm tra gói trạng thái và sâu để phát hiện lưu lượng độc hại.

– Firewall dịch địa chỉ mạng (NAT)

Cho phép nhiều thiết bị có địa chỉ mạng độc lập kết nối với internet bằng một địa chỉ IP duy nhất, giữ ẩn các địa chỉ IP riêng lẻ. Do đó, những kẻ tấn công quét mạng để tìm địa chỉ IP không thể nắm bắt được các chi tiết cụ thể, mang lại khả năng bảo mật cao hơn trước các cuộc tấn công. Firewall NAT tương tự như Firewall proxy ở chỗ chúng hoạt động như một trung gian giữa một nhóm máy tính và lưu lượng truy cập bên ngoài.

– Firewall tầng ứng dụng

Lọc các gói ở lớp mạng, lớp truyền tải và ứng dụng, so sánh chúng với các gói tin cậy đã biết. Đây là một dạng của firewall quản lý kiểm tra toàn bộ gói và chỉ cho phép chúng vượt qua nếu chúng vượt qua từng lớp riêng lẻ. Firewall này kiểm tra các gói để xác định trạng thái của giao tiếp (do đó là tên) để đảm bảo tất cả các giao tiếp được khởi tạo chỉ diễn ra với các nguồn đáng tin cậy.

# CHƯƠNG 3. CORE SWITCH (SWITCH LAYER 3)

Chuyển mach lõi nằm trong lớp trên cùng của mạng doanh nghiệp (lớp lõi), có chức năng như switch đường trục cho truy cập LAN và tập trung nhiều tập hợp vào lõi. Vì 2 lớp thấp khác dựa vào nó, chuyển mạch lớp lõi phải là một chuyển mạch switch layer 3 dự phòng và rất mạnh mẽ để đảm bảo truyền dữ liệu tốc độ cao và đáng tin cậy hiệu quả.3 Một tính năng trên phần cứng của nó là chuyển mạch lõi thường là một chuyển đổi quang để phù hợp với cáp quang tốc độ cao và các mô-đun thu phát sợi quang.

Trong lớp core switch, chuyển mạch là kết thúc và định tuyến đang bắt đầu. Core switch cũng được trang bị các tính năng định tuyến lớp 3. Tốc độ thông thường của chuyển mạch lõi ít nhất là switch 10Gbps để xử lý lưu lượng truy cập cao trên đường lên.

Nếu các loại Switch Access thông thường chỉ dùng để kết nối với các máy tính thì Core Switch lại khác. Chức năng của Switch Core là chịu tải lớn từ các tầng và thường loại này là các Switch Layer 3 có khả năng Routing giống như Router vậy.

Cũng bởi vậy mà giá thành của dòng sản phẩm này thường cao hơn rất nhiều lần so với Switch Access thông thường.

# CHƯƠNG 4. ACCESS SWITCH (SWITCH LAYER 2)

## Access Switch là gì?

Switch Access là thiết bị chuyển mạch chia cổng cho các hệ thống hạ tầng mạng cuối cùng, giữa các máy tính với nhau.

Là một chuyển mạch truy cập access switch trong lớp truy cập của mạng doanh nghiệp. Hoặc trong trường hợp cấu trúc liên kết mạng không được tham gia như văn phòng nhỏ và môi trường gia đình, các access switch thông thường chỉ có thể được sử dụng để kết nối thiết bị đầu cuối. Chuyển mạch truy cập như vậy trên thị trường thường đi kèm với switch layer cổng đồng với một vài cổng SFP hoặc SFP+.

Access switch truy cập tiết kiệm năng lượng yên tĩnh với các cổng phong phú này lý tưởng cho các SMB, phòng thí nghiệm, trường học và những nơi khác đòi hỏi hoạt động im lặng. Để cung cấp PoE cho hạ tầng của bạn, switch cấp nguồn PoE cũng được sử dụng rộng rãi như là access switch truy cập cho camera giám sát IP, điện thoại VoIP và WAP.

## Điểm khác biệt giữa Core Switch và Switch Access

Core Switch được sử dụng ở một vị trí khác hoàn toàn so với các Switch Access do đó chúng cũng sở hữu những tính năng vượt trội hơn hẳn.

Core Switch được coi là xương sống của hệ thống mạng, thông thường trong mô hình 3 lớp của Cisco thì hệ thống Core Switch nằm trên cùng của mô hình 3 lớp và chúng thực hiện vận chuyển lượng lớn dữ liệu, tốc độ cao mà vẫn đảm bảo được độ tin cậy nhất định.

Khi chọn thiết bị này bạn cũng cần lưu ý chọn các giao thức định tuyến có thời gian thiết lập thấp nhất và có kèm bảng định tuyến đơn giản nhất.

Đơn giản hơn Switch Access được sử dụng để cung cấp kết nối cổng đến từng Client trên một mạng, mọi người vẫn hay gọi phân khúc dòng sản phẩm này là Desktop Layer và đặc biệt phù hợp với các tính năng của lớp Access như:

- Tiếp tục thực hiện các access control và policy từ lớp Phân Phối.

- Tạo ra các collision domain riêng biệt nhờ dùng các switch chứ không dùng hub/bridge.

- Lớp truy cập phải chọn các bộ chuyển mạch có mật độ cổng cao đồng thời phải có giá thành thấp, kết nối đến các máy trạm hoặc kết nối tốc độ Gigabit (1000 Mbps) đến thiết bị chuyển mạch ở lớp phân phối.

# CHƯƠNG 5. MODEM

## Modem là gì?

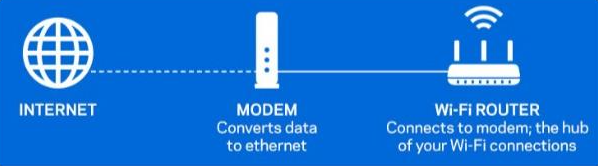
Modem là viết tắt của từ "modulator và demodulator" có nghĩa là thiết bị mã hóa và giải mã các xung điện. Modem là thiết bị giao tiếp với mạng lưới của các nhà cung cấp dịch vụ Internet (ISP) thông qua hệ thống cáp nối đồng trục, cáp quang hay đường dây điện thoại (DSL). Đây chính là cánh cổng để giúp bạn kết nối với internet quốc tế.



## Chức năng Modem

Modem có chức năng chuyển hóa các gói dữ liệu do ISP cung cấp thành kết nối Internet cho router hoặc các thiết bị có liên kết mạng khác qua địa chỉ IP.

## Cách hoạt động và chức năng của Modem



Như đã phân tích thì Modem nhận thông tin từ nhà cung cấp dịch vụ mạng Internet (ISP) thông qua đường dây điện thoại, cáp quang hoặc cáp đồng trục (tùy thuộc vào nhà cung cấp dịch vụ mạng) và chuyển đổi nó thành tín hiệu kỹ thuật số.

Vai trò của bộ định tuyến là đẩy tín hiệu này ra các thiết bị được kết nối, thông qua cáp Ethernet hoặc không dây Wi-Fi để tất cả các thiết bị của bạn có thể truy cập Internet.

# CHƯƠNG 6. ROUTER

## Router là gì?



Router (bộ định tuyến) là thiết bị mạng có chức năng chuyển tiếp gói dữ liệu giữa các mạng máy tính. Có thể hiểu, router thực hiện "chỉ đạo giao thông" trên Internet. Dữ liệu được gửi đi trên Internet dưới dạng gói, ví dụ như trang web hay email. Gói dữ liệu sẽ được chuyển tiếp từ router này đến router khác thông qua các mạng nhỏ, được kết nối với nhau để tạo thành mạng liên kết, cho đến khi gói dữ liệu đến được điểm đích. Quá trình chuyển gói dữ liệu như thế nào, làm sao để gói dữ liệu đến đúng "địa chỉ" bạn đọc sẽ được tìm hiểu kỹ hơn trong phần Quá trình định tuyến của Router.

Có nhiều kiểu router, từ đơn giản đến phức tạp. Các router thông thường được dùng cho kết nối Internet gia đình, còn nhiều router có mức giá “khủng” thường là business router, được dùng trong các doanh nghiệp, tổ chức lớn. Song, cho dù đắt hay rẻ, đơn giản hay phức tạp thì mọi router đều hoạt động với các nguyên tắc cơ bản như nhau.

Ở đây, chúng ta sẽ tập trung vào các router thông thường, quen thuộc với tất cả mọi người, nếu muốn biết thêm về business router thì bạn kéo xuống cuối bài viết nhé.

## Chức năng của router

Nói một cách đơn giản, router kết nối thiết bị trong một mạng bằng cách chuyển gói dữ liệu giữa chúng. Dữ liệu này có thể được gửi giữa các thiết bị hoặc từ thiết bị đến Internet. Router thực hiện nhiệm vụ này bằng cách gán địa chỉ IP cục bộ cho mỗi thiết bị trên mạng. Điều này đảm bảo gói dữ liệu đến đúng nơi, không bị thất lạc trong mạng.

Hãy tưởng tượng dữ liệu này như là một gói chuyển phát nhanh, nó cần một địa chỉ giao hàng để có thể gửi đến đúng người nhận. Mạng máy tính cục bộ giống như một con đường ngoại ô, chỉ biết vị trí tên đường mà không biết số nhà cụ thể trong thế giới rộng lớn (tức là World Wide Web) là không đủ.

Gói hàng này có thể gửi đến nhầm địa chỉ với lượng thông tin hạn chế. Do đó, router đảm bảo từng vị trí (thiết bị) đều có một số duy nhất để gói dữ liệu được gửi đến đúng vị trí.

Nếu cần trả lại dữ liệu cho người gửi hoặc gửi gói của riêng mình, router cũng thực hiện công việc này. Mặc dù nó xử lý từng gói riêng lẻ, nhưng nó thực hiện điều này rất nhanh, ngay cả khi nhiều thiết bị gửi dữ liệu cùng một lúc.

## Ưu và nhược điểm của Router

|  |  |
| --- | --- |
| **ƯU ĐIỂM** | **NHƯỢC ĐIỂM** |
| Giúp làm giảm lưu lượng mạng.  Giúp chia sẻ WiFi và kết nối mạng với nhiều máy.  Giảm tải dữ liệu bằng cách phân phối các gói dữ liệu. Cung cấp kết nối giữa các kiến trúc mạng khác nhau như Ethernet & Token ring,… | Tốc độ kết nối mạng bị giảm khi sử dụng nhiều máy tính .  Là thiết bị phụ thuộc (cần có modem mới chia sẻ được WiFi). |

## Modem và Router (Bộ định tuyến) khác gì nhau?

Về cơ bản, cả Modem và Router đều liên quan đến việc kết nối máy tính với internet, tuy nhiên giữa chúng tồn tại các điểm khác biệt nổi bật sau đây:

Cơ chế hoạt động

Modem: Chuyển đổi tín hiệu kỹ thuật số của máy tính, điện thoại… thành tín hiệu analog.

Router: Kiểm tra gói thông tin và xác minh đường dẫn của gói đó để truyền thành công đến thiết bị đích.

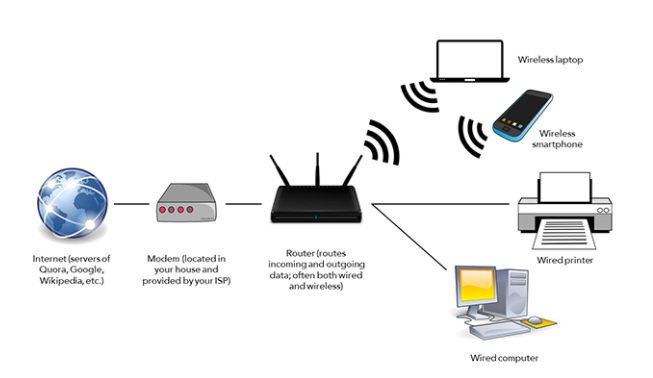
Tóm lại, router là để phần luồng các gói thông tin, gán IP cho các thiết bị trong hệ thống mạng. Tuy nhiên các thông tin truyền tải (trong cáp đồng, cáp quang) là analog (nó là dạng thông tin liên tục), nó khác với định dạng mà máy tính, điện thoại xử lý là digital (0 và 1) nên cần một thiết bị để đổi giữa hai thứ này. Các gói thông tin bạn gửi đi sẽ được modem chuyển từ digital sang analog để truyền đi trong thế giới mạng; khi các gói thông tin truyền từ thế giới mạng về máy bạn thì ngược lại, modem chuyển từ analog sang digital để máy tính, điện thoại đọc được thông tin.

Vị trí kết nối

Modem: Modem được kết nối trực tiếp với nhà mạng thông qua đường dây cáp quang, dây đồng… (hoặc cũng có thể không dây).

Router: Router được đặt giữa modem và hệ thống mạng. Mạng có thể là một tập hợp các máy tính hoặc một tập hợp gồm máy tính và switch, v.v… Modem và router được kết nối vật lý với nhau. Do đó, các thiết bị được kết hợp với router có thể truy cập Internet qua modem. Router có cổng Gigabit và Ethernet để kết nối với các thiết bị và hệ thống mạng khác. Các router phổ biến hiện nay cũng có WiFi để kết nối không dây.

Đôi khi Modem và Router được tích hợp chung vào một thiết bị, đó là cái “cục Wi-Fi” có thể cắm trực tiếp cáp quang vào mà nhà mạng trang bị cho bạn. Nhưng thường “cục” này khá hạn chế về khả năng phát Wi-Fi, vì vậy các bạn cũng nên sắm thêm một Router riêng để tận dụng tối đa băng thông.



Chế độ kết nối

Modem: Modem có các chế độ kết nối vật lý sau: Bán song công (Half Duplex), song công toàn phần ( Full Duplex), 4 dây và 2 dây.

Router: Các chế độ kết nối của Router là: User Execution, Administrative, Global Configuration.

Chức năng của Modem

Nén dữ liệu: Chức năng này nhằm giảm lượng thời gian gửi dữ liệu và giảm lượng lỗi trong tín hiệu..

Kiểm soát lưu lượng mạng

Truyền dữ liệu và sao lưu

Quản lý từ xa

Sửa lỗi: Khi thông tin được truyền giữa các modem, đôi khi nó có thể bị hỏng – nghĩa là các phần của dữ liệu bị thay đổi hoặc mất. Trong trường hợp này, modem cần sử dụng đến tính năng sửa lỗi để khắc phục nó.

Ưu/nhược điểm của Modem là gì?

Ưu điểm

Modem là con đường giao tiếp dữ liệu được sử dụng rộng rãi nhất bởi các ưu điểm mà nó mang lại như sau:

Chuyển đổi tín hiệu hiệu quả, nhanh chóng

Tốc độ truyền mạng cao

Cung cấp nhiều gói cước internet linh hoạt về giá cả, phù hợp với nhiều mục đích sử dụng khác nhau

Một số modem hoàn toàn tương thích với công nghệ fax. Tin nhắn fax có thể được gửi và nhận ngay lập tức bằng modem.

Nhược điểm

Bên cạnh các ưu điểm nêu trên thì Modem cũng có 1 số nhược điểm sau:

Một nhược điểm lớn của việc kết nối modem là nó có thể khiến máy tính của bạn dễ bị tin tặc và phần mềm độc hại tấn công. Tuy nhiên, để chống lại điều này, hầu hết các modem và bộ định tuyến đều có tường lửa tích hợp. Ngoài tường lửa, phần mềm bảo mật có thể được sử dụng cho mục đích này.

Khó khăn trong việc nâng cấp, phụ thuộc rất nhiều vào nhà cung cấp dịch vụ mạng ISP

Các dòng Modem bên ngoài thiếu tính di động.

Các dòng Modem DSL không khả dụng ở các vùng nông thôn hoặc vùng sâu vùng xa.

Một số loại Modem thịnh hành hiện nay

Modem được chia thành các loại cơ bản như sau:

Dựa theo Công suất định hướng

Chế độ bán song công (Half Duplex): Một modem bán song công cho phép truyền theo một hướng tại một thời điểm. Nếu modem được phát hiện trên đường truyền, tôi đưa ra dấu hiệu của nhà cung cấp dịch vụ đến cho DTE thông qua một tín hiệu điều khiển của giao diện kỹ thuật số của nó.

Chế độ song công toàn phần (Full Duplex): CMột modem song công đầy đủ cho phép truyền đồng thời theo cả hai hướng. Vì đường truyền vật lý cho mỗi hướng là riêng biệt, nên có thể sử dụng cùng một tần số sóng mang cho cả hai hướng.

Dựa theo Kết nối vào đường dây

Modem 4 dây: Trong kết nối 4 dây, một cặp dây được sử dụng cho sóng mang đi và cặp dây còn lại được sử dụng cho sóng mang đến. Do đó, cùng một tần số có thể được sử dụng để truyền ở cả hai đầu.

Modem dây: Modem 2 dây sử dụng cùng một cặp dây cho các nhà cung cấp dịch vụ đi và đến.

Dựa theo Phương tiện truyền dẫn

Modem vô tuyến: Được sử dụng để gửi dữ liệu qua một cặp kính một tín hiệu tần số vô tuyến.

Modem quang học: Được sử dụng để gửi dữ liệu qua một cặp sợi thủy tinh bằng cách sử dụng ánh sáng. Những modem như vậy sử dụng công nghệ hoàn toàn khác với những modem hoạt động trên dây chuyên dụng.

Modem quay số: chứa một mạch điện mô phỏng điện thoại. Tức là, modem có thể mô phỏng việc nhấc điện thoại, quay số hoặc treo điện thoại.

Dựa theo Chế độ truyền dẫn

Modem đồng bộ: Modem đồng bộ có thể xử lý một dòng bit dữ liệu liên tục nhưng yêu cầu tín hiệu đồng hồ. Để truyền đồng bộ các bit dữ liệu, DTE có thể sử dụng đồng hồ bên trong của nó và cung cấp đồng hồ tương tự cho modem.

Modem không đồng bộ: Modem không đồng bộ có thể xử lý các byte dữ liệu với các bit bắt đầu và dừng. Các xung thời gian bên trong được đồng bộ hóa lặp đi lặp lại với cạnh hàng đầu của xung bắt đầu

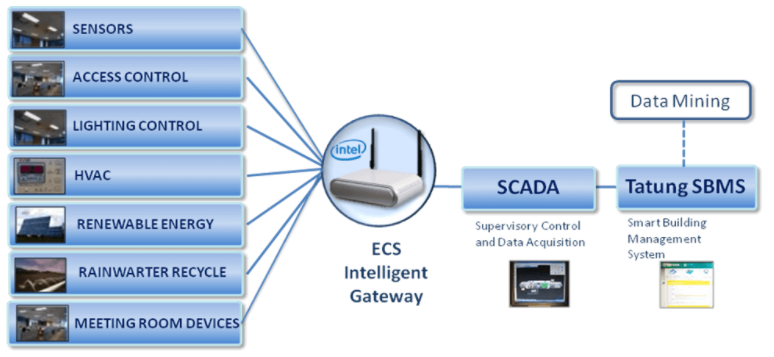
# CHƯƠNG 7. GATEWAY

## Gateway là gì?

Gateway là một nút mạng được sử dụng trong viễn thông nhằm kết nối hai mạng có giao thức truyền thông khác nhau có thể giao tiếp được với nhau. Gateway có vai trò xử lý đầu vào và ra của mạng vì tất cả dữ liệu phải đi qua hoặc giao tiếp với gateway trước khi được định tuyến. Trong hầu hết các mạng IP, lưu lượng duy nhất không đi qua gateway là lưu lượng truyền giữa các nút trên cùng một phân đoạn mạng cục bộ (LAN). Thuật ngữ default gateway hoặc network gateway cũng có thể được sử dụng để mô tả khái niệm trên.

Gateway được sử dụng chủ yếu trong các tình huống cá nhân hoặc doanh nghiệp muốn đơn giản hóa việc kết nối internet cho một thiết bị. Trong doanh nghiệp, một gateway cũng có thể hoạt động như một máy chủ proxy và tường lửa.

## gateway hoạt động



Tất cả các mạng đều có một ranh giới và giới hạn giao tiếp với các thiết bị được kết nối trực tiếp với nó. Do đó, nếu một mạng muốn giao tiếp với các thiết bị, nút hoặc mạng bên ngoài ranh giới đó, chúng yêu cầu chức năng của một gateway. Một gateway thường có những đặc trưng của sự kết hợp giữa router và modem.

Gateway hoạt động bên cạnh một mạng và quản lý tất cả dữ liệu được chuyển hướng nội bộ hoặc bên ngoài từ mạng đó. Khi một mạng muốn giao tiếp với mạng khác, gói dữ liệu được chuyển đến gateway và sau đó được chuyển đến đích thông qua đường truyền hiệu quả nhất. Ngoài dữ liệu định tuyến, một gateway cũng sẽ lưu trữ thông tin về đường dẫn nội bộ của mạng chủ và đường dẫn của bất kỳ mạng bổ sung nào gặp phải.

Gateway về cơ bản là bộ chuyển đổi giao thức, tạo điều kiện tương thích giữa hai giao thức và hoạt động trên bất kỳ lớp nào của mô hình kết nối hệ thống mở (OSI).

## Các loại gateway

Gateway có nhiều loại, nhiều định dạng và thực hiện nhiều nhiệm vụ khác nhau:

Web application firewalls (tường lửa web): loại này lọc lưu lượng truy cập đến và từ máy chủ web và xem xét dữ liệu lớp ứng dụng.

Cloud storage gateways (lưu trữ đám mây): loại này dịch các yêu cầu lưu trữ với các lệnh gọi API dịch vụ lưu trữ đám mây khác nhau. Nó cho phép các tổ chức tích hợp lưu trữ từ private cloud vào các ứng dụng mà không cần di chuyển vào public cloud.

API, SOA hay XML gateways: loại này quản lý lưu lượng truy cập vào và ra khỏi dịch vụ, kiến ​​trúc hướng dịch vụ vi mô hoặc dịch vụ web dựa trên nền tảng XML.

IoT gateways: loại này tổng hợp dữ liệu từ các thiết bị cấp hiện trường (cảm biến,..) trong môi trường IoT, chuyển đổi giữa các giao thức cảm biến và xử lý dữ liệu cảm biến trước khi gửi đi.

Media gateways: loại này chuyển đổi dữ liệu từ định dạng của một loại mạng sang định dạng cho một loại mạng khác.

Email security gateways (bảo mật email): loại này ngăn chặn việc truyền các email vi phạm chính sách của công ty hoặc chuyển thông tin với mục đích xấu.

VoIP trunk gateways: loại này tạo sự thuận lợi cho việc sử dụng các thiết bị dịch vụ điện thoại cũ đơn thuần, chẳng hạn như điện thoại cố định và máy fax, với mạng thoại qua IP (VoIP).

# CHƯƠNG 8. BRIDGE

## Bridge là gì?

## Bridge trong mạng máy tính, còn được gọi là switch Layer 2, là một loại thiết bị mạng, được sử dụng để tách mạng thành các phần. Trong mô hình OSI, một bridge hoạt động ở layer-2, tức là lớp liên kết dữ liệu. Chức năng chính của thiết bị này là kiểm tra lưu lượng đến và kiểm tra xem nên lọc hay chuyển tiếp lưu lượng đó.

## Đặc điểm

• Bridge là một thiết bị mạng lớp 2 hai cổng ban đầu được sử dụng để kết nối các phân đoạn mạng khác nhau. Hai cổng của bridge đều có một kênh chuyển mạch độc lập, thay vì chia sẻ một bus nối liền, miền xung đột có thể bị cô lập. Cầu có hiệu suất tốt hơn trung tâm và mỗi cổng trên trung tâm chia sẻ cùng một xe buýt bảng nối đa năng. Sau đó, cây cầu được thay thế bằng một bộ chuyển mạch có nhiều cổng hơn và cũng có thể cô lập các miền xung đột.

• Bridge giống như một bộ lặp thông minh. Bộ lặp nhận tín hiệu từ một cáp mạng, khuếch đại chúng và gửi chúng đến cáp tiếp theo. Trong khi đó, cây cầu nhạy cảm hơn với thông tin được tải lên từ cấp độ. Cầu nối là một công nghệ chuyển tiếp các khung, có thể cô lập các xung đột theo các khối MAC. Cầu nối nhiều phân đoạn của mạng ở lớp liên kết dữ liệu.

## Ưu điểm của Bridge

• Lọc lưu lượng. Cầu nối mạng có thể được sử dụng trên một phân đoạn mạng của mạng cục bộ. Lượng thông tin giữa các máy trạm được giới hạn trong phân đoạn mạng này và sẽ không đi qua cầu nối đến các phân đoạn mạng khác.

• Mở rộng phạm vi vật lý và tăng số lượng máy trạm tối đa trong toàn bộ mạng LAN.

• Các lớp vật lý khác nhau có thể được sử dụng và các mạng cục bộ khác nhau có thể được kết nối với nhau.

• Cải thiện độ tin cậy. Nếu mạng LAN lớn hơn được chia thành nhiều mạng LAN nhỏ hơn và lượng thông tin trong mỗi mạng LAN nhỏ cao hơn đáng kể so với lượng thông tin giữa các mạng thì hiệu suất của toàn bộ mạng kết nối sẽ tốt hơn.

## Nhược điểm của cầu

• Vì cầu đầu tiên phải lưu trữ và tra cứu bảng trạm cho khung đã nhận, sau đó chuyển tiếp nó, điều này làm tăng độ trễ.

• Không có chức năng điều khiển luồng trong lớp con MAC. Khi tải trên mạng nặng, hiện tượng tràn có thể xảy ra do không đủ dung lượng lưu trữ của bộ đệm cầu nối, dẫn đến mất khung hình.

• Khi các phân đoạn mạng có các lớp con MAC khác nhau được bắc cầu với nhau, cây cầu phải sửa đổi nội dung của các trường nhất định của khung trước khi chuyển tiếp một khung để đáp ứng các yêu cầu của lớp con MAC khác và tăng độ trễ.

• Cầu nối mạng chỉ phù hợp với mạng cục bộ nơi số lượng người dùng không quá nhiều (không quá vài trăm) và lượng thông tin không quá lớn, nếu không có thể xảy ra bão phát sóng lớn.

## Sự khác biệt giữa Bridge và Switch

|  |  |
| --- | --- |
| **Bridge** | **Switch** |
| Chuyển tiếp gói trong bridge được thực hiện bằng phần mềm. Vì vậy, bridge là dựa trên phần mềm. | Chuyển tiếp gói trong Bộ chuyển mạch được thực hiện bằng ASICS (Mạch tích hợp dành riêng cho ứng dụng). Do đó, một công tắc dựa trên phần cứng. |
| Phương thức chuyển đổi của một Bridge là lưu trữ và chuyển tiếp. | Phương thức chuyển đổi của Switch có thể được lưu trữ và chuyển tiếp, cắt qua hoặc không phân mảnh. |
| Một Bridge chỉ có 2 cổng. | Một bộ chuyển mạch có thể xử lý nhiều cổng. |
| Cầu nối là một thiết bị kết nối hai mạng LAN và kiểm soát luồng dữ liệu giữa chúng. | Switch là một thiết bị mạng tìm hiểu máy nào được kết nối với cổng của nó bằng cách sử dụng Địa chỉ IP của thiết bị. |
| Cầu chia miền va chạm thành hai phần. Các cầu nối có thể tạo miền xung đột nhưng không tạo miền quảng bá. | Công tắc được sử dụng để kết nối các trạm làm việc hoặc hệ thống máy tính. Nếu có 20 máy trạm được kết nối với một bộ chuyển mạch thì sẽ có miền xung đột riêng cho mỗi nút. |

## Sự khác biệt giữa Bridge và Router

Sự khác biệt chính giữa bridge và router là bridge quét địa chỉ MAC của thiết bị. Mặt khác, router quét địa chỉ IP của thiết bị.

|  |  |  |
| --- | --- | --- |
| **STT** | **BRIDGE** | **ROUTER** |
| 1. | Bridge hoạt động trong lớp liên kết dữ liệu. | Trong khi router hoạt động ở lớp mạng. |
| 2. | Thông qua bridge, dữ liệu hoặc thông tin không được lưu trữ và gửi dưới dạng gói tin. | Trong khi thông qua router, dữ liệu hoặc thông tin không được lưu trữ và gửi dưới dạng gói tin. |
| 3. | Chỉ có 2 cổng trong bridge. | Trong khi có hơn 2 cổng trong router. |
| 4. | Bridge kết nối hai mạng lan khác nhau. | Trong khi router được sử dụng bởi LAN cũng như MAN để kết nối. |
| 5. | Trong bridge, bảng định tuyến không được sử dụng. | Trong khi trong router, bảng định tuyến được sử dụng. |
| 6. | Bridge hoạt động trên một broadcast domain. | Trong khi router hoạt động trên nhiều hơn một broadcast domain. |
| 7. | Bridge rất dễ cấu hình. | Trong khi router khó thiết lập và cấu hình. |
| 8. | Bridge tập trung vào địa chỉ MAC. | Trong khi router tập trung vào địa chỉ IP. |
| 9. | Bridge tương đối rẻ. | Trong khi router là thiết bị tương đối đắt tiền. |
| 10. | Bridge tốt cho việc phân đoạn mạng và mở rộng mạng hiện có. | Trong khi router rất phù hợp để tham gia các mạng từ xa. |

# CHƯƠNG 9. REPETER

## Repeater là gì

Repeater là bộ khuếch đại tín hiệu, đảm bảo từ đó có thể truyền tín hiệu đi xa hơn nhưng không bị yếu đi.



Repeater là thiết bị ở lớp 1 (Physic Layer) trong mô hình OSI. Khi chúng ta sử dụng Repeater, tín hiệu vật lý ở đầu vào sẽ được repeater thu nhận, sau đó được khuếch đại, từ đó cung cấp tín hiệu ổn định và mạnh hơn cho đầu ra, để có thể đến được những vị trí xa hơn. Nếu bạn muốn đảm bảo tín hiệu với những khu vực văn phòng làm việc lớn, cách xa nhau thì bạn có thể dùng Repeater để khuếch đại tín hiệu.

Repeater còn được gọi với tên khác là bộ mở rộng sóng wifi, bộ kích sóng wifi, mạng lặp wifi.

## Ưu điểm của Repeater

Ưu điểm chắc chắn là giúp sóng wifi mạnh hơn, sóng wifi đó mạnh lên và phát wifi ra cho các thiết bị khác sử dụng với độ ổn định và tín hiệu cao hơn. Repeater Wifi lắp đặt nhanh chóng, không cần phải kéo dây rờm rà, phù hợp với nhà cao tầng, chủ nhà không muốn thay đổi kết cấu, khoan đục, dây nhợ lòng thòng

## Nhược điểm Repeater

Tùy loại Repeater mà có nhược điểm riêng, ví dụ Repeater wifi thì tùy thuộc vào sóng nhận.Với những sóng wifi nguồn mà chất lượng kém thì rất có thể kéo theo thiết bị thu sóng cũng sẽ bị hạn chế theo. Do vậy bạn nên lắp đặt thử nhiều vị trí để có một chất lượng sóng phát ra tốt nhất.

## Sự khác nhau giữa hub và repeater

|  |  |
| --- | --- |
| **Hub** | **Repeater** |
| Hub hoạt động trong tầng vật lý | Bộ lặp hoạt động trong vật lý và cũng trong lớp thứ ba của Hub hoạt động ở lớp vật lý.  osi, tức là, lớp điều khiển mạng. |
| Nó nhận đầu vào từ một công và phát nó đến một thiết hoặc bị khác được kết nối trong mạng. | Nó được sử dụng để sao chép hoặc tạo lại tín hiệu hoặc thông tin. |
| Một trung tâm hoạt động như một điểm kết nối trong mạng. | Bộ lặp không thông minh trong việc định tuyến so với cầu và chuyển mạch. |

# CHƯƠNG 10. WIRELESS

## Wireless là gì?

Wireless hay mạng không dây, ngày nay chúng đã trở thành một phần không thể thiếu trong cuộc sống khi bạn thấy chúng xuất hiện trong hầu khắp các lĩnh vực đời sống: Từ doanh nghiệp, trường học, các địa điểm giải trí và ngay cả trong từng hộ gia đình. Nhờ sự tiện lợi của mình, mạng không dây đã dần thay thể kết nối truyền thống bằng cáp truyền thống.

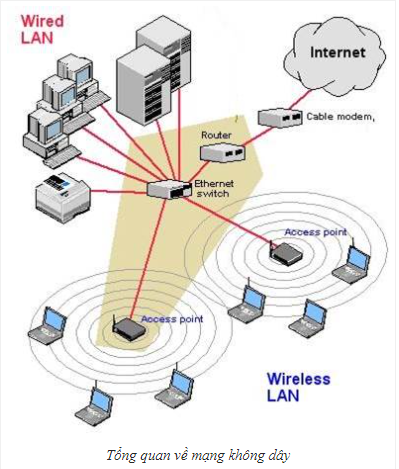
## Mạng không dây là gì?

Mạng không dây là một hệ thống các thiết bị được nhóm lại với nhau, có khả năng giao tiếp thông qua sóng vô tuyến thay vì các đường truyền dẫn bằng dây.

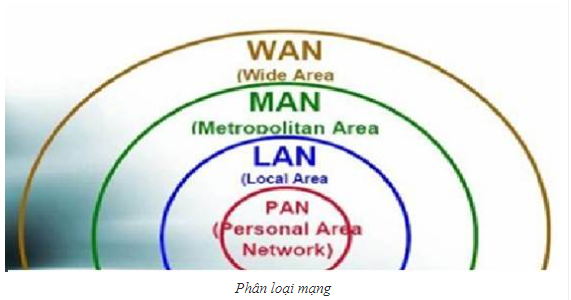
Đây là mạng dựa trên chuẩn IEEE 802.11 nên đôi khi nó còn được gọi là mạng 802.11 network Ethernet để nhấn mạnh rằng mạng này dựa trên mạng Ethernet truyền thống.

Wifi là gì?

Wi-Fi (Wireless Fidelity) là một tên gọi khác rất quen thuộc khi nói về mạng không dây.



## Phân loại mạng không dây



• WPAN: Mạng vô tuyến cá nhân

• WLAN: Mạng vô tuyến cục bộ

• WMAN: Mạng vô tuyến đô thị

• WWAN: Mạng vô tuyến diện rộng

• WRAN: Mạng vô tuyến khu vực

WPAN là gì?

WPAN là mạng vô tuyến cá nhân. Nhóm này bao gồm các công nghệ vô tuyến có vùng phủ nhỏ tầm vài mét đến hàng chục mét tối đa

Mục đích nối kết các thiết bị ngoại vi như máy in, bàn phím, chuột, đĩa cứng, khóa USB, đồng hồ, với điện thoại di động, máy tính. Các công nghệ trong nhóm này bao gồm: Bluetooth, Wibree, ZigBee, AWB, Wireless USB, EnOcean...

Đa phần các công nghệ này được chuẩn hóa bởi IEEE, cụ thể là nhóm làm việc (Working Group) 802.15. Do vậy các chuẩn còn được biết đến với tên như IEEE 802.15.4 hay IEEE 802.15.3.

WLAN là gì?

WLAN là mạng vô tuyến cục bộ. Nhóm này bao gồm các công nghệ có vùng phi tầm vài trăm mét. Nôi bật là công nghệ Wifi với nhiều chuẩn mở rộng khác nhau thuộc gia đình 802.11 a/b/g/hi...

WMAN là gì?

WMAN là mạng vô tuyến đô thị. Đại diện tiêu biểu của nhóm này chính là WiMAX ( Worldwide Interoperability for Microwave Access) hệ thống truy cập không dây bằng rộng. Vùng phủ sóng của nó sẽ tầm vài km (tầm 4-5km tối đa).

WWAN là gì?

WWAN là mạng vô tuyến diện rộng. Nhóm này bao gồm các công nghệ mạng thông tin di động như:

• UMTS(Universal Mobile Telecommunications Systems) • GSM(Global System for Mobile Communication) • CDMA2000(là một tiêu chuẩn công nghệ di động họ 3G)...

Vùng phủ của nó cũng tầm vài km đến tầm chục km.

WRAN là gì?

WRAN là mạng vô tuyến khu vực. Nhóm này đại diện là công nghệ 802.22 đang được nghiên cứu và phát triển bởi IEEE. Vùng phủ có nó sẽ lên tầm 40-100km. Mục đích là mang công nghệ truyền thông đến các vùng xa xôi hẻo lánh, khó triển khai các công nghệ khác.

Ưu điểm của Wireless Lan

• Chủ yếu ứng dụng trong mô hình mạng nhỏ.

• Có thể triển khai ở những nơi không thuận tiện về địa hình, không ổn định, không triển khai mạng có dây được.

• Khả năng thiết lập các thông số truyền sóng vô tuyến ngày càng đơn giản hơn.

• Lắp đặt, triển khai dễ dàng, đơn giản, nhanh chóng.

• Dễ thay đổi, nâng cấp, phát triển.

• Tuy giá thiết bị cao hơn với mạng có dây nhưng hiện nay có xu hướng giảm.

Nhược điểm của Wireless LAN

• Với mô hình lớn phải kết hợp với mạng có dây.

• Bị ảnh hưởng bởi các yếu tố bên ngoài như môi trường truyền sóng, can nhiễu do thời tiết.

• Chịu nhiều cuộc tấn công đa dạng, phức tạp, nguy hiểm của những kẻ phá hoại vô tình và cố tình, nguy cơ cao hơn mạng có dây.

• Yếu tố ảnh hưởng tới sức khỏe con người còn đang nghiên cứu.

Ứng dụng mạng không dây

• Cung cấp khả năng truy cập mạng một cách linh hoạt.

• Nối mạng giữa các tòa nhà cách xa nhau.

• Cung cấp dịch vụ truy cập mạng không dây – mở rộng mạng.

• Sử dụng cho văn phòng quy mô nhỏ , trường học, bệnh viện, nơi công cộng khác...

• Sử dụng trong tình huống cần thiết lập mạng trong thời gian ngắn.

# CHƯƠNG 11. MODULE QUANG

## SFP Module là gì ?

Module quang SFP hay còn được gọi bằng các tên gọi khác như là SFP transceiver, module SFP hay module quang là loại module được dùng cho các thiết bị như switch, converter, DSLAM, SDH có cổng (khe, slot) theo chuẩn SFP.

## Chuẩn SFP là gì?

SFP là viết tắt của chuẩn “Small Form Factor” .Small Form Factor (SFP) là thiết bị thu phát kích thước nhỏ gọn, có thể “gắn nóng” trực tiếp và sử dụng cho viễn thông cũng như truyền thông dữ liệu. Một đầu của SFP được gắn vào các thiết bị như là media converter, switch, router và thiết bị tương tự; đầu còn lại gắn cáp quang. Thiết bị này là một giao thức chuẩn phổ biến được hỗ trợ bởi các nhà sản xuất viễn thông và thiết bị mạng.

## SFP Module có những loại nào?

Cũng như bộ chuyển đổi quang điện – converter quang, SFP module cũng có rất nhiều loại và thường được chia làm 4 loại chính theo từng đặc điểm như ở bảng sau:

|  |  |
| --- | --- |
| **Đặc điểm** | **Phân loại** |
| Tốc độ | 155M (10/100 Mbps)  1.25G (1000 Mbps)  10G, 40G, 100G,… |
| SDH | STM-1  STM-4  STM-16 |
| Loại cáp quang | Multi mode (đa mốt)  Single mode (đơn mốt) |
| Số sợi quang | 2 sợi quang (2 FO/ dual fiber)  1 sợi quang (1 FO/ single fiber) |

## Tìm hiểu về chức năng DDM

DDM là chức năng “chẩn đoán, giám sát, cung cấp” cho người dùng các thông tin quan trọng liên quan đến tình trạng của các tín hiệu nhận và truyền trong quá trình hoạt động. Cách tiếp cận này hỗ trợ tối đa người dùng trong việc phát hiện lỗi cũng như rút ngắn được thời gian sửa chữa.

## Module quang dùng để làm gì?

Phần lớn các module quang thường có chức năng là thiết bị kết nối và chuẩn đoán, giám sát cũng như cung cấp cho người dùng các thông tin vô cùng quan trọng liên quan đến tình trạng hoạt động tín hiệu của hệ thống. Trong điều kiện tiêu chuẩn, thiết bị này có thể hỗ trợ với khoảng cách tối đa lên tới 140km.

Nhờ có các tính năng nổi bật mà Module hoàn toàn có thể hỗ trợ người dùng cô lập và nhanh chóng phát hiện các lỗi từ đó có để đưa ra các phương án xử lý một cách dễ dàng và tiết kiệm thời gian nhất.

Module quang còn có hệ thống chuẩn đoán các thông số kĩ thuật đảm bảo độ chính xác trong công tác thu, phát hiện xử lý công suất máy.

Thông thường kết quả của giá trị thiết bị sẽ nằm ở một trong các thông số như: từ trở kháng khuếch đại Trans, điện áp từ trường tương tự; trình điều khiển laser, Ở bộ khuếch đại sau… tuỳ thuộc trong từng trường hợp để xác định module quang dùng để làm gì . Sau đó các kĩ sư sẽ sử dụng một vật dụng ADC để số hóa mọi giá trị và xử lý dữ liệu thu về được.

# CHƯƠNG 12. BỘ CHUYỂN ĐỔI QUANG ĐIỆN

## Module quang là gì?

Module quang hay còn gọi là Transceiver, SFP – Small Form Factor là một thiết bị chuyển tín hiệu quang sang tín hiệu số. Thiết bị này được thiết kế để sử dụng cho đầu nối (connector) dạng small form factor (SFP) có khả năng cắm nóng và hỗ trợ các chuẩn SONET, Gigabit Ethernet, Fibre Channel, và nhiều chuẩn truyền dẫn khác . Nó được sử dụng cho các thiết bị như switch, converter, router,…có cổng (khe) theo chuẩn SFP hoặc QSFP. Ngày nay module quang được sử dụng phổ biến trong ngành viễn thông và được nhiều nhà sản xuất thiết bị mạng phát triển.

## Sự hình thành và phát triển

Module quang (Transcerver) được hình thành và phát triển theo dòng chảy của công nghệ. Ngày trước khi công nghệ đồng vẫn còn được sử dụng người ta chỉ cần dùng các đầu RJ45+ cat5,6 để kết nối các thiết bị mạng với nhau. Ngày nay, công nghệ đồng không còn đáp ứng được nhu cầu sử dụng của con người nữa. Công nghệ quang ra đời và phát triển dần thay thế công nghệ đồng. Công nghệ quang giúp con người giải quyết nhu cầu sử dụng internet tốc độ cao của mình, nhưng nó kéo theo một vấn đề kết nối giữa dây quang với các cổng uplinks và downlink của các thiết bị mạng, vì vậy SFP ra đời để giải quyết vấn đề này.



## Phải chăng SFP nào cũng như nhau?

Câu trả lời là không. Có 3 cách phân loại SFP:

Dùng loại cáp quang: multi mode hay single mode

Theo tốc độ: 1.25Gbs (SFP), 10Gbs (SFP+, XFP), 16G, 25G (SFP25), QSFP 40G hay QSFP 100G

Theo số lượng dây quang: 1 sợi hay 2 sợi

# CHƯƠNG 13. CÁC VẤN ĐỀ LIÊN QUAN ĐÉN IP

## ****IP là gì?****

IP hay Internet Protocol là địa chỉ số có trên mọi thiết bị kết nối mạng để chia sẻ dữ liệu với nhau giao thức kết nối Internet.

IP có công dụng điều hướng dữ liệu. Được dùng sử dụng bởi các máy chủ nguồn và đích để truyền dữ liệu trong mạng máy tính. Hãy hình dung địa chỉ IP tương tự như địa chỉ nhà riêng, hoặc địa chỉ mà các doanh nghiệp cung cấp để người khác có thể nhận diện. Vì vậy, khi bạn truy cập email hay website, dù IP được cung cấp không gắn trực tiếp với thiết bị thì những con số này vẫn tiết lộ một vài thông tin về bạn.

## IP dùng để làm gì?

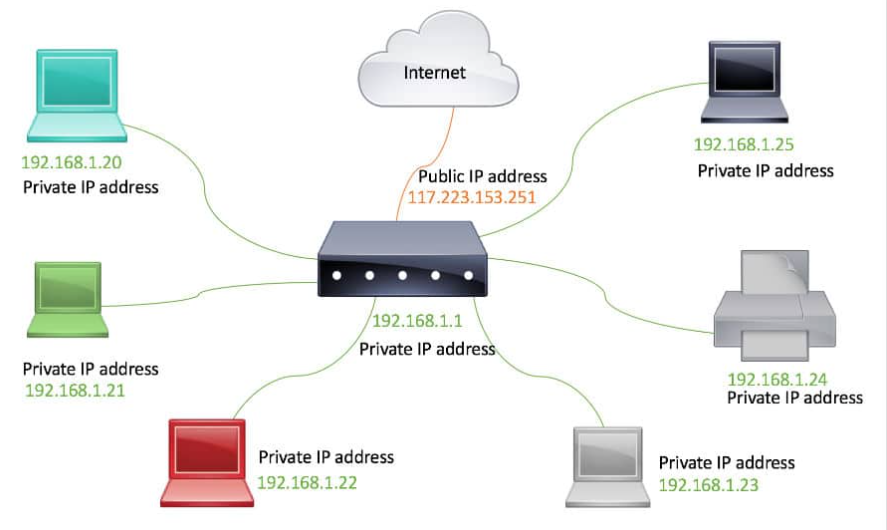
IP sẽ giúp các thiết bị trên mạng Internet có thể phân biệt, chia sẻ và giao tiếp với nhau. Nó sẽ cung cấp danh tính cho các thiết bị khi chúng kết nối mạng tương tự như địa chỉ doanh nghiệp có vị trí cụ thể.

## Ưu và nhược điểm của địa chỉ IP là gì?

IP là giao thức kết nối thông minh giúp truy cập mạng lưới internet dễ dàng hơn. Đồng thời IP giúp quản lý hệ thống mạng của người dùng đơn giản hơn. Mỗi máy tính, thiết bị đều có một địa chỉ IP riêng biệt.

IP tuy có nhiều ưu điểm, song cũng tồn tại những nhược điểm. Trong đó, người dùng sẽ dễ dàng bị khai thác các thông tin cá nhân thông qua địa chỉ IP nếu bị hacker xâm nhập. Ngoài ra, mọi hoạt động truy cập của người dùng đều sẽ bị để lại địa chỉ IP.

## Phân loại IP



Tính đến nay có 4 loại hình IP thông dụng. Mỗi loại IP có thể là địa chỉ IPv4 hoặc địa chỉ IPv6. Dưới đây là chi tiết về 4 loại IP: IP Private, IP Public, IP tĩnh, IP động

* IP Private là gì?

IP private còn được gọi là IP nội bộ. Đây là dãy các IP chỉ được sử dụng cho những máy tính thuộc một mạng nội bộ như mạng nhà trường, công ty, tổ chức…

IP Private hỗ trợ các máy tính trong hệ thống kết nối với nhau. Chúng sẽ không kết nối trực tiếp với các máy tính bên ngoài hệ thống. IP Private được thiết lập thủ công hoặc do router thiết lập tự động.

* IP Public là gì?

IP Public là địa chỉ IP cộng đồng. Đây là IP sử dụng trong mạng gia đình hoặc doanh nghiệp để kết nối Internet.

Địa chỉ IP Public là yếu tố thiết yếu với bất kỳ phần cứng mạng có thể truy cập công khai nào. Ví dụ như router gia đình hoặc các server. Các thông số của IP Public cần được ghi nhớ chính xác. Đặc biệt khi thuê máy chủ để thiết lập kết nối chính xác cho website của mình.

* IP tĩnh là gì?

IP tĩnh là địa chỉ được định cấu hình thủ công cho thiết bị. IP này được gọi “tĩnh”do nó không hề thay đổi khác với DHCP thay đổi mỗi khi mất và kết nối lại.

Địa chỉ IP tĩnh giúp kết nối Internet nhanh chóng không cân đợi cấp phát IP. IP tĩnh còn giúp tăng tốc độ tải website, download file torrent. IP tĩnh giữ đường truyền ổn định với máy tính nằm trong hệ thống mạng nội bộ.

Bất lợi lớn của IP tĩnh chính là cấu hình thủ công. Mọi thiết bị đều yêu cầu thiết lập địa chỉ IP tĩnh và cấu hình đúng router để giao tiếp với thiết bị đó. Điều này gây mất rất nhiều thời gian cho bạn khi thiết lập.

* IP động là gì?

IP động là IP được gán tự động cho từng kết nối hoặc node của mạng. Ví dụ như điện thoại thông minh, máy tính,……

IP động hoạt động ngược lại so với IP tĩnh bằng cách sử dụng phương thức DHCP. Việc gán địa chỉ IP tự động này được thực hiện bằng giao thức DHCP và luôn được thay đổi mỗi khi bạn ngắt và kết nối lại.

IP động mang nhiều ưu điểm như: tính linh hoạt3, dễ cài đặt và dễ quản lý. Số lượng thiết bị kết nối sẽ ít bị giới hạn với IP động. Vì sao vậy? Những thiết bị không cần thiết sẽ ngắt kết nối và giải phóng IP cho các thiết bị mới sử dụng.

IP động được ứng dụng rộng rãi nhất. Nó tồn tại khi các hộ gia đình sử dụng IP được gán tự động từ router. Tuy nhiên, mọi thiết bị sẽ yêu cầu IP của router để máy tính truy cập vào mạng. Địa chỉ IP động của router sẽ luôn thay đổi theo định kỳ. Điều này dẫn đến việc xung đột IP khi các máy mới vào sử dụng IP của máy đang dùng trong hệ thống mạng.

## ****Subnet Mask là gì?****

Subnet mask là dãy số có dạng 32 hay 128 bit. Subnet Mask dùng để phân đoạn địa chỉ IP đang tồn tại trên mạng TCP/IP. Từ đó chia địa chỉ đó thành địa chỉ network và địa chỉ host riêng biệt. Quá trình này có thể chia nhỏ host của IP thành các subnet phụ để định tuyến lưu lượng trong các subnet lớn hơn.

Subnet mask có tất cả các bit network. Subnet bằng 1, các bit host đều bằng 0.

Tất cả các máy trong cùng một hệ thống mạng phải có cùng subnet.

Bộ định tuyến dùng phép logic AND để phân biệt được các subnet (mạng con).

## IPv4 là gì?

IPv4 hay Internet Protocol version 4 là bản thứ tư của các giao thức Internet. IP – Internet Protocol là một giao thức của chồng giao thức. Giao thức này còn gọi là TCP/IP thuộc về lớp Internet. Tương ứng với lớp thứ ba (lớp network) của mô hình OSI.

Địa chỉ IPv4 thường được viết theo dạng gồm bốn nhóm số thập phân. Nó được ngăn cách nhau bằng dấu chấm. Do 32 bit chia đều cho bốn nhóm số. Mỗi nhóm sẽ gồm 8 bit dữ liệu. Chúng thường gọi là một oc-tet, nghĩa là bộ 8-bit nhị phân. Giá trị của mỗi oc-tet sẽ gồm 2^8 = 256 giá trị nằm trong khoảng từ 0 (8 bits toàn 0) đến 255 (8 bits toàn 1).

## IPv6 là gì?

IPv6 là phiên bản thứ 6 cũng là phiên bản mới nhất của IP. IPv6 hay Internet Protocol version 6 là giao thức truyền thông được IETF phát triển. IPv6 dùng để giải quyết vấn đề cạn kiệt địa chỉ IPv4. Nó mang nhiều cải tiến và được ứng dụng rộng rãi hơn so với IPv4.