

Tài liệu đọc

Hỗ Trợ Công Nghệ Thông Tin

Khóa 2: Bit và Byte của máy tính

Phần 1: Tài liệu đọc bổ trợ

[Bài đọc 1](#)

Giới thiệu mạng máy tính

[1.1 Mạng máy tính cơ bản](#)

Mô tả cách máy tính kết nối trong mạng
Mạng có dây và mạng không dây
Mô tả đặc điểm của các mạng LAN, MAN, WAN, VLAN
Mô tả một số giao thức mạng căn bản

[1.2 Tổng quan mô hình mạng](#)

Giới thiệu về mô hình mạng 5-tầng và mô hình OSI
So sánh giống và khác biệt giữa các mô hình

[Bài đọc 2](#)

Thiết bị mạng

[2.1 Cáp mạng](#)

Giới thiệu về các loại cáp mạng như cáp đồng, cáp quang, cáp xoắn đôi
Mô tả về hiện tượng nhiễu xuyên âm

[2.2 Thiết bị mạng](#)

Mô tả các thiết bị chính được sử dụng trong kết nối mạng gồm Hub, Repeater, Bridge, Switch, Router
Giải thích về miền đưng độ

[2.3 Giắc cắm mạng](#)

Mô tả cấu tạo giắc cắm RJ45, cách thức bấm dây mạng
Các tín hiệu trạng thái

[Bài đọc 3](#)

Tầng Vật lý

[3.1 Chức năng và dịch vụ trên tầng vật lý](#)

	3.2 Giao tiếp trong tầng vật lý Mô tả về đơn công Mô tả về song công Mô tả về bán song công
Bài đọc 4	Tầng liên kết dữ liệu
	4.1 Chức năng và dịch vụ trên tầng liên kết dữ liệu 4.2 Địa chỉ vật lý (MAC) 4.3 Các kiểu định tuyến Unicast Multicast Broadcast 4.4 Cấu trúc khung dữ liệu trong tầng liên kết
Bài đọc 5	Tầng mạng
	2.1 Chức năng và dịch vụ trên tầng mạng 2.2 Cấu trúc địa chỉ Mô tả về IPv4 và IPv6 Mô tả các lớp địa chỉ IP (A, B, C, D, E) Không gian địa chỉ không thể định tuyến Cấp phát địa chỉ IP với CIDR Giao thức phân giải địa chỉ 2.3 Cấu trúc gói tin tầng mạng (IP datagram) 2.4 Cách thức chia mạng con Định danh mạng con (subnet ID) Mặt nạ mạng con (subnet mask) 2.5 Cách thức định tuyến Định tuyến Bảng định tuyến Số hiệu mạng ASN Các giao thức định tuyến
Bài đọc 6	Tầng vận chuyển
	6.1 Chức năng và vai trò của tầng vận chuyển 6.2 Gói tin TCP segment 6.3 Giao thức trên tầng vận chuyển Giao thức hướng kết nối (TCP) và phi kết nối (UDP) Cơ chế bắt tay 3 bước

	<p>6.4 Cổng và socket Cổng và số hiệu socket TCP socket và các trạng thái</p> <p>6.5 Giới thiệu về tường lửa (firewall)</p>
Bài đọc 7	Tầng ứng dụng
	<p>7.1 Vai trò và đặc điểm của tầng ứng dụng Vai trò và giao thức So sánh tầng ứng dụng mô hình OSI</p> <p>7.2 Quá trình thực thi của 5 tầng</p>
Bài đọc 8	Hệ thống phân giải tên miền
	<p>8.1 Tên miền và hệ thống phân giải tên miền Tên miền và hệ thống phân giải Cấu tạo tên miền</p> <p>8.2 Máy chủ DNS Máy chủ DNS và phân loại Phối hợp giữa các máy chủ DNS Giao thức của máy chủ DNS Bản lưu thông tin trên máy chủ DNS</p> <p>8.3 Giao thức DHCP DHCP và chiến lược cấp phát địa chỉ IP Tìm kiếm máy chủ DHCP</p>
Bài đọc 9	Mạng riêng ảo và dịch vụ proxy
	<p>9.1 Mạng riêng ảo Biên dịch địa chỉ mạng Mạng riêng ảo</p> <p>9.2 Máy chủ proxy Vai trò, cách thức hoạt động và các loại proxy</p>
Bài đọc 10	Kết nối đến mạng Internet
	<p>10.1 Kết nối qua tổng đài Kết nối quay số Kết nối băng thông rộng Công nghệ T-carrier Đường thuê bao số</p>

	<p>Bảng thông rộng cáp Kết nối quang</p> <p>10.2 Mạng diện rộng Mạng WAN VPN điểm-điểm</p> <p>10.3 Mạng không dây Giới thiệu mạng không dây Cấu hình mạng không dây Kênh Bảo mật mạng không dây</p> <p>10.4 Mạng viễn thông 10.5 Điện toán đám mây Điện toán đám mây và công nghệ ảo hóa Mọi thứ như một dịch vụ Lưu trữ đám mây</p>
Bài đọc 11	Sự cố mạng và cách khắc phục
	<p>11.1 Giao thức ICMP 11.2 Ping 11.3 Traceroute 11.4 Kiểm tra cổng 11.5 Kiểm tra DNS</p>

Phần 2: Hướng dẫn trả lời câu hỏi - Quiz

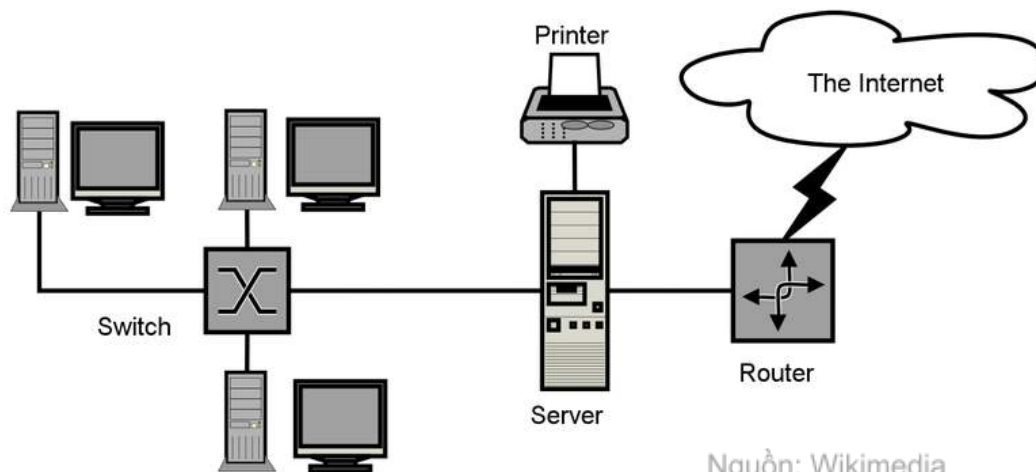
Phần 1

TÀI LIỆU ĐỌC BỔ TRỢ

Bài đọc 1. Giới Thiệu Mạng Máy Tính

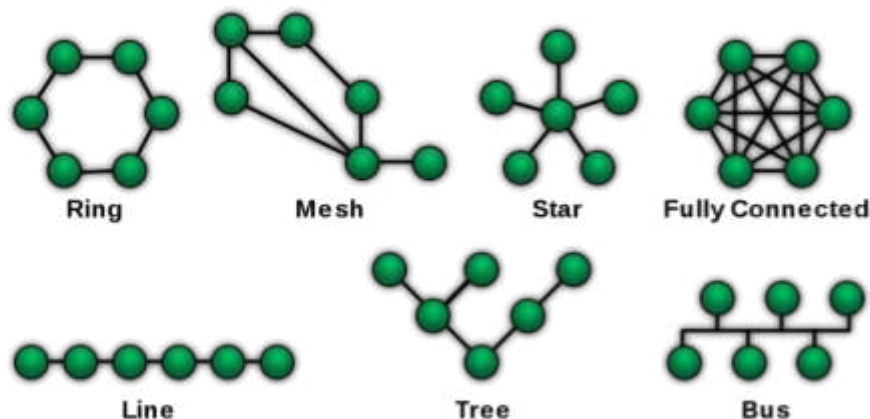
1. Mạng máy tính cơ bản

Một tập các máy tính được kết nối với nhau để giao tiếp, chia sẻ các tài nguyên tạo thành mạng máy tính (computer network).



Các máy tính được nối lại với nhau để giao tiếp, và thứ được giao tiếp đó chính là dữ liệu. Để truyền được dữ liệu từ vài byte đến hàng trăm ngàn byte, dữ liệu cần chia nhỏ và đóng gói theo một định dạng nhất định. Điều này giống như chúng ta vận chuyển hàng hóa từ nơi này đến nơi khác. Trong lĩnh vực mạng, họ gọi gói hàng vận chuyển là gói tin mạng. Phương tiện để các gói tin di chuyển trên đó đến các máy tính trong mạng được gọi là liên kết mạng. Một số phương tiện phổ biến gồm dây điện, sợi quang và không gian.

Đối với mạng không dây (Wi-Fi), các thiết bị kết nối với nhau qua sóng vô tuyến. Mạng không dây được đặc tả dưới họ chuẩn IEEE 802.11. Một số chuẩn cụ thể gồm 802.11a/b/g/n/ac/ax/be. Chúng thường giống nhau về giao thức cơ sở, nhưng khác nhau dải tần số.

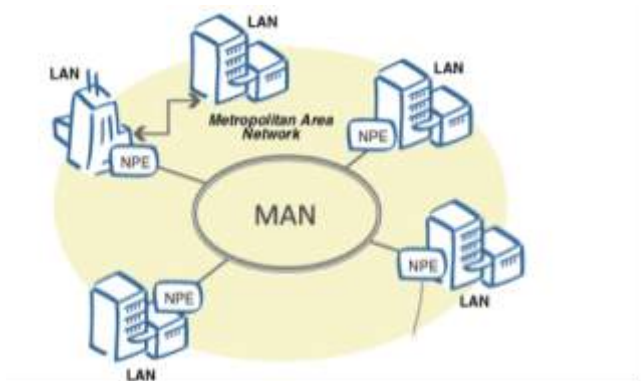


Nguồn: Wikipedia

Khi lắp các máy tính với nhau bằng dây dẫn, ta có nhiều cách để kết nối. Đồ hình mạng là cách sắp xếp các thành phần trong mạng như đi dây, bố trí các thiết bị, máy móc để hình thành ra một cấu trúc liên kết. Trong hình, ta có một số đồ hình phổ biến như dạng vòng (ring), dạng cây (tree), dạng hình sao (star), dạng bus, v.v. Trong khi đó, nút mạng là điểm phân phối lại khi chúng nhận được dữ liệu, hoặc là điểm đầu cuối trong giao tiếp mạng. Để dễ hiểu, ta có thể hình dung nút mạng là người gửi thư, bưu điện, người đưa thư và người sẽ nhận thư trong dịch vụ chuyển phát bưu phẩm ngoài cuộc sống. Một số nút mạng thông dụng như card mạng trong máy tính của chúng ta, hub, repeater, switch.

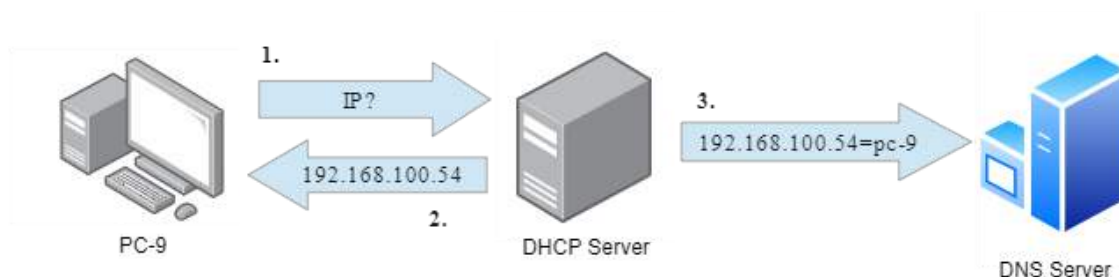
Sau khi đã kết nối vật lý các máy với nhau, chúng ta cũng cần có thêm các quy tắc để thông tin được truyền tải một cách chính xác và đầy đủ. Một tập hợp các quy tắc, các tiêu chuẩn để các máy tính có thể giao tiếp được với nhau một cách thông suốt được gọi là giao thức giao tiếp hay giao thức mạng. Nó giống như trong các cuộc nói chuyện của con người, chúng ta cũng đề ra các quy tắc giao tiếp như ai sẽ nói trước, ai nói sau, trình tự nói, cách hành văn để mọi người đều có thể nghe và hiểu được những gì đang trao đổi.

Trong quá trình thực thi, nhiều máy tính có thể kết nối ở khoảng cách rất xa. Thuật ngữ phạm vi kết nối mô tả về khu vực bao phủ của mạng. Ví dụ như mạng LAN thì khu vực bao phủ nhỏ, giới hạn trong khoảng vài km đổ lại, còn mạng MAN bao phủ khu vực lớn hơn như trong một thành phố.



Nguồn: Wikimedia

Mỗi máy tính tham gia mạng sẽ có nhiều mục tiêu khác nhau. Các mục tiêu này được thể hiện thông qua các ứng dụng người dùng chạy trên máy. Dịch vụ mạng là các ứng dụng chạy trên máy chủ để cung cấp các chức năng cho người dùng. Ví dụ như trong hình, máy chủ DHCP cấp địa chỉ cho một máy tính trong khi đó máy chủ DNS lại ánh xạ địa chỉ thành tên miền.



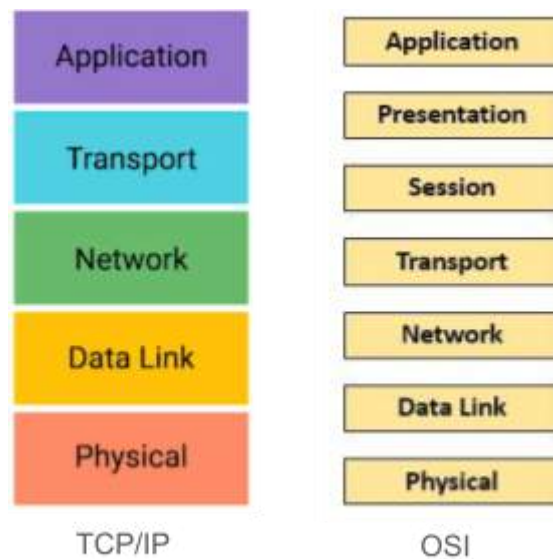
Bên cạnh đồ hình, cách thức kết nối, giao thức kết nối để đảm bảo cơ sở hạ tầng cơ bản cho mạng máy tính hoạt động thì hai tiêu chí khác cũng cần được quan tâm gồm chất lượng mạng và bảo mật mạng. Chất lượng mạng được thể hiện thông qua các chỉ số như băng thông, độ trễ, chất lượng dịch vụ. Trong khi đó, bảo mật mạng liên quan đến việc bảo vệ, giám sát các hoạt động, bảo mật dữ liệu thông qua mã hóa đầu cuối.

2. Tổng quan mô hình mạng

Qua thời gian, các thiết bị kết nối mạng trở nên đa dạng và phức tạp, số lượng máy tính kết nối với nhau bắt đầu tăng lên chưa kể có nhiều ứng dụng trên một máy cùng đồng thời có nhu cầu giao tiếp mạng. Điều này khiến cho một giao thức đơn lẻ không còn phù hợp để nắm giữ giao tiếp này được. Vì vậy, các nhà phát triển đã kết hợp nhiều giao thức lại với nhau để tạo ra một kiến trúc tổng thể và gọi là mô hình mạng (network model). Do mô hình mạng có sự trùng với một khái niệm bên thiết kế cơ sở dữ liệu nên

người ta sử dụng các thuật ngữ thay thế như network stack hay protocol suites. Một số mô hình mạng phổ biến gồm mô hình OSI, mô hình TCP/IP 5 lớp.

Một mô hình mạng bao gồm các tầng (layer) để truyền dữ liệu giữa các máy tính. Mỗi tầng có một chức năng cụ thể và thường bao gồm các giao thức. Mô hình mô hình ra đời khá sớm là TCP/IP. Mô hình này dựa trên hai giao thức chính là giao thức TCP và giao thức IP, và bao gồm 5 tầng là tầng vật lý (physical), tầng liên kết dữ liệu (data link), tầng mạng (network), tầng vận chuyển (transport) và tầng ứng dụng (application).



Nguồn: wikipedia

Một mô hình về sau khác, mô hình OSI, cũng dần trở nên phổ biến. Mô hình này bao gồm 7 tầng, cụ thể là tầng vật lý (physical), tầng liên kết dữ liệu (data link), tầng mạng (network), tầng vận chuyển (transport), tầng phiên (session), tầng trình diễn (presentation), và cuối cùng là tầng ứng dụng (application). Có thể xem tầng ứng dụng trong mô hình 5 tầng tương đương với 3 tầng cuối trong mô hình OSI, cụ thể là tầng ứng dụng, tầng trình diễn và tầng phiên. Tuy nhiên, mức chi tiết sẽ cao hơn và giúp cho quá trình truyền gói tin giữa các dịch vụ trở nên thuận tiện và đa dạng hơn.

Trong khóa học này, chúng ta tập trung chính vào mô hình TCP/IP 5 lớp vì về cơ bản chúng thể hiện các đặc điểm chính trong quá trình giao tiếp giữa các máy tính. Bảng bên dưới thể hiện tổng quan về mô hình TCP/IP. Một số thông tin trong bảng gồm tên từng tầng, giao thức trên mỗi tầng, đơn vị dữ liệu và phương pháp xác định địa chỉ.

#	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc..	Messages	n/a
4	Transport	TCP/UDP	Segment	Port #'s
3	Network	IP	Datagram	IP address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

Tầng vật lý mô tả các đặc trưng, các chuẩn phần cứng để kết nối các thiết bị trong mạng. Tầng liên kết dữ liệu (data link layer) đảm nhiệm định nghĩa một cách chung để diễn giải các tín hiệu được gửi và nhận từ tầng vật lý giúp cho các thiết bị mạng có thể giao tiếp với nhau. Tầng liên kết dữ liệu nhận dữ liệu từ tầng mạng, đóng gói chúng thành các khung tin (frame) bằng cách bổ sung các thông tin như địa chỉ MAC của máy nguồn và đích. Sau đó sử dụng tầng vật lý để truyền đến máy tính khác trong mạng. Giao thức thường được sử dụng trong tầng này là giao thức Ethernet.

Tầng thứ 3 trong mô hình 5 lớp TCP/IP là tầng mạng, đôi khi cũng được gọi là tầng Internet vì nó cho phép gửi dữ liệu qua nhiều mạng khác nhau mà ta gọi đó là liên mạng sử dụng thiết bị định tuyến (router). Dữ liệu được đóng gói ở tầng mạng được gọi là packet. Giao thức phổ biến trong tầng này là IP (Internet Protocol). Trong khi tầng mạng chuyển gói tin giữa hai nút mạng thì tầng vận chuyển chuyển gói tin giữa các tiến trình ở máy nguồn và máy đích một cách chính xác. Hay nói cách khác, do trên một máy tính, chúng ta có rất nhiều chương trình cùng chạy, nên tầng vận chuyển sẽ phải tổ chức, sắp xếp chương trình nào trên máy đích sẽ nhận dữ liệu từ chương trình nào trên máy nguồn. Tầng vận chuyển có hai cơ chế chuyển thông dụng là TCP và UDP.

Tầng cuối cùng là tầng ứng dụng. Đây là tầng xác định cách dữ liệu được định dạng, mã hóa, giải mã, trình tự giao tiếp và được thống nhất giữa các ứng dụng. Tầng này chứng kiến rất nhiều giao thức khác nhau như HTTP, FTP, SMTP, v.v.

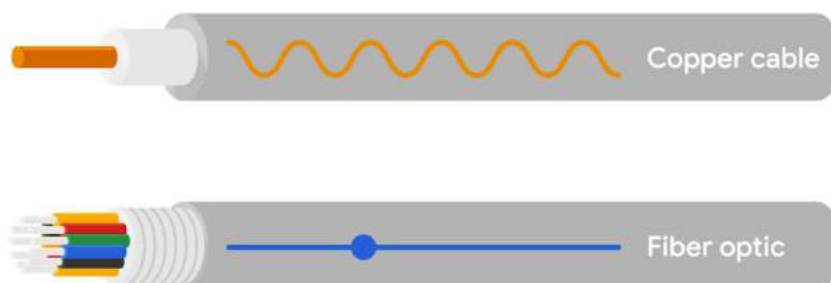
Để dễ hình dung về 5 tầng trong mô hình TCP/IP, ta có thể liên hệ đến việc giao hàng trong thực tế. Khi giao một món hàng, ta cần phương tiện vận chuyển và đường để đi. Những thứ đó ta có thể xem như tương đương với tầng vật lý. Trong khi đó, tầng liên kết dữ liệu giống như khi đến một ngã rẽ, ta cần xác định ngã rẽ nào để đi đến điểm giao lộ

tiếp theo, ví dụ có thể hỏi người dân địa phương. Tăng mạng chính là lộ trình mà ta đã vạch ra để di chuyển đến nhà khách hàng. Khi đã đến nhà, tăng vận chuyển giúp ta xác định ai sẽ là người nhận đúng nơi đó. Và cuối cùng, khi khách hàng nhận được hàng, họ cần tiến hành các thủ tục như mở ra kiểm tra, sử dụng thử và xác nhận đơn hàng.

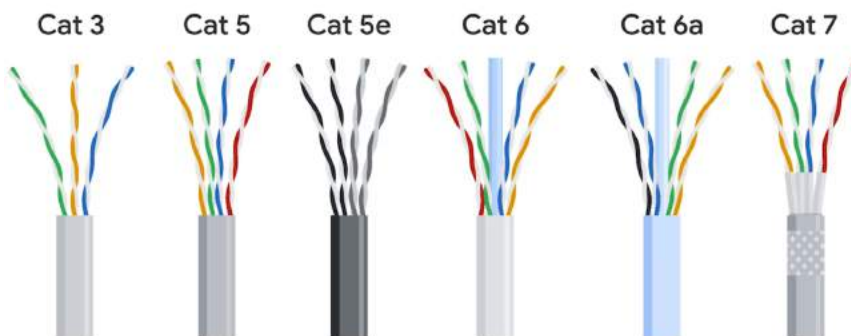
Bài đọc 2. Thiết bị Mạng

1. Cáp mạng

Cáp mạng (cable) là sợi dây được sử dụng để kết nối các thiết bị khác nhau và cho phép dữ liệu truyền tải trên đó. Cáp mạng được phân chia làm hai loại chính gồm cáp đồng và cáp quang. Cáp đồng sử dụng dây đồng làm vật liệu truyền. Dữ liệu được truyền bằng cách áp điện thế lên đường dây để thể hiện trạng thái có và không có điện, từ đó được hiểu là tín hiệu 0, 1. Trong khi đó, cáp quang sử dụng xung ánh sáng để thể hiện cho tín hiệu 0,1. Cáp đồng thường được xoắn theo từng đôi một để giảm nhiễu điện từ.



Cáp đồng xoắn đôi có nhiều phiên bản cải tiến, phổ biến trong số đó là Cat 5, Cat 5e, Cat 6. Các phiên bản về sau cải thiện tốc độ và khắc phục hiện tượng nhiễu xuyên âm (crosstalk). đương nhiên, chi phí sẽ tăng lên khi mua các cáp phiên bản mới.



Hiện tượng nhiễu xuyên âm là hiện tượng xung điện ở sợi dây này tạo ra hiệu ứng không mong muốn ở sợi khác. Hiện tượng này chỉ xảy ra khi chúng ta sử dụng các cáp đồng. Khi nhiễu xảy ra, dữ liệu truyền trong mạng không còn chính xác, điều này khiến các máy tính phải gửi lại nhiều lần. Hệ quả là ảnh hưởng băng thông mạng.

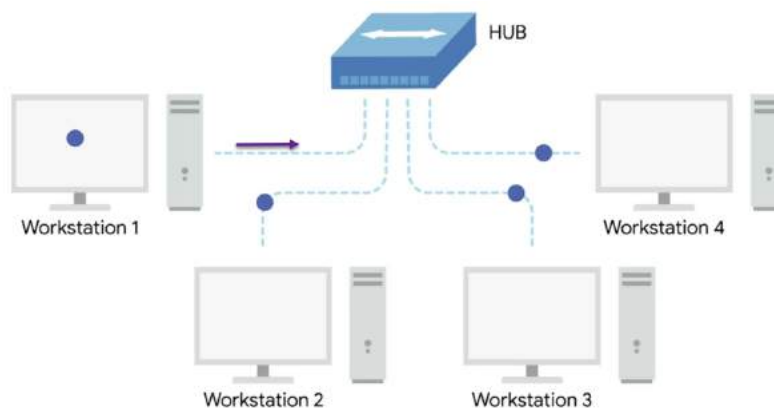
Cáp quang hay sợi quang dùng ánh sáng để truyền tín hiệu nên đạt được tốc độ nhanh hơn so với cáp đồng, không bị hiện tượng nhiễu điện từ, và khi truyền nhận ở khoảng cách xa, chúng ít bị mất mát dữ liệu. Tuy nhiên, bất lợi của cáp quang nằm ở chỗ chi phí đắt, dễ đứt gãy và khó đấu nối hơn so với cáp đồng.



Nguồn: pixabay

2. Thiết bị mạng

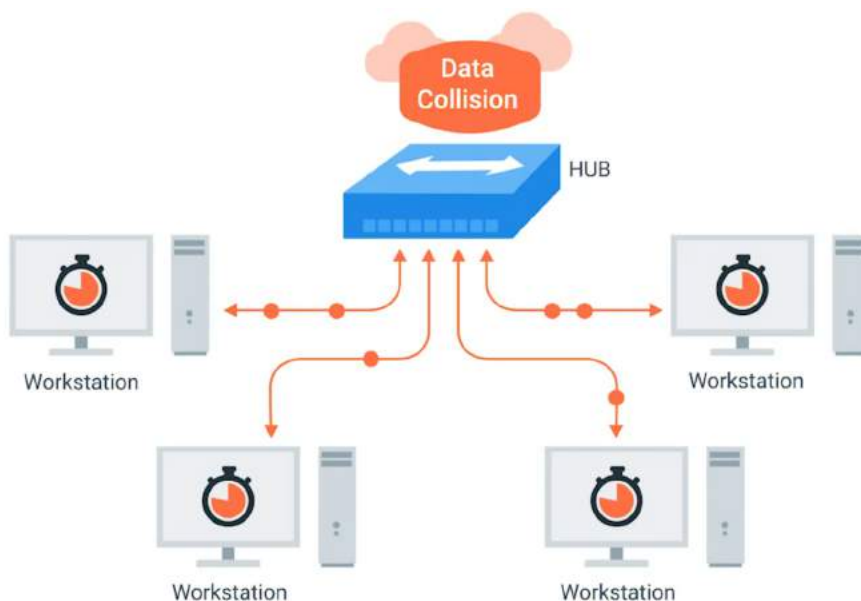
Mạng máy tính thường bao gồm rất nhiều máy, chúng ta không thể dùng dây dẫn để kết nối từng cặp máy lại với nhau để giao tiếp được. Do đó, mạng máy tính cần các thiết bị hỗ trợ khác. Thiết bị đơn giản nhất trong số đó là bộ chia mạng (Hub). Khi các máy tính kết nối đến hub, chúng có thể giao tiếp với nhau mà không cần phải nối trực tiếp với nhau từng đôi một.



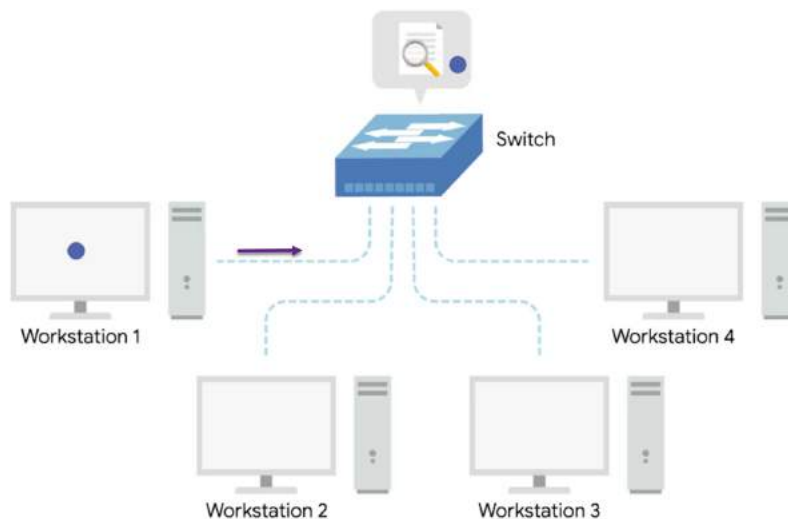
Hub có đặc điểm là khi một máy tính gửi tín hiệu, tất cả các máy cắm chung hub đều nhận được tín hiệu. Một máy tính nhận được sẽ xem xét xử lý thông điệp nếu nó nghĩ rằng dành cho nó, hoặc bỏ qua trong trường hợp ngược lại. Chúng ta có thể liên hệ hub giống như ổ cắm điện cho các thiết bị gia dụng trong nhà, tất cả các thiết bị cắm vào ổ cắm điện đều có điện sử dụng.

Do khi một máy gửi, các máy khác đều nhận được. Điều này gây ra nhiều vấn đề, đặc biệt là vấn đề ùn tắc. Nếu nhiều thiết bị gửi tín hiệu cùng lúc, hiện tượng ùn tắc sẽ xảy

ra, tín hiệu bị nhiễu và không còn ý nghĩa. Do đó, các máy phải đợi một khoảng thời gian và lắng nghe đường truyền để gửi lại. Khái niệm miền đụng độ (collision domain) để ám chỉ những mạng chỉ cho phép một thiết bị giao tiếp ở một thời điểm. Điều này dẫn đến kết nối trong mạng thường chậm và Hub thường không được sử dụng nhiều trong thực tế.

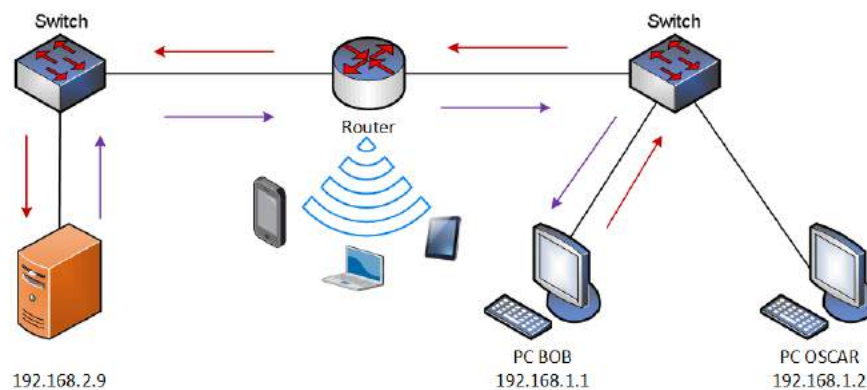


Trong khi hub gửi tín hiệu đến tất cả máy khác trong mạng khi chúng nhận được thông tin, bộ chuyển mạch (switch) khi nhận được tín hiệu, chúng sẽ kiểm tra địa chỉ của người nhận và gửi dữ liệu về chỉ nơi đó. Điều này khắc phục hiện tượng đụng độ và làm cho tốc độ mạng nhanh hơn. Để có thể chuyển đúng gói tin cho bên nhận, switch ghi nhớ các thiết bị mà được gắn đến jack cắm của nó.



Khi lắp đặt, hub hoạt động ở tầng vật lý trong mô hình TCP/IP, còn switch hoạt động ở tầng liên kết dữ liệu. Hub và switch chỉ phù hợp với mạng nhỏ lẻ như mạng LAN, không phù hợp để kết nối nhiều mạng lại với nhau.

Để kết nối nhiều mạng khác nhau, chúng ta sử dụng thiết bị gọi là bộ định tuyến (router). Thiết bị này giúp chuyển tiếp gói tin giữa các mạng khác nhau, kể cả mạng có dây và không dây.



Router là thiết bị hoạt động ở tầng 3 của mô hình TCP/IP, chúng lưu trữ một bảng định tuyến chứa thông tin để xác định đường đi của gói tin trong mạng. Chúng ta thường sử dụng router để kết nối đến mạng Internet thông qua nhà cung cấp dịch vụ internet (ISP). Bản thân ISP cũng thiết lập router để định hướng gói tin truyền đến router ở nhà chúng ta.

Một vấn đề nữa là dữ liệu có thể truyền giữa hai máy tính nằm ở khoảng cách xa, như vậy phải qua rất nhiều router khác nhau. Để giúp xác định đường đi tốt cho gói tin, một giao thức được tạo ra được gọi là BGP (Border Gateway Protocol). BGP là giao thức giúp xác định đường đi tối ưu nhất để chuyển tiếp gói tin qua nhiều router.

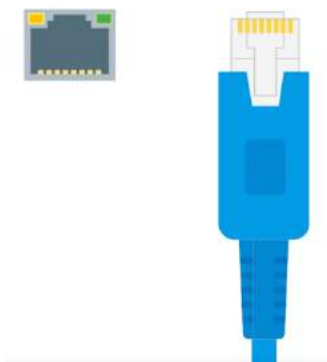
Trong kết nối mạng, ngoài dây dẫn và các thiết bị hỗ trợ truyền nhận dữ liệu, chúng ta cần đề cập đến hai loại phổ biến khác là máy chủ (server) và máy khách (client). Hiểu đơn giản, máy chủ là hệ thống máy tính hay phần mềm cung cấp dữ liệu cho các thiết bị được gọi là máy khách.

3. Giắc cắm mạng

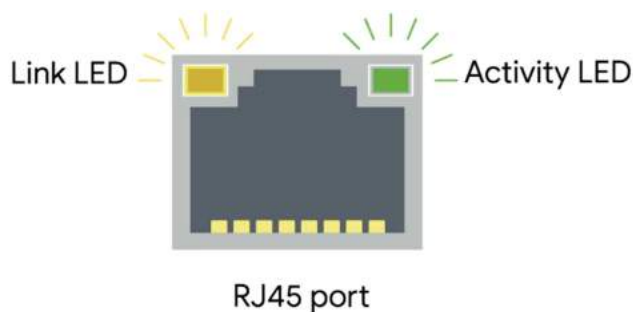
Để đấu nối dây mạng đến các thiết bị mạng, người ta phải thiết kế đầu cắm và cổng cắm. Chuẩn thiết kế đầu nối phổ biến là RJ45. Cáp mạng có đầu cắm RJ45 có thể kết nối với cổng mạng RJ45. Cổng mạng thường được gắn trực tiếp vào các thiết bị tạo thành mạng máy tính. Switch sẽ có nhiều cổng mạng vì mục đích của chúng là kết nối nhiều

thiết bị. Nhưng máy chủ và máy tính để bàn, thường chỉ có một hoặc hai. Máy tính xách tay, máy tính bảng hoặc điện thoại thậm chí không có cổng này.

RJ45 port RJ45 plug



Trên cổng cắm thường được trang bị 2 đèn led nhỏ để báo hiệu thông tin kết nối. Đèn liên kết (link led) báo hiệu cáp đã được kết nối đúng ở cả hai thiết bị, còn đèn hoạt động (activity led) báo hiệu dữ liệu đang được truyền nhận. Trước đây, đèn LED hoạt động nhấp nháy tương ứng trực tiếp với các số 0 và 1 được gửi đi. Tuy nhiên, ngày nay mạng máy tính quá nhanh nên đèn LED hoạt động không thực sự thể hiện giao tiếp này nhiều ngoài việc chỉ để cập lưu lượng truy cập có hay không. Đôi khi cùng một đèn LED được sử dụng cho cả trạng thái liên kết và hoạt động.



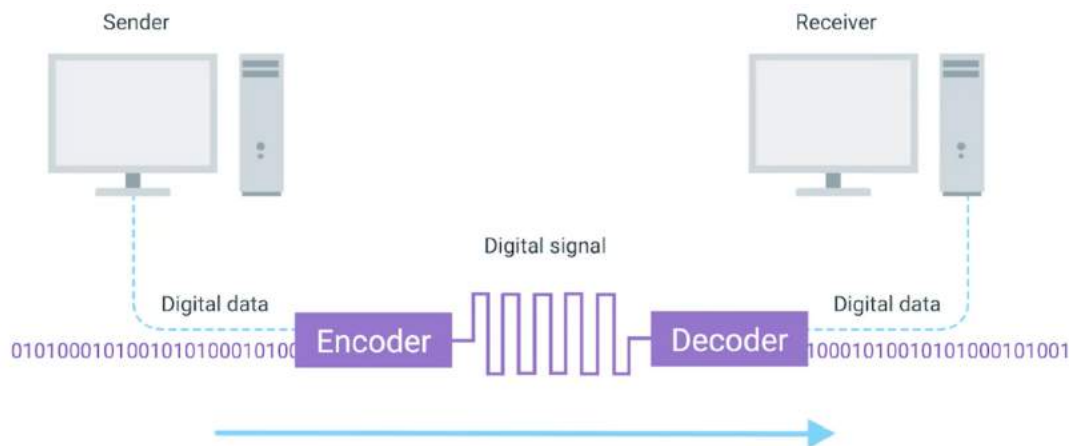
Để quản lý việc đấu nối tập trung nhiều dây mạng cho gọn, chúng ta thường chạy các dây dẫn âm tường đến một bảng cắm (patch panel). Đây là thiết bị chứa rất nhiều cổng mạng. Nhưng nó không có tính năng gì khác ngoài là hộp chứa các điểm cuối của nhiều đường cáp. Sau đó, các cáp được chạy từ bảng cắm đến switch hoặc router để cung cấp quyền truy cập mạng đến các máy tính ở đầu kia của các liên kết đó.

Bài đọc 3. Tầng Vật Lý

1. Chức năng và dịch vụ trên tầng vật lý

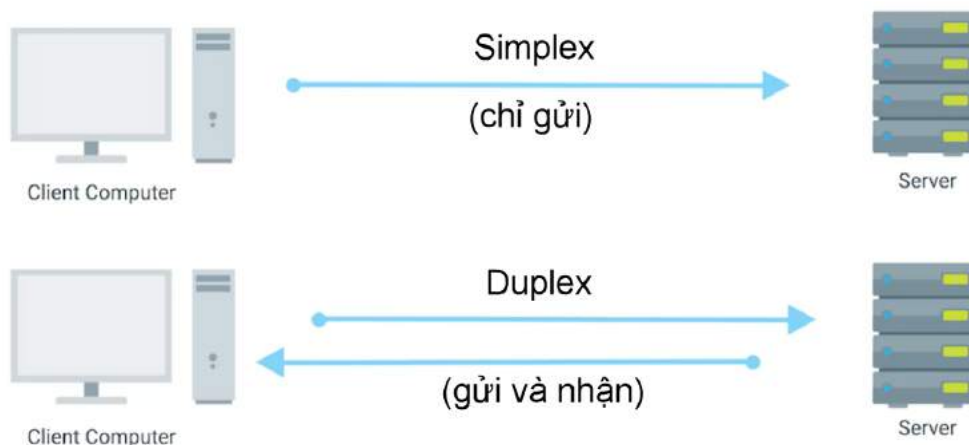
Tầng vật lý là tầng thể hiện các đặc trưng, các chuẩn phần cứng sử dụng để kết nối các máy tính lại với nhau. Nhiệm vụ chính của tầng vật lý là di chuyển các bit 1, 0 từ một nguồn thông qua liên kết để đến điểm tiếp theo. Tín hiệu mạng chủ yếu được truyền qua các dây dẫn bằng cáp đồng hoặc cáp quang. Cáp đồng là các sợi cáp xoắn đôi để chống lại hiện tượng nhiễu điện từ và nhiễu xuyên âm (crosstalk). Ví dụ, cáp Cat6 có đến 8 sợi dây dẫn được xoắn thành 4 cặp. Cáp quang sử dụng ánh sáng để truyền tín hiệu.

Trong mạng cáp đồng, khi được kết nối với các thiết bị ở cả hai đầu, sẽ mang điện tích không đổi. Số 1 và 0 được gửi qua các cáp mạng thông qua một quá trình được gọi là điều chế (modulation). Điều chế là một cách thay đổi điện áp của điện tích di chuyển trên cáp. Khi được sử dụng cho mạng máy tính, loại điều chế này được gọi cụ thể hơn là mã hóa đường truyền (line coding). Mã hóa đường truyền cho phép các thiết bị ở một trong hai đầu của một liên kết hiểu rằng điện tích ở một trạng thái nhất định là số 0 hay số 1. Thông qua kỹ thuật có vẻ đơn giản này, các mạng hiện đại có khả năng di chuyển 10 tỷ tín hiệu trên một cáp mạng mỗi giây.



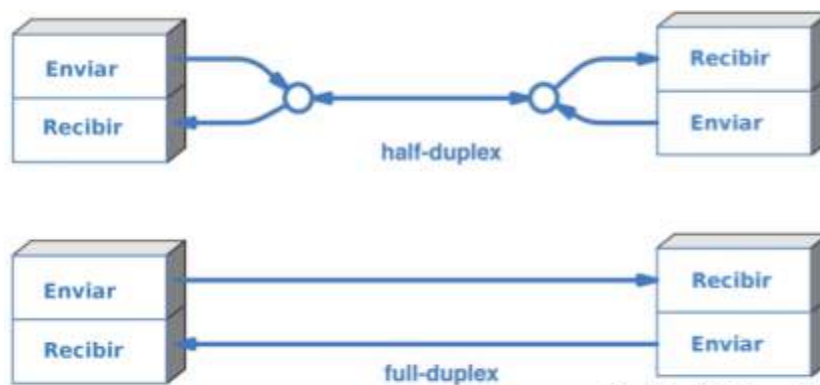
2. Giao tiếp trong tầng vật lý

Cáp đồng với nhiều sợi dây và mỗi sợi đóng vai trò khác nhau trong quá trình giao tiếp mạng. Vai trò này phụ thuộc vào công nghệ truyền dẫn. Công nghệ truyền dẫn là cách thông tin di chuyển giữa hai điểm kết nối. Người ta chia làm hai loại gồm giao tiếp đơn công (simplex communication) và giao tiếp song công (duplex communication).



Giao tiếp đơn công chỉ cho phép tín hiệu di chuyển theo một hướng nhất định. Ví dụ, tín hiệu từ đài phát thanh đến radio nhà dân thuộc loại giao tiếp đơn công. Còn giao tiếp song công cho phép tín hiệu di chuyển ở cả hai hướng. Ví dụ, khi gọi điện thoại, chúng ta có thể nói và nghe cùng một lúc.

Trong giao tiếp song công, người ta chia thành 2 loại con là bán song công (half-duplex) và song công toàn phần (full-duplex). Giao tiếp bán song công chỉ cho phép tín hiệu chạy theo một hướng nhất định tại một thời điểm. Nghĩa là khi một thiết bị đang gửi dữ liệu thì thiết bị khác phải đợi. Ngược lại, giao tiếp song công toàn phần cho phép cùng lúc tín hiệu di chuyển ở cả hai chiều.

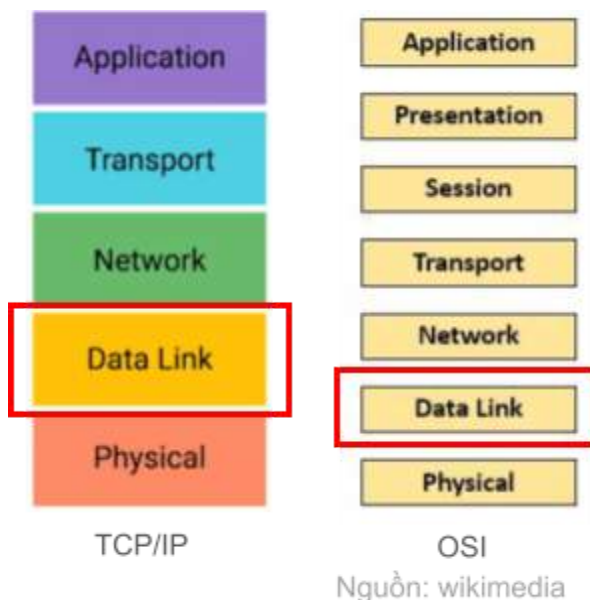


Nguồn: Wikimedia

Bài đọc 4. Tầng Liên Kết Dữ Liệu

1. Chức năng và dịch vụ trên tầng liên kết dữ liệu

Tầng thứ hai trong mô hình mạng 5 lớp TCP/IP là tầng liên kết dữ liệu. Giao thức được sử dụng rộng rãi nhất để gửi dữ liệu qua các liên kết riêng lẻ được gọi là Ethernet. Ethernet và tầng liên kết dữ liệu cung cấp phương tiện để phần mềm ở các mức cao hơn của ngăn xếp mạng (network stack) gửi và nhận dữ liệu.



Hay nói cách khác, tầng liên kết nhận dữ liệu từ tầng trên và sử dụng dịch vụ ở tầng vật lý để gửi và nhận các gói dữ liệu giữa các máy tính một cách thành công.

Ngoài ra, hai máy tính gửi dữ liệu qua dây cùng một lúc sẽ dẫn đến sự va chạm, dẫn đến kết quả cuối cùng là tín hiệu khi nhận sẽ không thể hiểu được. Để khắc phục hiện tượng đụng độ (collision), giao thức Ethernet sử dụng kỹ thuật CSMA/CD. Nguyên lý của kỹ thuật này là trong quá trình truyền dữ liệu, nếu một máy tính phát hiện đụng độ, nó sẽ dừng quá trình truyền lại. Sau đó đợi một khoảng thời gian ngẫu nhiên và gửi lại nếu đường truyền rảnh. Khoảng thời gian ngẫu nhiên này giúp ngăn không cho các máy tính liên quan đến vụ đụng độ lại đụng độ trong lần tiếp theo khi chúng cố gắng truyền tải bất cứ thứ gì. Khi một phân đoạn mạng là một miền đụng độ (collision domain), điều đó có nghĩa là tất cả các thiết bị trên phân đoạn đó nhận được tất cả các giao tiếp trên toàn bộ phân đoạn.

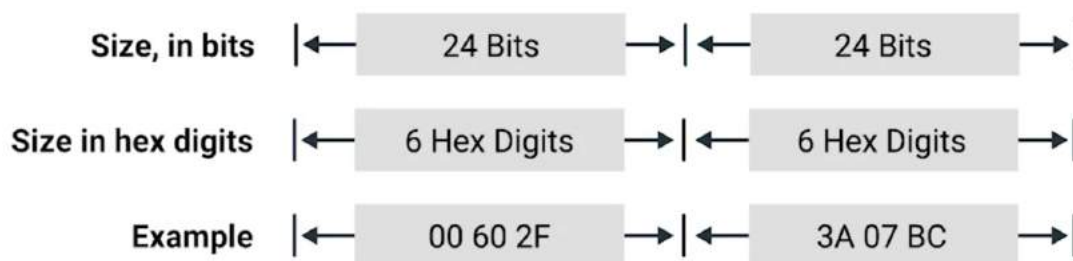


2. Địa chỉ vật lý

Mạng máy tính được hình thành bởi kết nối của nhiều máy tính và dĩ nhiên trong quá trình giao tiếp, các máy tính sẽ có nhu cầu giao tiếp riêng với nhau thay vì giao tiếp với tất cả các máy trong mạng. Để gói tin được truyền bởi ai và cho ai, ta cần cách để ghi thông tin này. Trên mạng, cách thức ghi thông tin này dựa trên một phương tiện là địa chỉ vật lý của thiết bị hay MAC (media access control). Địa chỉ MAC là định danh duy nhất toàn cầu được nhà sản xuất gán cho một card mạng.

Địa chỉ MAC được cấu thành bởi 48 bit. Tổng số địa chỉ MAC có thể tồn tại là 2^{48} hay 281.474.976.710.656 khả năng độc lập. Con số này là rất lớn và dễ dàng để đảm bảo các thiết bị được gán một địa chỉ đơn nhất trên toàn cầu.

Các bit này được chia thành 6 nhóm, mỗi nhóm là 8 bit được thể hiện dưới dạng số hệ thập phân. Hệ thập phân là số được cấu tạo từ 16 ký tự phân biệt gồm 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A (độ lớn tương đương với 10), B (độ lớn tương đương với 11), C (độ lớn = 12), D (độ lớn = 13), E (độ lớn = 14), và F (độ lớn = 15). Sở dĩ hệ 16 phải dùng các ký hiệu thay cho giá trị số là vì mỗi giá trị chỉ được biểu diễn bởi 1 ký tự để tránh nhập nhằng trong quá trình phân tách giữa các thành phần.



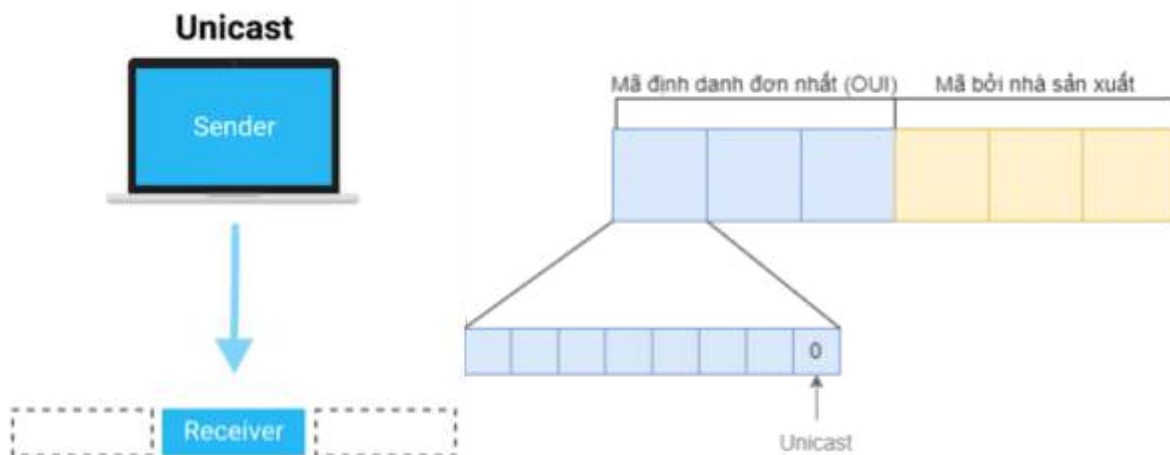
Các số thuộc 3 nhóm đầu là mã định danh đơn nhất của nhà sản xuất do tổ chức IEEE quản lý, còn lại 3 nhóm sau là mã được gán tùy ý bởi nhà sản xuất đó, miễn sao đảm bảo tính đơn nhất của thiết bị.

Ethernet sử dụng địa chỉ MAC để đảm bảo rằng dữ liệu gửi đi có cả địa chỉ máy truyền lẫn máy nhận. Bằng cách này, ngay cả trên một phân đoạn mạng, hoạt động như một

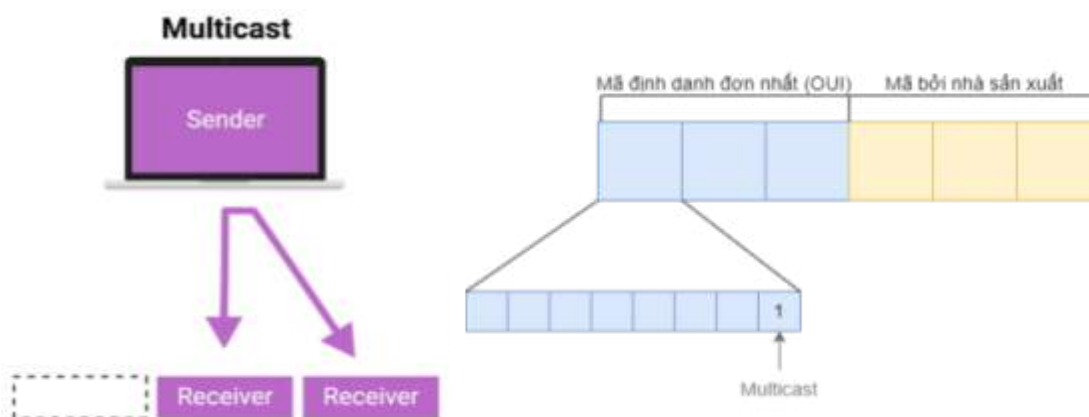
miền xung đột duy nhất, mỗi nút trên mạng biết gói tin nào dành cho nó, gói tin nào không.

3. Các kiểu định tuyến

Ethernet hỗ trợ 3 cơ chế để định tuyến dữ liệu là cơ chế unicast, multicast và broadcast. Cơ chế Unicast là cơ chế truyền một-một, nghĩa là chỉ có một người gửi và một người nhận. Dấu hiệu để biết cơ chế Unicast đó là bit có ý nghĩa thấp nhất (LSB) của số đầu tiên trên địa chỉ máy nhận được gán đến giá trị 0.



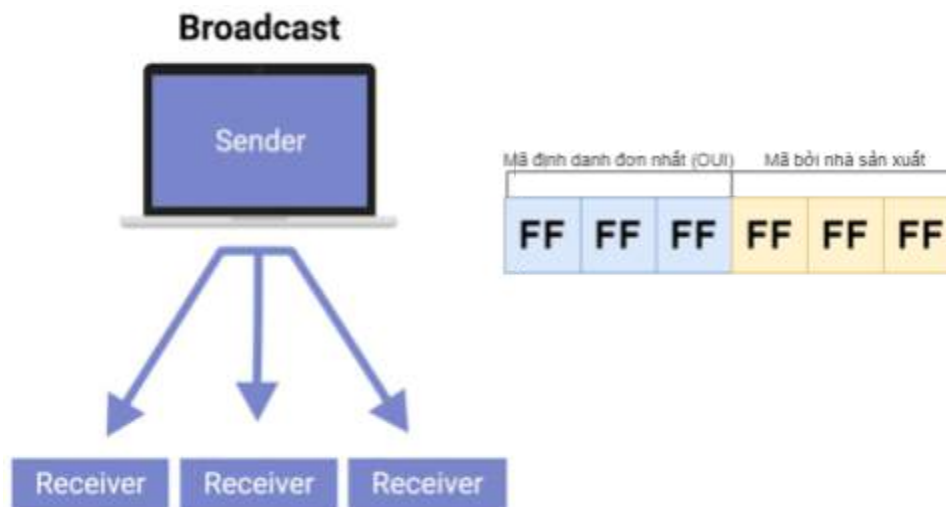
Cơ chế Multicast là cơ chế truyền một-nhiều, nghĩa là một người gửi và nhiều người nhận. Dấu hiệu để biết cơ chế Multicast đó là bit có ý nghĩa thấp nhất (LSB) của số đầu tiên trên địa chỉ máy nhận được gán đến giá trị 1.



Dữ liệu cho multicast được đặt tương tự cho tất cả các thiết bị trên tín hiệu mạng cục bộ. Điều khác biệt là nó sẽ được chấp nhận hoặc loại bỏ bởi mỗi thiết bị tùy thuộc vào

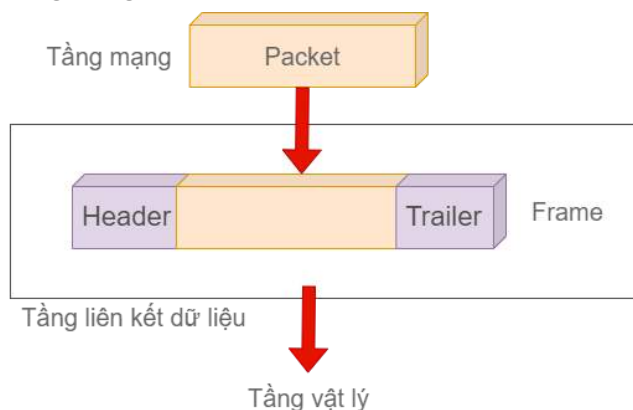
các tiêu chí ngoài địa chỉ MAC của riêng chúng. Các card mạng có thể được cấu hình để chấp nhận danh sách các địa chỉ multicast được cấu hình cho loại giao tiếp này.

Cơ chế Broadcast là cơ chế truyền một-tất cả, nghĩa là một người gửi và mọi người đều nhận được. Lúc này địa chỉ của người nhận là toàn giá trị F (FF: FF: FF: FF: FF: FF). Mục tiêu của cơ chế này muốn truyền thông điệp ra toàn bộ mạng để tìm kiếm một thông tin nào đó mà chúng không biết thiết bị nào thực sự đang nắm giữ nó.



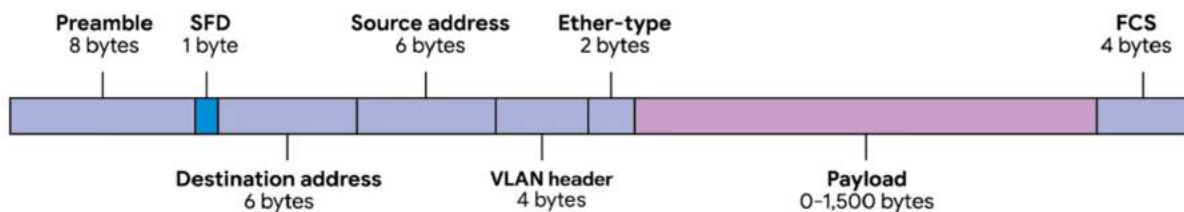
4. Cấu trúc khung dữ liệu trong tầng liên kết

Dữ liệu trong tầng liên kết được gọi là khung Ethernet. Khung Ethernet là một gói dữ liệu chứa các thông tin cần thiết trong giao thức Ethernet. Gói dữ liệu này sẽ được chuyển đến card mạng trong tầng vật lý để chuyển đi đến các máy trong mạng.



Một khung Ethernet được cấu tạo gồm 7 phần:

- Phần đầu được gọi là Preamble có kích thước 8 byte. Trong đó 7 byte đầu là vùng đệm giữa các khung và được sử dụng để đồng bộ đồng hồ và điều hòa tốc độ gửi dữ liệu. 1 byte còn lại là dấu hiệu để biết điểm bắt đầu khung.
- Hai phần tiếp theo là địa chỉ MAC của máy đích và máy nguồn.
- Phần thứ 4 trong Ethernet là VLAN Header, cho phép chúng ta tổ chức nhiều mạng LAN logic thực thi trên cùng thiết bị mạng, hay chúng ta gọi nó là mạng LAN ảo (virtual LAN).
- Theo sau VLAN là phần EtherType để mô tả loại Ethernet. Tiếp theo đó là Payload. Đây chính là phần dữ liệu chính cần truyền, nó chứa dữ liệu của tất cả các tầng phía trên trong mô hình TCP/IP.
- Cuối cùng trong khung Ethernet là chuỗi kiểm tra khung (frame check sequence). Chuỗi này chứa trị tổng kiểm được tính toán bởi quá trình kiểm dư chu trình, gọi tắt là CRC. Quá trình CRC thực hiện các phép tính toán học để kiểm tra dữ liệu đến có nguyên vẹn. Nếu không, nó thông báo đến các giao thức ở tầng trên để quyết định dữ liệu có cần phải gửi lại.

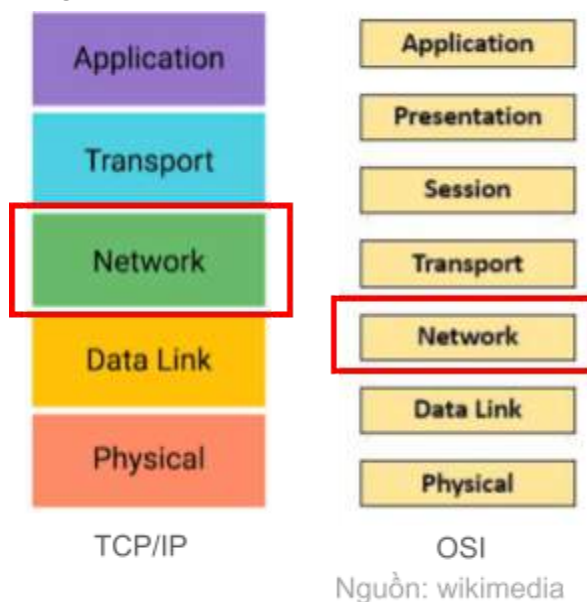


Bài đọc 5. Tầng Mạng

1. Chức năng và dịch vụ trên tầng mạng

Trên mạng cục bộ hoặc mạng LAN, các nút có thể giao tiếp với nhau thông qua địa chỉ MAC vật lý của chúng. Điều này hoạt động tốt trên quy mô nhỏ vì các bộ chuyển mạch có thể nhanh chóng tìm ra các địa chỉ MAC được kết nối với các cổng khác để chuyển tiếp các đường truyền một cách thích hợp. Nhưng địa chỉ MAC không phải là một chiến lược tốt cho quy mô lớn hơn. Mọi card mạng trên toàn cầu đều có một địa chỉ MAC duy nhất và chúng không được sắp xếp theo bất kỳ cách nào có trật tự. Do đó, không có cách nào để biết một địa chỉ MAC đang ở đâu, vì vậy nó không phải là giải pháp hợp lý để liên lạc đường dài. Tầng thứ 3 trong mô hình TCP/IP ra đời để giải quyết vấn đề trên.

Tầng thứ 3 có tên là tầng mạng (network layer), đôi khi cũng được gọi là tầng Internet vì nó cho phép gửi dữ liệu qua nhiều mạng khác nhau sử dụng thiết bị định tuyến (router). Giao thức phổ biến trong tầng này là IP (Internet Protocol).



2. Cấu trúc địa chỉ

Địa chỉ IPv4 và IPv6

Địa chỉ IPv4

Để định danh các máy tính, người ta sử dụng địa chỉ IP. Địa chỉ IP là số gồm 4 octet với mỗi octet là nhóm 8 bit. Có thể xem IP là một chuỗi gồm 4 số thập phân, mỗi số có giá trị từ 0 đến 255.

12.34.56.78

00001100.00100010.00111000.01001110

Ví dụ dãy số 12.34.56.78 là địa chỉ IP hợp lệ, nhưng dãy số 123.456.789.100 không hợp lệ vì nó có các số lớn, không thể biểu diễn bằng 8 bit. Định dạng này được gọi là ký hiệu thập phân có dấu chấm. Địa chỉ IP được phân thành nhiều nhóm dành cho các tổ chức và công ty khác nhau thay vì được xác định bởi các nhà sản xuất phần cứng. Điều này có nghĩa là địa chỉ IP có nhiều thứ bậc và dễ lưu trữ dữ liệu hơn so với địa chỉ vật lý.

Địa chỉ IP thuộc về mạng, không phải của thiết bị được gắn vào mạng đó. Vì vậy, máy tính xách tay của bạn sẽ luôn có cùng một địa chỉ MAC cho dù bạn sử dụng nó ở đâu, nhưng nó sẽ có một địa chỉ IP được gán ở quán Internet khác với địa chỉ IP được gán ở nhà. Mỗi mạng LAN tại quán Internet hoặc mạng LAN tại nhà sẽ chịu trách nhiệm riêng trong việc cấp địa chỉ IP cho máy tính xách tay của bạn khi kết nối.

Địa chỉ IP có thể được thiết lập thủ công hoặc tự động thông qua công nghệ DHCP. Địa chỉ IP được gán tự động gọi là địa chỉ IP động. Tuy nhiên, trong một số ngữ cảnh ta có thể gán thủ công địa chỉ IP và các địa chỉ này gọi là địa chỉ IP tĩnh. Thông thường, địa chỉ IP tĩnh được dành riêng cho máy chủ và thiết bị mạng, trong khi địa chỉ IP động được dành riêng cho máy khách.

Địa chỉ IPv6

Tổ chức cấp phát số hiệu Internet (IANA – Internet Assigned Numbers Authority) là tổ chức phi lợi nhuận giám sát việc cấp phát địa chỉ IP và giao thức Internet. Các hoạt động của IANA có thể được gom thành ba nhóm chính gồm tên miền, tài nguyên số và gán giao thức. Tổ chức này thông báo IPv4 không còn đủ để cấp cho mỗi thiết bị. Do đó, IPv6 ra đời để giải quyết vấn đề này. IPv6 có độ dài 128 bit và có thể cấp cho 2^{128} thiết bị. Đây là con số cực lớn. IPv6 được viết thành cụm gồm 8 nhóm, mỗi nhóm gồm 16 bit và được biểu diễn dưới dạng số hệ 16 (hệ hexa).

2001:0db8:0000:0000:0000:ff00:0012:3456

Với cách biểu diễn đầy đủ, IPv6 trở nên rất dài. Để có thể viết ngắn gọn lại người ta đưa ra quy tắc. Quy tắc thứ nhất là bỏ đi các số 0 đầu mỗi nhóm. Quy tắc thứ hai là bất kỳ nhóm liên tiếp nào toàn số 0 thì có thể thay bằng dấu hai chấm.

2001:0db8:0000:0000:0000:ff00:0012:3456

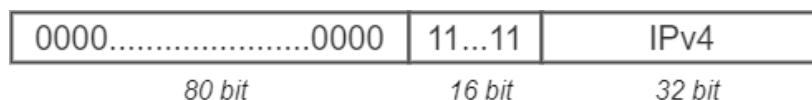


2001:db8::ff00:12:3456

Địa chỉ loopback của IPv6 có dạng ::1. Để gửi một nhóm các máy (multicast), IPv6 sử dụng địa chỉ FF00::.. Trong khi đó, để gửi đến một máy trong liên kết cục bộ (link-local unicast), IPv6 sử dụng địa chỉ FF80::..

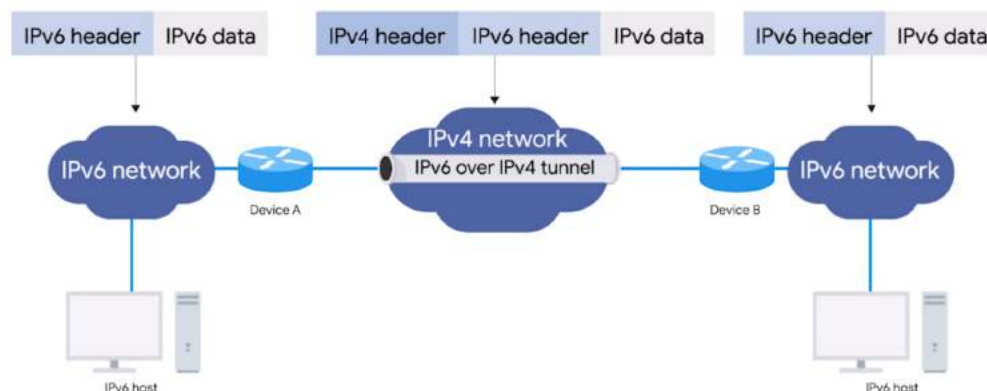
Địa chỉ link-local unicast dùng để giao tiếp trong một phân đoạn mạng và được cấu hình dựa trên địa chỉ MAC của máy. IPv6 của máy này được tạo bằng cách chuyển địa chỉ MAC thành số 64 bit đơn nhất và đưa vào một phần của địa chỉ của máy. Máy đích khi nhận tín hiệu ARP broadcast, nó sẽ gửi lại tín hiệu ARP response chứa địa chỉ MAC của máy đích. Bảng ARP cục bộ hết hạn sau một khoảng thời gian để đảm bảo thông tin luôn được cập nhật.

IPv6 sử dụng 64 bit đầu làm định danh mạng (network ID) và 64 bit sau làm định danh máy tính (host ID). Do có nhiều thiết bị cũ không có IPv6 nên cần một cách để duy trì cả hai phiên bản IP này. Chúng ta có thể ánh xạ IPv6 đến một địa chỉ IPv4 bằng cách, 80 bit đầu của IPv6 là số 0, theo sau là 16 bit 1 và 32 bit còn lại tương đương với IPv4.



169.291.13.133 = 0:0:0:0:FFFF:A9DB:0D85

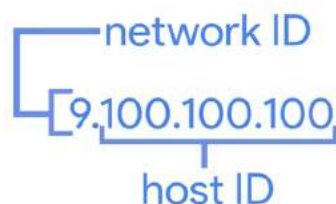
Để tận dụng hạng tầng sẵn có của mạng IPv4, một đường hầm IPv6 được tạo ra bằng cách thực hiện bao đóng gói tin IPv6 trong một gói tin IPv4 và chuyển qua mạng. Tại đầu kia, một server IPv6 sẽ thực hiện mở gói tin và chuyển ngược trở lại IPv4 để truyền cho các thiết bị xài IPv6. Thay vì cấu hình phức tạp, một số công ty được gọi là IPv6 tunnel broker đứng ra làm trung gian cung cấp dịch vụ để tạo kết nối cho các thiết bị dùng IPv6 với hạ tầng mạng hiện tại.



Phân lớp địa chỉ IP

Trong các phần tiếp theo, chúng ta tập trung vào địa chỉ IPv4. Một số cách thức cũng diễn ra tương tự trên IPv6.

Địa chỉ IPv4 được chia làm 2 thành phần gồm định danh mạng được gọi là network ID và định danh máy là host ID. Nếu chúng ta thay đổi giá trị trong phần host id để gán cho các máy khác nhưng giữ nguyên phần network id thì nghĩa là các máy này sẽ nằm chung một mạng với nhau.



Để quản lý việc cấp phát địa chỉ IP, các nhà phát triển đã phân địa chỉ IP thành 5 lớp khác nhau là A, B, C, D, E. Phổ dụng là các lớp A, B, C. Các lớp A sử dụng 1 byte đầu là định danh mạng. Do đó phần còn lại là 3 byte, tức là 24 bit nên số máy có thể gán được là $2^{24} = 16.777.216$. Trong khi đó lớp B sử dụng 2 byte đầu và số máy có thể gán được là $2^{16} = 65.536$. Còn lớp C dùng 3 byte để xác định nên còn lại 1 byte để gán cho các máy nên số máy có thể gán được là $2^8 = 256$.

Địa chỉ lớp D luôn bắt đầu bằng bit 1110 và được sử dụng cơ chế multicast, đó là cách một IP đơn lẻ có thể được gửi đến toàn bộ mạng cùng một lúc. Các địa chỉ này bắt đầu bằng các giá trị thập phân từ 224 đến 239. Cuối cùng, địa chỉ lớp E là tất cả các địa chỉ IP còn lại. Các địa chỉ lớp E không được sử dụng để gán cho máy tính thông thường mà chỉ sử dụng cho mục đích thử nghiệm.

Class A	Class B	Class C
<u>123.456.780.00</u>	<u>123.456.780.00</u>	<u>123.456.780.00</u>
network ID	network ID	network ID

Khi cho trước một địa chỉ IP, để biết IP thuộc lớp nào, người ta đưa ra một số quy ước. Nếu bit đầu tiên bên trái nhất của địa chỉ IP là 0 thì địa chỉ này thuộc lớp A. Một cách dễ hiểu hơn là nếu byte có giá trị từ 0 đến 127 thì chúng ta sẽ hiểu chúng thuộc về lớp A. Tương tự, một IP thuộc về lớp B nếu 2 bit đầu tiên là 10, lớp C là 110, lớp D là 1110 và lớp E là 1111.

Không gian địa chỉ không thể định tuyến

Không gian địa chỉ không thể định tuyến (non-routable address space) là các địa chỉ IP dành riêng cho mạng cá nhân như mạng cục bộ LAN. Các gói tin với địa chỉ IP này về cơ bản sẽ không được định tuyến ra Internet bởi các router. Đây vừa là giải pháp để đảm bảo an ninh cho mạng vừa là giải pháp để giải quyết tình trạng thiếu hụt địa chỉ IPv4. Bất kỳ ai cũng có thể sử dụng không gian địa chỉ này và không cần phải đăng ký. Mặc dù các IP này dùng để giao tiếp cục bộ, nhưng vẫn có một kỹ thuật để có thể kết nối các máy ra Internet thông qua kỹ thuật NAT (Network Address Translation).

Có 3 không gian địa chỉ thuộc nhóm này gồm 10.0.0.0/8, 172.16.0.0/12 và 192.168.0.0/16.

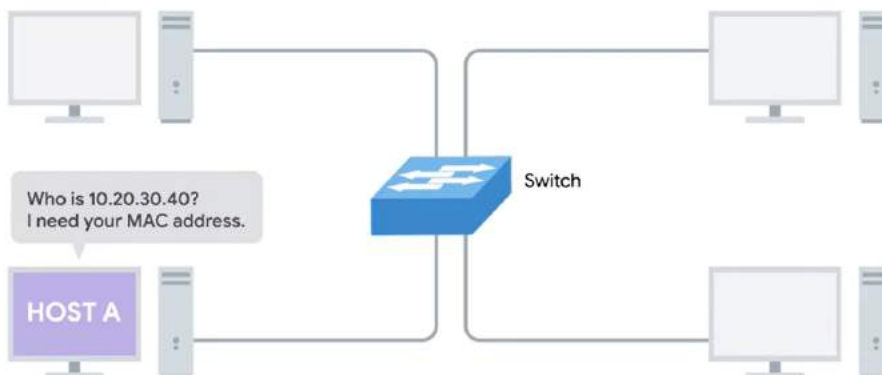
Cấp phát địa chỉ IP với CIDR

Phân lớp mạng theo cách phân chia lớp A, B, C có nhiều nhược điểm. Cụ thể, lớp A có số lượng máy quá nhiều, trong khi lớp C thì lại có số máy quá ít. Một doanh nghiệp đăng ký mạng lớp C thường không thể đủ số địa chỉ cần cấp cho các máy. Do đó họ thường phải đăng ký thêm địa chỉ mạng lớp C khác. Điều này gây cho việc định tuyến trở nên phức tạp. Một hệ thống mới được xây dựng để thay thế cách phân lớp A, B, C trong việc định vị địa chỉ IP là CIDR. Hệ thống này giúp làm chậm sự phình lên của bảng định tuyến và giảm sự cạn kiệt nhanh chóng của địa chỉ IPv4.

CIDR (Classless Inter Domain Routing) là phương pháp cấp phát địa chỉ IP có dạng địa chỉ IP/tiền tố mạng (network prefix). Trong đó, tiền tố mạng là số bit đầu tiên trong địa chỉ IP được sử dụng để định danh mạng. Với cách này, các nhà cung cấp dịch vụ internet (ISP) có thể sử dụng một dãy các địa chỉ IP liên tục để cấp phát địa chỉ cho người dùng, từ đó tạo sự dễ dàng trong quá trình định tuyến.

Giao thức phân giải địa chỉ

Trong tầng liên kết dữ liệu, gói dữ liệu IP diagram từ tầng mạng sẽ được đóng gói với địa chỉ MAC của nơi nhận. Như vậy ta cần biết địa chỉ MAC của máy đích này. Để xác định địa chỉ MAC, giao thức phân giải địa chỉ, gọi tắt là ARP, được tạo ra. Trong giao thức này, máy gửi sẽ tra địa chỉ IP trong bảng ARP cục bộ để tìm địa chỉ MAC. Nếu không có, nó sẽ broadcast gói tin ra toàn bộ mạng để có được thông tin.



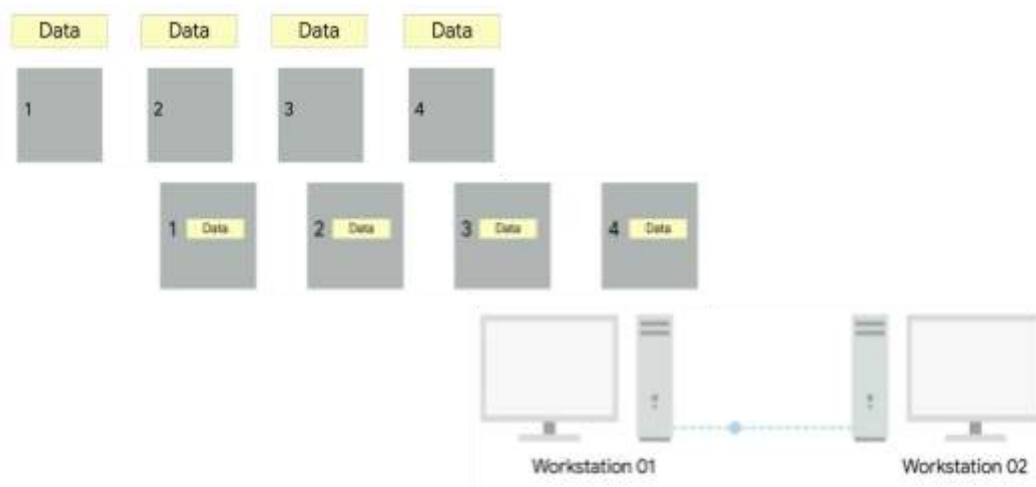
Máy đích khi nhận tín hiệu ARP broadcast, nó sẽ gửi lại tín hiệu ARP response chứa địa chỉ MAC của máy đích. Bảng ARP cục bộ sẽ hết hạn sau một khoảng thời gian để đảm bảo thông tin luôn được cập nhật.

3. Cấu trúc gói tin tầng mạng

Gói dữ liệu được hình thành trong tầng mạng là IP diagram. Chúng gồm 2 phần chính là phần header và phần dữ liệu. Phần header của IP diagram chứa nhiều thành phần hơn so với khung tin trong tầng liên kết dữ liệu.

0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification			Flags	Fragment Offset	
TTL	Protocol		Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	

Cụ thể, phần header của IP diagram gồm một số trường sau. Trường version để ghi loại phiên bản IP, có thể là IPv4 hoặc IPv6. Trường header length mô tả chiều dài header. Trong khi đó, trường service type là loại chất lượng dịch vụ còn total length là độ dài của IP diagram. Tiếp theo trong phần header là các trường identification, flags và fragment offset. Do dữ liệu có thể có kích thước lớn nên chúng không thể chứa trong một IP diagram duy nhất mà cần phải cắt thành nhiều gói nhỏ hơn và truyền đi trong mạng. Quá trình chia nhỏ gói tin diagram được gọi là fragmentation hay phân mảnh dữ liệu. Những gói nhỏ khi di chuyển đến máy đích nếu nó có cùng mã id thì chúng thuộc về cùng một gói dữ liệu ban đầu. Máy đích sẽ ghép chúng lại thành một dữ liệu hoàn chỉnh. Do các gói tin đi theo nhiều đường khác nhau để đến máy đích nên có thể có gói đến trước, gói đến sau. Trường fragment offset chứa các giá trị được đầu nhận sử dụng để ghép tất cả các phần của gói bị phân mảnh theo đúng thứ tự.



Trường tiếp theo là TTL. TTL viết tắt của từ time to live, nghĩa thời gian sống của gói tin hay nói cụ thể hơn là số router tối đa mà gói tin đi qua trước khi bị bỏ đi. Mỗi lần gói tin đi qua một router, giá trị TTL sẽ giảm đi một. Khi đạt giá trị 0 thì router sẽ không tiếp tục gửi chúng đi nữa. Mục tiêu của TTL nhằm tránh gói tin bị định tuyến sai và dẫn đến lặp vô tận trong quá trình gửi.

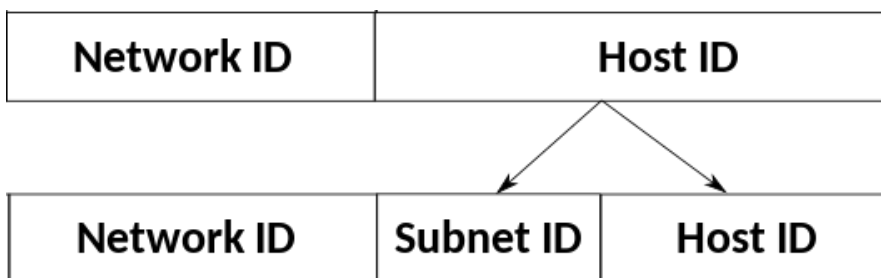
Tiếp theo là trường Protocol để xác định loại giao thức của tầng vận chuyển. Chúng thường là giao thức TCP hoặc UDP. Phần header checksum là chuỗi dùng để kiểm tra lỗi gói tin. Hai phần kế là Source và Destination IP Address, đó là địa chỉ IP của máy nguồn và đích.

Phần Options được dùng để thiết lập các đặc trưng đặc biệt dành cho mục đích kiểm thử. Do phần này có chiều dài thay đổi nên cần phải điền thêm các giá trị tạm để gói tin IP diagram luôn có kích thước cố định. Phần điền giá trị tạm được gọi là padding.

4. Cách thức chia mạng con

Định danh mạng con

Mạng máy tính lớn có thể được tách thành nhiều mạng nhỏ hơn, mỗi mạng nhỏ được gọi là mạng con (subnet). Để chia một mạng thành nhiều mạng con, chúng ta cần một cách để nhóm các IP lại thành một nhóm. Ví dụ, với địa chỉ mạng lớp C, chúng ta sẽ có khoảng 256 thiết bị khác nhau. Để tách mạng này ra thành 4 mạng con, ta cần sử dụng mặt nạ mạng con (subnet mask). Mặt nạ mạng con thực chất là một chuỗi bit tương tự như địa chỉ IP, sau khi thực hiện phép luận lý AND trên bit với địa chỉ IP của máy tính, ta sẽ có được 3 thành phần: network id, subnet id, và host id.



Mặt nạ mạng con

Mặt nạ mạng con giúp ta tách phần host id thành hai phần là subnet id và host id mới. Subnet id giống như mã định danh cho mạng con, còn host id vẫn là mã định danh cho máy tính trong mạng con. Ta cũng có thể kết hợp network id và subnet id và xem chúng như một id của mạng con. Các thiết bị mạng như router dựa trên mã định danh dạng này để điều hướng gói tin về đúng phần mạng đang có máy tính với địa chỉ xác định trước đó.

Trước khi đi vào ví dụ minh họa cách tìm địa chỉ mạng con, ta cần hiểu cách thức biểu diễn số ở hệ nhị phân và toán tử AND trên hệ đó. Hệ nhị phân là hệ chỉ có 2 giá trị phân biệt là 0 và 1. Để biểu diễn một số hệ 10 (thập phân) mà ta vẫn dùng hằng ngày dưới dạng hệ nhị phân, ta thực hiện một số phép chuyển đổi. Có nhiều cách để chuyển đổi nhưng chúng ta có thể nhìn nó với cách sau. Giả sử chúng ta có một dãy 8 bit, nhìn từ phải sang trái, chúng ta sẽ hình dung mỗi vị trí mang trong nó lần lượt các giá trị 1, 2, 4, 8, 16, 32, 64, 128. Chúng ta có thể thấy một quy luật của dãy số này là bắt đầu từ 1, số kế bên sẽ gấp đôi số hiện tại.

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0

Nếu ô nào có bit 1 thì giá trị này được đưa vào để tính tổng để ra được số hệ 10. Ví dụ trong dãy bit 0 0 0 0 1 0 1 0, chúng ta có hai ô bật lên tức là hai ô đang chứa số 1. Hai ô này có giá trị là 2 và 8. Ta thực hiện tính tổng hai giá trị được giá trị 10. Như vậy dãy bit 00001010 thể hiện cho đếm 10 đơn vị.

128	64	32	16	8	4	2	1
0	0	0	0	1	0	1	0
$8 + 2 = 10$							

Với một dãy bit cho trước thì có thể biểu diễn được bao nhiêu số phân biệt? Mỗi vị trí bit, chúng ta có 2 giá trị phân biệt như vậy với n bit ta sẽ có 2^n giá trị phân biệt. Nếu chỉ xét số dương thì phạm vi giá trị sẽ từ 0 đến $2^n - 1$. Ví dụ, với 8 bit sẽ có 2^8 bằng 256 số giá trị phân biệt, phạm vi từ 0 đến 255.

Các phép tính trên hệ nhị phân cũng khá tương tự với hệ thập phân ngoài trừ một số trường hợp. Ví dụ với phép cộng, các kết quả của biểu thức giống với hệ thập phân ngoài trừ phép tính $1 + 1$, kết quả là 10. Bảng bên dưới cũng thể hiện phép tính luận lý OR và AND.

$0 + 0 = 0$	$1 \text{ OR } 0 = 1$
$0 + 1 = 1$	$0 \text{ OR } 0 = 0$
$1 + 0 = 1$	$1 \text{ OR } 1 = 1$
$1 + 1 = 10$	$1 \text{ AND } 1 = 1$
	$1 \text{ AND } 0 = 0$
	$0 \text{ AND } 0 = 0$

Bây giờ, ta sử dụng các giá trị nhị phân cùng với phép luận lý AND để tạo ra địa chỉ mạng con. Xem xét ví dụ sau:

(Hệ 10)

Địa chỉ IP (nhị phân)	11000000	10101000	00001010	00101100	192.168.10.44
Mặt nạ mạng (nhị phân)	11111111	11111111	11111111	11111000	255.255.255.248
AND bit					
Id mặt nạ mạng	11000000	10101000	00001010	00101000	192.148.10.40

Trong ví dụ, địa chỉ IP 192.168.10.44 tương ứng với chuỗi bit trên cùng. Mặt nạ mạng con 255.255.255.248 tương ứng với chuỗi bit thứ hai. Áp dụng phép AND trên từng bit của hai địa chỉ này, ta sẽ nhận được id của mặt nạ mạng con là 192.148.10.40 tương ứng với chuỗi bit cuối cùng, không tính địa chỉ máy. Các máy khác trong mạng con này sẽ có dải IP từ 192.148.10.40 (tương ứng với 000), .41 (tương ứng với 001), v.v..., cho đến .47 (tương ứng với 111) của 3 bit còn lại.

Do mặt nạ mạng con tuân theo quy luật bắt đầu một tập các bit 1 và kết thúc với các bit 0 nên để viết ngắn gọn, ta chỉ cần ghi số lượng số 1. Trong ví dụ, mặt nạ gồm 27 số 1 nên ta chỉ cần ghi là /27.

Địa chỉ IP	9.100.100.100
Mặt nạ (hệ 10)	255 . 255 . 255 . 224
Mặt nạ (hệ nhị phân)	11111111 11111111 11111111 11100000
Dạng viết gọn	9.100.100.100/27

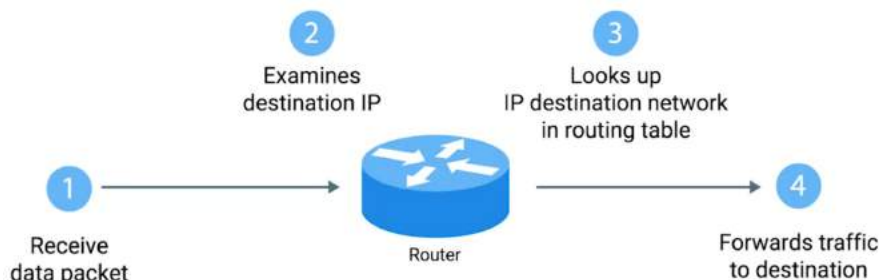
5. Cách thức định tuyến

Định tuyến

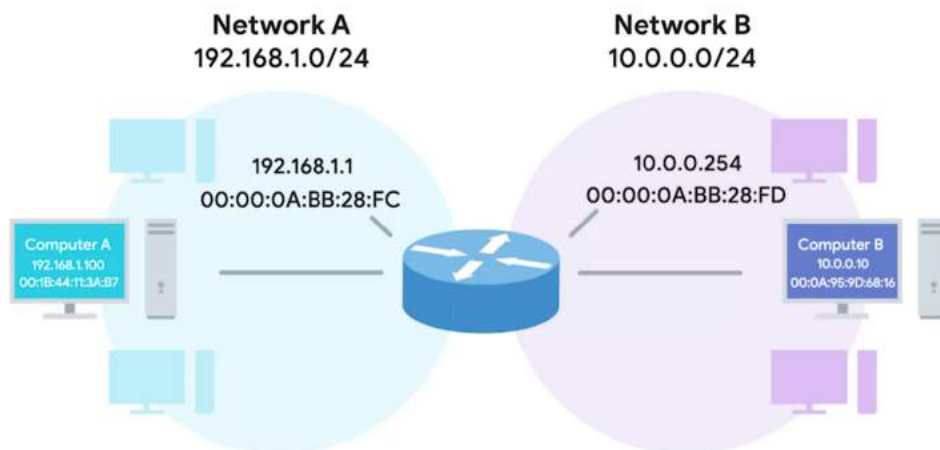
Để kết nối nhiều mạng khác nhau, chúng ta sử dụng thiết bị gọi là bộ định tuyến (router). Thiết bị này giúp chuyển tiếp gói tin giữa các mạng khác nhau, kể cả mạng có dây và không dây. Để định tuyến một gói tin từ máy nguồn đến máy đích, router thường tiến hành bốn bước chính:

1. Nhận dữ liệu từ một máy
2. Kiểm tra IP máy đích
3. Trang mạng của IP này trong bảng định tuyến

4. Chuyển gói tin đến mạng đích



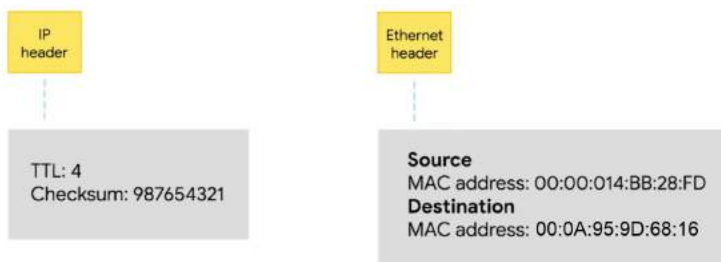
Ví dụ một máy tính A có địa chỉ là 192.168.1.100 muốn gửi dữ liệu đến máy tính B có địa chỉ là 10.0.0.10. Máy tính A tra bảng ARP cục bộ của nó để xác định địa chỉ MAC của máy B, tuy nhiên nó phát hiện không có. Điều này đồng nghĩa với việc máy B không nằm trong cùng mạng con với nó. Lúc này máy tính A gửi gói tin đến địa chỉ MAC của router. Router nhận và xử lý gói tin này bởi vì địa chỉ đích đề cập đến chính nó. Router mở gói tin ra để xác định IP đích mà máy A muốn gửi.



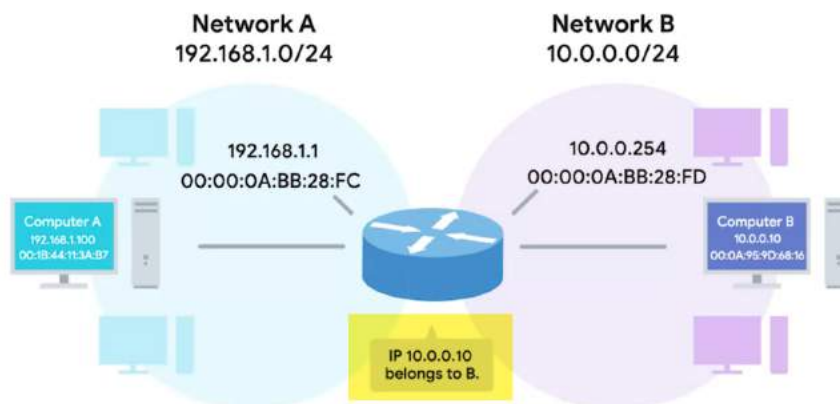
Router tra địa chỉ 10.0.0.10 trong bảng định tuyến (routing table) để xác định mạng mà địa chỉ này thuộc về. Bảng định tuyến là bảng dữ liệu chứa danh sách các đường đi đến mạng đích. Đối với ví dụ trên, địa chỉ IP thuộc mạng B. Bởi vì mạng B có kết nối một bước (nối trực tiếp) nên router sẽ tra được địa chỉ MAC của máy B trong ARP của nó.

Network name	Network range
A	192.168.1.0/24
B	10.0.0.0/24

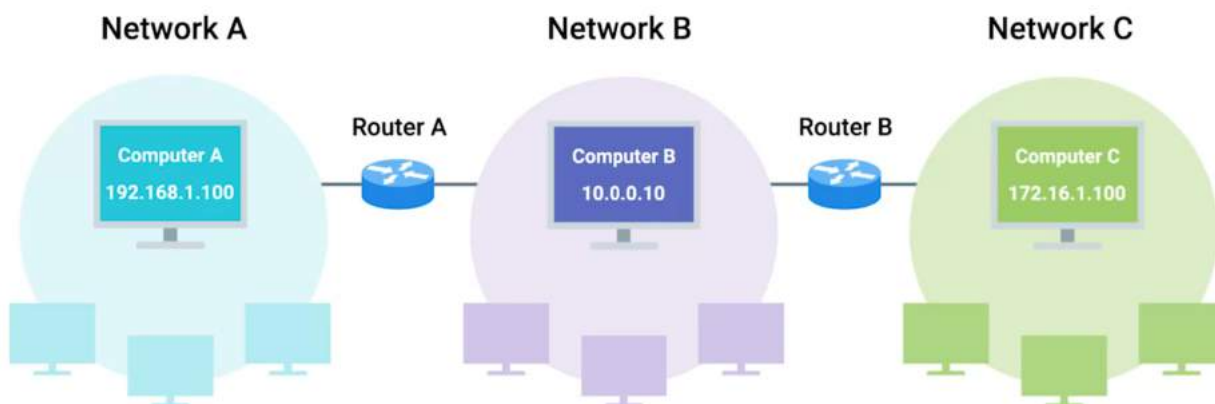
Router đóng gói lại gói tin với MAC nguồn là địa chỉ MAC của chính nó và MAC đích là của máy B. Các giá trị như TTL (time to live) và checksum cũng được cập nhật do gói tin đã thay đổi.



Router gửi gói tin này đến máy B.



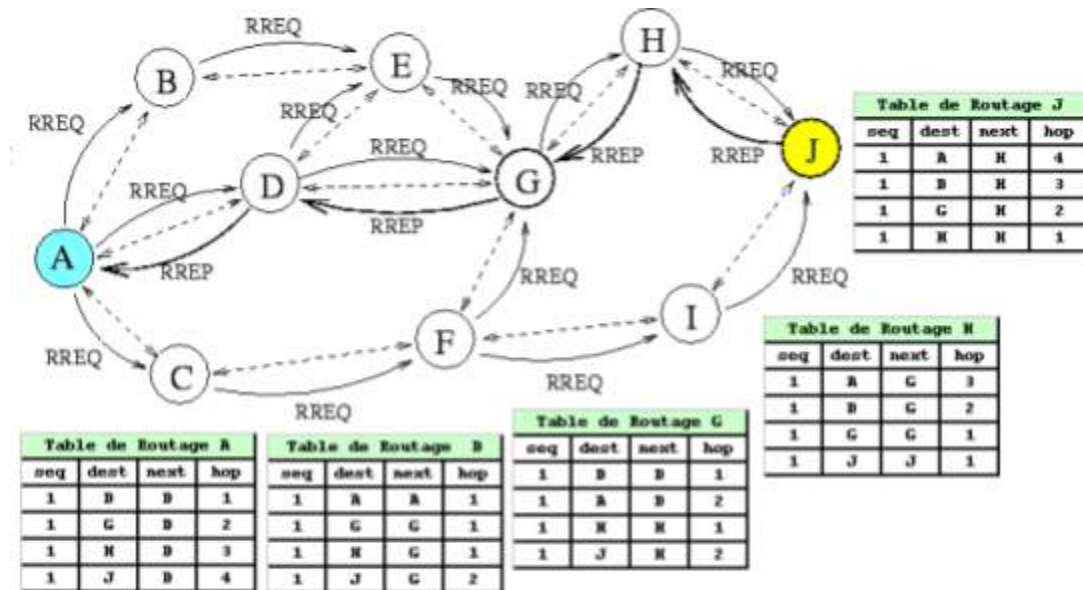
Quá trình diễn ra tương tự trong trường hợp gói tin được gửi ở những máy nằm ở các mạng xa hơn.



Bảng định tuyến

Bảng định tuyến (routing table) là bảng dữ liệu chứa danh sách các đường đi đến mạng đích. Chúng thường có bốn cột. Hai cột đầu về mạng đích (destination network)

chứa thông tin về các mạng mà router biết. Mỗi mạng gồm mã mạng, mặt nạ mạng. Cột thứ ba là nút kế tiếp (next hop), đó chính máy được kết nối trực tiếp đến router mà có thông tin về mạng đích. Cột cuối cùng là tổng bước (total hops) chính là tổng số router cần qua để đi đến đích một cách ngắn nhất.



Nguồn: Wikimedia

Số hiệu mạng ASN

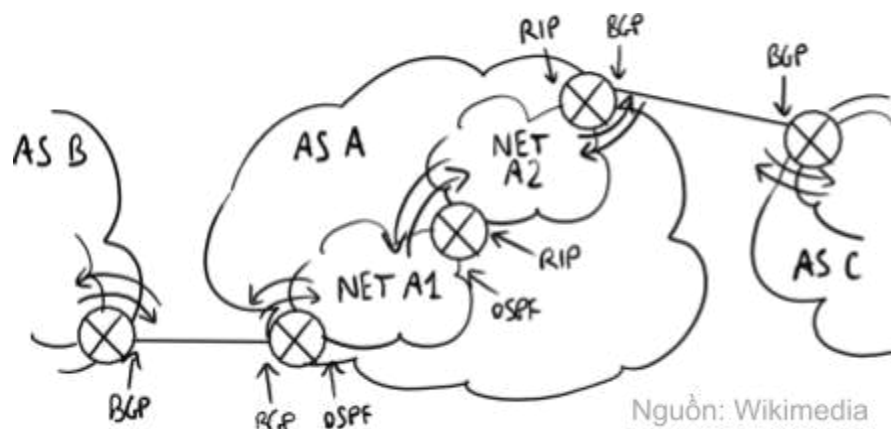
Số hiệu mạng (ASN – Autonomous System Number) là số được sử dụng để định danh một mạng tham gia vào các hoạt động định tuyến chung trên Internet. Số này do tổ chức cấp phát số hiệu Internet (IANA) quản lý.

Các giao thức định tuyến

Giao thức định tuyến là cách thức các router giao tiếp với router khác để chia sẻ thông tin nhằm tìm ra đường đi ngắn nhất đến mạng đích. Có 2 loại giao thức định tuyến là loại giao thức cổng trong và loại giao thức cổng ngoài.

Loại giao thức cổng trong là cách thức chia sẻ thông tin nội bộ bên trong một hệ thống tự trị (AS – autonomous System). Hệ thống tự trị là một tập hợp các router được đặt dưới sự quản lý chung của một tổ chức, công ty. Hai giao thức phổ biến thuộc nhóm này là RIP và OSPF.

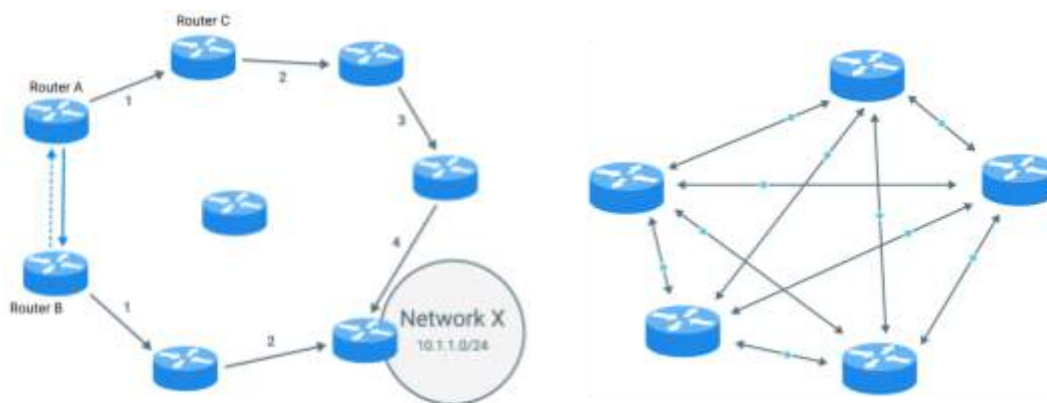
Loại giao thức cổng ngoài là cách thức chia sẻ thông tin giữa các tổ chức với nhau. Trong loại này, giao thức phổ biến là BGP.



Giao thức cổng trong được chia thành 2 giao thức con, đại diện cho 2 cách để duy trì trạng thái kết nối và cập nhật đường đi. Giao thức thứ nhất là giao thức định tuyến vectơ khoảng cách và giao thức con thứ hai là định tuyến trạng thái liên kết (link state).

Giao thức định tuyến vectơ khoảng cách dựa trên các kết nối láng giềng mà thường được mô tả với tên RIP (routing information protocol). Giao thức này không cần lưu trữ nhiều thông tin, tuy nhiên việc định tuyến không đảm bảo ra đường đi tốt hay không được cập nhật liên tục.

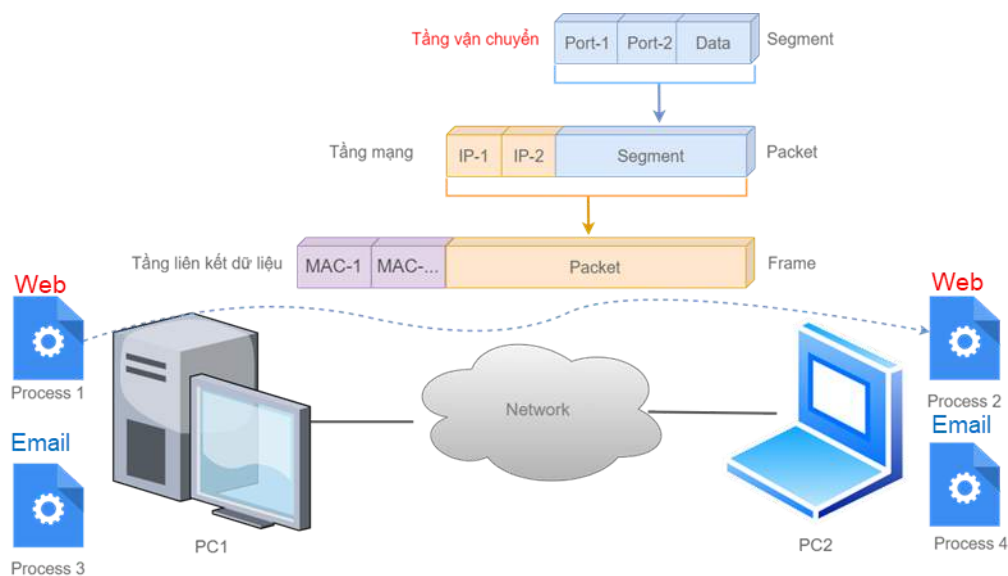
Trong khi đó, giao thức định tuyến trạng thái liên kết dựa trên liên kết đầy đủ của từng cặp router để tìm đường đi tối ưu. Giao thức này được biết đến với tên OSPF (open shortest path first). Giao thức OSPF tốn nhiều không gian lưu trữ cũng như đòi hỏi tính toán nhiều, tuy nhiên nó lại cho kết quả định tuyến tốt hơn.



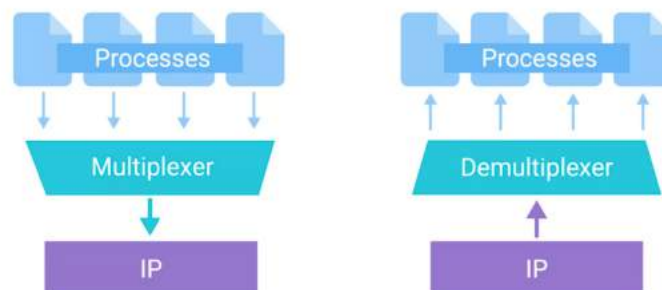
Bài đọc 6. Tầng Vận Chuyển

1. Chức năng và vai trò của tầng vận chuyển

Tầng vận chuyển thực hiện chuyển gói tin giữa các ứng dụng ở máy nguồn và máy đích. Hay nói cách khác, do trên một máy tính, chúng ta có rất nhiều chương trình cùng chạy, nên tầng vận chuyển sẽ phải tổ chức, sắp xếp chương trình nào trên máy đích sẽ nhận dữ liệu từ chương trình nào trên máy nguồn. Tầng vận chuyển có hai giao thức thông dụng là TCP và UDP.

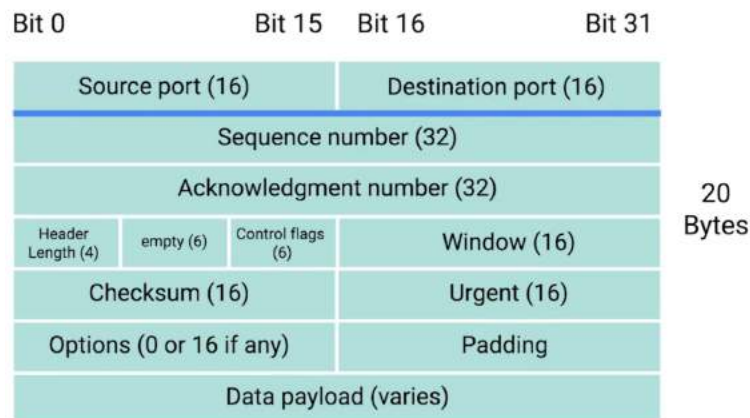


Để tiết kiệm tài nguyên đường truyền, tầng vận chuyển thực hiện ghép nhiều chuỗi dữ liệu của các ứng dụng lại để truyền đi một lần. Quá trình này gọi là multiplexing được thực hiện bởi bộ multiplexer, quá trình tách được gọi là demultiplexing.



2. Gói tin TCP Segment

TCP segment là gói tin được hình thành ở tầng vận chuyển, sau đó được đóng gói thành IP datagram ở tầng mạng, và khung tin Ethernet ở tầng liên kết dữ liệu. Cấu trúc TCP segment gồm hai phần chính là TCP header và dữ liệu được nhận từ tầng ứng dụng.



Hai thành phần đầu tiên của TCP Header là port nguồn và đích để biểu diễn cổng mà ứng dụng nguồn gửi dữ liệu và ứng dụng đích xử lý nó. Port máy nguồn thường được chọn từ một miền đặc biệt có giá trị cao, các port này chỉ là các port tạm thời (ephemeral port).

Thành phần thứ ba là số thứ tự. Đây là chỉ số xác định TCP segment đang chứa đoạn nào của dữ liệu đang truyền. Do dữ liệu ban đầu có thể kích thước lớn, không thể vừa cho một gói tin TCP segment nên chúng phải tách thành nhiều đoạn dữ liệu nhỏ hơn. Chính vậy ta cần đánh số thứ tự để có thể ghép lại đúng sau này.

Các phần còn lại của gói tin TCP Header gồm Acknowledgement number là chỉ số segment được mong đợi tiếp theo; thành phần kế cho biết độ dài của header; cờ điều khiển để xác định gói tin TCP; cửa sổ TCP là miền các số tuần tự; checksum để kiểm tra lỗi; urgent để xác định độ quan trọng của gói tin; options chứa các chức năng thêm và padding là làm cho header có kích thước đầy đủ.

Để kiểm soát tiến trình giao tiếp giữa hai máy, TCP tạo ra một số cờ để các bên biết được những gì cần thực hiện. Có tổng cộng 6 cờ khác nhau. Cờ thứ nhất là URG, để nói rằng gói tin này là cấp bách và cần xử lý dữ liệu trong này. Cờ ACK, yêu cầu xác nhận và kiểm tra số thứ tự Ack. Cờ PSH yêu cầu thiết bị nhận đẩy dữ liệu nằm trong vùng đệm đến ứng dụng cần xử lý càng sớm càng tốt. Cờ RST để thực hiện lại từ đầu. Cờ SYN để yêu cầu kiểm tra số phân đoạn cho việc đồng bộ. Cờ FIN để đóng kết nối.

3. Giao thức trên tầng vận chuyển

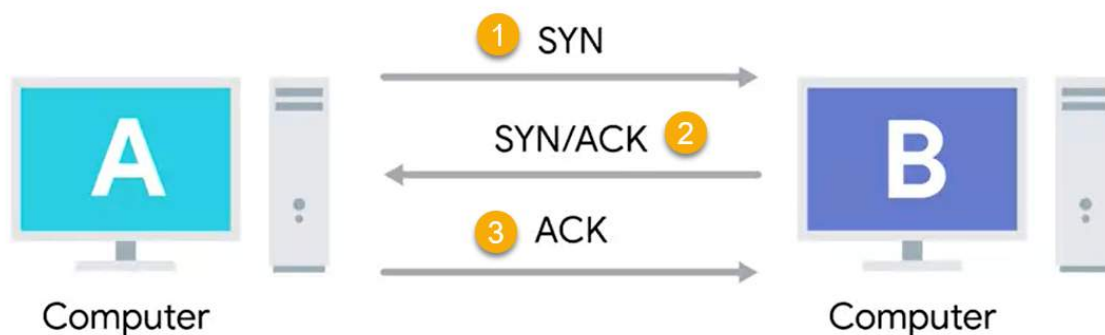
Giao thức hướng kết nối (TCP) và phi kết nối (UDP)

Giao thức hướng kết nối là giao thức yêu cầu phải khởi tạo kết nối trước khi gửi dữ liệu và đảm bảo dữ liệu được gửi tin cậy. Để đạt được điều đó, mỗi đoạn dữ liệu gửi đều phải được xác nhận bởi bên nhận. Giao thức TCP là giao thức hướng kết nối. Khi một gói tin vì vấn đề gì đó không nhận được phản hồi, máy gửi sẽ thực hiện gửi lại nó. Nhờ có số thứ tự trên từng gói nên bên nhận vẫn đảm bảo xử lý được các gói tin một cách đúng đắn.

Giao thức phi kết nối là giao thức không cần khởi tạo trước khi gửi dữ liệu, do đó dữ liệu không đảm bảo sẽ đến được đích. Giao thức này phù hợp cho việc gửi dữ liệu không quá quan trọng, việc mất mát một mảnh dữ liệu có thể không ảnh hưởng nhiều. Điểm lợi của giao thức này là tốc độ sẽ nhanh hơn do không thực hiện quá nhiều bước xác nhận dữ liệu. Một số ứng dụng như hội nghị truyền hình, việc mất vài khung hình trong quá trình truyền sẽ không gây ảnh hưởng nhiều. UDP (User Datagram Protocol) là một giao thức phi kết nối.

Cơ chế bắt tay 3 bước

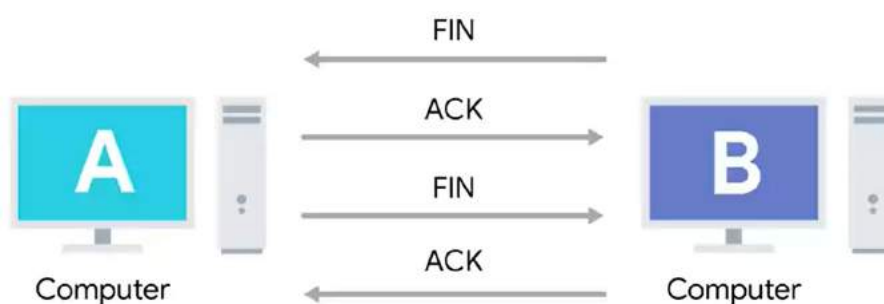
Do cơ chế TCP là cơ chế đảm bảo gói tin được nhận đầy đủ và chính xác, nên trước khi truyền dữ liệu, giao thức TCP cần khởi tạo và thiết lập kênh kết nối. Quá trình khởi tạo được thực hiện theo quy trình bắt tay 3 bước (three way handshake).



Trong bước 1, máy A gửi gói TCP segment với cờ SYN bật lên để khởi tạo kết nối đến B và đi kèm 1 con số tuần tự (SEQ) để xác định gói tin sẽ gửi tiếp theo. Trong bước 2, máy B gửi ngược lại gói tin với cờ SYN và ACK bật lên để nói rằng đồng ý kết nối. Tại bước 3, máy A gửi tiếp gói tin với cờ ACK để xác nhận rằng đã nhận được lời đồng ý và sẽ bắt đầu tiến hành truyền dữ liệu.

Khi cơ chế bắt tay hoàn thành, 2 máy sẽ gửi dữ liệu cùng với thông tin SEQ và ACK để biết những gì đã được gửi và nhận. Ví dụ, khi server nhận được gói tin, nó sẽ dùng một số để theo vết gói tin. Số này chính là số thứ tự nó sẽ mong đợi ở gói tin tiếp theo. Với cách này, dữ liệu sẽ được truyền đầy đủ và chính xác.

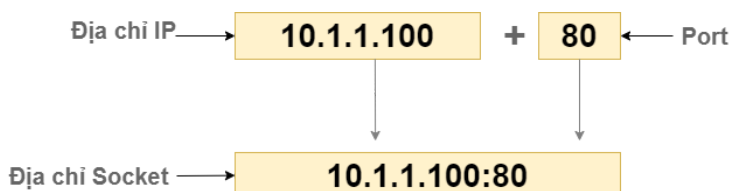
Khi muốn kết thúc kết nối, TCP thực hiện quá trình bắt tay 4 bước. Hai máy lần lượt gửi các gói tin với cờ FIN và cờ ACK. Như trong hình dưới, máy B gửi gói tin với cờ FIN để thông báo đóng kết nối, máy A khi nhận được sẽ gửi gói tin phản hồi với cờ ACK để xác nhận đã nhận được gói tin. Máy A cũng gửi một gói tin với cờ FIN để thông báo nó cũng đóng kết nối và đến lượt máy B sẽ phản hồi lại là đã nhận được gói tin.



4. Cổng và socket

Cổng và số hiệu socket

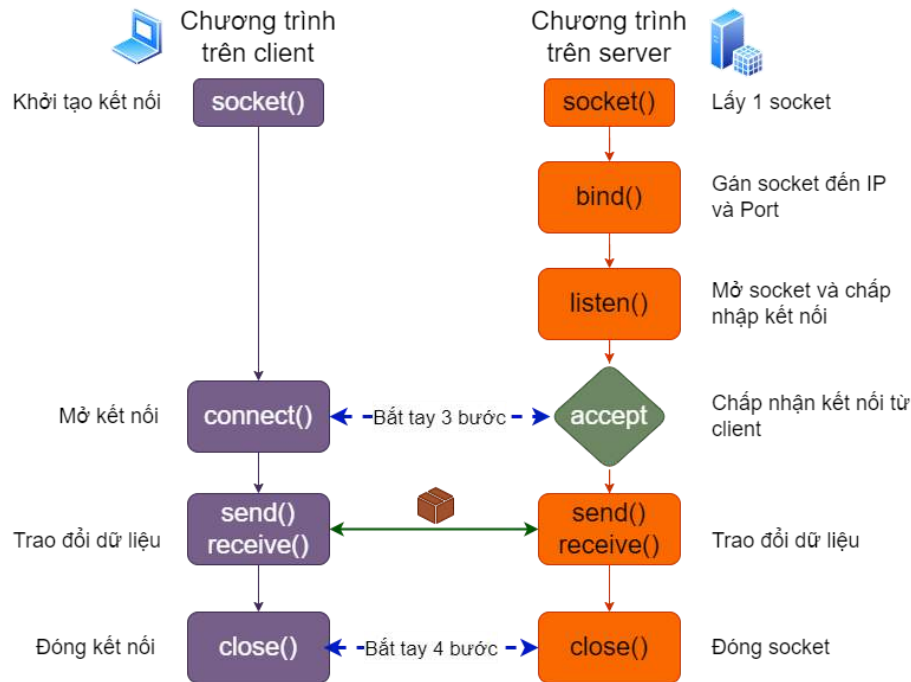
Các dịch vụ mạng khác nhau khi chạy sẽ lắng nghe tín hiệu ở các cổng xác định. Thuật ngữ hay dùng là cổng (port). Cổng là một số 16 bit được viết với dấu hai chấm sau địa chỉ IP. Như vậy, về mặt lý thuyết có 65.535 cổng có thể có. Chuỗi sau khi viết được gọi là địa chỉ socket hay số hiệu socket.



TCP Socket và các trạng thái

TCP socket là điểm đầu cuối trong giao tiếp của hai chương trình. Hình bên dưới mô tả quá trình giao tiếp giữa hai chương trình, một trên client, một trên server. Chương trình phía server sẽ lấy một socket và gán socket này đến IP và port cụ thể. Sau đó, nó sẽ mở socket và lắng nghe các kết nối từ các máy khác. Chương trình phía client khi muốn liên lạc với chương trình phía server sẽ khởi tạo cấu trúc với thông tin là địa chỉ socket gồm IP

và port của chương trình phía server. Tiếp theo, nó sẽ mở kết nối với quy trình bắt tay 3 bước và thực hiện gửi nhận dữ liệu.

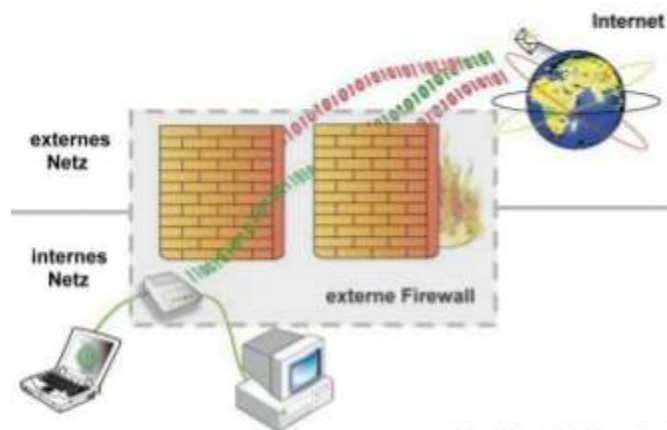


Trong quá trình thực thi, kết nối TCP sẽ trải qua một loạt các trạng thái của socket và các loại trạng thái này khác nhau ở mỗi hệ thống. Một số loại phổ biến gồm:

- Trạng thái LISTEN để cập socket đã sẵn sàng và lắng nghe kết nối đến, trạng thái này chỉ có ở phía máy chủ (server).
- Trạng thái SYN_SET mô tả yêu cầu đồng bộ đã được gửi nhưng kết nối chưa được khởi tạo, nó tương đương với bước 1 trong quy trình bắt tay 3 bước. Trạng thái này chỉ xuất hiện ở phía máy khách (client).
- Trạng thái SYN_RECEIVED mô tả yêu cầu đồng bộ đã được nhận và đã gửi lại gói tin SYN_ACK, nó tương đương với bước 3 trong bắt tay 3 bước. Trạng thái này chỉ xuất hiện ở phía máy chủ.
- Trạng thái ESTABLISHED mô tả kết nối đã được thiết lập, có thể gửi/nhận dữ liệu.
- Trạng thái FIN_WAIT mô tả trạng thái đã gửi tín hiệu FIN nhưng chưa nhận được tín hiệu ACK.
- Trạng thái CLOSE_WAIT mô tả kết nối đã đóng ở tầng TCP nhưng ứng dụng mở socket chưa giải phóng kết nối này.
- Trạng thái CLOSED mô tả kết nối đã đóng hoàn toàn.

5. Giới thiệu về tường lửa

Tường lửa là một hệ thống bảo mật mạng. Tường lửa thực hiện việc giám sát và ngăn chặn các giao tiếp không hợp lệ dựa trên các quy tắc đã định ra trước. Ở tầng vận chuyển, tường lửa giúp ngăn chặn giao tiếp ở các cổng xác định. Tường lửa đôi khi là thiết bị mạng độc lập, nhưng ta có thể coi chúng như một chương trình có thể chạy ở mọi chỗ. Đối với nhiều công ty và hầu hết tất cả người dùng gia đình, chức năng của router và tường lửa được thực hiện bởi cùng một thiết bị. Tường lửa cũng có thể chạy trên các máy chủ riêng lẻ thay vì là một thiết bị mạng. Tất cả các hệ điều hành đều có chức năng tường lửa được tích hợp sẵn. Bằng cách này, việc chặn hoặc cho phép lưu lượng đến các cổng khác nhau được thực hiện một cách tốt hơn.



Nguồn: Wikimedia

Bài đọc 7. Tầng Ứng Dụng

1. Vai trò và đặc điểm của tầng ứng dụng

Vai trò và giao thức

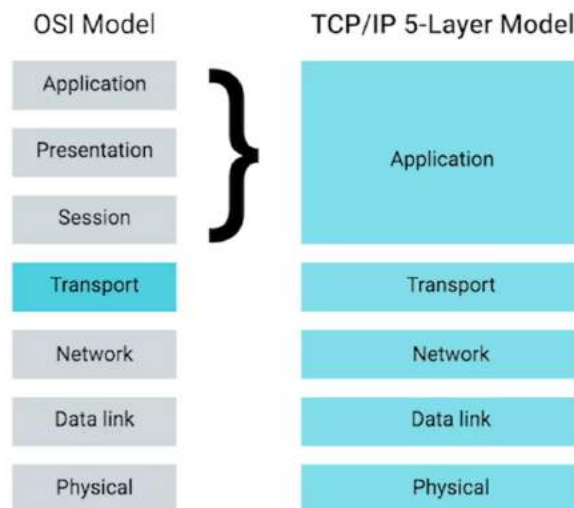
Tầng cuối cùng trong mô hình 5 lớp là tầng ứng dụng. Đây là tầng xác định cách dữ liệu được định dạng, mã hóa, giải mã, trình tự giao tiếp, v.v... và được thống nhất giữa các ứng dụng.

Nội dung gói tin của tầng ứng dụng là toàn bộ nội dung của bất kỳ ứng dụng dữ liệu nào muốn gửi cho nhau. Đó có thể là nội dung của một trang web, nếu một trình duyệt web đang kết nối với một máy chủ web. Cũng có thể là nội dung video trực tuyến của ứng dụng Netflix trên PlayStation kết nối với máy chủ Netflix.

So với các tầng bên dưới chỉ có 1 đến 2 giao thức chuẩn thì tầng này chứng kiến rất nhiều giao thức khác nhau như HTTP, FTP, SMTP, POP, TELNET, DHCP, DNS, v.v. tùy thuộc vào cách các ứng dụng giao tiếp với nhau. Ví dụ, trong quá trình duyệt web, ta thấy có rất nhiều trình duyệt khác nhau như Chrome, Internet Explorer, Safari. Các trình duyệt web liên lạc với máy chủ để yêu cầu nội dung. Các máy chủ web phổ biến nhất là Microsoft IIS, Apache và nginx. Tuy nhiên, dù trình duyệt web hay máy chủ nào, chúng cần nói chuyện với cùng giao thức. Giao thức phổ biến trong trường hợp này là HTTP. Tuy nhiên, giao thức này không phù hợp cho các trao đổi đòi hỏi an toàn nên một giao thức bổ sung là HTTPS.

So sánh tầng ứng dụng mô hình OSI

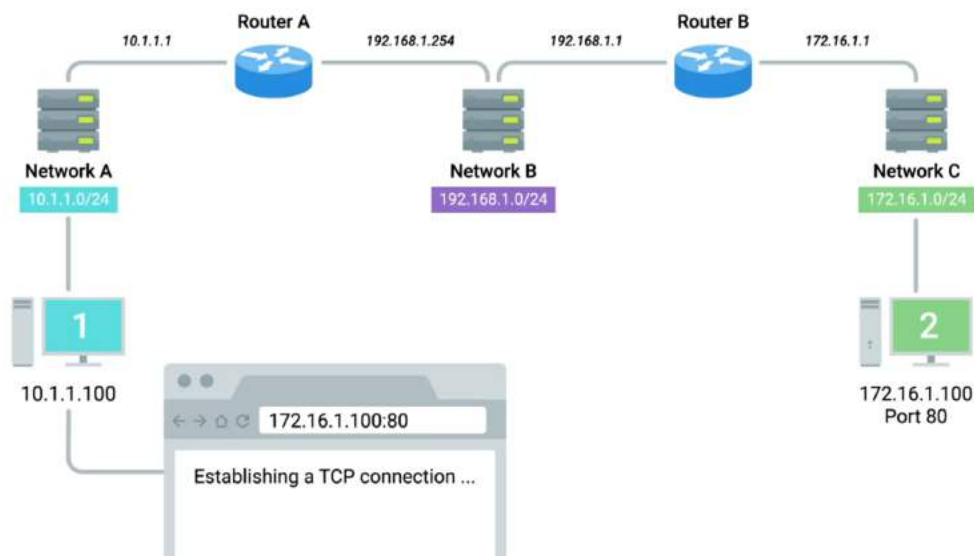
Một mô hình khác cũng phổ biến ngày nay là mô hình OSI gồm 7 tầng. So với mô hình 5 tầng thì OSI bổ sung thêm 2 tầng ở giữa tầng vận chuyển và tầng ứng dụng. Cụ thể là tầng phiên và tầng trình diễn. Người ta thường xem 3 tầng trên cùng này tương đương với tầng ứng dụng trong mô hình 5 tầng nhưng có tính chuyên biệt cao hơn.



Cụ thể, tầng thứ năm trong mô hình OSI là tầng phiên. Tầng phiên chịu trách nhiệm về những thứ như tạo điều kiện giao tiếp giữa các ứng dụng thực tế và tầng vận chuyển. Trong khi đó, tầng trình bày chịu trách nhiệm đảm bảo rằng dữ liệu tầng ứng dụng chưa được đóng gói thực sự có thể được hiểu bởi ứng dụng liên quan. Tầng này trên máy truyền dữ liệu làm nhiệm vụ dịch dữ liệu được gửi từ tầng ứng dụng sang định dạng chung. Và tại máy tính nhận, lại chuyển từ định dạng chung sang định dạng của tầng ứng dụng. Ngoài ra có thể thực hiện việc nén dữ liệu. Tầng cuối cùng của mô hình OSI là tầng ứng dụng và có chức năng khá tương tự trên mô hình 5 tầng.

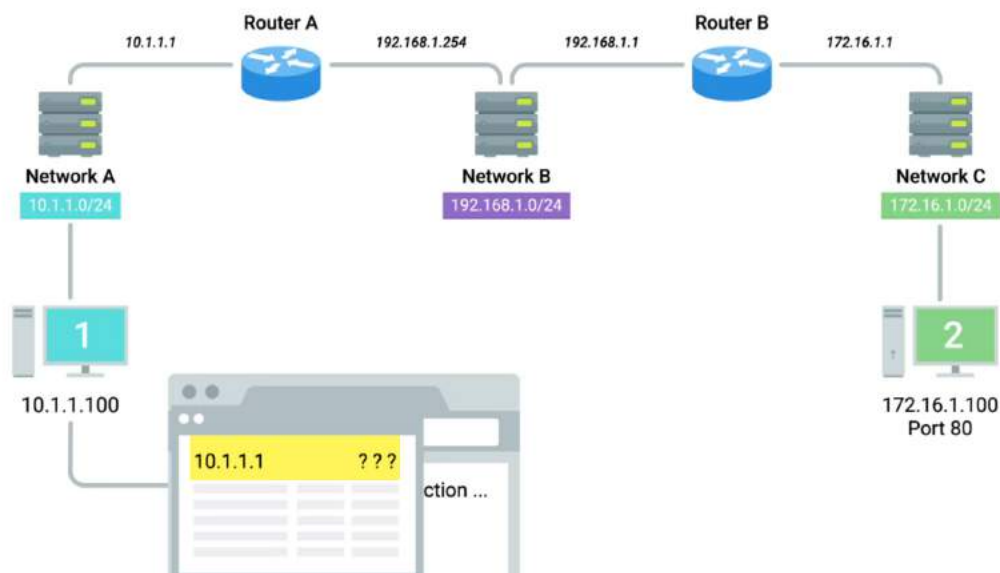
2. Quá trình thực thi của 5 tầng

Để hiểu toàn bộ cách thức mô hình mạng 5 tầng làm việc, chúng ta cùng đi qua một tình huống ví dụ. Một mạng máy tính gồm 3 mạng con được gọi là A, B, C như hình bên dưới.

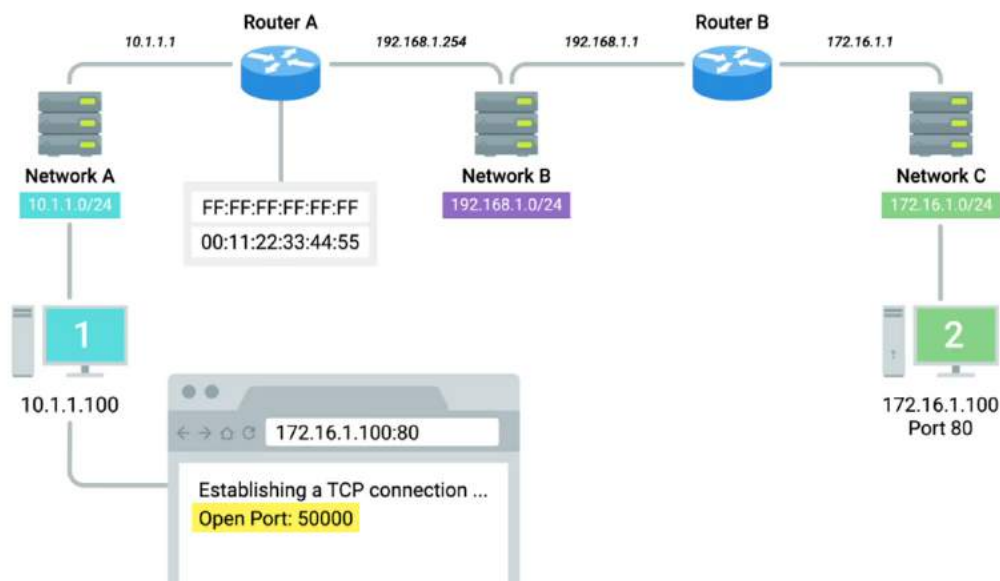


Mạng A có địa chỉ là 10.1.1.0/24, mạng B có địa chỉ là 192.168.1.0/24, và mạng C có địa chỉ là 172.16.1.0/24. Đó cũng là địa chỉ của các thiết bị Switch trong mạng tương ứng. Các mạng này nối với nhau bởi 2 router. Một máy khách (máy 1) chạy trình duyệt Web để yêu cầu nội dung được đặt tại mạng A và một máy chủ (máy 2) phục vụ nội dung được đặt tại mạng C.

Trình duyệt trên máy 1 muốn truy cập trang web có địa chỉ 172.16.1.100:80. Tuy nhiên, máy 1 phát hiện máy có địa chỉ 172.16.1.100 không ở cùng mạng với mình nên cần phải gửi gói tin đến Router A để router này định tuyến gói tin đến đích giúp. Để máy 1 gửi gói tin đến Router A thì nó cần biết địa chỉ MAC của router này. Giả sử nó tra bảng ARP cục bộ, nhưng không thấy. Vì vậy, máy 1 sẽ gửi gói tin broadcast ra toàn bộ mạng với IP đích: FF: FF: FF: FF.

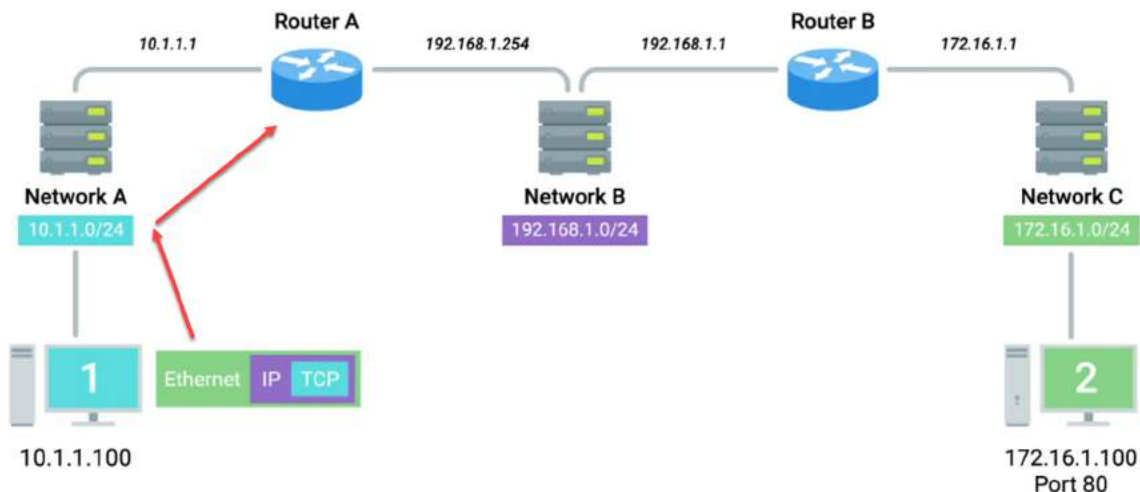


Router A nhận gói tin và phát hiện ra IP đích là FF:FF:FF:FF, nó biết là gửi cho chính nó. Router A gửi trả lại gói tin với địa chỉ MAC của nó. Máy 1 có được địa chỉ MAC của Router A nên tiến hành khởi tạo một socket để giao tiếp TCP giữa trình duyệt với chương trình đang lắng nghe ở port 80 trên máy 2. Giữa sử máy 1 mở port 50000.



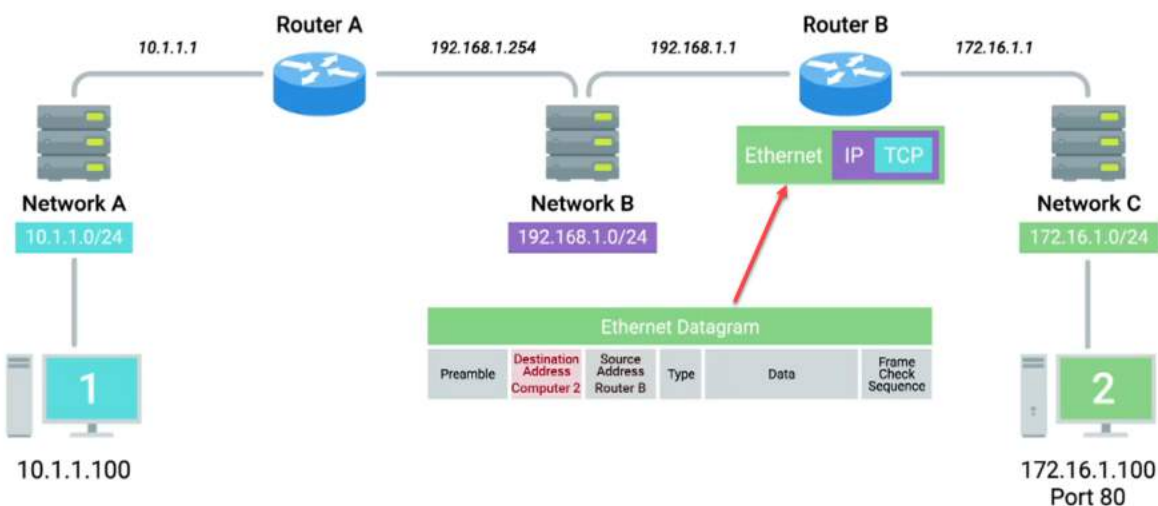
Tầng vận chuyển ở Máy 1 tạo gói tin TCP Datagram với port máy nguồn là 50000, port máy đích: 80, v.v... cùng với dữ liệu từ tầng ứng dụng. Tiếp theo, tầng mạng đóng gói TCP diagram vào thành gói IP datagram với IP máy nguồn 10.1.1.100, IP máy đích 172.16.1.100, thời gian sống (TTL) là 64 cùng với các thông tin khác. Xuống tới tầng liên kết dữ liệu, nó tiếp tục đóng gói IP datagram thành Ethernet Datagram với địa chỉ MAC của máy nguồn,

địa chỉ MAC của router cùng các trường thông tin liên quan. Tầng vật lý gửi gói tin đến Switch của mạng A và đến lượt Switch chuyển nó đến Router A.

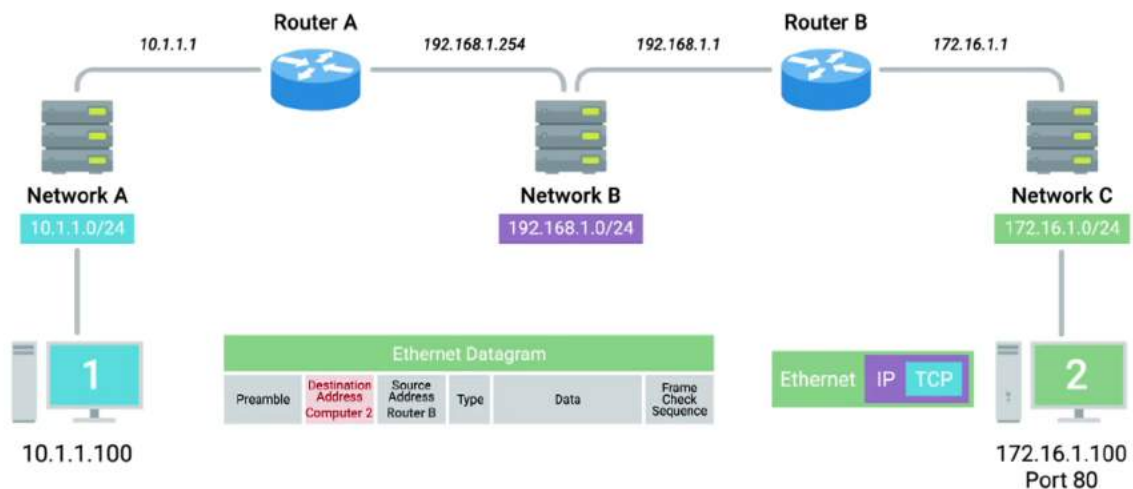


Router A bóc gói IP datagram và biết được địa chỉ IP đích mà nó cần gửi đến. Dựa trên IP, Router A biết được máy đích thuộc mạng nào. Router A tra bảng định tuyến để biết đường đi đến mạng của máy đích. Kết quả, đường đi ngắn nhất là đi qua Router B. Để chuyển gói tin đến Router B, Router A tra bảng ARP cục bộ để xác định địa chỉ MAC của Router B. Router A đóng gói lại gói tin Ethernet với địa chỉ MAC được cập nhật và tiếp gửi gói tin đi.

Khi gói tin đến Router B, Router B bóc gói tin ra và xác định được IP đích cần gửi đến, trong trường hợp này là IP của máy 2. Router B tra ARP và biết được địa chỉ MAC của máy 2 nên cập nhật lại thông tin trên gói Ethernet và gửi gói tin đến máy 2.



Máy 2 biết được gói tin gửi cho nó và thực hiện bóc gói tin ra để xác định ai gửi cho mình (IP Máy 1), muốn gì (cờ điều khiển) và ứng dụng nào sẽ trả lời (port 80). Quá trình máy 2 gửi thông tin phản hồi cũng thực hiện tương tự.



Bài đọc 8. Hệ Thống Phân Giải Tên Miền

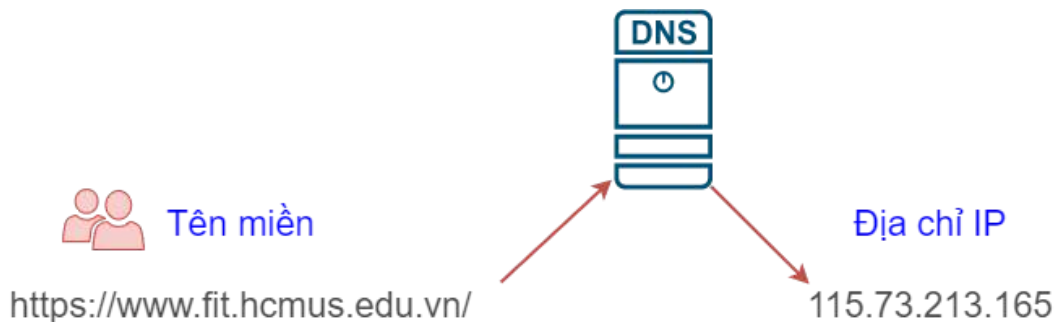
1. Tên miền và hệ thống phân giải tên miền

Tên miền và hệ thống phân giải

Để định danh các máy tính, người ta sử dụng địa chỉ IP. Chúng ta tập trung vào địa chỉ IPv4 trước. Địa chỉ IP là số gồm 4 octet, mỗi octet là nhóm 8 bit. Có thể xem IP là một chuỗi gồm 4 số thập phân, mỗi số có giá trị từ 0 đến 255. Để có thể giao tiếp với máy chủ (server), chúng ta cần biết được địa chỉ IP của nó. Tuy nhiên, việc nhớ địa chỉ IP của các máy chủ là điều không dễ đối với người dùng. Ngoài ra, công ty cung cấp dịch vụ có thể dời máy chủ của họ đến một nơi khác, dẫn đến máy này sẽ có IP mới. Công ty phải tìm cách thông báo địa chỉ mới này đến tất cả người dùng của họ, đồng thời người dùng cũng phải nhớ IP mới. Điều này đặt ra rất nhiều khó khăn cho tất cả các bên. Vì vậy, các nhà phát triển đã tạo ra tên miền (domain name).



Tên miền là một chuỗi các ký tự chữ cái để đại diện cho những tài nguyên Internet mà đa số được đánh địa chỉ bằng các con số. Điều này giúp cho con người dễ nhớ hơn. Mặc dù tên miền dễ nhớ cho con người, nhưng việc truy cập máy chủ vẫn cần có một địa chỉ IP của máy chủ đó. Để giải quyết vấn đề này, người ta tạo ra một dịch vụ gọi là hệ thống phân giải tên miền, viết tắt là DNS. Đây là dịch vụ biến đổi một chuỗi ký tự thành một địa chỉ IP.



Một điểm lợi nữa khi sử dụng DNS là khi một tổ chức mong muốn người dùng ở mỗi khu vực khác nhau truy cập đến máy chủ gần với họ nhất nhằm cải thiện tốc độ truy cập

dữ liệu. Để làm được điều này, cùng một tên miền, DNS có thể phân giải ra địa chỉ IP tùy vào khu vực của người dùng.

Cấu tạo tên miền

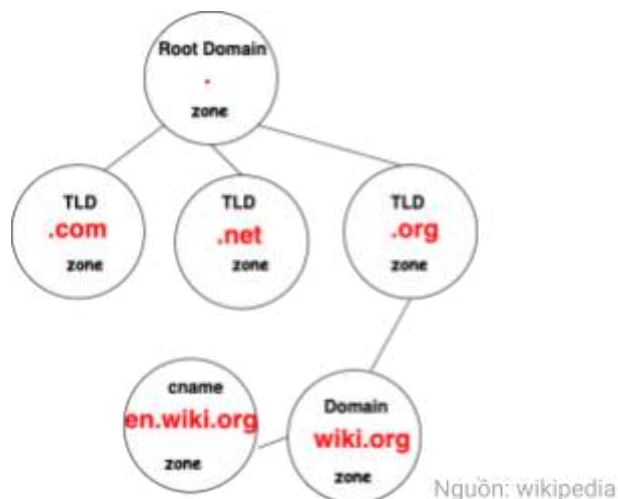
Tên miền bao gồm 3 thành phần chính gồm tên miền cấp cao, tên miền chính và tên miền phụ. Tên miền cấp cao được cấp phát và quản lý bởi tổ chức ICANN, một số tên miền cấp cao như .com, .net, .org, .vn. Tên miền chính được cấp phát và quản lý bởi tổ chức độc lập mà chúng ta hay gọi là nhà đăng ký tên miền. Một số tên miền chính như google, facebook, wikipedia. Tên miền phụ có thể xem như đó là tên máy chủ xử lý và trả về nội dung cho người dùng, tên này được đặt bởi nhà phát triển server.



Nguồn: wikimedia

Một tên miền có đầy đủ 3 thành phần được gọi là tên miền đủ điều kiện, gọi tắt là FQDN. Mỗi nhãn trong tên miền có độ dài tối đa 63 ký tự và tổng độ dài giới hạn là 255 ký tự.

Một tên miền có thể có nhiều tên miền con, để có thể quản lý việc phân giải tên miền một cách tốt hơn, người ta chia thành nhiều vùng khác nhau. Các vùng này được gọi là DNS Zone. Cấu trúc quản lý DNS Zone tuân theo cấu trúc phân tầng dạng cây.



Các DNS Zone được cấu hình thông qua các tập tin vùng (zone file). Các tập tin này chứa các bản ghi tài nguyên như SOA (Start of Authority), NS (name server), A, AAAA, CNAME, v.v... Có một loại tập tin đặc biệt là tập tin vùng tra cứu ngược (reverse lookup zone file) chứa bản ghi con trỏ (PTR) để chuyển IP ngược trở lại thành tên miền.

2. Máy chủ DNS

Máy chủ DNS và phân loại

Máy chủ DNS là máy tính chạy dịch vụ phân giải tên miền, chúng thường chứa một cơ sở dữ liệu của các IP và tên miền tương ứng. Dịch vụ này sử dụng một giao thức riêng để giao tiếp với các máy khác ở trong mạng.



Nguồn: Seobility

Máy chủ DNS được phân làm 5 loại chính gồm máy chủ tên miền đã lưu (caching name server), máy chủ tên miền đệ quy (recursive name server), máy chủ tên miền gốc

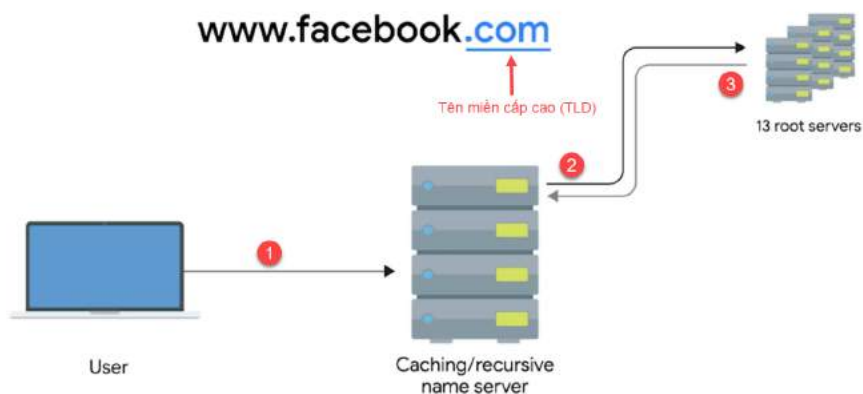
(root name server), máy chủ tên miền cấp cao (TLD name server), máy chủ tên miền có thẩm quyền (authoritative name server).

Phối hợp giữa các máy chủ DNS

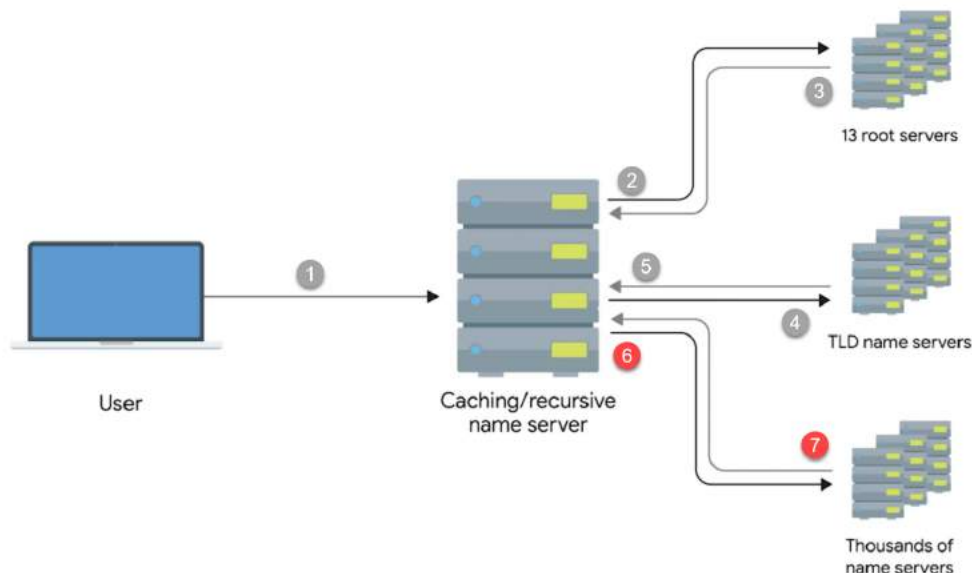
Khi có một yêu cầu phân giải tên miền, các loại DNS sẽ cùng tham gia để thực hiện yêu cầu này. Chúng ta cùng tìm hiểu cách các DNS phối hợp với nhau qua ví dụ sau.

Giả sử người dùng muốn truy cập trang web www.facebook.com. Để có địa chỉ IP của trang web đó, máy tính sẽ gửi yêu cầu đến một máy chủ DNS là máy chủ tên miền đã lưu, gọi tắt là CNS. Nếu CNS này có lưu trữ thông tin về tên miền facebook, nó sẽ trả về IP của tên miền này cho người dùng. Ngược lại, nếu CNS không có, máy chủ tên miền đệ quy (RNS) sẽ được hỏi.

Máy chủ RNS liên lạc tới một trong 13 server gốc (RS) bằng kỹ thuật anycast. Anycast là kỹ thuật được sử dụng để định tuyến gói tin đến các điểm đích khác nhau phụ thuộc trên các yếu tố như vị trí, độ nghẽn hay tình trạng liên kết. RS chỉ định một máy chủ tên miền cấp cao (TLD_NS) dựa trên phần đuôi trong tên miền của trang facebook, cụ thể là .com để xử lý tiếp yêu cầu.



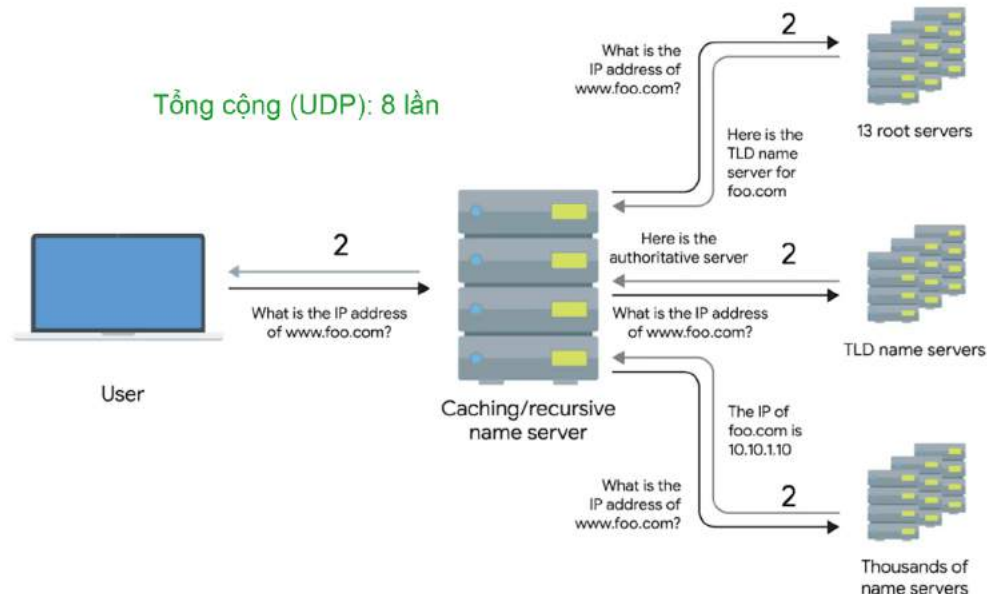
RNS biết được TLD_NS nên liên lạc tới máy chủ này để hỏi thông tin. TLD_NS khi nhận được yêu cầu sẽ tra cứu máy chủ tên miền có thẩm quyền (ANS) có thể trả lời IP của trang web và trả về cho RNS. RNS tiếp tục liên lạc với ANS để hỏi IP cụ thể của trang web. ANS tra cứu cơ sở dữ liệu và trả về địa chỉ IP của trang web. RNS lưu lại thông tin vào bộ nhớ để dành trả lời cho truy vấn lần sau (nếu có).



CNS và RNS thường được cấu hình trên cùng một máy vì khi RNS nhận được thông tin phân giải, RNS cũng lưu vào vùng nhớ để phục vụ truy vấn lần sau. Thông tin trong bộ nhớ có thời gian sống (time to live) nhất định. Sau đó, chúng sẽ bị xóa để cập nhật lại thông tin mới nhất của các máy chủ.

Giao thức của máy chủ DNS

Để phân giải một tên miền như toàn bộ quá trình trước, nếu DNS sử dụng giao thức TCP, nó sẽ mất ít nhất 44 lần gửi/nhận gói tin. Con số này thực sự lớn, nhất là chúng ta cần truy cập rất nhiều trang web trong ngày. Thay vào đó, DNS sử dụng giao thức UDP để thực hiện phân giải tên miền và tốn chỉ 8 lần gửi/nhận. Khi không nhận được gói tin, DNS chỉ cần gửi lại gói tin.



Ngày nay, DNS server có thể sử dụng cả 2 giao thức TCP, UDP để thực hiện phân giải tên miền vì một số gói tin phân giải tên miền lớn nên cần khởi tạo kết nối TCP. Tuy nhiên, UDP vẫn là phương thức phổ biến hơn.

Bản lưu thông tin trên máy chủ DNS

Thông tin phân giải tên miền được DNS server lưu dưới dạng các bản ghi trong cơ sở dữ liệu (resource record). Các thuộc tính của bản này được thể hiện trong bảng bên dưới. Mỗi bản ghi được phân theo từng loại khác nhau.

Trường	Mô tả
NAME	Tên bản ghi (ví dụ: tên miền)
TYPE	Loại bản ghi
CLASS	Mã lớp
TTL	Thời gian theo giây để RR còn hiệu lực
RDLENGTH	Độ dài trường RDATA
RDATA	Dữ liệu (ví dụ như địa chỉ IP, độ ưu tiên, v.v..)

Có nhiều loại bản ghi tài nguyên để máy chủ DNS phân biệt các thông tin cần trả về. Một số loại phổ biến như loại A dùng để ánh xạ tên miền thành địa chỉ IPv4, loại AAAA để ánh xạ tên miền thành địa chỉ IPv6, loại CNAME để chuyển tiếp tên miền thành tên miền khác, loại MX (Mail Exchange) để chuyển dịch vụ email đến server xác định. Loại SRV định

nghĩa vị trí của các dịch vụ khác, loại TXT chứa văn bản mô tả thông tin server. Loại NS mô tả máy chủ tên miền được cấp quyền cho một miền/miền con và loại SOA mô tả thông tin phân quyền từ phía máy chủ tiếp nhận tên miền.

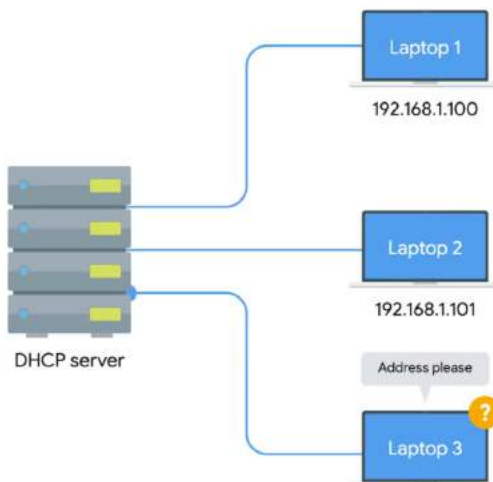
Nếu có nhiều bản ghi cho một tên miền, thì DNS server sẽ trả về tất cả các giá trị theo thứ tự dựa trên nguyên tắc xoay vòng (round robin). Nghĩa là nếu trước nó đã trả ra thứ tự 1, 2, 3 thì lần tiếp theo nó trả về 2, 3, 1 và lần tiếp nữa nó sẽ trả về 3, 2, 1. Điều này đảm bảo cho máy chủ nào cũng được sử dụng.

Name	Type	Data
www.foo.com	A	10.0.0.1
www.foo.com	A	10.0.0.2
www.foo.com	A	10.0.0.3

3. Giao thức DHCP

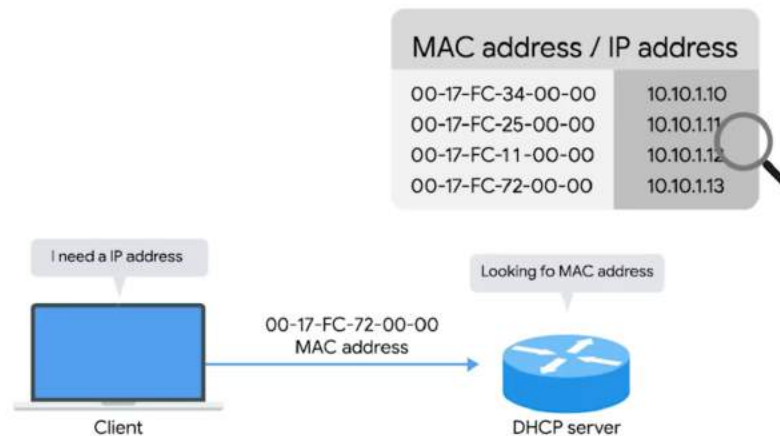
DHCP và chiến lược cấp phát địa chỉ IP

Các máy tính khi tham gia mạng đều cần có một IP. Tuy nhiên, việc gán thủ công từng thiết bị sẽ gây mất thời gian và công sức. DHCP là giao thức tự động tiến trình cấu hình cho các máy trong mạng. Một máy tính khi mới kết nối đến mạng, nó có thể hỏi máy chủ DHCP để nhận tất cả cấu hình mạng cho nó, cụ thể hơn đó là địa chỉ IP.



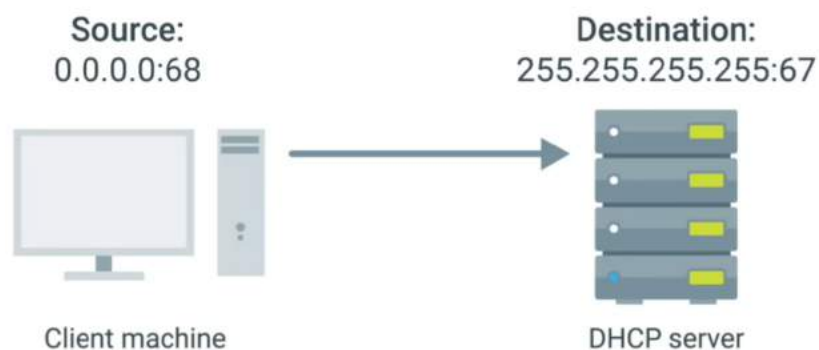
DHCP có 3 chiến lược khác nhau để cấp phát địa chỉ IP. Thứ nhất là cấp phát động (dynamic allocation), cách thứ hai là cấp phát tự động (automatic allocation) và cấp phát cố định (fixed allocation) là cách thứ 3.

- Trong cấp phát động, một dãy các địa chỉ IP được gán đến thiết bị và mỗi lần có thể gán khác nhau cho cùng một thiết bị.
- Trong cấp phát tự động, điều tương tự cũng diễn ra nhưng nếu thiết bị đã từng được gán một địa chỉ IP nào thì khi kết nối lại, nó sẽ được gán lại IP đó nếu IP đó chưa được gán cho thiết bị nào đang kết nối hiện tại.
- Trong cấp phát cố định, DHCP server duy trì một danh sách các địa chỉ MAC được gán IP cố định, khi một thiết bị kết nối khớp với địa chỉ MAC nào trong danh sách thì nó sẽ được gán IP tương ứng đã được xác định trước. Nếu không tìm thấy, DHCP có thể chuyển sang chế độ động, hoặc tự động, hoặc có thể từ chối gán để tăng cường chế độ bảo mật.



Tìm kiếm máy chủ DHCP

Khi một máy tính mới kết nối vào mạng, nó không có IP và cũng không biết địa chỉ IP của máy chủ DHCP. Nó tiến hành gửi một gói tin có tên gọi là DHCPDISCOVER ra toàn mạng với một số quy ước gồm máy chủ DHCP lắng nghe gói tin UDP trên cổng 67, máy tính gửi gói tin UDP ở cổng 68. Địa chỉ IP đích là 255.255.255.255, đó là địa chỉ broadcast và IP nguồn là 0.0.0.0



Máy chủ DHCP nhận được sẽ phản hồi với gói tin DHCPOFFER với port đích là 68, port nguồn là 67, IP đích 255.255.255.255, IP nguồn là IP thực sự của máy chủ DHCP cùng với các thông tin để cấu hình máy như IP sẽ được cấp cho máy tính mới. Lúc này máy tính nhận được gói tin có địa chỉ MAC ứng với địa chỉ của nó sẽ mở ra và thực hiện tiếp một gói tin tiếp theo để xác nhận. Cụ thể, máy tính mới gửi tiếp gói tin DHCPREQUEST đến máy chủ DHCP để đồng ý với cấu hình mạng mà nó được cấp. Máy chủ DHCP cuối cùng gửi gói tin phản hồi DHCPACK để xác nhận toàn bộ quá trình.

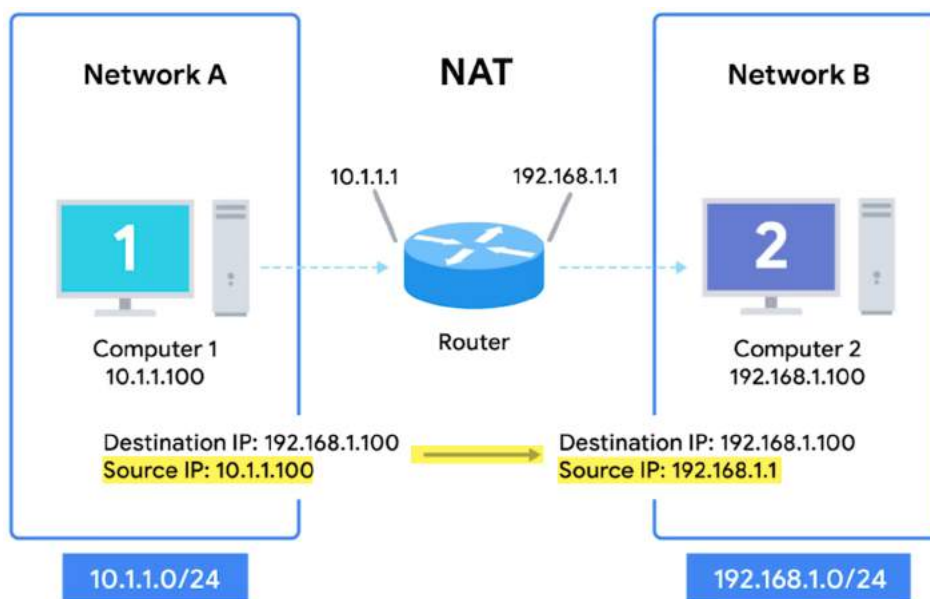
Bài đọc 9. Mạng Riêng Ảo và Dịch Vụ Proxy

1. Mạng riêng ảo

Biên dịch địa chỉ mạng

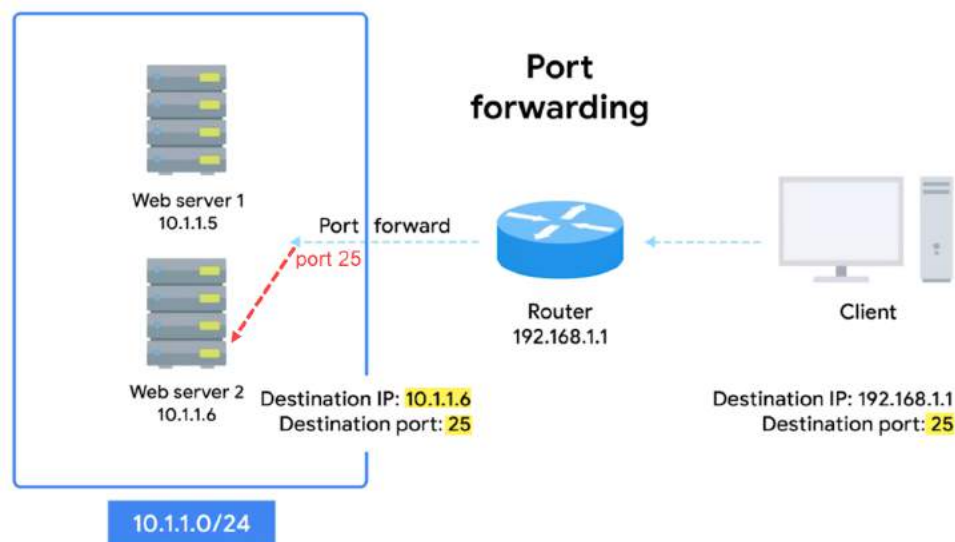
Biên dịch địa chỉ mạng, gọi tắt là NAT, là quá trình thay đổi địa chỉ IP thành một địa chỉ khác khi gói tin đi qua router hoặc firewall (tường lửa). Mục đích của việc này nhằm tăng cường tính bảo mật cho mạng.

Khi router bật NAT, ví dụ như outbound NAT (NAT hướng ngoài), gói tin gửi đi qua router sẽ bị viết lại địa chỉ IP nguồn và gói tin gửi về sẽ bị viết lại IP đích. Cách hoạt động này của NAT được gọi là giả mạo IP (IP masquerading). Điều này giúp cho toàn bộ không gian địa chỉ của mạng A được bảo vệ và ẩn khỏi mạng bên ngoài. NAT loại này cũng được gọi là NAT 1-nhiều.



Mỗi máy khi gửi gói tin đều khởi tạo một socket với port được đánh số tạm trong đoạn từ 49152 đến 65535. Để biết gói tin trả về cho máy nào, router sử dụng kỹ thuật duy trì cổng (port preservation), nghĩa là router sẽ giữ nguyên port máy nguồn khi đi qua NAT và chỉ đổi địa chỉ IP. Nếu 2 máy khác nhau gửi cùng port thì router sẽ chọn ngẫu nhiên một port chưa dùng.

Chuyển tiếp cổng (port forwarding) là kỹ thuật để chuyển các gói tin ở một cổng, ví dụ cổng 25, luôn về một máy cụ thể là 10.1.1.6.



Mỗi máy tính trong mạng có thể không cần gán địa chỉ IP internet mà chỉ cần IP trong không gian địa chỉ không thể định tuyến (non-routable address space) (ví dụ: 192.168.1.1, 10.0.0.0, 172.16.0.0, v.v.). Để kết nối đến Internet, ta có thể sử dụng kỹ thuật NAT. Bằng cách phối hợp giữa NAT và không gian địa chỉ không thể định tuyến giúp giải quyết vấn đề khan hiếm địa chỉ IPv4.

Mạng riêng ảo

Mạng riêng ảo, gọi tắt là VPN (virtual private network) là kỹ thuật cho phép mở rộng một mạng riêng hay mạng cục bộ đến những máy mà không được đặt trong mạng này. Ví dụ một người ở nhà có thể kết nối đến các tài nguyên trong một công ty như một máy được đặt tại đó.

VPN sử dụng giao thức đường ống (tunneling protocol) để kết nối máy ngoài mạng cục bộ. Dữ liệu được mã hóa ở đầu và cuối đường ống theo phương thức xác thực 2 yếu tố (two-factor authentication). Xác thực 2 yếu tố là phương thức xác thực cần nhiều hơn một tên người dùng và một mật khẩu.



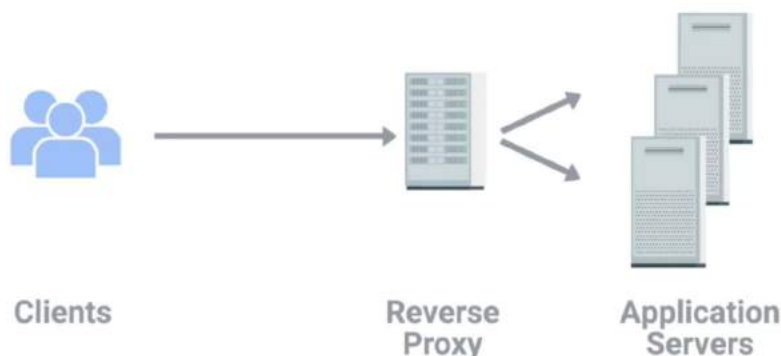
2. Máy chủ Proxy

Máy chủ Proxy là một máy chủ đóng vai trò như một máy khách để truy xuất một dịch vụ. Proxy nằm giữa các máy khách và các máy chủ khác, cung cấp một số lợi ích bổ sung, ẩn danh, bảo mật, lọc nội dung, tăng hiệu suất, một số thứ khác.

Có nhiều loại proxy, tùy thuộc vào chức năng của nó. Web proxy là proxy được sử dụng như máy trung gian để chuyển tiếp thông tin và kiểm soát việc truy cập internet của máy khách. Trong thời kỳ đầu của mạng Internet, hầu hết các kết nối chậm hơn nhiều so với hiện nay, rất nhiều tổ chức đã sử dụng web proxy để tăng hiệu suất. Bằng cách dùng web proxy, một tổ chức sẽ hướng tất cả lưu lượng truy cập web qua nó, cho phép chính máy chủ proxy thực sự truy xuất dữ liệu trang web từ Internet. Sau đó, nó sẽ lưu vào bộ nhớ cache dữ liệu này. Bằng cách này, nếu ai đó yêu cầu cùng một trang web, nó có thể chỉ trả lại dữ liệu đã lưu trong bộ nhớ cache thay vì phải truy xuất bản sao mới mỗi lần. Tuy nhiên, cách này không còn phù hợp ngày nay do nội dung trang web thay đổi gần như tức thời (ví dụ nội dung trên các trang mạng xã hội).

Ngày nay, một cách sử dụng phổ biến hơn của web proxy có thể là để ngăn ai đó truy cập vào trang web nào đó, chẳng hạn như Twitter. Một công ty có thể quyết định rằng việc truy cập Twitter trong giờ làm việc sẽ làm giảm năng suất. Bằng cách sử dụng web proxy, họ có thể hướng tất cả lưu lượng truy cập web đến nó, cho phép proxy kiểm tra dữ liệu nào đang được yêu cầu, sau đó cho phép hoặc từ chối yêu cầu này, tùy thuộc vào trang web nào đang được truy cập.

Reverse proxy được sử dụng để thể hiện một máy chủ duy nhất đến người dùng nhưng bên trong là một loạt các máy chủ cùng thực hiện. Các trang web phổ biến, như Twitter, nhận được nhiều lưu lượng truy cập đến nỗi không có cách nào mà một máy chủ web duy nhất có thể xử lý tất cả. Các trang web dạng này cần rất nhiều máy chủ để theo kịp xử lý tất cả các yêu cầu đến. Chính vì vậy, họ sử dụng reverse proxy.



Reverse proxy cũng có thể thực hiện một số công việc trước khi chuyển đến các máy chủ phía sau ví dụ như mã hóa/giải mã gói tin.

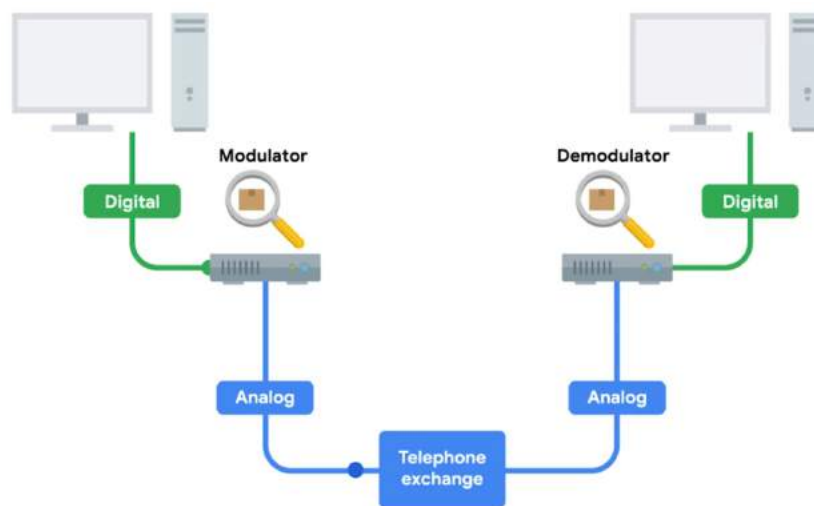
Bài đọc 10: Kết Nối Đến Mạng Internet

1. Kết nối qua tổng đài

Kết nối quay số

POTS (Plain Old Telephone Service) là một dịch vụ điện thoại truyền tín hiệu tuần tự qua các cặp dây đồng. POTS cũng được gọi là mạng điện thoại chuyển mạch công cộng (Public Switched Telephone Network). Vào thập niên 1970, hai sinh viên Đại học Duke thử kết nối 2 máy tính ở khoảng cách xa bằng dây điện thoại và sau đó phát triển một mạng USENET, tiền thân của mạng Internet sau này.

Kết nối quay số sử dụng POTS để truyền dữ liệu. Quá trình truyền bắt đầu bằng cách quay số điện thoại. Thiết bị thực hiện quay số được gọi là modem (modulator demodulator). Modem nhận dữ liệu ở dạng máy tính có thể hiểu (tín hiệu dạng số) và sau đó chuyển chúng thành bước sóng âm nghe được (tín hiệu tuần tự). Sóng âm này được chuyển đi qua công nghệ POTS.

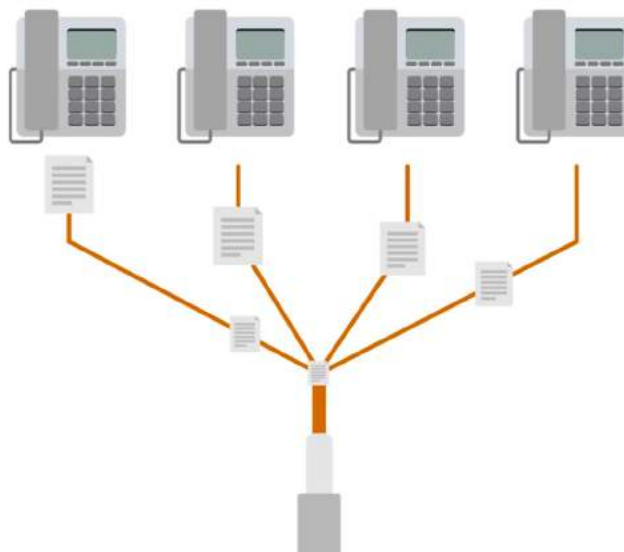


Để đo tốc độ truyền tín hiệu truyền theo dạng quay số này, người ta sử dụng một chỉ số gọi là tỷ lệ baud (baud rate). Tỷ lệ baud là số lượng bit truyền qua đường dây điện thoại trong một giây. Kết nối quay số thời điểm ban đầu có tốc độ truyền tín hiệu khá chậm. Qua thời gian, các nhà phát triển nâng cấp hệ thống để có tốc độ truyền tốt hơn. Từ đó ra đời kết nối băng thông rộng (broadband).

Kết nối băng thông rộng

Công nghệ T-carrier

Băng thông rộng là công nghệ truyền tải nhiều tín hiệu cùng lúc, cho phép kết nối với tốc độ cao và luôn sẵn sàng. Một công nghệ băng thông rộng có thể kể đến là công nghệ T-carrier được phát triển bởi AT&T. Công nghệ T-carrier cho phép nhiều cuộc gọi thoại được di chuyển qua một sợi dây cáp cùng lúc. Phiên bản T1 mang 24 cuộc gọi điện thoại cùng lúc trên một cặp dây đồng xoắn, đạt tốc độ 1.544 Mb/s. Sau đó, nó cũng được sử dụng để truyền dữ liệu Internet. Phiên bản T3 gồm 28 đường T1 và có thể đạt tốc độ 44.736 Mb/s.



Đường thuê bao số

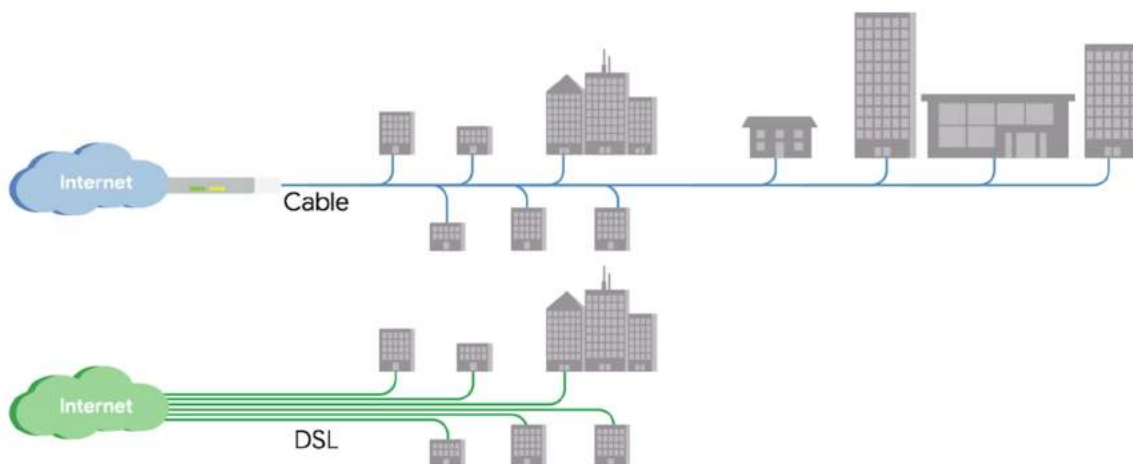
Đường thuê bao số gọi tắt là DSL thực hiện truyền dữ liệu ở một miền tần số không giao thoa với cuộc gọi điện thoại. Vì vậy, nó cho phép việc gọi điện thoại và truyền tải dữ liệu được diễn ra đồng thời, tốc độ truyền dữ liệu nhanh hơn. Thiết bị để chuyển đổi được biết đến với tên DSLAM. Khác với model quay số, modem DSLAM chỉ cần thiết lập kết nối 1 lần và giữ kết nối đó xuyên suốt cho đến khi tắt modem. Có nhiều loại DSL nhưng nổi bật là ADSL (Asymmetric Digital Subscriber Line) và SDSL (Symmetric Digital Subscriber Line). ADSL được đặc trưng bởi tốc độ dữ liệu đi ra hay tải lên chậm nhưng tốc độ đi xuống hay tải xuống lại nhanh. Công nghệ thứ hai là SDSL, nó khác với ADSL ở chỗ tốc độ tải lên và tải xuống bằng nhau. Điều này phù hợp với các kết nối ở phía máy chủ, do cần cung cấp dữ liệu là chủ yếu. Về sau, chúng ta có phiên bản cải tiến là HDHS (High Bit-rate Digital Subscriber Line) cho tốc độ nhanh hơn.

Băng thông rộng cáp

Các công ty truyền hình cáp nhận ra rằng các loại cáp đồng trục được sử dụng trong truyền hình cáp có khả năng truyền nhiều dữ liệu hơn những gì cần thiết để xem TV. Bằng cách sử dụng các tần số không gây nhiễu sóng truyền hình, các công nghệ truy cập Internet dựa trên cáp có thể cung cấp truy cập Internet tốc độ cao trên cùng các loại cáp này. Công nghệ kết nối băng thông rộng này được gọi băng thông rộng cáp (cable broadband). Khi so sánh với các giải pháp băng thông rộng khác là cáp thường được gọi là công nghệ băng thông chia sẻ (shared bandwidth technology).

Trong công nghệ băng thông chia sẻ, nhiều người sử dụng dùng chung băng thông cho đến khi đường truyền đến mạng lõi của ISP. Ngày nay, hầu hết các nhà khai thác cáp cố gắng nâng cấp mạng của họ đến mức người dùng cuối có thể không nhận thấy băng thông của họ được chia sẻ. Tuy nhiên, kết nối Internet bằng cáp vẫn bị ảnh hưởng nhiều trong thời gian có nhiều người sử dụng đồng thời.

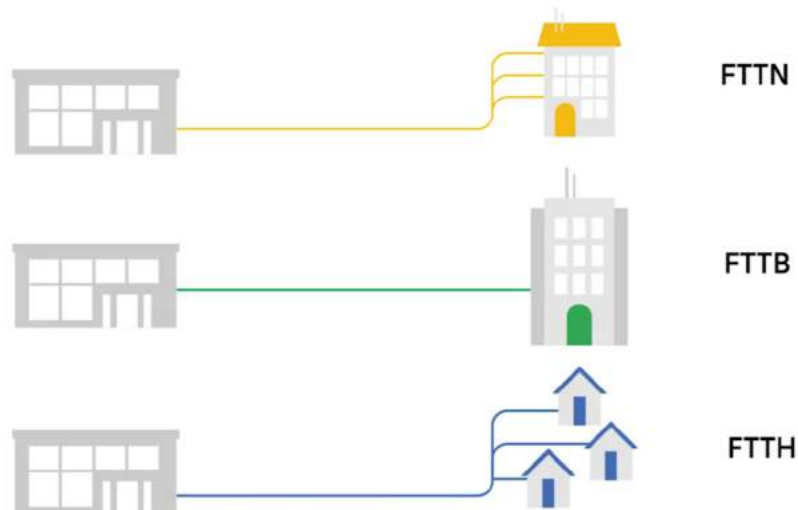
Kết nối Internet cáp thường được quản lý bởi một modem cáp. Đây là một thiết bị nằm ở rìa mạng của người dùng và kết nối với hệ thống CMTS. CMTS là thiết bị nối nhiều kết nối cáp với mạng lõi của ISP.



Kết nối quang

Kết nối sợi quang (fiber connection) sử dụng ánh sáng để truyền tải dữ liệu thay vì dòng điện. Do đó, tốc độ sẽ nhanh hơn cũng như truyền tải đi xa trước khi tín hiệu bị suy giảm. Tuy nhiên, chi phí sản xuất và lắp đặt cao, dẫn đến ban đầu nó chỉ phù hợp để kết nối các ISP (nhà cung cấp dịch vụ internet) với nhau. Sự phát triển công nghệ kết nối sợi quang được thể hiện qua cụm từ FTTX (Fiber to X), nghĩa là mạng kết nối quang phổ biến được đến đâu. FTTN (Fiber to the Neighborhood) mô tả kết nối quang đến được một tú

vật lý trung tâm. Trong khi đó, FTTB (Fiber to the Business) mô tả kết nối quang đến được doanh nghiệp, và FTTH (Fiber to the Home) mô tả kết nối được đến từng hộ gia đình. Thuật ngữ FTTP (Fiber to the Premise) là tên gọi chung của FTTB và FTTH.



Khi kết nối đến đầu cuối, người dùng cần một thiết bị gọi là bộ đầu cuối mạng quang ONT (Optical Network Terminator). Đây là thiết bị được sử dụng để chuyển đổi tín hiệu trong kết nối quang thành các tín hiệu trong mạng cáp xoắn đôi truyền thống.

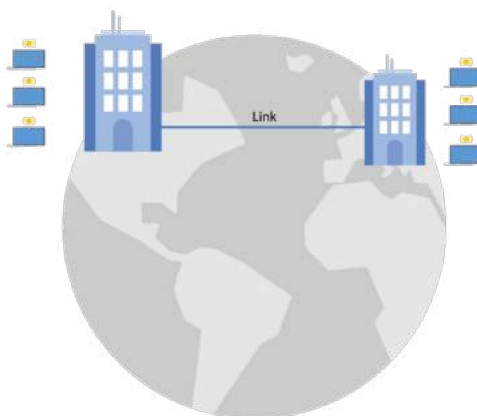
2. Mạng diện rộng

Mạng WAN

Khi nói về phạm vi kết nối, người ta muốn mô tả về khu vực bao phủ của mạng. Ví dụ như mạng LAN thì khu vực bao phủ nhỏ, giới hạn trong khoảng vài km đồ lại, còn mạng MAN bao phủ khu vực lớn hơn như trong một thành phố. Khi kết nối các máy nằm ở xa hơn như giữa quốc gia này với quốc gia khác, ta dùng thuật ngữ WAN. Mạng diện rộng WAN là công nghệ giúp các mạng làm việc với nhau như một mạng đơn nhất nhưng trải dài qua nhiều vùng địa lý khác nhau.



Công nghệ WAN thường yêu cầu chúng ta ký hợp đồng Internet với các nhà cung cấp dịch (ISP). ISP này xử lý việc gửi dữ liệu từ nơi này sang nơi khác. Vì vậy, chúng có thể giống như tất cả các máy tính ở cùng một vị trí thực tế. Thiết lập mạng WAN gồm một bước. Mỗi mạng ở hai đầu kết nối đến ISP và dữ liệu đi đến ISP sẽ kết thúc ở điểm phân giới của mỗi bên trước khi tiếp sang phía kia. Khu vực giữa mỗi điểm phân giới và mạng của ISP được gọi là vòng lặp cục bộ (local loop).

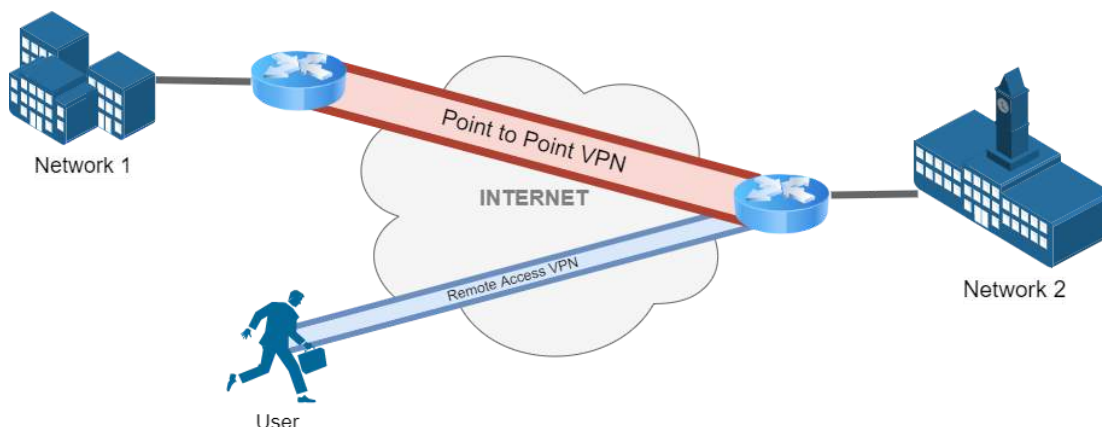


Vòng lặp cục bộ này giống như đường truyền T-carrier hoặc kết nối quang tới văn phòng khu vực địa phương của nhà cung cấp. Từ đó, nó sẽ kết nối với mạng lõi của ISP và Internet. Mạng WAN hoạt động bằng cách sử dụng một số giao thức khác nhau ở tầng liên kết dữ liệu để truyền dữ liệu.

VPN điểm-điểm

Một giải pháp thay thế cho các công nghệ WAN là VPN điểm-điểm (point-to-point VPN). Công nghệ WAN phù hợp khi cần truyền một lượng lớn dữ liệu qua nhiều nơi, do công nghệ WAN được xây dựng để hỗ trợ tốc độ nhanh. Đường truyền cáp hoặc đường

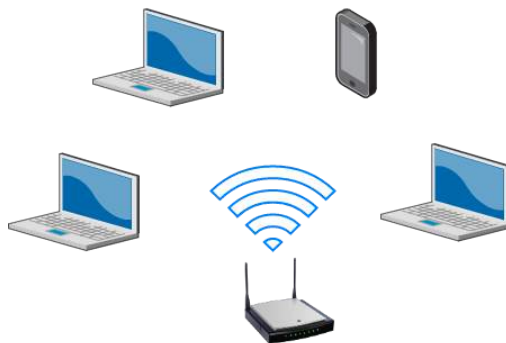
DSL có thể rẻ hơn nhưng nó không thể xử lý tải cần thiết trong các trường hợp này. Tuy nhiên, các công ty ngày càng chuyển nhiều dịch vụ nội bộ của họ lên đám mây. Với giải pháp đám mây, nhiều doanh nghiệp không còn yêu cầu kết nối tốc độ cực cao giữa các khu vực đặt công ty của họ nữa. Điều này làm cho công nghệ WAN hoàn toàn không cần thiết. Thay vào đó, các công ty có thể sử dụng point-to-point VPN để đảm bảo rằng các khu vực khác nhau vẫn có thể giao tiếp với nhau. Point-to-point VPN, còn được gọi là site-to-site VPN, thiết lập một đường hầm VPN giữa hai khu vực. Điều này hoạt động rất giống cách thiết lập VPN truyền thống cho phép người dùng cá nhân hành động như thể họ đang ở trên mạng mà họ đang kết nối. Điểm khác chỉ là đường hầm của VPN được xử lý bởi các thiết bị mạng ở hai bên, do đó người dùng không phải thiết lập kết nối của riêng họ.



3. Mạng không dây

Giới thiệu mạng không dây

Mạng không dây (wireless network) là cách thức kết nối mạng mà không cần dây dẫn, phương tiện truyền tải dữ liệu là sóng vô tuyến.



Mạng không dây được đặc tả dưới họ chuẩn IEEE 802.11. Một số chuẩn cụ thể gồm 802.11a/b/g/n/ac/ax/be. Chúng thường giống nhau về giao thức cơ sở, nhưng khác nhau dải tần số. Dải tần số là một khoảng xác định trong phổ vô tuyến được chấp nhận để sử dụng cho việc giao tiếp. Ví dụ như tần số FM trong khoảng từ 88 MHz đến 108 MHz. WiFi phổ biến với 2 tần số là 2.4 GHz và 5 GHz.

Khung tin của chuẩn 802.11 bao gồm một số trường như Frame control, duration, 4 địa chỉ MAC, Sequence control và FCS. Frame control chứa giá trị của các trường phụ mô tả cách khung tin được xử lý, duration là khoảng thời gian toàn bộ khung tin thực thi để các thiết bị nhận biết được bao lâu nó phải lắng nghe để nhận dữ liệu. Tiếp là 4 địa chỉ MAC. Ở giữa 4 địa chỉ có trường sequence control để ghi lại số thứ tự của khung tin. FCS là các bit dùng để kiểm tra lỗi khung tin.

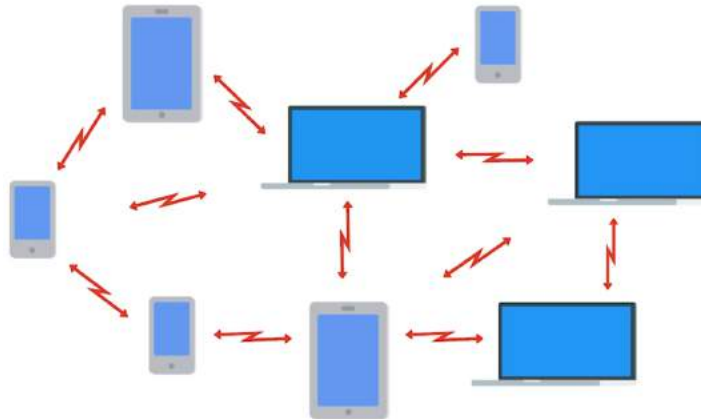


Điểm truy cập không dây (Wireless Access Point - AP) là một thiết bị làm cầu nối giữa mạng không dây và có dây. Một số AP được cấu hình chỉ để làm nhiệm vụ lặp lại gói tin cho AP khác. Do đó, khung tin có 4 địa chỉ MAC. Một địa chỉ là của thiết bị gửi dữ liệu, một địa chỉ của thiết bị đích, MAC của thiết bị nhận và MAC chuyển tiếp dữ liệu tiếp tục.

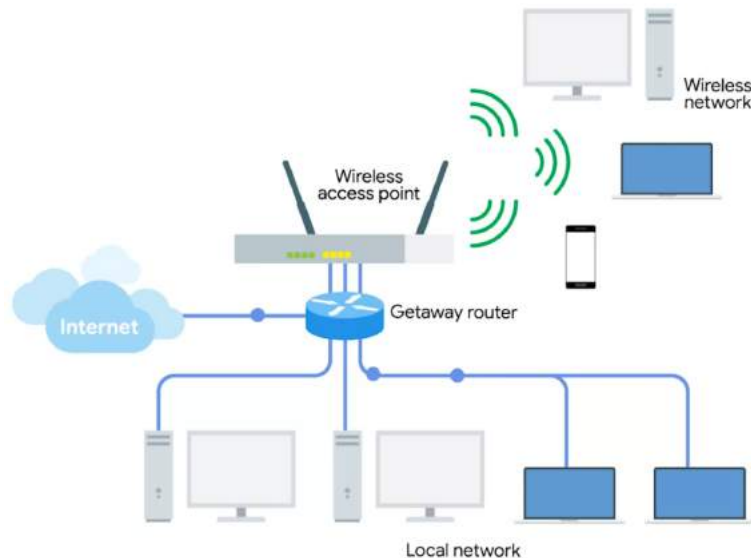
Cấu hình mạng không dây

Mạng không dây có thể được cấu hình theo 3 cách: mạng tùy biến không dây (Wireless ad-hoc network), mạng cục bộ không dây (Wireless LAN), mạng lưới không dây (Wireless mesh network)

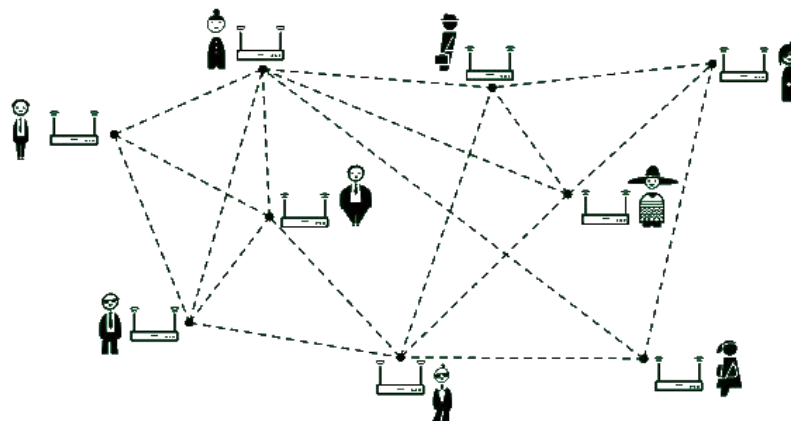
Mạng tùy biến không dây được xem là mạng đơn giản nhất, chúng bao gồm một tập hợp các thiết bị kết nối với nhau mà không cần kiến trúc mạng phức tạp nào hỗ trợ. Trong mạng, mỗi thiết bị giao tiếp với nhau bên trong phạm vi và tất cả các nút mạng hỗ trợ truyền gói tin. Mặc dù loại mạng này không phổ biến nhưng chúng có thể được sử dụng trong một số tình huống như trao đổi hình ảnh, thông tin giữa các điện thoại với nhau, hoặc tạo kết nối tạm để giao tiếp với nhau khi hệ thống mạng hiện tại bị sập.



Trong khi đó, mạng cục bộ không dây (WLAN) lại bao gồm một hoặc nhiều điểm truy cập (AP) đóng vai trò làm cầu nối giữa mạng có dây và không dây. Loại mạng này phổ biến trong các kết nối thực tế vì chúng cho phép làm việc với các công nghệ mạng có dây truyền thống và các thiết bị hỗ trợ kết nối khác.



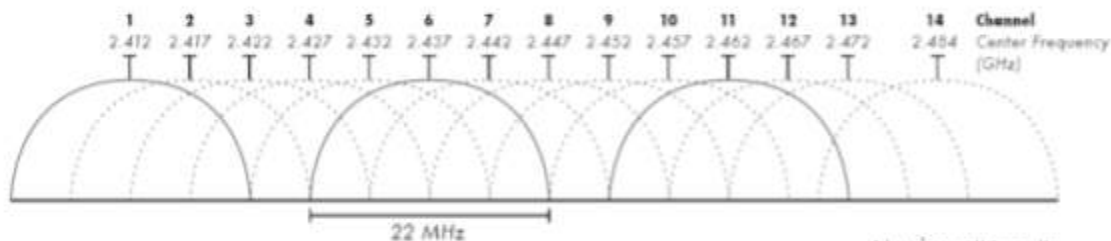
Mạng lưới không dây hay mạng mesh không dây được hình thành với chỉ các điểm truy cập (AP) kết nối với nhau và các thiết bị khác sẽ nối với AP để giao tiếp. Có thể thấy, mạng này không cần chạy các đoạn cáp để kết nối các thiết bị với nhau.



Kênh

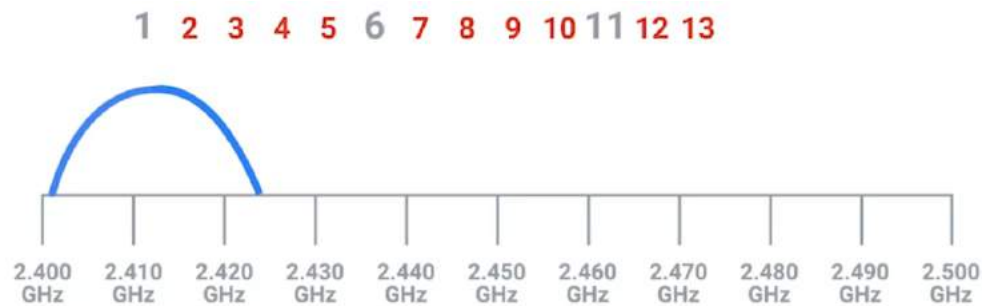
Miền đụng độ (collision domain) là phần mạng chỉ cho phép 1 máy giao tiếp tại một thời điểm, nếu có nhiều hơn sẽ gây nhiễu tín hiệu (đụng độ). Nếu đụng độ, các máy phải đợi một khoảng thời gian để gửi lại, điều này dẫn đến mạng chậm. Trong mạng có dây, giải pháp để tránh đụng độ là dùng Switch. Tuy nhiên, switch không thể áp dụng cho mạng không dây vì tín hiệu không đi qua dây dẫn.

Kênh (channel) giúp khắc phục một phần vấn đề đụng độ. Kênh là đoạn nhỏ, đơn lẻ của toàn bộ dải tần số được sử dụng bởi một mạng không dây.

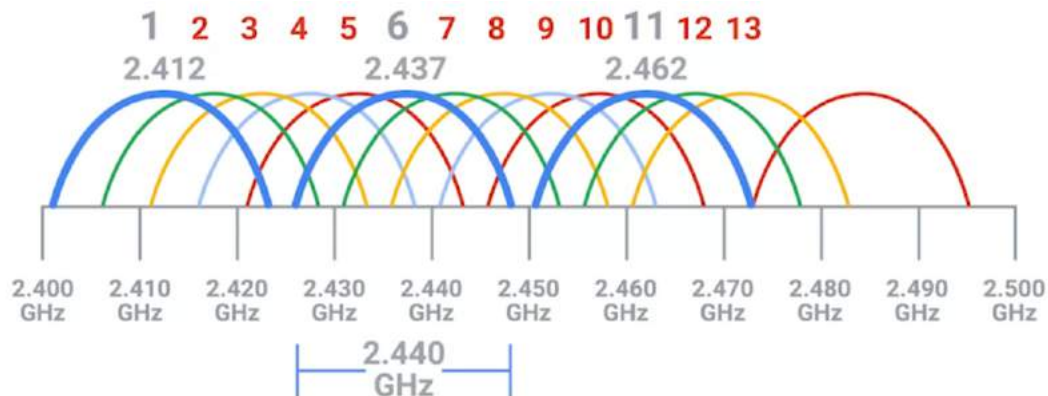


Nguồn: wikipedia

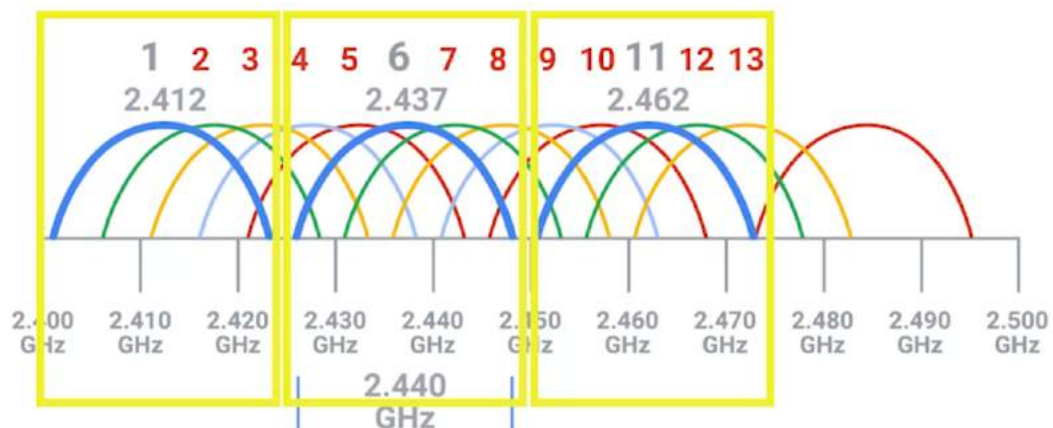
Xét mạng không dây tần số 2.4GHz, dải tần số này có nghĩa là ta có thể thực thi từ 2.4 GHz đến 2.5 GHz. Giữa 2 tuần số (2.4 và 2.5) là các kênh có độ rộng bằng nhau và bằng con số xác định tùy vào mỗi quốc gia, khu vực. Độ rộng thường đo bằng đơn vị MHz. Ví dụ, với độ rộng kênh là 22 MHz, kênh 1 thực thi ở tần số 2,412 GHz thì tín hiệu sóng trong miền tần số giữa 2,401GHz và 2,423 GHz.



Một số kênh chồng lên nhau nhưng chúng đủ xa để giao thoa với cái khác.



Các kênh hoàn toàn không đụng độ là 1, 6, 11.



Bảo mật mạng không dây

Với mạng không dây, do không có cáp nên khi sóng vô tuyến được phát qua không khí, bất kỳ ai trong phạm vi phủ sóng về mặt lý thuyết có thể thu được tín hiệu dù dữ liệu có dành cho họ hay không. Để giải quyết vấn đề này, WEP (wired equivalent privacy) đã được phát minh. Công nghệ này mã hóa dữ liệu lại để bảo vệ thông tin được truyền trong

mạng. Tuy nhiên, chuẩn mã hóa WEP rất yếu vì dùng chỉ 40 bit cho khóa và mất vài phút cho máy tính ngày nay để bẻ khóa.

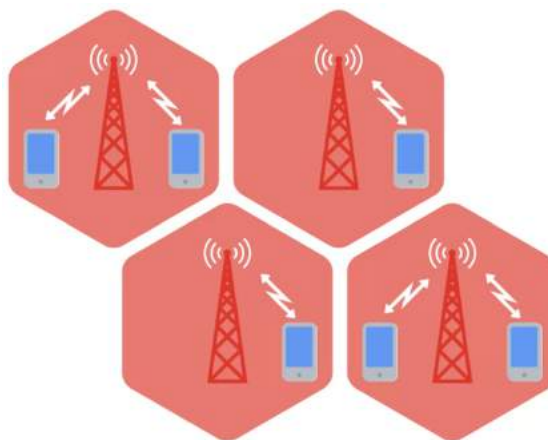
Một kỹ thuật khác ra đời thay thế cho WEP đó là WPA (Wi-Fi Protected Access). WPA sử dụng khóa độ dài 128 bit. Phiên bản sau của nó là WPA2 có khóa độ dài 256 bit rất khó để bẻ khóa và được sử dụng phổ biến ngày nay.

Bên cạnh mã hóa dữ liệu, mạng không dây còn có cách bảo mật khác là lọc địa chỉ MAC. Cách bảo mật này được thực hiện bằng cách cấu hình điểm truy cập (AP) để cho phép chỉ các kết nối từ một tập của các địa chỉ MAC đã xác định trước.

4. Mạng viễn thông

Một loại mạng không dây phổ biến khác là mạng viễn thông, còn được gọi là mạng di động (cellular/mobile network). Mạng di động hiện đã phổ biến trên toàn thế giới. Ở một số nơi, sử dụng mạng di động để truy cập Internet là cách kết nối phổ biến nhất. Ở cấp độ cao, mạng di động có rất nhiều điểm chung với mạng không dây chuẩn 802.11. Chúng cũng có rất nhiều đặc tả kỹ thuật di động khác nhau. Mạng di động hoạt động trên sóng vô tuyến và có các dải tần số cụ thể dành riêng cho việc truyền dữ liệu di động. Một trong những điểm khác biệt lớn nhất là các tần số này có thể di chuyển trên khoảng cách xa dễ dàng hơn, thường là trên nhiều km.

Mạng viễn thông được hình thành từ các tế bào (cell). Mỗi tế bào được gán một tần số nhất định và không chồng chéo với tế bào bên cạnh. Trạm phát sóng (cell tower) sẽ truyền phát và nhận các tín hiệu. Chúng giống với thiết bị điểm truy cập (AP) trong mạng không dây thông thường nhưng phạm vi rộng hơn.



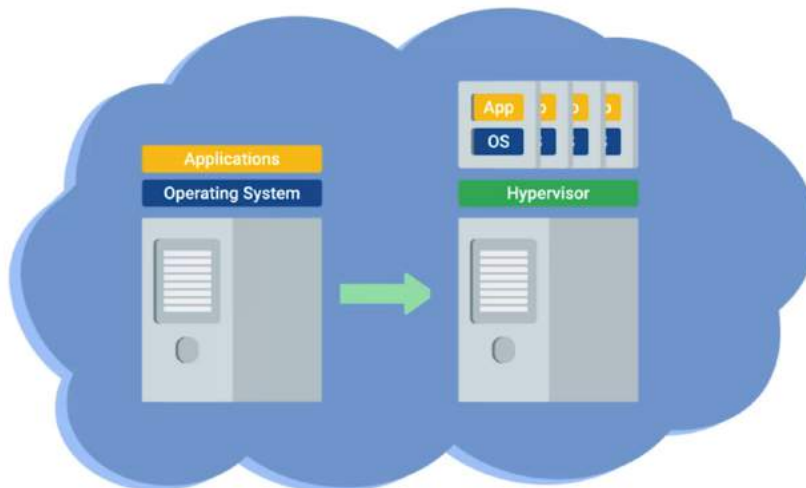
Rất nhiều thiết bị ngày nay sử dụng mạng di động để liên lạc. Và không chỉ điện thoại, máy tính bảng và một số máy tính xách tay cũng có ăng-ten di động.

5. Điện toán đám mây

Điện toán đám mây và công nghệ ảo hóa

Điện toán đám mây (cloud computing) là công nghệ cho phép tài nguyên máy tính được chia sẻ để nhiều người cùng sử dụng. Người dùng ở đây bao gồm cả công ty, doanh nghiệp. Điện toán đám mây giúp giảm chi phí phải vận hành hệ thống mạng và đảm bảo truy xuất ổn định cũng như sẵn sàng mọi lúc do được xây dựng bởi bên thứ ba chuyên về nền tảng kỹ thuật như Google, Amazon, v.v...

Ảo hóa phần cứng được xem là trái tim của điện toán đám mây. Với công nghệ ảo hóa, một máy tính vật lý có thể giả lập thành nhiều máy ảo. Công nghệ ảo hóa phần cứng là hypervisor. Hypervisor là một phần mềm chạy và quản lý các máy ảo đồng thời cung cấp cho người dùng nền tảng điều hành ảo như thể là phần cứng thực tế. Với ảo hóa, một máy tính vật lý duy nhất có thể hoạt động như một máy chủ lưu trữ cho nhiều phiên bản ảo độc lập. Chúng đều chạy hệ điều hành độc lập của riêng mình.



Một số thuật ngữ liên quan đến cloud như:

- Public cloud là một cụm lớn các máy được vận hành bởi một công ty khác.
- Private cloud là một cụm lớn các máy được vận hành bởi chính công ty.
- Hybrid cloud là thuật ngữ dùng để mô tả tình huống công ty có thể chạy những công nghệ độc quyền trên private cloud, còn giao các công việc ít nhạy cảm cho các public cloud.

Mọi thứ như một dịch vụ

Mọi thứ như một dịch vụ (Everything as a Service) là một khái niệm mô tả cách các công ty sử dụng các dịch vụ được cung cấp sẵn thay vì phải tự xây dựng, quản lý và bảo trì chúng. Các loại dịch vụ điện toán đám mây phổ biến như IaaS, PaaS, SaaS.

IaaS là dịch vụ cơ sở hạ tầng như mạng máy tính, các máy chủ. Trong khi đó, PaaS là dịch vụ cung cấp môi trường để người dùng phát triển và triển khai ứng dụng của mình, ví dụ như Windows Azure, Google App Engine. SaaS là dịch vụ cấp phép sử dụng phần mềm cho người khác trong khi vẫn giữ phần mềm đó được lưu trữ và quản lý tập trung. Office 365 của Microsoft là một ví dụ cho SaaS.

Lưu trữ đám mây

Nếu chúng ta đã từng nghe Google Drive, One Drive, hay Dropbox thì đó chính là lưu trữ đám mây. Việc chứa dữ liệu trên các máy chủ cloud mang lại rất nhiều lợi ích như có thể truy cập từ bất kỳ đâu, bất kỳ thiết bị nào. Chi phí hợp lý so với mua ổ cứng. Dữ liệu được bảo vệ khỏi việc mất mát do các vấn đề liên quan đến phần cứng, v.v....

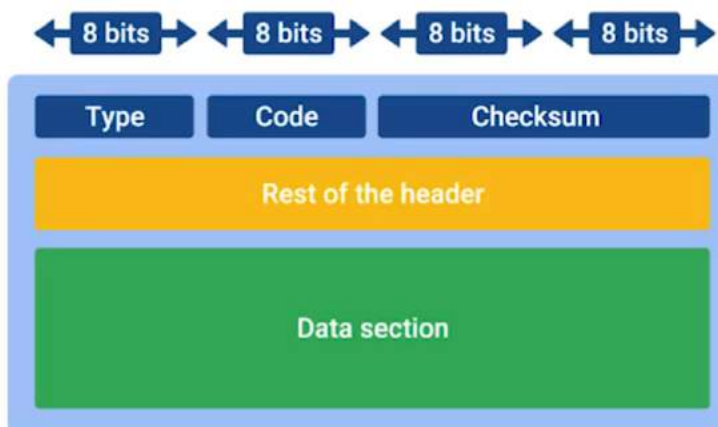
Bài đọc 11. Sự Cố Mạng và Cách Khắc Phục

1. Giao thức ICMP

Khi xảy ra lỗi mạng, thiết bị phát hiện ra nó cần một số cách để truyền thông tin. Một số sự cố có thể xảy ra như bộ định tuyến không biết cách định tuyến đến đích hoặc không thể truy cập một cổng nhất định. Thậm chí có thể là do thời gian sống (TTL) của một gói dữ liệu IP đã hết hạn và không có bộ định tuyến nào nữa được thực hiện.

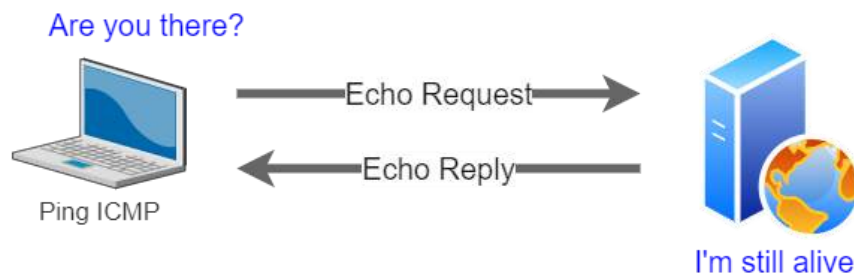
Đối với tất cả các sự cố, chúng ta cần một giao thức thông điệp điều khiển Internet (ICMP) để thông báo những vấn đề này. ICMP là một giao thức để xác định nguyên nhân quá trình truyền bị lỗi. ICMP chủ yếu được sử dụng bởi bộ định tuyến hoặc máy chủ từ xa để thông báo lý do tại sao quá trình truyền bị lỗi trở lại nguồn của quá trình truyền.

Gói tin ICMP có header gồm các trường như type là loại của thông điệp ICMP, code để mô tả rõ hơn về lỗi, checksum để kiểm tra tính toàn vẹn của gói tin, rest of header để dành gửi thêm dữ liệu, data section chứa một phần dữ liệu gây nên lỗi. Cụ thể sẽ chứa IP header và 8 byte đầu của dữ liệu bị lỗi.



2. Ping

Ping là một công cụ để kiểm tra xem có thể kết nối tới một máy tính hay không. Khi thực thi, ping gửi một gói tin ICMP được gọi là Echo Request đến máy đích. Nếu máy đích nhận được nó sẽ gửi về gói tin Echo Reply để xác nhận. Nếu không nhận được, kết nối đang có vấn đề.



Để thực hiện lệnh Ping, ta chỉ cần nhập dòng lệnh Ping và địa chỉ máy đích hoặc tên miền trong cửa sổ shell. Thông tin trả về gồm địa chỉ phản hồi, kích thước, thời gian và giá trị thời gian sống (TTL).

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\cindy> ping 8.8.8.8

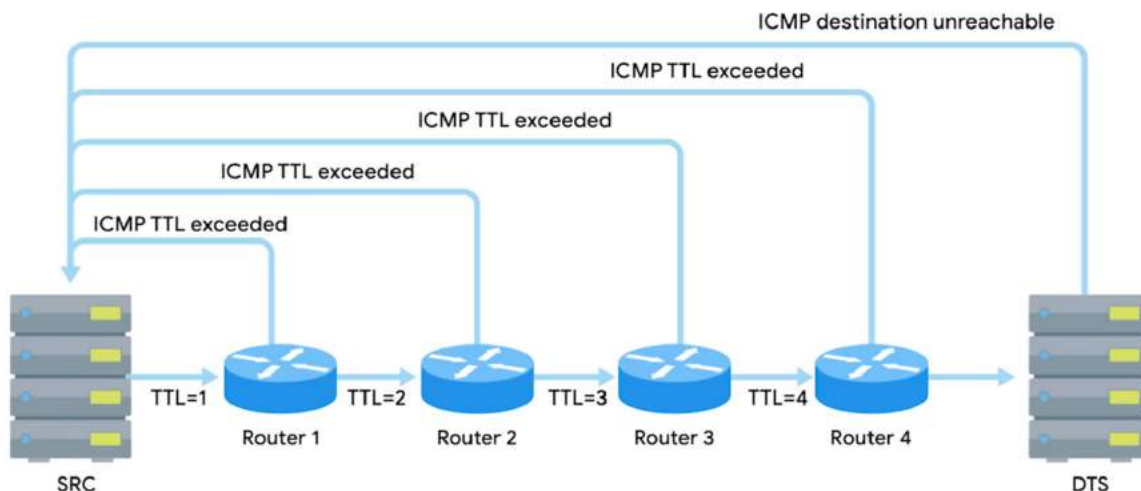
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=3ms TTL=56
Reply from 8.8.8.8: bytes=32 time=3ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 3ms
PS C:\Users\cindy>
```

3. Traceroute

Traceroute là công cụ dùng để chẩn đoán vấn đề dựa trên các đường định tuyến giữa hai nút. Traceroute dựa trên trường TTL (Time to Live) để xác định vấn đề trên đường định tuyến. Khi TTL bị giảm về 0, gói tin sẽ bị trả về với thông báo lỗi là vượt quá thời gian (Time Exceeded).

Quá trình thực hiện cụ thể gồm: traceroute gửi một loạt các gói tin với TTL được thiết lập khác nhau và lần lượt với giá trị 1, 2, 3, ... Mỗi giá trị TTL, traceroute sẽ gửi 3 gói tin để đảm bảo thông tin chính xác. Với gói tin TTL = 1, nó sẽ bị gửi trả về khi mới đến được 1 máy đầu tiên trong đường đi. Với gói tin TTL = 2, nó sẽ bị gửi trả về khi đi được 2 máy trên đường đi. Cứ thế cho đến khi đến được máy đích. Qua các gói tin ICMP Time Exceeded được trả về, nó sẽ biết được đường đi của gói tin đến đích gặp vấn đề chỗ nào.



Lệnh traceroute được thực hiện với tên miền cần kiểm tra. Thông tin trả về gồm số thứ tự máy đã đi qua, thời gian của mỗi gói tin trong 3 gói tin gửi, và IP của từng máy. Trên mỗi hệ điều hành khác nhau thì tên lệnh cho traceroute có thay đổi. Ví dụ như trên Windows, lệnh có tên là tracert. Ngoài ra, một số công cụ tương tự với các tính năng thêm như lệnh mtr trên Linux và MacOS, lệnh pathping trên Windows.

```
cindy@cindy-nyc:~$ traceroute google.com
traceroute to google.com (216.58.195.78), 30 hops max, 60 byte packets
 1 100.111.191.252 (100.111.191.252) 2.768 ms 3.427 ms 4.609 ms
 2 172.27.120.113 (172.27.120.113) 4.694 ms 5.065 ms 5.144 ms
 3 172.27.104.17 (172.27.104.17) 8.696 ms 8.704 ms 9.214 ms
 4 104.133.2.193 (104.133.2.193) 9.227 ms 9.547 ms 9.552 ms
 5 72.14.210.37 (72.14.210.37) 9.775 ms 72.14.210.99 (72.14.210.99) 10.480 ms 72
 6 108.170.242.81 (108.170.242.81) 14.063 ms 3.441 ms 4.297 ms
 7 108.170.235.237 (108.170.235.237) 5.194 ms 5.191 ms 108.170.235.239 (108.170.
 8 sfo07s16-in-f78.1e100.net (216.58.195.78) 5.150 ms 5.154 ms 5.131 ms
cindy@cindy-nyc:~$
```

4. Kiểm tra cổng

Đôi khi sự cố bắt nguồn từ cổng. Để kiểm tra một cổng trên máy đích có hoạt động không, ta có thể dùng công cụ netcat trên Linux, MacOS, hay test-netconnection trên Windows. Các lệnh này cũng hỗ trợ một số tham số như -v, -z để thay đổi cách thể hiện kết quả xuất ra.

```
cindy@cindy-nyc:~$ nc -z -v google.com 80
Connection to google.com 80 port [tcp/http] succeeded!
cindy@cindy-nyc:~$
```

5. Kiểm tra DNS

Hệ thống phân giải tên miền là một phần quan trọng trong cách thức hoạt động của Internet. Hệ điều hành đảm nhiệm tất cả các hoạt động này. Tuy nhiên, đôi khi sự cố đến từ hệ thống phân giải tên miền. Thậm chí, ngoài máy chủ DNS được cung cấp bởi nhà cung cấp dịch vụ Internet (ISP), chúng ta có thể tự xây dựng máy chủ DNS để phục vụ phân giải tên cho các máy cục bộ. Một số công ty trên thế giới xây dựng các máy chủ DNS và cho mọi người sử dụng miễn phí như máy chủ của tổ chức mức 3 gồm các IP từ 4.2.2.1 đến 4.2.2.6, hay máy chủ DNS của Google ở địa chỉ 8.8.8.8 và 8.8.4.4. Đôi khi các máy chủ này có thể gặp trục trặc ở tên miền nào đó, nên chúng ta cũng cần kiểm tra xem vấn đề có phải đến từ đó không.

Để kiểm tra việc phân giải tên miền, ta có thể sử dụng công cụ nslookup. Trong quá trình dùng lệnh, ta có thể bỏ trống tên miền để vào giao diện tương tác của nslookup. Để thay đổi máy chủ phân giải tên miền, dùng từ khóa *server*.

```
cindy@cindy-nyc:~$ nslookup twitter.com
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   twitter.com
Address: 104.244.42.193
Name:   twitter.com
Address: 104.244.42.65
```

Một vấn đề có thể đến từ tập tin Host. Tập tin Host là một tập tin chứa mỗi dòng là địa chỉ mạng và tên máy. Trong tập tin này có một số địa chỉ gọi là loopback. Đây là địa chỉ trỏ về chính máy đó. Các địa chỉ như 127.0.0.1 (IPv4) và ::1 (IPv6) là địa chỉ loopback được cấu hình cho mọi thiết bị. Người dùng có thể vô tình thiết lập một tên miền vào địa chỉ loopback và dẫn đến sự cố không truy cập được đúng địa chỉ của máy chủ cung cấp dịch vụ.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#   127.0.0.1      localhost
#   ::1            localhost
```

Phần 2

HƯỚNG DẪN

TRẢ LỜI CÂU HỎI

Phần Giới thiệu mạng máy tính

1. Câu nào sau đây là một ví dụ về giao thức ở tầng mạng (tầng 3)?

- A. Ethernet
- B. TCP
- C. IP
- D. UDP

Đáp án: C

2. Sự khác biệt giữa máy khách và máy chủ là gì?

- A. Máy chủ yêu cầu dữ liệu và máy khách phản hồi yêu cầu đó
- B. Máy khách và máy chủ là tên gọi khác nhau cho cùng một thứ
- C. Máy khách hoạt động trên tầng liên kết dữ liệu và máy chủ hoạt động trên tầng mạng
- D. Máy khách yêu cầu dữ liệu và máy chủ đáp ứng yêu cầu đó

Đáp án: D

3. Câu nào sau đây là ví dụ về các tầng trong mô hình mạng 5 lớp? Đánh dấu vào tất cả các câu phù hợp.

- A. Tầng vật lý
- B. Tầng trình diễn
- C. Tầng ứng dụng
- D. Tầng vận chuyển

Đáp án: A,C,D

4. Câu nào sau đây mô tả chính xác sự khác biệt giữa hub và switch? Đánh dấu vào tất cả các câu phù hợp.

- A. Hub là thiết bị tầng vật lý và switch là thiết bị tầng liên kết dữ liệu.
- B. Hub là phiên bản phức tạp hơn của switch
- C. Switch ghi nhớ thiết bị nào được kết nối đến trên mỗi giắc cắm, trong khi đó hub thì

không

- D. Hub gây ra các miền đụng độ lớn hơn

Đáp án: A,C,D

5. LAN viết tắt của từ gì?

- A. Mạng khu vực lớn (Large Area Network)
- B. Mạng sẵn có cục bộ (Locally Available Network)
- C. Mạng khu vực nhỏ (Little Area Network)
- D. Mạng khu vực cục bộ (Local Area Network)

Đáp án: D

6. Router là gì?

- A. Một thiết bị biết cách chuyển tiếp dữ liệu giữa các mạng độc lập
- B. Một phiên bản nâng cấp hơn của switch
- C. Một thiết bị tăng vật lý mà ngăn chặn hiện tượng nhiễu xuyên âm (crosstalk)
- D. Một thiết bị mạng được sử dụng một cách đặc biệt dành cho sợi quang

Đáp án: A

7. Một thiết bị biết cách chuyển tiếp dữ liệu giữa các mạng độc lập được gọi là.....

- A. Router
- B. Switch
- C. Hub
- D. Node

Đáp án: A

8. Một thứ yêu cầu dữ liệu từ máy chủ được biết với tên?

- A. Switch

- B. Router
- C. Server
- D. Client

Đáp án: D

9. Một thiết bị kết nối với rất nhiều thiết bị và nhớ từng cái ở mỗi cổng giao tiếp được biết với tên gọi là

- A. Hub
- B. Switch
- C. Router
- D. Server

Đáp án: B

10. TCP viết tắt của từ....?

- A. Transmission Control Protocol
- B. Tapioca Coconut Pudding
- C. Translational Carrier Pathway
- D. Topical Control Pathogen

Đáp án: A

11. Tầng nào trong mô hình TCP/IP chịu trách nhiệm định nghĩa cách thức chung diễn giải tín hiệu để mà các thiết bị mạng có thể giao tiếp?

- A. Tầng liên kết dữ liệu (data link)
- B. Tầng vận chuyển (transport)
- C. Tầng ứng dụng (application)
- D. Tầng mạng (network)

Đáp án: A

12. Một người có nhiều trang web đang mở và cũng đang sử dụng email. Tầng nào trong mô hình TCP/IP chịu trách nhiệm sắp xếp dữ liệu để gửi email và các trang web đến vị trí thích hợp?

- A. Tầng ứng dụng (application)
- B. Tầng vận chuyển (transport)
- C. Tầng mạng (network)
- D. Tầng liên kết dữ liệu (data link)

Đáp án: B

13. Giao thức Ethernet nằm ở tầng nào của mô hình TCP/IP?

- A. Tầng liên kết dữ liệu (data link)
- B. Tầng ứng dụng (application)
- C. Tầng vận chuyển (transport)
- D. Tầng vật lý (physical)

Đáp án: A

14. Nhiều hệ thống cố gắng gửi dữ liệu cùng lúc. Các xung điện gửi xuyên qua dây cáp sẽ giao thoa với nhau. Thuật ngữ nào mô tả hiện tượng này?

Mạng con (subnet)

- A. Mạng cục bộ (LAN)
- B. Miền đụng độ (collision domain)
- C. Mạng diện rộng (WAN)

Đáp án: C

15. Một người sử dụng đăng nhập vào một máy tính và mở email. Thiết bị nào sẽ cung cấp email đến máy tính?

- A. Server

- B. Switch
- C. Router
- D. Hub

Đáp án: A

Phần Tầng vật lý

1. Loại điều chế nào được sử dụng bởi mạng máy tính dùng cáp xoắn đôi?

- A. Kim bấm dây mạng (line crimping)
- B. Giao tiếp đơn kênh (simplex communication)
- C. Mã đường truyền (line coding)
- D. RJ45

Đáp án: C

2. Sự khác biệt giữa truyền song công toàn phần (full duplex) và bán song công (half duplex) là gì?

- A. Full duplex chậm hơn half duplex
- B. Full duplex cho phép giao tiếp theo hai chiều cùng lúc; half duplex nghĩa là chỉ một phía có thể giao tiếp ở một thời điểm nhất định
- C. Full duplex là một dạng giao tiếp đơn kênh (simplex)
- D. Half duplex xảy ra khi hub được sử dụng; full duplex xảy ra khi switch được sử dụng

Đáp án: B

3. Bạn lên xe hơi và mở radio. Loại giao tiếp nào mà radio sử dụng?

- A. Bán song công (half duplex)
- B. Song công đầy đủ (full duplex)
- C. Đơn công

D. Xoắn đôi

Đáp án: C

4. Loại đầu cắm phổ biến trong các cáp mạng xoắn đôi là loại nào?

- A. Registered Jack 46
- B. Registered Jack 11
- C. Registered Jack 35
- D. Registered Jack 45

Đáp án: D

5. Tủ thông tin liên lạc có một thiết bị gồm 48 cổng. Chức năng duy nhất của thiết bị là cung cấp các cổng. Loại thiết bị nào được đặt trong tủ này?

- A. Hub
- B. Patch panel
- C. Switch
- D. Router

Đáp án: B

Phân tầng liên kết dữ liệu

1. Có bao nhiêu octet (8 bit) trong một địa chỉ MAC?

- A. 4
- B. 6
- C. 5
- D. 8

Đáp án: B

2. Địa chỉ nào được sử dụng cho Ethernet broadcast?

- A. 00:00:00:00:00:00
- B. 11:11:11:11:11:11
- C. FF:00:FF:00:FF:00
- D. FF:FF:FF:FF:FF:FF

Đáp án: D

3. Kiểm dư chu trình (CRC) là gì?

- A. Một cách để 2 máy tính đồng bộ đồng hồ của chúng
- B. Một kỹ thuật cho phép nhiều mạng LAN logic thực thi trên cùng một thiết bị
- C. Một phép tính toán học được sử dụng để đảm bảo tất cả dữ liệu đến đều nguyên vẹn
- D. Dữ liệu thực sự được vận chuyển bởi khung tin Ethernet

Đáp án: C

4. Địa chỉ MAC viết tắt của từ:

- A. Media Access Control
- B. Message Authentication Check
- C. Maximum Allowable Cost
- D. Memory Access Controller

Đáp án: A

5. Ký tự B trong một địa chỉ MAC thể hiện giá trị nào?

- A. 10
- B. 9
- C. 11

D. 15

Đáp án: C

6. Loại cơ chế truyền nào có giá trị 0 tại một bit đặc biệt trong địa chỉ MAC máy đích?

- A. Multicast
- B. Broadcast
- C. Unicast
- D. Singlecast

Đáp án: C

7. Đoạn nào trong một khung Ethernet chứa dữ liệu từ tầng cao hơn, như IP và tầng vận chuyển, tầng ứng dụng?

- A. EtherType
- B. Frame Check Sequence
- C. Preamble
- D. Payload

Đáp án: D

Phần Tầng mạng

1. Vui lòng chọn tất cả các địa chỉ IP hợp lệ. Đánh dấu vào tất cả những câu phù hợp.

- A. 257.70.312.49
- B. 8.8.8.8
- C. 123.456.123.456
- D. 192.168.1.1

Đáp án: B,D

2. Mạng lớp C có bao nhiêu địa chỉ IP?

- A. 1 địa chỉ
- B. 256 địa chỉ
- C. 65.536 địa chỉ
- D. 16.777.216 địa chỉ

Đáp án: B

3. Điều gì xảy ra với trường TTL của một gói tin IP datagram mỗi khi nó đến một bộ định tuyến?

- A. Trường TTL được tăng lên 1 đơn vị
- B. Trường TTL được thiết lập lại về 0
- C. Trường TTL được sử dụng để kiểm dư chu trình (CRC)
- D. Trường TTL giảm đi 1 đơn vị

Đáp án: D

4. CIDR là viết tắt của thuật ngữ gì?

- A. Classless Internet Destination Routing
- B. Classless Inter-Domain Routing
- C. Classfull Inter-Destination Routing
- D. Classfull Identification Routing

Đáp án: B

5. Câu nào sau đây là dạng đúng của ký hiệu CIDR?

- A. 192.168.1.0 + 255.255.255.0
- B. 192.168.1.0\24
- C. 192.168.1.0:24

D. 192.168.1.0/24

Đáp án: D

6. Mặt nạ mạng con có cấu tạo bao nhiêu octet (byte)?

A. 1

B. 2

C. 3

D. 4

Đáp án: D

7. Chọn các ví dụ về giao thức định tuyến. Đánh dấu vào tất cả những câu phù hợp.

A. Hypertext Transfer Protocol

B. Routing Information Protocol

C. Border Gateway Protocol

D. User Datagram Protocol

E. Transmission Control Protocol

Đáp án: B,C

8. Ai được phép sử dụng không gian địa chỉ không thể định tuyến?

A. Bất kỳ người nào

B. IETF

C. IANA

D. Nó chỉ dành cho mục đích kiểm tra

Đáp án: A

9. Một bảng định tuyến điển hình có thể chứa nội dung nào sau đây? Đánh dấu vào tất cả những câu phù hợp.

- A. Mạng đích
- B. Địa chỉ máy đích
- C. TTL
- D. Tổng bước

Đáp án: A,D

10. Một broadcast ARP được gửi đến một địa chỉ MAC đặc biệt là

- A. FF:FF:FF:FF:FF:FF
- B. 00:00:00:00:00:00
- C. 255.255.255.255
- D. 192.168.0.1

Đáp án: A

11. Tiến trình lấy một mạng lớn và chia nó thành nhiều mạng con nhỏ hơn được biết đến với thuật ngữ nào?

- A. Encapsulation
- B. Fragmentation
- C. Subnetting
- D. Routing

Đáp án: C

12. Giao thức cổng trong được sử dụng bởi các router để mà chia sẻ thông tin bên trong một

- A. Miền đụng độ (collision domain)
- B. Mạng con (subnet)
- C. Hệ thống tự trị (autonomous system)
- D. Mạng đích (destination system)

Đáp án: C

13. Cóoctet trong một địa chỉ IP.

- A. 2
- B. 4
- C. 8
- D. 16

Đáp án: B

14. Trong hệ nhị phân, $1 + 1 = \dots$

- A. 2
- B. 10
- C. 1
- D. 0

Đáp án: B

15. Một octet trong địa chỉ IP thể hiện phạm vi nào của số hệ 10?

- A. 0-250
- B. 0-255
- C. 1-255
- D. 0-155

Đáp án: B

16. Giao thức nào giao tiếp dữ liệu giữa các router đại diện các cạnh của hệ thống tự trị?

- A. Giao thức cổng trong (interior gateway)
- B. Giao thức vectơ khoảng cách (distance-vector)

- C. Giao thức cổng ngoài (exterior gateway)
- D. Giao thức trạng thái liên kết (link state)

Đáp án: C

17. Trên mạng LAN, định danh nào mà các nút trong mạng sử dụng để giao tiếp nội bộ với nhau?

- A. Địa chỉ IP động (dynamic IP address)
- B. Địa chỉ IP tĩnh (static IP address)
- C. Địa chỉ MAC vật lý (physical MAC address)
- D. Dây số EIN (EIN serial)

Đáp án: C

18. Số nào không thể được biểu diễn bởi 8 bit dữ liệu?

- A. 128
- B. 232
- C. 12
- D. 436

Đáp án: D

19. Tiến trình lấy một gói tin IP datagram và chia thành nhiều datagram nhỏ hơn được gọi là?

- A. Gom nhóm (clustering)
- B. Cân bằng tải (load balancing)
- C. Tường lửa NAT (NAT firewall)
- D. Phân mảnh (fragmentation)

Đáp án: D

20. Mục đích của một phản hồi ARP là gì?

- A. Để một máy tính đang broadcast (phát tán) một thông điệp ARP biết địa chỉ MAC nào để đặt vào trường địa chỉ phần cứng máy đích
- B. Cải thiện bảo mật xác thực
- C. Gửi một thông điệp ACK đến máy tính đang broadcast
- D. Để ngăn chặn một cơn lũ các gói UDP

Đáp án: A

21. Mặt nạ mạng con 255.255.255.0 để cập điều gì cho router?

- A. Phần nào của một địa chỉ IP là ID mạng con và phần nào là ID máy
- B. IP tĩnh của router cổng
- C. Máy kế tiếp trên đường định tuyến mạng
- D. Địa chỉ MAC của một máy

Đáp án: A

22. Số khả năng lớn nhất ở hệ 10 được thể hiện trong 16 bit?

- A. 65536
- B. 16
- C. 1600
- D. 256

Đáp án: A

23. Máy tính A muốn gửi một số dữ liệu đến máy B. Máy A biết rằng máy B không ở trong mạng cục bộ của nó, vì vậy nó gửi gói tin đến router giữa mạng A và mạng B. Dựa trên số máy mạng đã xảy ra, hãy cho biết trường TTL sẽ giảm bao nhiêu lần để đi từ máy A đến máy B?

- A. 6
- B. 2

- C. 8
- D. 1

Đáp án: B

24. Loại không gian địa chỉ mạng nào cho phép các nút trên mạng giao tiếp với nhau, nhưng ngăn chặn bất kỳ router chuyển tiếp gói tin ra và vào mạng đó?

- A. Địa chỉ MAC
- B. Không gian địa chỉ không thể định tuyến
- C. Mặt nạ mạng con
- D. Địa chỉ IP

Đáp án: B

Phần tầng vận chuyển

1. Thứ tự nào của cờ trong TCP segment tạo nên quy trình bắt tay ba bước?

- A. FIN, FIN/ACK, ACK
- B. SYN, ACK, SYN, ACK
- C. SYN, SYN/ACK, ACK
- D. SYN, ACK, FIN

Đáp án: B

2. Các giao thức tầng vận chuyển, như TCP và UDP, giới thiệu khái niệm về cổng (port). Bao nhiêu bit để biểu diễn cổng?

- A. 4 bit
- B. 8 bit
- C. 16 bit
- D. 32 bit

Đáp án: C

3. Chọn tất cả các cờ điều khiển TCP hợp lệ.

- A. CLOSE
- B. RST
- C. ACK
- D. WAIT
- E. LISTEN
- F. URG

Đáp án: B,C,F

4. Thiết bị ngăn chặn các giao tiếp khớp với các tiêu chí định trước được gọi là _____.

- A. Router
- B. Firewall
- C. Switch
- D. Hub

Đáp án: B

5. Nếu một TCP socket đã sẵn sàng và lắng nghe tín hiệu đến, nó đang ở trạng thái nào?

- A. ESTABLISHED
- B. CLOSE_WAIT
- C. SYN_SENT
- D. LISTEN

Đáp án: D

6. Ví dụ phổ biến của giao thức hướng kết nối là _____

- A. UDP
- B. TCP
- C. IP

Đáp án: B

7. Khái niệm về việc nhận dữ liệu tất cả đều hướng đến cùng một nút và phân phối nó đến dịch vụ nhận thích hợp được biết đến như _____

- A. Ghép kênh
- B. Tách kênh
- C. Định tuyến
- D. Đóng gói

Đáp án: B

8. Tầng vận chuyển quản lý việc ghép kênh và tách kênh qua loại thiết bị nào?

- A. Hub
- B. Switch
- C. Port
- D. Router

Đáp án: C

9. FTP thường lắng nghe trên cổng nào?

- A. 25
- B. 80
- C. 443
- D. 21

Đáp án: D

10. Trường nào trong TCP header được chọn từ các cổng tạm?

- A. Số xác nhận (acknowledgement number)
- B. Số thứ tự (sequence number)
- C. Cổng đích (destination port)
- D. Cổng nguồn (source port)

Đáp án: D

11. Một giao thức giữa hai thiết bị vượt quá giới hạn cực đại của một kích thước khung Ethernet. TCP chia dữ liệu ra thành những đoạn. Trường nào trong phần header giúp đỡ lưu vết của nhiều đoạn dữ liệu?

- A. Tổng kiểm (checksum)
- B. Số thứ tự (sequence number)
- C. Con trỏ khẩn cấp (urgent pointer)
- D. Số xác nhận (acknowledgement number)

Đáp án: B

12. Giao thức TCP sẽ gửi tất cả các đoạn dữ liệu theo thứ tự nào?

- A. Ngẫu nhiên
- B. Lớn nhất đến nhỏ nhất
- C. Tuần tự
- D. Ưu tiên

Đáp án: C

13. Khi nào sử dụng TCP thích hợp nhất?

- A. Khi đang lắng nghe radio
- B. Khi đang duyệt một website tin tức

- C. Khi đang phát trực tiếp một đoạn phim
- D. Khi đang gọi điện thoại

Đáp án: B

14. Giá trị 1 trong cờ điều khiển ACK thể hiện điều gì?

- A. Trường số xác nhận cần được kiểm tra
- B. Nó là lần đầu chuyển dữ liệu
- C. Có 1 gói tin cần vận chuyển
- D. Có nhiều hơn một gói tin cần vận chuyển

Đáp án: A

15. Một thiết bị trong kết nối TCP sẵn sàng để đóng kết nối. Thiết bị khác đang trong kết nối đồng ý. Điều gì đã xảy ra?

- A. Bắt tay
- B. Bắt tay bốn bước
- C. Bắt tay ba bước
- D. Bắt tay hai bước

Đáp án: B

Phần tầng ứng dụng

1. Khác với mô hình năm lớp, mô hình mạng OSI thêm hai lớp nữa trên đầu tầng ứng dụng. Chọn các ví dụ về các lớp mới này bên dưới.

- A. Tầng trình bày (presentation layer)
- B. Tầng mã hóa (encryption layer)
- C. Tầng nén (compression layer)
- D. Tầng phiên (session layer)

Đáp án: A,D

2. Ví dụ về thứ nào sau đây hoạt động ở tầng ứng dụng?

- A. Trình duyệt web
- B. Router
- C. TCP
- D. UDP

Đáp án: A

3. Giá trị tiêu chuẩn cho trường TTL là gì?

- A. 8
- B. 16
- C. 32
- D. 64

Đáp án: D

4. HTTP là một ví dụ của một giao thức tầng _____

- A. Vận chuyển
- B. Liên kết dữ liệu
- C. Ứng dụng
- D. Mạng

Đáp án: C

5. Dữ liệu tầng ứng dụng sống trong phần nào của giao thức tầng vận chuyển

- A. Data payload
- B. Header
- C. Footer

D. flags

Đáp án: C

6. Trình bày theo cách hiểu của bạn, hãy mô tả điều gì xảy ra ở mỗi tầng của mô hình mạng khi một máy trên mạng thiết lập kết nối TCP với một máy khác. Giả sử, cả hai mạng đều được kết nối với cùng một router.

Mô tả cần đề cập:

- 5 tầng của mô hình TCP
- Địa chỉ MAC
- Địa chỉ IP
- Cổng TCP
- Kiểm tra lỗi
- Bảng định tuyến
- TTL (thời gian sống)

Phân giải tên miền

1. DNS thường sử dụng giao thức lớp truyền tải nào?

- A. ICMP
- B. TCP
- C. UDP
- D. IP

Đáp án: C

2. DNS TTL xác định điều gì?

- A. Có bao nhiêu lượt phân giải DNS có thể diễn ra trước khi IP phải thay đổi
- B. DNS có thể cách bạn bao xa

- C. Có bao nhiêu bước trong tiến trình phân giải
- D. Khoảng thời gian một mục DNS được phép lưu trong bộ nhớ đệm

Đáp án: D

3. Có bao nhiêu máy chủ gốc?

- A. 8
- B. 13
- C. 16
- D. 17

Đáp án: B

4. Một bản ghi A chứa những gì?

- A. CNAME
- B. Địa chỉ IPv4
- C. Địa chỉ IPv6
- D. Tên miền đủ điều kiện

Đáp án: B

5. Chọn tất cả câu đúng.

- A. Một tên miền có thể trỏ đến một IP
- B. Một tên miền có thể trỏ đến nhiều IP
- C. Nhiều tên miền có thể trỏ đến cùng IP

Đáp án: A,B,C

6. MX viết tắt của _____

- A. Micro extreme
- B. Micro exchange

- C. Mail exchange
- D. Meta exchange

Đáp án: C

7. Một tên miền đủ điều kiện có thể chứa bao nhiêu ký tự?

- A. 63
- B. 64
- C. 127
- D. 255

Đáp án: D

8. Bốn thứ mà tất cả các máy tính cần được cấu hình để hoạt động trên một mạng hiện đại là gì? Đánh dấu vào tất cả những gì phù hợp.

- A. Máy chủ NTP
- B. Địa chỉ IP
- C. Gateway mặc định
- D. Cổng TCP
- E. Mặt nạ mạng con
- F. Địa chỉ MAC
- G. Máy chủ tên miền

Đáp án: B,C,E,G

9. Khi sử dụng DHCP cấp phát cố định, điều gì được sử dụng để xác định IP của máy tính?

- A. Vị trí
- B. Bản ghi
- C. Địa chỉ MAC
- D. Mặt nạ mạng con

Đáp án: C

10. Tiến trình mà máy khách sử dụng các lần thử DHCP để lấy thông tin cấu hình mạng được gọi là _____.

- A. DHCP Discovery
- B. DHCP Offer
- C. DHCP Request
- D. DHCP Acknowledgement

Đáp án: A

11. NAT giải quyết vấn đề về không gian địa chỉ IPv4 đang bị thu hẹp bằng cách _____.

- A. cho phép các mạng sử dụng ít địa chỉ IP hơn về tổng thể
- B. cho phép người sử dụng chuyển sang ipv6 khi họ muốn
- C. cho phép máy tính sử dụng không gian địa chỉ không định tuyến để giao tiếp với mạng Internet
- D. thực hiện giả mạo IP

Đáp án: C

12. Kỹ thuật nào cho phép dữ liệu đi vào trong thông qua NAT?

- A. Duy trì cổng (port preservation)
- B. Chuyển tiếp cổng (port forwarding)
- C. Phân quyền cổng (port authority)
- D. Cổng tạm

Đáp án: B

13. Tổng số địa chỉ IPv4 xấp xỉ:

- A. 4.2 triệu
- B. 4.2 tỷ
- C. 4.2 nghìn tỷ
- D. Không thể đếm xuể

Đáp án: B

14. Xác thực hai yếu tố là_____.

- A. một phương pháp mà bạn xác thực hai lần
- B. một phương thức yêu cầu hai tên người dùng
- C. một phương pháp mà bạn cần nhiều hơn tên người dùng và mật khẩu
- D. một phương pháp mà bạn cần hai mật khẩu

Đáp án: C

15. VPN được biết đến như một giao thức _____

- A. Tầng mạng (network layer)
- B. Tầng liên kết dữ liệu (data link layer)
- C. Phi kết nối (connectionless)
- D. Đường ống (tunneling)

Đáp án: D

16. Một proxy là một thứ mà_____.

- A. Giao tiếp như một thứ khác
- B. Cho phép nhiều thiết bị nói chuyện với một thiết bị khác
- C. Mã hóa dữ liệu được gửi qua Internet
- D. Gửi dữ liệu qua một khúc mạng

Đáp án: A

17. Một kỹ thuật được sử dụng để định tuyến gói tin đến các điểm đến khác nhau, tùy thuộc vào các yếu tố như vị trí, tắc nghẽn hoặc tình trạng liên kết, được gọi là _____

- A. Unicast
- B. Anycast
- C. Multicast
- D. Broadcast

Đáp án: B

18. Một khái niệm liên quan đến việc lặp lại danh sách từng mục một theo thứ tự được gọi là _____

- A. Xoay vòng (round robin)
- B. đệ quy (recursion)
- C. Tra cứu phân quyền (authoritative lookup)
- D. Ghép kênh (multiplexing)

Đáp án: A

19. Cùng với địa chỉ IP, mặt nạ mạng con và máy chủ tên miền, thứ khác cần thiết để máy tính hoạt động trên mạng là _____

- A. Proxy
- B. Gateway
- C. Máy chủ NTP
- D. FQDN

Đáp án: B

20. Khi một dải địa chỉ IP được sử dụng cho các thiết bị khách và một trong những IP này được cấp cho các thiết bị khi chúng yêu cầu, cách này được gọi là cấp phát _____

- A. Tự động (automatic)
- B. Động (dynamic)

C. Cố định (fixed)

Đáp án: B

21. Khi NAT ẩn IP nguồn của một thiết bị gốc, điều này được gọi là _____

- A. Chuyển tiếp cổng (port forwarding)
- B. Định tuyến (routing)
- C. Chuyển mạch (switching)
- D. Giả mạo IP (IP masquerading)

Đáp án: D

22. Ở mức thấp nhất, máy tính hiểu được dữ liệu nào?

- A. Chữ số thập lục phân (hệ 16)
- B. Địa chỉ MAC
- C. Số nhị phân
- D. Địa chỉ IP

Đáp án: C

23. Phần "www" của tên miền được xác định bằng lựa chọn nào sau đây? Đánh dấu vào tất cả những câu phù hợp.

- A. Tên miền cấp cao
- B. Tên miền phụ
- C. Tên miền đủ tiêu chuẩn
- D. Tên máy tính

Đáp án: B

24. Kỹ sư hệ thống CNTT tạo một vùng hệ thống tên miền (DNS) mới có chứa các bản ghi tài nguyên con trỏ (PTR). Loại vùng nào đã được tạo?

- A. Start of Authority (SOA)
- B. Tên miền đủ tiêu chuẩn
- C. Tên miền phụ
- D. Tra cứu ngược

Đáp án: D

25. NAT thường được thực hiện với những thiết bị phần cứng nào? Chọn tất cả các câu phù hợp.

- A. Hub
- B. Router
- C. Firewall
- D. Swicht

Đáp án: A,C

26. Cổng nào trên một máy chủ tên miền được sử dụng cho gói tin yêu cầu tên miền UDP?

- A. 80
- B. 22
- C. 25
- D. 53

Đáp án: D

27. Một tên miền đủ tiêu chuẩn (FQDN) giới hạn bao nhiêu ký tự?

- A. 127
- B. 53
- C. 63
- D. 255

Đáp án: D

28. Điều nào sau đây KHÔNG được cấu hình bởi máy chủ DHCP?

- A. Địa chỉ MAC
- B. Địa chỉ IP
- C. Địa chỉ gateway
- D. Địa chỉ mặt nạ mạng con

Đáp án: A

29. Hệ thống nội bộ đằng sau tường lửa cần được cấu hình để truy cập từ xa. NAT cần được cấu hình như thế nào?

- A. Duy trì (preservation)
- B. Viết lại (rewriting)
- C. Chuyển tiếp cổng (port forwarding)
- D. NAT một-nhiều

Đáp án: C

30. Dịch vụ nào hành xử như thể một máy tính khách để truy cập một dịch vụ khác?

- A. DNS
- B. Ống VPN
- C. Máy chủ proxy
- D. DHCP

Đáp án: C

31. Trong quá trình phân giải tên, kỹ thuật nào được sử dụng để tránh tắc nghẽn khi truy vấn máy chủ?

- A. Redirect

- B. Anycast
- C. Lookup
- D. Hierarchy

Đáp án: B

Phần Kết Nối Quay Số và Bảng Thông Rộng

1. Một thuật ngữ khác cho POTS là _____.

- A. Public Available Telephone Network
- B. Public Switched Telephone Exchange
- C. Phone Switched Transport Network
- D. Public Switched Telephone Network
- E. Public Available Telephone Exchange

Đáp án: D

2. Tỷ lệ baud là phép đo số _____.

- A. gói có thể được gửi qua một đường dây điện thoại mỗi giây
- B. byte có thể được gửi qua đường dây điện thoại mỗi giây
- C. bit có thể được gửi qua một đường dây điện thoại mỗi giây
- D. phân đoạn dữ liệu có thể được gửi qua một đường dây điện thoại mỗi giây

Đáp án: C

3. T1 là viết tắt của _____.

- A. Transmission 1
- B. Transportation 1
- C. Transmission System 1

D. Transportation System 1

Đáp án: C

4. Đường T1 nhanh bao nhiêu?

- A. 128 Mb/s
- B. 1.544 Mb/s
- C. 1 Mb/s
- D. 44.763 Mb/s

Đáp án: B

5. Chọn tất cả các câu đúng về kết nối internet cáp.

- A. Chúng ta kết nối bằng thông rộng
- B. Chúng là kết nối không dây
- C. Chúng là kết nối quay số
- D. Chúng là kết nối bằng thông được chia sẻ

Đáp án: A,D

6. Tốc độ kết nối quay số có thể gửi dữ liệu qua dây điện thoại được gọi là tỉ lệ _____

- A. Baud
- B. Dữ liệu
- C. Truyền nhận
- D. Âm thanh

Đáp án: A

7. Tên chính xác hơn cho modem được sử dụng cho kết nối DSL _____

- A. POTS

- B. DSLAM
- C. CMTS
- D. ONT

Đáp án: B

8. ONT được viết tắt của từ _____

- A. Optical Network Telephone
- B. Optional Network Traffic
- C. Optical Network Tether
- D. Optical Network Terminator

Đáp án: D

9. Các modem giao tiếp dữ liệu bằng cách sử dụng phương thức nào?

- A. Sạc điện (electric charge)
- B. Bước sóng âm nghe được (audible wavelength)
- C. Tần số vô tuyến (radio frequency)
- D. Xung ánh sáng

Đáp án: B

10. Hệ thống Internet nào, vẫn tồn tại cho đến ngày nay, được xây dựng vào những ngày đầu của mạng quay số?

- A. Bảng thông rộng
- B. WWW
- C. USENET
- D. Hệ thống bảng thông báo (Bulletin Board System)

Đáp án: C

11. Đường T1 hỗ trợ bao nhiêu trao đổi thoại cùng lúc?

- A. 28
- B. 23
- C. 24
- D. 20

Đáp án: C

Phần Mạng Diện Rộng, Mạng Không Dây và Mạng Viễn Thông

1. WAN viết tắt của _____.

- A. Wireless Area Network
- B. Wide Area Network
- C. Wired Area Network
- D. Wireless Local Area Network

Đáp án: B

2. Trong mạng WAN, khu vực giữa điểm phân giới và mạng lõi của ISP được gọi là _____.

- A. Access Point
- B. Local link
- C. Local loop
- D. Local Area Network

Đáp án: C

3. Point-to-point VPN còn được gọi là _____.

- A. Site-to-site VPN
- B. One-to-many VPN
- C. Port forwarding VPN
- D. Data link VPN

Đáp án: C

4. Header của 802.11 có bao nhiêu trường địa chỉ?

- A. 1
- B. 2
- C. 3
- D. 4

Đáp án: D

5. Một kênh không dây là _____

- A. Một kết nối không dây điểm-đến-điểm
- B. Một phần của một dải tần số
- C. Một ví dụ của mạng tùy biến
- D. Một miền đưng độ

Đáp án: B

6. Chọn tất cả các tần số mà mạng không dây thường hoạt động.

- A. 88 Mhz
- B. 1.544 Ghz
- C. 2.4 Ghz
- D. 5 Ghz

Đáp án: C, D

7. Mạng không dây truyền thông liên quan đến các điểm truy cập (AP) mà tất cả đều có kết nối có dây được gọi là _____

- A. LAN
- B. WLAN
- C. WAN
- D. Mạng tùy biến (ad-hoc)

Đáp án: B

8. WPA viết tắt của _____

- A. WiFi Protected Access
- B. Wireless Protection Augmentation
- C. WiFi Proxy Access
- D. Wired Protected Access

Đáp án: A

9. Đường dây thuê bao kỹ thuật số (DSL) là tùy chọn kết nối Internet duy nhất có sẵn cho một văn phòng nhỏ ở một nơi vắng vẻ. Loại nào sẽ cung cấp tốc độ trên 1,544 Mb/s?

- A. DSLAM
- B. SDSL
- C. HDSL
- D. ADSL

Đáp án: C

10. Mạng riêng ảo điểm-điểm (VPN) sử dụng loại thiết bị này tại mỗi điểm.

- A. PPPoE
- B. Firewall

- C. Multiplexer
- D. Model

Đáp án: B

11. Khung 802.11 chứa một số trường. Trường nào mô tả phiên bản 802.11 đang được sử dụng?

- A. Duration
- B. Frame control
- C. Sequence control
- D. Address

Đáp án: B

12. Cái nào sau đây KHÔNG phải là một loại kết nối mạng diện rộng (WAN)?

- A. Frame relay
- B. Asynchronous Transfer Mode (ATM)
- C. High-Level Data Link Control (HDLC)
- D. Digital Subscriber Line (DSL)

Đáp án: D

13. Hai đặc trưng của một mạng không dây băng tần 5 Ghz là gì? Chọn tất cả câu đúng.

- A. Tốc độ thấp
- B. Phạm vi hẹp
- C. Tốc độ nhanh
- D. Phạm vi rộng

Đáp án: B,C

14. Một nhà CNTT nghi ngờ rằng một thiết bị trái phép được kết nối với mạng không dây. Đây

là kết quả của việc chia sẻ mật khẩu trên một thiết bị được mang từ nhà. Điều gì được đặt ra để ngăn chặn hoạt động như vậy?

- A. Bộ lọc MAC
- B. Chống kênh
- C. WAP2
- D. Miễn đựng độ

Đáp án: A

15. Các cáp Cat5 và Cat6 liên quan đến tầng nào?

- A. Vật lý
- B. Trình bày
- C. Vận chuyển
- D. Liên kết dữ liệu

Đáp án: A

16. Hai thuận lợi mà cấu hình một mạng mesh không dây mang lại? Chọn tất cả các câu thích hợp.

- A. Phạm vi
- B. Cài đặt bảo mật WiFi
- C. Tốc độ
- D. Cấu hình tùy biến

Đáp án: A, C

Phần khắc phục sự cố mạng

1. Giao thức được sử dụng để thông báo lỗi mạng được gọi là _____.

- A. TCP

- B. Traceroute
- C. ICMP
- D. UDP

Đáp án: C

2. Tiện ích ping gửi loại tin nhắn nào?

- A. Destination Network Unreachable
- B. Echo Reply
- C. Destination Network Unknown
- D. Echo Request

Đáp án: D

3. Trên Windows, một trong những công cụ bạn có thể sử dụng để xác minh kết nối với một cổng cụ thể là _____.

- A. ping
- B. Tet-NetConnection
- C. NC (netcat)
- D. tracert

Đáp án: B

4. Khả năng để một giao thức hoặc chương trình xác định rằng đã xảy ra sự cố được gọi là _____.

- A. Tính dư thừa
- B. Xác nhận dữ liệu
- C. Phát hiện lỗi
- D. Phục hồi dữ liệu

Đáp án: C

5. Một công nghệ sử dụng công cụ netcat trên hệ thống Linux. Trong số các lựa chọn sau, lựa chọn nào có cú pháp thích hợp?

- A. nc -v 80
- B. nc google.com -z
- C. nc google.com
- D. nc google.com 80

Đáp án: D

6. Trường đầu tiên của gói ICMP mô tả loại thông báo. Những lựa chọn nào sau đây là ví dụ về loại thông báo? Đánh dấu vào tất cả những câu phù hợp.

- A. Destination port unreachable (không đến được cổng đích)
- B. Destination unreachable (không đến được máy đích)
- C. Time exceeded (vượt ngưỡng thời gian)
- D. Destination network unreachable (không đến được mạng đích)

Đáp án: B,C

7. Bạn chạy lệnh Test-NetConnection trên PC Windows trong khi chỉ cung cấp tên máy chủ. Kết quả là, lệnh sử dụng hành động mặc định nào?

- A. Private tunnel (đường hầm riêng tư)
- B. Name server lookup (tra cứu máy chủ tên miền)
- C. Network address translation (chuyển đổi địa chỉ mạng)
- D. Echo request (yêu cầu echo)

Đáp án: D

Phần DNS

1. Một trong những máy chủ DNS công cộng của Cấp 3 là _____.

- A. 4.2.2.3
- B. 8.8.8.8
- C. 127.0.0.1
- D. 192.168.1.1

Đáp án: A

2. Một công cụ kiểm tra phân giải DNS có sẵn trên tất cả các hệ điều hành máy tính là _____.

- A. host
- B. ping
- C. tracert
- D. nslookup

Đáp án: D

3. Tổ chức chịu trách nhiệm quản lý DNS ở cấp độ toàn cầu là _____.

- A. IANA
- B. Google
- C. ICANN
- D. RFC

Đáp án: C

4. Trong một phiên nslookup tương tác, bạn sẽ sử dụng từ khóa _____ để thay đổi máy chủ DNS mà bạn đang sử dụng.

- A. server
- B. client
- C. FQDN
- D. DNS

Đáp án: A

5. Traceroute sử dụng gói UDP trên hệ điều hành nào sau đây? Đánh dấu vào tất cả những câu phù hợp.

- A. Windows 7
- B. Windows 10
- C. Mac OS
- D. Linux

Đáp án: C,D

6. Khi đăng ký một tên miền mới, máy chủ của tổ chức đăng ký tên miền hoặc máy chủ thuộc sở hữu của mình có thể được sử dụng làm máy chủ định danh. Máy chủ định danh sẽ cung cấp chức năng gì cho tên miền?

- A. Address reservation (giữ chỗ địa chỉ)
- B. Authoritative (thẩm quyền)
- C. Error recovery (phục hồi lỗi)
- D. Domain transfer (chuyển miền)

Đáp án: B

Phần điện toán đám mây

1. Một phần mềm chạy và quản lý các máy ảo được gọi là _____.

- A. Virtual Instance
- B. Hypervisor
- C. Cloud computing device
- D. Cloud storage device

Đáp án: B

2. Office 365 Outlook là một ví dụ về _____.

- A. IaaS
- B. PaaS
- C. SaaS
- D. FaaS

Đáp án: C

3. Đám mây lai (hybrid cloud) là _____.

- A. Một sự kết hợp của public cloud và private cloud
- B. Một sự kết hợp của public cloud và ảo hóa phần cứng
- C. Một sự kết hợp của host ảo và guest ảo
- D. Một sự kết hợp của private cloud và mạng mesh

Đáp án: A

4. Với ảo hóa, một máy vật lý duy nhất, được gọi là máy chủ, có thể chạy nhiều phiên bản ảo riêng lẻ, được gọi là _____.

- A. client
- B. guest
- C. server
- D. cloud

Đáp án: B

5. PaaS viết tắt của từ

- A. Platform as a Service
- B. Packets as a Service
- C. Preamble as a Service

D. Platform as a Schedule

Đáp án: A

6. Tên của việc cung cấp dịch vụ dựa trên ảo hóa phần cứng là gì?

- A. Network Address Translation (NAT)
- B. Subnetting
- C. Domain Name System (DNS) service model
- D. Cloud computing

Đáp án: D

7. Là người ra quyết định về CNTT, bạn có kế hoạch đáp ứng nhu cầu kinh doanh bằng cách sử dụng phần mềm như một dịch vụ. Những lựa chọn nào để bạn triển khai?

- A. Linux Workstation
- B. Virtual Firewall
- C. Office 365
- D. Windows Server 2019

Đáp án: C

8. Một công ty điều hành các công nghệ nhạy cảm tại địa phương, trong khi ủy thác các công nghệ ít nhạy cảm hơn cho cơ sở người dùng rộng lớn hơn. Mô hình phân phối đám mây nào đang được sử dụng?

- A. Private
- B. Hybrid
- C. Public
- D. Community

Đáp án: B

Phần Địa Chỉ IPv6

1. Địa chỉ IPv6 dài bao nhiêu bit?

- A. 16
- B. 32
- C. 64
- D. 128

Đáp án: D

2. Trường đầu tiên trong IPv6 header là _____.

- A. Class
- B. Version
- C. Địa chỉ nguồn
- D. Dữ liệu

Đáp án: B

3. Trường trong IPv6 header cho biết có bao nhiêu bộ định tuyến có thể chuyển tiếp một gói trước khi gói bị loại bỏ được gọi là _____.

- A. TTL
- B. Next header
- C. Router forward
- D. Hop limit

Đáp án: D

4. Trường TTL trong IPv4 header tương đương với trường _____ trong IPv6 header.

- A. hop limit
- B. traffic class
- C. next header

D. flow label

Đáp án: A

5. Có bao nhiêu số 0 được tìm thấy ở đầu địa chỉ IPv6 mà tương quan với địa chỉ IPv4?

- A. 40
- B. 128
- C. 32
- D. 80

Đáp án: D

6. Để dữ liệu truy cập IPv6 di chuyển trên mạng IPv4, hai công nghệ nào được sử dụng?
Đánh dấu vào tất cả những câu phù hợp.

- A. Packet
- B. IPv4 Tunnel
- C. IPv6 Tunnel
- D. Datagram

Đáp án: C, D

7. Kích thước của trường payload length của IPv6?

- A. 20 bit
- B. 8 bit
- C. 32 bit
- D. 16 bit

Đáp án: D
