

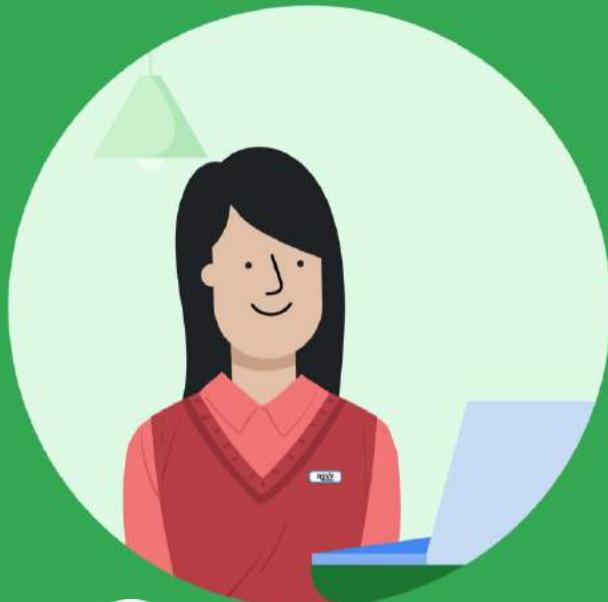


Bit và Byte Của Mạng Máy Tính

Nhóm biên soạn:

1. Lê Ngọc Thành
2. Phạm Trọng Nghĩa
3. Tạ Việt Phương
4. Trương Tấn Khoa

Năm 2022



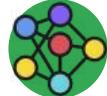
1 GIỚI THIỆU MẠNG MÁY TÍNH



NỘI DUNG



Mạng máy tính và các thuật ngữ cơ bản



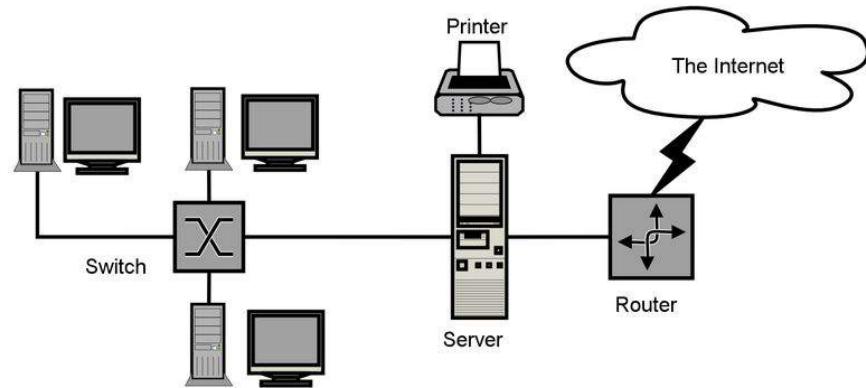
Mô hình mạng



Thiết bị mạng

Mạng máy tính

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)



Nguồn: Wikimedia

Các thuật ngữ

Một số thuật ngữ liên quan

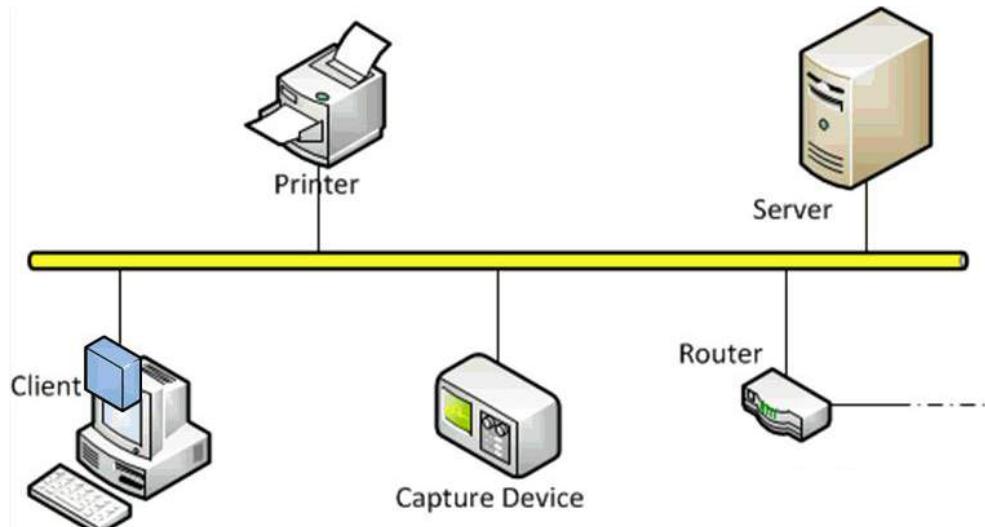


- Bảo mật (security)
- Phạm vi kết nối (spatial scope)
- Liên kết mạng (network link)**
- Dịch vụ mạng (network service)
- Gói tin mạng (network packet)**
- Giao thức giao tiếp (communication protocol)
- Đồ hình mạng (network topology)**
- Chất lượng (network performance)
- Nút mạng (network node)



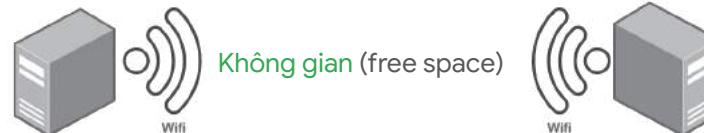
Gói tin mạng

Gói tin mạng (network packet) là một **đoạn dữ liệu** được **đóng gói** theo **một định dạng nhất định** và truyền đi trong mạng



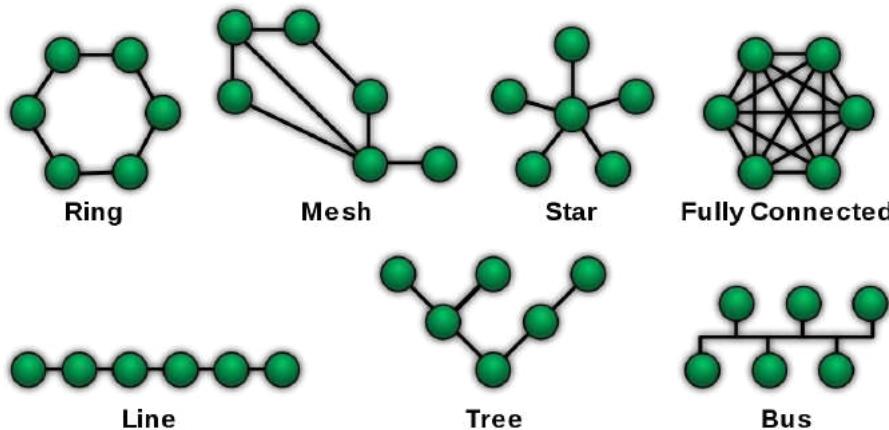
Liên kết mạng

- Liên kết mạng (network link) là phương tiện truyền nhận để **liên kết** các thiết bị hình thành nên mạng máy tính.
- Các loại phương tiện gồm:



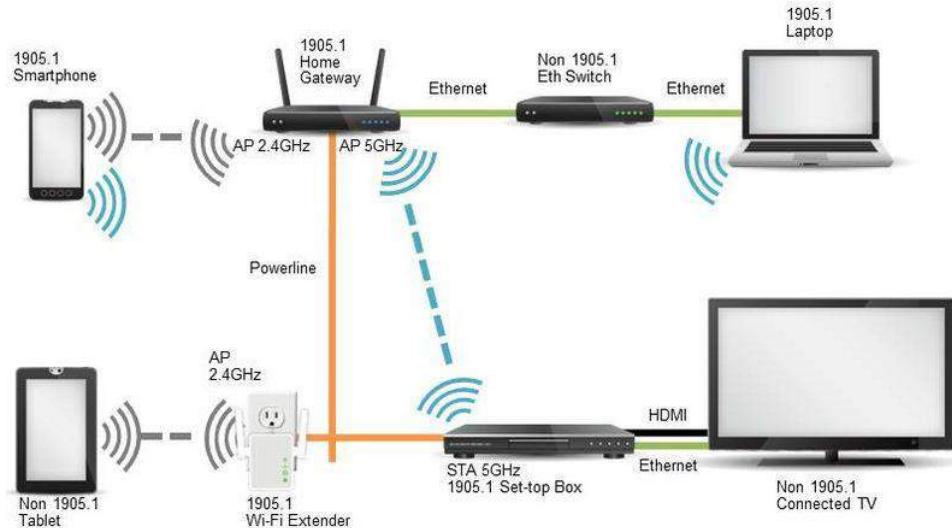
Đồ hình mạng

Cách sắp xếp các thành phần trong mạng như dây dẫn, thiết bị để hình thành ra một cấu trúc liên kết mạng hay **đồ hình mạng** (network topology)



Nút mạng

- Một nút mạng (network node) hoặc là một **điểm phân phối lại** hoặc là một **điểm cuối** trong giao tiếp mạng.
- Một số nút mạng như card mạng, hub, repeater, switch, v.v.



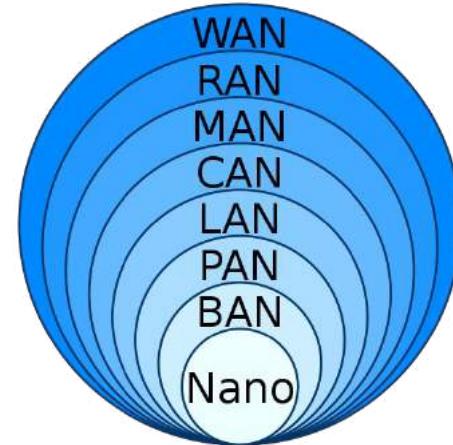
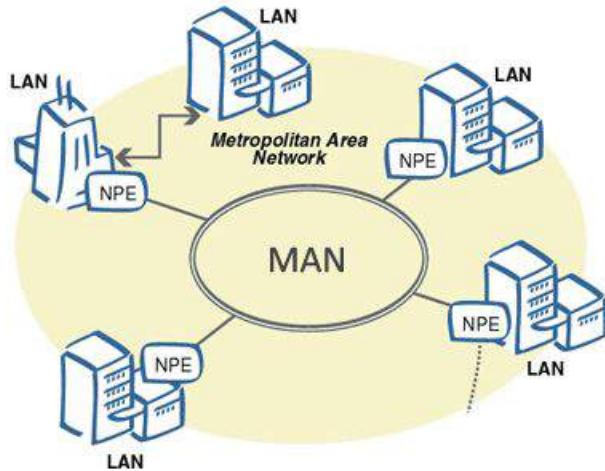
Giao thức giao tiếp

- Giao thức giao tiếp (communication protocol) là **tập các quy tắc** để các máy tính có thể trao đổi thông tin với **nhau** một cách đầy đủ và chính xác.
- Một số giao thức phổ biến: TCP/IP, HTTP, HTTPS, FTP, SMTP, v.v.



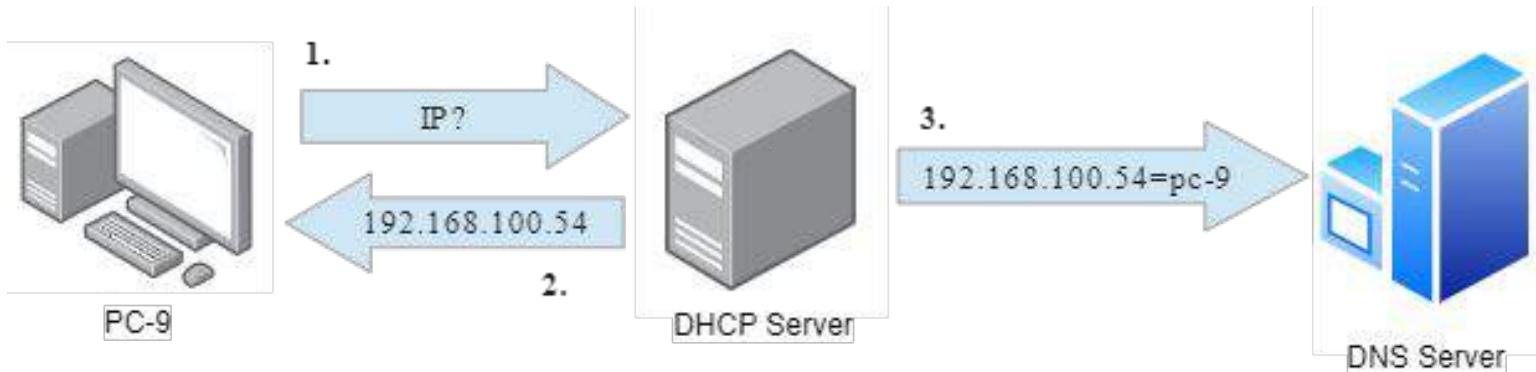
Phạm vi kết nối

Phạm vi kết nối (spatial scope) mô tả về độ bao phủ của một mạng



Dịch vụ mạng

- Dịch vụ mạng (network service) là **các ứng dụng chạy trên máy chủ** để cung cấp các chức năng cho người dùng hoặc phục vụ cho quá trình vận hành của chính nó.
- Ví dụ: DNS, DHCP, File Server, v.v.



Chất lượng và bảo mật mạng

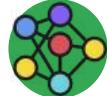
- Chất lượng được đo qua một số chỉ số như băng thông, độ trễ, chất lượng dịch vụ, v.v
- Bảo mật mạng liên quan đến bảo vệ, giám sát các hoạt động bất thường trong mạng, mã hóa đầu-cuối, v.v.



NỘI DUNG



Mạng máy tính và các thuật ngữ cơ bản



Mô hình mạng



Thiết bị mạng

Mô hình mạng

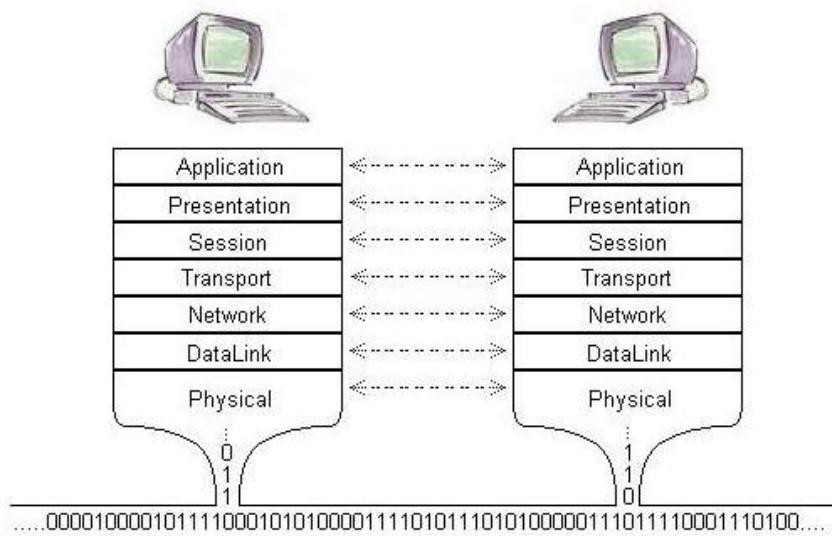
- Mô hình mạng (network model) là một thiết kế hoặc kiến trúc tổng thể để thực hiện giao tiếp giữa các hệ thống khác nhau.
- Một số thuật ngữ thay thế: **chồng giao thức mạng** (network stack), **bộ giao thức** (protocol suite)
- Một số mô hình mạng phổ biến: mô hình OSI, mô hình TCP/IP 5 lớp.



Kiến trúc tầng

Một mô hình mạng bao gồm **các tầng** (layer).

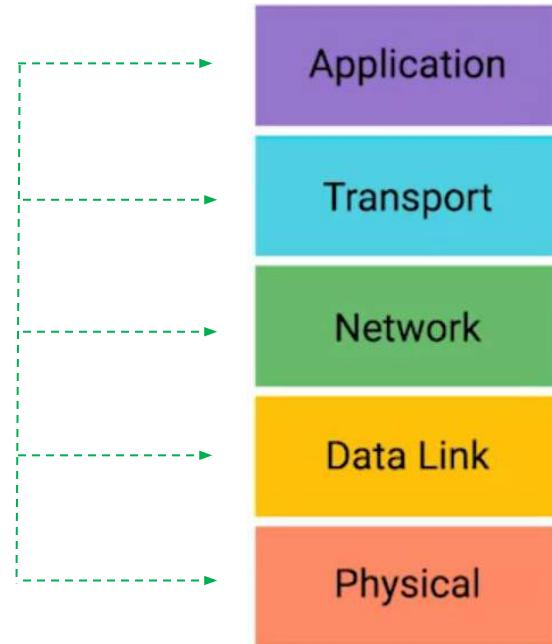
- Mỗi tầng thể hiện một **chức năng cụ thể**
- Bên trong tầng, thường **có các giao thức** (protocol) để thực hiện các nhiệm vụ cụ thể



Mô hình TCP/IP

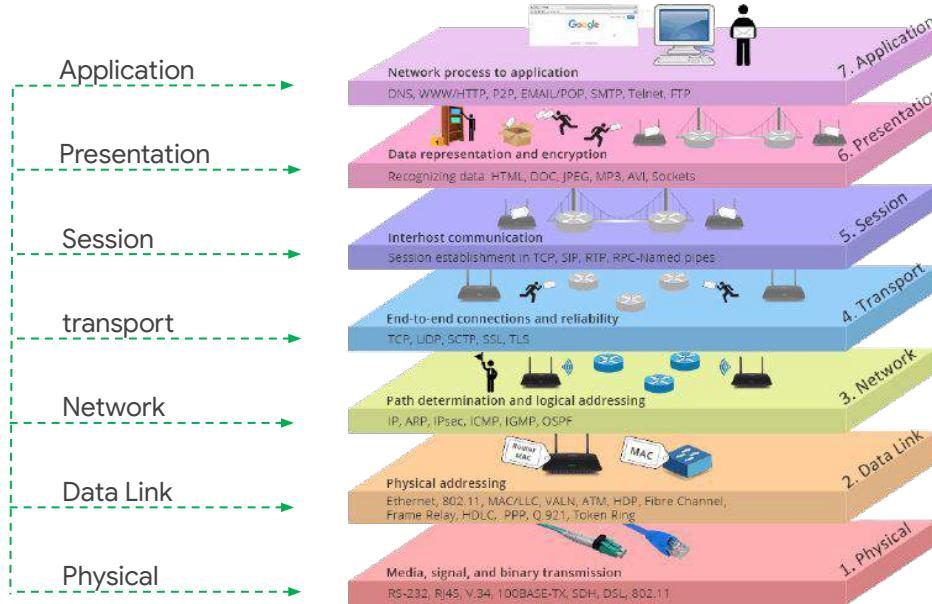


Mô hình TCP/IP
gồm 5 tầng



Mô hình OSI

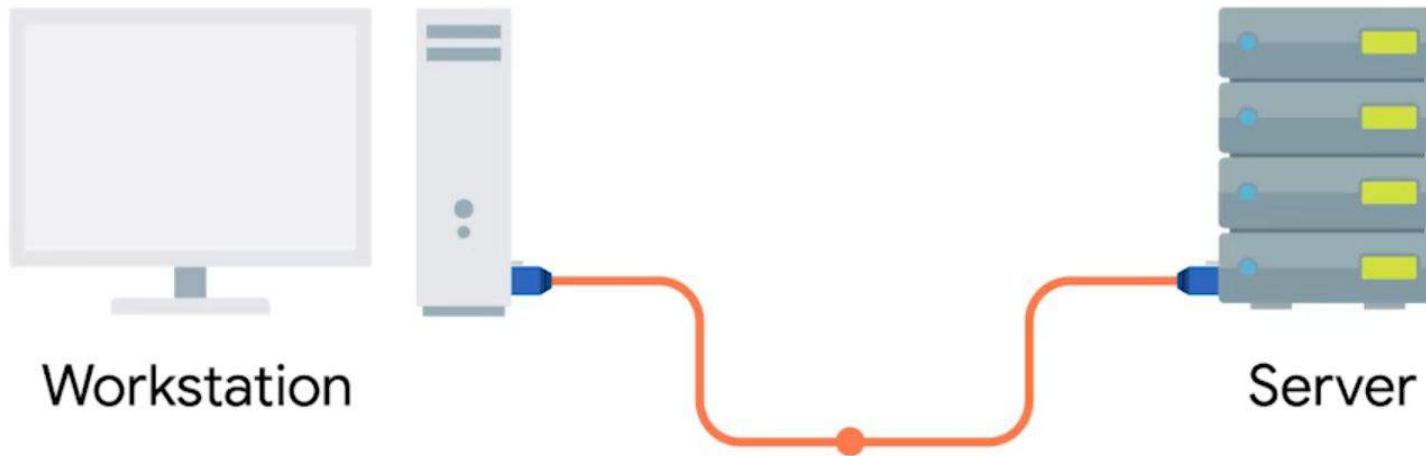
Mô hình OSI là mô hình
thông dụng, gồm 7 tầng



Tổng quan mô hình TCP/IP 5 lớp

Tầng 1: Tầng vật lý

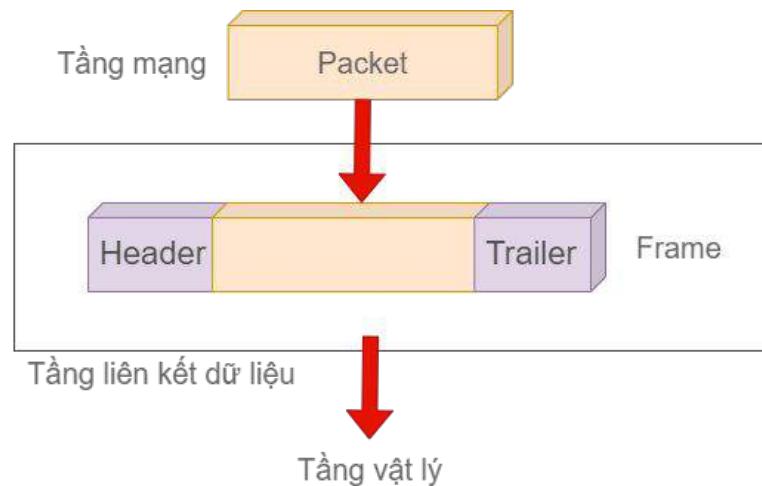
Tầng vật lý (physical layer) thể hiện các đặc trưng, các chuẩn phần cứng sử dụng để kết nối mạng



Tầng 2: Tầng liên kết dữ liệu

Tầng liên kết dữ liệu (data link layer) đảm nhiệm định nghĩa một cách chung để diễn giải các tín hiệu giúp cho các thiết bị mạng có thể giao tiếp với nhau.

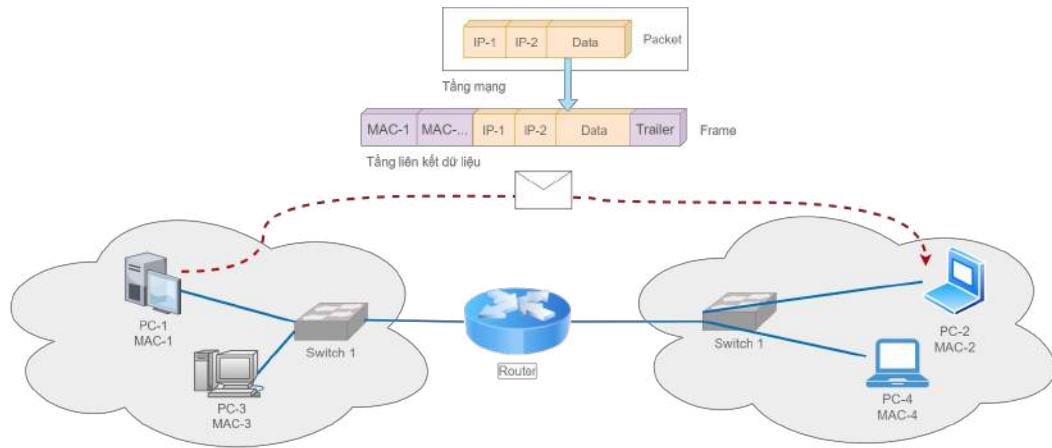
- Thực hiện lấy dữ liệu từ tầng mạng, đóng gói chúng thành các khung tin (frame)
- Mỗi frame có phần tiêu đề (header) chứa địa chỉ MAC, gói dữ liệu, và chuỗi kiểm tra
- Giao thức thường sử dụng là giao thức Ethernet



Tầng 3: Tầng mạng

Tầng mạng (network layer) cũng được xem là tầng Internet (IP layer) để gửi dữ liệu qua nhiều mạng khác nhau thông qua thiết bị định tuyến (router).

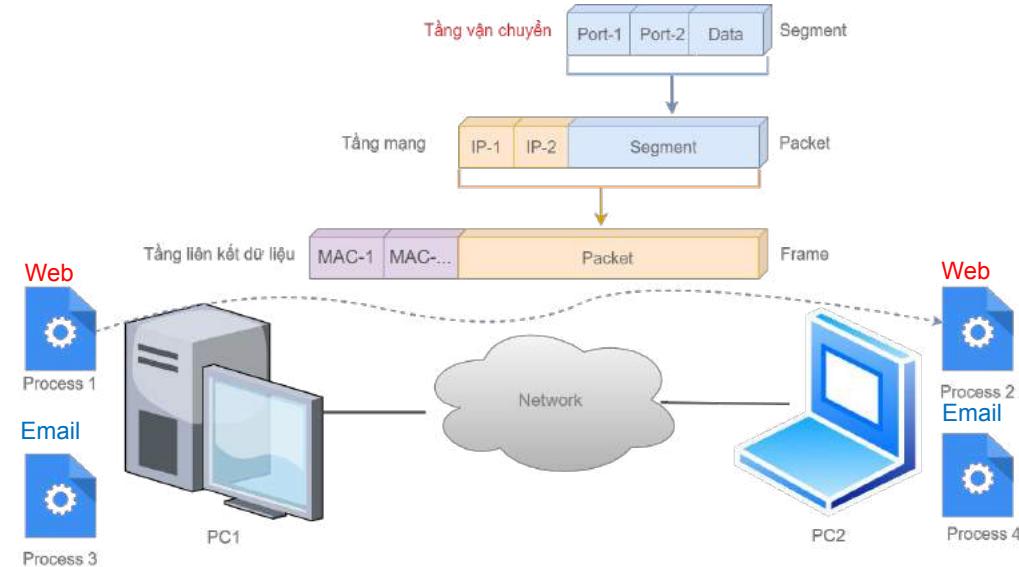
- Liên mạng (internetwork) là một nhóm các mạng khác nhau được kết nối lại.
- Giao thức phổ biến là IP (Internet Protocol)



Tầng 4: Tầng vận chuyển

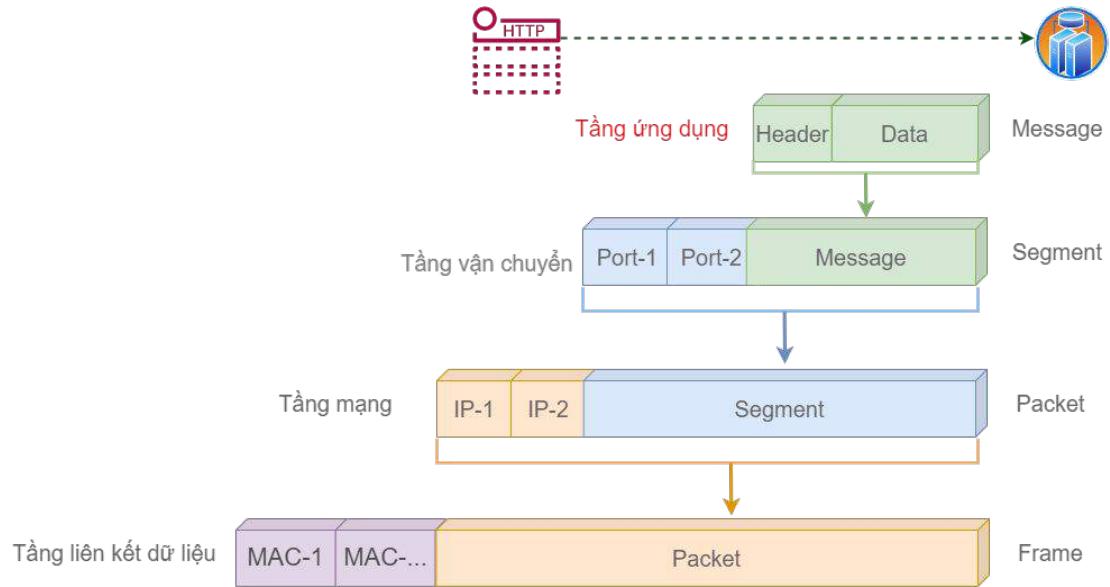
Tầng vận chuyển (transport layer) chuyển dữ liệu từ một tiến trình trên máy nguồn đến đúng một tiến trình trên máy đích.

- Nó sắp xếp các chương trình trên máy đích và máy nguồn sẽ nhận dữ liệu tương ứng.
- Giao thức phổ biến là **TCP** (Transmission Control Protocol) và **UDP** (User Datagram Protocol).



Tầng 5: Tầng ứng dụng

- Tầng ứng dụng (application layer) xác định cách dữ liệu được định dạng, mã hóa, giao tiếp, v.v., và được thống nhất giữa các ứng dụng.
- Rất nhiều giao thức khác nhau: HTTP, FTP, SMTP, POP, DNS, DHCP, v.v..



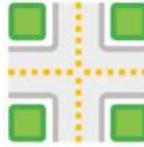
Ví dụ liên hệ TCP/IP

Có thể hình dung 5 tầng TCP/IP giống giao hàng trong thực tế:

- Tầng vật lý giống phương tiện vận chuyển và đường xá.
- Tầng liên kết dữ liệu giống như xác định hướng rẽ ở mỗi giao lộ để đến giao lộ khác
- Tầng mạng giống như lộ trình, đường đi từ nhà kho tới nhà khách hàng
- Tầng vận chuyển giống như xác định giao người nào trong nhà đó
- Tầng ứng dụng giống như quy trình mở gói hàng, sử dụng và xác nhận đơn đã giao



Physical



Data Link



Network



Transport



Application

NỘI DUNG



Mạng máy tính và các thuật ngữ cơ bản



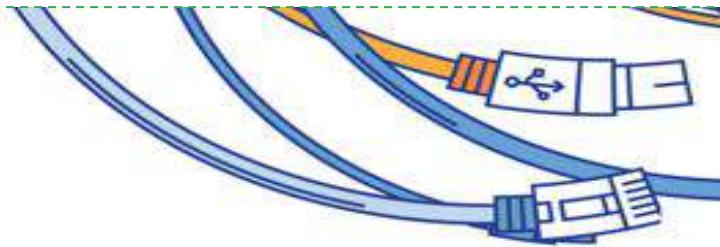
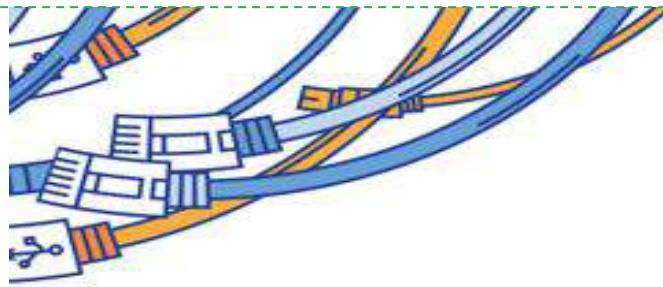
Mô hình mạng



Thiết bị mạng

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



Các loại cáp mạng

Cáp mạng được phân chia làm hai loại chính

Cáp đồng
(cáp xoắn đôi)



Copper cable

Cáp quang



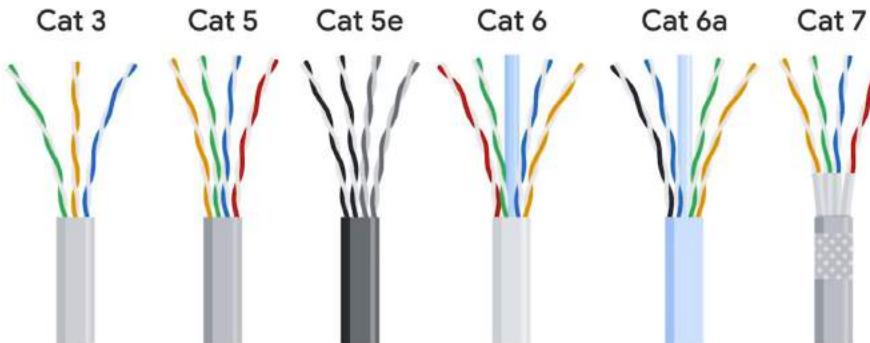
Fiber optic

Cáp đồng xoắn đôi

Cáp đồng xoắn đôi có nhiều phiên bản: Cat 3, Cat 5, Cat 5e, Cat 6, v.v.

- Các phiên bản sau cải thiện tốc độ và khắc phục hiện tượng nhiễu xuyên âm (crosstalk)

Nhiễu xuyên âm (crosstalk) là hiện tượng **xung điện ở sợi dây này tạo ra hiệu ứng không mong muốn ở sợi khác**.



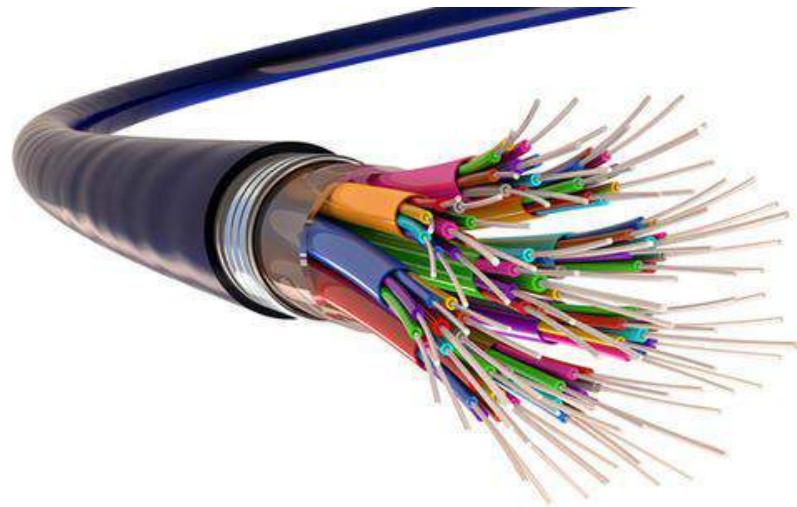
Sợi quang

Sợi quang dùng ánh sáng để truyền tín hiệu nên:

- Tốc độ nhanh hơn
- Không bị nhiễu điện từ
- Truyền nhận ở khoảng cách xa ít bị mất dữ liệu so với cáp đồng

Nhưng:

- Chi phí đắt hơn
- Dễ đứt gãy
- Khó đấu nối hơn



Hub

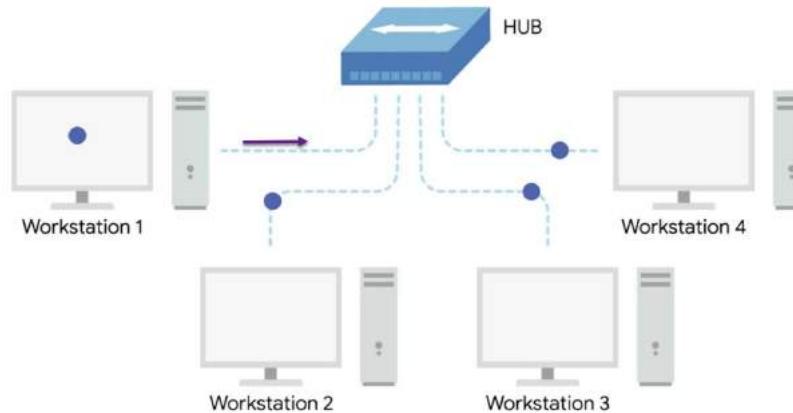
Bộ chia mạng (hub) là thiết bị dùng để nối nhiều máy tính lại với nhau



Hub

Đặc điểm của Hub:

- Khi một máy tính gửi tín hiệu, tất cả các máy cắm chung hub đều nhận được tín hiệu.
- Máy tính nhận hoặc xử lý nó, hoặc bỏ qua nó.

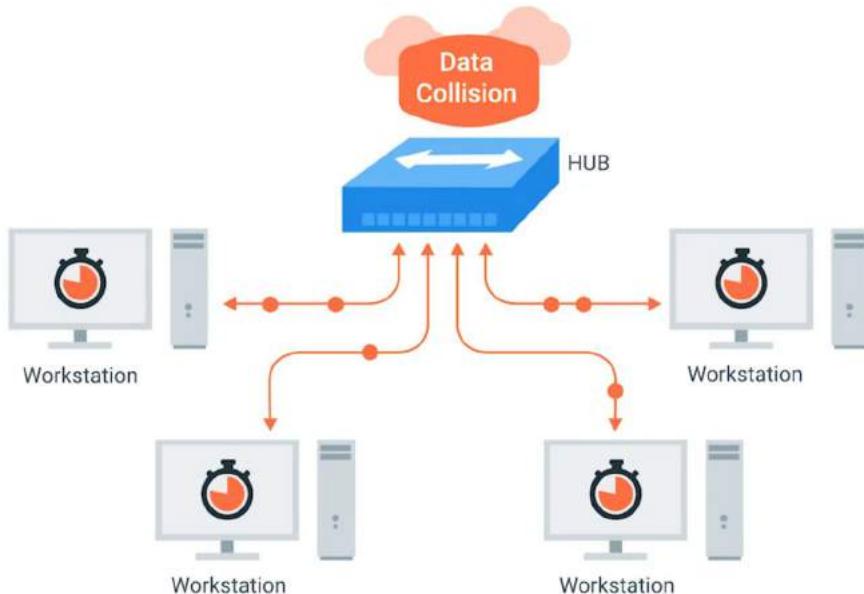


Hub

Kết nối mạng trong Hub thường bị vấn đề đụng độ (collision)

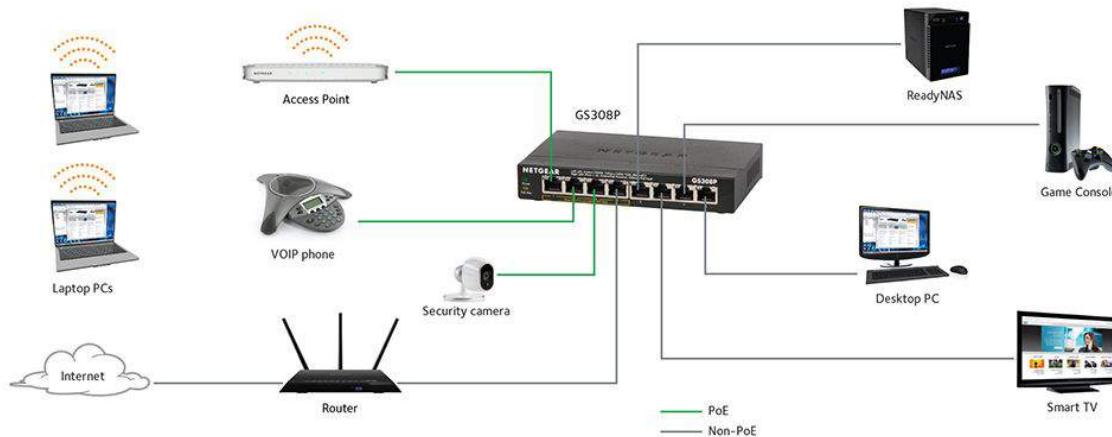
Miền đụng độ (collision domain) là một mạng máy tính chỉ cho phép một thiết bị giao tiếp ở một thời điểm.

- Nếu nhiều thiết bị gửi tín hiệu cùng lúc, đường truyền sẽ bị nhiễu.
- Các máy phải đợi một khoảng thời gian để gửi lại.



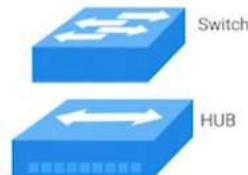
Switch

- **Bộ chuyển mạch** (switch) là thiết bị dùng để kết nối nhiều thiết bị với nhau.
- Khác với hub là switch **nhận tín hiệu từ một thiết bị, kiểm tra địa chỉ và gửi dữ liệu về chỉ nơi liên quan**.
- Switch ghi nhớ thiết bị nào được cắm đến nó.



Tầng hoạt động của Hub và Switch

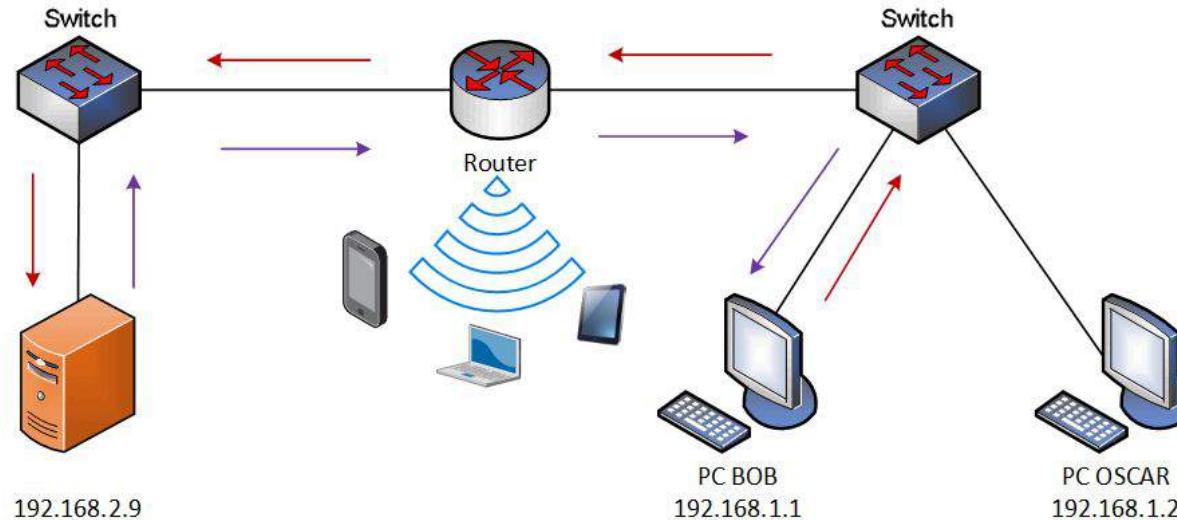
- Hub hoạt động ở **tầng vật lý**.
- Switch hoạt động ở **tầng liên kết dữ liệu**.
- Phù hợp với mạng đơn, LAN
- Hub và Switch không phù hợp để nối nhiều mạng với nhau



#	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

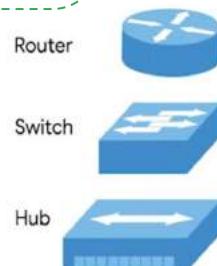
Router

Bộ định tuyến (router) là thiết bị chuyển tiếp dữ liệu giữa các mạng khác nhau



Router

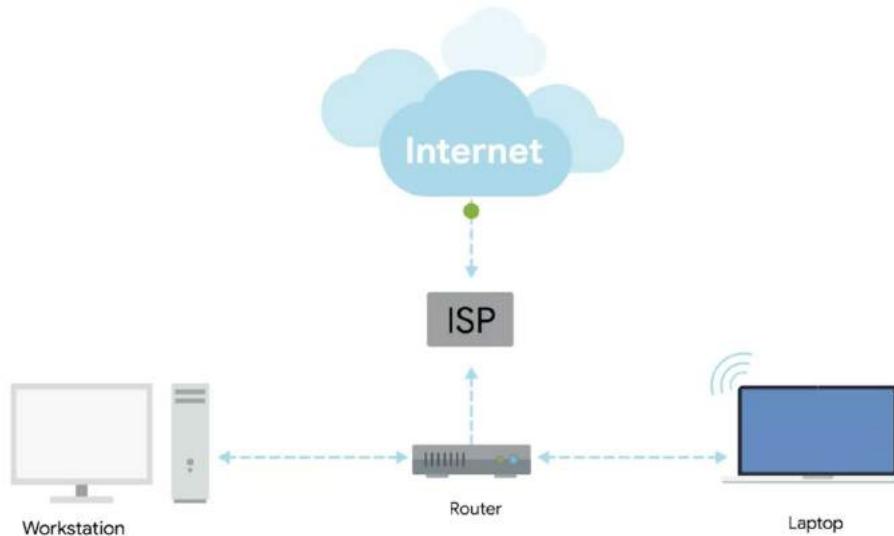
- Router **hoạt động ở tầng 3** trong mô hình TCP/IP.
- Router **lưu trữ một bảng định tuyến** (route table) chứa thông tin để định hướng đường đi gói tin giữa các mạng.



#	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, Wifi	Frames	MAC address
1	Physical	10 Base T, 802.11	Bits	n/a

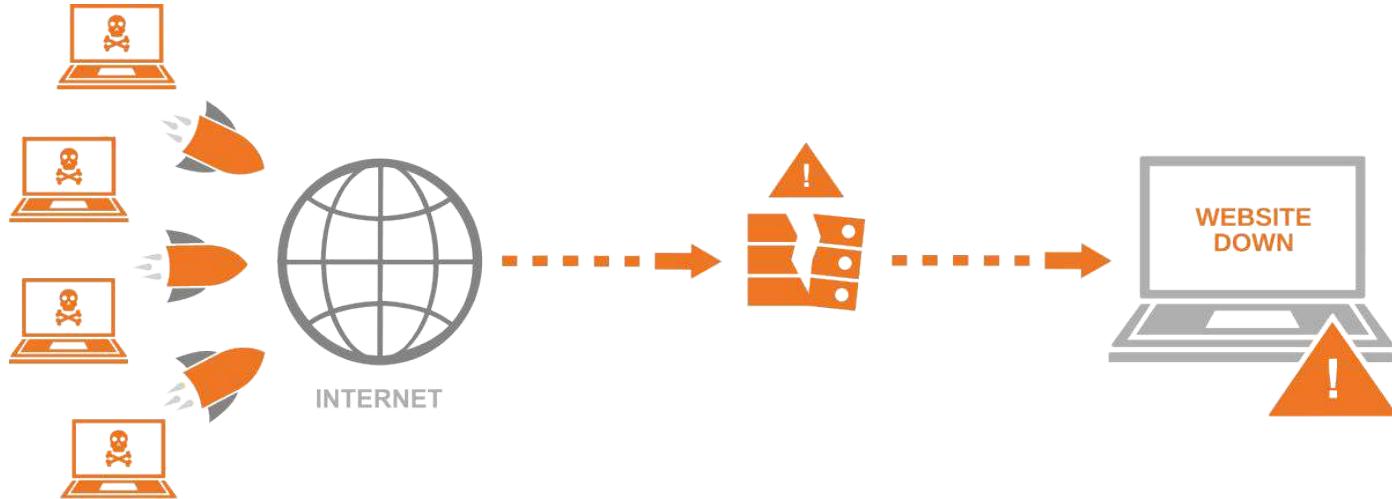
Router

Router thường được sử dụng để kết nối đến mạng Internet thông qua nhà cung cấp dịch vụ internet (ISP – Internet Service Protocol)



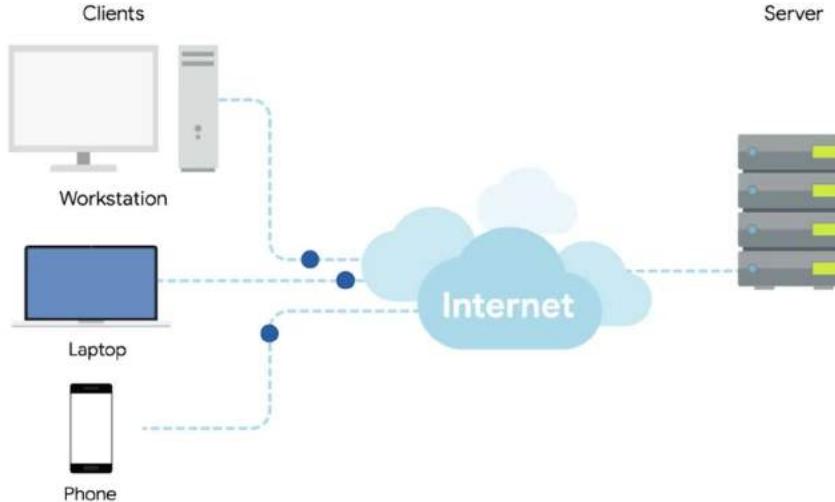
Router

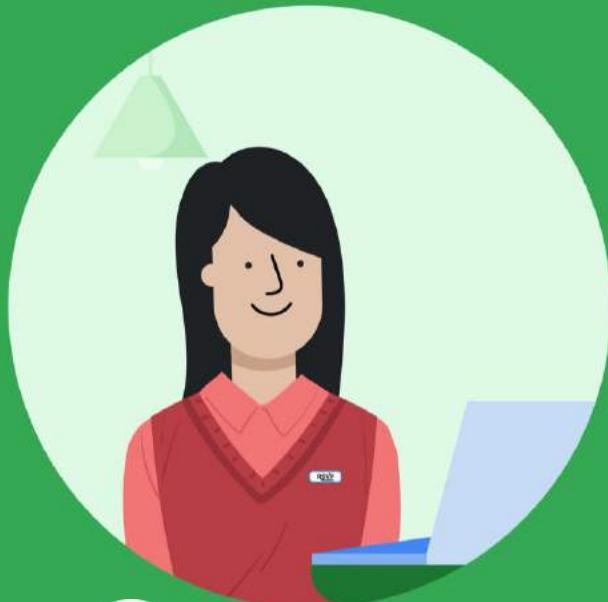
BGP (border gateway protocol) là giao thức giúp xác định đường đi tối ưu nhất để chuyển tiếp gói tin qua nhiều router trên khắp thế giới



Máy chủ và máy khách

Máy chủ (server) là hệ thống máy tính và phần mềm mà cung cấp chức năng hoặc dữ liệu cho các thiết bị, được gọi là máy khách (client).



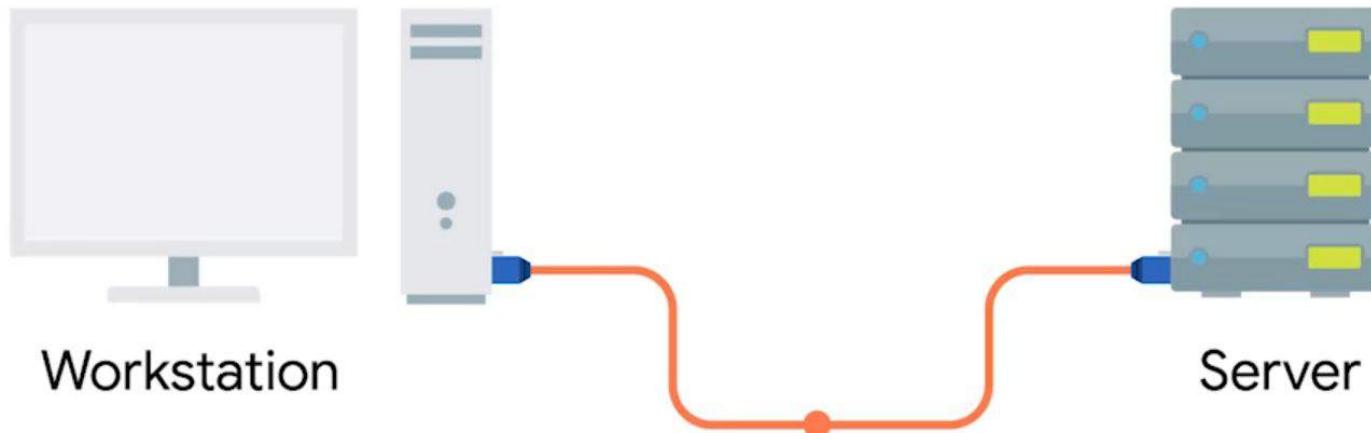


2 TẦNG VẬT LÝ



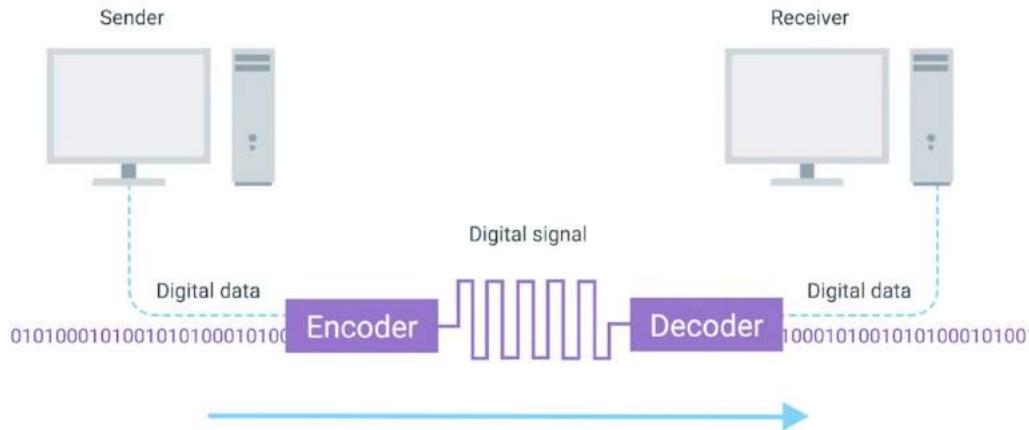
Tầng 1: Tầng vật lý

Tầng vật lý (physical layer) thể hiện **các đặc trưng, các chuẩn phần cứng** sử dụng để kết nối mạng



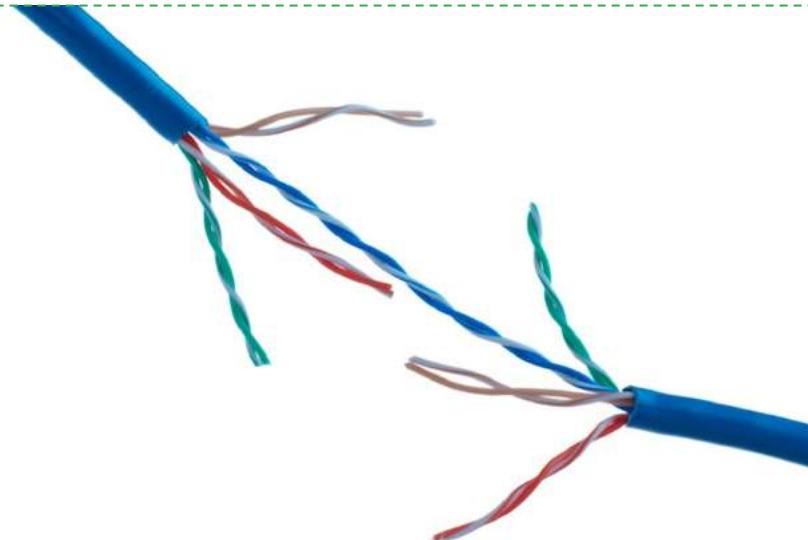
Nhiệm vụ tầng vật lý

- Tầng vật lý di chuyển các bit 1, 0 từ một đầu đến một đầu tiếp theo.
- Để **truyền tín hiệu 1, 0** trên dây cáp, ta cần **thực hiện một tiến trình điều chế** (modulation) được gọi là **mã hóa đường truyền** (line coding).



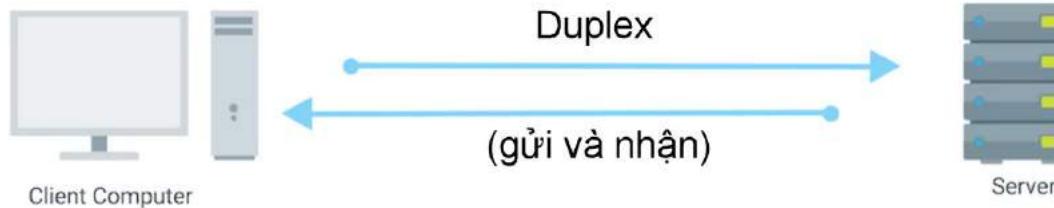
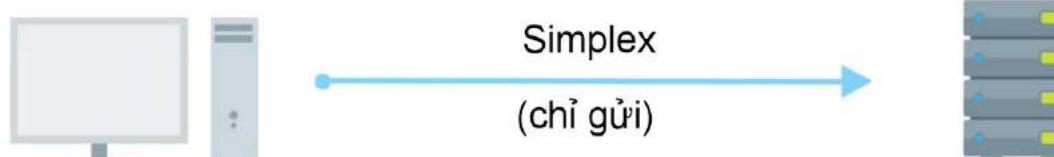
Cáp xoắn đôi

- Cáp xoắn đôi là các cặp dây điện xoắn vào nhau để chống lại nhiễu điện từ và nhiễu xuyên âm.
- Cáp Cat6 gồm 8 dây được xoắn thành 4 cặp.



Giao tiếp đơn công và song công

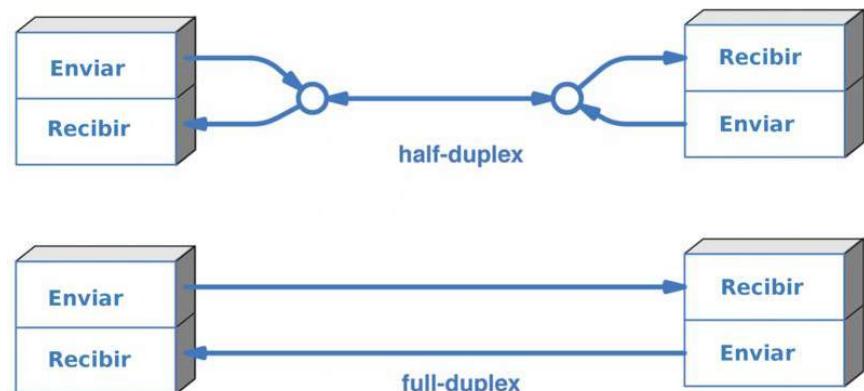
- Giao tiếp đơn công (simplex communication) là thông tin di chuyển chỉ một hướng.
- Giao tiếp song công (duplex communication) là thông tin di chuyển ở cả hai hướng.



Các loại giao tiếp song công

Giao tiếp song công được chia thành 2 loại con:

- Giao tiếp bán song công (half-duplex): trong một thời điểm, tín hiệu chỉ có thể chạy theo một hướng.
- Giao tiếp song công toàn phần (full-duplex): tín hiệu có thể đồng thời chạy theo cả hai hướng.



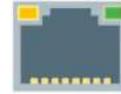
Nguồn: Wikimedia

Đầu cắm và cổng cắm

Đầu cắm (plug) và cổng cắm (port) dùng để nối dây mạng đến thiết bị mạng.

- Chuẩn phổ biến là **RJ45** (Registered Jack 45).

RJ45 port



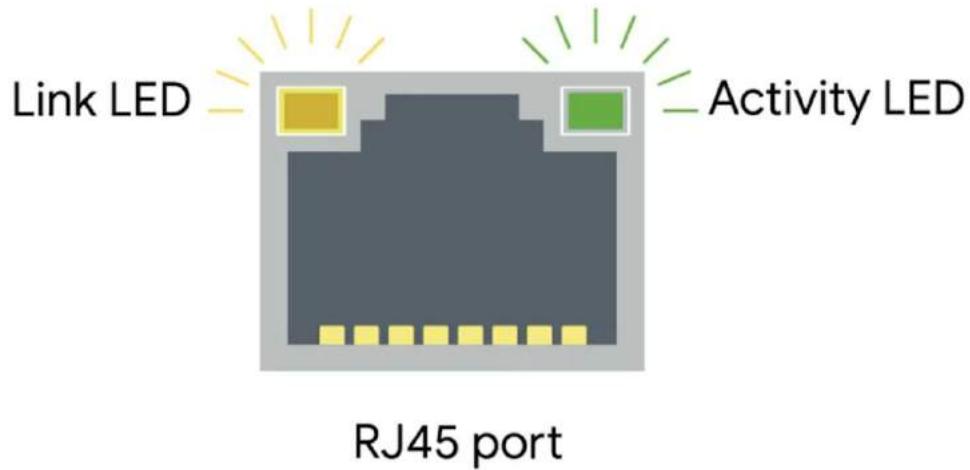
RJ45 plug



Tín hiệu kết nối

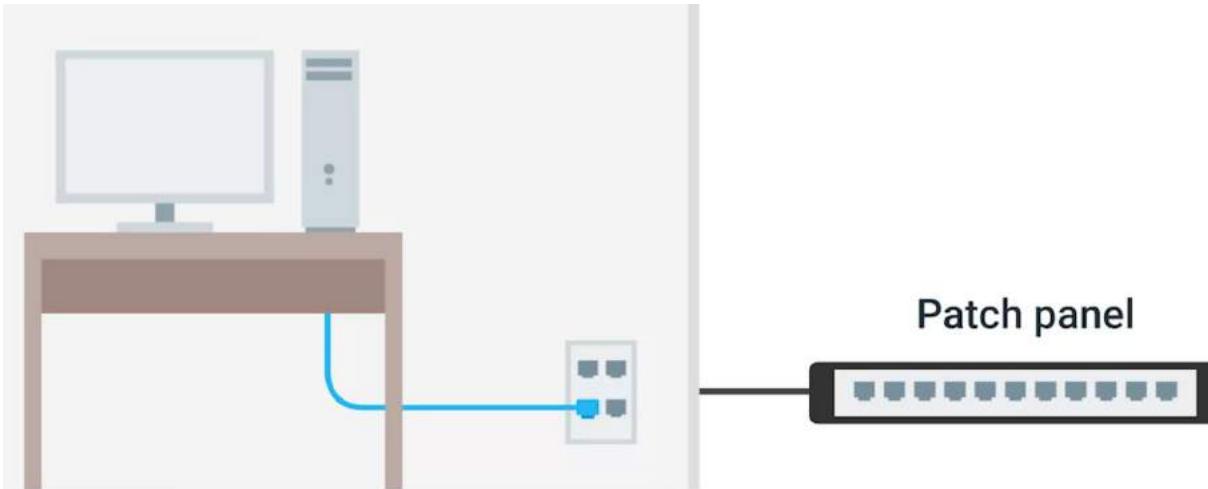
Trên cổng cắm thường trang bị **2 đèn led nhỏ**.

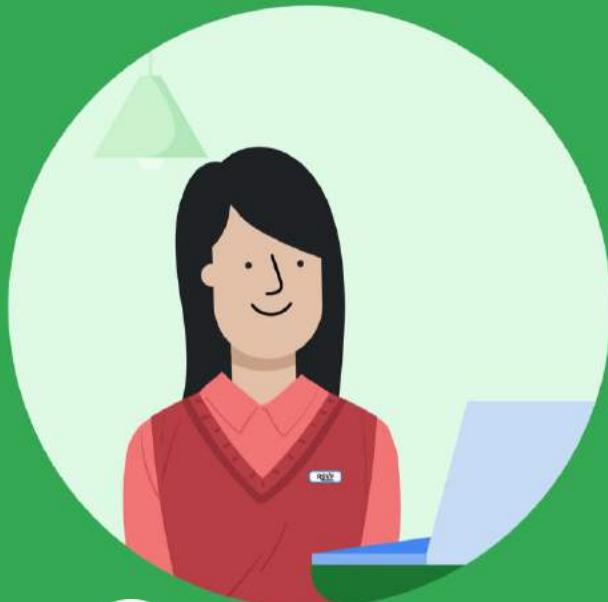
- Một đèn là **đèn liên kết** (link led): báo hiệu **cáp** được kết nối đúng cách.
- Một đèn là **đèn hoạt động** (activity led): báo hiệu **dữ liệu** đang truyền nhận.



Bảng cắm

Bảng cắm (patch panel) là thiết bị chứa rất nhiều cổng mạng được dùng để quản lý đầu nối tập trung dây mạng cho gọn.



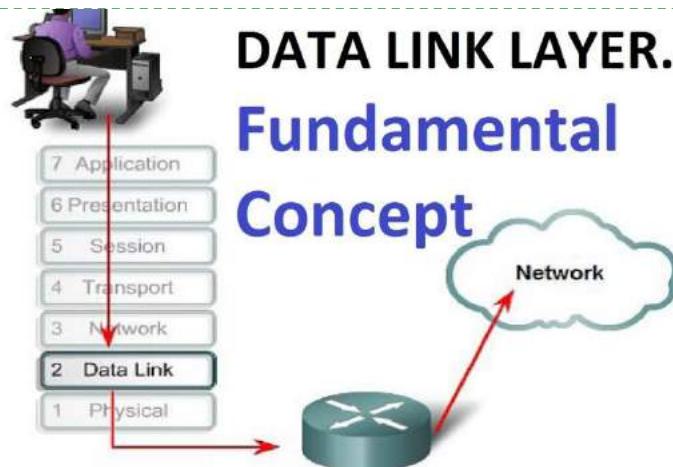


3 TĂNG LIÊN KẾT DỮ LIỆU



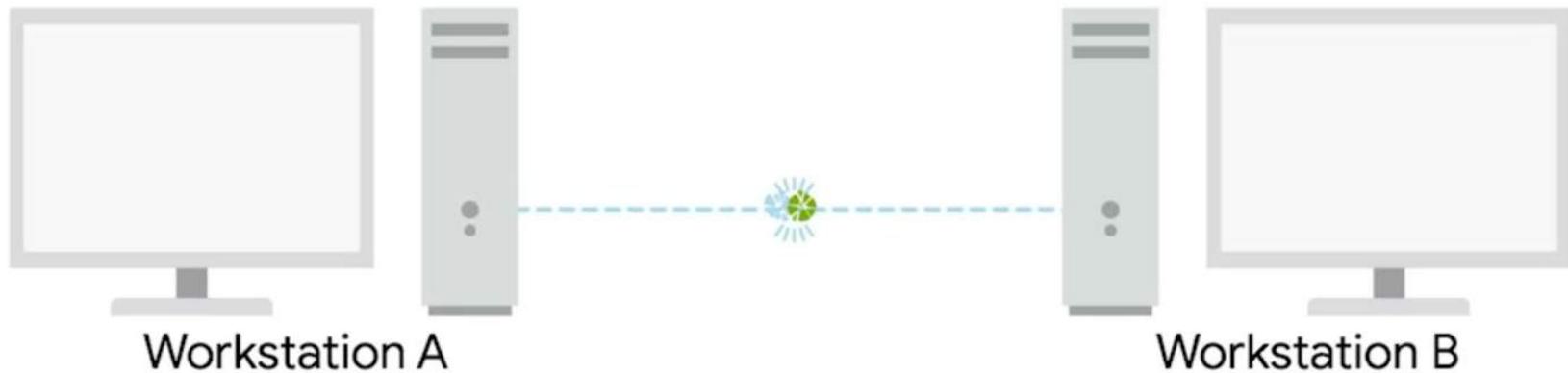
Tầng 2: Tầng liên kết dữ liệu

- Tầng liên kết dữ liệu (data link layer) sử dụng các dịch vụ ở tầng vật lý để **gửi** và nhận các gói dữ liệu (packet) qua các kênh giao tiếp một cách thành công.
- Giao thức thường sử dụng là **giao thức Ethernet**



Đụng độ tín hiệu

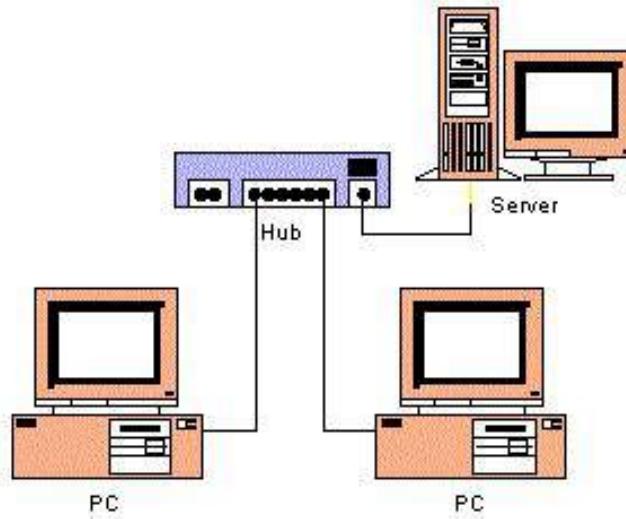
Khi có nhiều thiết bị cùng lúc gửi tín hiệu, hiện tượng đụng độ (collision) xảy ra



Ethernet và kỹ thuật CSMA/CD

Giao thức Ethernet sử dụng **kỹ thuật CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) để xử lý đụng độ.

- Khi xảy ra đụng độ, các máy tính phát hiện đụng độ và dừng quá trình truyền.
Mỗi thiết bị đợi một khoảng thời gian ngẫu nhiên, sau đó gửi lại.



Địa chỉ MAC

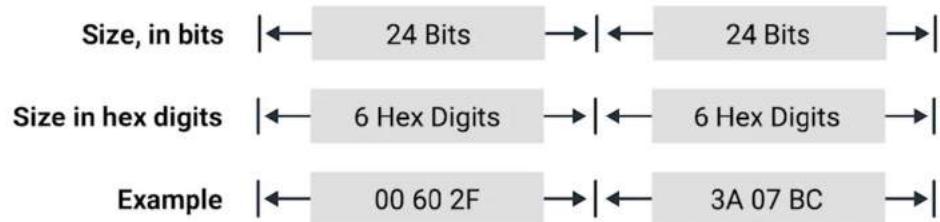
- Để biết gói tin được truyền từ thiết bị nào và cho thiết bị nào trong mạng, tầng liên kết dữ liệu sử dụng **địa chỉ MAC** (Media Access Control).
- Địa chỉ MAC là **định danh duy nhất toàn cầu** được nhà sản xuất gán cho một card mạng.



Địa chỉ MAC

Địa chỉ MAC là một **con số 48 bit** được chia thành 6 nhóm.

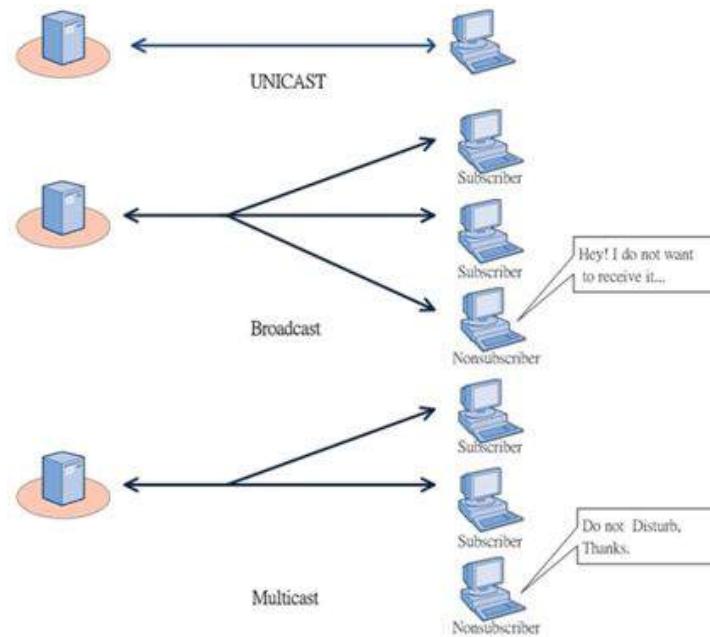
- Mỗi nhóm là 8 bit được thể hiện dưới dạng **số hệ 16** (hexa number)
➤ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A (=10), B (=11), C (=12), D (=13), E (=14), F (=15)
- 3 nhóm đầu là **mã định danh** đơn nhất của nhà sản xuất, 3 nhóm sau được **gán tùy ý** bởi nhà sản xuất miễn khæk biệt nhau.



Cơ chế định tuyến

Giao thức Ethernet hỗ trợ 3 cơ chế định tuyến dữ liệu:

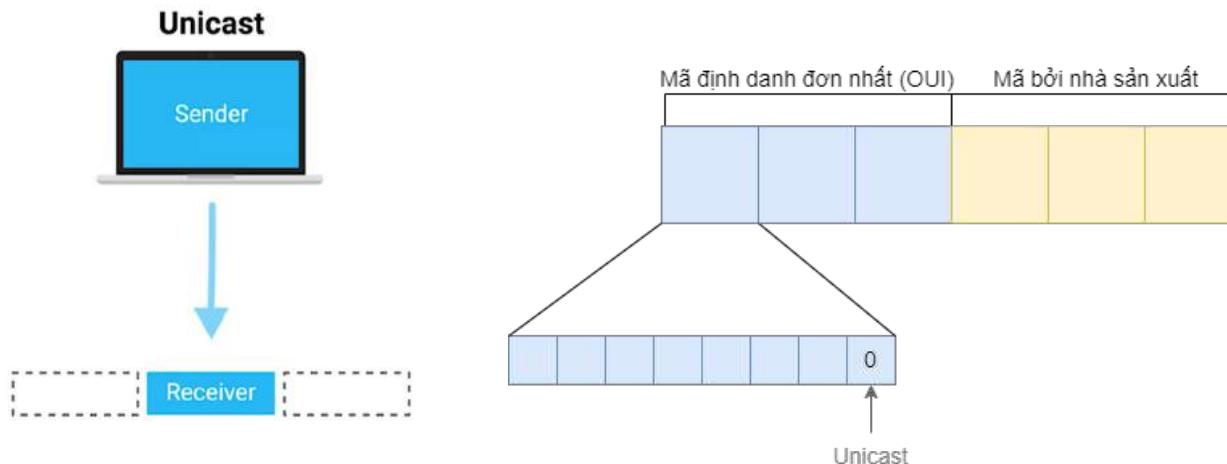
- Cơ chế Unicast
- Cơ chế Multicast
- Cơ chế Broadcast



Cơ chế Unicast

Unicast là cơ chế truyền **một-một** (một người gửi, một người nhận)

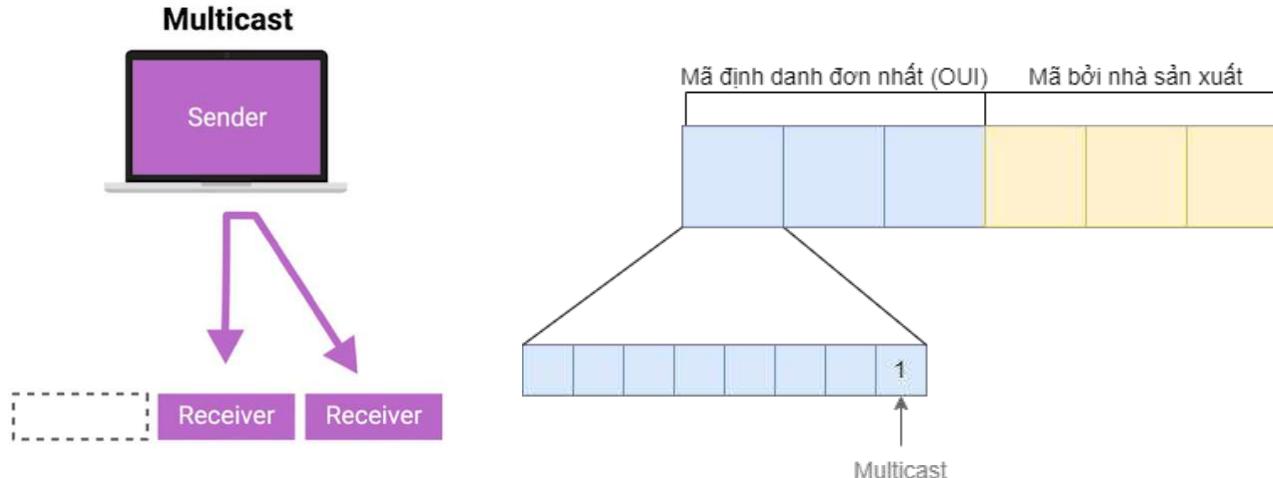
- Bit có ý nghĩa thấp nhất (LSB) của **bộ ba số đầu tiên** trên địa chỉ máy nhận được thiết lập đến 0.



Cơ chế Multicast

Multicast là cơ chế truyền **một-nhiều** (một người gửi, nhiều người nhận)

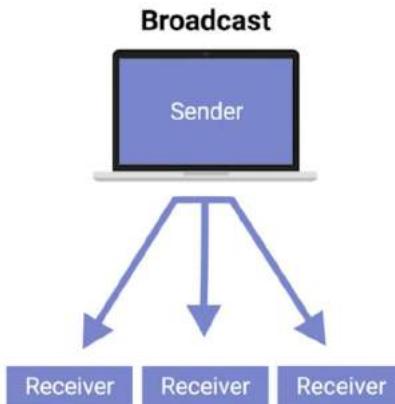
- Bit có ý nghĩa thấp nhất (LSB) của **số đầu tiên** trên địa chỉ máy nhận được thiết lập đến 1.



Cơ chế Broadcast

Broadcast là cơ chế truyền **một-tất cả** (một người gửi, mọi người đều nhận)

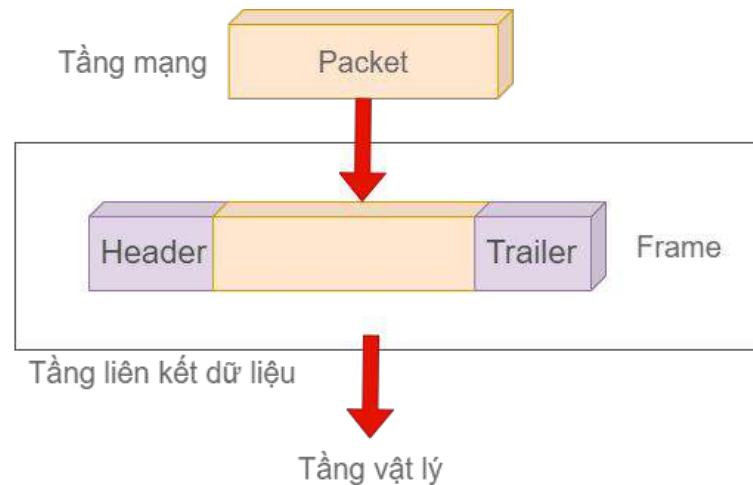
- Đại chỉ của máy nhận tất cả đều là F (FF:FF:FF:FF:FF:FF).



Mã định danh đơn nhất (OUI)	Mã bởi nhà sản xuất
FF FF FF	FF FF FF

Khung Ethernet

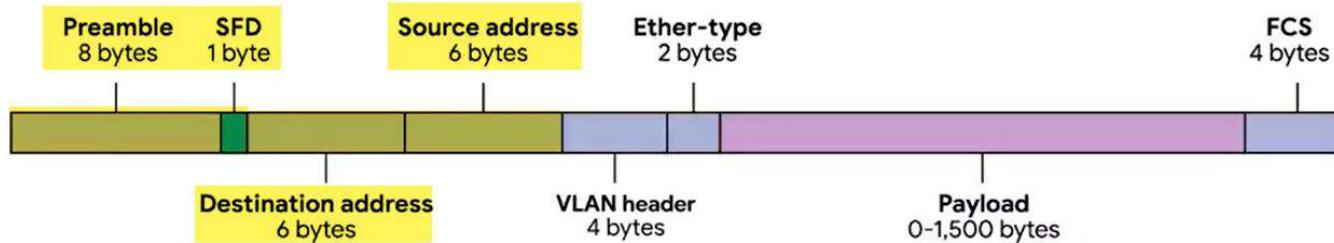
Khung Ethernet (Ethernet frame) là một gói dữ liệu chứa các thông tin cần thiết trong giao thức Ethernet.



Cấu trúc khung Ethernet

Khung Ethernet gồm:

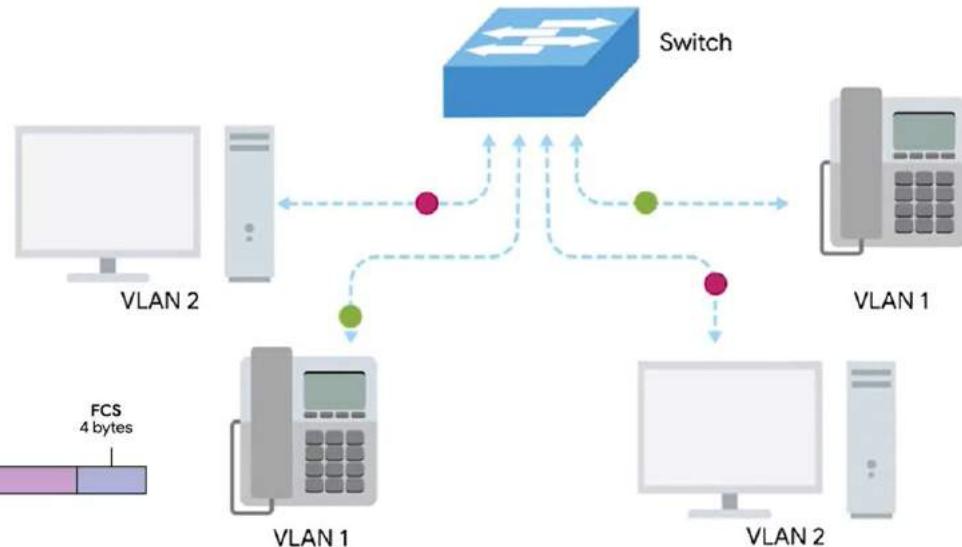
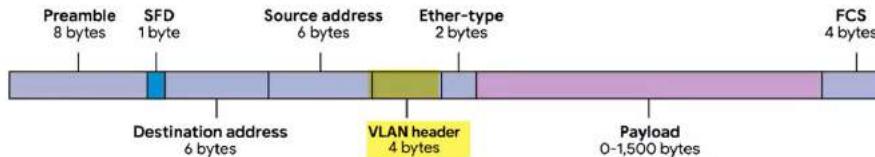
- Phần đầu gọi là Preamble: gồm 8 byte
- 7 byte đầu là vùng đệm giữa các khung và có thể sử dụng để đồng bộ đồng hồ và điều hòa tốc độ gửi dữ liệu.
- 1 byte còn lại là dấu hiệu phân cách điểm bắt đầu khung.
- Hai phần tiếp theo là địa chỉ MAC của máy đích và máy nguồn: 6 byte/địa chỉ



Cấu trúc khung Ethernet

Khung Ethernet gồm:

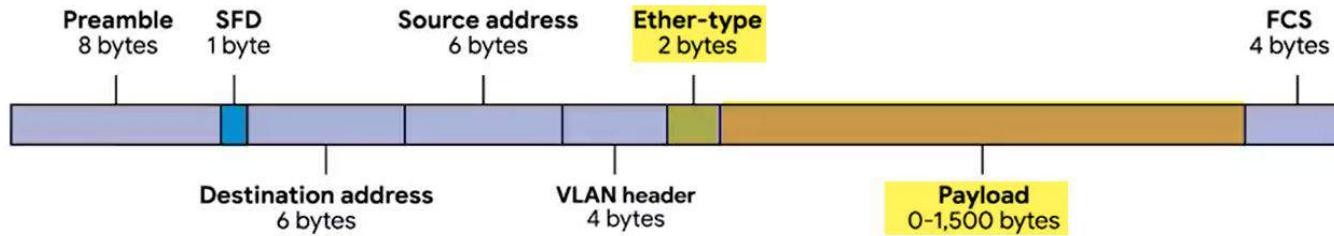
-
- Phần **VLAN** (Virtual LAN – mạng LAN ảo) cho phép nhiều mạng LAN logic thực thi trên cùng thiết bị mạng



Cấu trúc khung Ethernet

Khung Ethernet gồm:

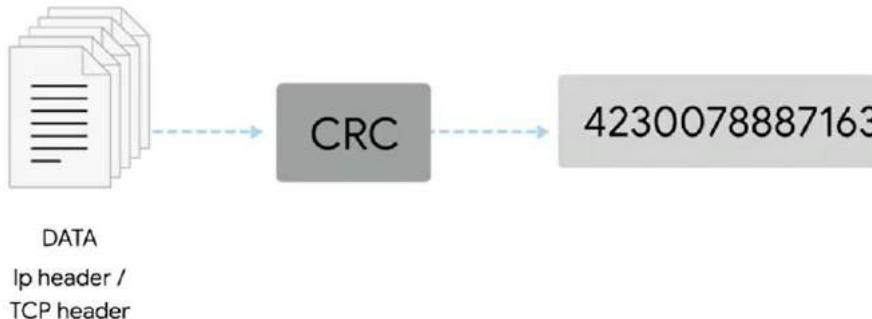
-
- Phần EtherType mô tả loại Ethernet
- **Phần Payload** là dữ liệu thực sự cần truyền, nó chứa dữ liệu của tất cả các tầng phía trên như tầng IP (tầng mạng), tầng vận chuyển, tầng ứng dụng

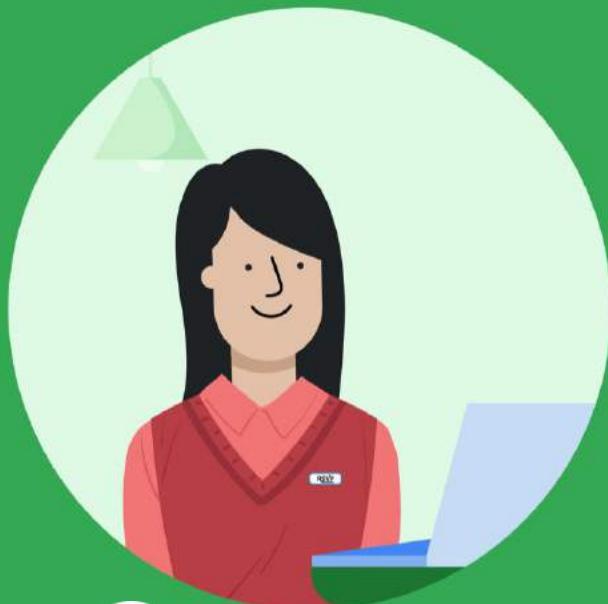


Cấu trúc khung Ethernet

Khung Ethernet gồm:

-
- Cuối cùng là **chuỗi kiểm tra khung** (Frame Check Sequence): chứa giá trị tổng kiểm (checksum) được tính toán bởi quá trình **kiểm dư chu trình** (CRC).
- Quá trình CRC thực hiện phép tính toán học được sử dụng để đảm bảo tất cả dữ liệu đến đều nguyên vẹn.





4 TẦNG MẠNG



NỘI DUNG



Tầng mạng



Phân lớp địa chỉ IP



Mạng con

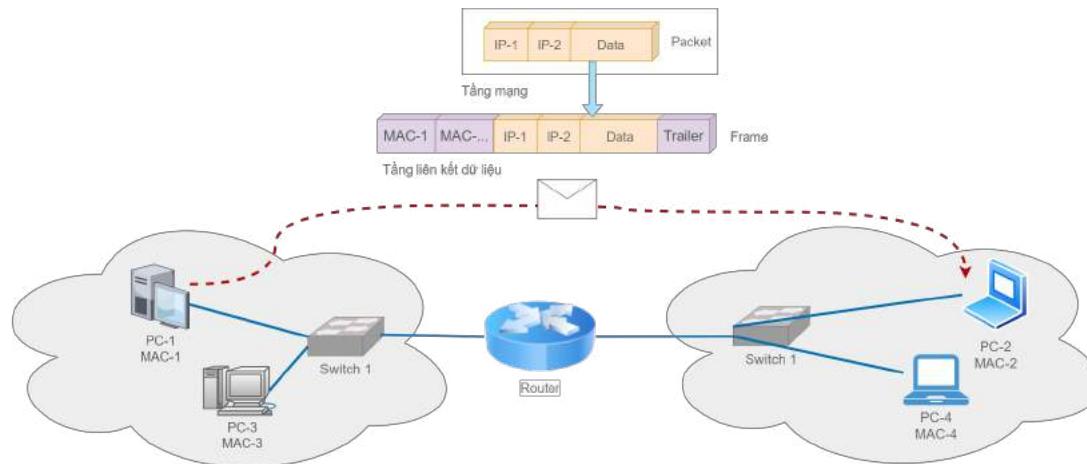


Định tuyến

Tầng 3: Tầng mạng

Tầng mạng (network layer) cũng được xem là tầng Internet (IP layer) để gửi dữ liệu qua nhiều mạng khác nhau thông qua thiết bị định tuyến (router).

- Giao thức phổ biến là IP (Internet Protocol)



Địa chỉ IP

Địa chỉ IP là số gồm **4 octet** với mỗi octet được thể hiện bằng một con số thập phân có giá trị từ 0 đến 255.

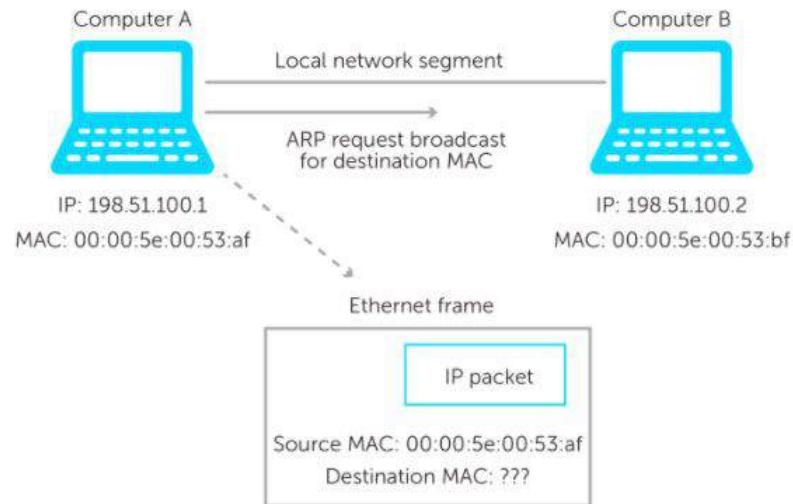
- Mỗi octet là nhóm 8 bit (có thể xem là 1 byte)

12.34.56.78

00001100.00100010.00111000.01001110

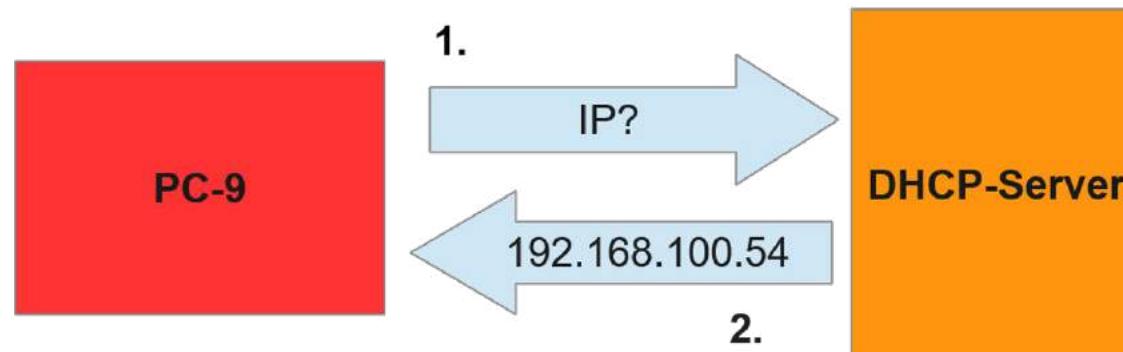
Địa chỉ IP và Địa chỉ MAC

- Địa chỉ IP là địa chỉ của máy khi tham gia mạng, và **thay đổi khi tham gia các mạng khác nhau**.
- Địa chỉ MAC là địa chỉ được gắn **độc nhất** cho máy và **không thay đổi** trong bất kỳ mạng nào.
- Địa chỉ IP hỗ trợ cho quá trình định tuyến (đường chuyển gói tin) dễ dàng hơn so với địa chỉ MAC do cách thức phân tầng quản lý.



Thiết lập địa chỉ IP

- Địa chỉ IP có thể được thiết lập thủ công hoặc tự động.
- Khi cắm vào thiết bị mạng như router, máy tính **được gán địa chỉ IP động** thông qua công nghệ DHCP (Dynamic Host Configuration Protocol).

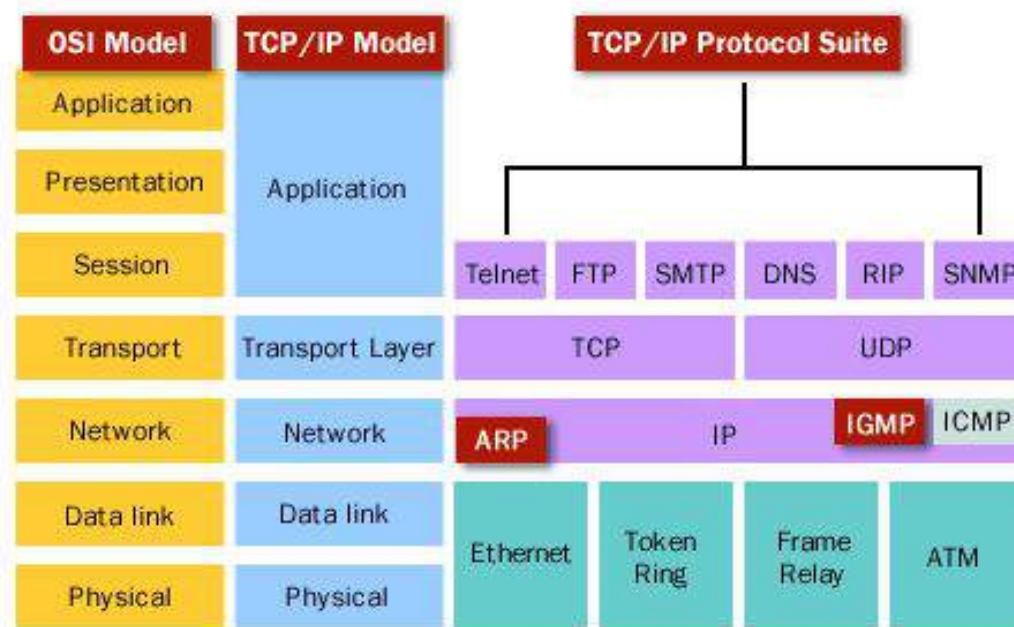


Gói tin IP diagram

IP diagram là gói dữ liệu
được hình thành trong tầng
mạng.

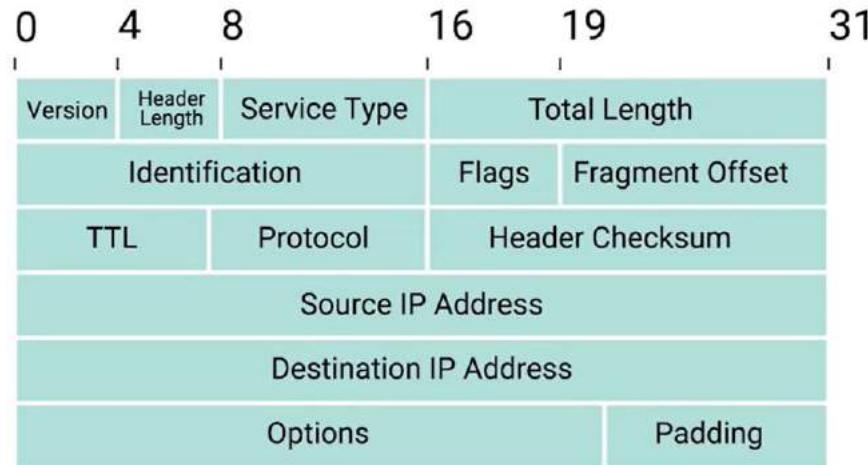
Bao gồm 2 phần chính:

- Phần Header
- Phần dữ liệu



Gói tin IP diagram

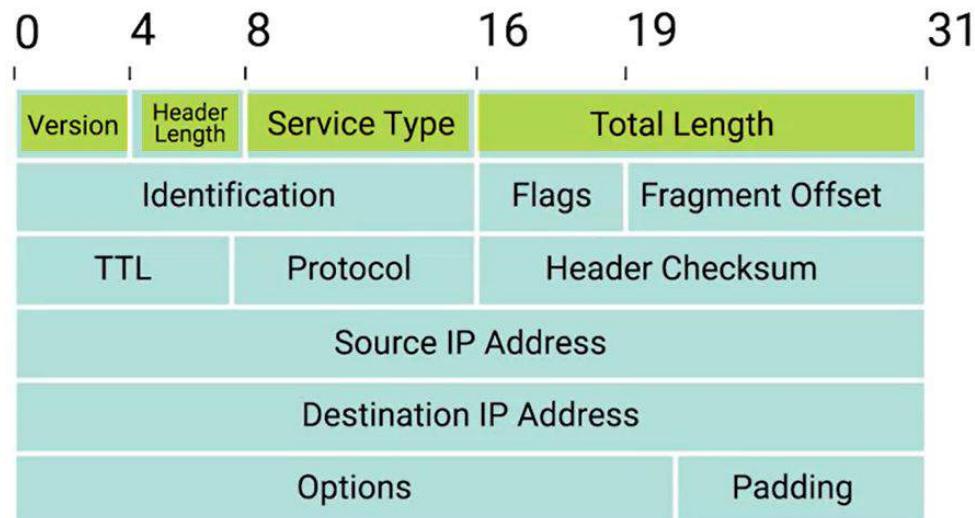
Phần header của IP diagram chứa nhiều thành phần



Gói tin IP diagram

Phần header của IP diagram gồm:

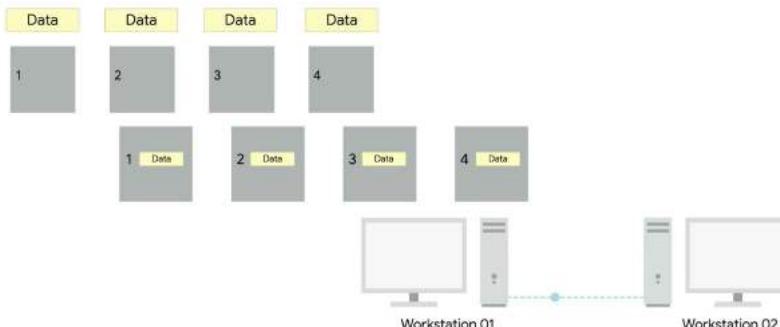
- **Version**: phiên bản IP (v4 hoặc v6)
- **Header length**: chiều dài header
- **Service type**: loại chất lượng dịch vụ
- **Total length**: độ dài của IP diagram



Gói tin IP diagram

Phần header của IP diagram gồm:

- ...
 - Identification**: các IP diagram thuộc về cùng 1 gói dữ liệu nếu có cùng mã ID
 - Flags**: có hay không dữ liệu bị tách ra thành nhiều gói dữ liệu
 - Fragment offset**: số thứ tự của fragment
- Quá trình chia nhỏ gói tin diagram được gọi là **fragmentation**.

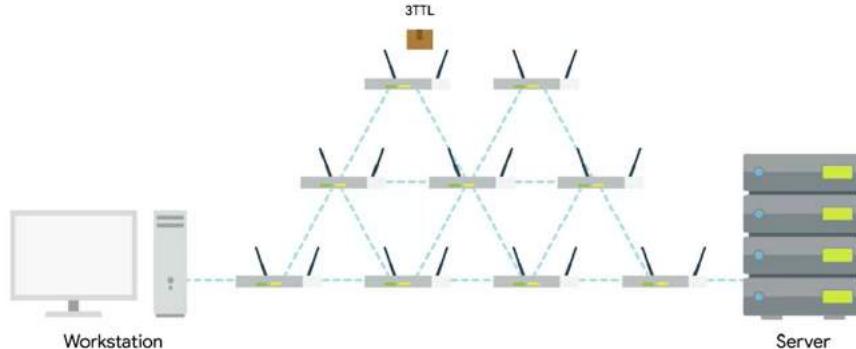


0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification		Flags	Fragment Offset		
TTL	Protocol	Header Checksum			
Source IP Address					
Destination IP Address					
Options		Padding			

Gói tin IP diagram

Phần header của IP diagram gồm:

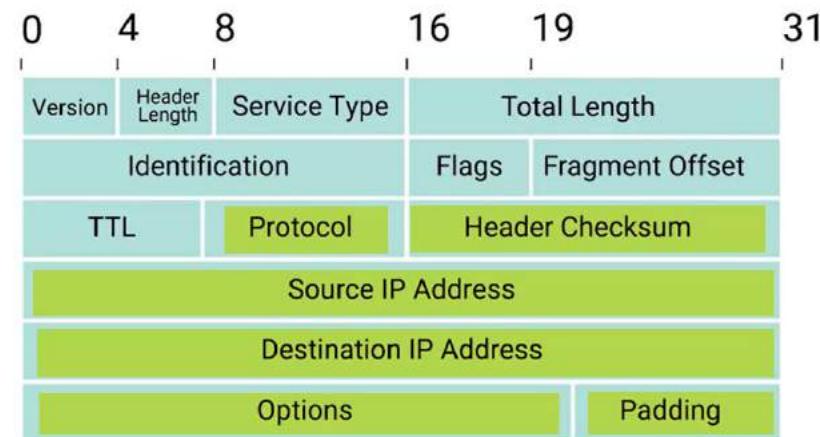
- ...
- TTL (time to live): thời gian sống



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		

Gói tin IP diagram

- **Source IP Address, Destination IP Address:** địa chỉ IP của máy nguồn và máy đích
- **Options:** thiết lập các đặc trưng đặc biệt để sử dụng cho mục đích kiểm thử, phần này có chiều dài thay đổi
- **Padding:** điền các giá trị thêm chỉ để đảm bảo IP diagram có kích thước cố định
- **Source IP Address, Destination IP Address:** địa chỉ IP của máy nguồn và máy đích
- **Options:** thiết lập các đặc trưng đặc biệt để sử dụng cho mục đích kiểm thử, phần này có chiều dài thay đổi
- **Padding:** điền các giá trị thêm chỉ để đảm bảo IP diagram có kích thước cố định



NỘI DUNG



Tầng mạng



Phân lớp địa chỉ IP



Mạng con

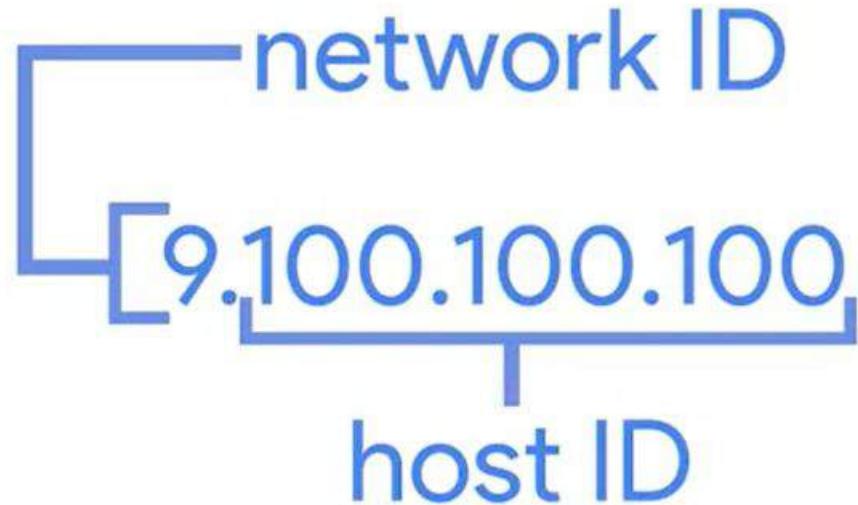


Định tuyến

Phân lớp địa chỉ IP

Địa chỉ IP gồm 2 thành phần:

- **Định danh mạng** (Network Id): xác định phân đoạn mạng
- **Định danh máy** (Host Id): xác định máy kết nối



Phân lớp địa chỉ IP

Để dễ quản lý và định tuyến, địa chỉ IP được phân thành 5 lớp: A, B,C,D,E

Số địa chỉ có thể gán của mỗi lớp:

- Lớp A: $2^{24} = 16.777.216$
- Lớp B: $2^{16} = 65.536$
- Lớp C: $2^8 = 256$

Class A
123.456.780.00
network ID

Class B
123.456.780.00
network ID

Class C
123.456.780.00
network ID

Phân lớp địa chỉ IP

Để xác định một IP thuộc về lớp nào, ta quy ước các bit bên trái nhất của byte đầu tiên:

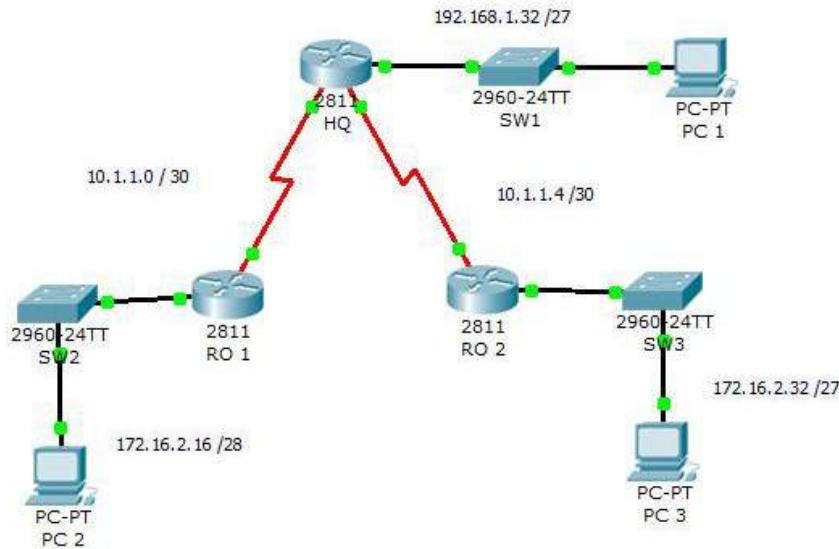
- Nếu bit đầu tiên là 0: lớp A (giá trị byte từ 0 đến 127)
- Nếu 2 bit đầu tiên là 10: lớp B (128-191)
- Nếu 3 bit đầu tiên là 110: lớp C (192-223)
- Nếu 4 bit đầu tiên là 1110: lớp D (224-239)
- Nếu 4 bit đầu tiên là 1111: lớp E (240-255)

Class	Left-most bit	Starting IP address	Last IP address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Hệ thống CIDR

CIDR (Classless Inter Domain Routing) là phương pháp định vị địa chỉ IP thay thế cho cách phân lớp A,B,C.

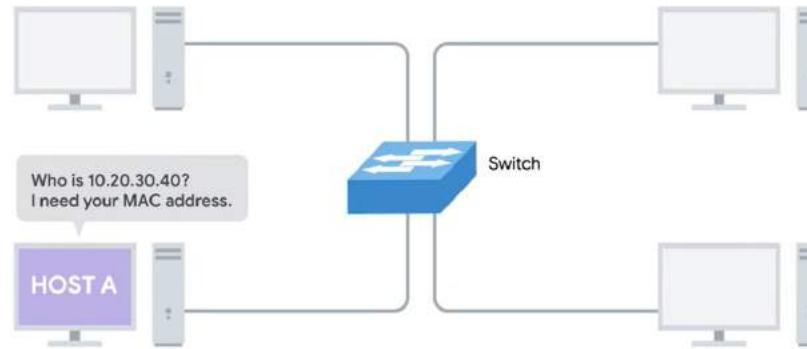
- Giúp làm chậm sự phình lên của bảng định tuyến
- Giúp giảm sự cạn kiệt nhanh chóng của địa chỉ IPv4



Giao thức phân giải địa chỉ

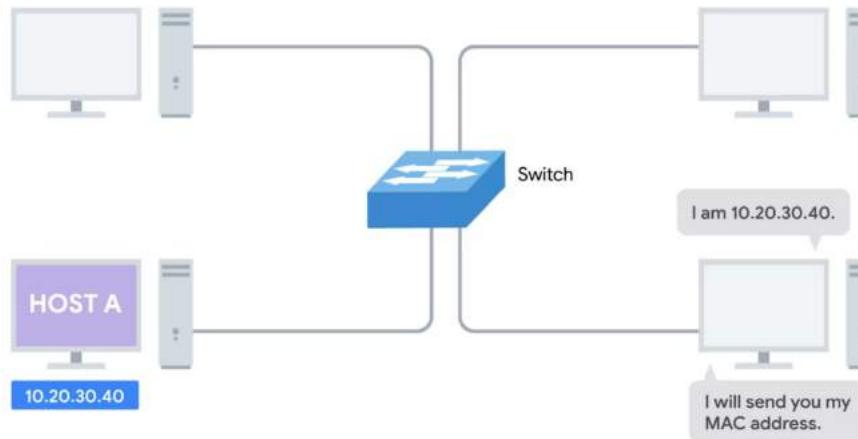
ARP (Address Resolution Protocol) là giao thức để xác định địa chỉ MAC của một địa chỉ IP xác định.

- Mỗi máy sẽ lưu trữ một bảng ARP cục bộ để tra.
- Nếu không có thì gửi gói tin ra toàn mạng theo cơ chế broadcast để hỏi.



Giao thức phân giải địa chỉ

Máy đích khi nhận tín hiệu ARP broadcast, nó sẽ gửi lại tín hiệu **ARP response** chứa địa chỉ MAC của máy đích



NỘI DUNG



Tầng mạng



Phân lớp địa chỉ IP



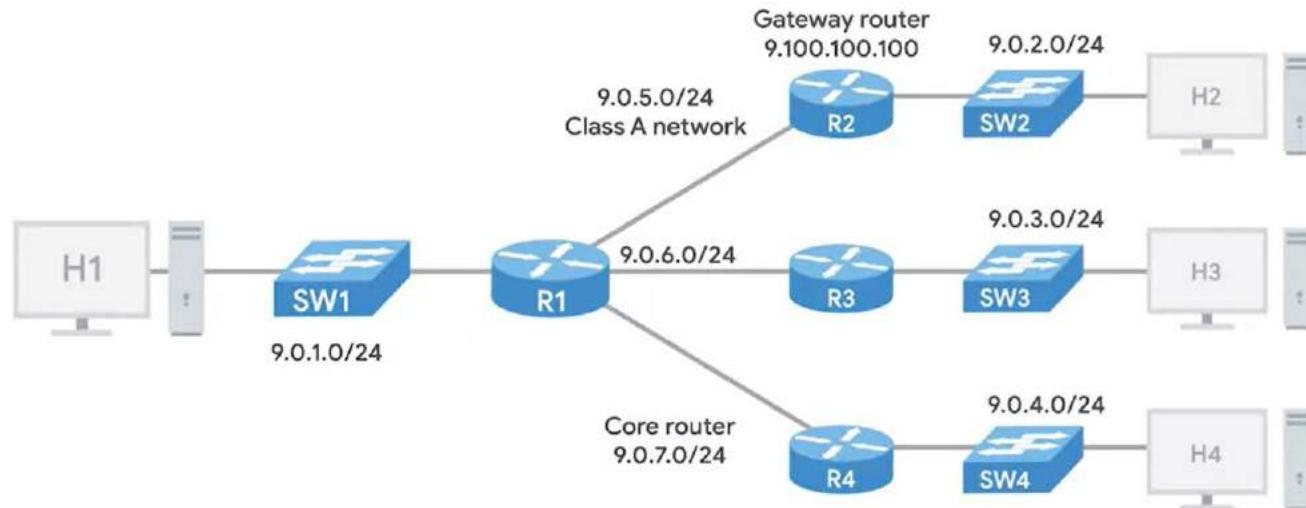
Mạng con



Định tuyến

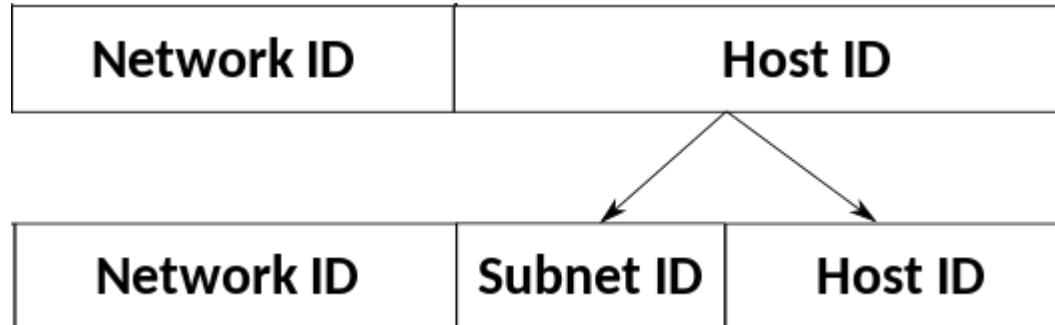
Mạng con

Mạng máy tính lớn có thể được tách thành nhiều mạng nhỏ hơn, mỗi mạng được gọi là **mạng con** (subnet)



Mặt nạ mạng con

- **Mặt nạ mạng con** (subnet mask) là một chuỗi bit tương tự như địa chỉ IP.
- Lấy mặt nạ mạng con **thực hiện phép luận lý AND** trên bit với địa chỉ IP của máy tính, ta sẽ **tính được: network id, subnet id và host id**.



Mặt nạ mạng con

Mã định danh mặt nạ mạng con (Subnet Mask Id) là **kết quả sau khi thực hiện phép luận lý AND** giữa mặt nạ mạng con với IP máy tính.

(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

Dạng viết tắt

Do mặt nạ mạng con theo quy luật gồm 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**

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

Biểu diễn số nguyên ở hệ nhị phân

- Hệ nhị phân là hệ chỉ có 2 giá trị phân biệt: 0 và 1
- Để biểu diễn một số hệ 10 (thập phân) dưới dạng hệ nhị phân, ta thực hiện phép chuyển đổi.
- Có thể hình dung mỗi vị trí mang trong nó một giá trị như hình sau:

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

- Ô nào có bit 1 thì giá trị tại ô đó được tính vào phép tính tổng để ra được giá trị hệ 10.

Biểu diễn số nguyên ở hệ nhị phân

Ví dụ

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

$$8 + 2 = 10$$

Số lượng giá trị phân biệt

- Mỗi vị trí bit, ta có 2 giá trị phân biệt
- Nên với n bit, số lượng giá trị phân biệt là 2^n
- Miền giá trị sẽ từ 0 đến $2^n - 1$ nếu chúng ta chỉ xét số dương

8 bit

$$2^8 = 256$$

0-255

4 bit

$$2^4 = 16$$

16 bit

$$2^{16} = 65536$$

Phép tính trên hệ nhị phân

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 10$$

$$1 \text{OR } 0 = 1$$

$$0 \text{OR } 0 = 0$$

$$1 \text{OR } 1 = 1$$

$$1 \text{AND } 1 = 1$$

$$1 \text{AND } 0 = 0$$

$$0 \text{AND } 0 = 0$$

Nhược điểm của phân lớp mạng

Phân lớp mạng theo cách như A, B, C có nhiều nhược điểm:

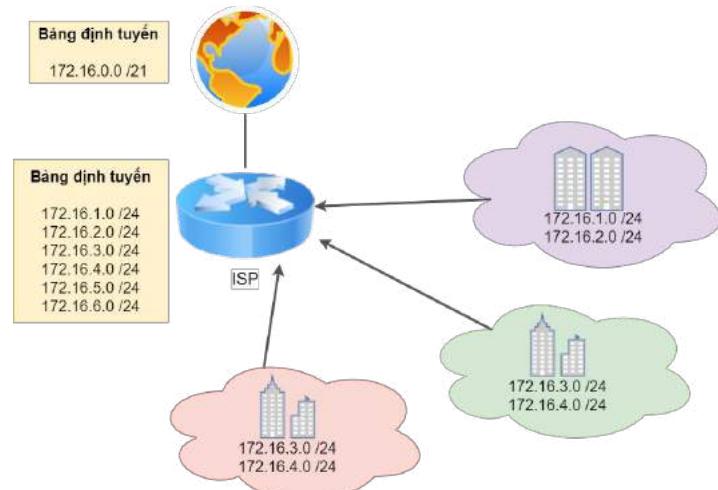
- Sự không cân bằng giữa các lớp
 - Bảng định tuyến phải chứa số lượng mạng lớn
 - Định tuyến phức tạp
- ...

Class	Mask short name	Max Hosts
A	255.0.0.0 11111111.00000000.00000000.00000000	/8 16,777,214
B	255.255.0.0 11111111.11111111.00000000.00000000	/16 65,534
C	255.255.255.0 11111111.11111111.11111111.00000000	/24 254
	255.255.240.0 11111111.11111111.11110000.00000000	/20 4,094
	255.255.255.224 11111111.11111111.11111111.11100000	/27 30
	255.255.255.252 11111111.11111111.11111111.11111100	/30 2

CIDR

CIDR (Classless Inter Domain Routing) là phương pháp cấp phát địa chỉ IP mà tại đó nó thể hiện **địa chỉ của một máy tính dưới dạng địa chỉ IP/tiền tố mạng (network prefix)**.

Tiền tố mạng là số bit đầu tiên trong địa chỉ IP được sử dụng để định danh mạng.



NỘI DUNG



Tầng mạng



Phân lớp địa chỉ IP



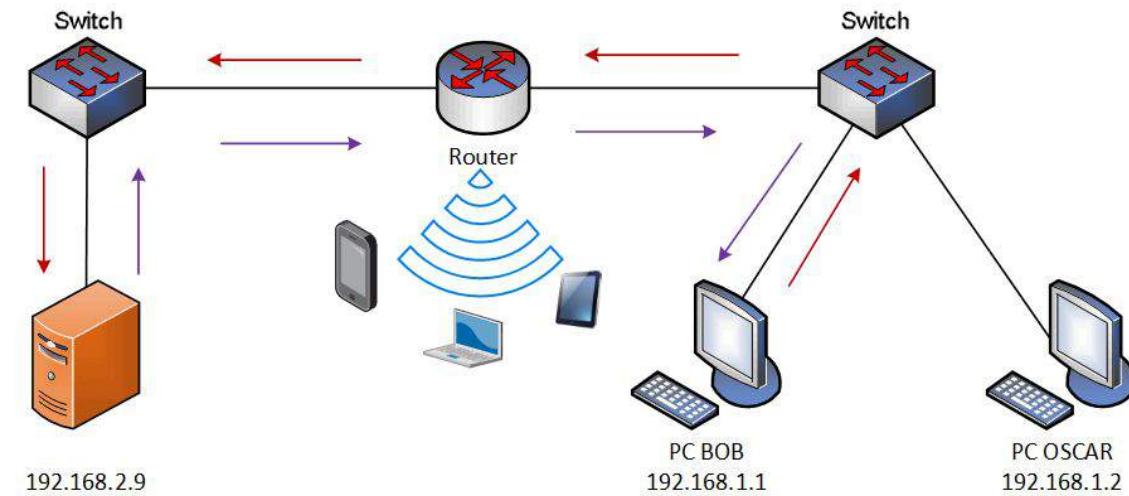
Mạng con



Định tuyến

Router

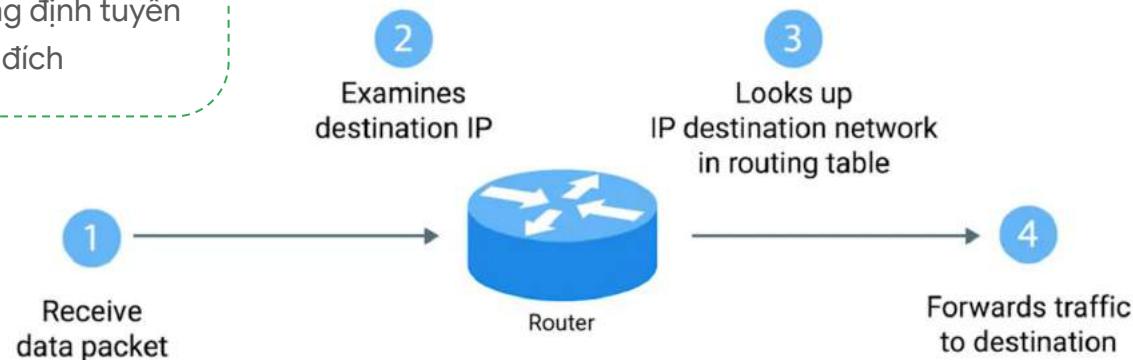
Bộ định tuyến (router) là thiết bị chuyển tiếp dữ liệu giữa các mạng khác nhau



Các bước định tuyến

Định tuyến gồm các bước:

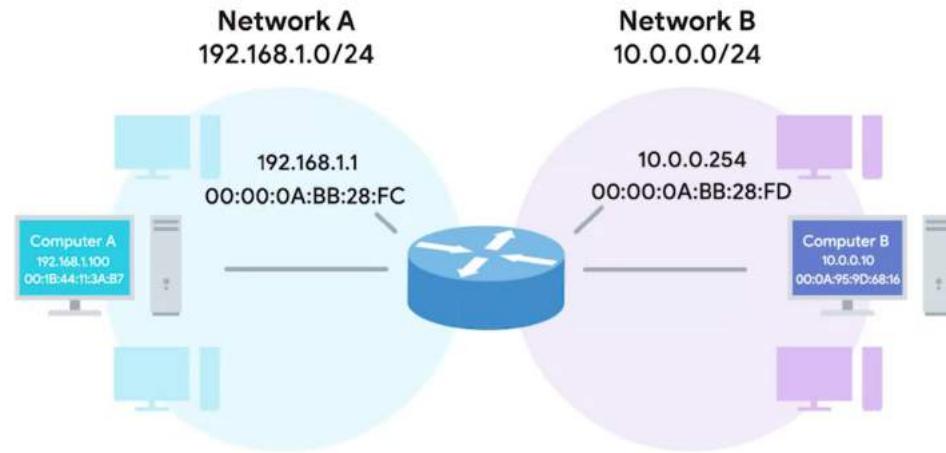
1. Nhận dữ liệu từ một máy
2. Kiểm tra IP máy đích
3. Tra mạng của IP này trong bảng định tuyến
4. Chuyển tiếp gói tin đến mạng đích



Các bước định tuyến

Ví dụ:

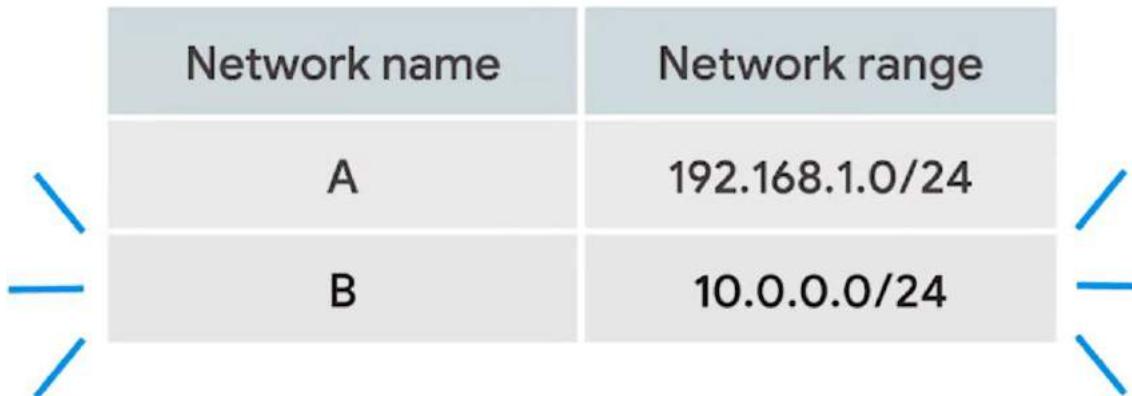
1. Máy tính A tra bảng ARP cục bộ của nó để xác định địa chỉ MAC của máy B, tuy nhiên nó phát hiện không có. Điều này đồng nghĩa với việc máy B không nằm trong cùng mạng con với nó.
2. Lúc này máy tính A gửi gói tin đến địa chỉ MAC của router.
3. Router nhận và xử lý gói tin này bởi vì địa chỉ đích đề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



Các bước định tuyến

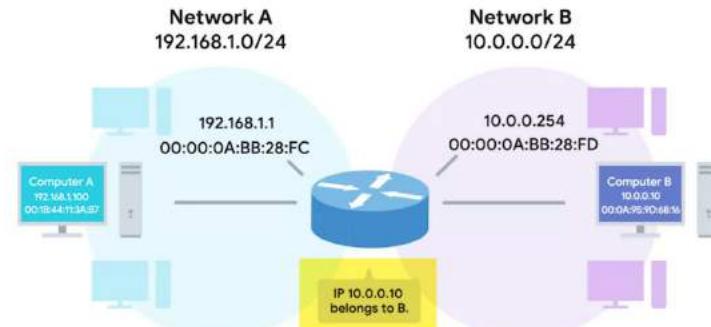
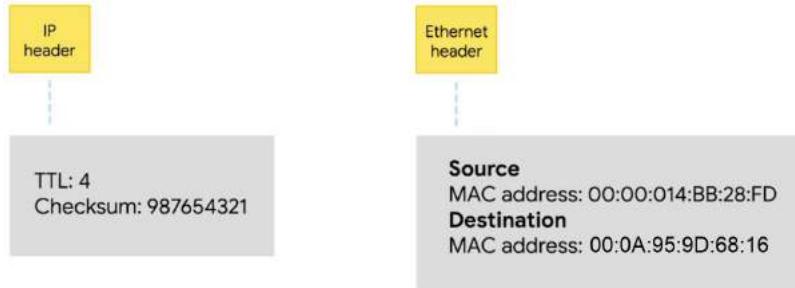
5. Router tra địa chỉ 10.0.0.10 trong bảng định tuyến (routing table) để xác định mạng mà địa chỉ này thuộc về. Trong trường hợp này là mạng B

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



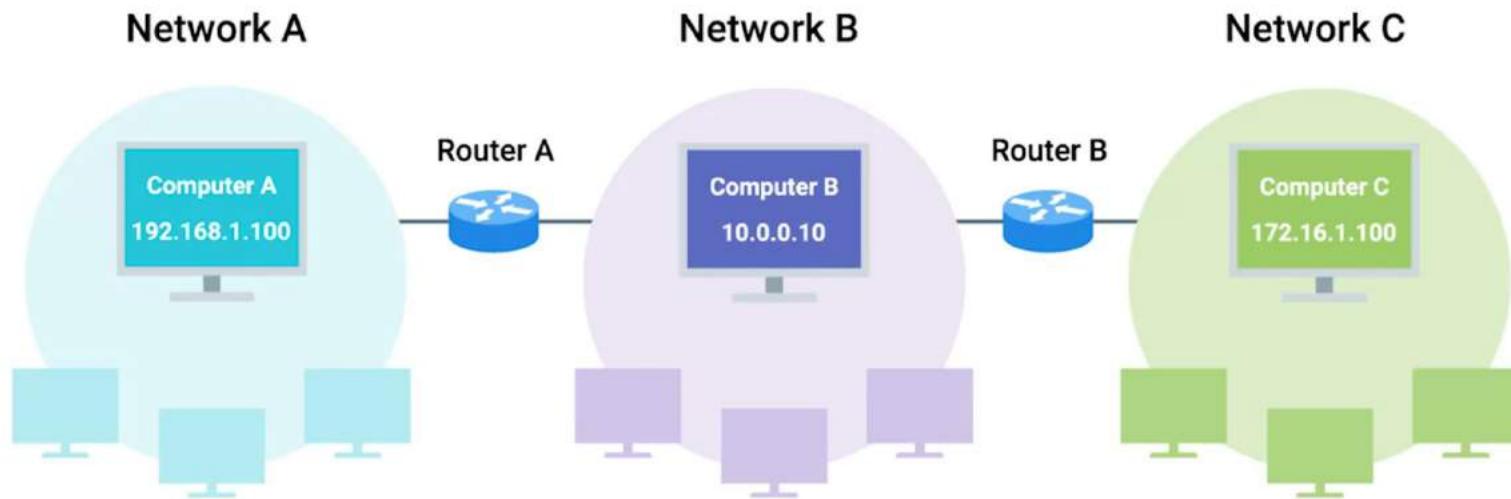
Các bước định tuyến

6. Bởi vì mạng B có kết nối 1 bước (nối trực tiếp) nên router sẽ tra được địa chỉ MAC của máy B trong ARP của nó.
7. Router đóng gói lại gói tin với MAC nguồn là địa chỉ MAC của chính nó và MAC đích là của máy B.
8. Router gửi gói tin này đến máy B.



Các bước định tuyến

Quá trình tương tự cho các máy ở mạng xa hơn

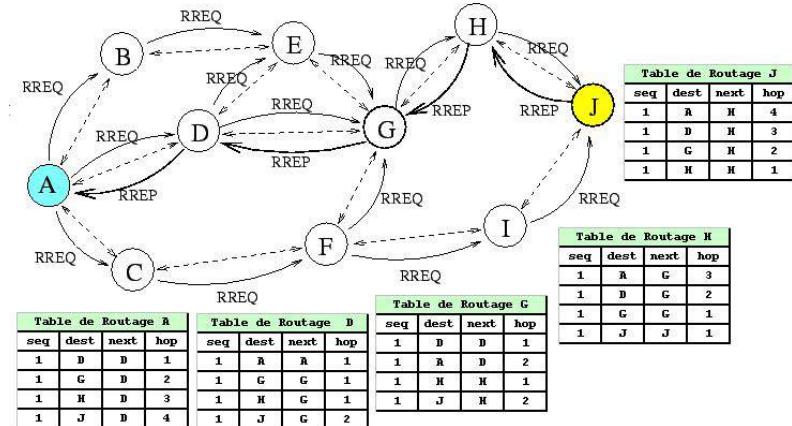


Bảng định tuyến

Bảng định tuyến (routing table) là bảng dữ liệu chứa danh sách các đường đi đến mạng đích.

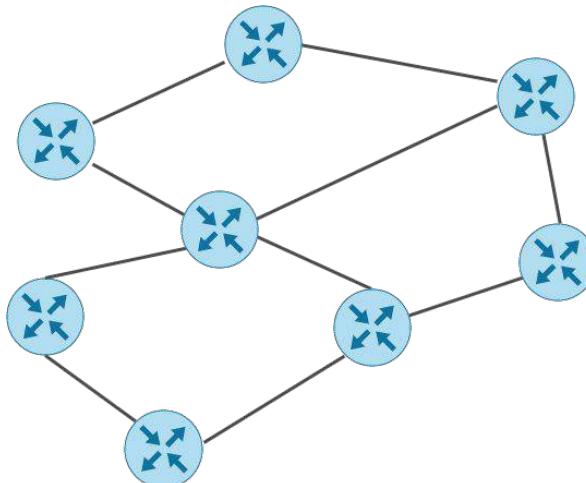
Thường có 4 cột:

- **Mạng đích** (destination network): thông tin về các mạng mà router biết. Mỗi mạng gồm cột mã mạng, cột mặt nạ mạng.
- **Nút kế tiếp** (next hop): máy được kết nối trực tiếp đến router mà nó có thông tin về mạng đích
- **Tổng bước** (total hops): tổng số router cần qua để đi đến đích ngắn nhất



Giao thức định tuyến

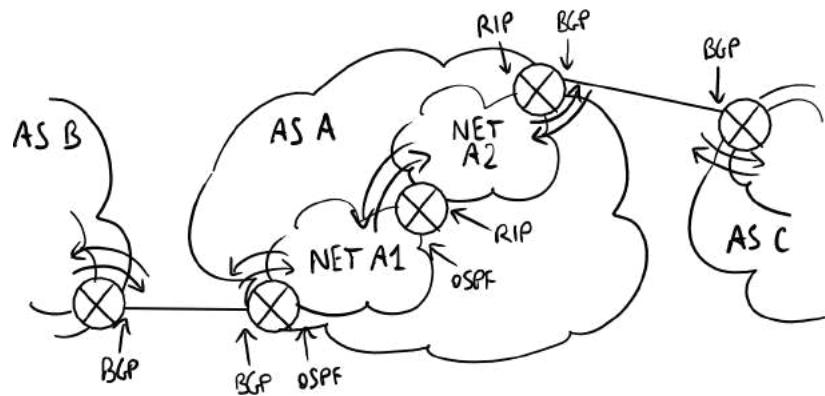
Giao thức định tuyến (routing protocol) là cách thức các router giao tiếp với nhau để chia sẻ thông tin nhằm xác định đường đi ngắn nhất đến mạng đích.



Giao thức định tuyến

Có 2 loại giao thức định tuyến:

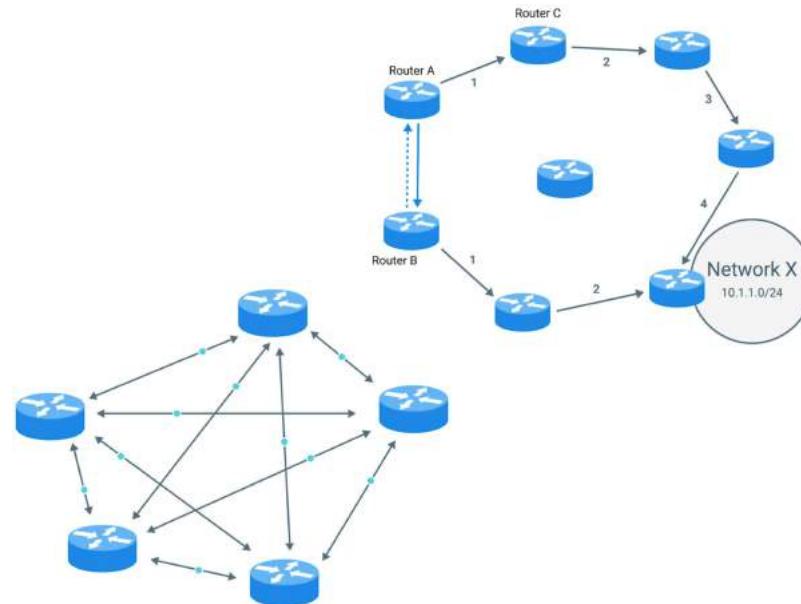
- Giao thức cổng trong (interior gateway protocol): chia sẻ thông tin nội bộ bên trong một hệ thống tự trị (AS – Autonomous System) (ví dụ như hệ thống các mạng LAN của công ty)
 - Giao thức phổ biến: RIP (Routing Information Protocol), OSPF (Open Shortest Path First)
- Giao thức cổng ngoài (exterior gateway protocol): chia sẻ thông tin giữa các AS với nhau
 - Giao thức phổ biến: BGP (Border Gateway Protocol)



Giao thức định tuyến

Giao thức cổng trong (interior gateway protocol) gồm 2 giao thức con:

- Giao thức định tuyến vectơ khoảng cách (distance-vector): tìm đường đi qua lảng giềng (RIP)
- Giao thức định tuyến trạng thái liên kết (link state): dựa trên liên kết đầy đủ của từng cặp router để tìm đường đi tối ưu (OSPF)



Hệ thống tự trị

Hệ thống tự trị (autonomous system) là một tập hợp các router được đặt dưới sự quản lý chung.

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.

- Do tổ chức cấp phát số hiệu Internet (IANA) quản lý.



Tổ chức IANA

Tổ chức cấp phát số hiệu Internet (IANA – Internet Assigned Numbers Authority) là tổ chức phi lợi nhuận giám sát việc định nghĩa địa chỉ IP và cấp phát giao thức Internet khác.



Internet Assigned Numbers Authority

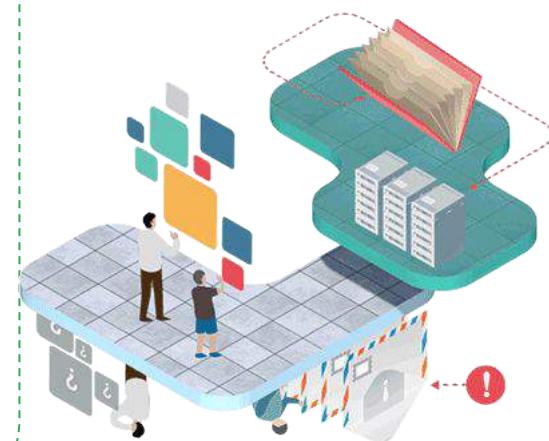
Không gian địa chỉ không thể định tuyến

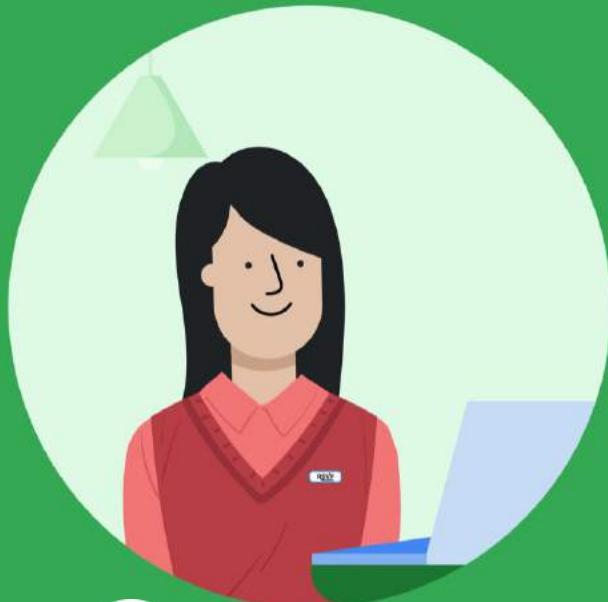
Không gian địa chỉ không thể định tuyến (non-routable address space) là các địa chỉ IP dành riêng cho mạng cá nhân (private network). Các gói tin với địa chỉ IP này về cơ bản sẽ không được định tuyến ra Internet bởi các router.

- Ai cũng có thể sử dụng không gian địa chỉ này và không cần phải đăng ký
- Để các máy giao tiếp ra mạng Internet, router dùng **kỹ thuật NAT** (Network Address Translation)

Có 3 không gian địa chỉ như vậy:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16





5 TẦNG VẬN CHUYỂN



NỘI DUNG



Tầng vận chuyển



TCP segment



Cơ chế bắt tay



Socket



Giao thức hướng kết
nối và phi kết nối

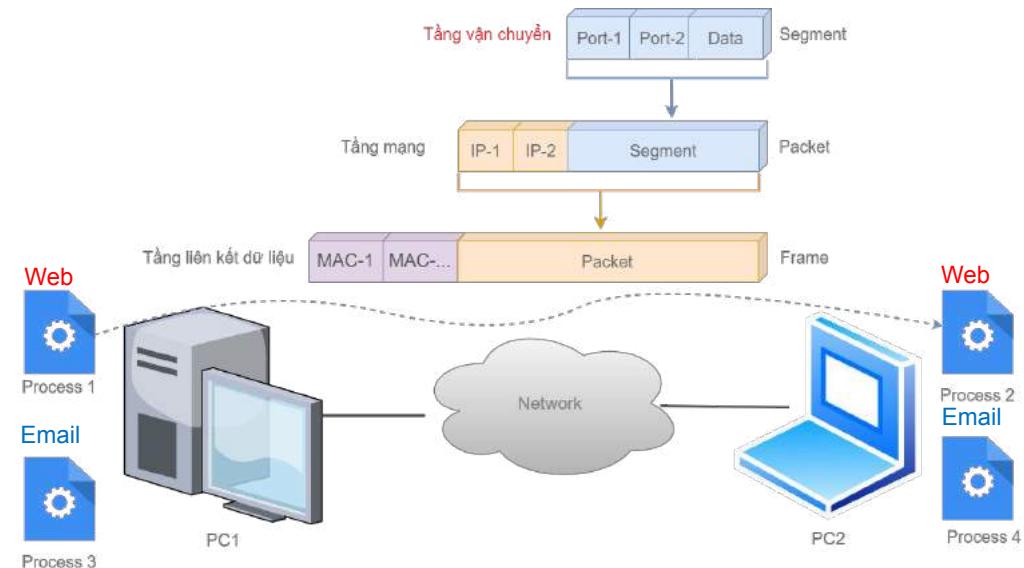


Tường lửa

Tầng 4: Tầng vận chuyển

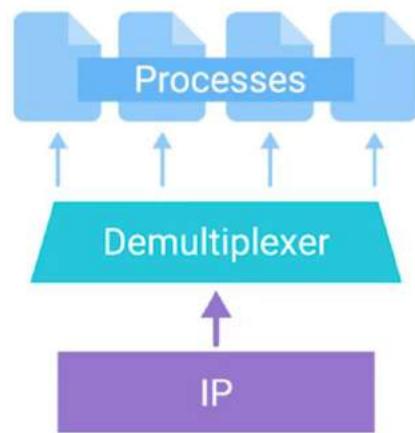
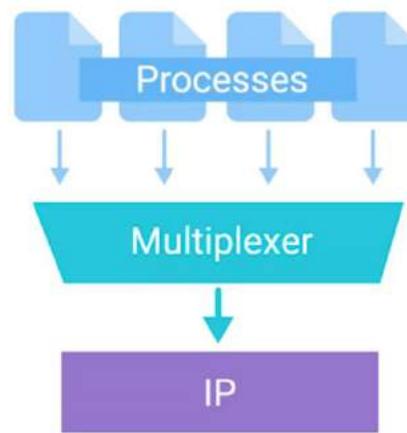
Tầng vận chuyển (transport layer) chuyển dữ liệu từ một ứng dụng trên máy nguồn đến đúng một ứng dụng trên máy đích.

- Giao thức phổ biến là **TCP** (Transmission Control Protocol) và **UDP** (User Datagram Protocol).



Ghép kênh và tách kênh

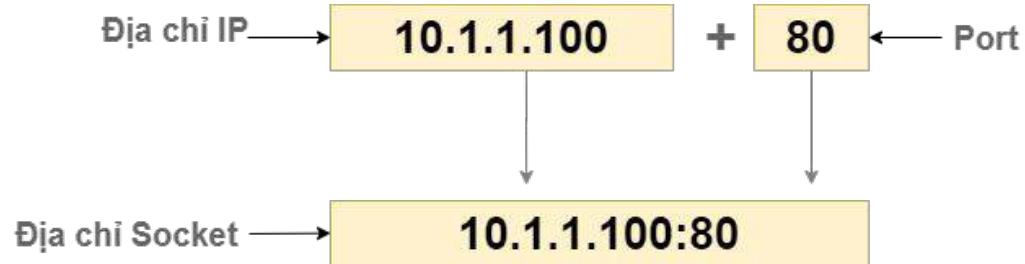
- Tầng vận chuyển có khả năng **ghép** nhiều chuỗi dữ liệu của các ứng dụng **lại** để truyền đi trong một lần giúp tiết kiệm tài nguyên đường truyền.
- Quá trình ghép được gọi là **multiplexing**, quá trình tách ở máy đích được gọi là **demultiplexing**.



Cổng

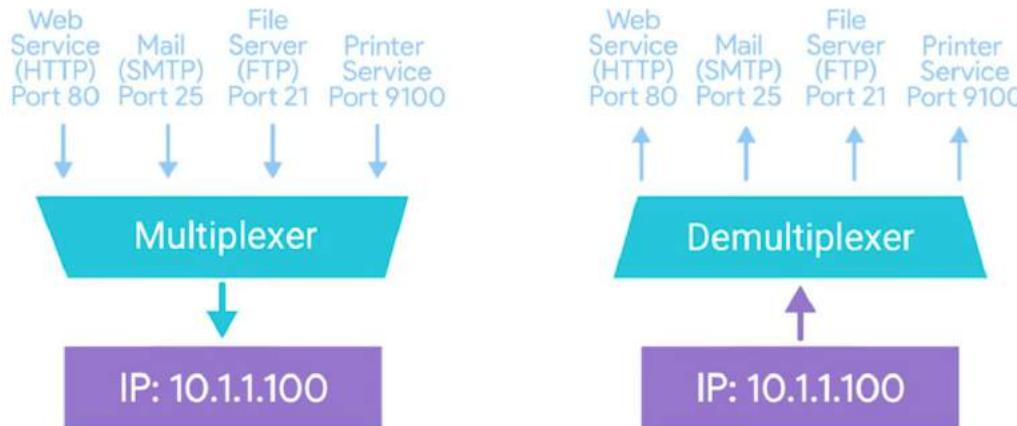
Các dịch vụ mạng khi chạy sẽ lắng nghe tín hiệu ở các cổng xác định (port)

- Port là số được viết với dấu hai chấm (:) sau địa chỉ IP
- Kích thước biểu diễn là 16 bit, do đó số lượng cổng về lý thuyết có thể có là 65535
- Ví dụ, 10.1.1.100:80 (được gọi là địa chỉ socket hay số socket)



Port và cơ chế ghép/tách kênh

Port và cơ chế ghép kêt, tách kêt giúp cho tầng vận chuyển có thể hỗ trợ giao tiếp giữa nhiều ứng dụng khác nhau của các máy trong mạng.



NỘI DUNG



Tầng vận chuyển



TCP segment



Cơ chế bắt tay



Socket



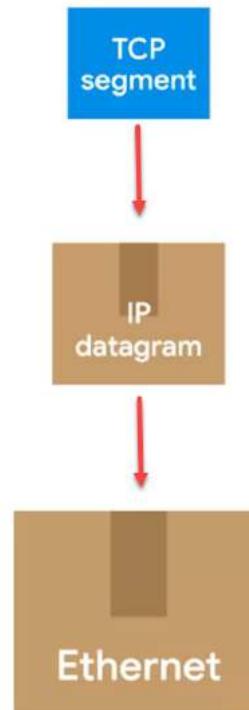
Giao thức hướng kết
nối và phi kết nối



Tường lửa

TCP segment

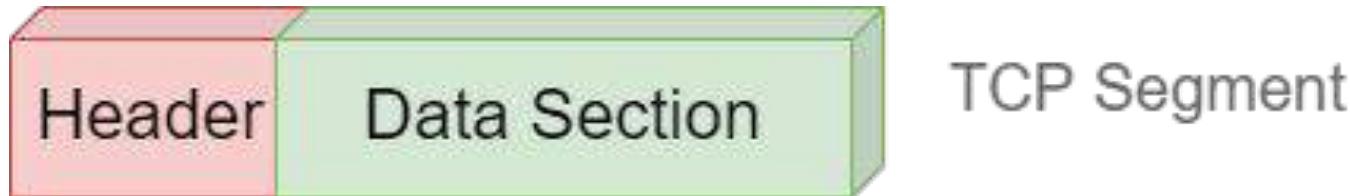
TCP segment là gói tín được hình thành ở tầng vận chuyển, sau đó được đóng gói thành IP datagram ở tầng mạng, và khung tin Ethernet ở tầng liên kết dữ liệu.



Cấu trúc của TCP segment

TCP segment gồm hai phần chính:

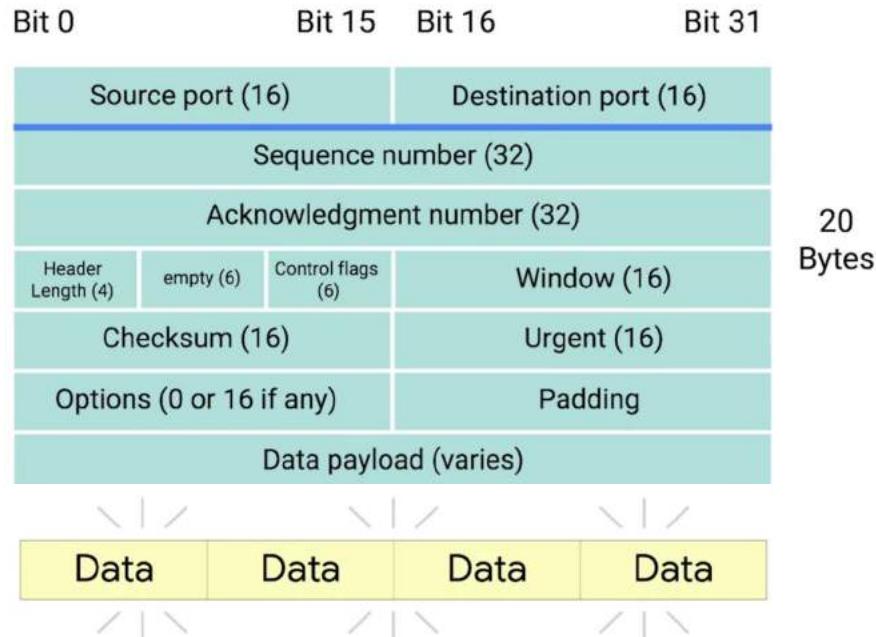
- **TCP header**: chứa thông tin mô tả gói tin
- **Dữ liệu**: phần dữ liệu mà tầng ứng dụng bỏ vào



TCP Header

TCP Header gồm các thông tin:

- Port nguồn và đích: là cổng mà ứng dụng nguồn gửi dữ liệu và ứng dụng đích xử lý nó.
- Port nguồn được chọn từ một miền đặc biệt có giá trị cao, được gọi là các port tạm thời (ephemeral port)
- Số thứ tự (sequence number): là chỉ số xác định TCP segment đang chứa đoạn nào của dữ liệu đang truyền.



TCP Header

TCP Header gồm các thông tin:

- ...
- **Ack number**: số thứ tự segment mong đợi tiếp theo
- **Độ dài của header**
- **Cờ điều khiển**
- **Cửa sổ TCP**: miền các số tuần tự nhận rồi mới xác nhận
- **Checksum**: kiểm tra lỗi
- **Urgent**: xác định độ quan trọng của gói tin
- **Options**: chức năng thêm
- **Padding**: làm header kích thước xác định

Bit 0	Bit 15	Bit 16	Bit 31			
Source port (16)		Destination port (16)				
Sequence number (32)						
Acknowledgment number (32)						
Header Length (4)	empty (6)	Control flags (6)	Window (16)			
Checksum (16)		Urgent (16)				
Options (0 or 16 if any)		Padding				
Data payload (varies)						

Cờ điều khiển

TCP tạo ra nhiều cờ để điều khiển kết nối giữa 2 hai máy:

- Cờ **URG** (urgent): để nói rằng gói tin này là cấp bách
- Cờ **ACK** (acknowledge): yêu cầu xác nhận, kiểm tra số thứ tự Ack
- Cờ **PSH** (push): yêu cầu thiết bị nhận đẩy dữ liệu nằm trong vùng đệm đến ứng dụng cần xử lý càng sớm càng tốt
- Cờ **RST** (reset): yêu cầu thực hiện gửi lại từ đầu do không thể xử lý các gói tin hiện tại.
- Cờ **SYN** (synchronize): yêu cầu kiểm tra số phân đoạn
- Cờ **FIN** (finish): đóng kết nối



NỘI DUNG



Tầng vận chuyển



TCP segment



Cơ chế bắt tay



Socket



Giao thức hướng kết
nối và phi kết nối

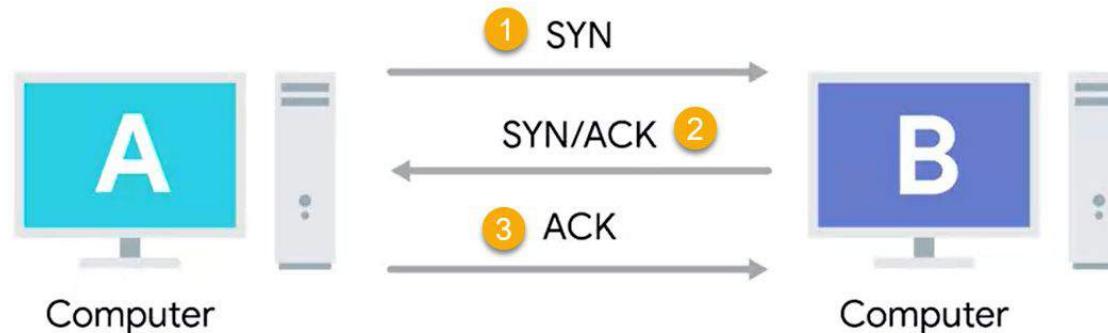


Tường lửa

Bắt tay 3 bước

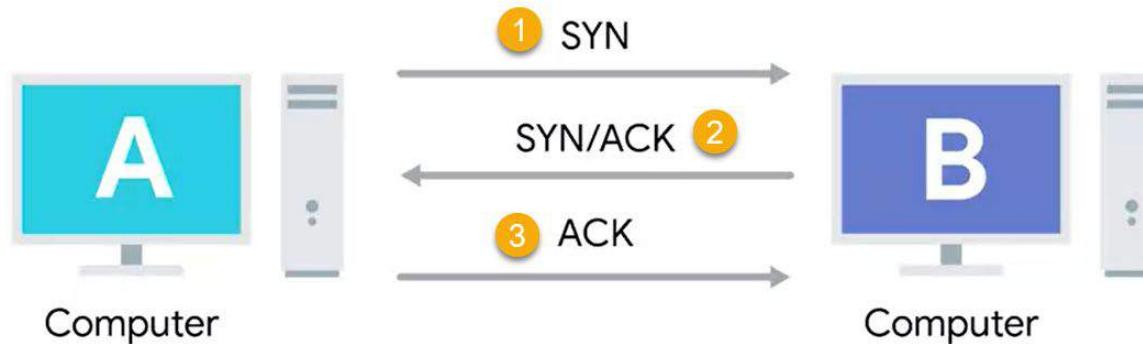
TCP cần **thiết lập** kênh kết nối trước khi chuyển dữ liệu đi.

Quá trình khởi tạo kết nối **theo quy trình bắt tay 3 bước** (three way handshake)



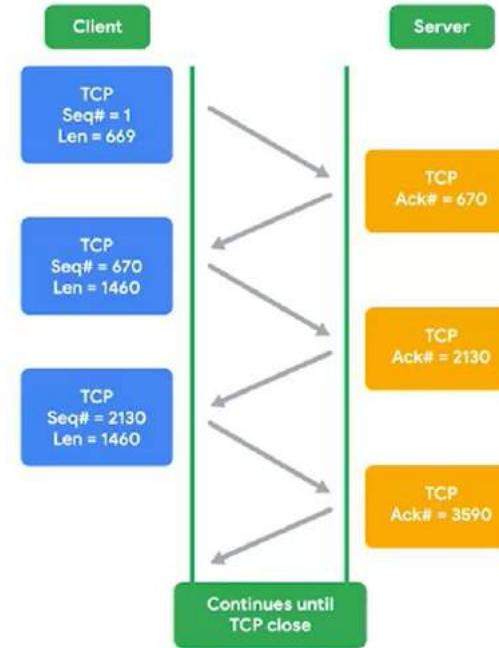
Bắt tay 3 bước

- **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.
- **Bước 2:** Máy B gửi ngược lại gói tin với cờ SYN và ACK bật lên để nói rằng đồng ý kết nối.
- **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.



Truyền dữ liệu

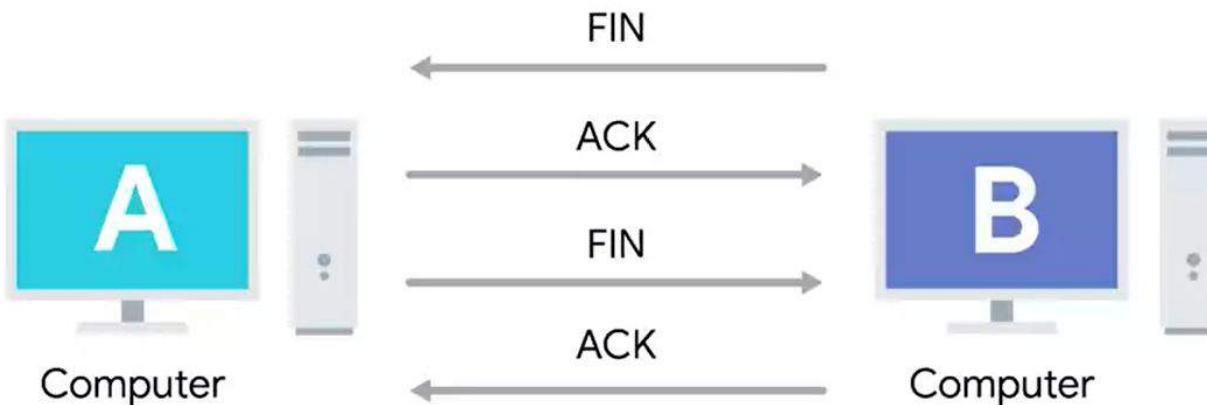
Khi cơ chế bắt tay hoàn thành,
2 máy sẽ gửi dữ liệu cùng với
thông tin SEQ và ACK để biết
những gì đã được gửi và nhận.



Bắt tay 4 bước

Kết thúc kết nối bằng bắt tay 4 bước

- Hai máy lần lượt gửi các gói tin với cờ FIN và cờ ACK.



NỘI DUNG



Tầng vận chuyển



TCP segment



Cơ chế bắt tay



Socket



Giao thức hướng kết
nối và phi kết nối



Tường lửa

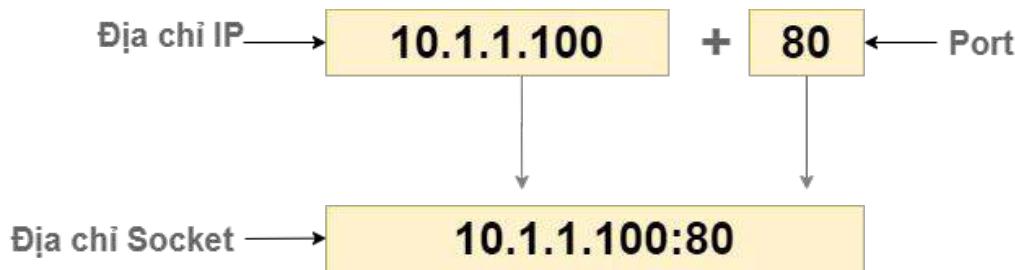
Socket

TCP socket là điểm đầu cuối trong giao tiếp của hai chương trình.

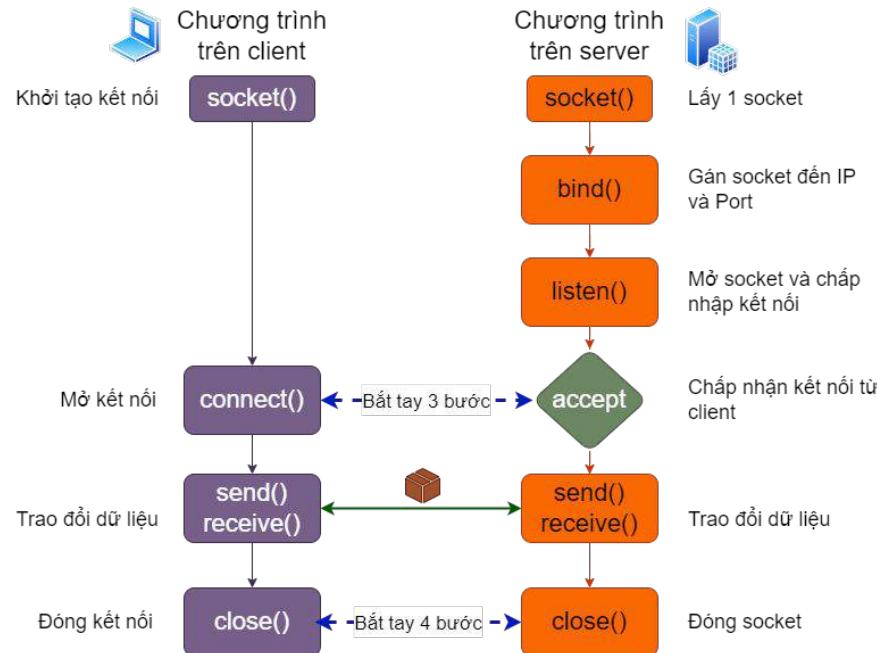
Để có thể giao tiếp, các chương trình cần khởi tạo/dăng ký socket.

TCP socket gồm 2 thành phần:

- Địa chỉ IP: máy nào nhận
- Port: chương trình nào nhận



Thực thi với Socket



Trạng thái của Socket



TCP Socket có nhiều trạng thái và khác nhau ở mỗi loại hệ thống:

- **LISTEN**: trạng thái sẵn sàng và lắng nghe kết nối đến (server)
- **SYN_SENT**: yêu cầu đồng bộ đã được gửi nhưng kết nối chưa được khởi tạo (client)
- **SYN_RECEIVED**: đã nhận yêu cầu đồng bộ và đã gửi lại SYN_ACK (server)
- **ESTABLISHED**: kết nối đã được thiết lập và có thể gửi/nhận dữ liệu (server, client)
- **FIN_WAIT**: đã gửi FIN nhưng chưa nhận được ACK (server, client)
- **CLOSE_WAIT**: kết nối đã đóng ở tầng TCP nhưng ứng dụng mở socket chưa giải phóng nó (server, client)
- **CLOSED**: kết nối đóng hoàn toàn (server, client)



NỘI DUNG



Tầng vận chuyển



TCP segment



Cơ chế bắt tay



Socket



Giao thức hướng kết
nối và phi kết nối

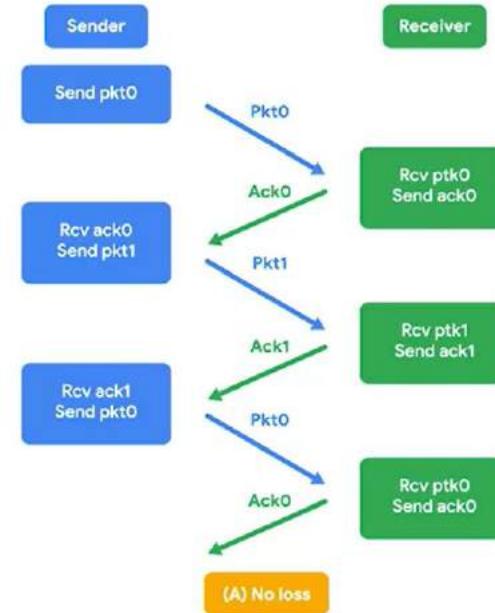


Tường lửa

Giao thức hướng kết nối

Giao thức hướng kết nối (connection-oriented protocol) là giao thức yêu cầu **phải khởi tạo kết nối trước** khi gửi dữ liệu và đảm bảo dữ liệu được gửi tin cậy.

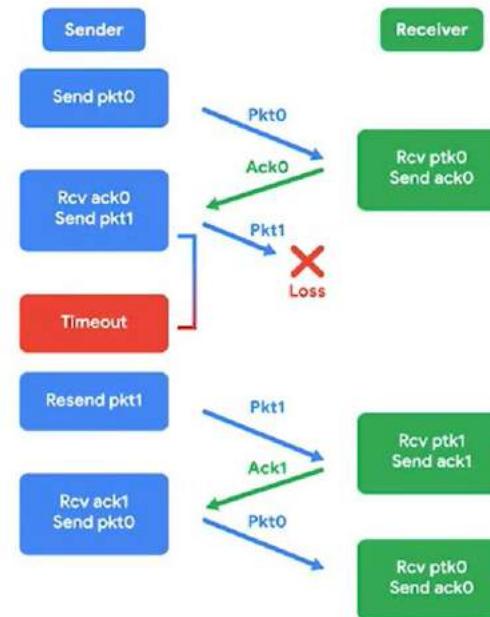
- Mỗi đoạn dữ liệu gửi đều phải được xác nhận (ACK).
- Giao thức TCP là giao thức hướng kết nối.



Giao thức hướng kết nối

Khi một gói tin lâu không nhận được phản hồi, nó sẽ được gửi lại.

- Nhờ có số thứ tự nên giúp máy đích tổ chức được dữ liệu một cách đúng đắn.

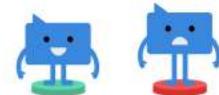


Giao thức phi kết nối



Giao thức phi kết nối (connectionless protocol) là giao thức **không cần khởi tạo trước** khi gửi dữ liệu.

- Dữ liệu không đảm bảo sẽ đến được người nhận.
 - Tốc độ sẽ nhanh hơn do không thực hiện quá nhiều bước xác nhận dữ liệu
 - Phù hợp cho việc gửi dữ liệu không quá quan trọng.
- Ví dụ: Hội nghị truyền hình (video conference), trò chơi trực tuyến, VoIP, DNS, ...
- UDP (User Datagram Protocol) là một giao thức phi kết nối.



NỘI DUNG



Tầng vận chuyển



TCP segment



Cơ chế bắt tay



Socket



Giao thức hướng kết
nối và phi kết nối

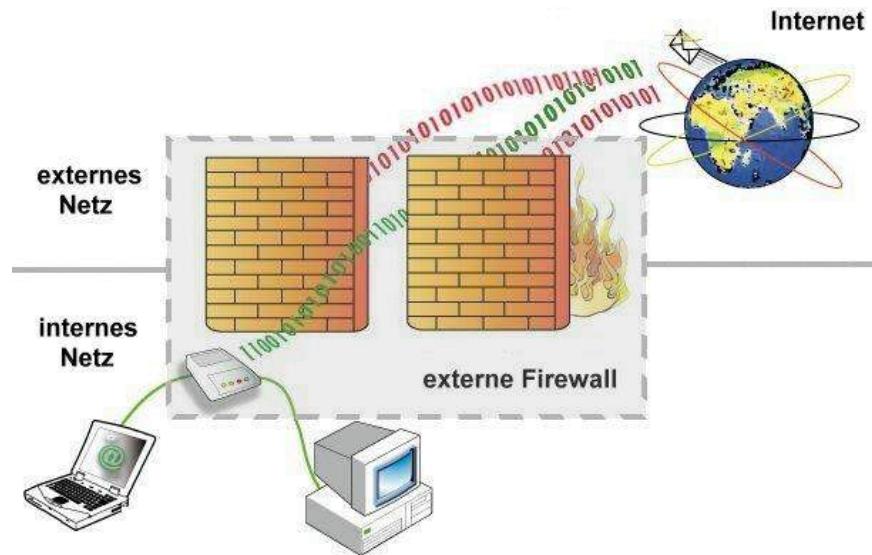


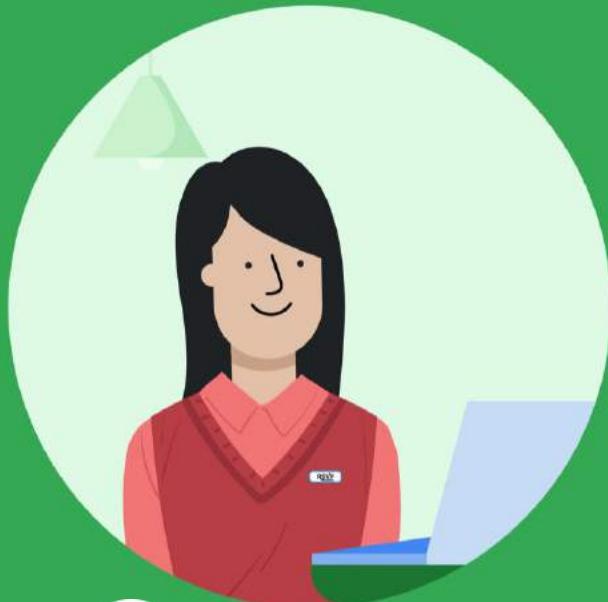
Tường lửa

Tường lửa

Tường lửa (firewall) là một hệ thống bảo mật mạng, 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 ngăn chặn giao tiếp các một cổng xác định.





6 TẦNG ỨNG DỤNG



NỘI DUNG



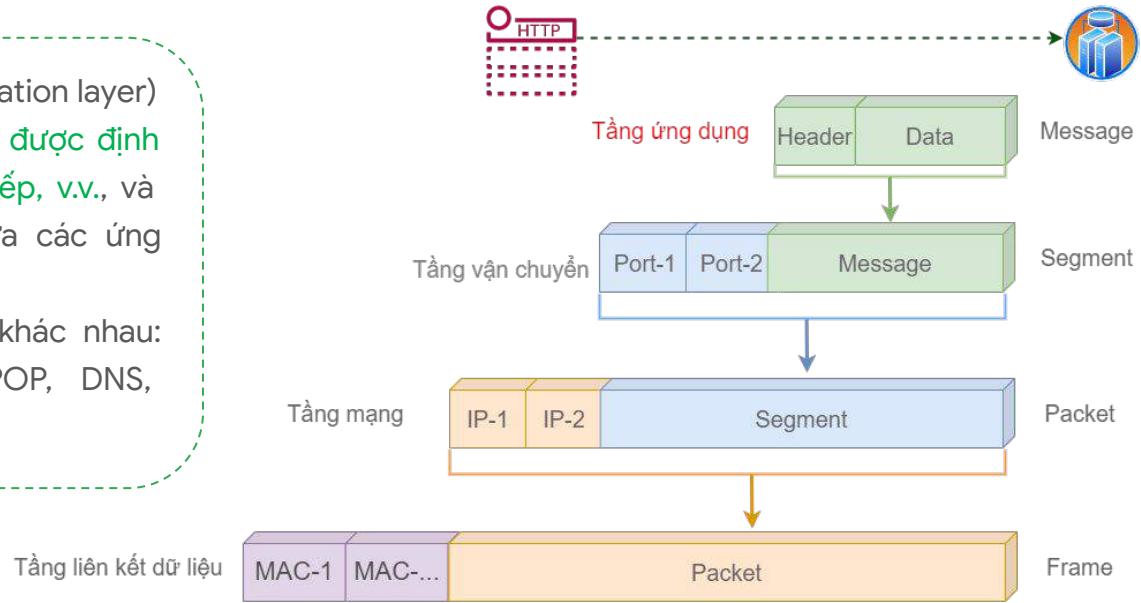
Tầng ứng dụng



Minh họa quá trình
thực thi của 5 tầng

Tầng 5: Tầng ứng dụng

- **Tầng ứng dụng** (application layer) xác định cách dữ liệu được định dạng, mã hóa, giao tiếp, v.v., và được thống nhất giữa các ứng dụng.
- Rất nhiều giao thức khác nhau: HTTP, FTP, SMTP, POP, DNS, DHCP, v.v..



Mô hình OSI

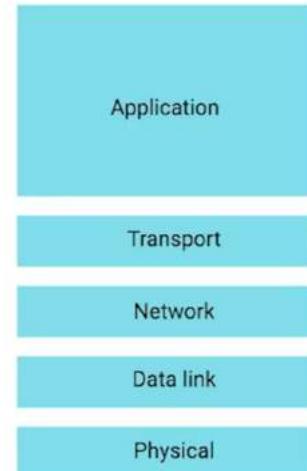
Mô hình OSI (Open Systems Interconnection) gồm 7 tầng.

- Bổ sung thêm 2 tầng giữa tầng vận chuyển và tầng ứng dụng. Cụ thể là **tầng phiên** và **tầng trình diễn**.
- 3 tầng trên cùng có thể xem như tương đương với tầng ứng dụng trong mô hình 5 tầng nhưng có độ chuyên biệt cao hơn.

OSI Model



TCP/IP 5-Layer Model



NỘI DUNG



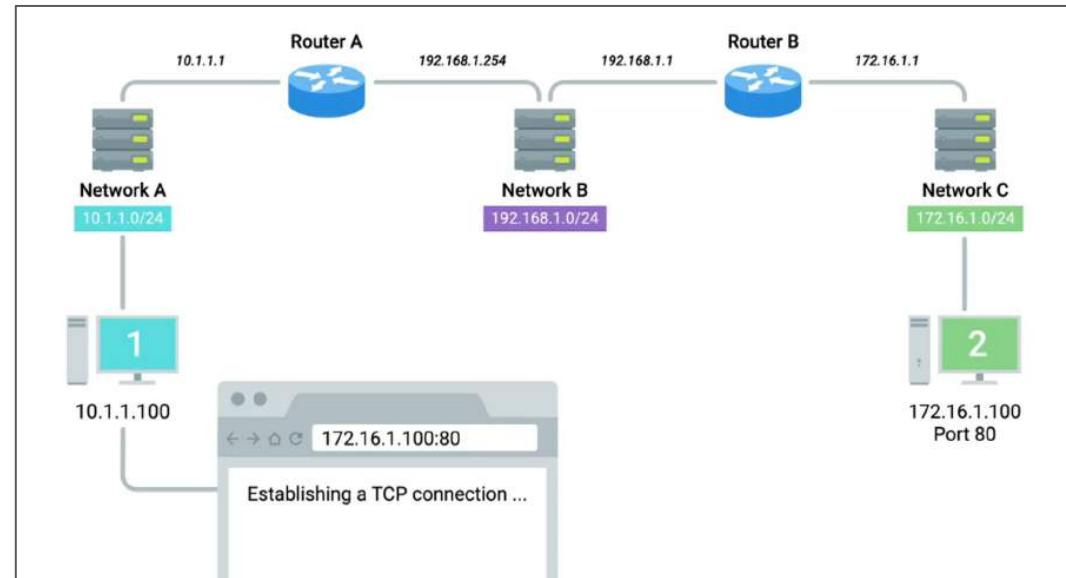
Tầng ứng dụng



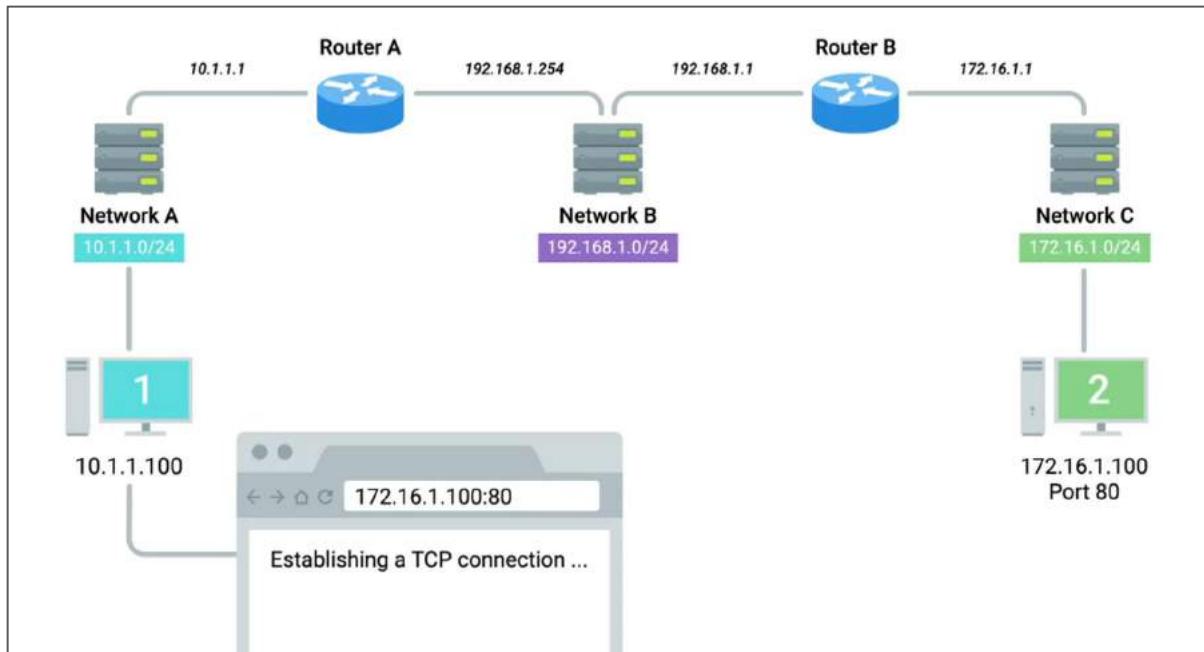
Minh họa quá trình
thực thi của 5 tầng

Hiện trạng mạng:

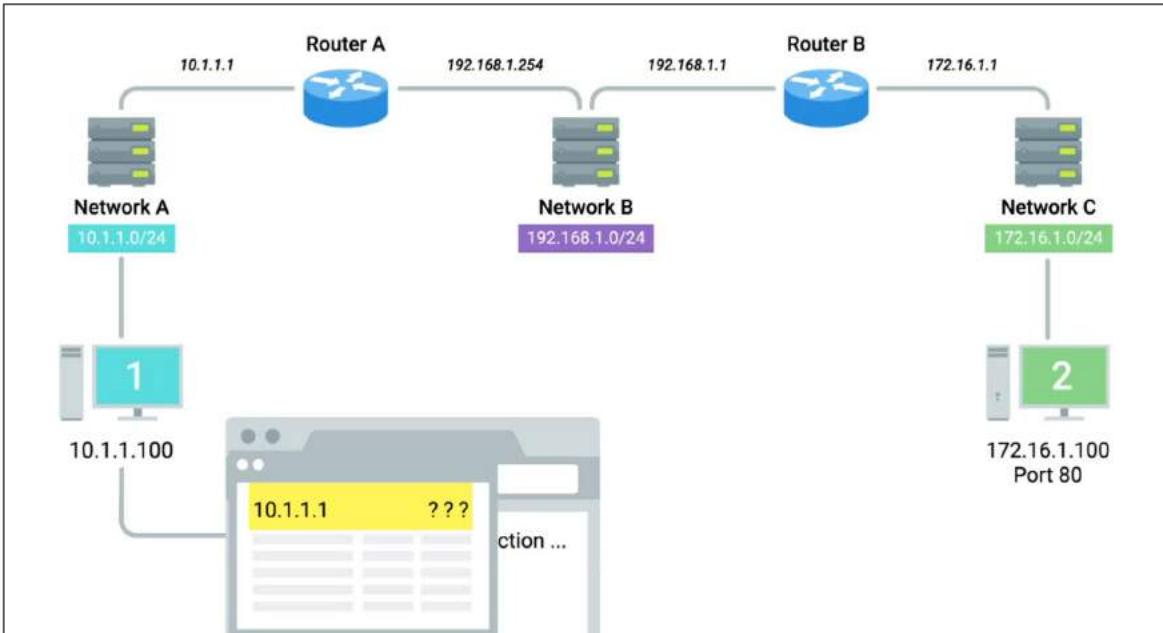
- 3 switch mạng A, B, C
- 2 router A, B
- 2 máy tính 1, 2
- Trình duyệt trên máy



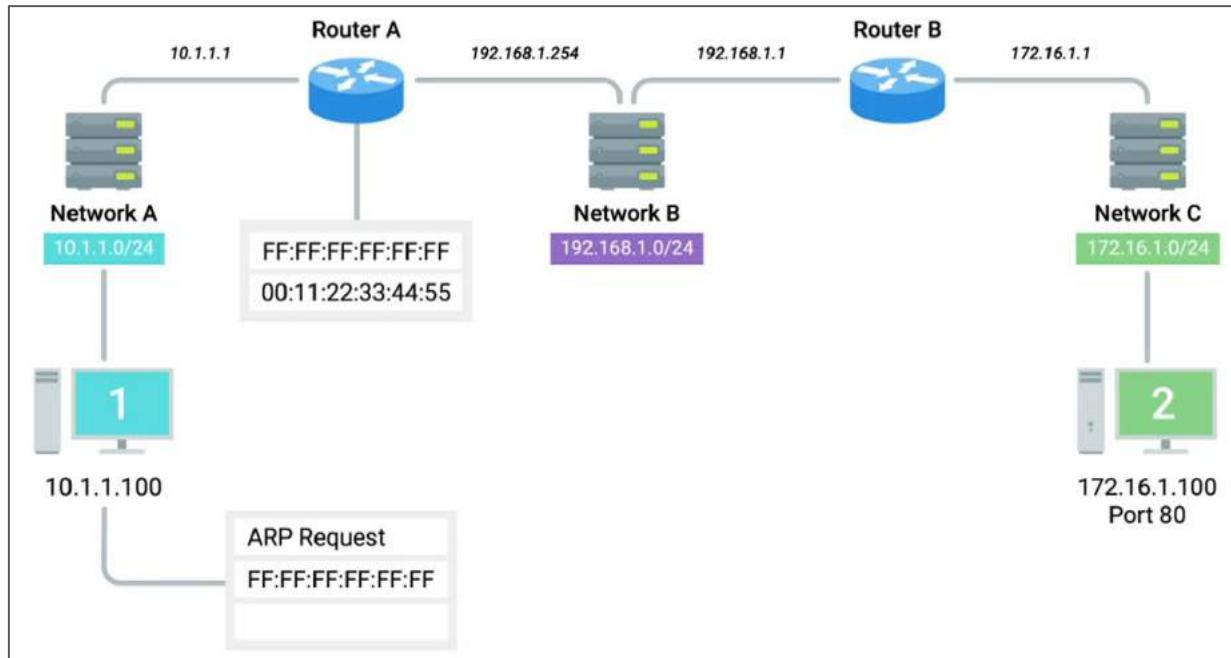
- Trình duyệt trên Máy 1 truy cập trang 172.16.1.100:80
- Máy 1 phát hiện máy có địa chỉ 172.16.1.100 không ở cùng mạng với mình nên cần phải gửi gói tin đến Router A để router này định tuyến gói tin đến đích giúp.



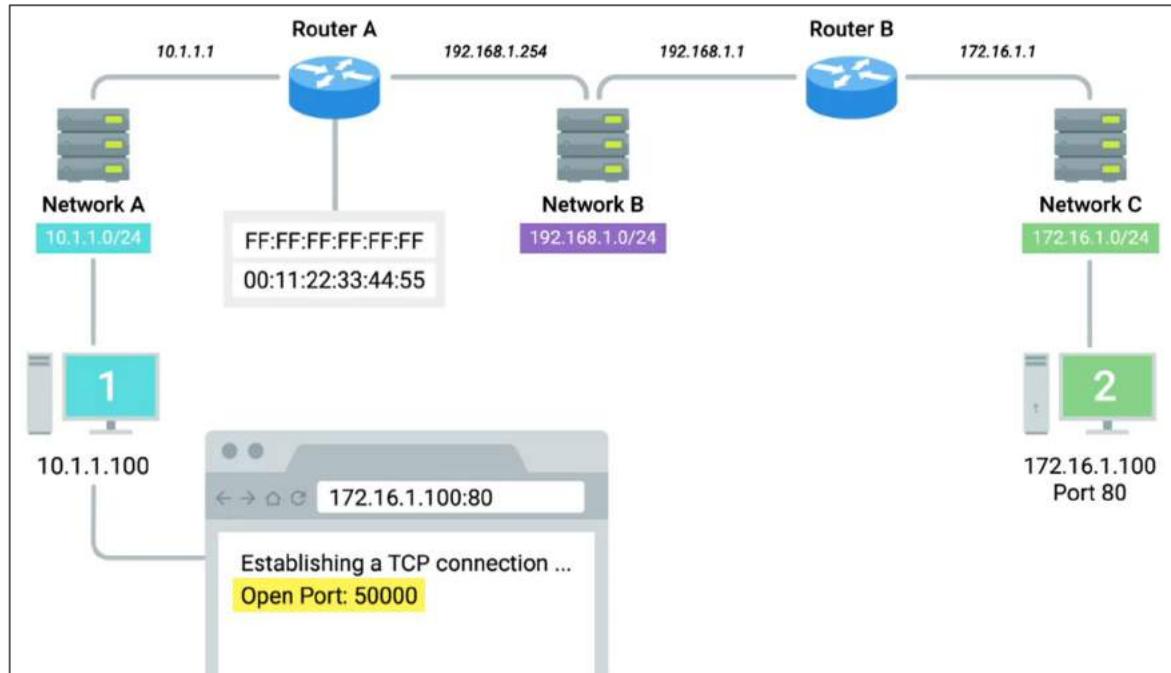
- Để Máy 1 gửi gói tin đến Router A thì máy 1 cần biết địa chỉ MAC của router này.
- Giả sử nó tra bảng ARP cục bộ, nhưng không thấy. Máy 1 sẽ gửi gói tin broadcast ra toàn bộ mạng với IP đích: FF: FF: FF: FF



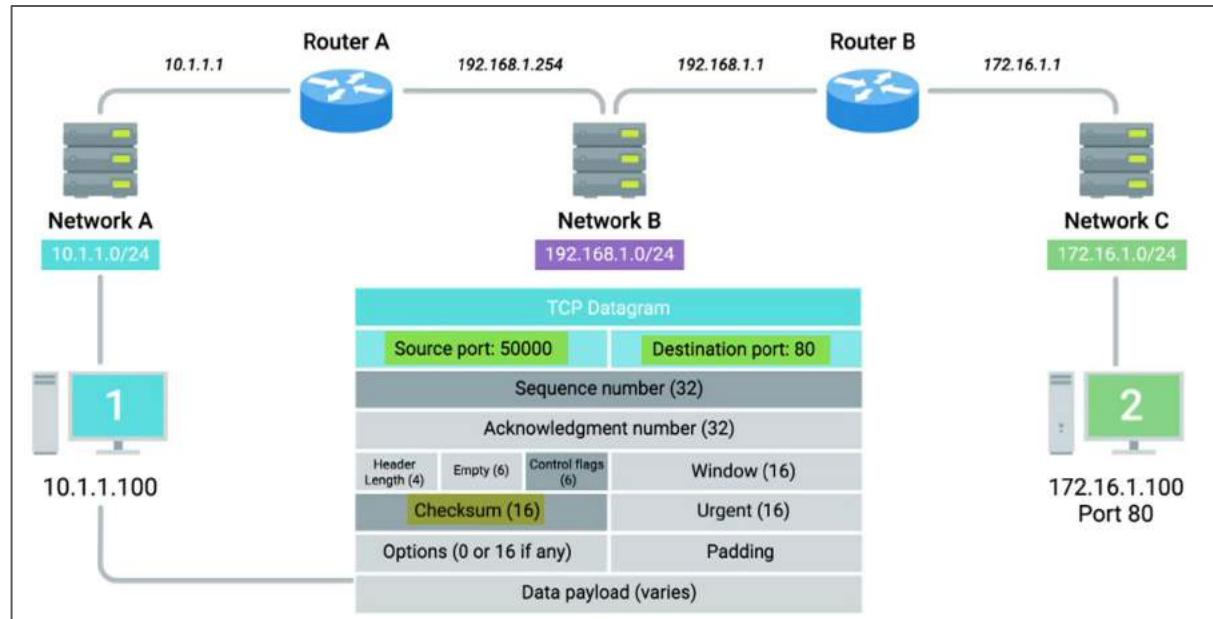
- 5. Router A nhận gói tin và phát hiện ra IP đích là FF:FF:FF:FF:FF, nó biết là gửi cho chính nó.
- 6. Router A gửi trả lại gói tin với địa chỉ MAC của nó.



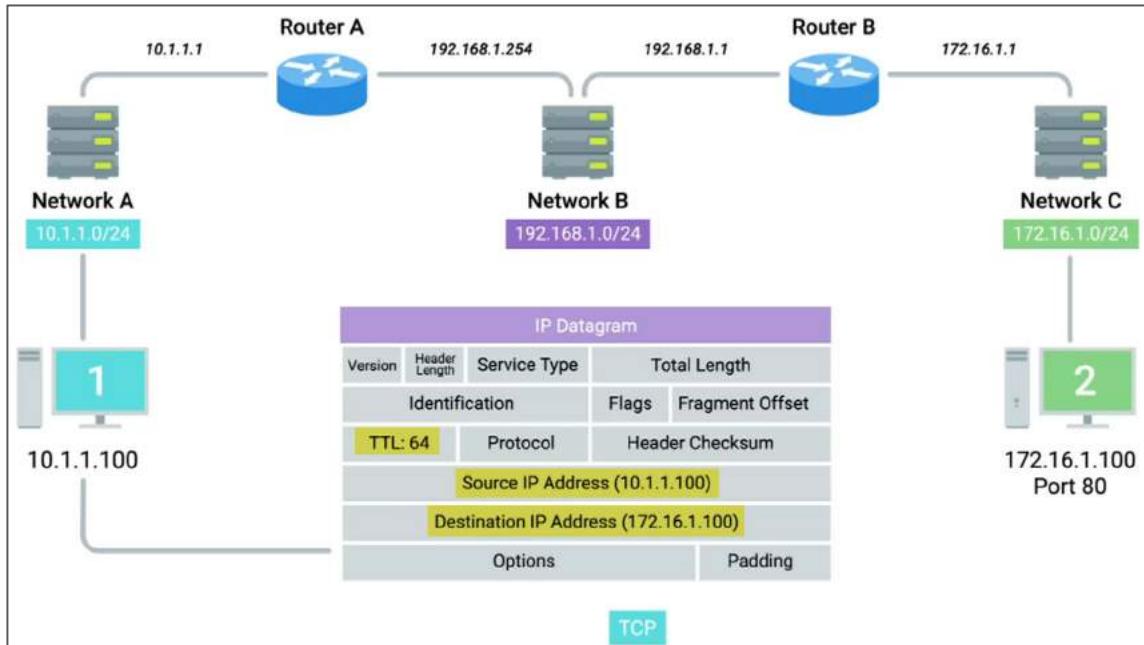
- 7. Máy 1 có được địa chỉ MAC của Router A.
- 8. Máy 1 khởi tạo 1 socket để giao tiếp TCP giữa chương trình duyệt với chương trình đang lắng nghe ở port 80 trên máy 2. Trong ví dụ này, Máy 1 mở port 50000



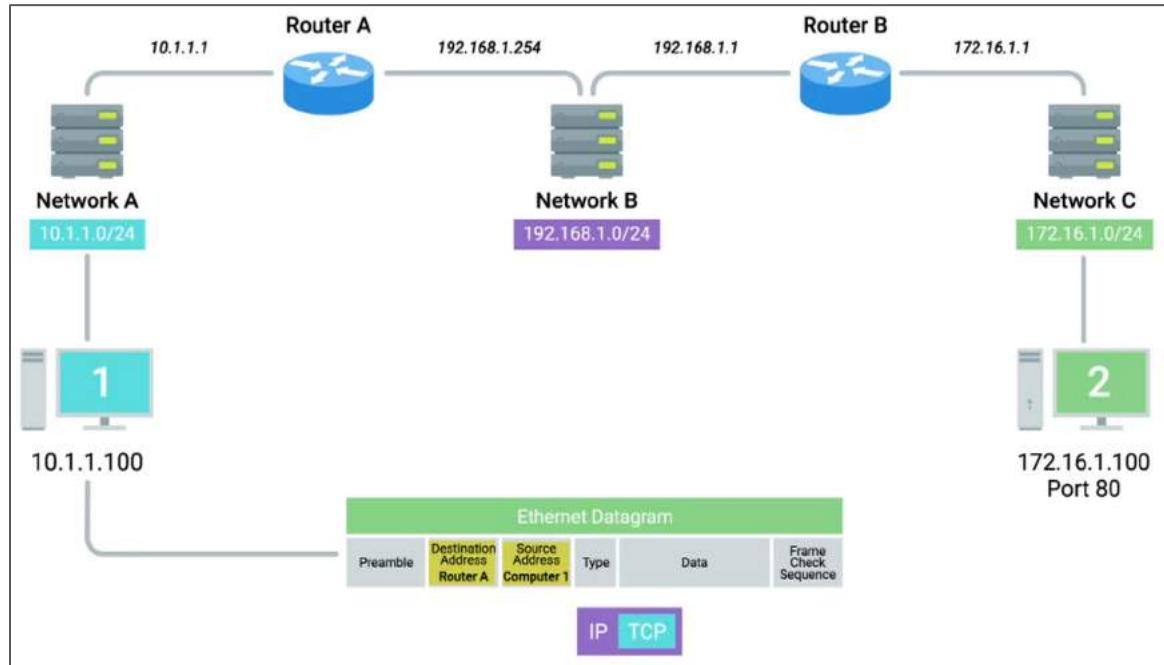
9. Tầng vận chuyển ở
Máy 1 tạo gói tin TCP
Datagram như trong
hình.
- Port máy nguồn: 50000
 - Port máy đích: 80
 - Checksum để kiểm tra gói tin chuyển tiếp đầy đủ.
 - Data payload: dữ liệu từ tầng ứng dụng.
 - V.v....



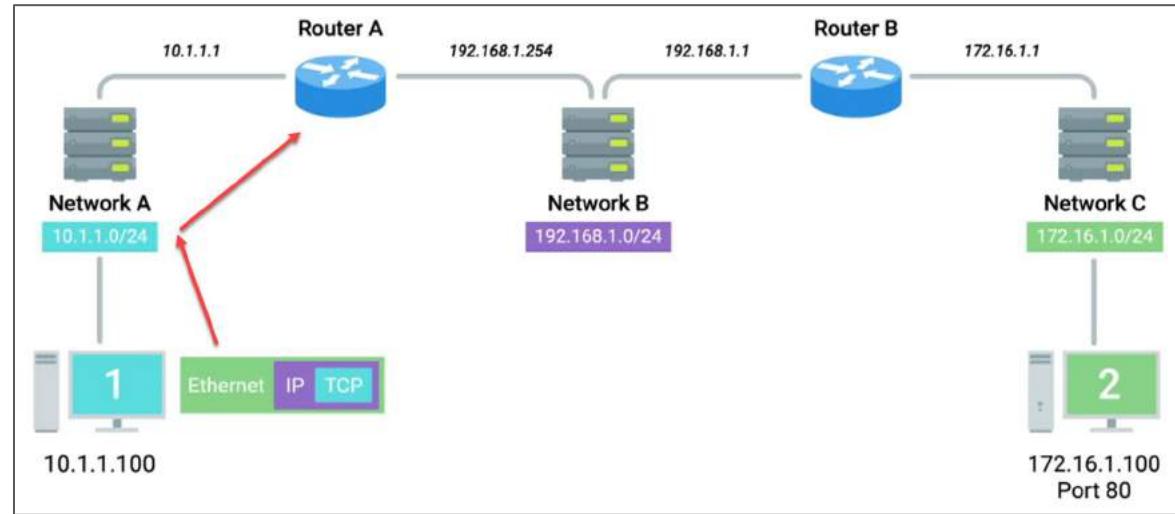
10. Tầng mạng đóng gói TCP datagram vào thành gói IP datagram.
- IP máy nguồn: 10.1.1.100
 - IP máy đích: 172.16.1.100
 - TTL (thời gian sống): giá trị chuẩn là 64
 - V.v....



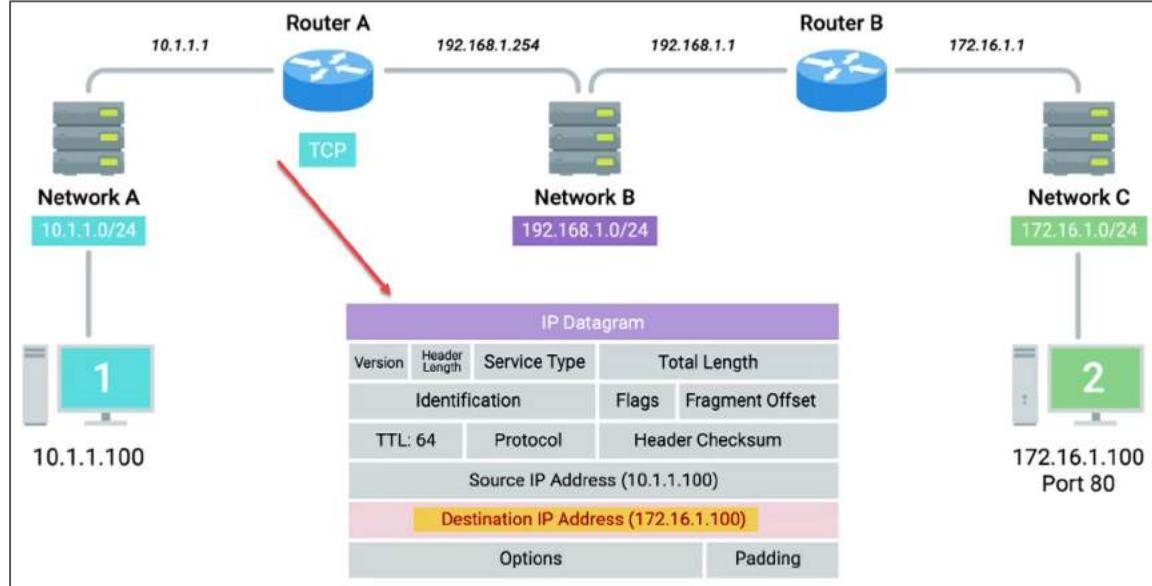
11. Tầng liên kết dữ liệu đóng gói IP datagram thành Ethernet Datagram
- MAC máy nguồn
 - MAC Router A
 - V.v....



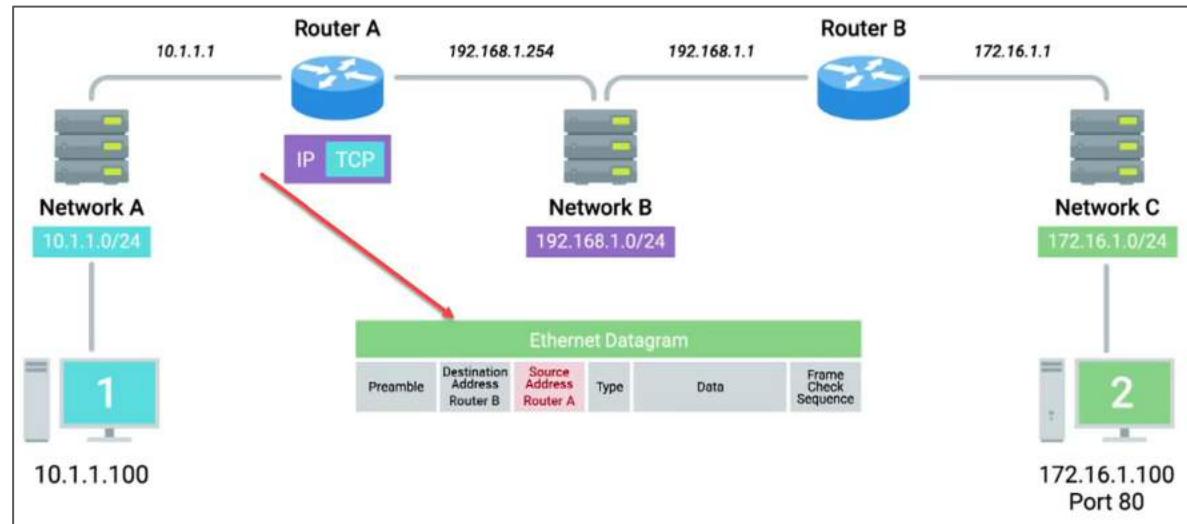
12. Máy 1 gửi nó đến Switch của mạng A và đến lượt Switch chuyển nó đến Router A



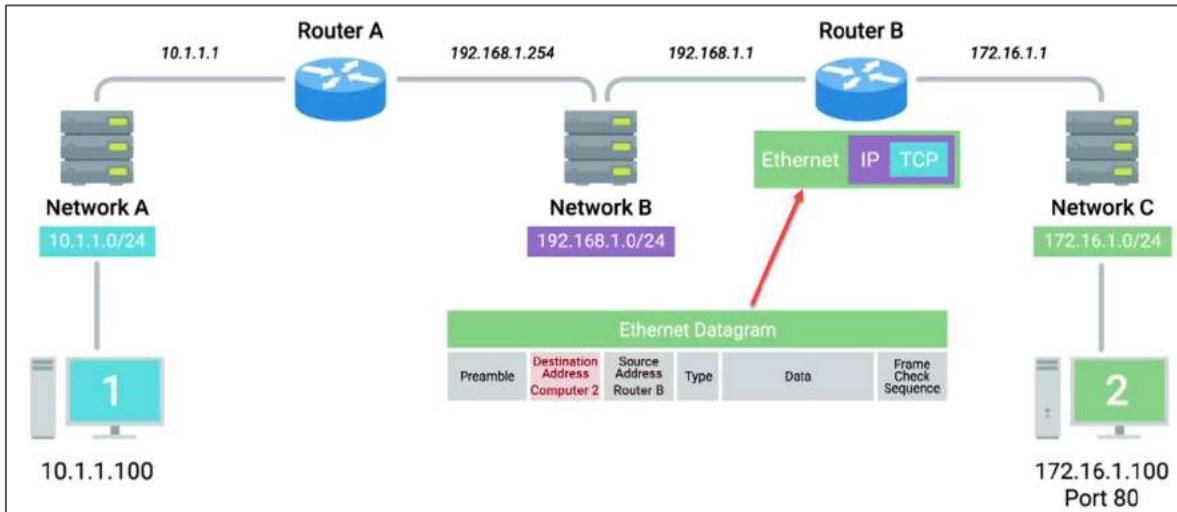
- 13. Router A bóc gói IP datagram và biết được địa chỉ IP đích mà nó cần gửi đến.
- 14. Dựa trên IP, Router A biết được máy đích thuộc mạng nào
- 15. Router A tra bảng định tuyến để biết đường đi đến mạng của máy đích. Kết quả, đường đi ngắn nhất là đi qua Router B



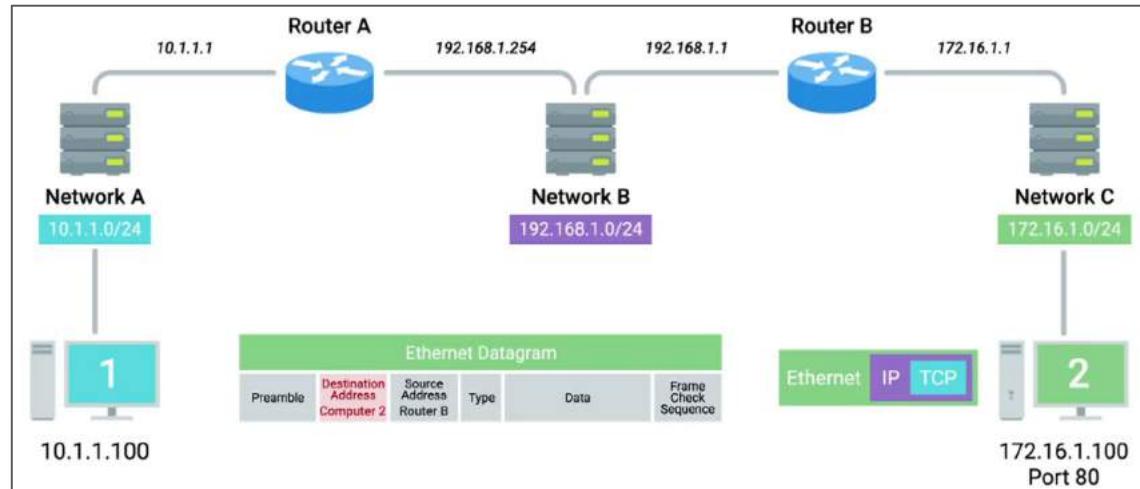
- 16. Để chuyển gói tin đến Router B, Router A tra bảng ARP cục bộ để xác định địa chỉ MAC của Router B.
- 17. Router A đóng gói lại gói tin Ethernet với địa chỉ MAC được cập nhật.
- 18. Router A gửi gói tin đi

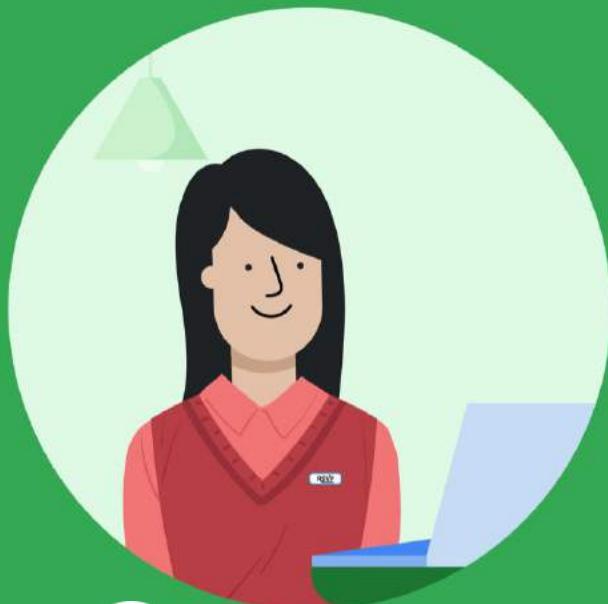


19. Khi gói tin đến Router B, Router B bóc gói tin ra và xác định được IP đích cần gửi đến, trong trường hợp này là IP của Máy 2.
20. Router B tra ARP và biết được địa chỉ MAC của Máy 2 nên cập nhật lại thông tin trên gói Ethernet.
21. Router B gửi gói tin đến Máy 2.



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





7 PHÂN GIẢI TÊN MIỀN



NỘI DUNG



Tên miền và hệ
thống phân giải



Máy chủ DNS



Giao thức DHCP



NAT và VPN



Máy chủ Proxy

Địa chỉ IP

Địa chỉ IP là số gồm 4 octet với mỗi octet được thể hiện bằng một con số thập phân có giá trị từ 0 đến 255.

- Mỗi octet là nhóm 8 bit (có thể xem là 1 byte)
- Tổng số địa chỉ IPv4 khoảng 4.2 tỷ địa chỉ

12.34.56.78

00001100.00100010.00111000.01001110

Liên lạc với server

Để liên lạc với server, chúng ta cần biết địa chỉ IP của nó.

Một số vấn đề:

- Nhớ địa chỉ IP là điều khó đối với con người
- Một tổ chức có thể dời server đến nơi khác, như vậy sẽ có IP mới

Tên miền (domain name)



Địa chỉ IP

115.73.213.165



Khó nhớ

Tên miền

<https://www.fit.hcmus.edu.vn/>



Dễ nhớ

Tên miền

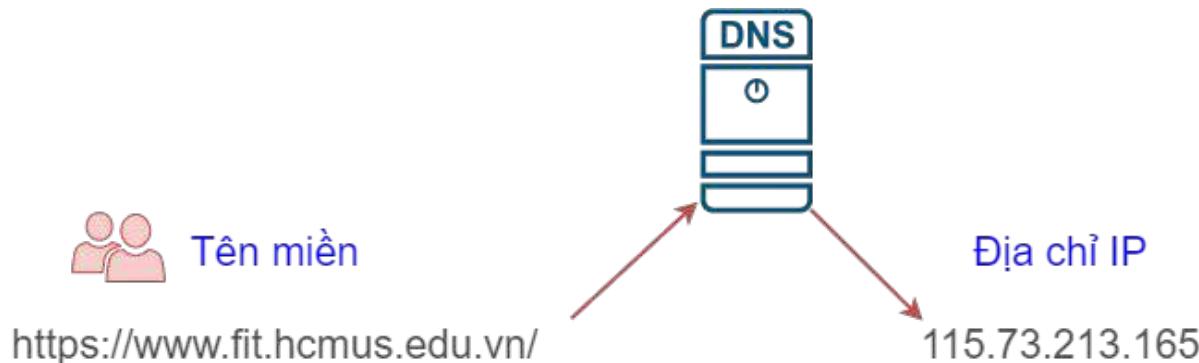
Tên miền (domain name) là một chuỗi ký tự chữ cái để đại diện cho những tài nguyên Internet mà đa số được đánh địa chỉ bằng số.

<https://en.wikipedia.org/wiki/Internet#Terminology>



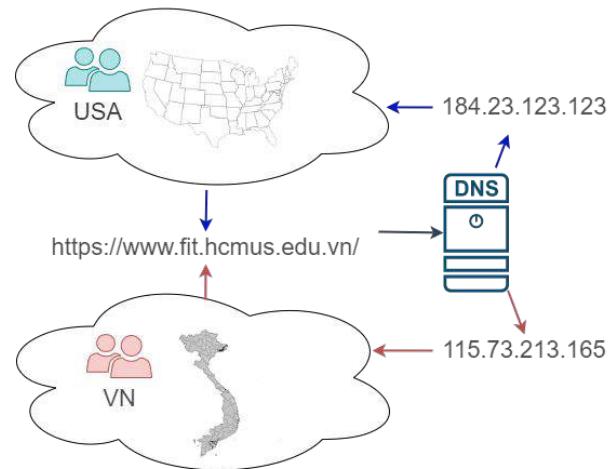
Hệ thống phân giải tên miền

Hệ thống phân giải tên miền (DNS – Domain Name System) là một dịch vụ mạng để biến đổi một chuỗi ký tự thành một địa chỉ IP.



Hệ thống phân giải tên miền

Một tổ chức có thể phân tán server ra nhiều vùng địa lý, DNS giúp người dùng truy cập đến server gần nhất.



NỘI DUNG



Tên miền và hệ
thống phân giải



Máy chủ DNS



Giao thức DHCP



NAT và VPN



Máy chủ Proxy

DNS Server

Máy chủ DNS (DNS Server) là máy tính chạy dịch vụ phân giải tên miền.

- Thường chứa một cơ sở dữ liệu của các IP và tên miền của chúng.
- Sử dụng một giao thức riêng để giao tiếp với các máy khác



Nguồn: Seobility

Các loại DNS Server

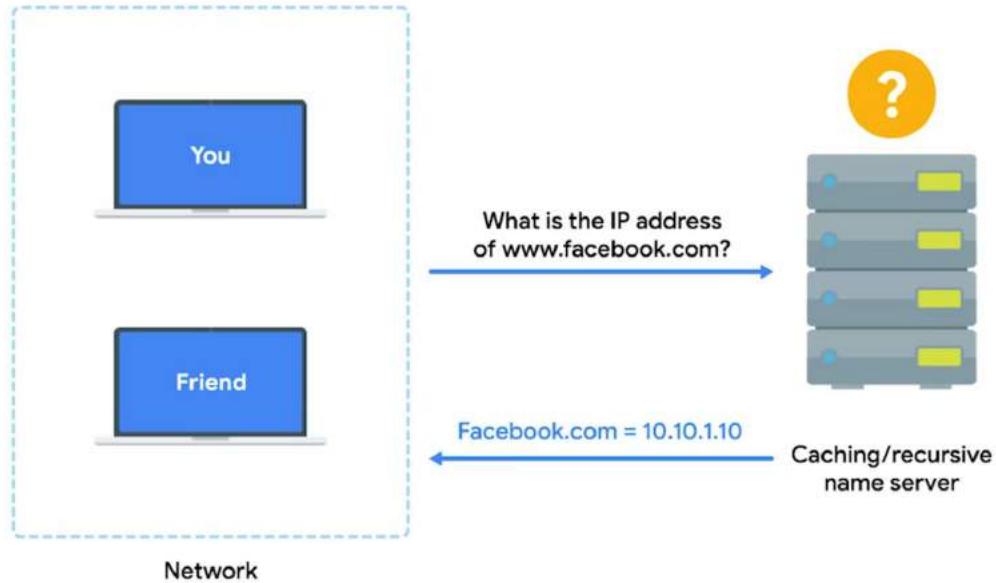
Có 5 loại DNS Server chính:

- Server tên miền đã lưu (caching name server)
- Server tên miền đệ quy (recursive name server)
- Server tên miền gốc (root name server)
- Server tên miền cấp cao (TLD name server)
- Server tên miền có thẩm quyền (authoritative name server)



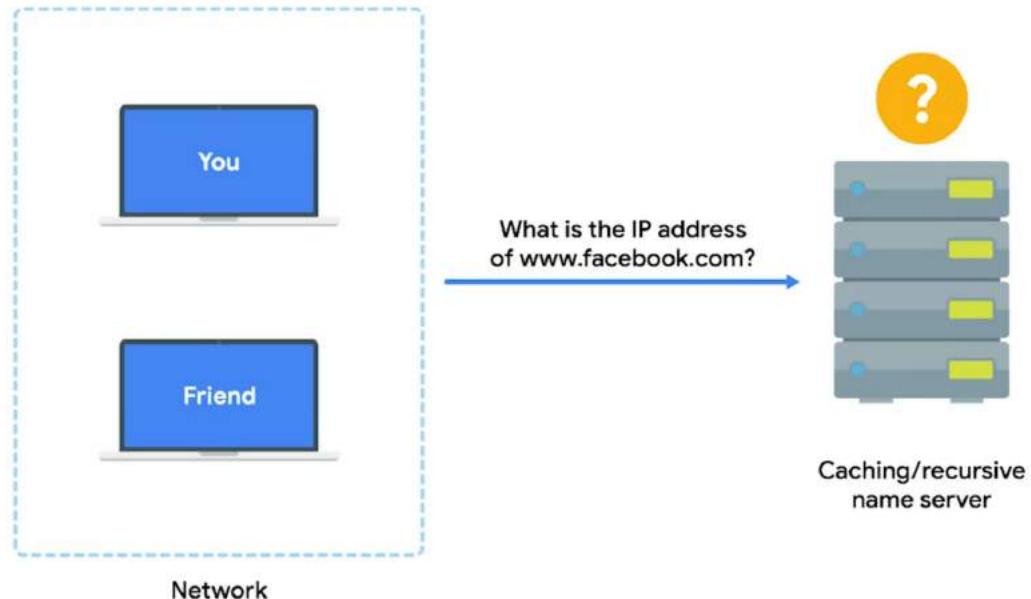
Phối hợp của các loại DNS Server

1. Người dùng muốn truy cập www.facebook.com
2. Yêu cầu được gửi đến Caching name server (CNS) để phân giải địa chỉ IP
3. Nếu CNS có lưu trữ thông tin, nó sẽ trả về IP cho người dùng



Phối hợp của các loại DNS Server

3. Nếu CNS không có, server tên miền đệ quy (RNS) sẽ bắt đầu hoạt động.

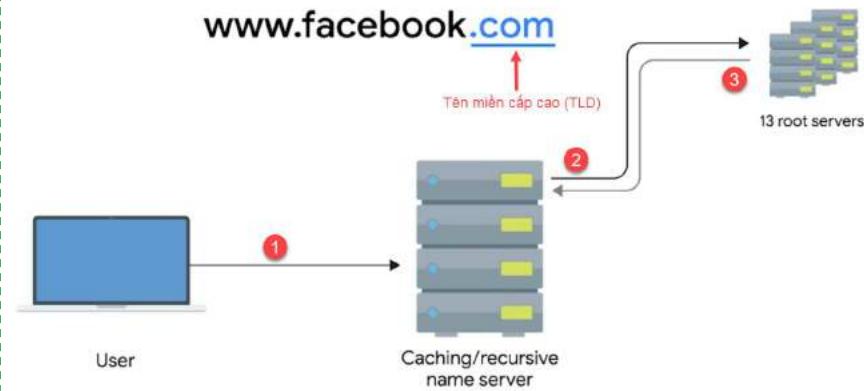


Phối hợp của các loại DNS Server

4. RNS liên lạc với một trong 13 server gốc (RS) bằng kỹ thuật anycast.

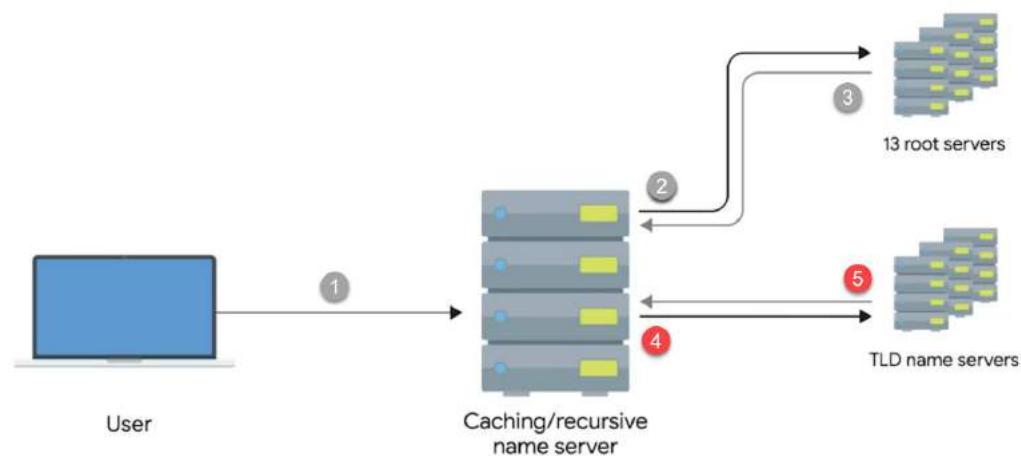
- Anycast là kỹ thuật được sử dụng để định tuyến gói tin đến các điểm đích khác nhau phụ thuộc trên các yếu tố như vị trí, độ nghẽn hay tình trạng liên kết.

5. RS chỉ định một server tên miền cấp cao (TLD_NS) để xử lý tiếp yêu cầu. Server tên miền cấp cao phụ thuộc vào đuôi tên miền.



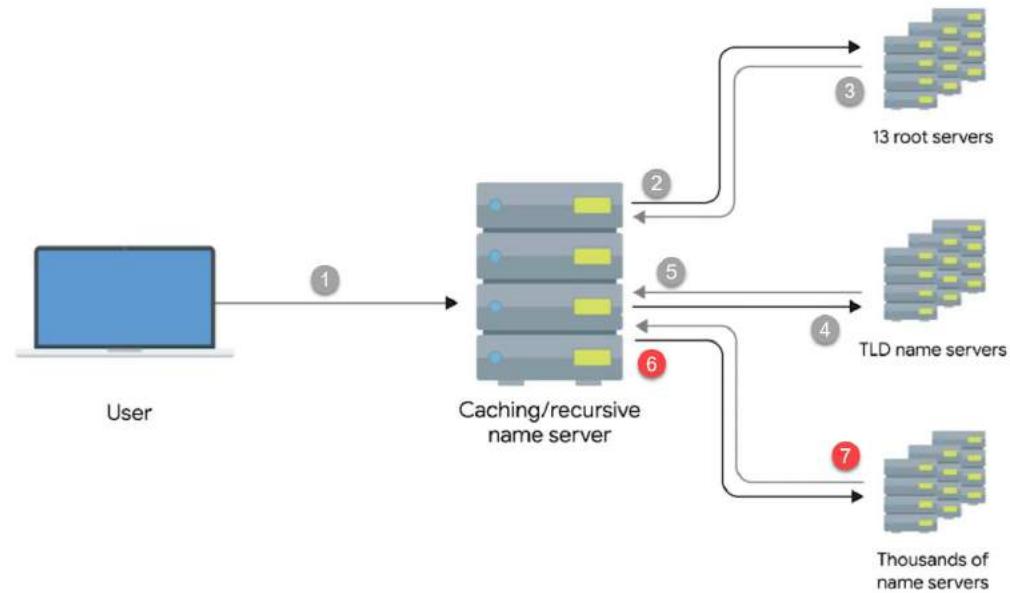
Phối hợp của các loại DNS Server

6. RNS biết được TLD_NS nên liên lạc tới server này để hỏi thông tin.
7. TLD_NS khi nhận được yêu cầu sẽ tra cứu một DNS tên miền có thẩm quyền (ANS) có thể trả lời IP của trang web và trả về cho RNS.



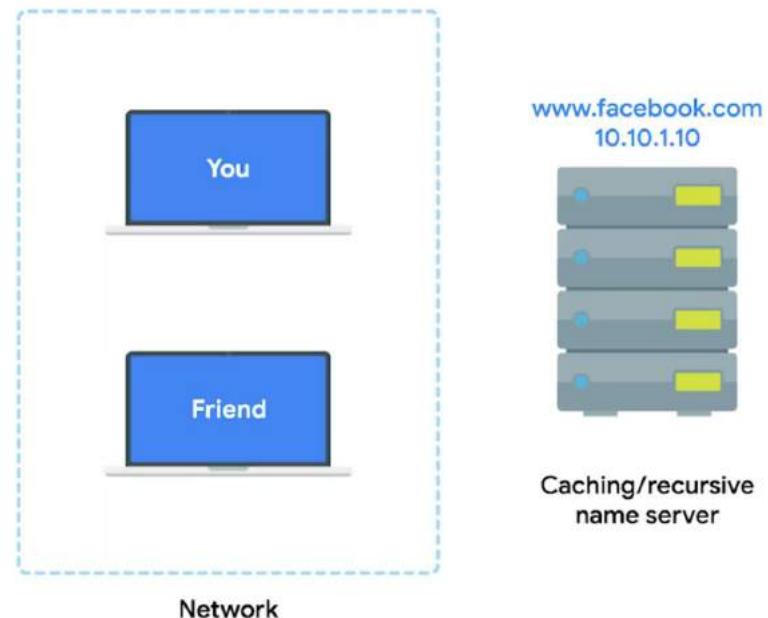
Phối hợp của các loại DNS Server

8. RNS tiếp tục liên lạc với ANS để hỏi IP cụ thể của trang web.
9. ANS tra cứu cơ sở dữ liệu và trả về địa chỉ IP của trang web.
10. RNS lưu lại thông tin vào bộ nhớ để dành trả lời cho truy vấn lâu sau (nếu có)



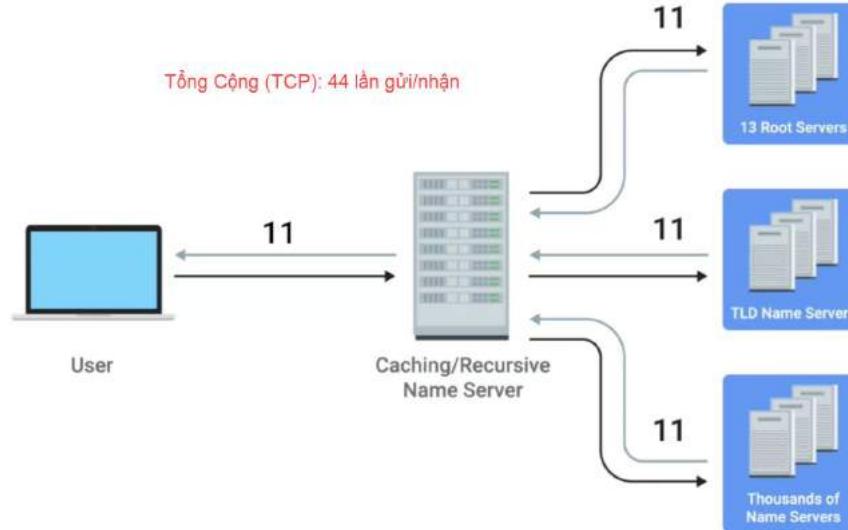
Phối hợp của các loại DNS Server

- 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 server.



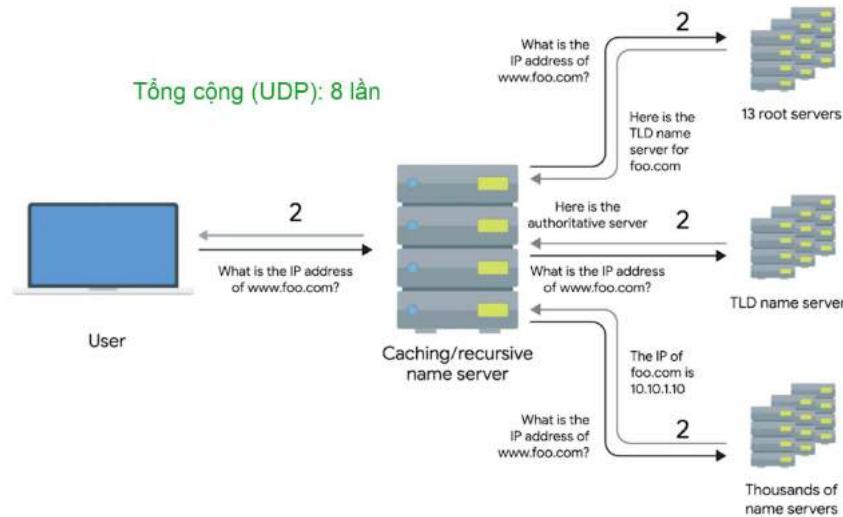
Giao thức của DNS server

Nếu DNS sử dụng giao thức TCP trên cổng 53 để thực hiện phân giải tên miền thì nó tốn rất nhiều lần gửi và nhận gói tin.



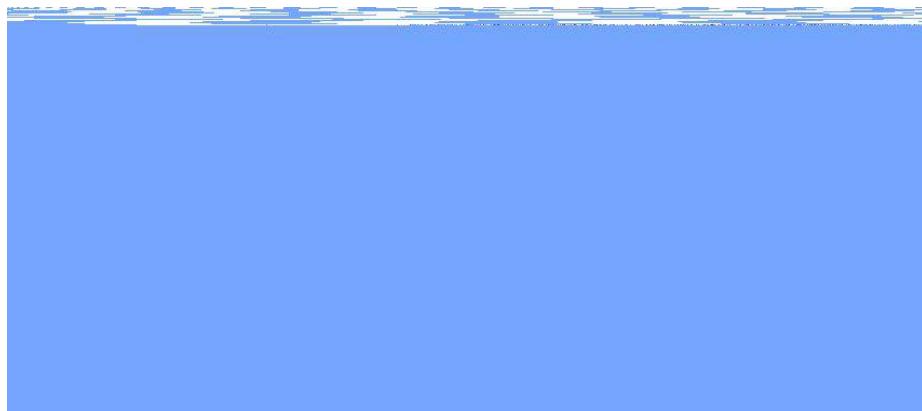
Giao thức của DNS server

DNS server sử dụng giao thức UDP trên cổng 53 để thực hiện phân giải tên miền sẽ tốn ít số lần gửi/nhận gói tin.



Giao thức của DNS server

- 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 DNS server

DNS Server lưu **thông tin phân giải tên miền** trong các **bản ghi** của cơ sở dữ liệu. Mỗi bản ghi được gọi là một **resource record (RR)**

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..)

Loại bản ghi

Có rất nhiều loại bản ghi tài nguyên nhưng phổ biến:

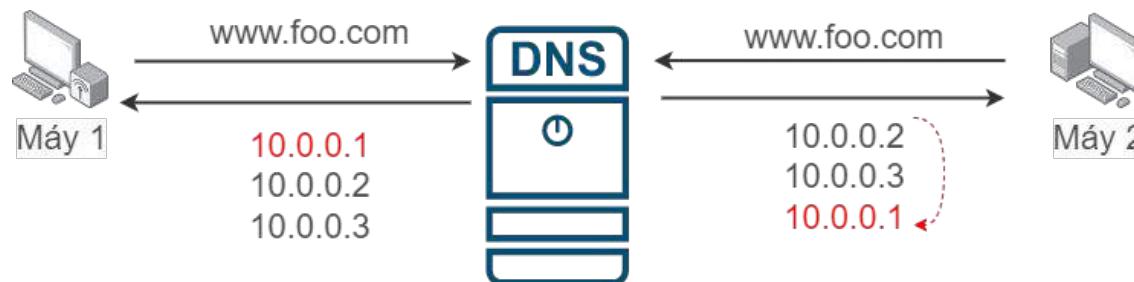
- Loại **A**: ánh xạ tên miền đến địa chỉ IPv4
- Loại **AAAA**: ánh xạ tên miền đến địa chỉ IPv6
- Loại **CNAME**: chuyển tiếp tên miền sang một tên miền khác
- Loại **MX (Mail Exchange)**: chuyển dịch vụ email đến server xác định
- Loại **SRV**: định nghĩa vị trí của các dịch vụ khác
- Loại **TXT**: chứa văn bản mô tả thông tin server
- Loại **NS**: mô tả server tên miền được cấp quyền cho một miền/miền con
- Loại **SOA**: thông tin phân quyền từ phía máy chủ tiếp nhận tên miền



Nhiều bản ghi cho một 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).

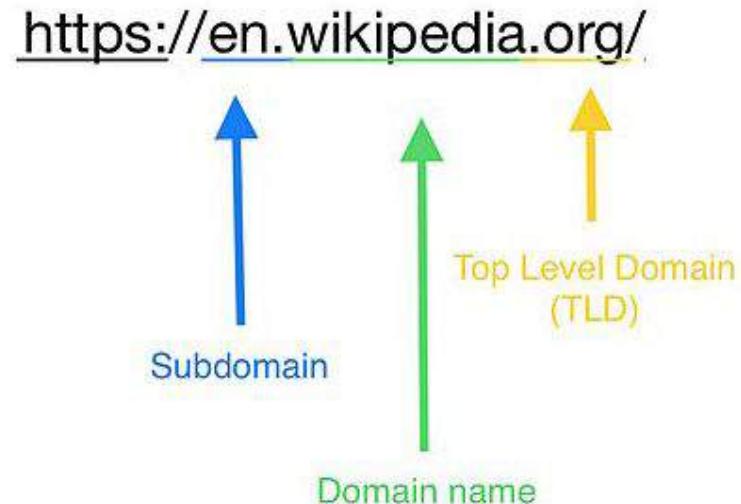
Name	Type	Data
www.foo.com	A	10.0.0.1
www.foo.com	A	10.0.0.2
www.foo.com	A	10.0.0.3



Cấu tạo tên miền

Tên miền bao gồm 3 thành phần chính:

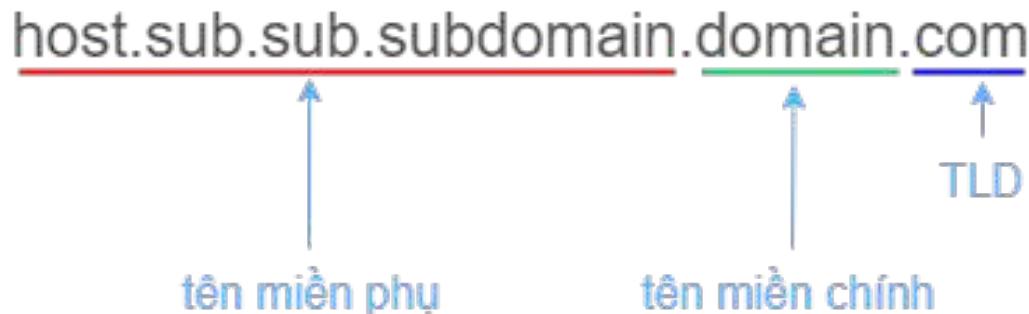
- **Tên miền cấp cao** (TLD – Top Level Domain)
 - Được cấp phát và quản lý bởi tổ chức ICANN (Internet Corporation for Assigned Names and Numbers)
 - Ví dụ: .com, .net, .org, .vn
- **Tên miền chính** (domain name)
 - Được cấp phát và quản lý bởi tổ chức độc lập và có ký kết với ICANN
 - Ví dụ: google, facebook, wikipedia
- **Tên miền phụ** (subdomain, host name)
 - Tên máy chủ xử lý và được gán bởi nhà phát triển



Cấu tạo tên miền

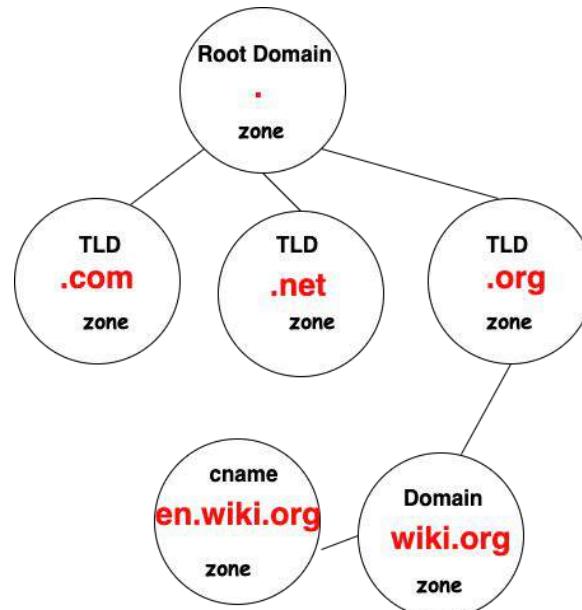
Một tên miền có đầy đủ 3 thành phần được gọi là **tên miền đủ điều kiện** (FQDN - Fully Qualified Domain Name)

- Mỗi nhãn (cách nhau bởi dấu chấm) tối đa 63 ký tự
- Độ dài giới hạn FQDN là 255 ký tự



DNS Zone

- Một tên miền có thể có nhiều tên miền con, để có thể quản lý tốt hơn, người ta **chia thành nhiều vùng khác nhau** và được gọi là **DNS Zone**.
- DNS Zone có **cấu trúc phân tầng dạng cây**.



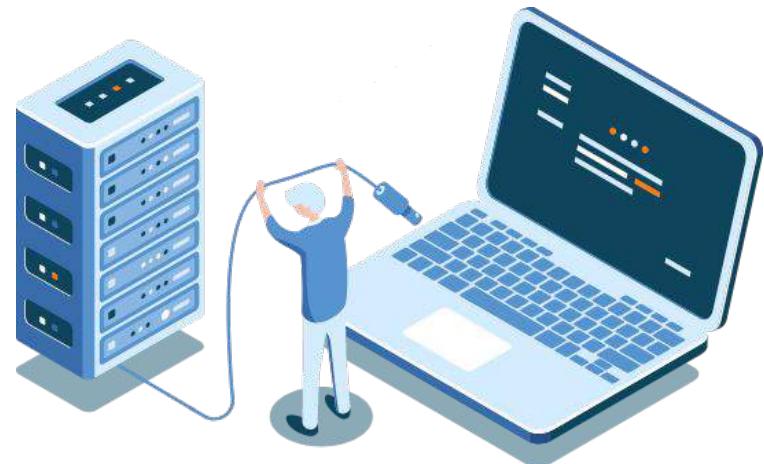
DNS Zone

DNS Zone được cấu hình thông qua các **tập tin vùng** (zone file).

Các tập tin vùng chứa các bảng ghi tài nguyên như:

- SOA (Start of Authority)
- NS (name server)
- A, AAAA, CNAME

Một loại tập tin đặc biệt là **tập tin vùng tra cứu ngược** (reverse lockup zone file) chứa bản ghi con trỏ (PTR) để **chuyển IP ngược lại thành tên miền**



NỘI DUNG



Tên miền và hệ
thống phân giải



Máy chủ DNS



Giao thức DHCP



NAT và VPN

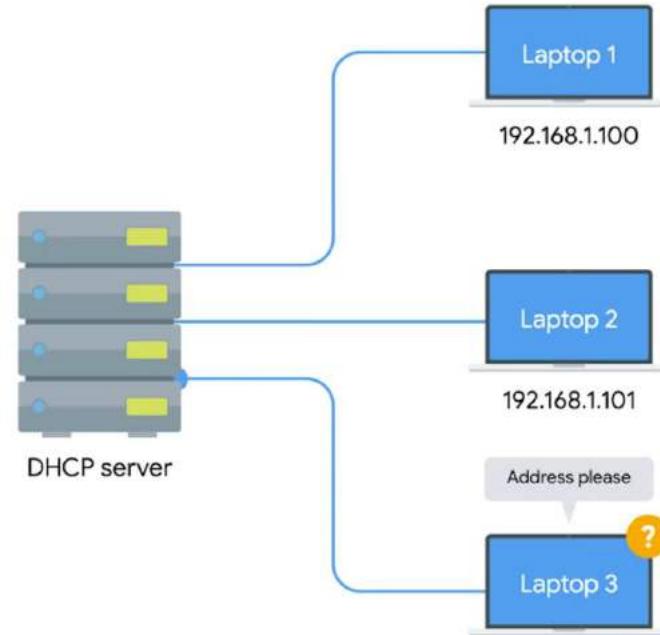


Máy chủ Proxy

Giao thức DHCP

DHCP (Dynamic Host Configuration Protocol) là giao thức **tự động tiến trình cấu hình** cho các máy trong mạng.

- Khi một máy kết nối đến mạng, nó có thể hỏi máy chủ DHCP để nhận tất cả cấu hình mạng



Cách cấp phát IP của DHCP

DHCP có 3 cách khác nhau để cấp phát địa chỉ IP:

- Cấp phát động (dynamic allocation)
- Cấp phát tự động (automatic allocation)
- Cấp phát cố định (fixed allocation)



Cách cấp phát IP của DHCP

DHCP có 3 cách khác nhau để cấp phát địa chỉ IP:

- Cấp phát động (dynamic allocation): một dãy các địa chỉ IP được gán đến các thiết bị; **mỗi lần** thiết bị kết nối **có thể** gán địa chỉ khác nhau.



Cách cấp phát IP của DHCP

DHCP có 3 cách khác nhau để cấp phát địa chỉ IP:

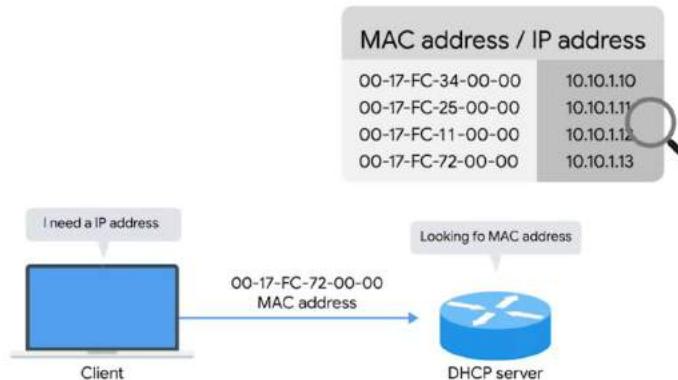
- **Cấp phát tự động** (automatic allocation): một dãy các địa chỉ IP được gán đến các thiết bị; nếu thiết bị đó đã được gán một địa chỉ IP nào đó trước đây rồi thì **địa chỉ IP này được sử dụng lại** để gán nếu chưa gán cho thiết bị khác.



Cách cấp phát IP của DHCP

DHCP có 3 cách để cấp phát địa chỉ IP:

- **Cấp phát cố định** (fixed allocation): một danh sách chứa **địa chỉ MAC và IP cố định** tương ứng được lưu trên DHCP server; khi thiết bị có địa chỉ MAC khớp với một cái trong danh sách, nó sẽ được gán IP đã được chỉ định trước.
- Nếu không tìm thấy, DHCP có thể chuyển sang chế độ động, hoặc tự động, hoặc có thể từ chối gán.



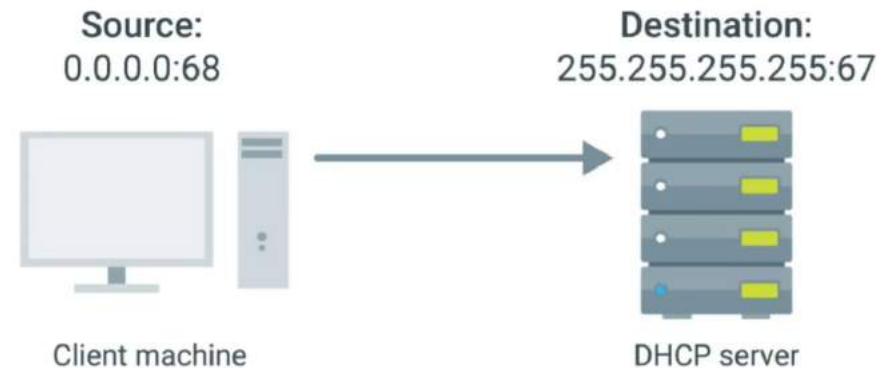
Tìm kiếm DHCP server

Máy tính khi mới kết nối sẽ **gửi một gói tin ra toàn mạng để tìm DHCP server.**

- Gói tin này được gọi là **DHCPDISCOVER**

Theo quy ước, gói tin **DHCPDISCOVER**:

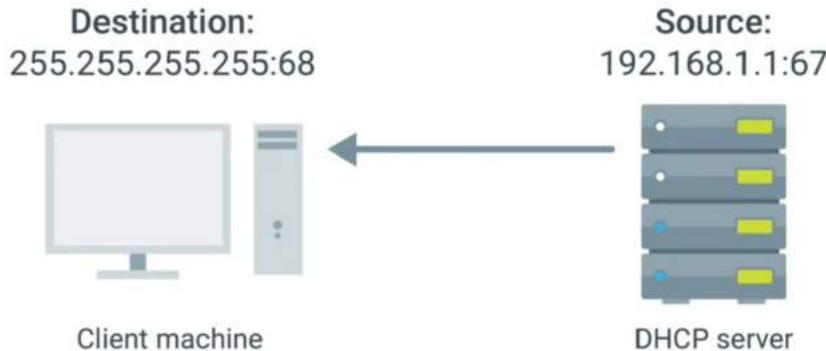
- **DHCP server lắng nghe** gói tin **UDP** trên **cổng 67** và **máy tính gửi** gói tin **DHCPDISCOVERY** từ **UDP cổng 68**.
- Địa chỉ IP đích là 255.255.255.255 (FF:FF:FF:FF:FF:FF), IP nguồn là 0.0.0.0



Tìm kiếm DHCP server

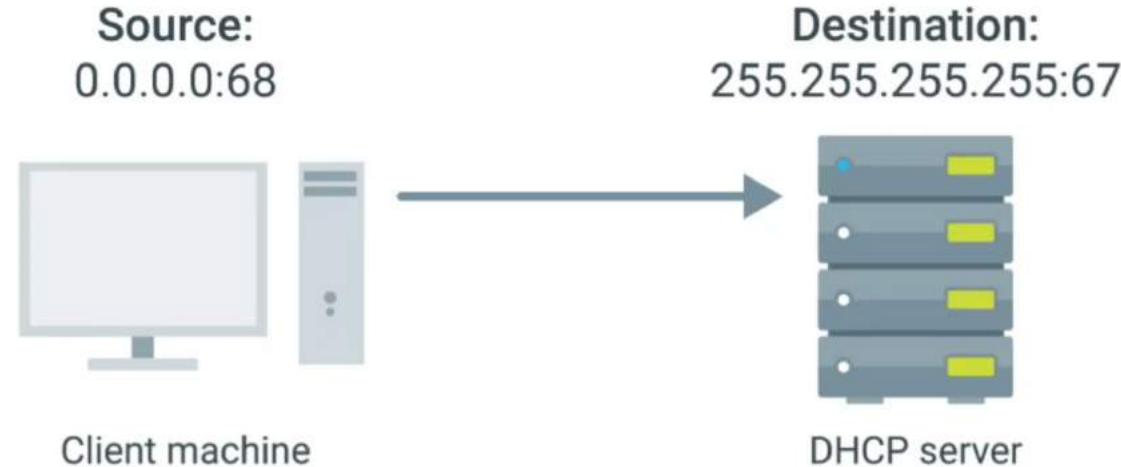
DHCP server nhận và phản hồi với **gói tin DHCPOFFER** gồm:

- Port đích là 68, port nguồn là 67
- IP đích: 255.255.255.255, IP nguồn là IP thực sự của DHCP server
- Thông tin cấu hình máy



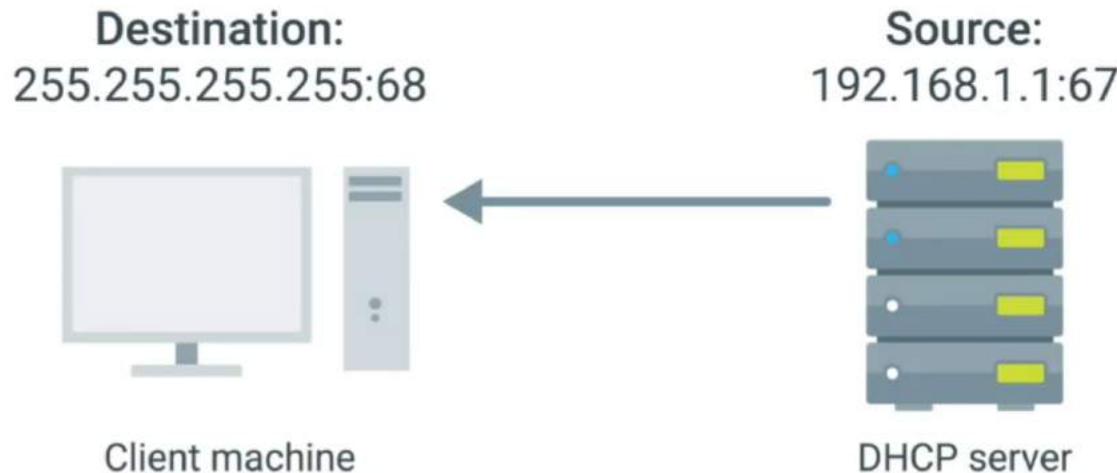
Tìm kiếm DHCP server

Máy tính gửi tiếp gói tin **DHCPREQUEST** để đồng ý với IP được cấp



Tìm kiếm DHCP server

Cuối cùng, DHCP server nhận được gói tin sê phản hồi gói tin **DHCPACK** để xác nhận.



NỘI DUNG



Tên miền và hệ
thống phân giải



Máy chủ DNS



Giao thức DHCP



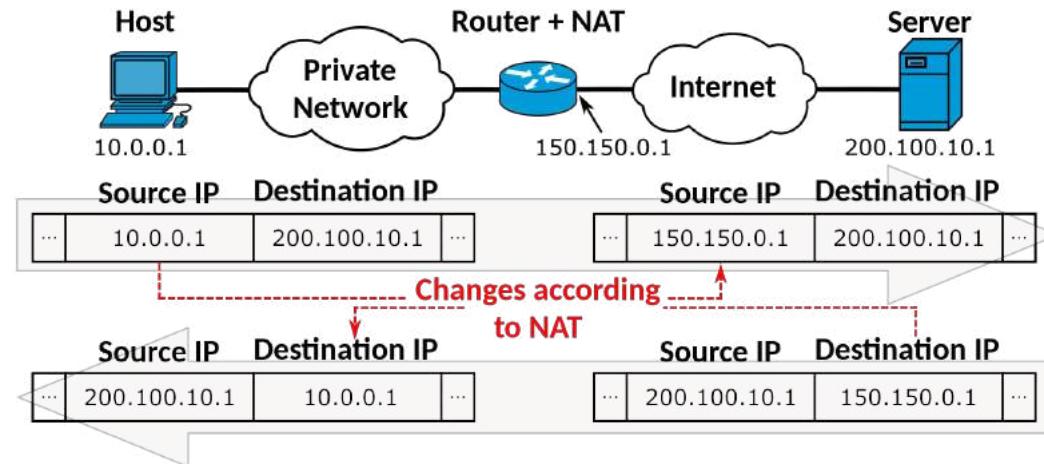
NAT và VPN



Máy chủ Proxy

NAT

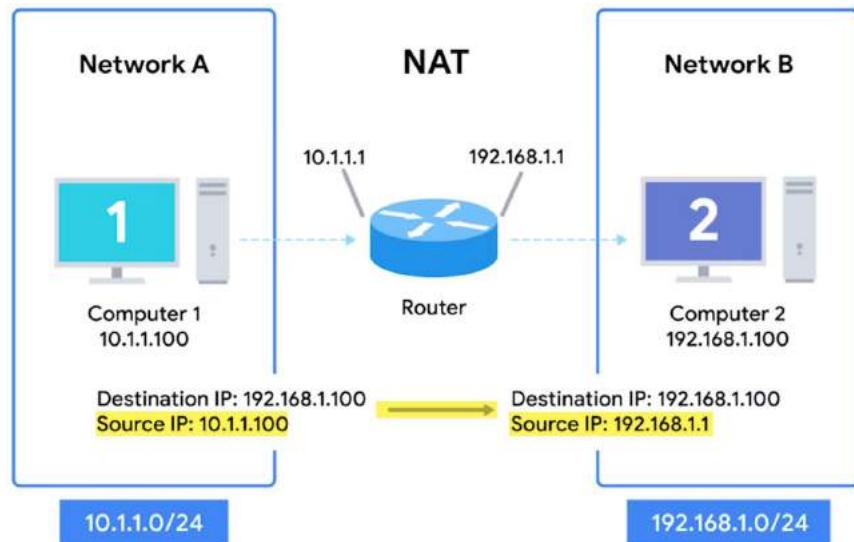
Biên dịch địa chỉ mạng (NAT- Network Address Translation) là quá trình **thay đổi** địa chỉ IP thành một địa chỉ khác khi gói tin đi qua **router** hoặc **firewall**



Cách hoạt động của NAT

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.

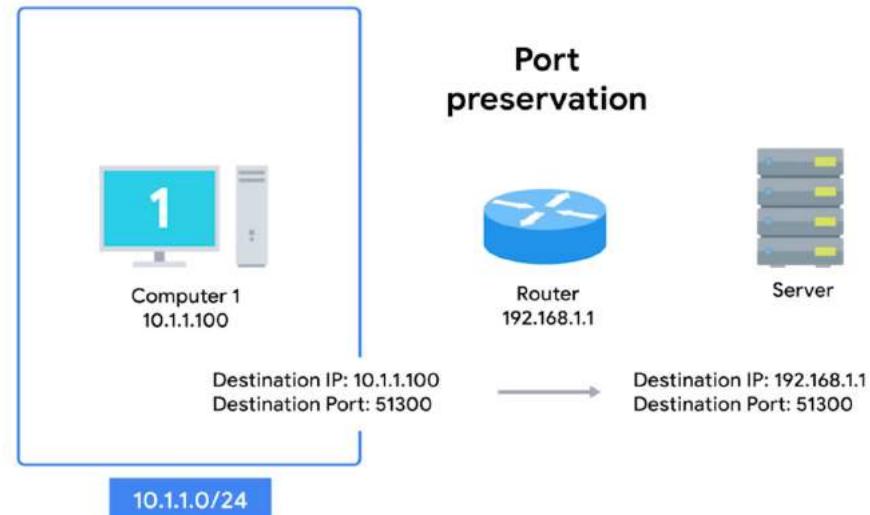
- Cách hoạt động này được gọi là **giả mạo IP** (IP masquerading)
- Đây là NAT dạng 1-Nhiều (one-to-many)



Cách hoạt động của NAT

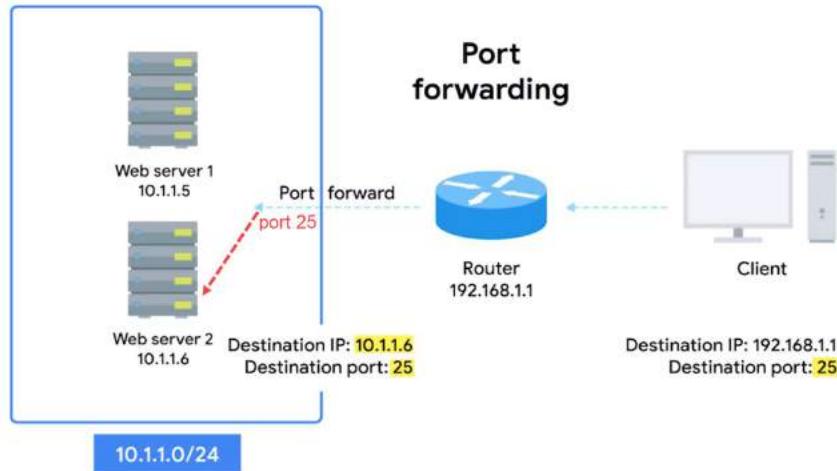
Để biết trả gói tin về cho máy nào, router sử dụng kỹ thuật được gọi là duy trì cổng (**port preservation**).

- Mỗi máy khi gửi gói tin đều khởi tạo một socket với port được đánh số tạm trong đoạn từ 49.152 đến 65.535.
- Port preservation là kỹ thuật **giữ nguyên** port máy nguồn khi qua router, chỉ đổi địa chỉ IP.



Cách hoạt động của NAT

Chuyển tiếp cổng (port forwarding) là kỹ thuật để chuyển các gói tin có cổng cụ thể luôn về một máy xác định



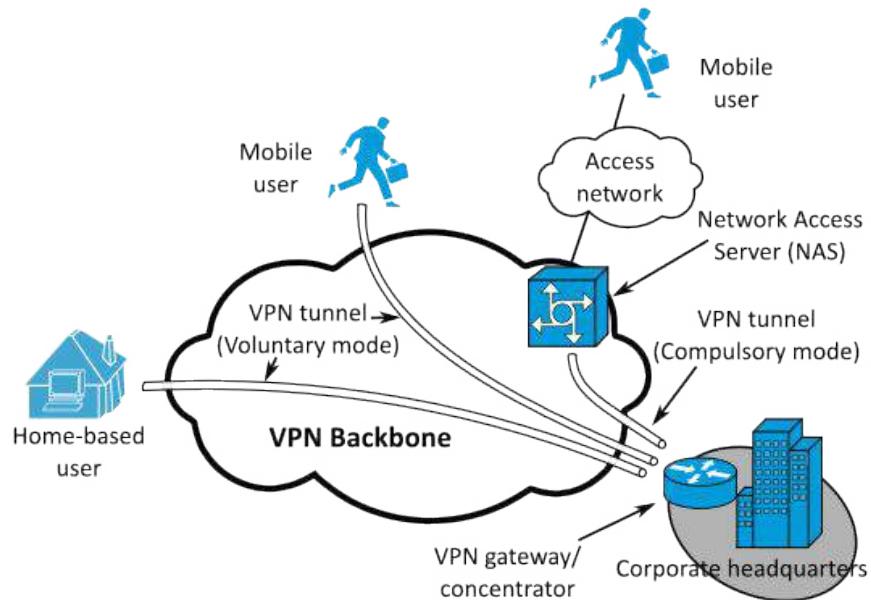
NAT + Không gian địa chỉ không thể định tuyến

- 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 phối hợp với 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 IP**.



VPN

Mạng riêng ảo (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.



VPN

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 chỉ một tên người dùng và một mật khẩu.



NỘI DUNG



Tên miền và hệ
thống phân giải



Máy chủ DNS



Giao thức DHCP



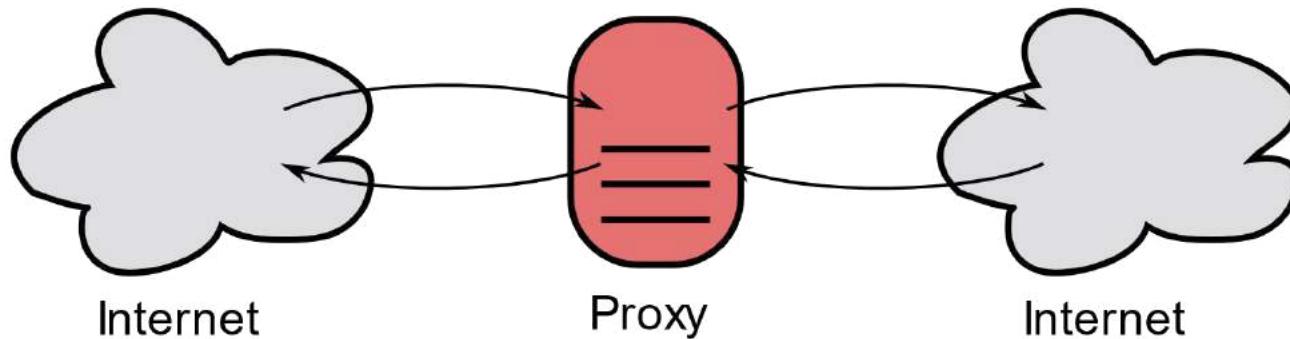
NAT và VPN



Máy chủ Proxy

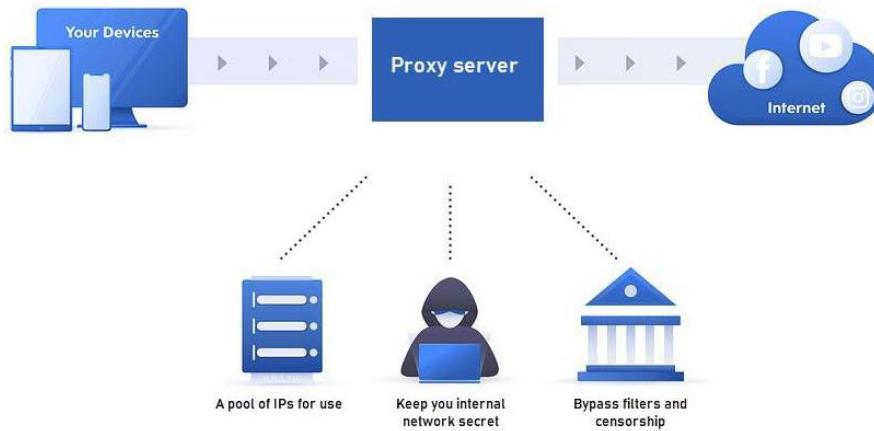
Proxy server

Proxy server là một server đóng vai trò như một client để truy xuất một dịch vụ



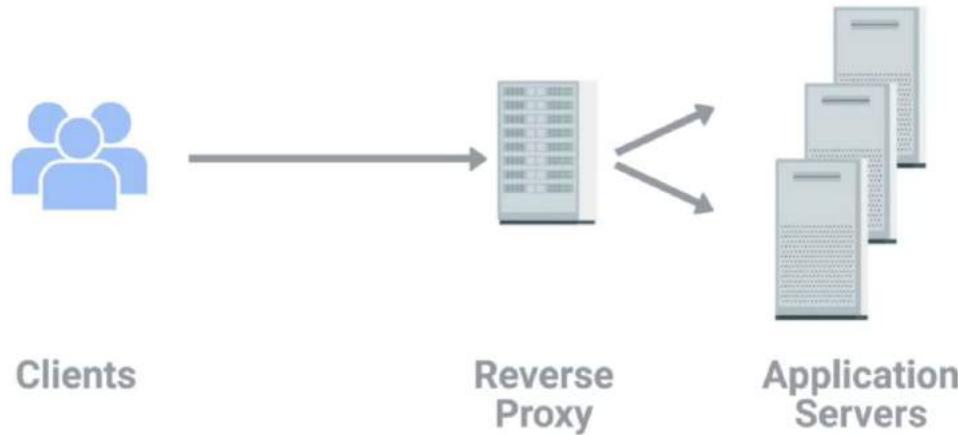
Web proxy

Web proxy được sử dụng như máy trung gian để lưu trữ tạm nội dung web và kiểm soát việc truy cập internet của máy khách.



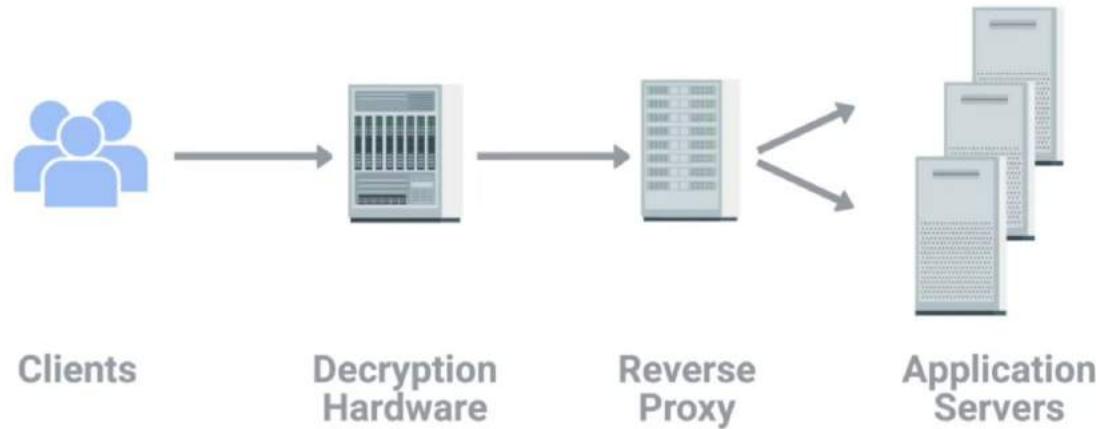
Reverse proxy

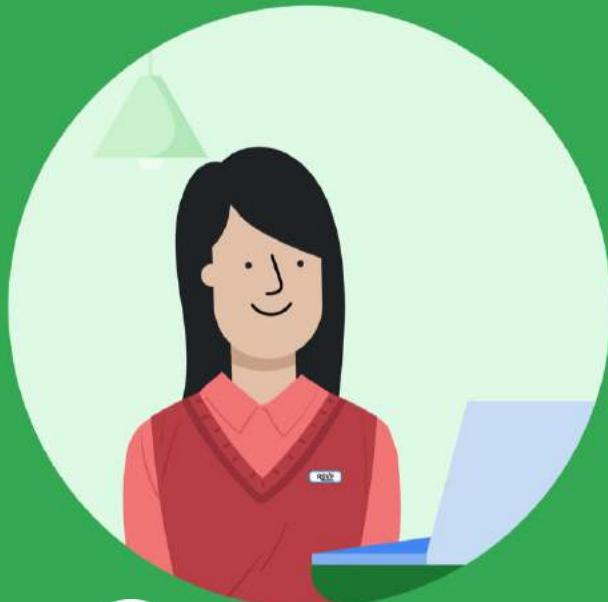
Reverse proxy được sử dụng để **thể hiện** một server duy nhất đến người dùng nhưng **bên trong** là một loạt các server cùng thực hiện



Reverse proxy

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





8 KẾT NỐI QUAY SỐ VÀ BĂNG THÔNG RỘNG



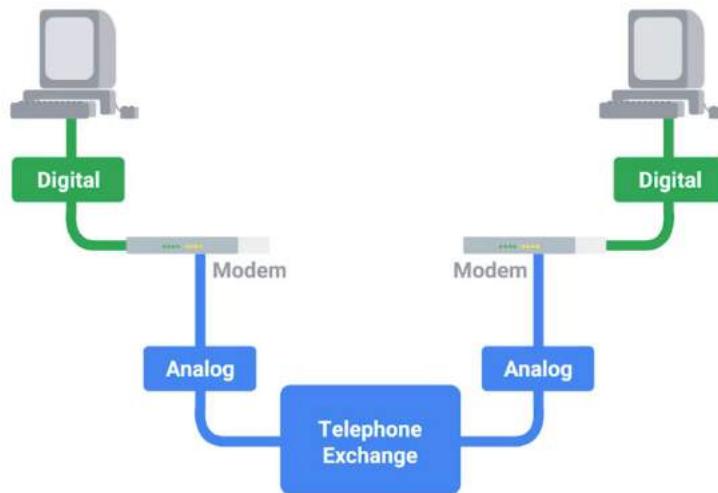
POTS

- 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).
- 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.



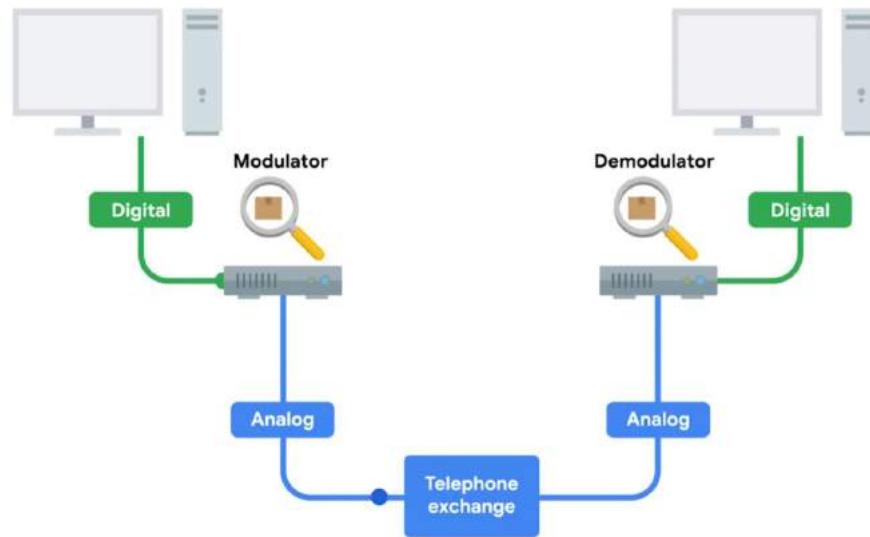
Kết nối quay số

- Một **kết nối quay số** sử dụng POTS để truyền dữ liệu được khởi tạo bằng cách thực hiện **quay số điện thoại**.
- Thiết bị thực hiện quay số được gọi là **modem**



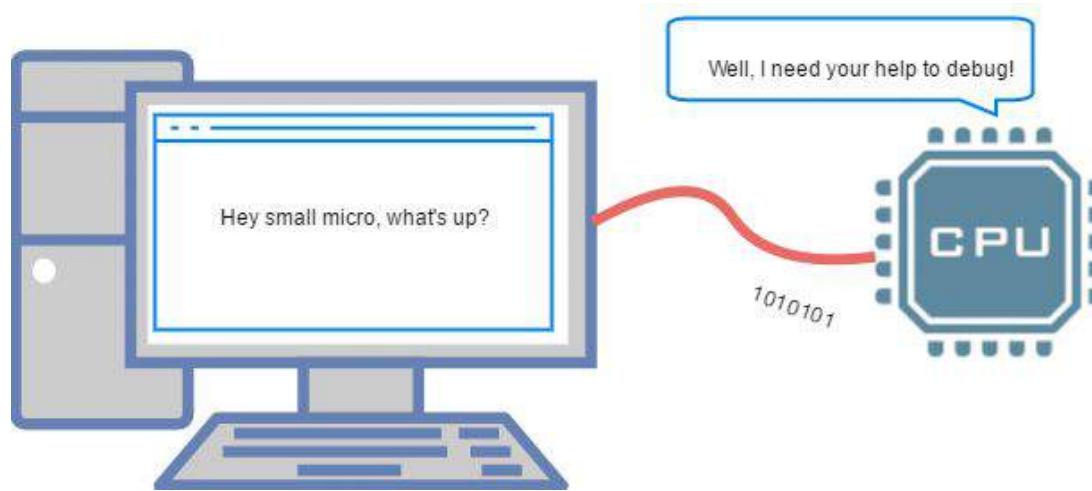
Modem

Modem (Modulator Demodulator) nhận dữ liệu ở dạng máy tính có thể hiểu và chuyển chúng thành bước sóng âm nghe được (audible wavelength) sau đó chuyển đi qua POTS.



Tỷ lệ Baud

Tỷ lệ baud (baud rate) là độ đo số lượng bit có thể truyền qua đường dây điện thoại trong một giây



Băng thông rộng

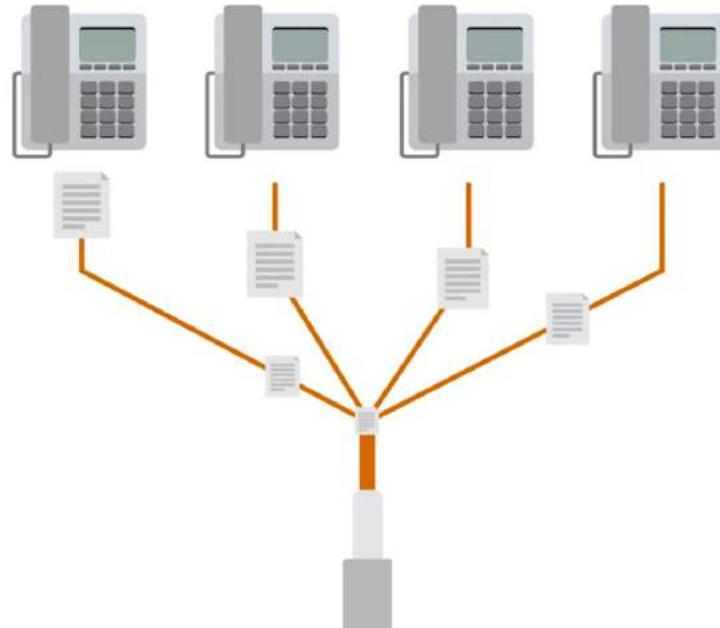
Băng thông rộng (broadband) là công nghệ truyền tải nhiều tín hiệu đồng thời, cho phép kết nối với tốc độ cao và luôn sẵn sàng



Công nghệ T-carrier

Công nghệ T-carrier là công nghệ cho phép **nhiều cuộc gọi thoại** được **dì chuyển** qua một sợi dây cáp **cùng lúc**.

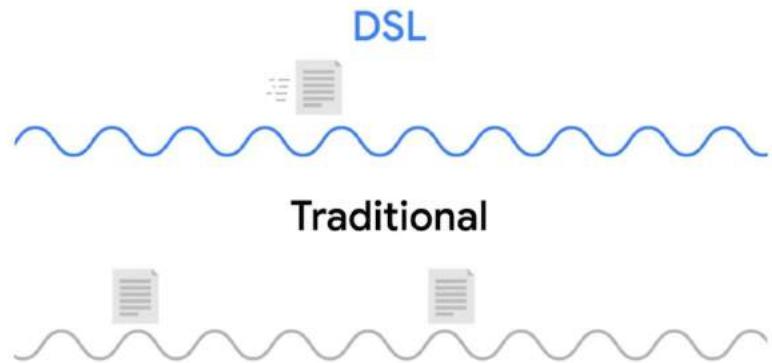
- Phiên bản T1 (**Transmission System 1**) mang 24 cuộc gọi điện thoại cùng lúc trên một cặp dây đồng xoắn.
- T1 đạt tốc độ **1.544 Mb/s** và cũng được sử dụng để truyền dữ liệu Internet.
- T3 gồm 28 đường T1, có thể đạt tốc độ 44.736 Mb/s



Đường thuê bao số

Đường thuê bao số (DSL - Digital Subscriber Line) thực hiện **truyền dữ liệu ở một miền tần số không giao thoa với cuộc gọi điện thoại**.

- Cho phép cuộc gọi điện thoại và truyền tải dữ liệu được diễn ra đồng thời
- Tốc độ nhanh hơn
- Modem được biết tới với tên **DSLAM** (Digital Subscriber Line Access Multiplexer)
- Chạy xuyên suốt



Đường thuê bao số

Có nhiều loại DSL nhưng nổi bật:

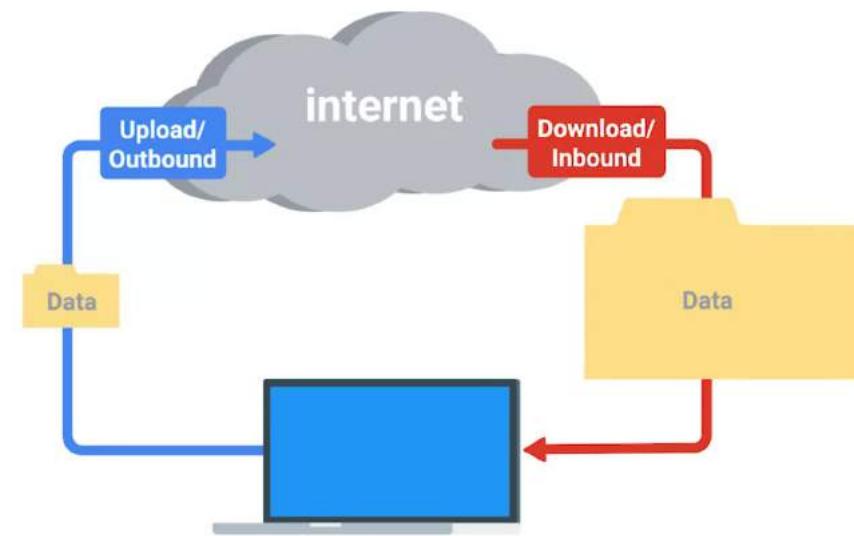
- ADSL (Asymmetric Digital Subscriber Line)
- SDSL (Symmetric Digital Subscriber Line)



Đường thuê bao số

Có nhiều loại DSL nhưng nổi bật:

- **ADSL** (Asymmetric Digital Subscriber Line): khác nhau giữa tốc độ tải lên (chậm) và tải xuống (nhanh).



Đường thuê bao số

Có nhiều loại DSL nhưng nổi bật:

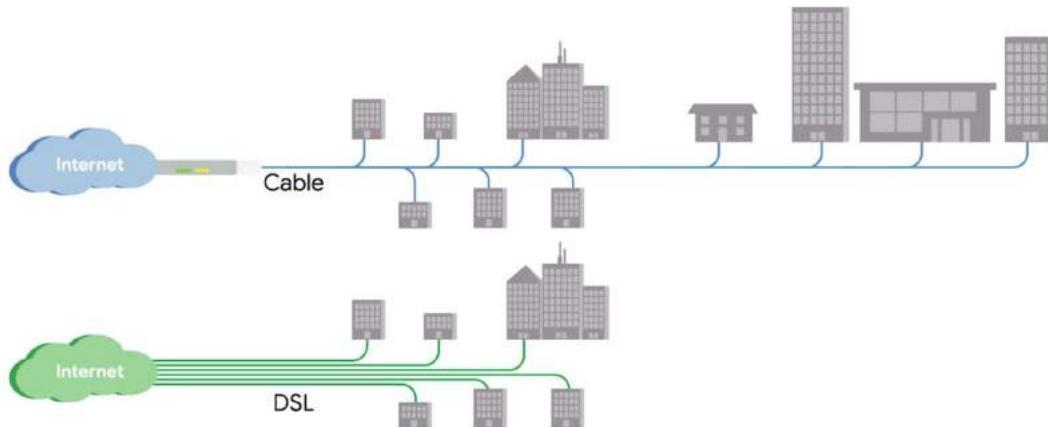
- SDSL (Symmetric Digital Subscriber Line): tốc độ tải lên và tải xuống bằng nhau
- Phù hợp với các máy chủ để cung cấp dữ liệu
- Phiên bản cải tiến HDHS (High Bit-rate Digital Subscriber Line) cho tốc độ nhanh hơn



Băng thông rộng cáp

Băng thông rộng cáp (cable broadband) cho phép **chia sẻ băng thông qua cùng sợi cáp**.

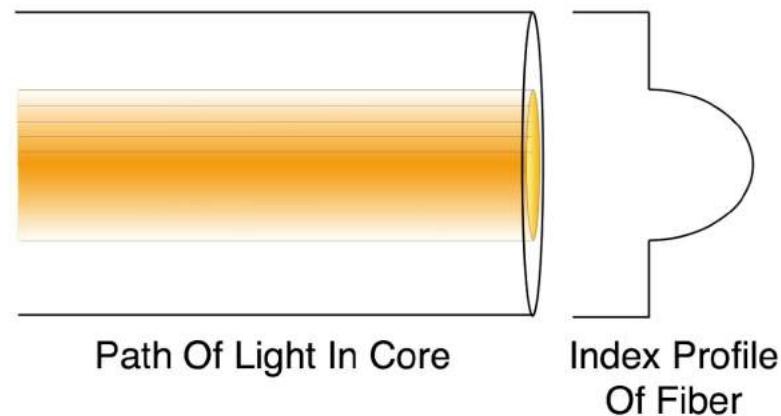
- **Cable modem** là thiết bị quản lý kết nối Internet và kết nối đến CMTS (cable modem termination system)



Kết nối sợi quang

Kết nối sợi quang (fiber connection) sử dụng ánh sáng để truyền tải dữ liệu thay vì dòng điện.

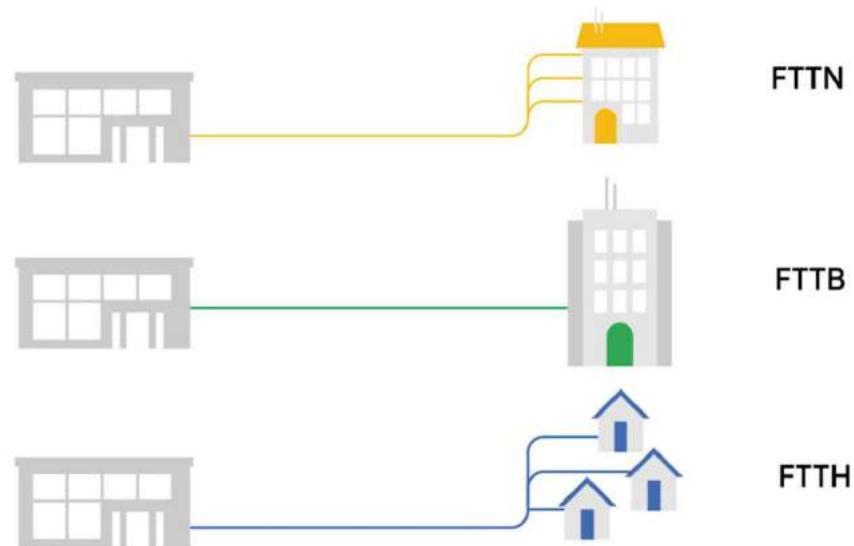
- Tốc độ nhanh
- Truyền tải đi xa trước khi tín hiệu bị suy giảm
- Chi phí sản xuất và lắp đặt cao



FTTX

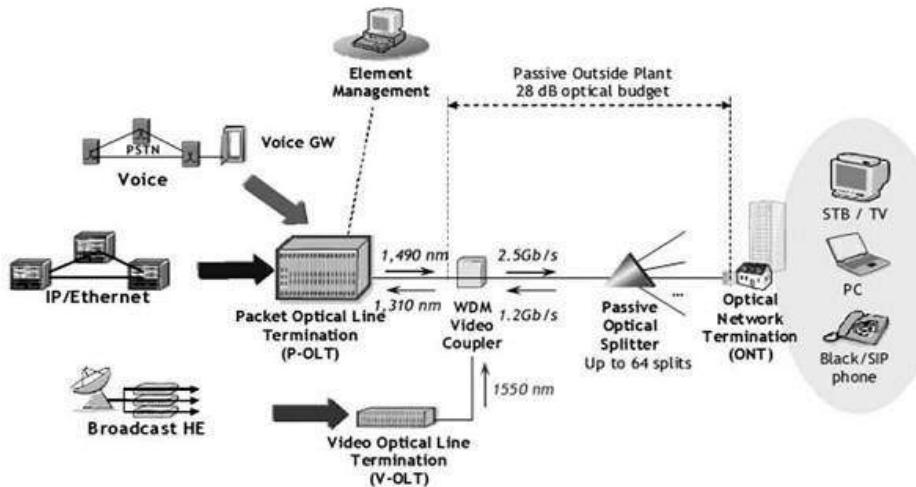
FTTX (Fiber to the X), nghĩa là mang kết nối quang phổ biến được đến đâu.

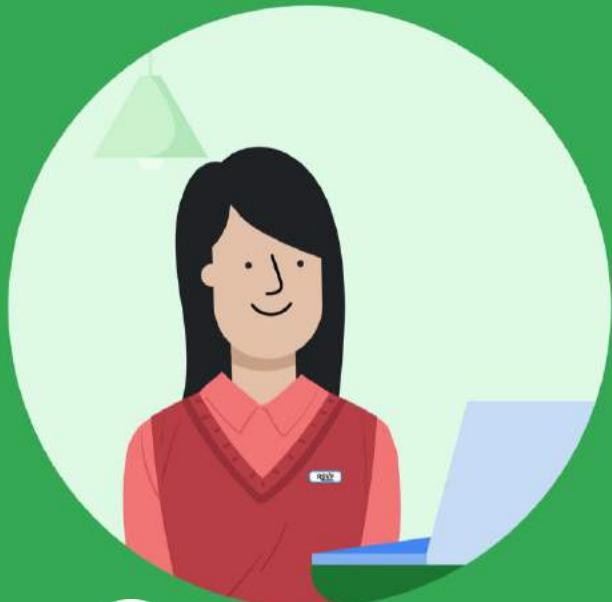
- **FTTN** (Fiber to the Neighborhood): kết nối quang đến được một **tủ vật lý trung tâm**.
- **FTTB** (Fiber to the Business): kết nối quang đến được **doanh nghiệp**
- **FTTH** (Fiber to the Home): kết nối được đến từng **hộ gia đình**
- **FTTP** (Fiber to the Premise) là tên gọi chung của FTTB và FTTH



Thiết bị chuyển đổi cho kết nối quang

Bộ đầu cuối mạng quang (ONT – Optical Network Terminator) được sử dụng để chuyển đổi tín hiệu trong kết nối quang thành các tín hiệu trong mạng cáp xoắn đôi truyền thống.





9

MẠNG DIỆN RỘNG MẠNG KHÔNG DÂY VÀ MẠNG VIỄN THÔNG



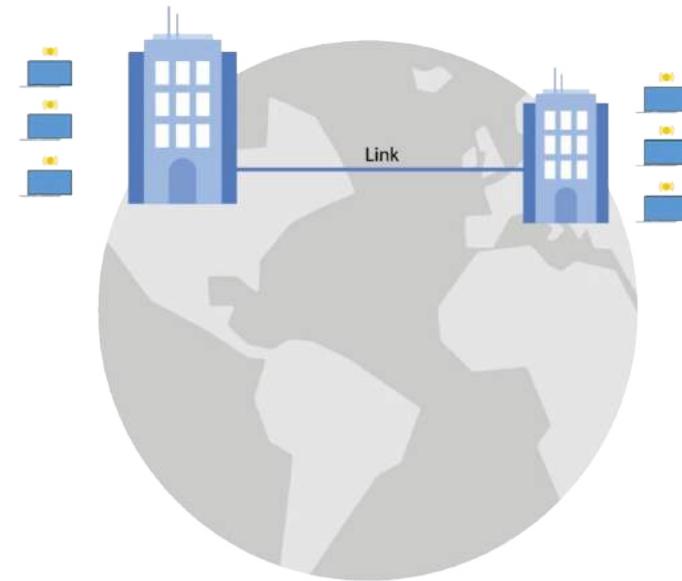
WAN

Mạng diện rộng (WAN – Wide Area Network) là công nghệ giúp các mạng làm việc với nhau như một mạng đơn nhất nhưng qua nhiều vị trí địa lý khác nhau.



Local loop

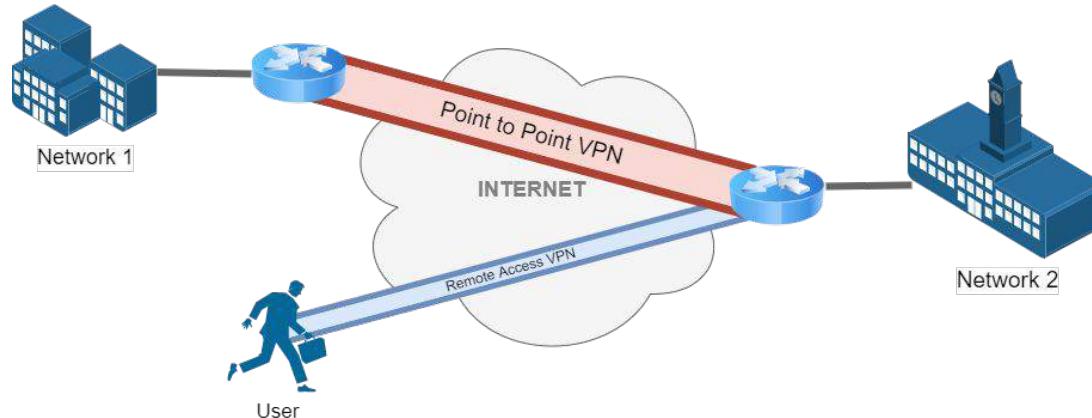
Local loop là một liên kết vật lý mà kết nối từ **điểm phân giới** (đầu cuối của mạng nội bộ trước khi ra ngoài) đến nhà cung cấp dịch vụ ISP.



Point-to-point VPN

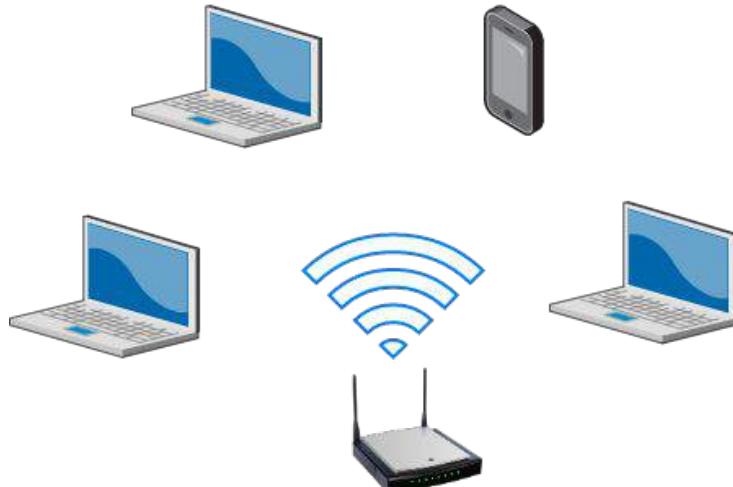
Point-to-point VPN (site-to-site VPN) là một dạng VPN dùng để kết nối nhiều mạng với nhau.

- Đường ống VPN được khởi tạo ở cả hai chiều.



Mạng không dây

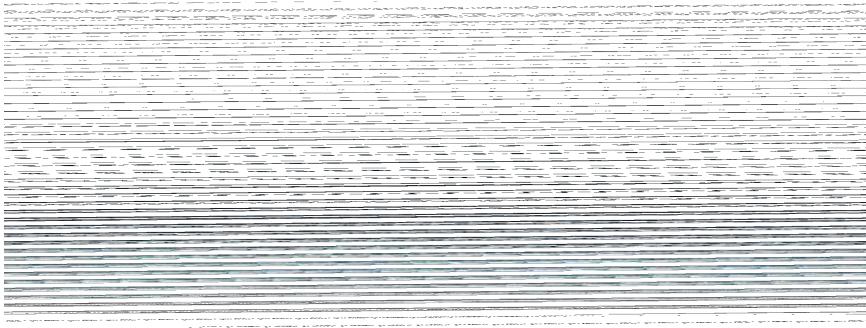
- Mạng không dây (wireless network) là cách thức kết nối mạng mà không cần dây dẫn.
- Các thiết bị mạng không dây kết nối với nhau qua sóng vô tuyến.



Chuẩn mạng không dây

Mạng không dây được đặc tả dưới **hệ chuẩn IEEE 802.11**.

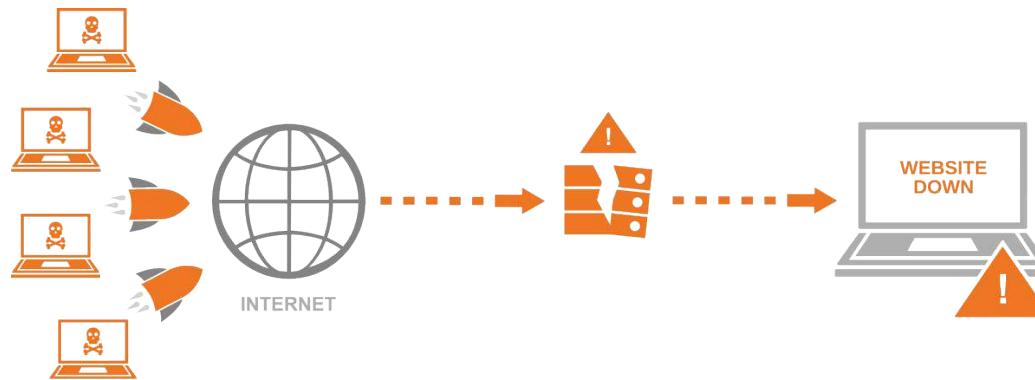
- Một số chuẩn cụ thể: 802.11a/b/g/n/ac/ax/be
- Thường giống nhau về giao thức cơ sở, khác nhau dài tần số.



Dải tần số

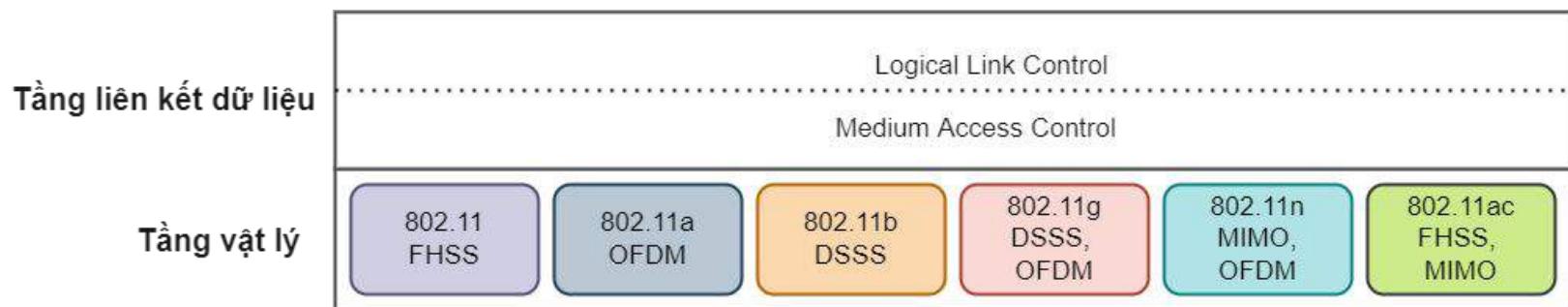
Dải tần số (frequency band) là một **khoảng xác định** trong **phổ vô tuyến** được chấp nhận để **sử dụng cho giao tiếp**.

- Tần số FM trong khoảng 88–108 MHz
- WiFi phổ biến với 2.4GHz và 5 GHz



Giao thức 802.11

Các giao thức 802.11 mô tả các thực thi ở **tầng vật lý** và **tầng liên kết dữ liệu**



Khung tin 802.11

Khung tin của chuẩn 802.11 bao gồm một số trường:

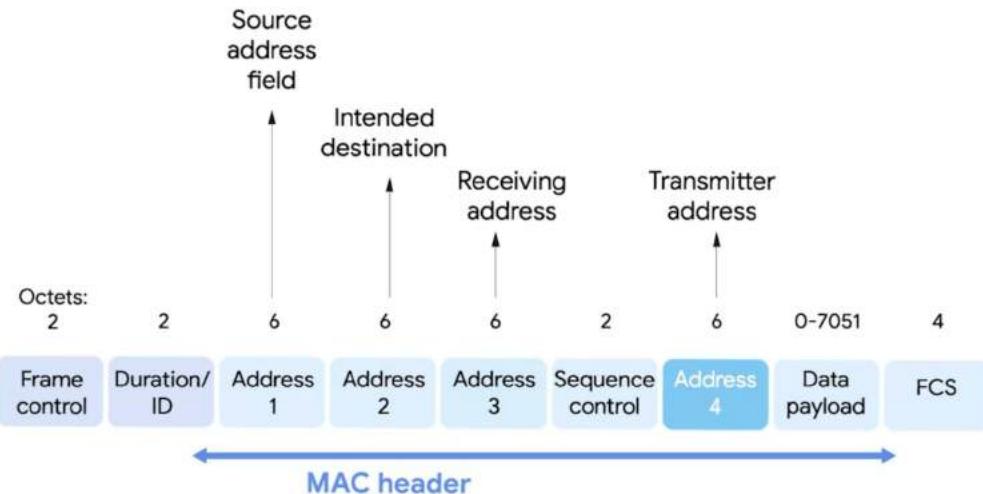
- **Frame control:** 16 bit, chứa giá trị của các trường phụ **mô tả phiên bản**, cách xử lý khung tin
- **Duration:** khoảng thời gian toàn bộ khung tin thực thi để thiết bị nhận biết được bao lâu nó phải lắng nghe.
- **4 địa chỉ MAC**
- **Sequence control:** số thứ tự của khung tin
- **FCS:** để kiểm tra lỗi (CRC)



Điểm truy cập không dây

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.
 - MAC thiết bị nguồn
 - MAC thiết bị đích
 - MAC nhận
 - MAC chuyển tiếp



Cấu hình mạng không dây

Mạng không dây có thể được cấu hình theo 3 cách:

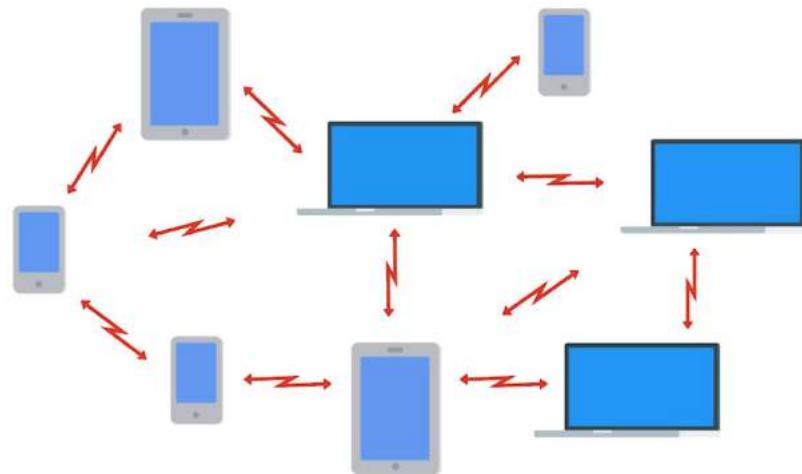
- Mạng tùy biến không dây (Wireless ad-hoc network)
- Mạng cục bộ không dây (Wireless LAN – WLAN)
- Mạng lưới không dây (Wireless mesh network)



Mạng tùy biến không dây

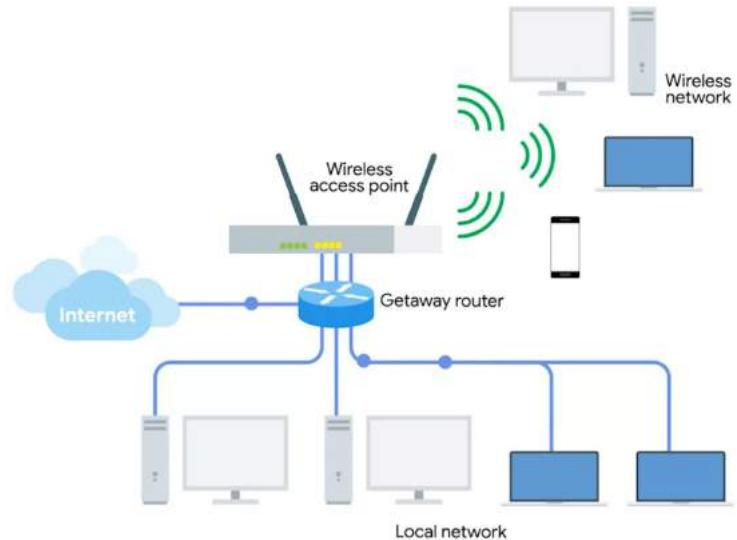
Mạng tùy biến không dây (Wireless ad-hoc network) là một **tập hợp các thiết bị kết nối với nhau mà không cần kiến trúc mạng phức tạp hỗ trợ**.

- Mỗi thiết bị giao tiếp với nhau bên trong phạm vi và **tất cả các nút mạng hỗ trợ truyền gói tin**.
- Ứng dụng: trao đổi hình ảnh, thông tin giữa các điện thoại với nhau.



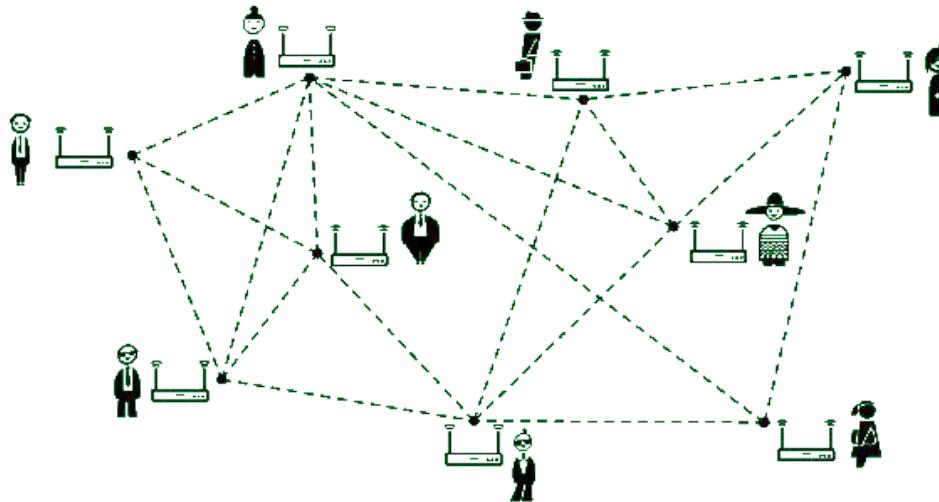
Mạng cục bộ không dây

Mạng cục bộ không dây (WLAN) bao gồm **một hoặc nhiều điểm truy cập (AP)** đóng vai trò làm cầu nối giữa mạng có dây và không dây.



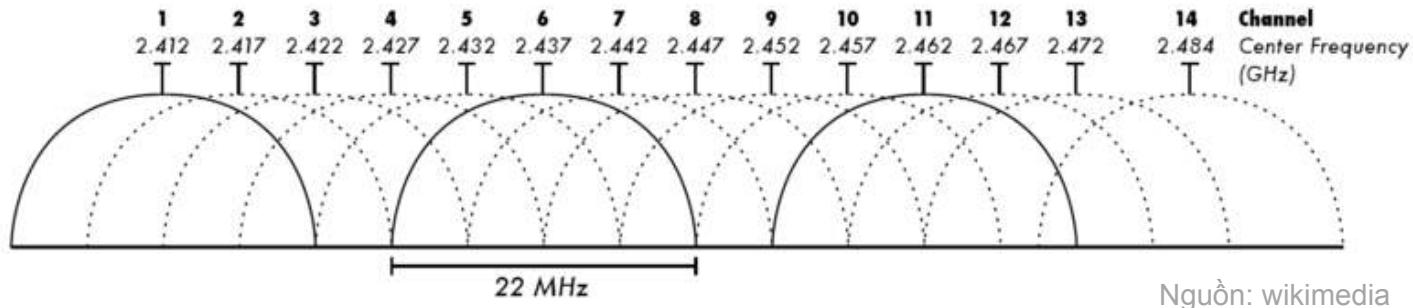
Mạng lưới không dây

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



Kênh

Kênh (channel) là **đoạn nhỏ, đơn lẻ** của toàn bộ **dải tần số** được sử dụng bởi một mạng không dây.



Nguồn: wikimedia

Miền đụng độ

- **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 mạng chậm**.
- Trong mạng có dây, **giải pháp** để tránh đụng độ là dùng Switch.
- Switch **không thể áp dụng cho mạng không dây** vì tín hiệu không đi qua dây dẫn.



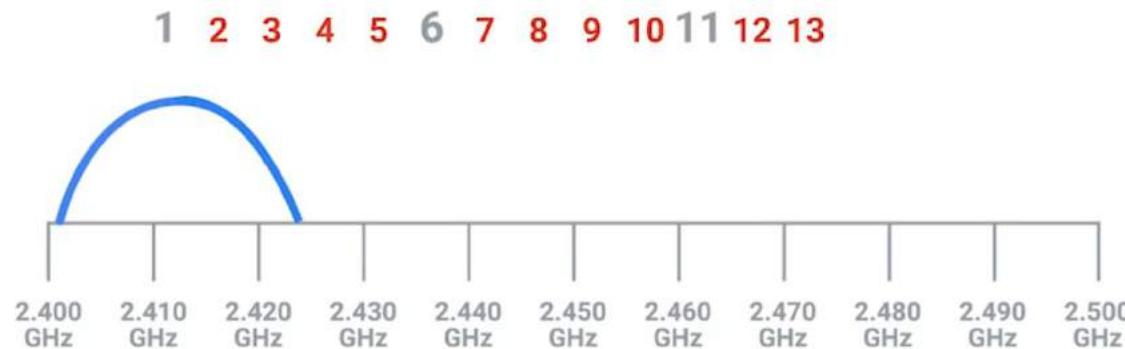
Kênh và miền dung độ

- Kênh giúp khắc phục một phần vấn đề dung độ.
- Dải tần số 2.4 GHz nghĩa là 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 (MHz) tùy vào mỗi khu vực.



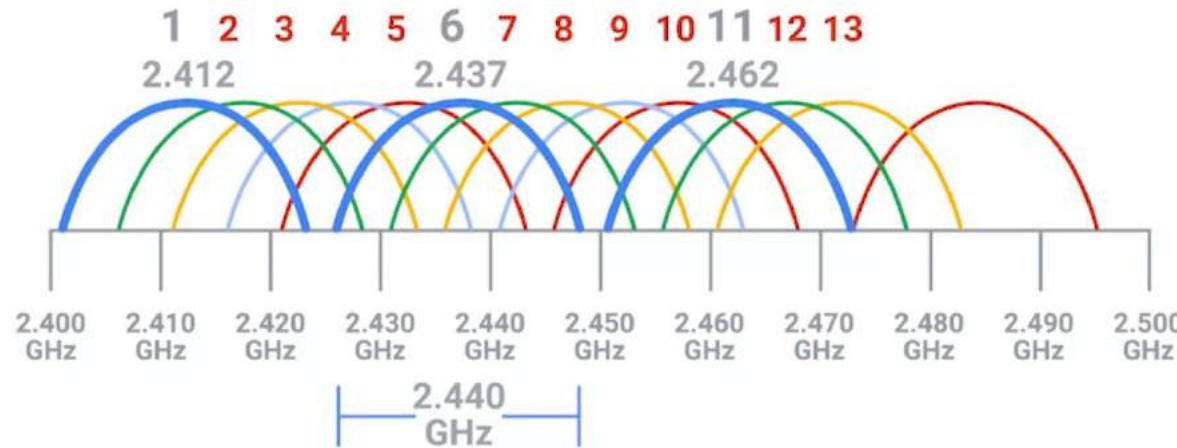
Kênh và miền dung độ

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



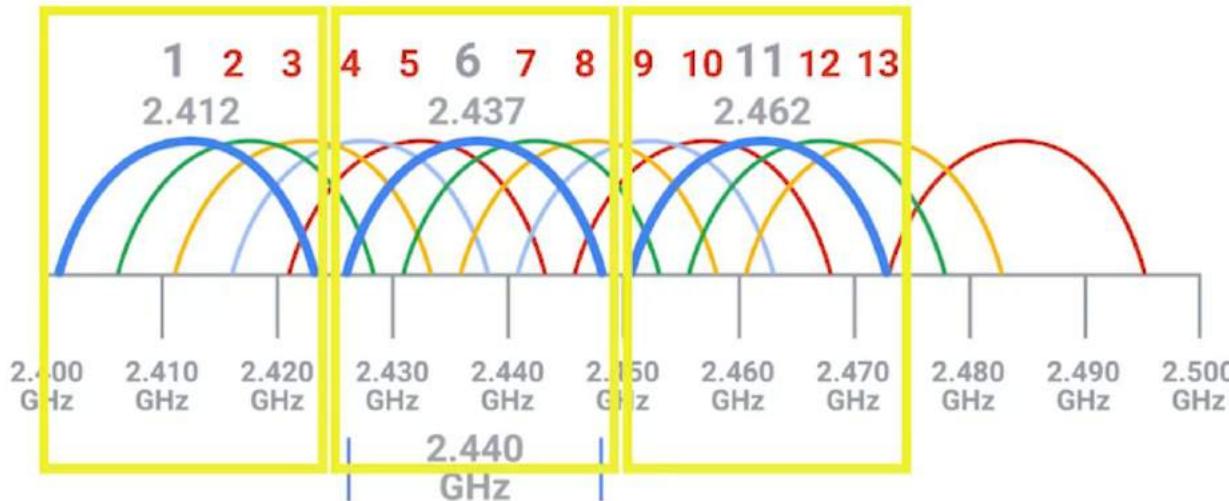
Kênh và miền dung độ

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



Kênh và miền dung độ

Các kênh hoàn toàn không dung độ là 1, 6, 11



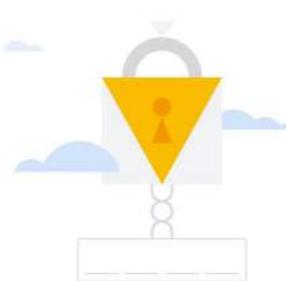
Bảo mật mạng không dây

WEP (Wired Equivalent Privacy) là một kỹ thuật mã hóa cung cấp mức độ riêng tư rất thấp.

- 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.

WPA (Wi-Fi Protected Access) sử dụng **khóa độ dài 128 bit**.

- WPA2 là phiên bản cải tiến với **khóa độ dài 256 bit** và được sử dụng phổ biến ngày nay.



Bảo mật mạng không dây

Một cách bảo mật khác là **lọc địa chỉ MAC**.

- Cấu hình điểm truy cập (AP) chỉ cho phép các kết nối từ một tập của các địa chỉ MAC đã xác định trước.

MAC: 12-34-56-78-90



MAC: 11-22-33-44-55



Mạng viễn thông

Mạng viễn thông (cellular/mobile network) là mạng kết nối các thiết bị di động.

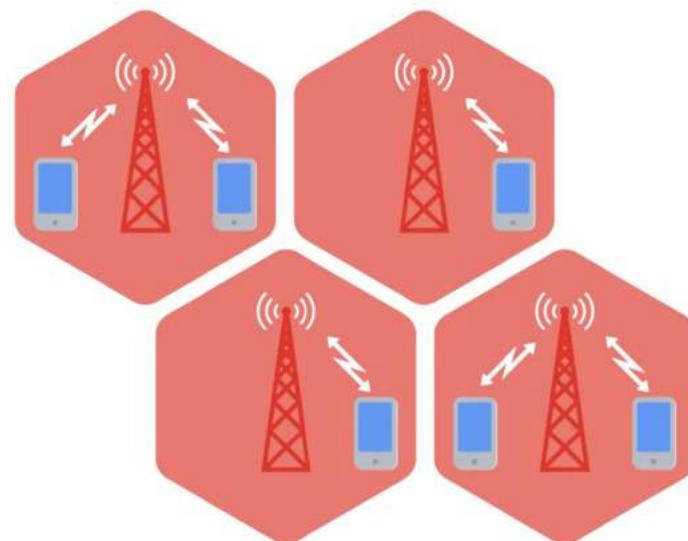
- Khá giống với mạng không dây nhưng sử dụng **tần số khác** và giúp cho **tín hiệu** được truyền đi xa.

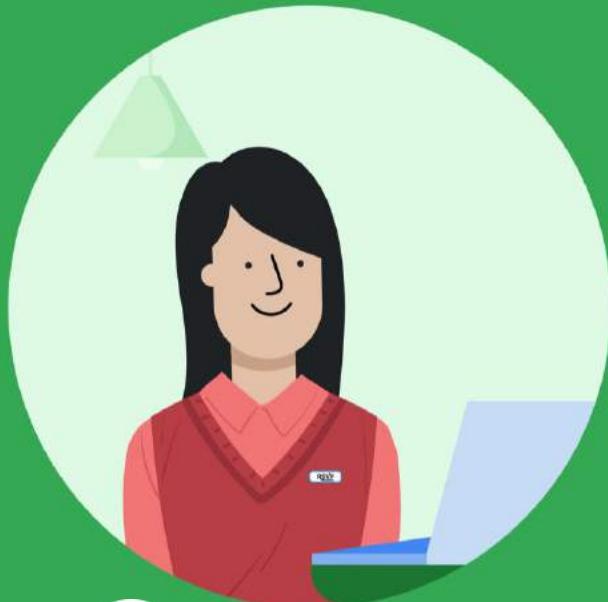
Phone frequency



Cấu tạo mạng viễn thông

- **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.
 - Giống với thiết bị **điểm truy cập (AP)** trong mạng không dây nhưng phạm vi rộng hơn.



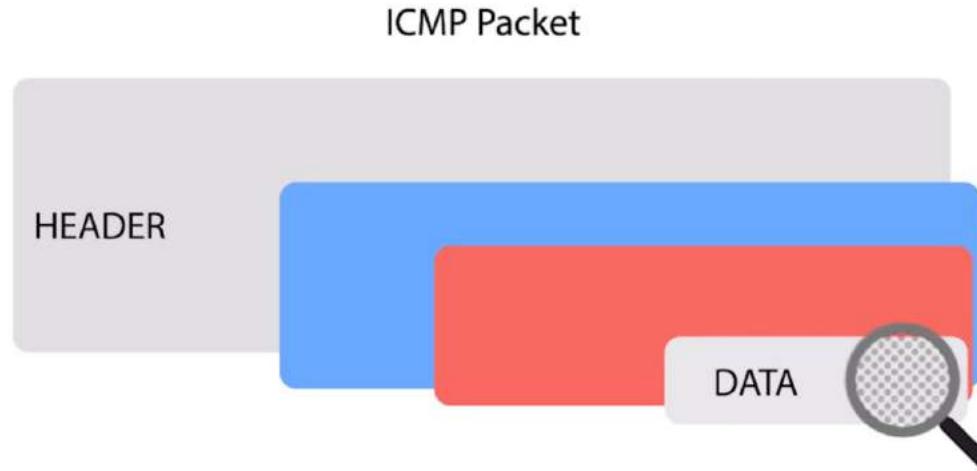


10 KHẮC PHỤC SỰ CỐ MẠNG



Giao thức ICMP

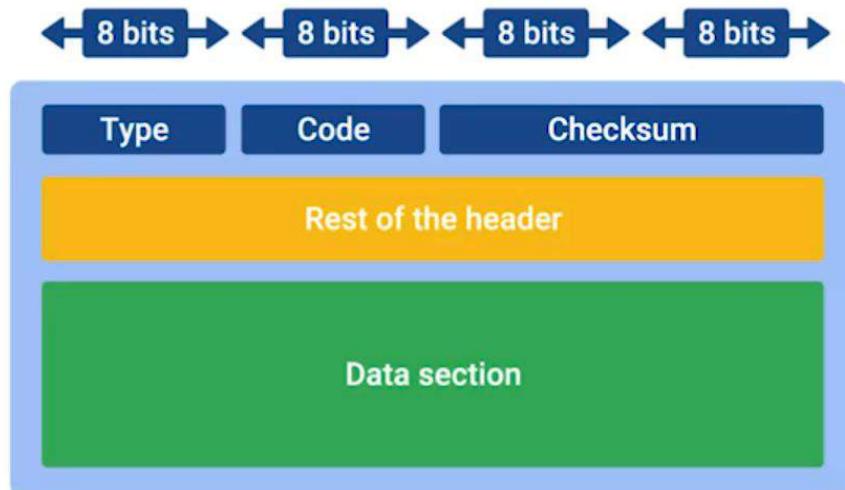
Giao thức thông điệp điều khiển Internet (Internet Control Message Protocol – ICMP) là một giao thức để xác định nguyên nhân quá trình truyền bị lỗi.



Gói tin ICMP

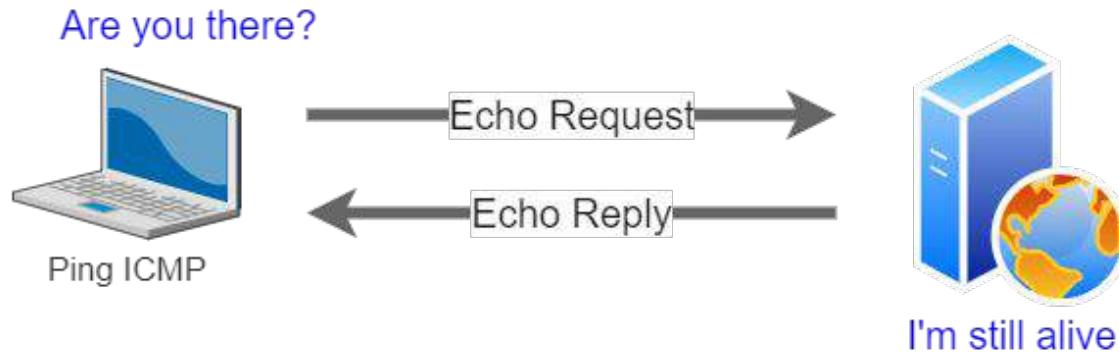
Gói tin ICMP gồm các trường:

- Type: loại của thông điệp như không đến được đích, hay quá thời gian
- Code: mã mô tả rõ hơn về lỗi
- Checksum: kiểm tra tính toàn vẹn gói tin
- Rest of the header: gửi thêm dữ liệu
- Data section: dữ liệu gửi mà bị lỗi
 - Toàn bộ IP header
 - 8 byte đầu của dữ liệu bị lỗi



Ping

- Ping (Packet Internet Groper) là một công cụ để kiểm tra xem có thể kết nối tới một máy tính hay không.
- 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.

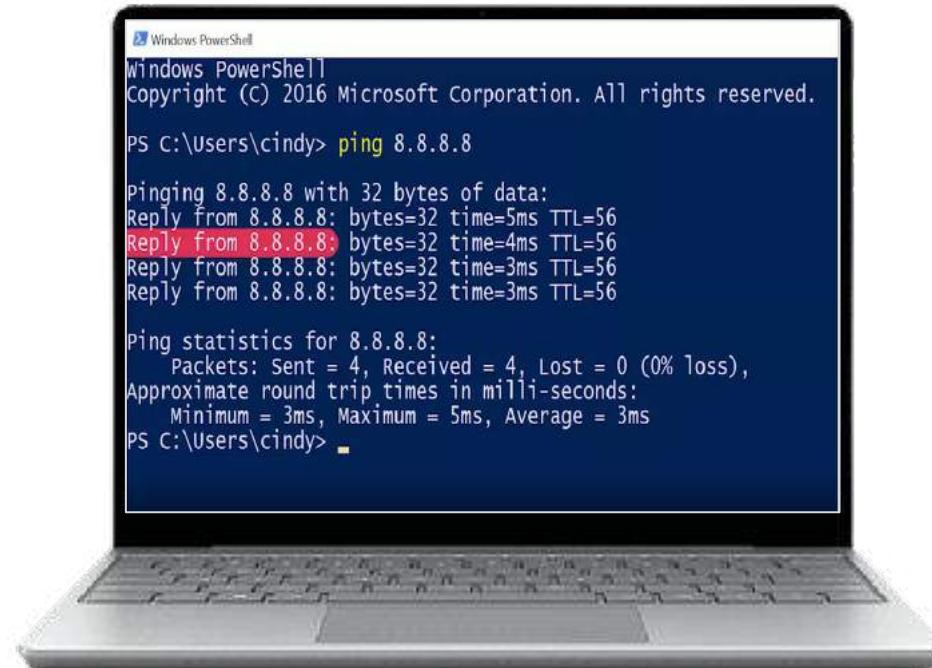


Ping

Lệnh: Ping + địa chỉ IP/FQDN

Thông tin trả về:

- Địa chỉ phản hồi
- Kích thước
- Thời gian
- TTL (thời gian sống)



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

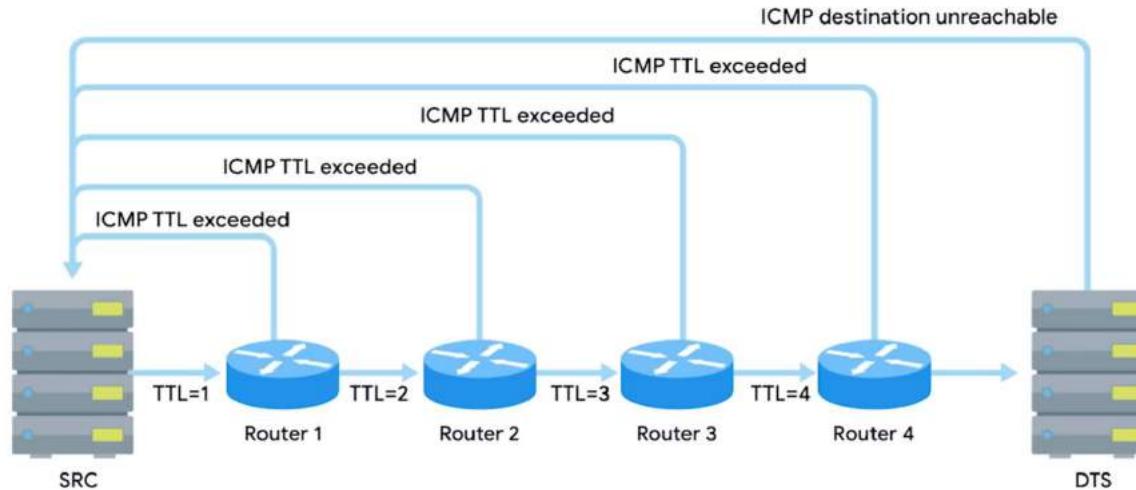
PS C:\Users\cindy> ping 8.8.8.8

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>
```

Traceroute

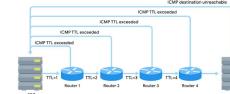
Traceroute là công cụ dùng để chẩn đoán vấn đề **dựa trên các đường định tuyến giữa hai nút**



Traceroute

Traceroute dựa trên trường TTL (Time to Live)

- Traceroute gửi một loạt các gói tin với TTL được thiết lập khác nhau và lần lượt với giá trị 1, 2, ...
- Mỗi TTL, Traceroute gửi 3 gói tin
- 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 gấp vấn đề chỗ nào



Traceroute

Lệnh: traceroute + IP/FQDN

Thông tin trả về:

- Số thứ tự máy đi qua
- Thời gian của 3 gói tin
- IP của từng máy

```
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 (108.170.235.239)
 8  sfo07s16-in-f78.1e100.net (216.58.195.78)  5.150 ms  5.154 ms  5.131 ms
```

Traceroute

Mỗi hệ điều hành khác nhau thì tên lệnh có thay đổi:

- Linux, MacOS: `traceroute`
- Windows: `tracert`

Một số công cụ tương tự:

- Linux, MacOS: `mtr`
- Windows: `pathping`



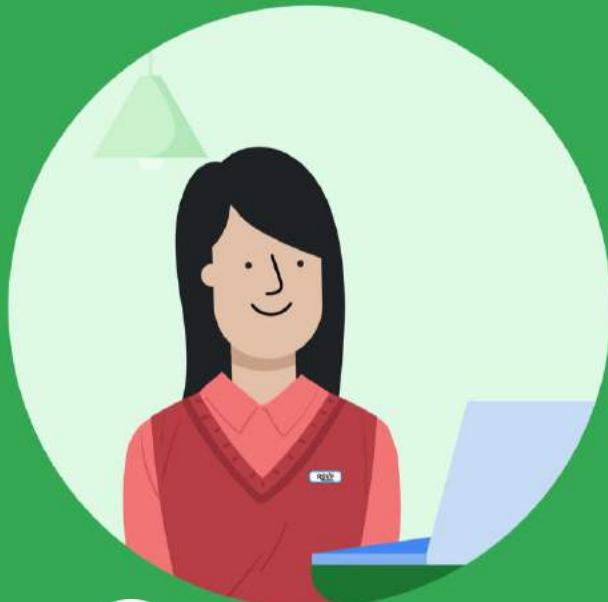
Kiểm tra Port

Một số công cụ để kiểm tra port trên máy đích có hoạt động không:

- Linux, MacOS: nc
- Windows: test-netconnection
 - Nếu không cung cấp port trong tham số thì mặc định tương đương với ping (echo request)

Một số tham số thêm của lệnh như -V, -Z để thay đổi cách thể hiện kết quả.

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



11 KIỂM TRA DNS



Công cụ nslookup

Công cụ nslookup được sử dụng để kiểm tra việc phân giải tên miền.

- 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`

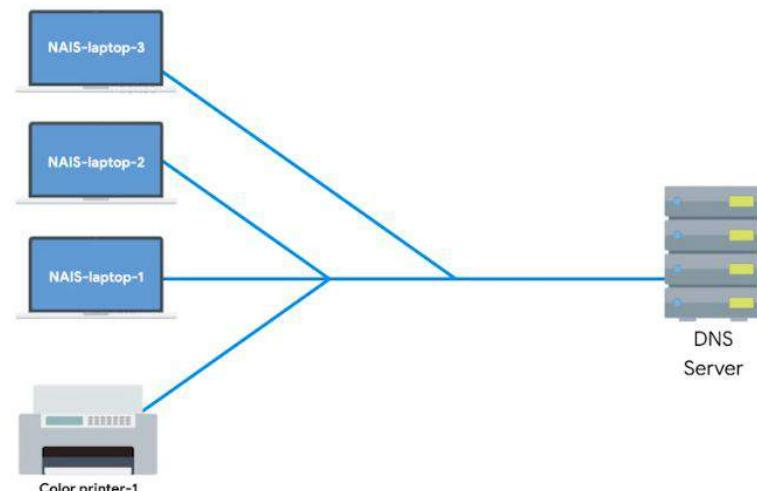
```
cindy@cindy-nyc:~$ nslookup twitter.com
Server:      127.0.1.1
Address:     127.0.1.1#53

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

DNS Server

Ngoài DNS Server được cung cấp bởi nhà cung cấp dịch vụ Internet (ISP), chúng ta có thể:

- **Tự xây dựng DNS Server** để phục vụ phân giải tên cho các máy cục bộ
- **Sử dụng các DNS Server công cộng** (public DNS Server)
 - Tổ chức mức 3:
 - 4.2.2.1, 4.2.2.2, 4.2.2.3,
 - 4.2.2.4, 4.2.2.5, 4.2.2.6
 - Google: 8.8.8.8, 8.8.4.4



Đăng ký tên miền

- Nhà cung cấp tên miền (registrar) là một **tổ chức cấp phát và quản lý tên miền**.
- Để đăng ký tên miền, ta chọn một nhà cung cấp và thực hiện các bước theo hướng dẫn trong trang của nhà cung cấp.



Tập tin Host

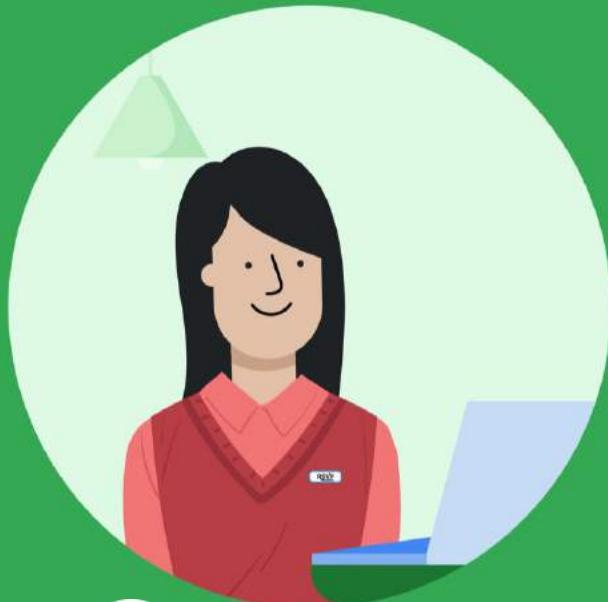
Tập tin Host là một tập tin chứa mỗi dòng là **địa chỉ mạng** và **tên máy**.

```
# 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
```

Tập tin Host

- Địa chỉ Loopback là địa chỉ trả về chính máy đó.
- 127.0.0.1 (IPv4) và ::1 (IPv6) là địa chỉ loopback được cấu hình cho mọi thiết bị



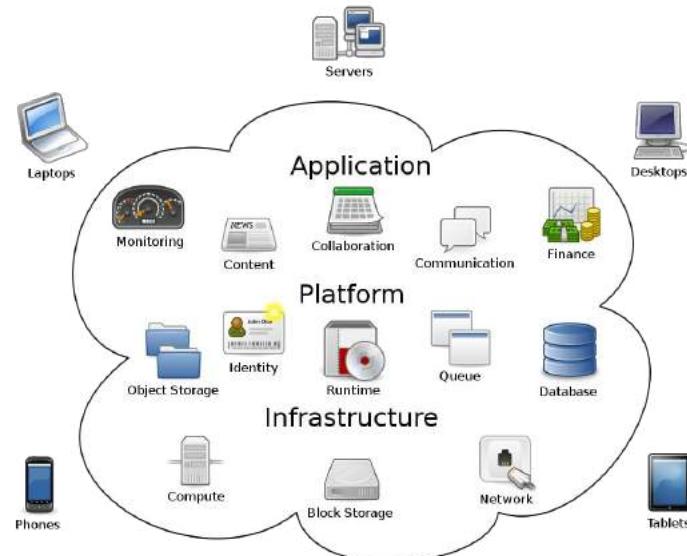


12 ĐIỆN TOÁN ĐÁM MÂY



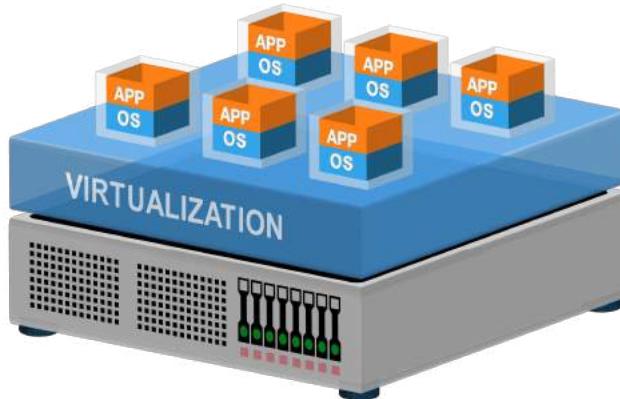
Điện toán đám mây

Điện toán đám mây (cloud computing) là công nghệ cho phép tài nguyên máy tính được chia sẻ để nhiều người có thể cùng sử dụng.



Ảo hóa phần cứng

- Ảo hóa phần cứng (hardware virtualization) là công nghệ chủ chốt của điện toán đám mây.
- Với công nghệ ảo hóa, một máy tính vật lý (host) có thể giả lập thành nhiều máy ảo (guest).

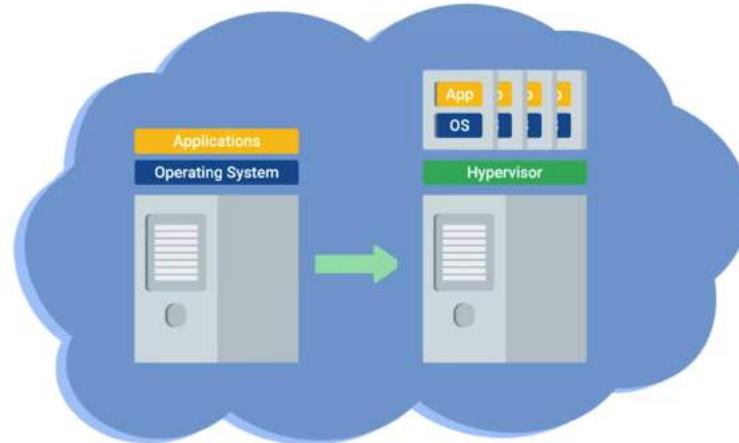


Nguồn: openclipart

Hypervisor

Hypervisor là một phần mềm chạy và quản lý các máy ảo.

- Cho phép mỗi máy ảo truy cập các tài nguyên phần cứng vật lý bên dưới.



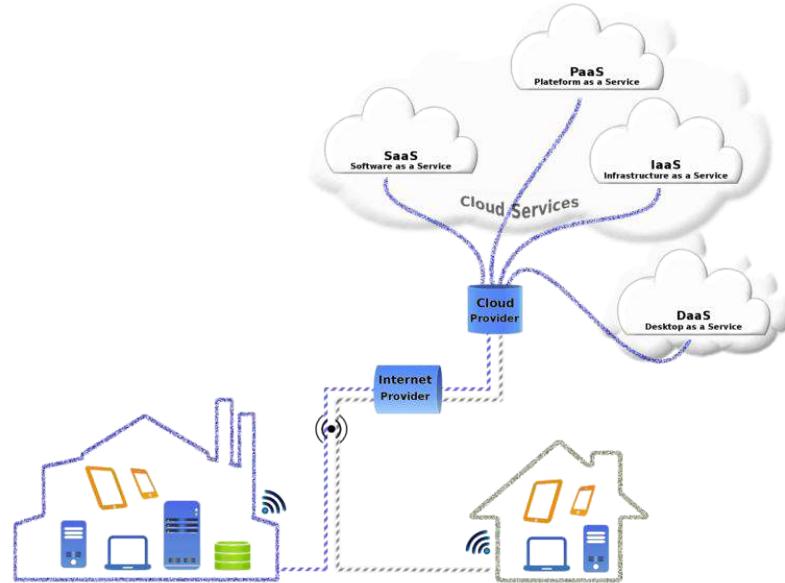
Public, private và hybrid cloud

- 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.





Mọi thứ như một dịch vụ

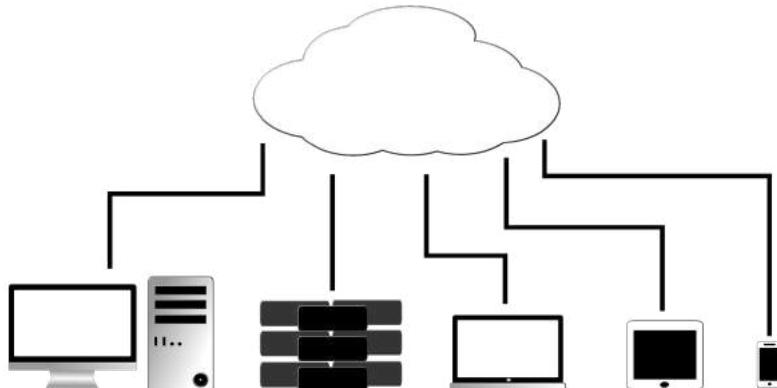
Các loại dịch vụ điện toán đám mây:

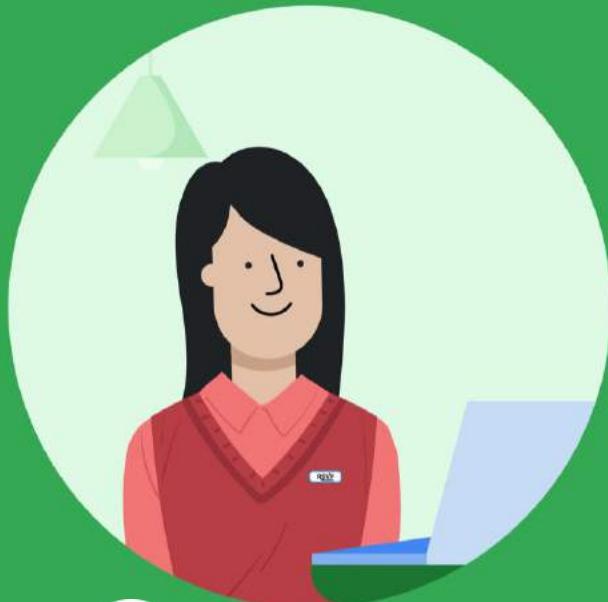
- **Infrastructure as a Service** (IaaS) là dịch vụ cơ sở hạ tầng như mạng máy tính, các máy chủ
- **Platform as a Service** (PaaS) là dịch vụ cung cấp môi trường để người dùng phát triển và triển khai ứng dụng của mình. Ví dụ như Windows Azure, Google App Engine.
- **Software as a Service** (SaaS) là 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. Ví dụ như Office 365 của Microsoft.

Lưu trữ đám mây

Lưu trữ đám mây (cloud storage) là vùng chứa dữ liệu trên các máy chủ đám mây.

- Người dùng có thể truy cập từ bất kỳ đâu
- Đồng bộ trên nhiều thiết bị
- Chi phí hợp lý
- Không sợ mất dữ liệu do lỗi phần cứng
- V.v



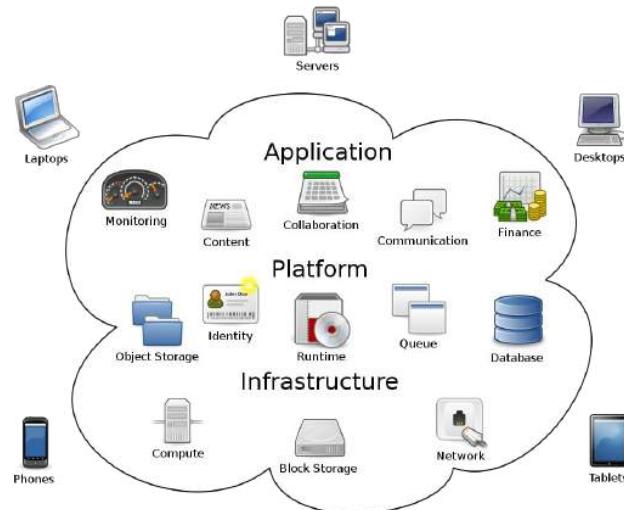


13 ĐỊA CHỈ IPV6



Điện toán đám mây

Điện toán đám mây (cloud computing) là công nghệ cho phép tài nguyên máy tính được chia sẻ để nhiều người có thể cùng sử dụng



Nguồn: wikipedia

IPv6

- IPv4 không còn đủ để cấp cho mỗi thiết bị một địa chỉ IPv4 (32 bit) riêng biệt
- IPv6 được tạo với **độ dài 128 bit** và có thể cấp cho 2¹²⁸ thiết bị
- IPv6 được **viết thành cụm** gồm 8 nhóm, **mỗi nhóm 16 bit** và được biểu diễn dưới dạng **số hệ 16**

2001:0db8:0000:0000:0000:ff00:0012:345

Quy ước viết gọn IPv6

IPv6 có thể viết ngắn lại với quy tắc:

- Bỏ đi các số 0 đầu mỗi nhóm
- 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 IPv6 cho loopback

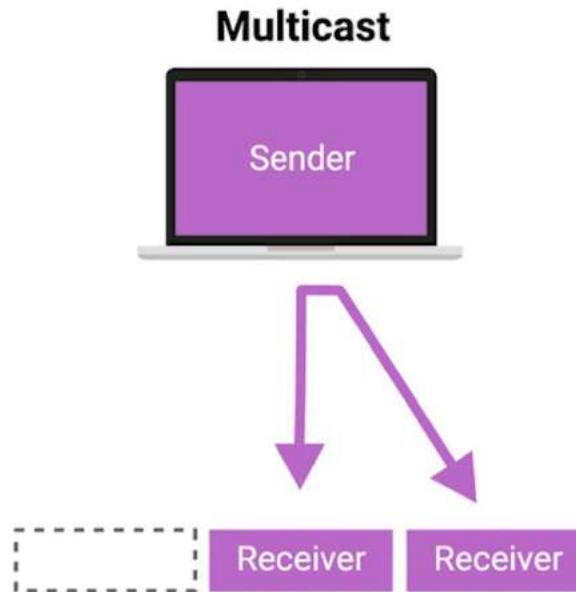
Địa chỉ loopback (trở về chính máy đó) của IPv6 là:

0000:0000:0000:0000:0000:0000:0000:0001

::1

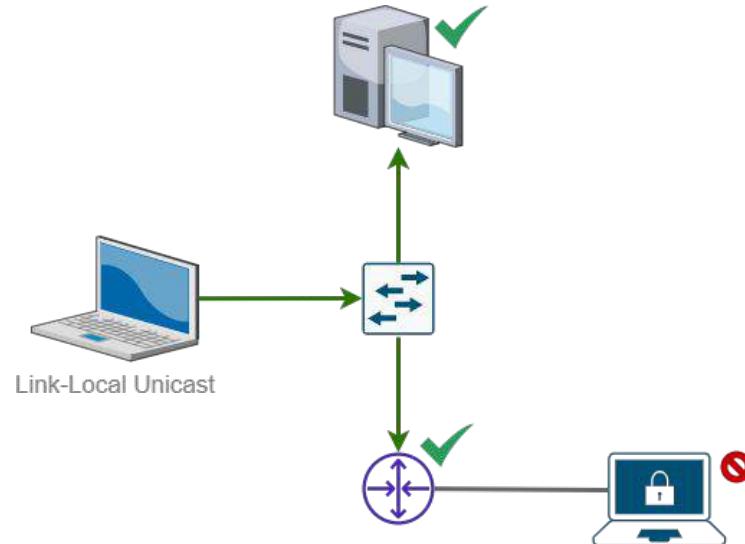
Địa chỉ IPv6 cho Multicast

Để gửi một nhóm các máy (Multicast), IPv6 sử dụng địa chỉ FFOO::



Địa chỉ IPv6 cho Link-Local Unicast

Để gửi đến một máy trong liên kết cục bộ (link-local unicast), IPv6 sử dụng địa chỉ FF80::



Địa chỉ Link-Local Unicast

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.



Định danh mạng và định danh máy

IPv6 sử dụng **64 bit đầu làm định danh mạng** (network ID) và **64 bit sau làm định danh máy tính** (host ID)

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

Network ID

Host ID

IPv6 Header

Cấu trúc header của IPv6 gồm:

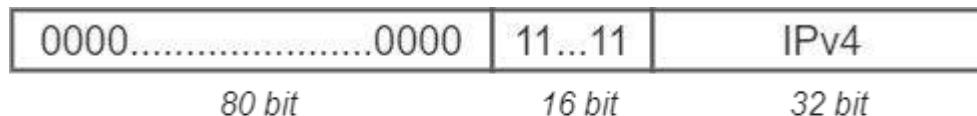
- Version: phiên bản IP
- Class: loại dữ liệu gửi
- Flow label: chất lượng mức dịch vụ
- Payload length: chiều dài dữ liệu
- Next header: xác định header của gói chứa cấu hình thêm đã được tách ra.
- Hop limit: tương đương với TTL
- Source/Destination address: địa chỉ nguồn và đích



Không gian địa chỉ ánh xạ IPv4

IPv6 có thể ánh xạ đến một địa chỉ IPv4 bằng cách:

- Bắt đầu với 80 bit 0
- Theo sau 16 bit 1
- 32 bit còn lại ánh xạ đến địa chỉ IPv4

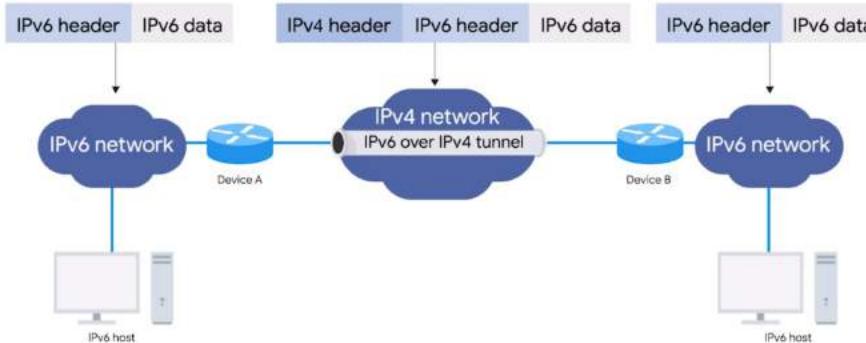


$$169.291.13.133 = 0:0:0:0:FFFF:A9DB:0D85$$

IPv6 Tunnel

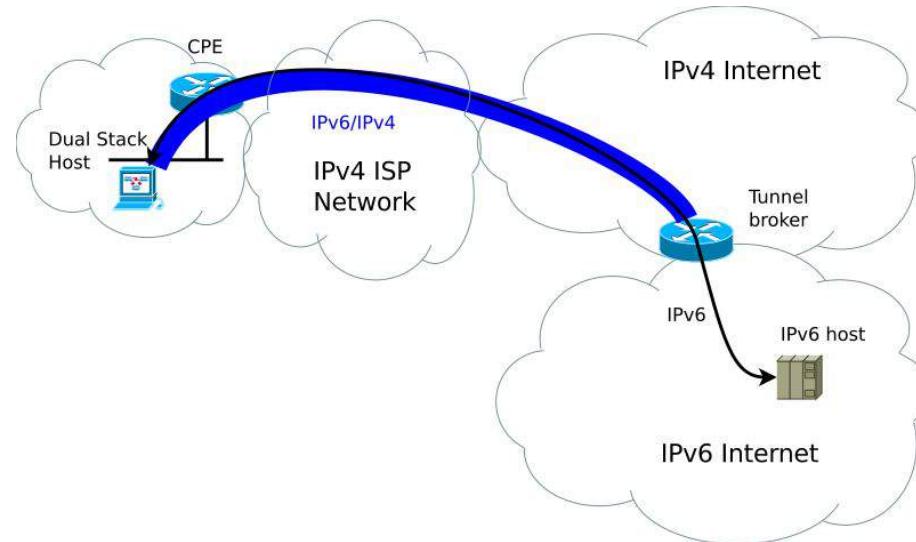
IPv6 Tunnel (đường hầm IPv6) là cách thức sử dụng hạ tầng sẵn có của mạng IPv4 để thực hiện các kết nối các thiết bị dùng IPv6.

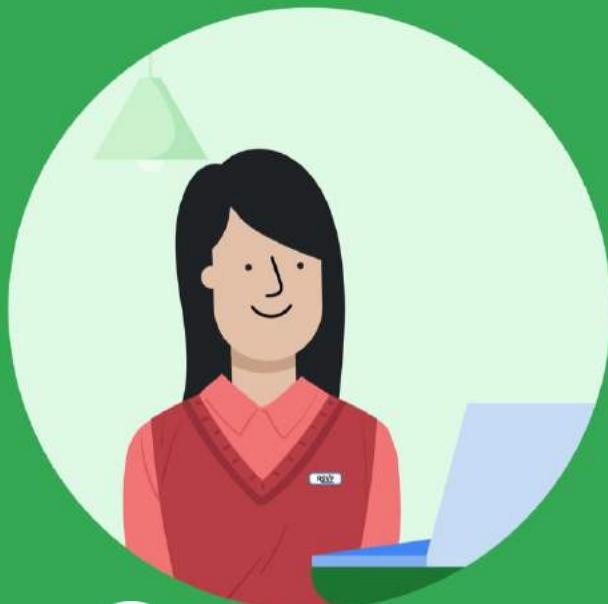
- Các server IPv6 thực hiện bao đóng dữ liệu IPv6 trong một gói tin **IPv4 datagram** và chuyển qua mạng IPv4
- Phía nhận thực hiện ngược lại



IPv6 tunnel broker

IPv6 tunnel broker là những tổ chức làm trung gian cung cấp dịch vụ để tạo kết nối các thiết bị dùng IPv6



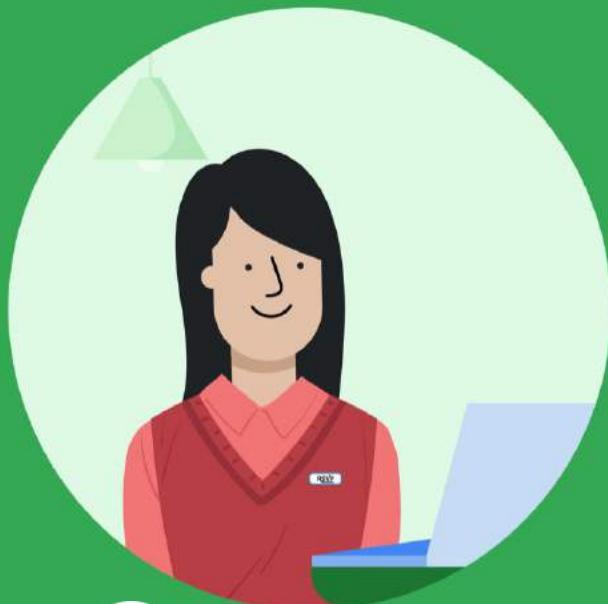


TỔNG KẾT



Những ý chính cần nắm

- Mô hình mạng 5-tầng TCP/IP và mô hình OSI.
- Các giao thức chuẩn, các công nghệ ở các tầng trong mô hình mạng.
- Các tính năng và công dụng của các thiết bị mạng.
- Các dịch vụ mạng gồm DNS, DHCP, NAT, VPN, proxy.
- Đặc điểm mạng băng thông rộng, mạng internet, mạng không dây.
- Kiểm tra và theo vết được các vấn đề xảy ra trong mạng.
- Các khái niệm liên quan đến điện toán đám mây và lưu trữ đám mây.



THANK YOU

