

Mô hình TCP/IP

- **TCP/IP là một hệ thống giao thức - một tập hợp các giao thức hỗ trợ việc lưu truyền trên mạng. Và lời giải đáp cho câu hỏi: "Giao thức là gì?" tìm hiểu**
 - TCP/IP là gì,
 - Hoạt động ra sao và
 - Nó bắt nguồn từ đâu?

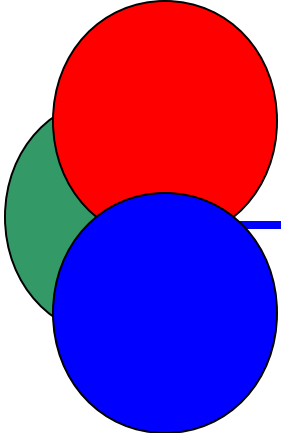
Giao thức

- Giao thức là những qui tắc qui định được đặt ra trước để khi trao đổi thông tin đối tượng được trao đổi có thể hiểu nhau được
- Ví dụ:
 - ngôn ngữ giao tiếp
 - Lời nói theo từng thứ tiếng
 - Khẩu hình (người câm)
 - Các cử chỉ
 - Qui tắc trao đổi trong mạng máy tính
 - TCP/IP, IPX/SPX,

giao thức TCP/IP

- **Bộ giao thức TCP/IP**, ngắn gọn là **TCP/IP** (tiếng Anh: *Internet protocol suite* hoặc *IP suite* hoặc *TCP/IP protocol suite* - bộ giao thức liên mạng),
- Định nghĩa :TCP/IP là một bộ các **giao thức truyền thông** cài đặt **chồng giao thức** mà **Internet** và hầu hết các mạng máy tính thương mại đang chạy trên đó.
- Bộ giao thức này được đặt tên theo hai giao thức chính của nó là **TCP** (*tranmission control protocol*) và **IP** (*internet protocol*). Chúng cũng là hai giao thức đầu tiên được định nghĩa.
- .

- bộ giao thức TCP/IP có thể được coi là một tập hợp các tầng, mỗi tầng giải quyết một tập các vấn đề có liên quan đến việc truyền dữ liệu, và cung cấp cho các **giao thức tầng cấp trên** một dịch vụ được định nghĩa rõ ràng dựa trên việc sử dụng các dịch vụ của các tầng thấp hơn.
- Về mặt logic, các tầng trên gần với người dùng hơn và làm việc với dữ liệu trừu tượng hơn, chúng dựa vào các **giao thức tầng cấp dưới** để biến đổi dữ liệu thành các dạng mà cuối cùng có thể được truyền đi một cách vật lý



So sánh giữa mô hình OSI và TCP/IP

Mô hình OSI

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Datalink

1 Physical

TCP/IP

Application

Transport

Internet

Network Access

Lịch sử

- Vào cuối những năm 1960 và đầu 1970, Trung tâm nghiên cứu cấp cao (Advanced Research Projects Agency - ARPA) thuộc bộ quốc phòng Mỹ (Department of Defense - DoD) được giao trách nhiệm phát triển mạng ARPANET bao gồm mạng của những tổ chức quân đội, các trường đại học và các tổ chức nghiên cứu và được dùng để hỗ trợ cho những dự án nghiên cứu khoa học và quân đội

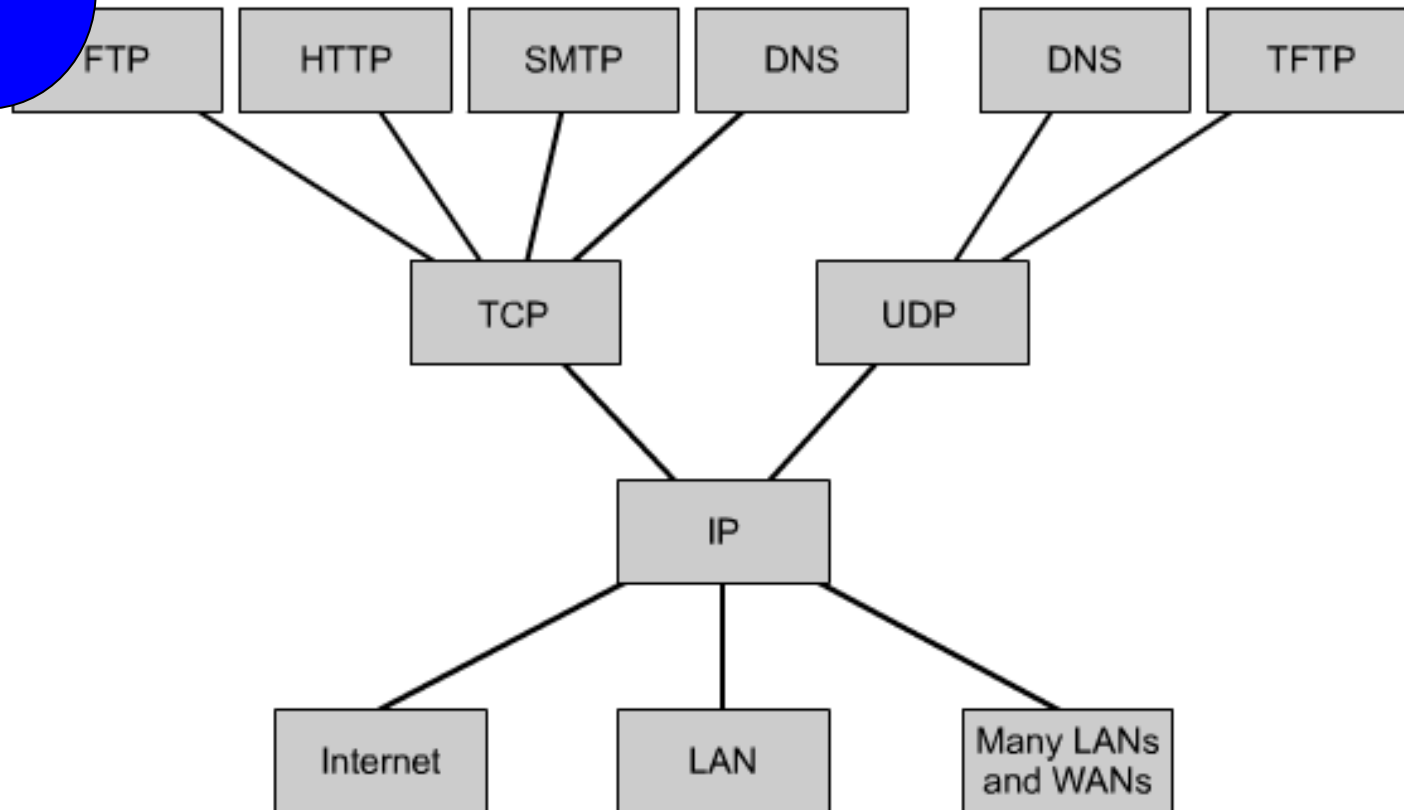
Lịch sử

- Vào năm 1975, cuộc thử nghiệm thông nối hai mạng lưới TCP/IP, giữa Stanford và UCL đã được tiến hành. Vào tháng 11 năm 1977, một cuộc thử nghiệm thông nối ba mạng lưới TCP/IP, giữa Mỹ, Anh và Na-uy đã được chỉ đạo. Giữa năm 1978 và 1983, một số những bản mẫu của TCP/IP đã được thiết kế tại nhiều trung tâm nghiên cứu.

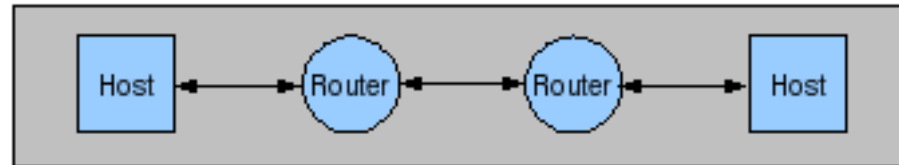
Lịch sử

- Đầu những năm 1980, một bộ giao thức mới được đưa ra làm giao thức chuẩn cho mạng ARPANET và các mạng của DoD mang tên DARPA Internet protocol suit, thường được gọi là bộ giao thức TCP/IP hay còn gọi tắt là TCP/IP (Transmission Control Protocol/Internet Protocol).

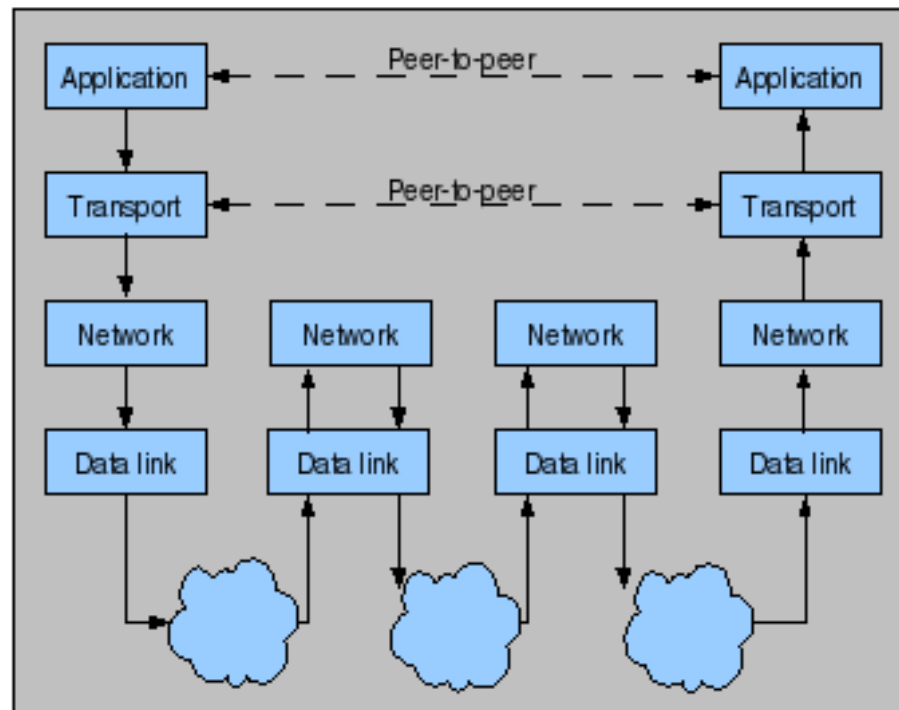
Các giao thức của TCP/IP



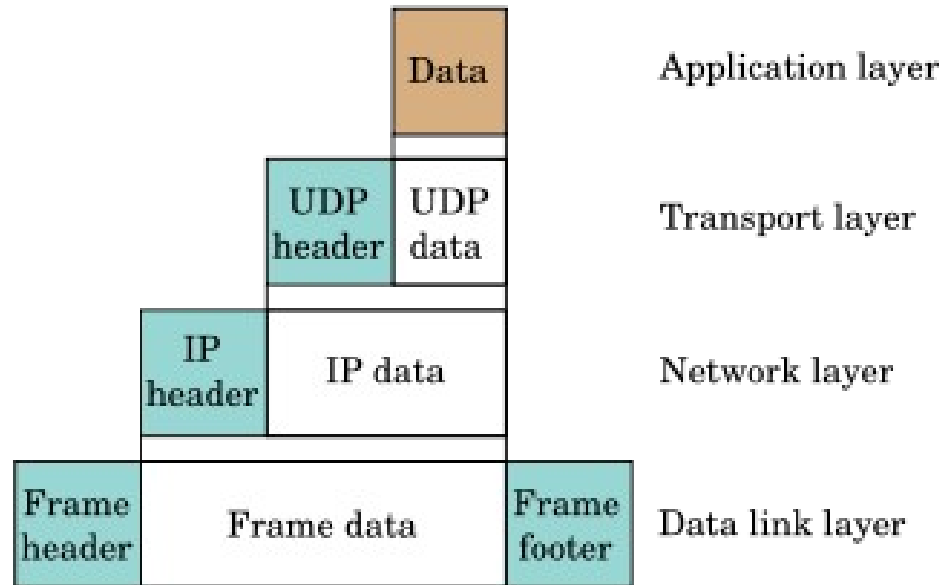
Network connections



Stack connections



Mô hình mã hóa dữ liệu của UDP



Network Access

- Tầng liên kết - phương pháp được sử dụng để chuyển các gói tin từ tầng mạng tới các máy chủ (*host*) khác nhau - không hẳn là một phần của bộ giao thức TCP/IP, vì giao thức IP có thể chạy trên nhiều tầng liên kết khác nhau. Các quá trình truyền các gói tin trên một liên kết cho trước và nhận các gói tin từ một liên kết cho trước có thể được điều khiển cả trong phần mềm điều vận thiết bị (*device driver*) dành cho các mạng, cũng như trong phần sụn (*firmware*) hay các chipset chuyên dụng. Những thứ đó sẽ thực hiện các chức năng liên kết dữ liệu chẳng hạn như bổ sung một tín đầu (*packet header*) để chuẩn bị cho việc truyền gói tin đó, rồi thực sự truyền frame dữ liệu qua một môi trường vật lý.
- Đối với truy nhập Internet qua modem quay số, các gói IP thường được truyền bằng cách sử dụng giao thức PPP. Đối với truy nhập Internet băng thông rộng (*broadband*) như ADSL hay modem cáp, giao thức PPPoE thường được sử dụng. Mạng dây cục bộ (*local wired network*) thường sử dụng Ethernet, còn mạng không dây cục bộ thường dùng chuẩn IEEE 802.11. Đối với các mạng diện rộng (*wide-area network*), các giao thức thường được sử dụng là PPP đối với các đường T-carrier hoặc E-carrier, Frame relay, ATM (*Asynchronous Transfer Mode*), hoặc giao thức packet over SONET/SDH (POS).

Network Access

- Tầng liên kết còn có thể là tầng nơi các gói tin được chặn (*intercepted*) để gửi qua một **mạng riêng ảo** (*virtual private network*). Khi xong việc, dữ liệu tầng liên kết được coi là dữ liệu của ứng dụng và tiếp tục đi xuống theo chồng giao thức TCP/IP để được thực sự truyền đi. Tại đầu nhận, dữ liệu đi lên theo chồng TCP/IP hai lần (một lần cho mạng riêng ảo và lần thứ hai cho việc định tuyến).
- Tầng liên kết còn có thể được xem là bao gồm cả **tầng vật lý** - tầng là kết hợp của các thành phần mạng vật lý thực sự (**hub**, các **bộ lặp** (*repeater*), **cáp mạng**, **cáp quang**, **cáp đồng trục** (*coaxial cable*), **cạc mạng**, các HBA (Host Bus Adapter) và các thiết bị nối mạng có liên quan: RJ-45, BNC, etc), và các đặc tả mức thấp về các tín hiệu (mức **hiệu điện thế**, **tần số**, v.v..).

Tầng mạng -network

- **tầng mạng** giải quyết các vấn đề dẫn các gói tin qua một mạng đơn. Một số ví dụ về các giao thức như vậy là **X.25**, và **giao thức Host/IMP** của mạng **ARPANET**.
- Với sự xuất hiện của khái niệm **liên mạng**, các chức năng mới đã được bổ sung cho tầng này, đó là chức năng dẫn đường cho dữ liệu từ **mạng** nguồn đến mạng đích. Nhiệm vụ này thường đòi hỏi việc **định tuyến** cho gói tin qua một mạng lưới của các mạng máy tính, đó là **liên mạng**.

Tầng mạng -network

- Trong bộ giao thức liên mạng, giao thức **IP** thực hiện nhiệm vụ cơ bản dẫn đường dữ liệu từ nguồn tới đích. IP có thể chuyển dữ liệu theo yêu cầu của nhiều **giao thức tầng trên** khác nhau; mỗi giao thức trong đó được định danh bởi một số hiệu giao thức duy nhất: **giao thức ICMP** (*Internet Control Message Protocol*) là giao thức 1 và **giao thức IGMP** (*Internet Group Management Protocol*) là giao thức 2.
- Một số giao thức truyền bởi IP, chẳng hạn ICMP (dùng để gửi thông tin chẩn đoán về truyền dữ liệu bằng IP) và IGMP (dùng để quản lý dữ liệu đa truyền (*multicast*)), được đặt lên trên IP nhưng thực hiện các chức năng của tầng liên mạng, điều này minh họa một sự bất tương thích giữa liên mạng và chồng TCP/IP và **mô hình OSI**. Tất cả các giao thức định tuyến, chẳng hạn **giao thức BGP** (*Border Gateway Protocol*), **giao thức OSPF**, và **giao thức RIP** (*Routing information protocol*), đều thực sự là một phần của tầng mạng, mặc dù chúng có thể có vẻ thuộc về phần trên của chồng giao thức

Transport-Tầng giao vận

- Trách nhiệm của **tầng giao vận** là kết hợp các khả năng truyền thông điệp **trực tiếp** (*end-to-end*) không phụ thuộc vào mạng bên dưới, kèm theo **kiểm soát lỗi** (*error control*), phân mảnh (*fragmentation*) và **điều khiển lưu lượng**. Việc truyền thông điệp trực tiếp hay kết nối các ứng dụng tại tầng giao vận có thể được phân loại như sau:
 - 1. **định hướng kết nối** (*connection-oriented*), ví dụ **TCP**
 - 2. **phi kết nối** (*connectionless*), ví dụ **UDP**

Transport-Tầng giao vận

- Tầng giao vận có thể được xem như một cơ chế vận chuyển thông thường, nghĩa là trách nhiệm của một phương tiện vận tải là đảm bảo rằng hàng hóa/hành khách của nó đến đích an toàn và đầy đủ.
- Tầng giao vận cung cấp dịch vụ kết nối các ứng dụng với nhau thông qua việc sử dụng các **cổng TCP và UDP**. Do IP chỉ cung cấp dịch vụ phát chuyển nỗ lực tối đa (*best effort delivery*), tầng giao vận là tầng đầu tiên giải quyết vấn đề độ tin cậy.

TCP

- TCP là một giao thức định hướng kết nối. Nó giải quyết nhiều vấn đề độ tin cậy để cung cấp một **dòng byte đáng tin cậy** (*reliable byte stream*):
- dữ liệu đến đích đúng thứ tự
- sửa lỗi dữ liệu ở mức độ tối thiểu
- dữ liệu trùng lặp bị loại bỏ
- các gói tin bị thất lạc/loại bỏ được gửi lại
- có kiểm soát tắc nghẽn giao thông dữ liệu
- Tuy các giao thức định tuyến động (*dynamic routing protocol*) khớp về kỹ thuật với tầng giao vận trong bộ giao thức TCP/IP (do chúng chạy trên IP), nhưng chúng thường được xem là một phần của tầng mạng. Một ví dụ là **giao thức OSPF** (số hiệu giao thức IP là 89).
- Giao thức mới hơn, **SCTP** (*Stream Control Transmission Protocol*), cũng là một cơ chế giao vận **định hướng kết nối** "đáng tin cậy". Giao thức này định hướng dòng (*stream-oriented*), chứ không định hướng byte như TCP, và cung cấp nhiều dòng đa công (*multiplexed*) trên một kết nối. Nó còn hỗ trợ **multi-homed**, trong đó một đầu của kết nối có thể được đại diện bởi nhiều **địa chỉ IP** (đại diện cho nhiều giao diện vật lý), sao cho, nếu một giao diện vật lý thất bại thì kết nối vẫn không bị gián đoạn. Giao thức này ban đầu được phát triển dành cho các ứng dụng điện thoại (để vận chuyển **SS7** trên **giao thức IP**), nhưng nó cũng có thể được sử dụng cho các ứng dụng khác.

UDP

- **UDP** là một giao thức **datagram phi kết nối**. Cũng như IP, nó là một giao thức **nỗ lực tối đa** hay "không đáng tin cậy". Vấn đề duy nhất về độ tin cậy mà nó giải quyết là sửa lỗi dữ liệu (dù chỉ bằng một thuật toán **tổng kiểm** yếu). UDP thường được dùng cho các ứng dụng như các **phương tiện truyền thông theo dòng** (*streaming media*) chứa âm thanh và hình ảnh, v.v., trong đó, vấn đề gửi đến đúng giờ có vai trò quan trọng hơn độ tin cậy, hoặc cho các ứng dụng truy vấn/đáp ứng đơn giản như tra cứu **tên miền**, trong đó, phụ phí của việc thiết lập một kết nối đáng tin cậy lớn một cách không cân xứng.

Một số giao thức khác -transport

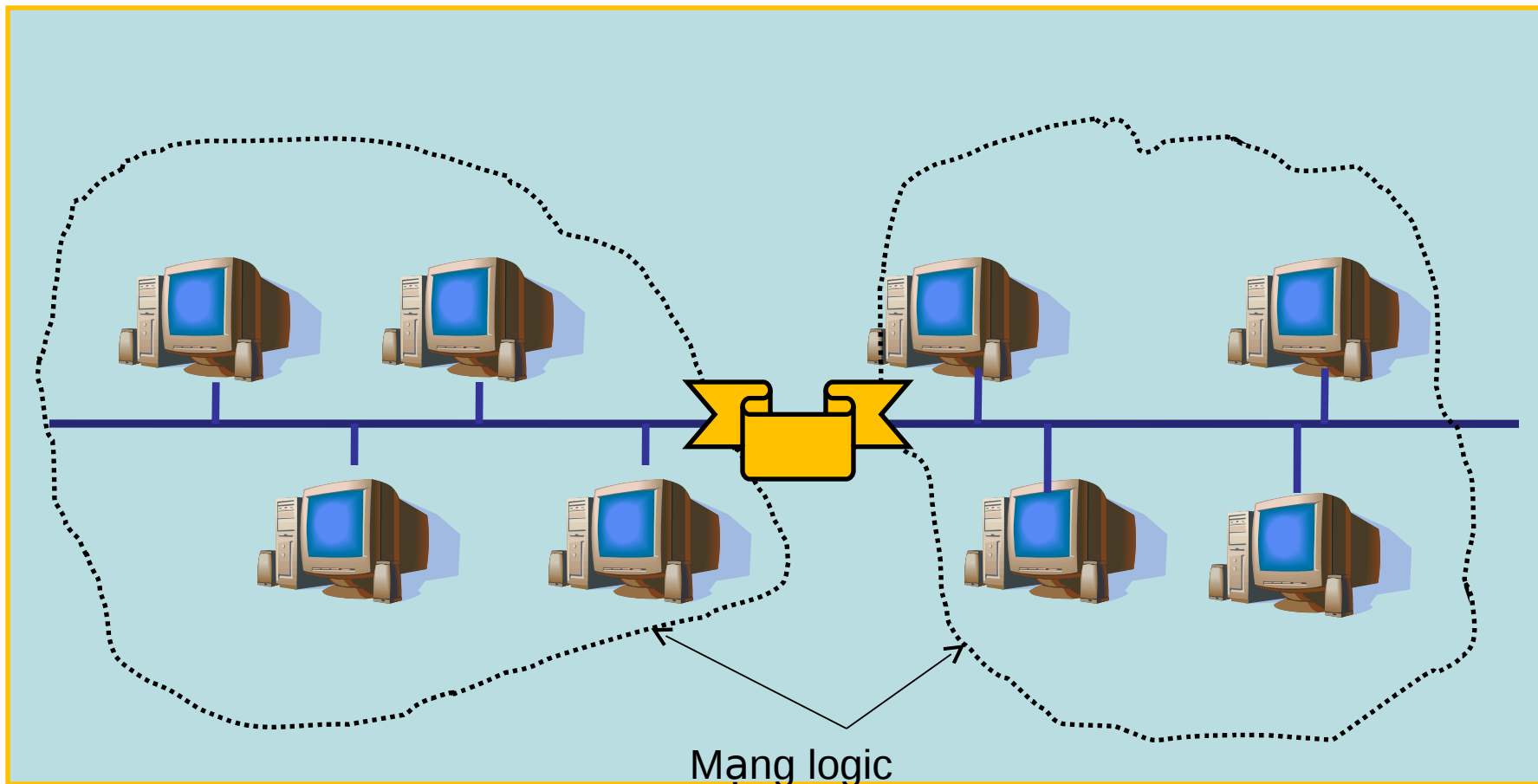
- Giao thức **DCCP** hiện đang được phát triển bởi **IETF** (*Internet Engineering Task Force*). Nó cung cấp nội dung **điều khiển lưu lượng** của TCP, trong khi đối với người dùng, nó giữ bề ngoài như mô hình dịch vụ datagram của UDP.
- Cả TCP và UDP được dùng cho một số ứng dụng bậc cao (*high-level*). Các ứng dụng tại các địa chỉ mạng cho trước được phân biệt bởi **cổng TCP hay UDP** của nó. Theo quy ước, các cổng "nổi tiếng" được liên kết với một số ứng dụng cụ thể. (Xem *Danh sách cổng TCP và UDP*.)
- RTP (*Real-time Transport Protocol* - giao thức giao vận thời gian thực) là một giao thức datagram được thiết kế cho dữ liệu **thời gian thực** (*real-time*), chẳng hạn **hình và tiếng được truyền theo dòng** (*streaming audio and video*). RTP là một giao thức tầng phiên sử dụng định dạng gói tin UDP làm căn bản. Tuy nhiên, nó được đặt vào tầng giao vận của chồng giao thức TCP/IP.

Tầng ứng dụng

- **Tầng ứng dụng** là nơi các chương trình mạng thường dùng nhất làm việc nhằm liên lạc giữa các nút trong một mạng.
- Giao tiếp xảy ra trong tầng này là tùy theo các ứng dụng cụ thể và dữ liệu được truyền từ chương trình, trong định dạng được sử dụng nội bộ bởi ứng dụng này, và được **đóng gói** theo một giao thức tầng giao vận.
- Do chồng TCP/IP không có tầng nào nằm giữa ứng dụng và các tầng giao vận, tầng ứng dụng trong bộ TCP/IP phải bao gồm các giao thức hoạt động như các giao thức tại **tầng trình diễn** và **tầng phiên** của **mô hình OSI**. Việc này thường được thực hiện qua các **thư viện lập trình**.
- Dữ liệu thực để gửi qua mạng được truyền cho tầng ứng dụng, nơi nó được đóng gói theo giao thức tầng ứng dụng. Từ đó, dữ liệu được truyền xuống **giao thức tầng thấp** tại tầng giao vận.
- Hai giao thức tầng thấp thông dụng nhất là **TCP** và **UDP**. Mỗi ứng dụng sử dụng dịch vụ của một trong hai giao thức trên đều cần có **cổng**. Hầu hết các ứng dụng thông dụng có các cổng đặc biệt được cấp sẵn cho các **chương trình phục vụ (server)** (**HTTP** - Giao thức truyền siêu văn bản dùng cổng 80; **FTP** - Giao thức truyền tệp dùng cổng 21, v.v..) trong khi các **trình khách (client)** sử dụng các **cổng tạm thời (ephemeral port)**.
- Các **thiết bị định tuyến** và **thiết bị chuyển mạch** không sử dụng tầng này nhưng các ứng dụng **điều chỉnh thông lượng (bandwidth throttling)** thì có dùng.

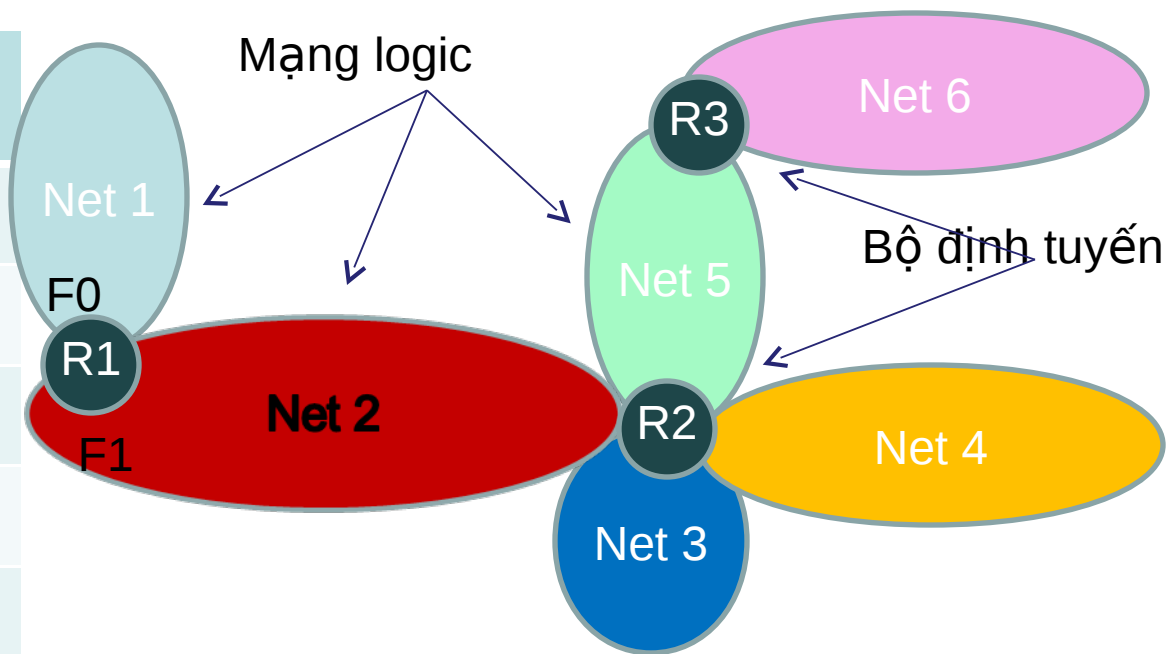
Internet

Mạng vật lý



Bảng định tuyến R1

net	interface	Hop count
Net 1	F0	0
Net 2	F1	0
Net 3	F1	1
Net 4	F1	1
Net 5	F1	1
Net 6	F1	2



IP

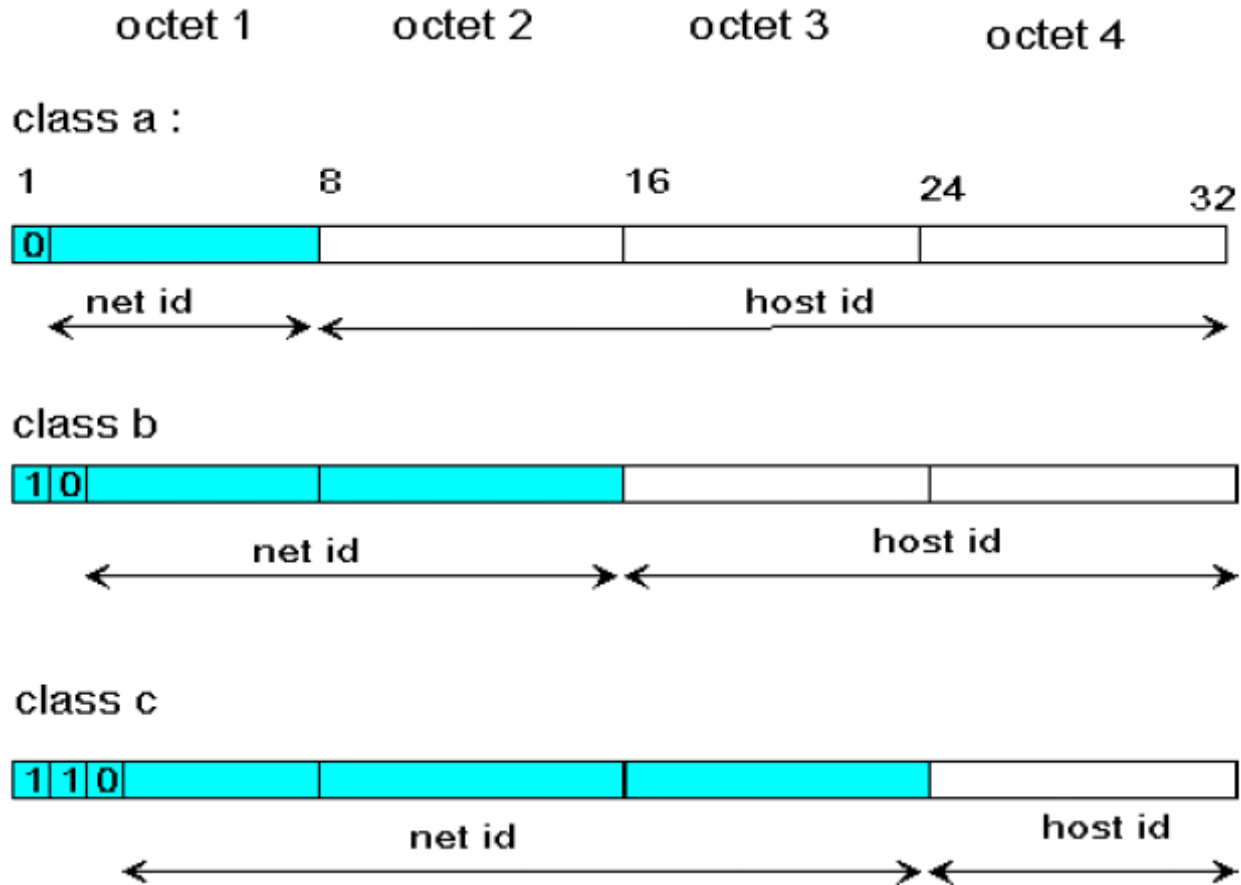
- mạng Internet tổ chức chỉ có một cấp, các mạng máy tính dù nhỏ, dù to khi nối vào Internet đều bình đẳng với nhau
- mỗi một khách hàng hay một máy chủ (Host) hoặc Router đều có một địa chỉ internet duy nhất mà không được phép trùng với bất kỳ ai

- Để địa chỉ không được trùng nhau cần phải có cấu trúc địa chỉ đặc biệt quản lý thống nhất
- Tổ chức của Internet gọi là Trung tâm thông tin mạng Internet - Network Information Center (NIC) chủ trì phân phối, NIC chỉ phân địa chỉ mạng (Net ID) còn
- địa chỉ máy chủ trên mạng đó (Host ID) do các Tổ chức quản lý Internet của từng quốc gia một tự phân phối

Cấu trúc địa chỉ IP

- Địa chỉ IP đang được sử dụng hiện tại (IPv4) có 32 bit chia thành 4 Octet (mỗi Octet có 8 bit, tương đương 1 byte) cách đếm đều từ trái qua phải bit 1 cho đến bit 32, các Octet tách biệt nhau bằng dấu chấm (.)
- X.X.X.X
- Với x :0-255
- 203.162.8.197 → 11001011.10100010.00001000.11000101
- 2.7.300.40 **x**

Các lớp địa chỉ IP



Khoảng IP của các lớp

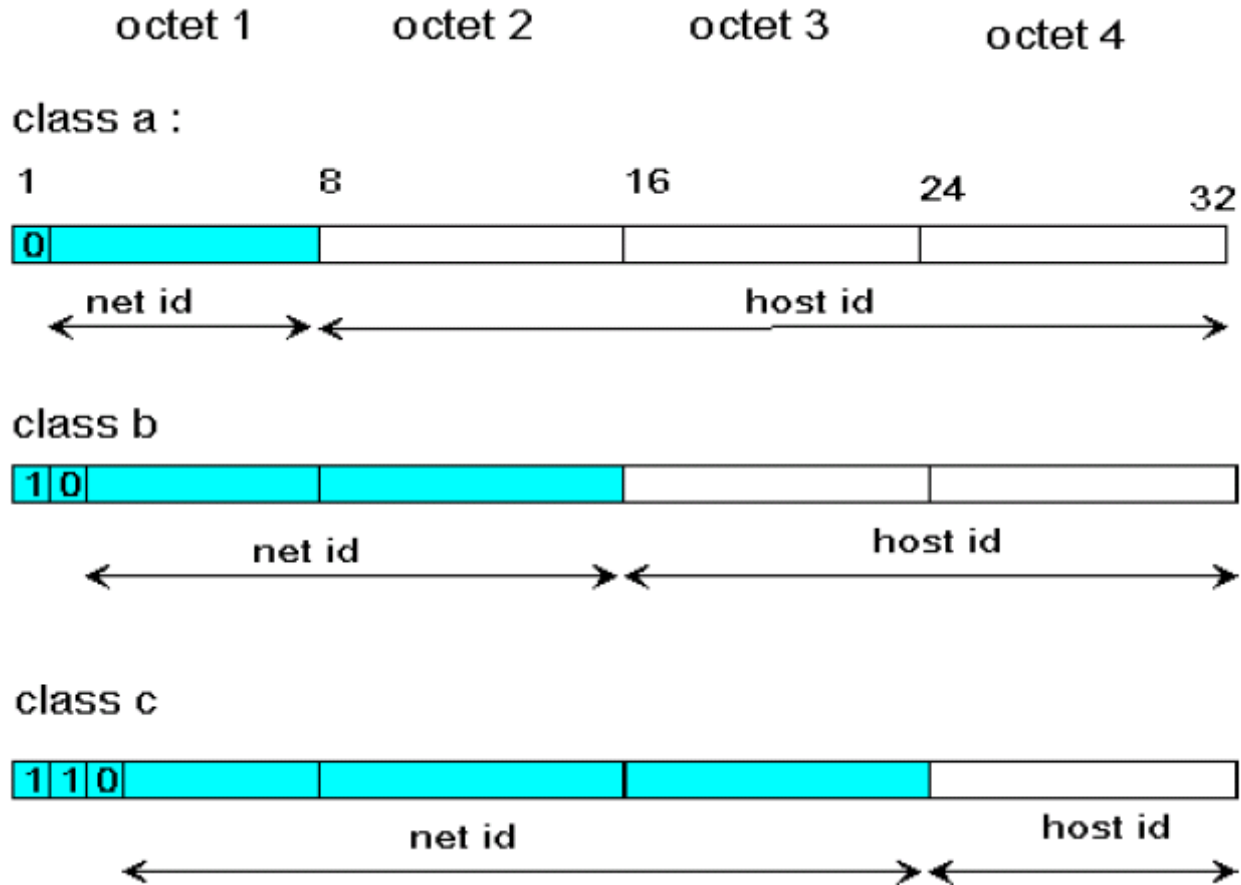
- A Từ 0.0.0.0 đến 127.0.0.0
- B Từ 128.0.0.0 đến 191.255.0.0
- C Từ 192.0.0.0 đến 223.255.255.0
- D Từ 224.0.0.0 đến 239.255.255.0 Không phân
- E Từ 240.0.0.0 đến 255.0.0.0 Không phân

Cấu trúc logic

- Có 2 phần
- netID : địa chỉ mạng
- hostID địa chỉ máy trên netID



Net ID của mot IP



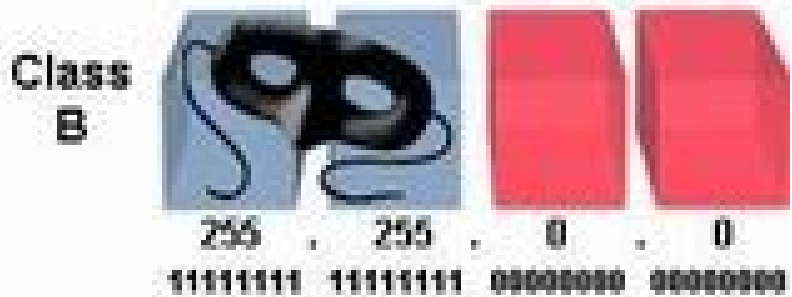
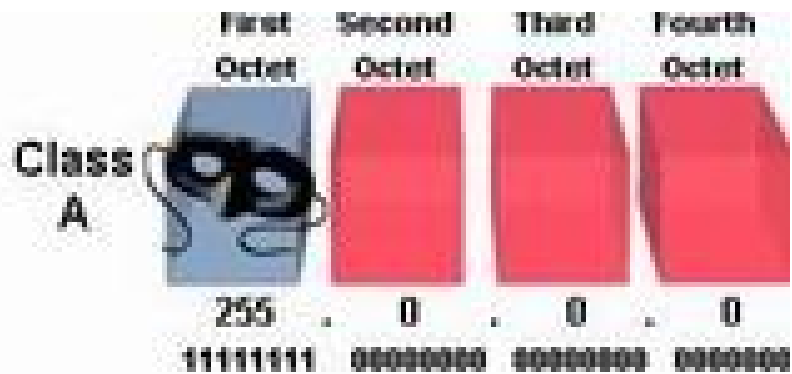
Ví dụ

- 192.168.13.7
- 156.89.123.89
- 19.56.2.1
- 89.2.4.5

- 67.89.56.89
- 67.78.87.78
- 156.90.123.80

Net mask

- Là một dãy số 32 bit dùng để nhận diện ra netID
- $\text{netID} = \text{IP address AND netmask}$
- Ví dụ:
- IP 203.162.7.123 netmask 255.255.255.0
✂ → netID= IP 203.162.7.0
- IP 203.162.7.123 netmask 255.255.0.0
✂ → netID= IP ?????
- IP 203.162.0.123 netmask 255.255.255.0
✂ → netID= IP ?????



Bảng tóm tắt

Lớp	netID	subnetmask	Số máy/mạng	Số mạng
A	x.0.0.0	255.0.0.0	256*256*256	128
B	x.x.0.0	255.255.0.0	256*256	64*256
C	x.x.x.0	255.255.255.0	256	32*256*256

Một số địa chỉ đặc biệt

- Địa chỉ loopback là các địa chỉ có 127.x.x.x
- Địa chỉ broad cast là địa chỉ mạng sẽ dùng để quảng bá mạng mình cho các mạng khác biết . Mục đích giúp cho các router cập nhật bảng định tuyến
- Địa chỉ broadcast được qui định là địa chỉ cuối cùng của một mạng
- Ví dụ: 167.8.5.0 thì broadcast là 167.8.255.255
- 192.45.67.1
- 154.63.72.5

Một số lưu ý

- Các máy cùng mạng sẽ có cùng NETID, subnetmask và khác host ID
- 2 máy khác mạng hoặc khác NET ID hoặc khác subnet mask

Private address

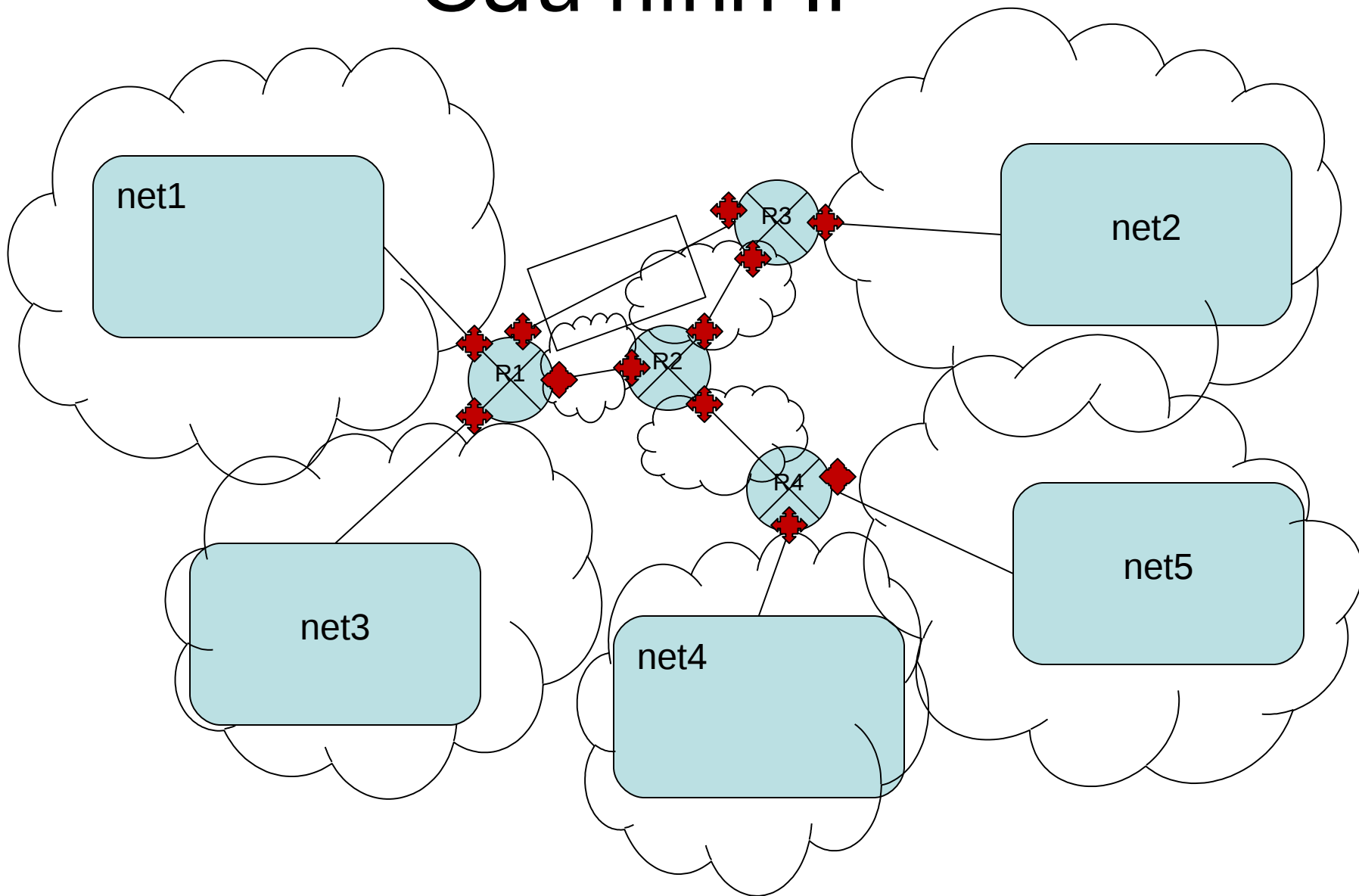
- Là vùng địa chỉ cho phép cấu hình mạng cục bộ mà không cần phải mua
- Không được sử dụng trên internet để cấp phát

Lớp	Khoảng mạng	Số mạng
A	10.0.0.0	1
B	172.16.0.0-172.31.0.0	16
C	192.168.x.0	256

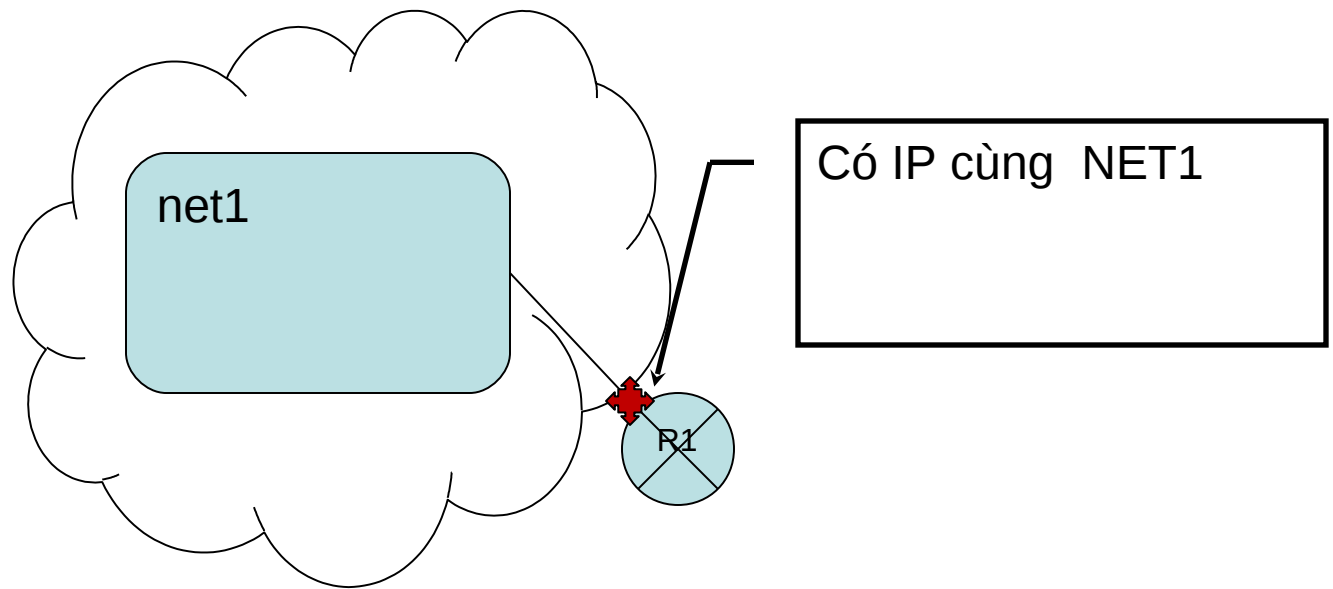
Cách chia mạng con

- Một NETID thật trên internet phải mua
- Do nhu cầu chia tách mạng con trong 1 đơn vị
- Do số máy trên một mạng quá nhiều
✂ → chia nhỏ mạng → nhiều mạng con

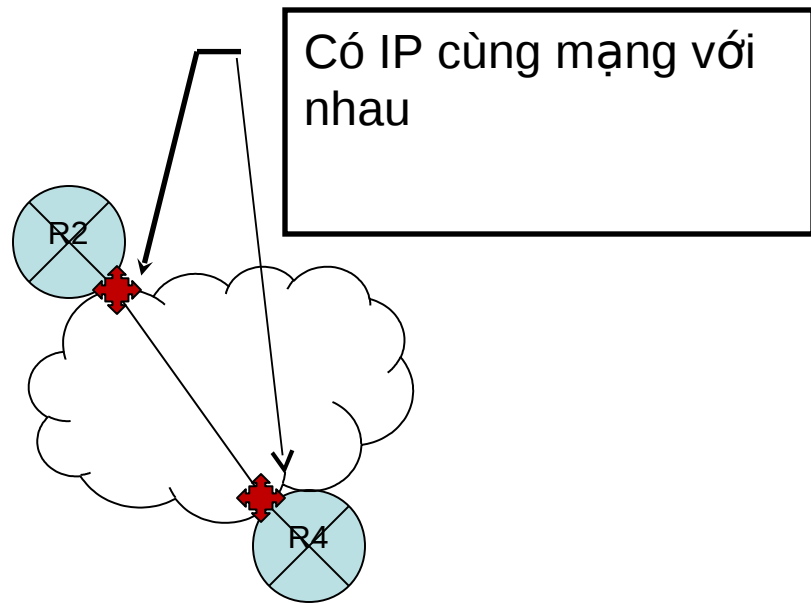
Cấu hình IP

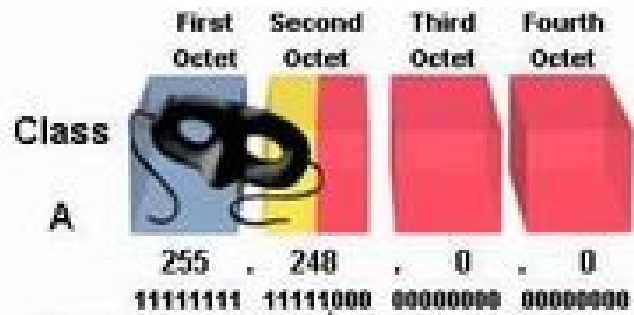


Cấu hình IP



Cấu hình IP

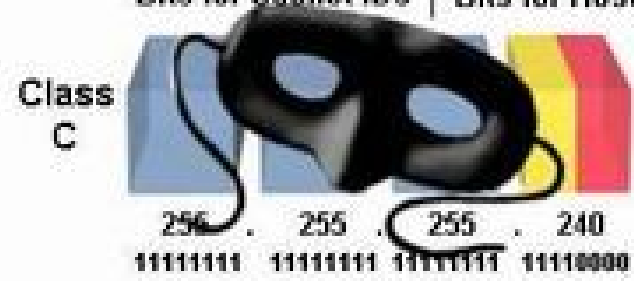


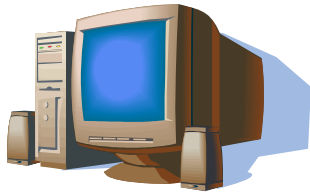


Bits for Subnet IDs | Bits for Host IDs

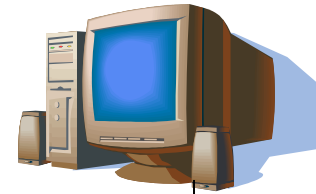


Bits for Subnet IDs | Bits for Host IDs





192.168.1.57



192.168.1.51



255.255.255.0



255.255.255.192



255.255.255.248



- 0... 10000000 000...
- 1... 001...
- 00... 010...
- 01... 011... 11100000
- 10... 11000000 100...
- 11... 101...
110...
111...

Ví dụ

- 57 : 00101111
- 90 : 01011010
- 172.16.1.3 255.255.255.0
- 172.17.7.8 255.255.0.0
- 172.30.1.8 255.255.255.192
- 192.168.1.8 255.255.255.0

Cách chia

- Có m bit còn dư
- Mượn n bit
- Vậy có thể có 2^n mạng ,
- $2^n - 2$ mạng được sử dụng
- Số bù là $m < 8 \rightarrow (2^{m-n}) / 2^8$
- $M > 8 \rightarrow ((2^{m-n}) / 256) \bmod 256$ (***)
- Số trong subnetmask : $(2^m - 2^{m-n}) \bmod 256$
- $N < 8 \rightarrow x$
- Nếu $n > 8 \rightarrow 255.x$
- $n > 16 \rightarrow 255.255.x$

Số bù dùng để

- Số bù dùng để ghi khoảng mạng
- Vd : số bù là 32 của mạng 172.16.0.0
- Mạng 1 172.16.0.0
172.16.31.255
- Mạng 2 . 172.16.32.0
172.16.63.255
- Mạng 3 172.16.64.0
172.16.95.255
- Mạng : 172.16.96.0

- Số máy trên 1 mạng con là:
- $2^{m-n} - 2$ máy trên mạng

- Mượn 1 bit có 2 mạng \rightarrow số bù là 128 \rightarrow 128
- Mượn 2 bit có 4 mạng \rightarrow số bù là 64 \rightarrow 192
- Mượn 3 bit có 8 mạng \rightarrow số bù là 32 \rightarrow 224
- Mượn 4 bit có 16 mạng \rightarrow số bù là 16 \rightarrow 240
- Mượn 5 bit có 32 mạng \rightarrow số bù là 8 \rightarrow 248
- Mượn 6 bit có 64 mạng \rightarrow số bù là 4 \rightarrow 252
- Mượn 7 bit có 128 mạng \rightarrow số bù là 2 \rightarrow 254
- Mượn 8 bit có 256 mạng \rightarrow số bù là 1 \rightarrow 255

Bài tập

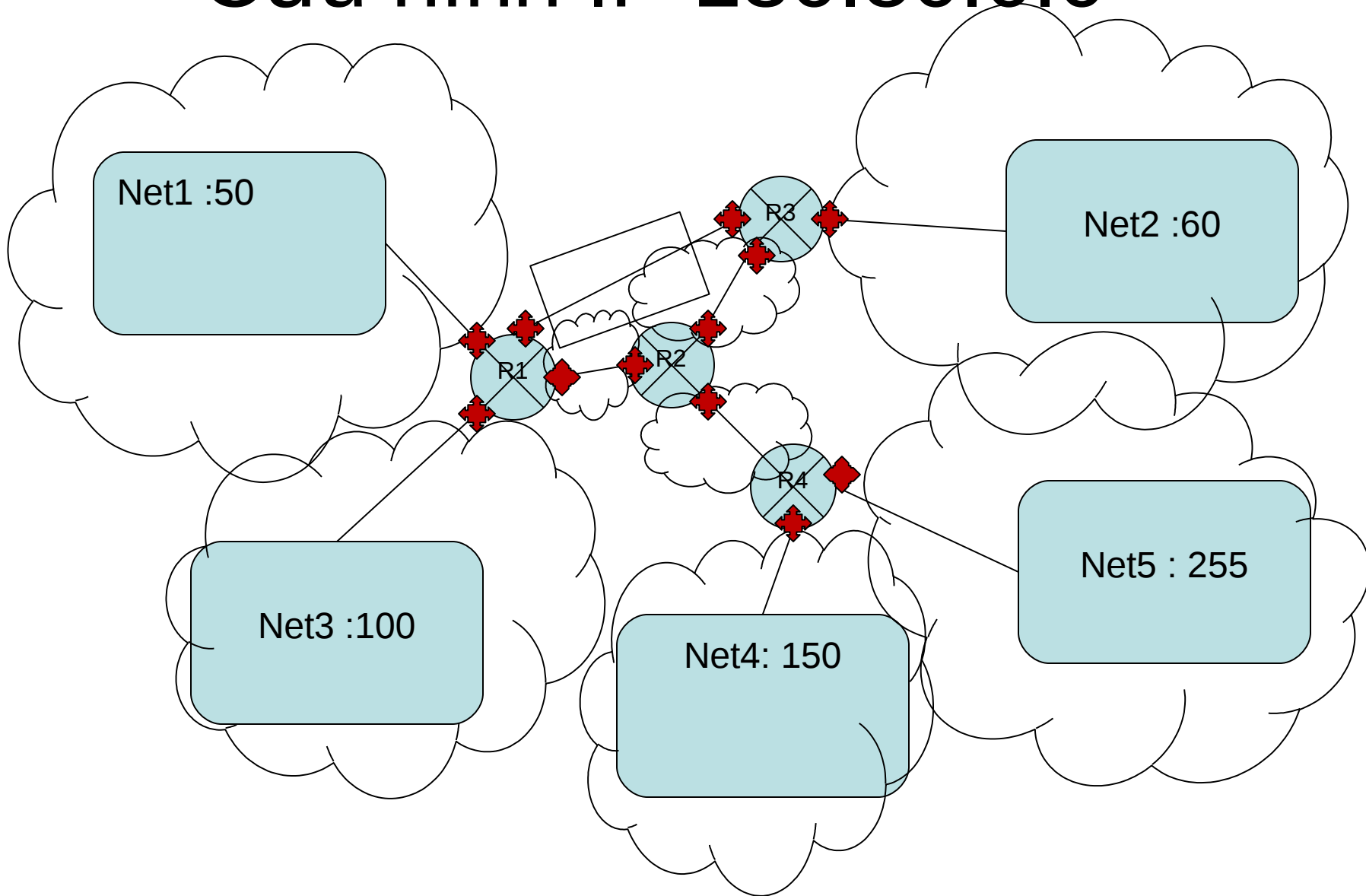
- Kiểm tra xem các IP có cùng mạng hay không
- Cho 178.203.123.1 và 178.203.132.100
 - a) Subnetmask là 255.255.255.0
 - b) Subnetmask là 255.255.0.0
 - c) Subnetmask là 255.0.0.0
 - d) Subnetmask là 255.255.192.0
 - e) Subnetmask là 255.255.224.0
 - f) Subnetmask là 255.255.255.224

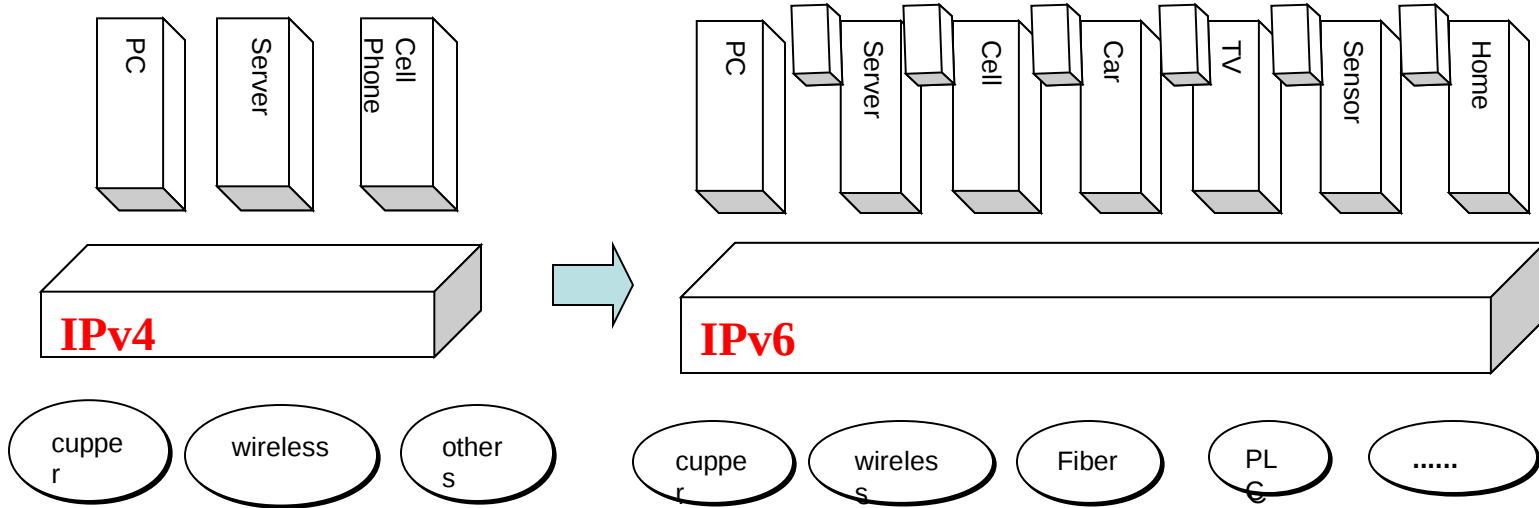
Bài tập 2

- Một công ty mua được một khoảng mạng là 159.7.0.0 công ty có 14 phòng làm việc và muốn mỗi phòng có thể có 255 máy và độc lập với nhau(khác mạng)
- Hãy chia mạng con và cho biết khoảng mạng như thế nào

- 19.168.1.0 255.255.255.0
- 19.0.0.0
- Cần chia 8 mạng phải sử dụng được
- Các mạng là gì
- Địa chỉ mạng, địa chỉ broadcast của từng mạng
- Số máy trên 1 mạng
- subnetmask

Cấu hình IP 130.50.0.0





Sự biến đổi của Internet

1.3. Mục tiêu phát triển IPv6

IPv6 được thiết kế với những mục tiêu và ưu điểm sau:

- * Không gian địa chỉ lớn hơn và dễ dàng quản lý không gian địa chỉ.
- * Hỗ trợ kết nối đầu cuối-đầu cuối và loại bỏ hoàn toàn công nghệ NAT
- * Quản trị TCP/IP dễ dàng hơn: DHCP được sử dụng trong IPv4 nhằm giảm cấu hình thủ công TCP/IP cho host. IPv6 được thiết kế với khả năng tự động cấu hình, không cần sử dụng máy chủ DHCP, hỗ trợ hơn nữa trong việc giảm cấu hình thủ công.
- * Cấu trúc định tuyến tốt hơn: Định tuyến IPv6 được thiết kế hoàn toàn phân cấp.

1.3. Mục tiêu phát triển IPv6 (2)

* **Hỗ trợ tốt hơn Multicast**: Multicast là một tùy chọn của địa chỉ IPv4, tuy nhiên khả năng hỗ trợ và tính phổ dụng chưa cao.

* **Hỗ trợ bảo mật tốt hơn**: IPv4 được thiết kế tại thời điểm chỉ có các mạng nhỏ, biết rõ nhau kết nối với nhau. Do vậy bảo mật chưa phải là một vấn đề được quan tâm. Song hiện nay, bảo mật mạng internet trở thành một vấn đề rất lớn, là mối quan tâm hàng đầu.

* **Hỗ trợ tốt hơn cho di động**: Thời điểm IPv4 được thiết kế, chưa tồn tại khái niệm về thiết bị IP di động. Trong thế hệ mạng mới, dạng thiết bị này ngày càng phát triển, đòi hỏi cấu trúc giao thức Internet có sự hỗ trợ tốt hơn.

2. Đặc điểm của IPv6

- * Định dạng Header mới.
- * Vùng địa chỉ lớn.
- * Cơ sở hạ tầng định tuyến và đánh giá địa chỉ phân cấp và hiệu quả.
- * Cấu hình địa chỉ Stateless and stateful .
- * Bảo mật Built-in .
- * Hỗ trợ tốt hơn cho QoS - Quality of Service
- * Giao thức mới cho sự tương tác nút kế .
- * Có khả năng mở rộng ra.

1. Không gian địa chỉ IPv6

Hầu hết đặc tính của địa chỉ IPv6 là sử dụng nhiều địa chỉ lớn. Kích thước của một địa chỉ IPv6 là 128 bit gấp 4 lần địa chỉ IPv4. Không gian địa chỉ 32 bit cho phép 2^{32} hoặc 4,294,967,296 địa chỉ. Không gian 128 bit cho phép 2^{128} hoặc

340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×10^{38}) địa chỉ.

2. Cú pháp địa chỉ IPv6

Địa chỉ IPv6 có độ dài là 128 bit nhị phân, được phân thành 8 nhóm, mỗi nhóm là khối 16 bit, mỗi khối 16 bit này được chuyển dạng hexa 4 bit và được phân biệt với nhau bằng dấu hai chấm (“ : ”)

2. Cú pháp địa chỉ IPv6 (2)

Ví dụ :

- Cho một địa chỉ IPv6 ở dạng nhị phân như sau:

```
0010000111011010000000001101001100000000000000000010111100111011000
0001010101010000000001111111111111110001010001001110001011010
```

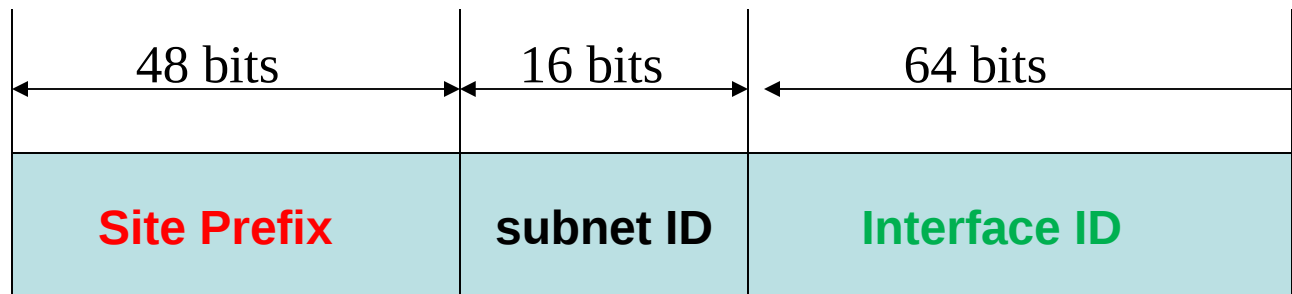
- Địa chỉ được chia thành từng khối 16 bit như sau :

```
0010000111011010  0000000011010011  0000000000000000  0000000000000000
0000000000000000  0000000000000000  111111000101000  1001110001011010
```

- Mỗi khối được chuyển sang 4 số hexa và chia cách nhau bằng dấu 2 chấm(“ : ”)

```
21DA:00D3:0000:0000:0000:0000:FE28:9C5A
```

21DA:00D3:0000:0000:0000:0000:FE28:9C5A



Hình minh họa các phần của địa chỉ IP v6

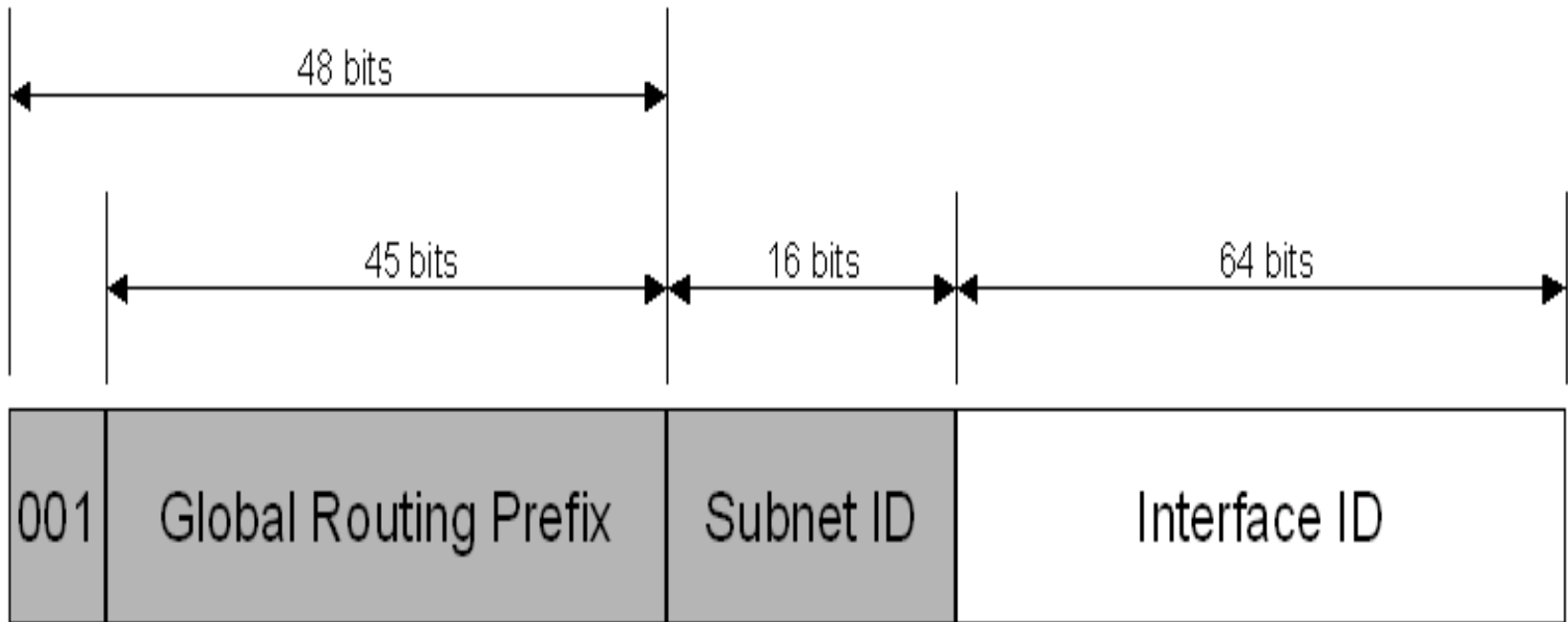
Chú ý: IPv6 chỉ dùng tiền tố chứ không dùng subnet mask như IPv4.

5. Địa chỉ Unicast IPv6

- * Địa chỉ Unicast toàn cầu
- * Địa chỉ Link-local
- * Địa chỉ Site-local
- * Địa chỉ đặc biệt
- * Địa chỉ tương thích

a. Địa chỉ Unicast toàn cầu

- Đây là dạng địa chỉ tương đương với địa chỉ IPv4 public. Chúng được định tuyến và có thể liên kết tới trên phạm vi toàn cầu. Việc phân bổ và cấp phát dạng địa chỉ này do hệ thống các tổ chức quản lý địa chỉ quốc tế đảm nhiệm. Phạm vi tính duy nhất của địa chỉ Unicast định danh toàn cầu là toàn bộ mạng Internet IPv6.
- Không như địa chỉ IPv4, với cấu trúc định tuyến vừa phân cấp, vừa không phân cấp, địa chỉ Internet IPv6 được cải tiến trong thiết kế để đảm bảo có một cấu trúc định tuyến và đánh địa chỉ phân cấp rõ ràng.
- Mục tiêu quan trọng nhất trong quản lý địa chỉ IPv4 là “sử dụng hiệu quả, tiết kiệm”, “tính tổ hợp”, “tính có đăng ký”. Đối với địa chỉ IPv6, mục tiêu hàng đầu là “tính tổ hợp”.

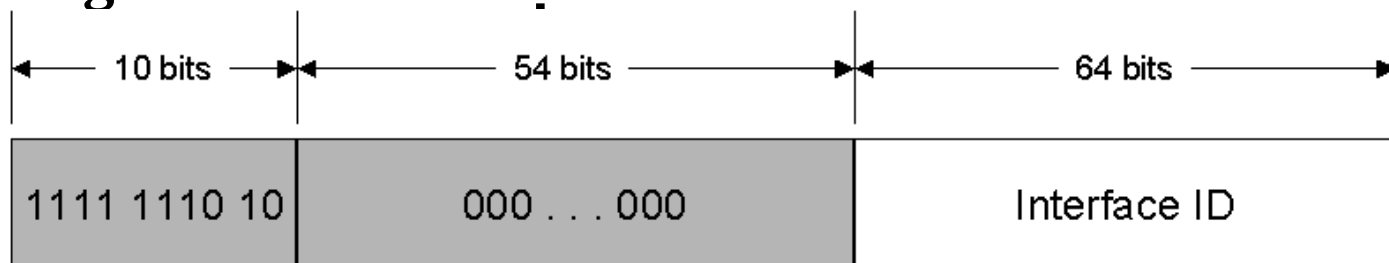


Địa chỉ Unicast toàn cầu

b. Địa chỉ Link-local

Các địa chỉ link-local được dùng bởi các node khi truyền thông với các node láng giềng trên cùng một liên kết. Ví dụ: như trên cùng một mạng IPv6 liên kết đơn không có router, các địa chỉ link-local được dùng để truyền thông giữa các host trên link.

Một địa chỉ link-local cần thiết cho các quá trình xử lý discovery láng giềng và luôn luôn tự động được cấu hình ngay cả khi không có tất cả các địa chỉ UNICAST khác.



Mô tả cấu trúc của một Link-Local

Địa chỉ Link-Local luôn bắt đầu với FE80. Và với 64 bit xác định Interface. Prefix cho địa chỉ Link-Local luôn là: FE80::/64. Một router IPv6 không chuyển lưu lượng IPv6 vượt ngoài giới hạn liên kết.

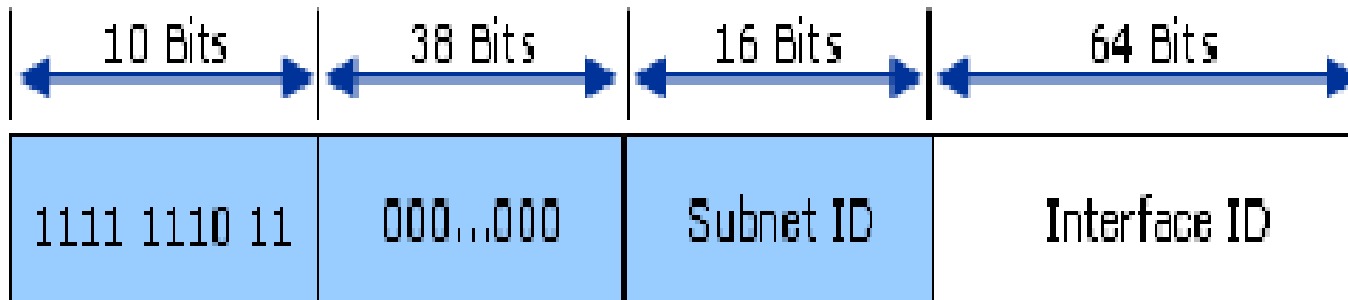
c. Địa chỉ Site-local

★ Địa chỉ IPv6 Site-local được thiết kế với mục đích sử dụng trong phạm vi một mạng, tương đương với địa chỉ dùng riêng (private) trong IPv4 .

★ Phạm vi tính duy nhất của dạng địa chỉ này là phạm vi trong một mạng dùng riêng

Ví dụ: một mạng office, một tổ hợp mạng office của một tổ chức...

★ Địa chỉ site-local có thể được dùng trùng lặp bởi nhiều tổ chức mà không gây xung đột định tuyến IPv6 toàn cầu.



d. Địa chỉ đặc biệt

IPv6 sử dụng 2 địa chỉ đặc biệt sau :

*** 0:0:0:0:0:0:0:0** hay **::** dạng địa chỉ “không định danh” được sử dụng để thể hiện rằng hiện tại node không có địa chỉ. Địa chỉ **::** được sử dụng làm địa chỉ nguồn cho các gói tin trong thủ tục kiểm tra sự trùng lặp địa chỉ link-local và không được gán cho một giao diện hoặc được sử dụng làm địa chỉ đích.

*** 0:0:0:0:0:0:0:1** hay **::1** được sử dụng làm địa chỉ xác định giao diện loopback, cho phép một node gửi gói tin cho chính nó, tương đương với địa chỉ 127.0.0.1 của IPv4. Các gói tin có địa chỉ đích **::1** không được gửi trên đường link hay forward đi bởi router. Phạm vi của dạng địa chỉ này là phạm vi node

e. Địa chỉ tương thích

Địa chỉ tương thích được định nghĩa nhằm mục đích hỗ trợ việc chuyển đổi từ địa chỉ IPv4 sang địa chỉ IPv6, bao gồm:

- Sử dụng trong công nghệ biên dịch giữa địa chỉ IPv4-IPv6
- Hoặc sử dụng cho một hình thức chuyển đổi được gọi là “đường hầm – tunnel”, lợi dụng cơ sở hạ tầng sẵn có của mạng IPv4 kết nối các mạng IPv6 bằng cách bọc gói tin IPv6 vào trong gói tin đánh địa chỉ IPv4 để truyền đi trên mạng IPv4.