Chương 4: Nội dung

4.1 Giới thiệu

4.2 Các mạng mạch ảo và mạng chuyển gói

4.3 Kiến trúc của bộ định tuyến

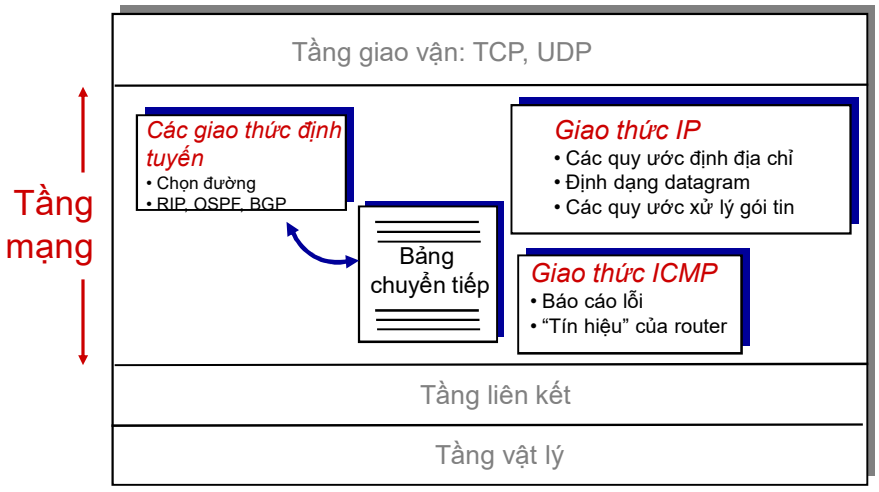
4.4 IP: Internet Protocol
- Định dạng gói tin
- Định địa chỉ IPv4
- ICMP
- IPv6

4.5 Các giải thuật định tuyến
- Link state
- Distance vector
- Hierarchical routing

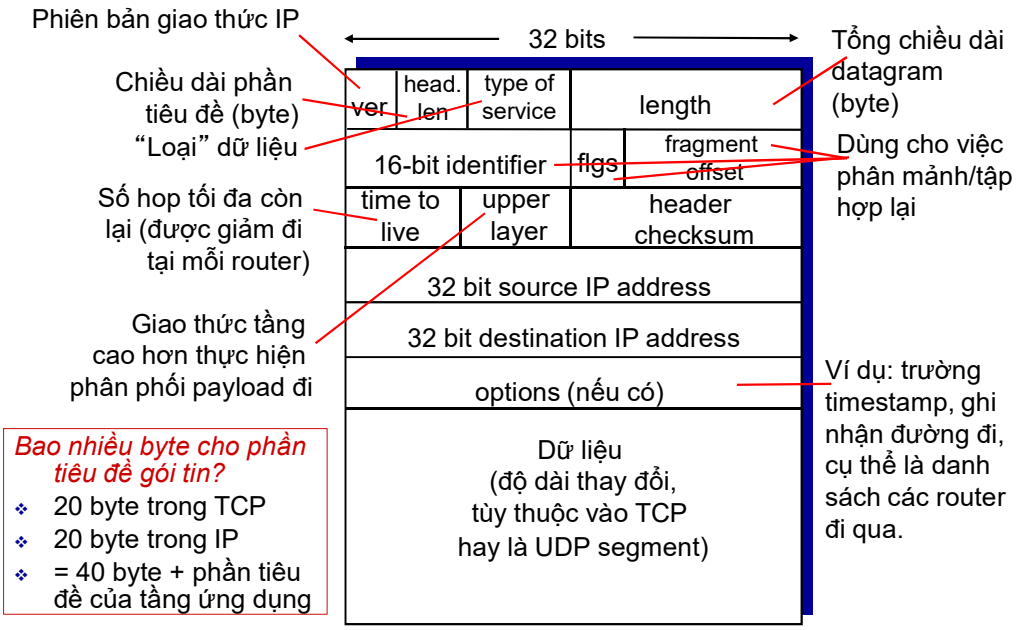
4.6 Định tuyến trong mạng Internet
- RIP
- OSPF
- BGP

Tầng mạng trong mạng Internet

Chức năng của tầng mạng tại bộ định tuyến và host:



Định dạng IP datagram

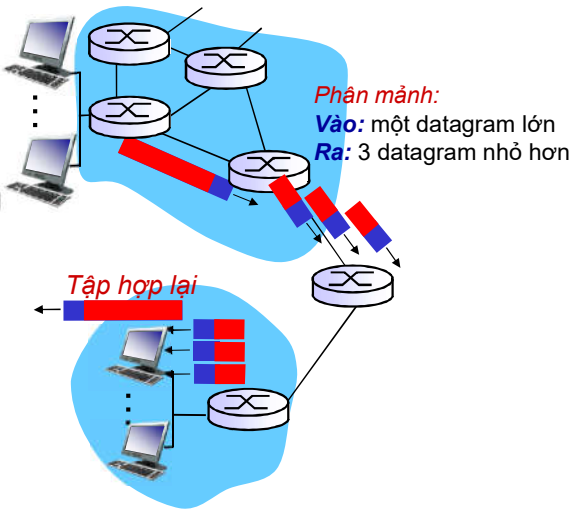


Bao nhiêu byte cho phần tiêu đề gói tin?

- 20 byte trong TCP
- 20 byte trong IP
- = 40 byte + phần tiêu đề của tầng ứng dụng

Phân mảnh và tập hợp lại gói tin IP

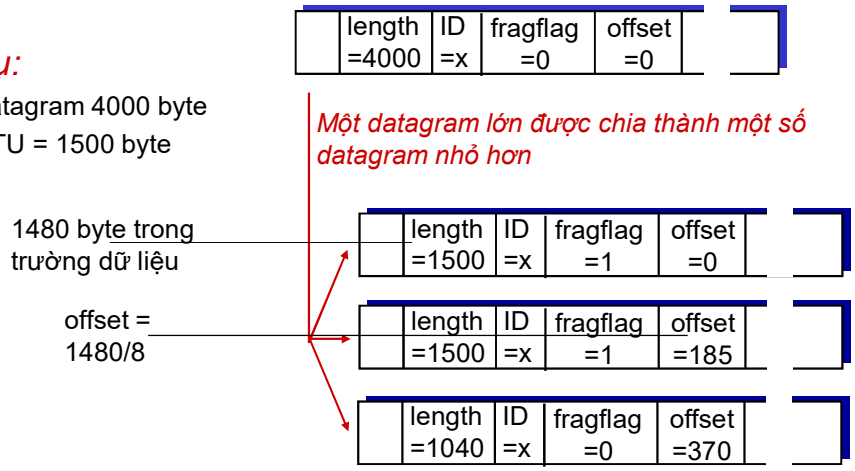
- Các liên kết mạng có MTU (max.transfer size) – frame mức liên kết lớn nhất có thể.
  - Các loại liên kết khác nhau sẽ có MTU khác nhau
- IP datagram lớn sẽ được chia ("phân mảnh") bên trong mạng
  - Một datagram sẽ được chia thành một số datagram
  - Chúng sẽ được "tập hợp lại" tại đích cuối cùng
  - Các bit trong tiêu đề IP được dùng để xác định thứ tự liên quan đến các mảnh



Phân mảnh và tập hợp lại gói tin IP

Ví dụ:

- Datagram 4000 byte
- MTU = 1500 byte



Chương 4: Nội dung

4.1 Giới thiệu

4.2 Các mạng mạch ảo và mạng chuyển gói

4.3 Kiến trúc của bộ định tuyến

4.4 IP: Internet Protocol

- Định dạng gói tin
- Định địa chỉ IPv4
- ICMP
- IPv6

4.5 Các giải thuật định tuyến

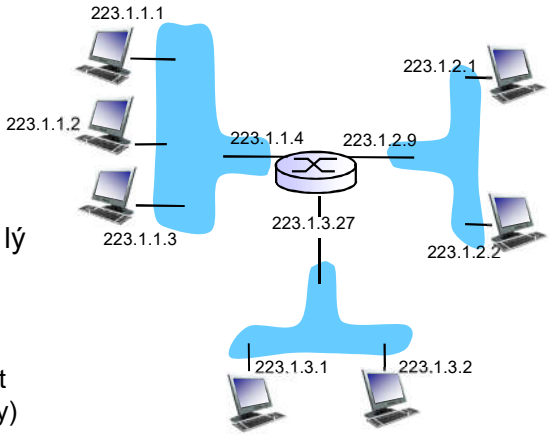
- Link state
- Distance vector
- Hierarchical routing

4.6 Định tuyến trong mạng Internet

- RIP
- OSPF
- BGP

Định địa chỉ IP: giới thiệu

- *Địa chỉ IP:* 32-bit định danh cho *giao diện (interface) của* host và router
- *Giao diện:* kết nối giữa host/router với liên kết vật lý
  - Một router thường có nhiều giao diện
  - Một host có một hoặc hai giao diện (Ví dụ: Ethernet có dây, 802.11 không dây)
- *Địa chỉ IP được gắn với từng giao diện*



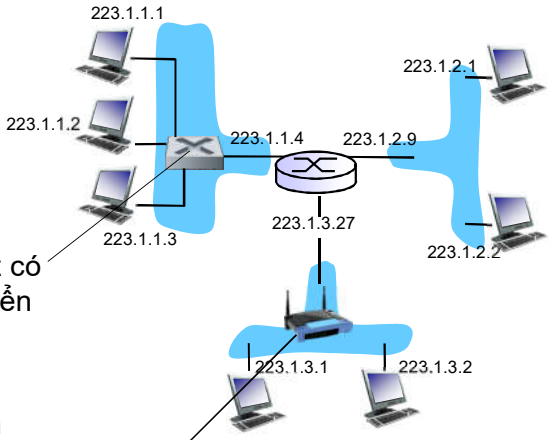
223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Định địa chỉ IP: giới thiệu

Hỏi: Thực tế các giao diện được kết nối như thế nào?

Trả lời: Sẽ học trong các chương sau (5,6).



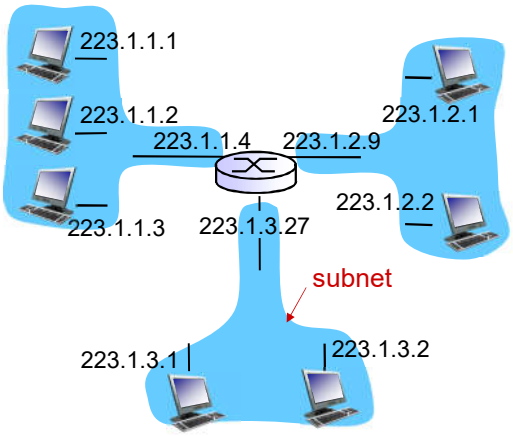
Trả lời: Các giao diện Ethernet có dây được kết nối bởi các chuyển mạch Ethernet

Hiện tại: Không cần quan tâm đến việc các giao diện được kết nối với nhau như thế nào (mà không có sự can thiệp của router)

Trả lời: Các giao diện WiFi không dây được kết nối bởi trạm cơ sở WiFi

Subnet (Mạng con)

- Địa chỉ IP:
  - Phần subnet – các bit cao (bên trái)
  - Phần host – các bit thấp (bên phải)
- *Subnet là gì?*
  - Các giao diện của thiết bị có cùng phần subnet của địa chỉ IP
  - Có thể tìm thấy nhau mà *không cần sự can thiệp của router*

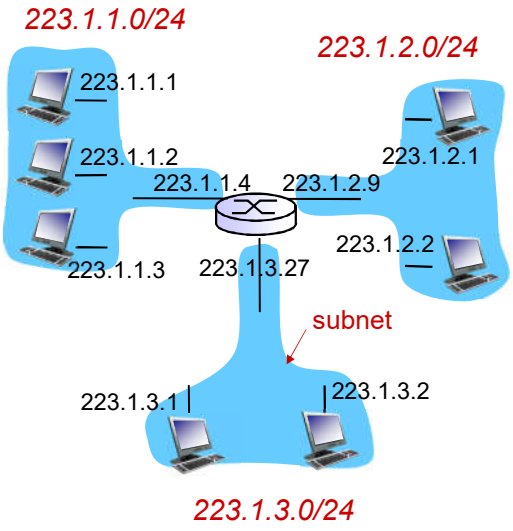


Mạng có 3 subnet

Subnet

Phương pháp

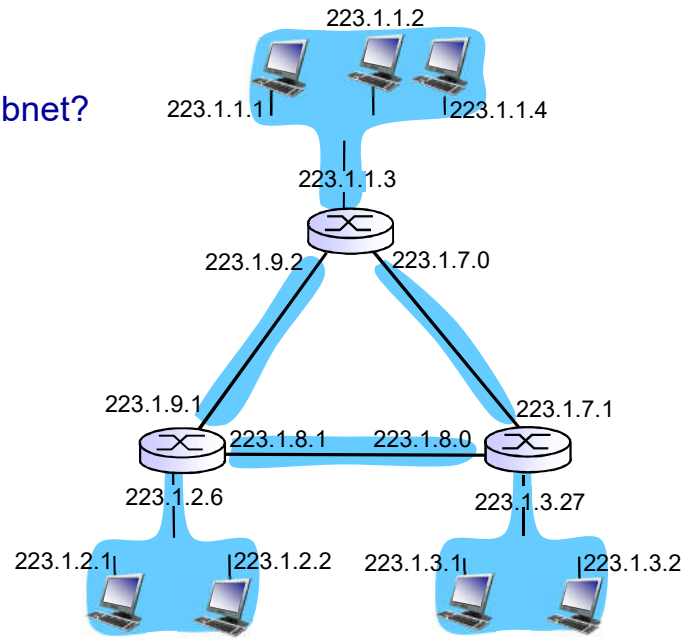
- Để xác định các subnet, tách mỗi giao diện từ host hoặc router, tạo thành các vùng mạng độc lập
- Mỗi mạng độc lập được gọi là một *subnet*



Mặt nạ mạng con (subnet mask): /24

Subnet

Có bao nhiêu subnet?



Định địa chỉ IP: Phân lớp địa chỉ IPv4

	8bits	8bits	8bits	8bits
Class A	0 7bit	H	H	H
Class B	1 0 6bit	N	H	H
Class C	1 1 0 5bit	N	N	H
Class D	1 1 1 0 Multicast			
Class E	1 1 1 1 Reserve for future use			

	# of network	# of hosts
Class A	128	2^24
Class B	16384	65536
Class C	2^21	256

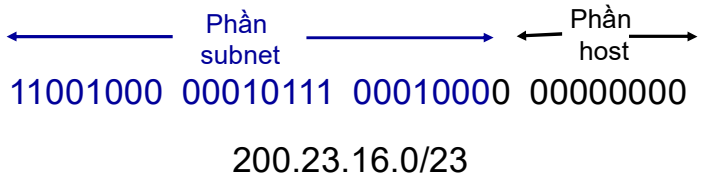
Hạn chế: lãng phí không gian địa chỉ

- Việc phân chia cứng thành các lớp (A, B, C, D, E) làm hạn chế việc sử dụng toàn bộ không gian địa chỉ

Định địa chỉ IP: CIDR

CIDR: Classless Inter Domain Routing

- Phần địa chỉ của subnet có độ dài tùy ý
- Định dạng địa chỉ: a.b.c.d/x, với x là số bit trong phần subnet của địa chỉ



200.23.16.0/23

Làm thế nào để có được một địa chỉ IP?

Hỏi: Làm thế nào để một *host* lấy được một địa chỉ IP?

- Mã hóa cứng trong một tệp bởi người quản trị hệ thống
  - Windows: control-panel->network->configuration->tcp/ip ->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: tự động lấy địa chỉ từ server
  - "plug-and-play"

DHCP: Dynamic Host Configuration Protocol

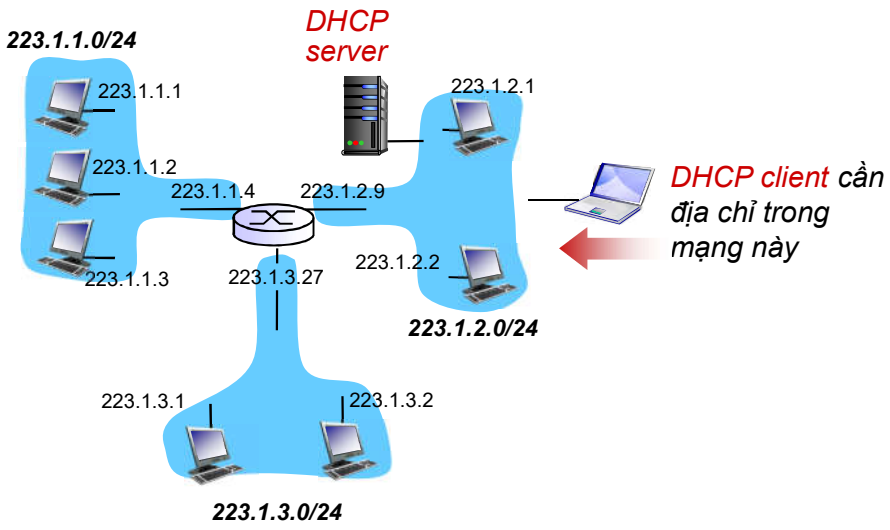
Mục đích: cho phép host có được địa chỉ IP *một cách tự động* từ server mạng khi kết nối vào mạng

- Có thể làm mới địa chỉ đang dùng
- Cho phép dùng lại địa chỉ (chỉ giữ địa chỉ khi đang kết nối)
- Hỗ trợ cho người dùng di động khi muốn kết nối vào mạng

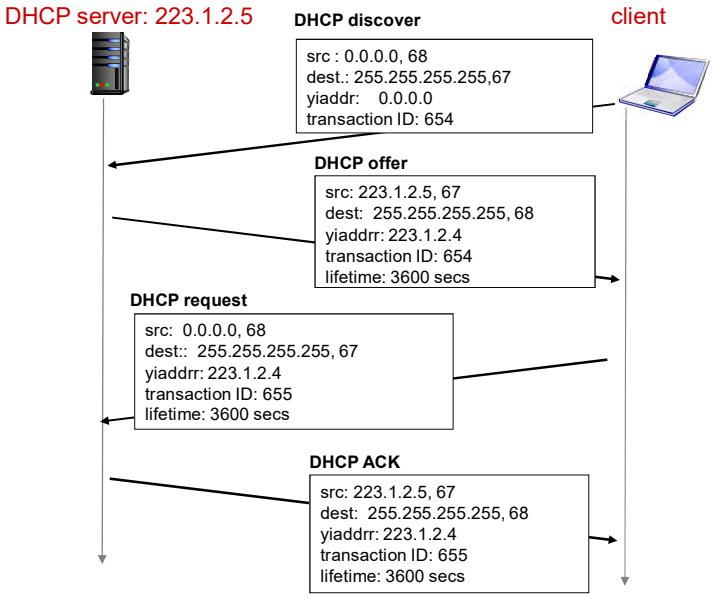
Khái quát DHCP:

- Host gửi thông điệp quảng bá "DHCP discover" [optional]
- DHCP server trả lời bằng thông điệp "DHCP offer" [optional]
- Host yêu cầu địa chỉ IP bằng thông điệp "DHCP request"
- DHCP server gửi địa chỉ bằng thông điệp "DHCP ack"

Kịch bản DHCP client-server



Kịch bản DHCP client-server

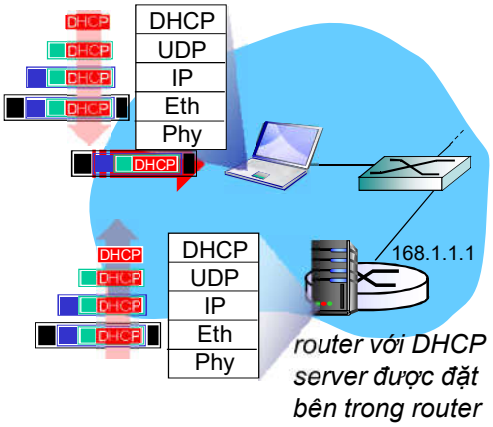


DHCP: có nhiều địa chỉ IP hơn

DHCP có thể cho phép có nhiều địa chỉ IP hơn số địa chỉ IP được phân bổ cho subnet:

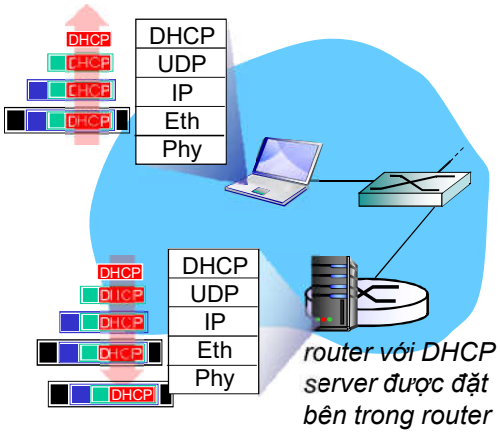
- Địa chỉ của router của hop đầu tiên cho client
- Tên và địa chỉ IP của DNS sever
- Mặt nạ mạng (chỉ ra phần host và phần mạng của một địa chỉ)

DHCP: Ví dụ



- Laptop đang kết nối cần một địa chỉ IP, địa chỉ IP của router của hop đầu tiên, địa chỉ của DNS server: dùng DHCP
- DHCP yêu cầu sẽ được đóng gói trong UDP, UDP được đóng gói trong IP, và IP được đóng gói trong 802.1 Ethernet
- Gửi quảng bá khung Ethernet (đích: FFFFFFFFFFFF) trên mạng LAN, được router đang chạy DHCP server nhận
- Ethernet được cắt bỏ phần tiêu đề thành IP, IP được cắt bỏ phần tiêu đề thành UDP, UDP được cắt bỏ phần tiêu đề thành DHCP.

DHCP: Ví dụ



- DCP server định dạng DHCP ACK bao gồm địa chỉ IP của client, địa chỉ IP của router của hop đầu tiên cho client, tên và địa chỉ IP của DNS server
- Sau khi được đóng gói ở DHCP server, frame được chuyển tiếp cho client, việc cắt bỏ các phần tiêu đề để thành thông điệp DHCP được thực hiện tại client
- Lúc này, client biết được địa chỉ IP của nó, tên và địa chỉ IP của DSN server, và địa chỉ IP của router của hop đầu tiên của nó.

DHCP: đầu ra trong Wireshark (LAN ở nhà)

Yêu cầu

```
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP Request
Option: (61) Client identifier
    Length: 7; Value: 010016D323688A;
    Hardware type: Ethernet
    Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
    Length: 11; Value: 010F03062C2E2F1F21F92B
    1 = Subnet Mask; 15 = Domain Name
    3 = Router; 6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    .....
```

Đáp ứng

```
Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
    Length: 12; Value: 445747E2445749F244574092;
    IP Address: 68.87.71.226;
    IP Address: 68.87.73.242;
    IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."
```


Làm thế nào có được một địa chỉ IP?

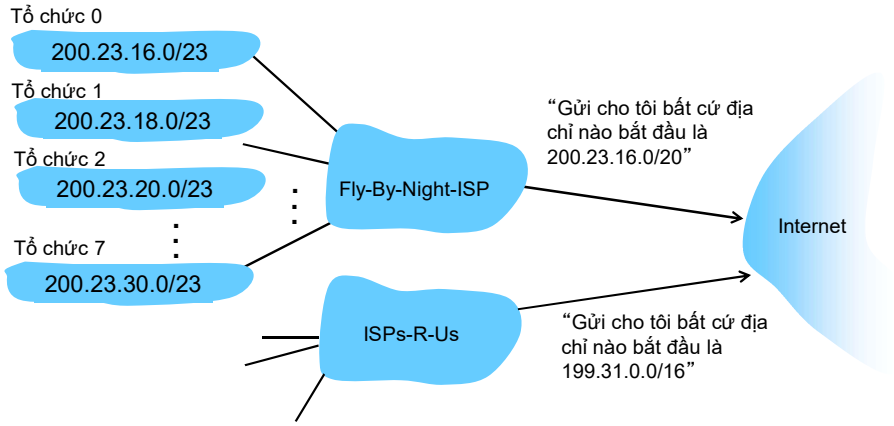
Hỏi: Làm thế nào để mạng có được phần subnet của địa chỉ IP?

Trả lời: Lấy theo phần được phân bổ từ không gian địa chỉ của nhà cung cấp ISP.

Khối của ISP	11001000 00010111 00010000	00000000	200.23.16.0/20
Tổ chức 0	11001000 00010111 00010000	00000000	200.23.16.0/23
Tổ chức 1	11001000 00010111 00010010	00000000	200.23.18.0/23
Tổ chức 2	11001000 00010111 00010100	00000000	200.23.20.0/23
...	.....	....	....
Tổ chức 7	11001000 00010111 00011110	00000000	200.23.30.0/23

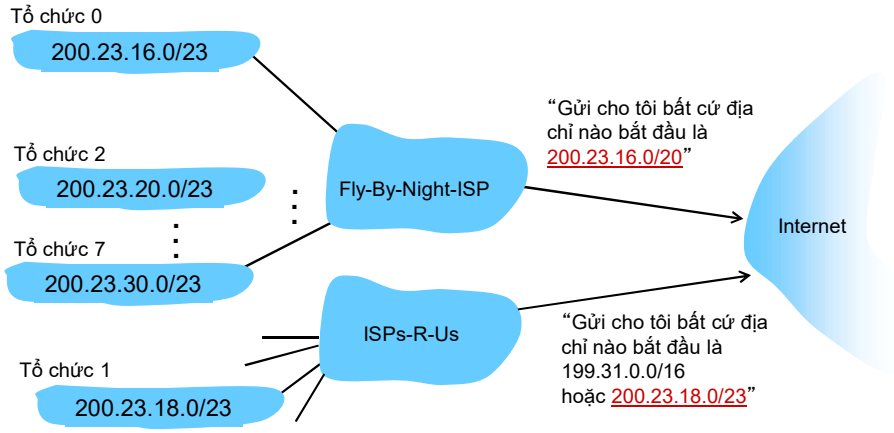
Định địa chỉ phân cấp: tích hợp định tuyến

Định địa chỉ phân cấp cho phép quảng bá hiệu quả thông tin định tuyến:



Định địa chỉ phân cấp: định tuyến cụ thể hơn

ISPs-R-Us có nhiều cách định tuyến cụ thể hơn đến Tổ chức 1



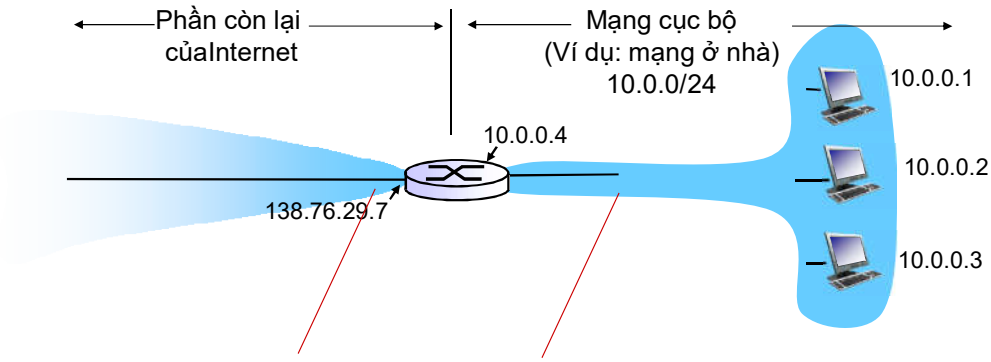
Định địa chỉ IP...

Hỏi: Làm thế nào một ISP có thể lấy được khối địa chỉ?

Trả lời: ICANN: Internet Corporation for Assigned Names and Numbers http://www.icann.org/

- Phân bổ địa chỉ
- Quản lý DNS
- Gán các tên miền, giải quyết tranh chấp

NAT: network address translation (chuyển đổi địa chỉ mạng)



Tất cả các datagram *đi ra khỏi* mạng cục bộ đều có *cùng* địa chỉ IP NAT nguồn duy nhất là 138.76.29.7 với các số hiệu cổng nguồn khác nhau

Các datagram với nguồn và đích khác nhau trong mạng này có địa chỉ 10.0.0/24 cho nguồn và đích

NAT: network address translation

Lý do: Mạng cục bộ chỉ dùng một địa chỉ IP đối với hệ thống mạng bên ngoài:

- Không cần thiết sử dụng cả dãy địa chỉ từ một ISP: chỉ cần một địa chỉ cho tất cả các dịch vụ
- Có thể thay đổi địa chỉ của dịch vụ trong mạng cục bộ mà không cần thông báo với hệ thống mạng bên ngoài.
- Có thể thay đổi ISP mà không cần thay đổi địa chỉ của các dịch vụ bên trong mạng cục bộ
- Hệ thống mạng bên ngoài không nhìn thấy, cũng không biết được địa chỉ rõ ràng của các thiết bị bên trong mạng cục bộ (tăng tính bảo mật)

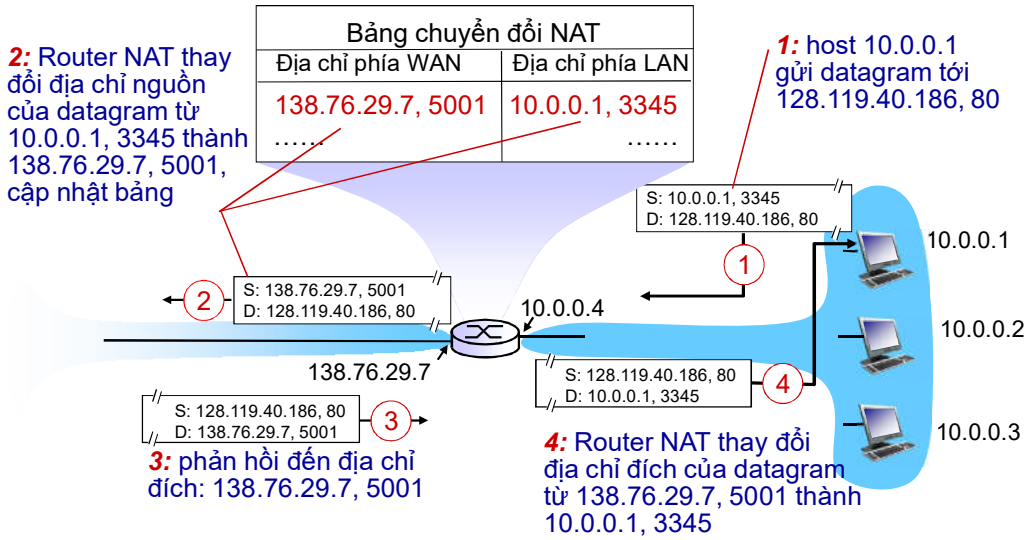
NAT: network address translation

Cài đặt: Router NAT phải:

- *Các datagram đi ra: thay thế* (địa chỉ IP nguồn, số cổng) của mỗi datagram đi ra ngoài thành (địa chỉ IP NAT, số cổng mới)

  . . . các client/server ở xa sẽ dùng (địa chỉ IP NAT, số cổng mới) như là địa chỉ đích
- *Ghi nhớ (trong bảng chuyển đổi NAT)* mọi cặp chuyển đổi (địa chỉ IP nguồn, số cổng) thành (địa chỉ IP NAT, số cổng mới)
- *Các datagram đi đến: thay thế* (địa chỉ IP NAT, số cổng mới) trong trường địa chỉ đích của mọi datagram đi đến thành (địa chỉ IP nguồn, số cổng) tương ứng được lưu trong bảng NAT.

NAT: network address translation

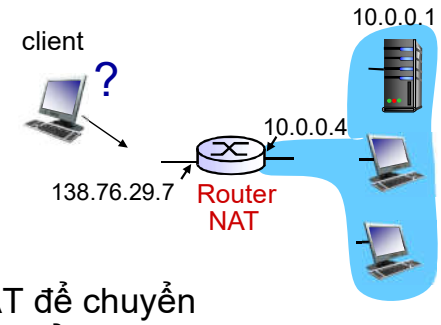


NAT: network address translation

- Trường số hiệu cổng gồm 16-bit :
  - 60.000 kết nối đồng thời chỉ với một địa chỉ phía LAN!
- NAT hiện vẫn còn đang gây tranh cãi
  - Các router chỉ nên xử lý đến tầng 3
  - Vi phạm thỏa thuận end-to-end
    - Các nhà thiết kế ứng dụng phải xem xét đến khả năng NAT, ví dụ ứng dụng P2P
  - Việc thiếu địa chỉ nên được thay bằng cách giải quyết là dùng IPv6

Vấn đề đi qua NAT

- Client muốn kết nối tới server có địa chỉ 10.0.0.1
  - Địa chỉ 10.0.0.1 của server được đặt trong mạng LAN (client không thể sử dụng địa chỉ này là địa chỉ đích)
  - Từ bên ngoài, client chỉ nhìn thấy địa chỉ NAT là 138.76.29.7

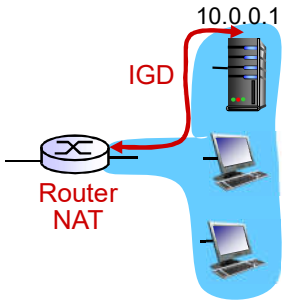


- *Giải pháp 1:* Cấu hình tĩnh NAT để chuyển tiếp các yêu cầu kết nối đến tới cổng đã xác định của server
  - Ví dụ: (138.76.29.7, cổng 2500) sẽ luôn được chuyển tiếp tới (10.0.0.1, cổng 25000)

Vấn đề đi qua NAT

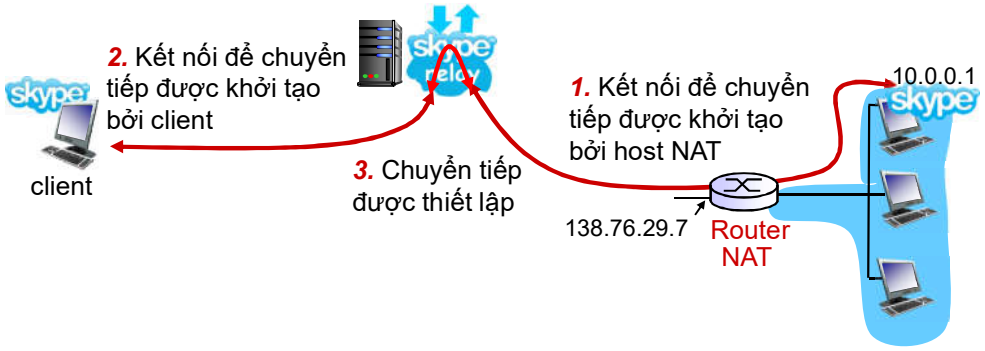
- *Giải pháp 2:* Dùng giao thức Universal Plug and Play (UPnP) Internet Gateway Device (IGD), cho phép chuyển đổi NAT:
  - Ghi nhớ địa chỉ IP công khai (138.76.29.7)
  - Thêm/xóa các ánh xạ cổng (trong khoảng thời gian cho phép)

Ví dụ: Cấu hình ánh xạ cổng NAT tĩnh tự động



Vấn đề đi qua NAT

- *Giải pháp 3:* chuyển tiếp (được dùng trong Skype)
  - Client NAT thiết lập kết nối để chuyển tiếp
  - Client bên ngoài kết nối để chuyển tiếp
  - Chuyển tiếp giữa các gói tin của các cầu để kết nối



Chương 4: Nội dung

ICMP: internet control message protocol

- Được sử dụng bởi các host & các router để truyền thông tin tầng mạng
  - Báo cáo lỗi: không tìm được host, mạng, cổng, giao thức
  - Phản hồi yêu cầu/đáp ứng (được dùng bởi ping)
- "Ở phía trên" trong tầng mạng:
  - Các thông điệp ICMP được mang trong các IP datagram
- Thông điệp ICMP: type, code và 8 byte đầu tiên của IP datagram mô tả nguyên nhân lỗi

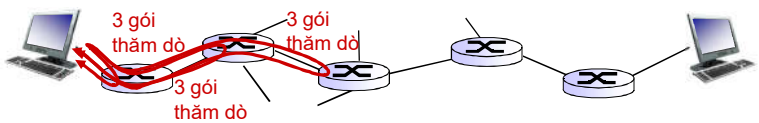
Type	Code	description (mô tả)
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Traceroute và ICMP

- Nguồn gửi chuỗi UDP segments tới đích
  - Segment đầu tiên được thiết lập TTL=1
  - Segment thứ hai TTL=2, ...
  - Không giống với số hiệu cổng
- Khi datagram thứ *n* tới router *n*:
  - Router bỏ qua các datagram
  - Và gửi đến nguồn thông điệp ICMP (type 11, code 0)
  - Thông điệp ICMP có chứa tên của router & địa chỉ IP
- Khi thông điệp ICMP đến, nguồn tính toán các RTT

Điều kiện dừng:

- UDP segment cuối cùng đến được host đích.
- Đích trả lại thông điệp ICMP "port unreachable" (type 3, code 3) → cổng không có
- Nguồn dừng lại



IPv6: Lý do

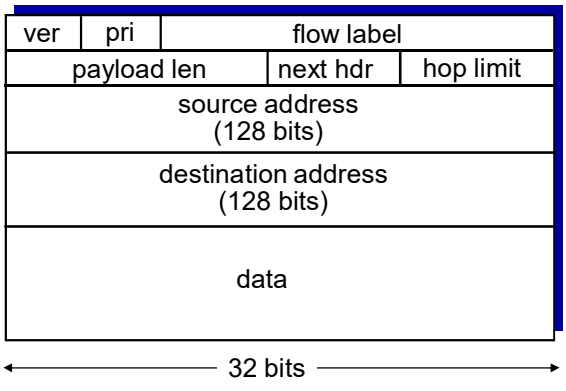
- *Động lực thúc đẩy ban đầu:* không gian địa chỉ 32-bit sắp được cấp phát hết.
- Động lực bổ sung:
  - Định dạng tiêu đề (header) giúp tăng tốc độ xử lý/chuyển tiếp
  - Tiêu đề thay đổi giúp tạo điều kiện cho QoS

Định dạng IPv6 datagram:

- Phần tiêu đề có chiều dài cố định 40 byte
- Không cho phép phân mảnh gói tin

Định dạng IPv6 datagram

- *Priority (ưu tiên):* xác định ưu tiên giữa các datagram trong luồng
- *Flow Label (nhãn luồng):* xác định các datagram trong cùng một "luồng".
- *Next header:* xác định giao thức tầng cao hơn cho dữ liệu

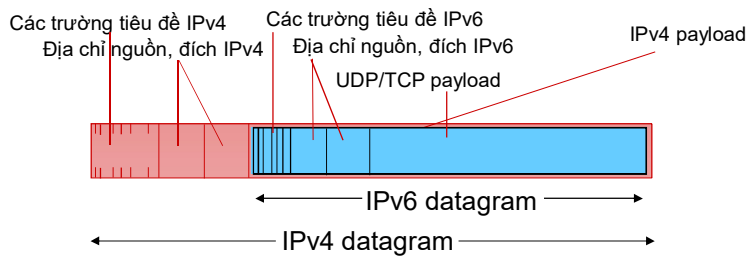


Những thay đổi của IPv6 so với IPv4

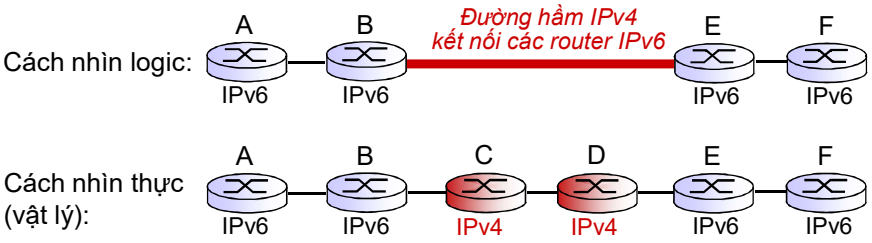
- *Checksum*: bỏ hoàn toàn, nhằm giảm thời gian xử lý tại mỗi hop
- *Options:* được phép, nhưng nằm ngoài phần tiêu đề, được xác định trong trường "Next Header"
- *ICMPv6:* phiên bản mới của ICMP
  - Các loại thông điệp bổ sung, ví dụ: "Packet Too Big"
  - Các chức năng quản lý nhóm multicast

Chuyển đổi từ IPv4 sang IPv6

- Không phải tất cả các router đều có thể được nâng cấp đồng thời
  - Không có ngày dành riêng cho việc chuyển đổi (flag days)
  - Mạng sẽ hoạt động như thế nào với việc sử dụng đồng thời các router IPv4 và IPv6?
- *Tunneling (đường hầm): Payload* của IPv6 datagram được mang trong IPv4 datagram giữa các router IPv4



Tunneling



Tunneling