Bài tập

Lấy 4 số cuối của mã sinh viên S1 = ABCD

→ Chuyển theo nguyên tắc

S1’=(9-A)(9-B)(9-C)(9-D)

→ Chuyển sang nhị phân

→ Tính mã Parity (9-D) chẵn/lẻ → mã chẵn/lẻ

→ Chuyển sang nhị phân số S2 = 7982

→ Tìm mã checksum của S1’, S2

→ Cho M(x) = 10011000, tìm R(x) khi kiểm tra lỗi dùng mã CRC biết G(x)=110101

Bài tập

Lấy 4 số ngày sinh + tháng sinh: S1 = ABCD

→ Chuyển theo nguyên tắc

S1’ = DCBA

→ Chuyển sang nhị phân

→ Tính mã Parity nếu C chẵn/lẻ → mã chẵn/lẻ

→ Chuyển sang nhị phân số S2 = 7982

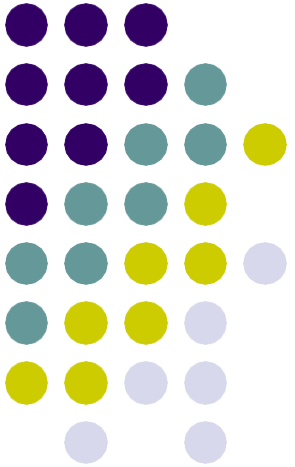
→ Tìm mã checksum của S1’, S2

→ Cho M(x) = 10011000, tìm R(x) khi kiểm tra lỗi dùng mã CRC biết G(x)=110101

Chương 5:
Tầng mạng – Network Layer

Giảng viên: Nguyễn Đức Toàn

Bộ môn Truyền thông và Mạng máy tính
Viện CNTT&TT - ĐHBK Hà Nội



Tổng quan

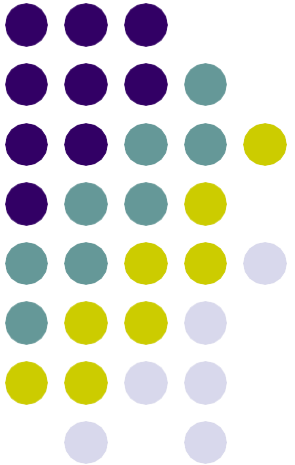
- Tuần trước…
  - Các chức năng tầng Liên kết dữ liệu
  - Các phương pháp kiểm soát lỗi
  - Các phương pháp đa truy nhập
- Tuần này
  - Giới thiệu về tầng mạng
  - Giao thức tầng mạng – Internet Protocol
  - Địa chỉ IP và khuôn dạng gói tin IP

Giới thiệu về tầng mạng

Khái niệm cơ bản

Nguyên lý lưu-và-chuyển tiếp

Giao thức Internet Protocol - IP

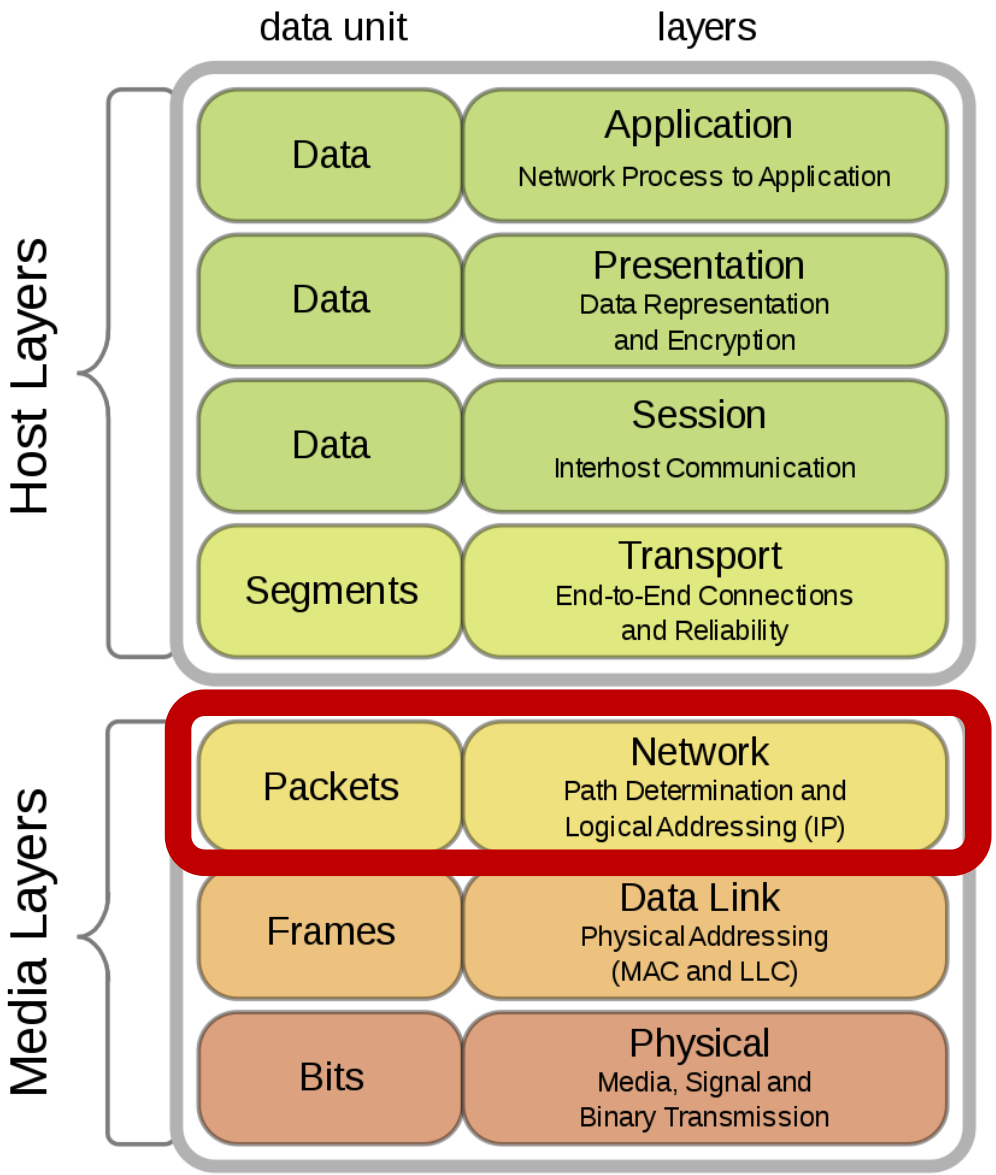


Giới thiệu về Tầng mạng

- Nhận protocol data unit (PDU) từ tầng Transport
- Gán địa chỉ IP
- Encapsulation/Decapsulation (thêm/bớt IP header)

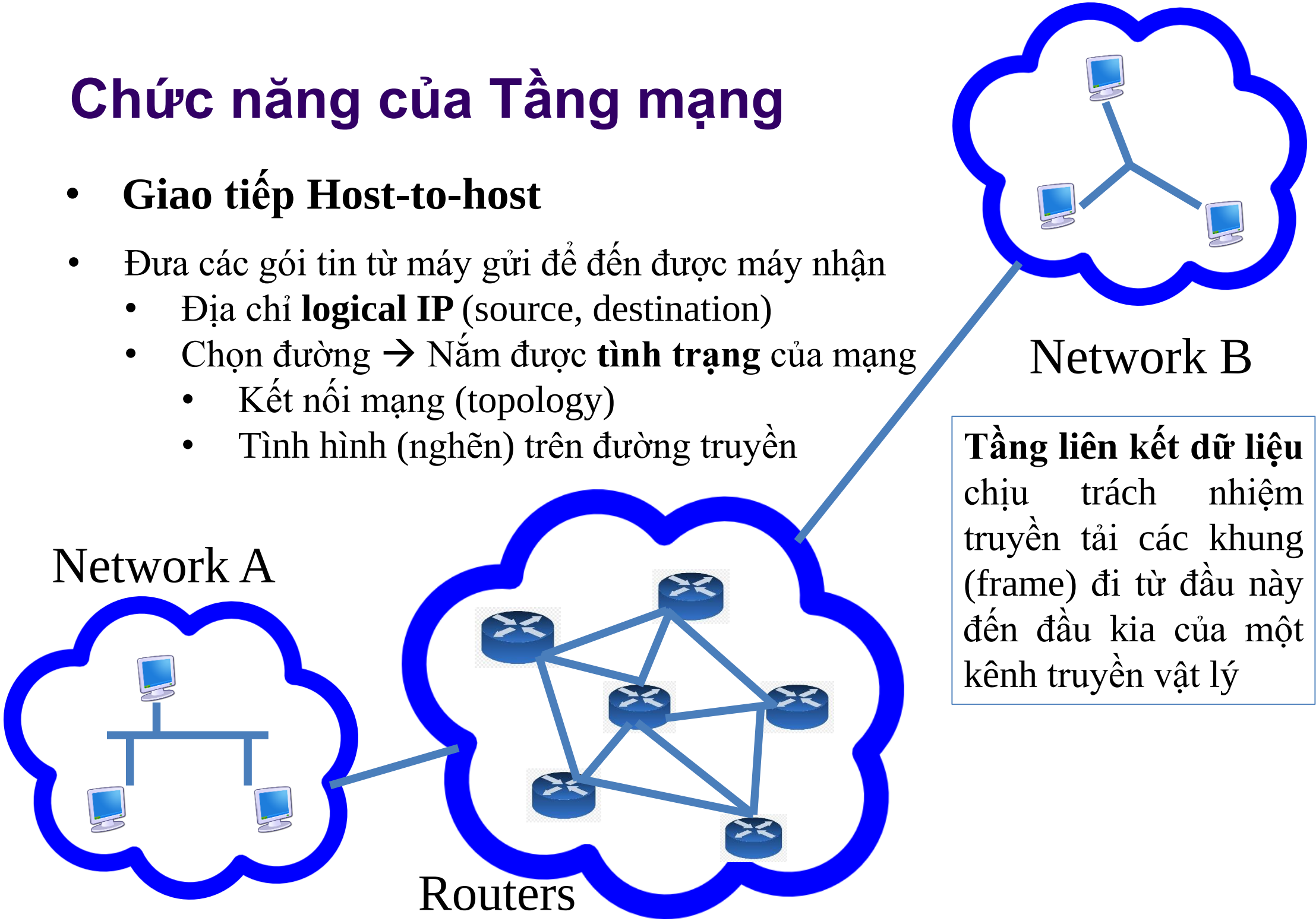
→ IP packets

- Định tuyến



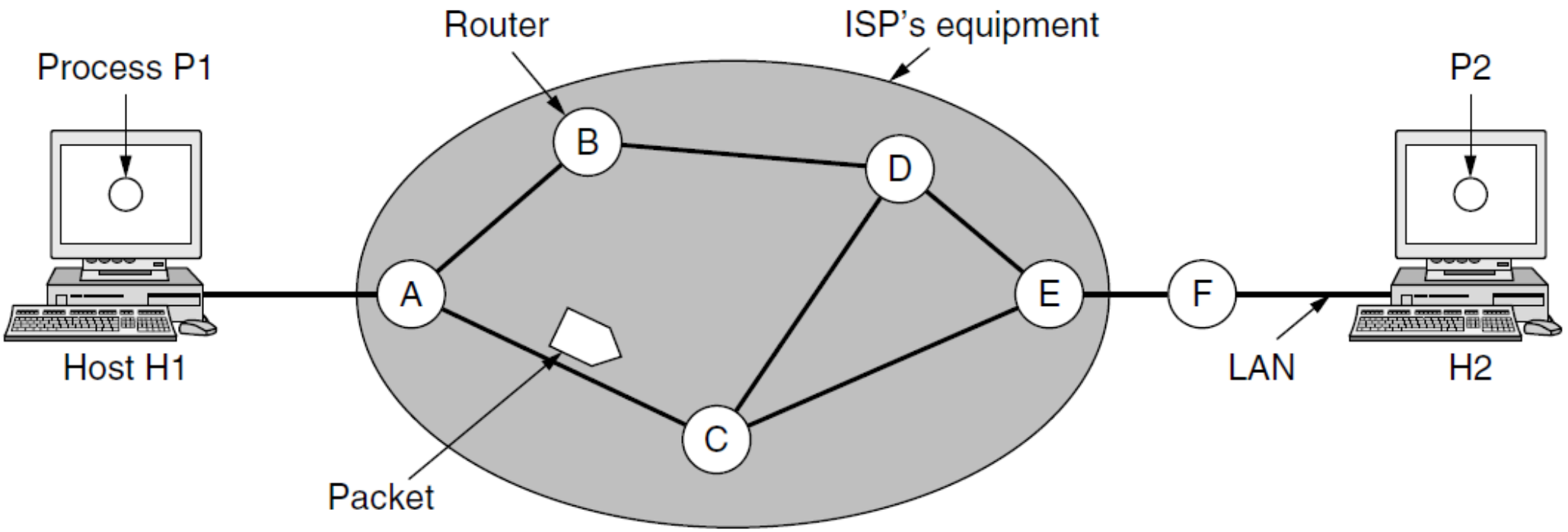
Chức năng của Tầng mạng

- **Giao tiếp Host-to-host**
- Đưa các gói tin từ máy gửi để đến được máy nhận
  - Địa chỉ **logical IP** (source, destination)
  - Chọn đường → Nắm được **tình trạng** của mạng
    - Kết nối mạng (topology)
    - Tình hình (nghẽn) trên đường truyền



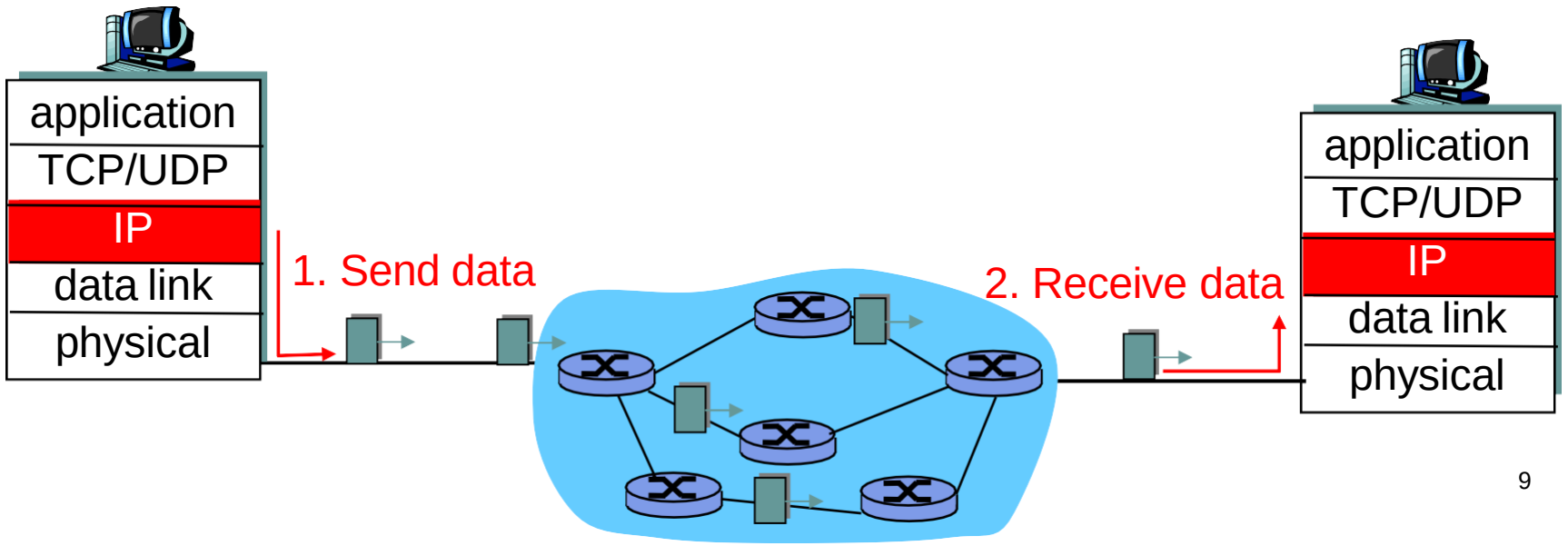
Tầng liên kết dữ liệu chịu trách nhiệm truyền tải các khung (frame) đi từ đầu này đến đầu kia của một kênh truyền vật lý

Nguyên lý lưu-và-chuyển tiếp

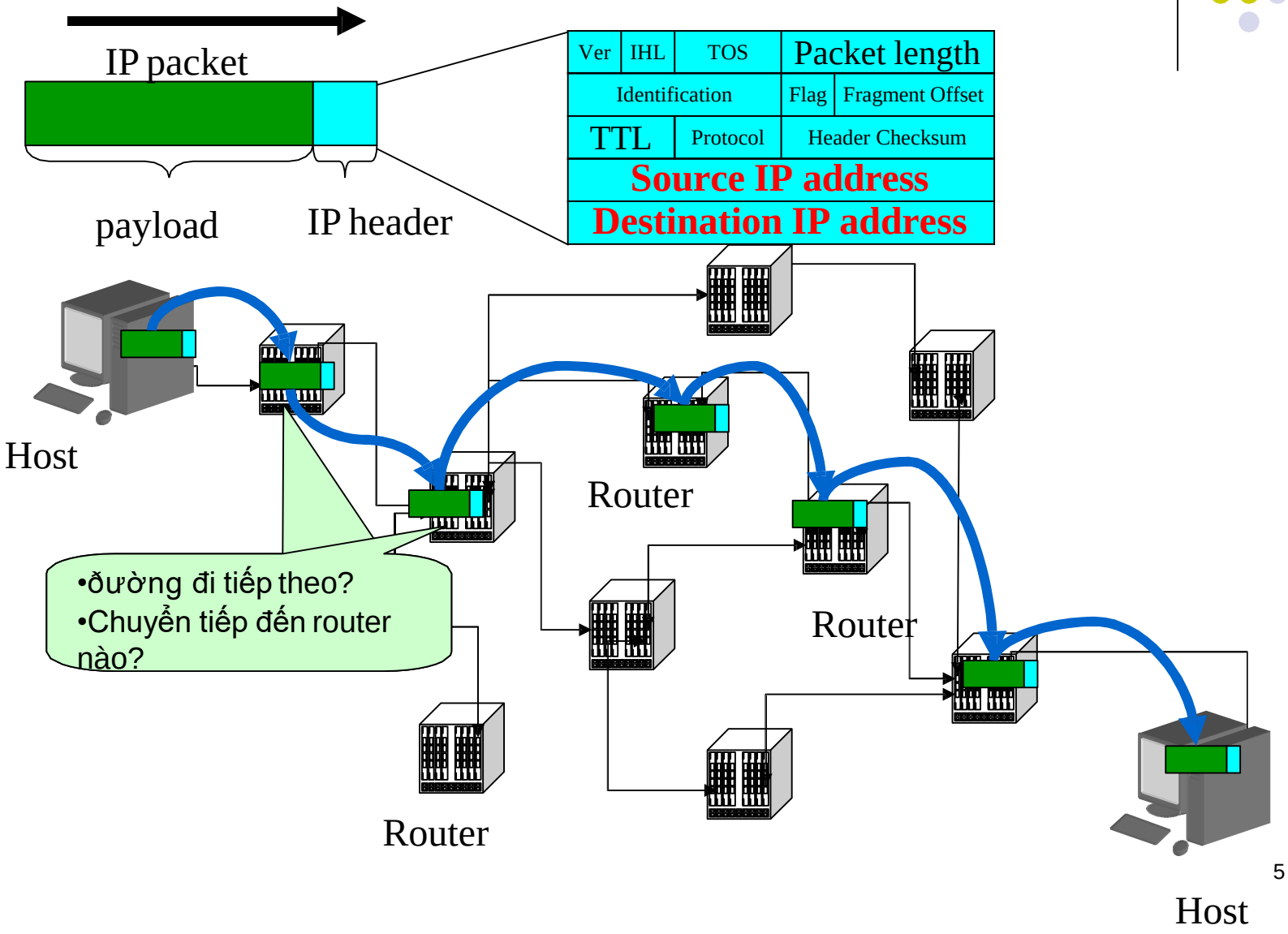


Internet Protocol

- Là một giao thức ở tầng mạng
- Hai chức năng cơ bản
  - Chọn đường (*Routing*): Xác định đường đi của gói tin từ nguồn đến đích
  - Chuyển tiếp (*Forwarding)*: Chuyển dữ liệu từ đầu vào tới đầu ra của bộ định tuyến (router)
  - VD



Chọn đường và chuyển tiếp gói tin



Nhắc lại: Network layer vs. Transport layer

- Network: Tìm **đường đi** cho gói tin giữa các máy trạm thông qua các bộ định tuyến
  - Nhanh tới đích
- Transport: Giữa các tiến trình trên máy trạm
  - Thứ tự gói tin..

Đặc điểm của giao thức IP

- Không tin cậy / nhanh
  - Truyền dữ liệu theo phương thức "*best effort*"
  - IP không có cơ chế phục hồi lỗi
  - Khi cần, sẽ sử dụng dịch vụ tầng trên để đảm bảo độ tin cậy (TCP)
- Giao thức không liên kết
  - Các gói tin được xử lý độc lập

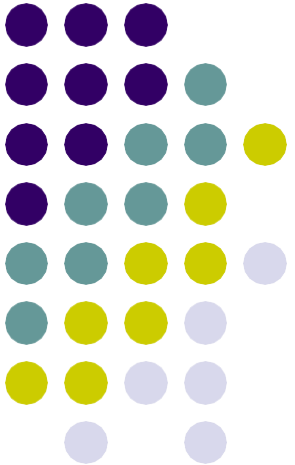
Địa chỉ IPv4

Phân lớp địa chỉ IP

CIDR – địa chỉ IP không phân lớp

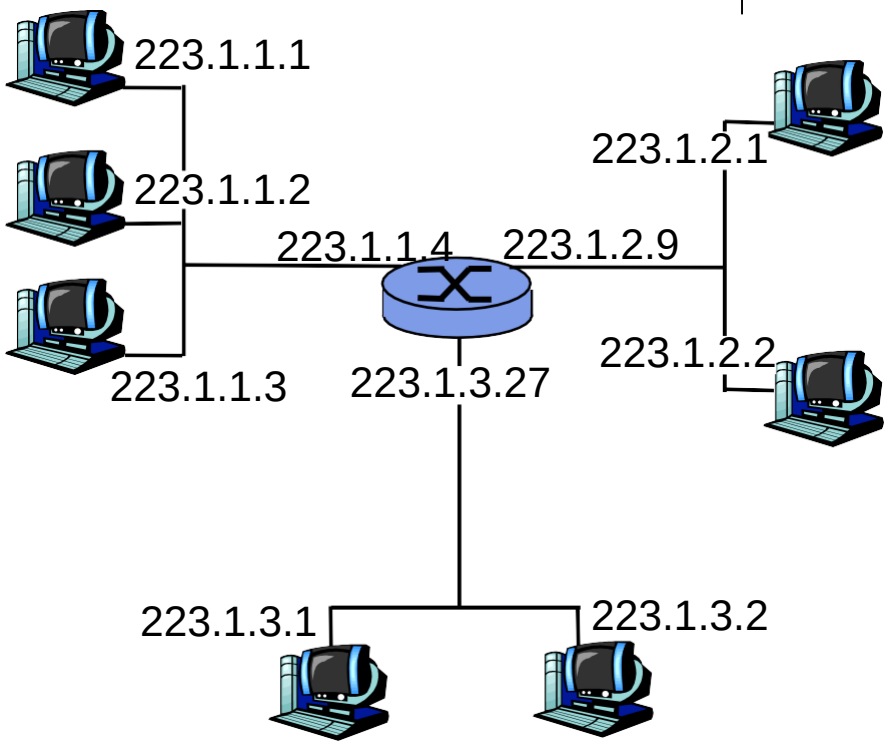
Mạng con và mặt nạ mạng

Các địa chỉ IP đặc biệt



Địa chỉ IP (IPv4)

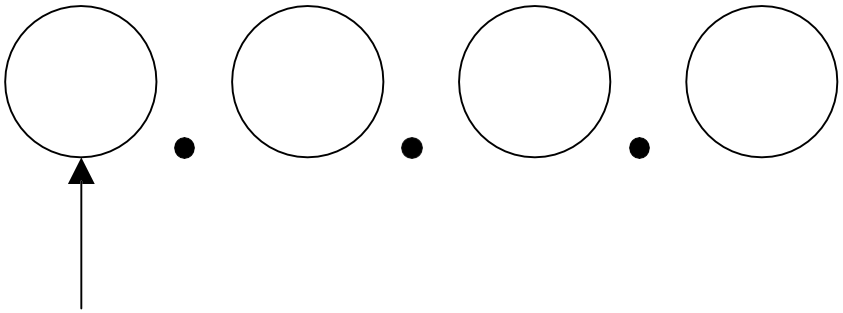
- Địa chỉ IPv4 : Một số 32-bit để định danh giao diện máy trạm, bộ định tuyến
- Mỗi địa chỉ IP được gán cho một giao diện
- Địa chỉ IP có tính duy nhất



223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Ký hiệu thập phân có chấm

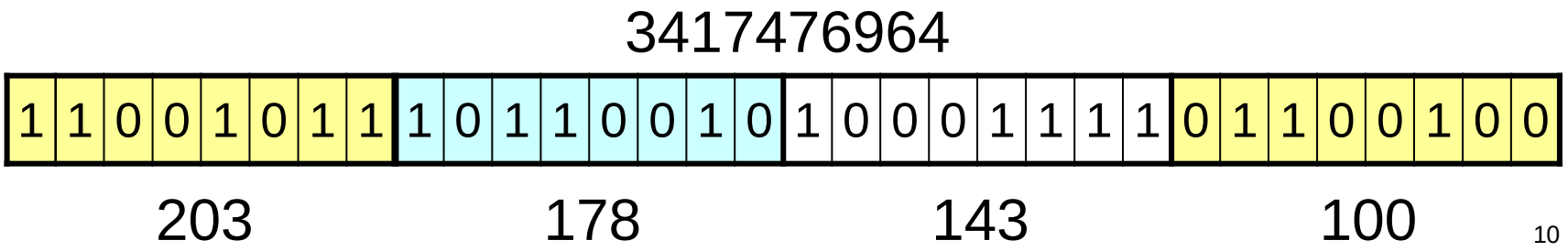


8 bits
0 – 255 integer

Ví dụ:

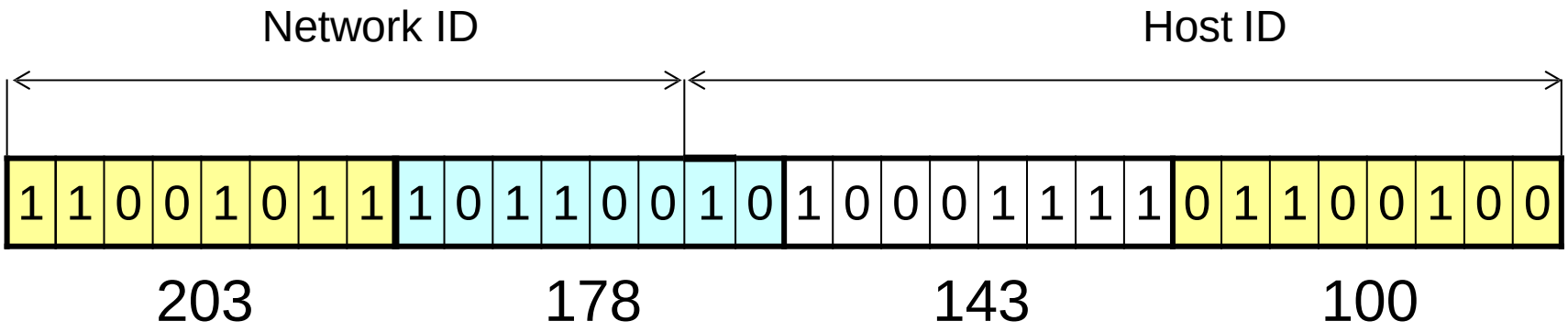
203.178.136.63	o
259.12.49.192	x
133.27.4.27	o

Sử dụng 4 phần 8 bits để miêu tả một địa chỉ 32 bits



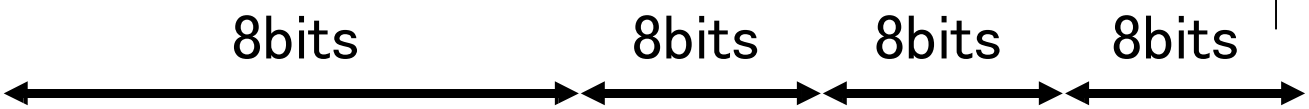
Địa chỉ máy trạm, địa chỉ mạng

- Địa chỉ IP có hai phần
  - Host ID – địa chỉ máy trạm
  - Network ID – địa chỉ mạng



- Làm thế nào biết được phần nào là cho máy trạm, phần nào cho mạng?
  - Phân lớp địa chỉ
  - Không phân lớp – CIDR

Phân lớp địa chỉ IP



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

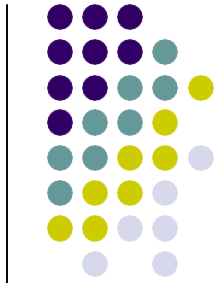
Hạn chế của việc phân lớp địa chỉ

- 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

Cách giải quyết …

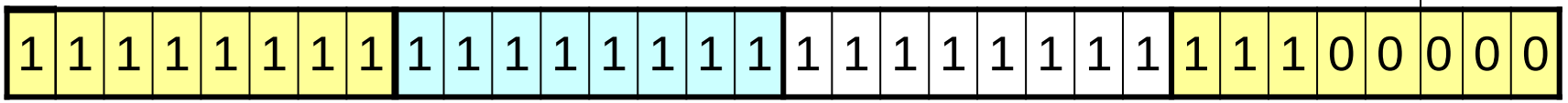
- CIDR: Classless Inter Domain Routing
  - Phần địa chỉ mạng sẽ có độ dài bất kỳ
  - Dạng địa chỉ: a.b.c.d/x, trong đó x (mặt nạ mạng) là số bit trong phần ứng với địa chỉ mạng

Mặt nạ mạng



- Mặt nạ mạng chia một địa chỉ IP làm 2 phần
  - Phần ứng với máy trạm
  - Phần ứng với mạng
- Dùng toán tử AND
  - Tính địa chỉ mạng
  - Tính khoảng địa chỉ IP

Mô tả mặt nạ mạng



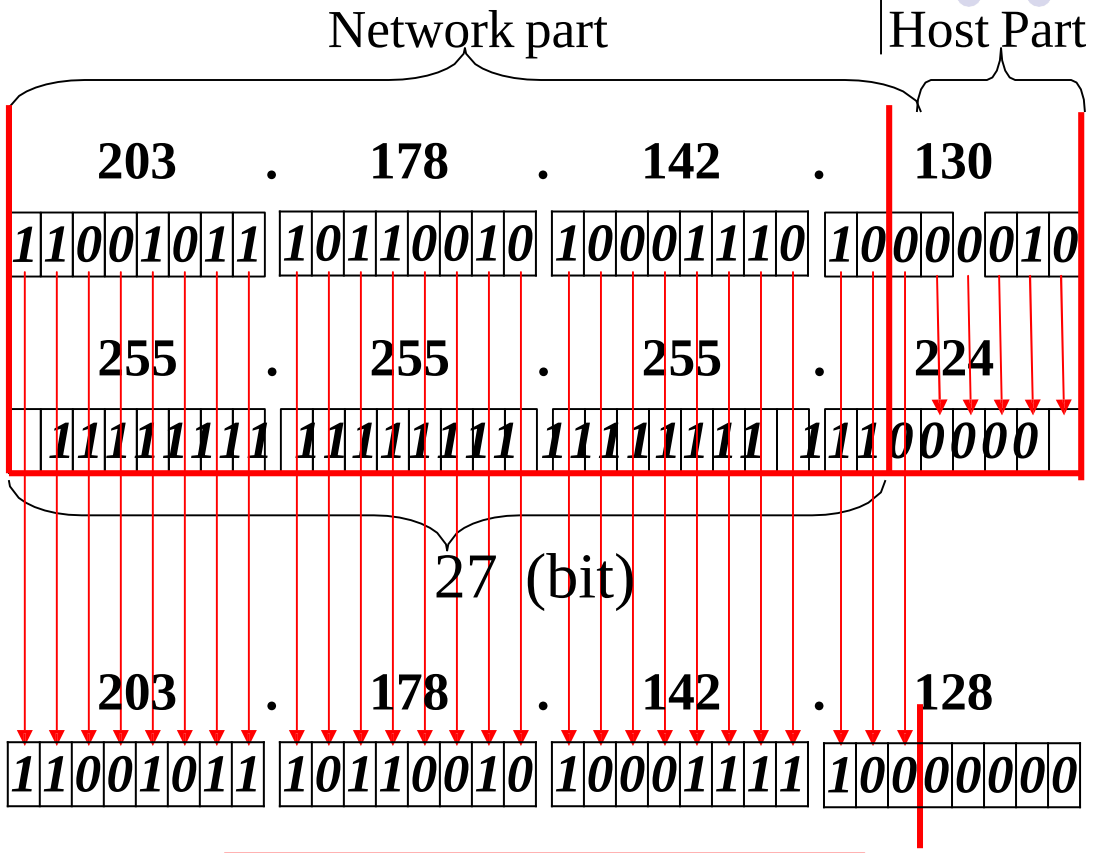
- 255.255.255.224
- /27
- 0xFFFFFFE0

- Sẽ là một trong các số:

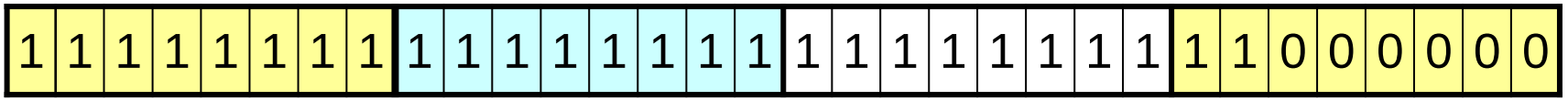
0 248 128 252 192 254

224 255 240

Cách tính địa chỉ mạng



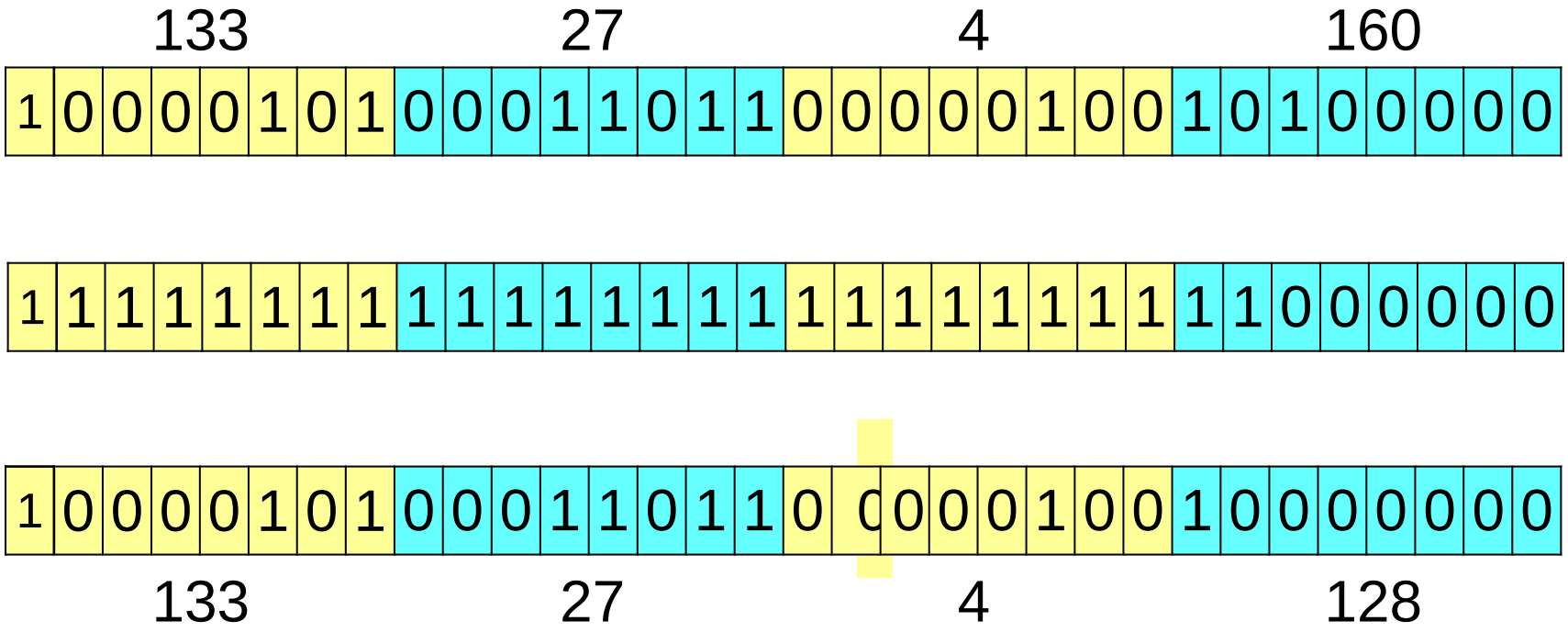
Mặt nạ mạng và kích thước mạng



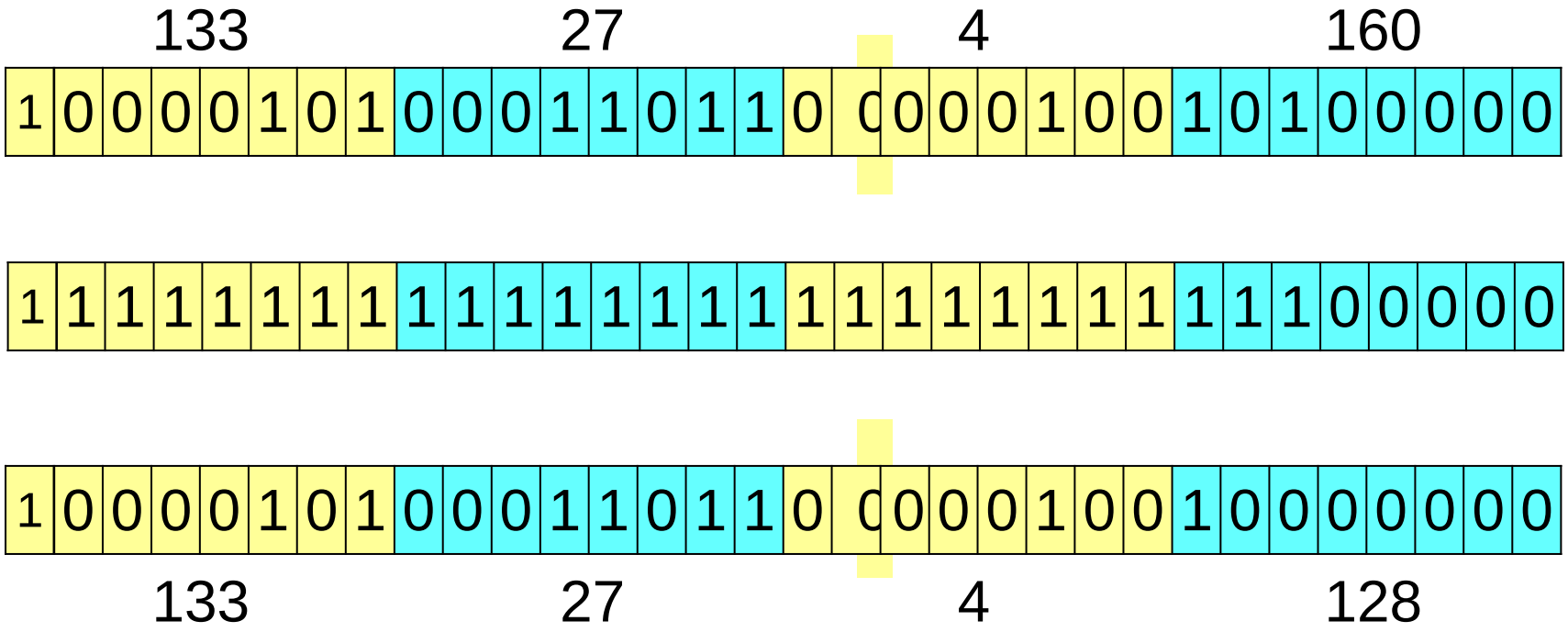
- Kích thước
  - Theo lũy thừa 2
- RFC1878

- Trong trường hợp /26
  - Phần máy trạm = 6 bits
  - 2^6=64
  - Dải địa chỉ có thể gán:
    - 0 - 63
    - 64 - 127
    - 128 - 191
    - 192 - 255

Địa chỉ mạng hay máy trạm (1)



Địa chỉ mạng hay máy trạm (2)



Các dạng địa chỉ

- Địa chỉ mạng
  - Địa chỉ IP gán cho một mạng
- Địa chỉ máy trạm
  - Địa chỉ IP gán cho một card mạng
- Địa chỉ quảng bá
  - Địa chỉ dùng để gửi cho tất cả các máy trạm trong mạng
  - Toàn bit 1 phần ứng với địa chỉ máy trạm

Địa chỉ IP và mặt nạ mạng

- Địa chỉ nào là địa chỉ máy trạm, địa chỉ mạng, địa chỉ quảng bá?

(1) 203.178.142.128 /25

(2) 203.178.142.128 /24

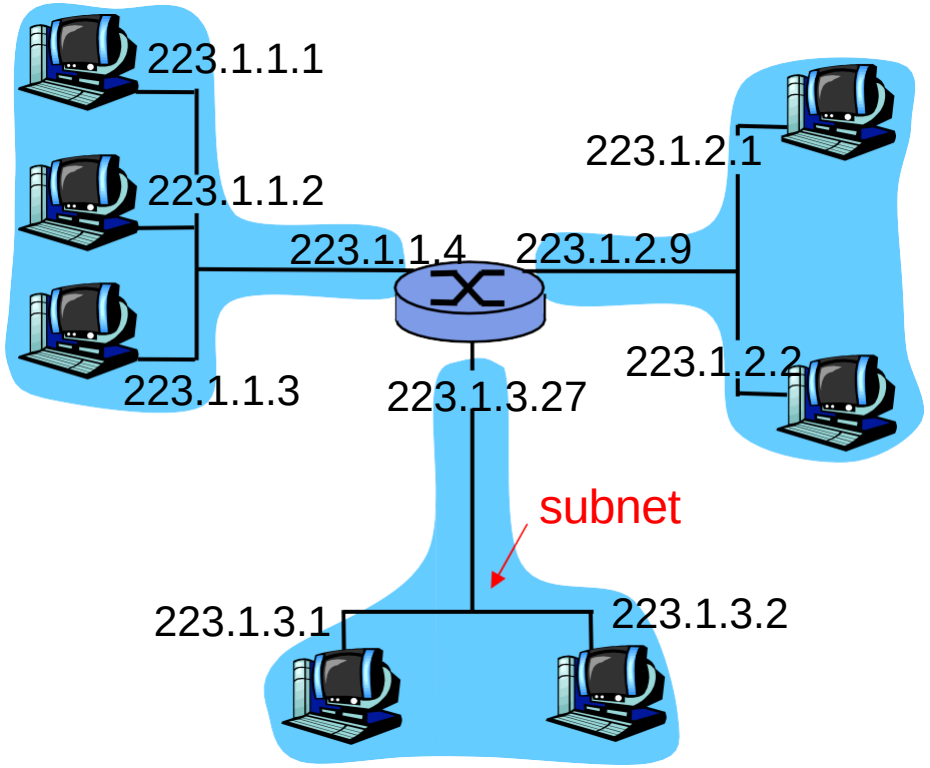
(3) 203.178.142.127 /25

(4) 203.178.142.127 /24

- Lưu ý: Với cách địa chỉ hóa theo CIDR, địa chỉ IP và mặt nạ mạng luôn phải đi cùng nhau

Mạng con - subnet

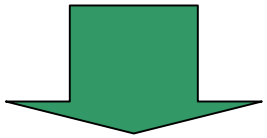
- Là một phần của một mạng nào đó
  - ISP thường được gán một khối địa chỉ IP
  - Một vài mạng con sẽ được tạo ra
- Tạo subnet như thế nào
  - Sử dụng một mặt nạ mạng dài hơn



Mạng với 3 mạng con

Ví dụ: Chia làm 2 subnets

11001000 00010111 00010000 00000000
200. 23. 16. 0 /24

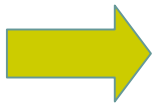


11001000 00010111 00010000 00000000
200. 23. 16. 0 /25

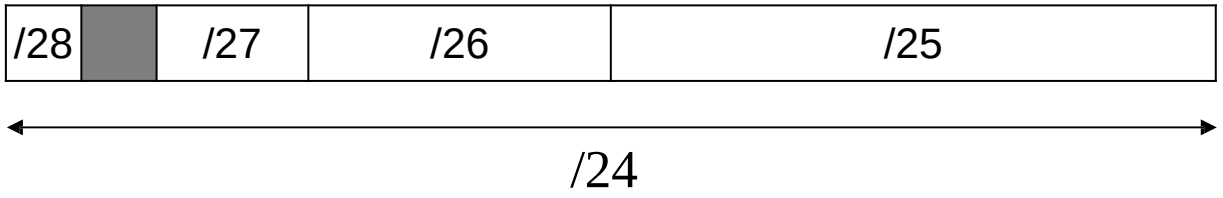
11001000 00010111 00010000 10000000
200. 23. 16. 128 /25

Ví dụ: Chia làm 4 subnets

- Mạng với mặt nạ /24
- Cần tạo 4 mạng con
  - Mạng với 14 máy tính
  - Mạng với 30 máy tính
  - Mạng với 31 máy tính
  - Mạng với 70 máy tính



/28
/27
/26
/25



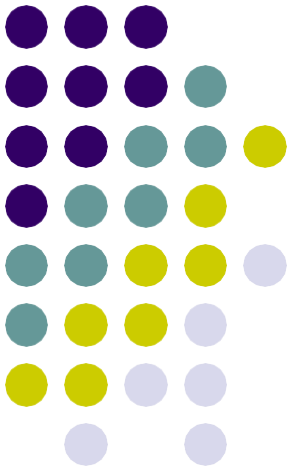
Không gian địa chỉ IPv4

- Theo lý thuyết
  - Có thể là 0.0.0.0 ～ 255.255.255.255
  - Một số địa chỉ đặc biệt
- Địa chỉ IP đặc biệt (RFC1918)

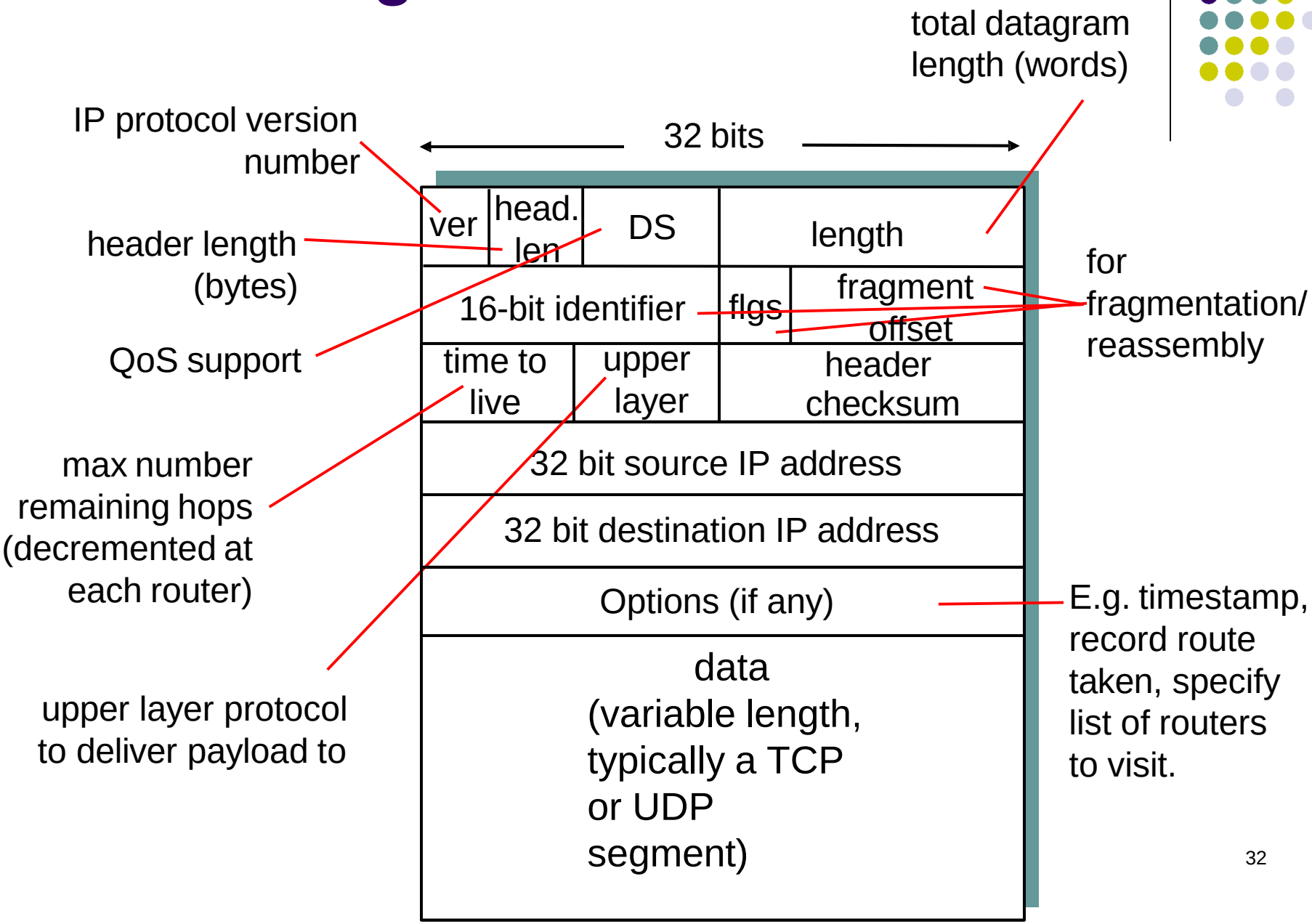
Private address	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
Loopback address	127.0.0.0
Multicast address	224.0.0.0 ～239.255.255.255

- Địa chỉ liên kết nội bộ: 169.254.0.0/16

Khuôn dạng gói tin IP



Phần đầu gói tin IP



IP header (1)

- Phiên bản giao thức (4 bits)
  - IPv4
  - IPv6
- Độ dài phần đầu: 4bits
  - Tính theo từ (4 bytes)
  - Min: 5
  - Max: 60

IP header (2)

- DS (Differentiated Service : 8bits)
  - Tên cũ: Type of Service
  - Hiện tại được sử dụng trong quản lý QoS
  - Diffserv

IP header (3)

- Độ dài toàn bộ, tính cả phần đầu (16 bits)
  - Theo bytes
  - Max: 65536
- ID – Số hiệu gói tin
  - Dùng để xác định một chuỗi các gói tin của một gói tin bị phân mảnh
- Flag – Cờ
- Fragmentation offset – Vị trí gói tin phân mảnh trong gói tin ban đầu

IP header (4)

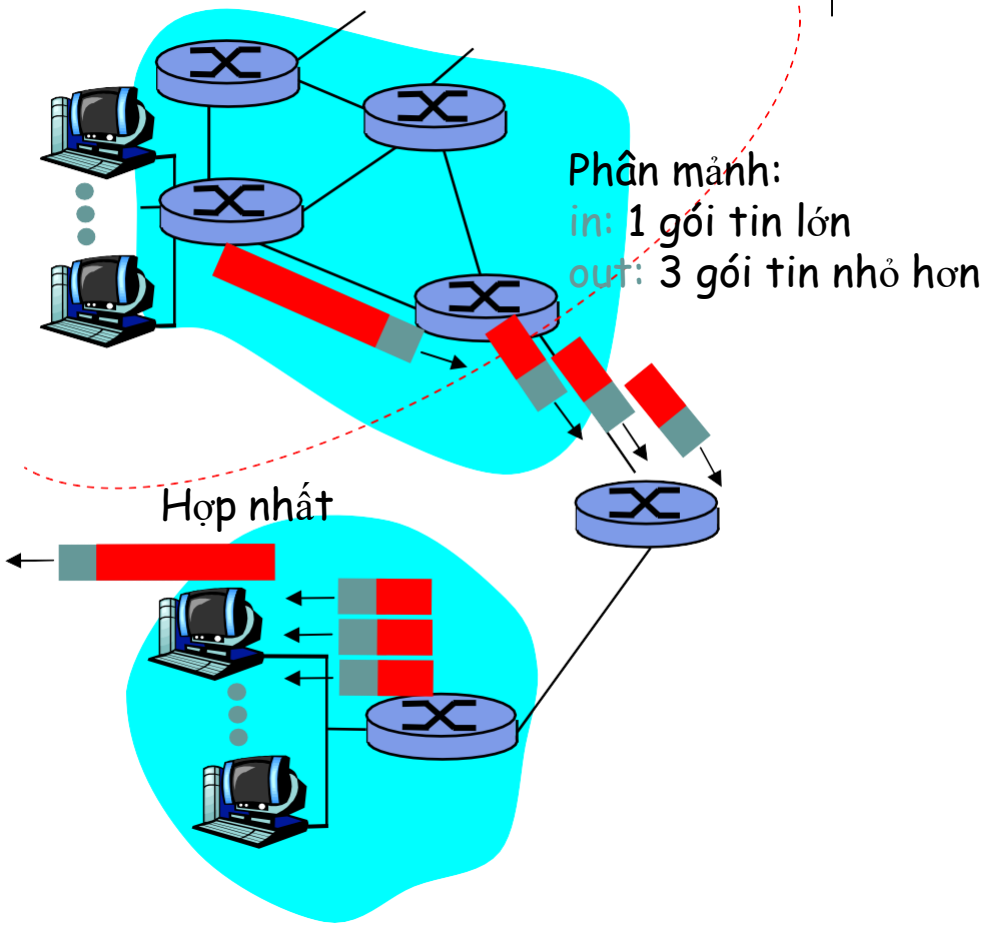
- TTL, 8 bits – Thời gian sống
  - Độ dài đường đi gói tin có thể đi qua
  - Max: 255
  - Router giảm TTL đi 1 đơn vị khi xử lý
  - Gói tin bị hủy nếu TTL bằng 0
- Protocol – giao thức tầng trên
  - Giao thức giao vận phía trên (TCP, UDP,…)
  - Các giao thức tầng mạng khác (ICMP, IGMP, OSPF) cũng có trường này

IP header (4)

- Checksum – Mã kiểm soát lỗi
- Địa chỉ IP nguồn
  - 32 bit, địa chỉ của trạm gửi
- Địa chỉ IP đích
  - 32 bit, địa chỉ của trạm đích

Phân mảnh gói tin (1)

- Đường truyền có một giá trị MTU (Kích thước đơn vị dữ liệu tối đa)
- Các đường truyền khác nhau có MTU khác nhau
- Một gói tin IP lớn quá MTU sẽ bị
  - Chia làm nhiều gói tin nhỏ hơn
  - Được tập hợp lại tại trạm đích

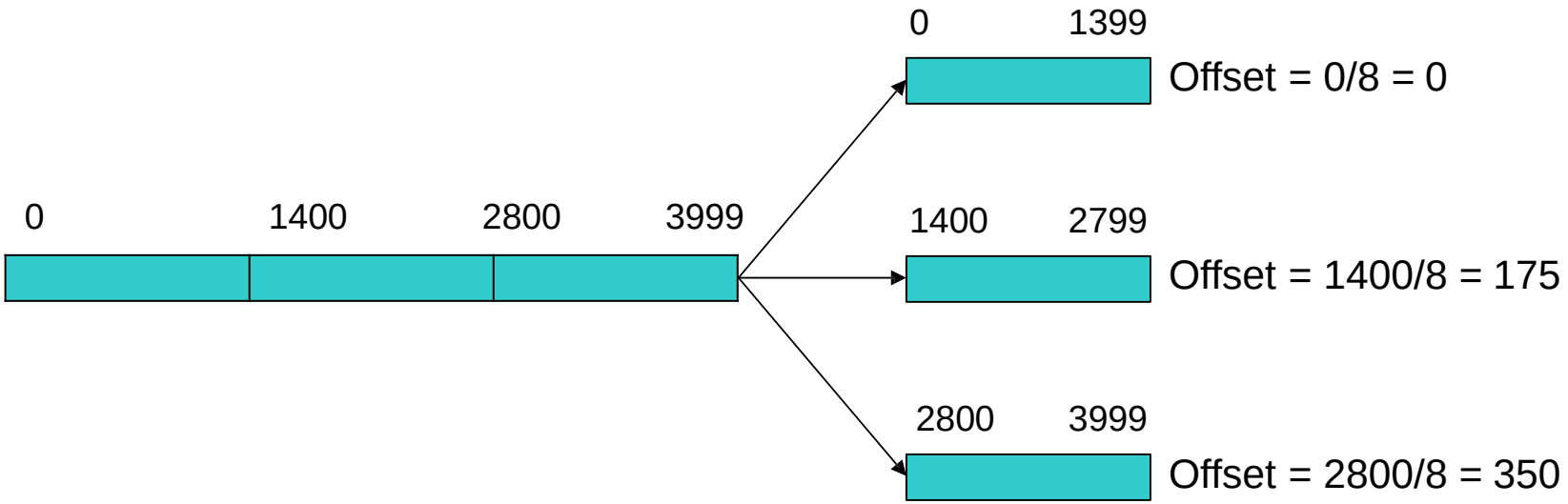


Phân mảnh (2)

- Trường Identification
  - ID được sử dụng để tìm các phần của gói tin
- Flags – cờ (3 bits)
  - Dự phòng
  - Không được phép phân mảnh
  - Còn phân mảnh
    - Dùng để tập hợp gói tin

Phân mảnh (3)

- Độ lệch - Offset
  - Vị trí của gói tin phân mảnh trong gói tin ban đầu
  - Theo đơn vị 8 bytes

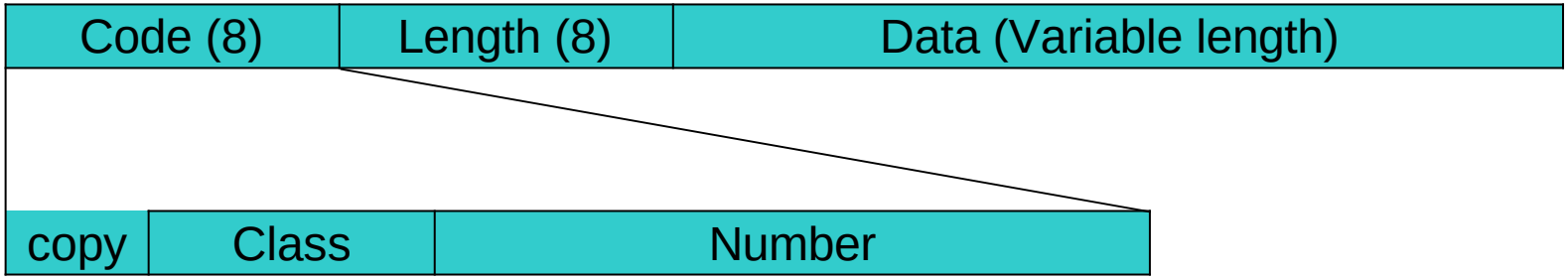


Checksum

- Mã kiểm soát lỗi cho phần đầu
- Tại bên gửi
  - Đặt checksum = 0
  - Tổng theo các số 16 bits
  - Đảo bit tất cả
- Tại bên nhận
  - Tổng tất cả theo các số 16 bit
  - Phải thu được toàn các bit 1
  - Nếu không, gói tin bị lỗi

Tùy chọn

- Dùng để thêm vào các chức năng mới
  - Có thể tới 40 bytes



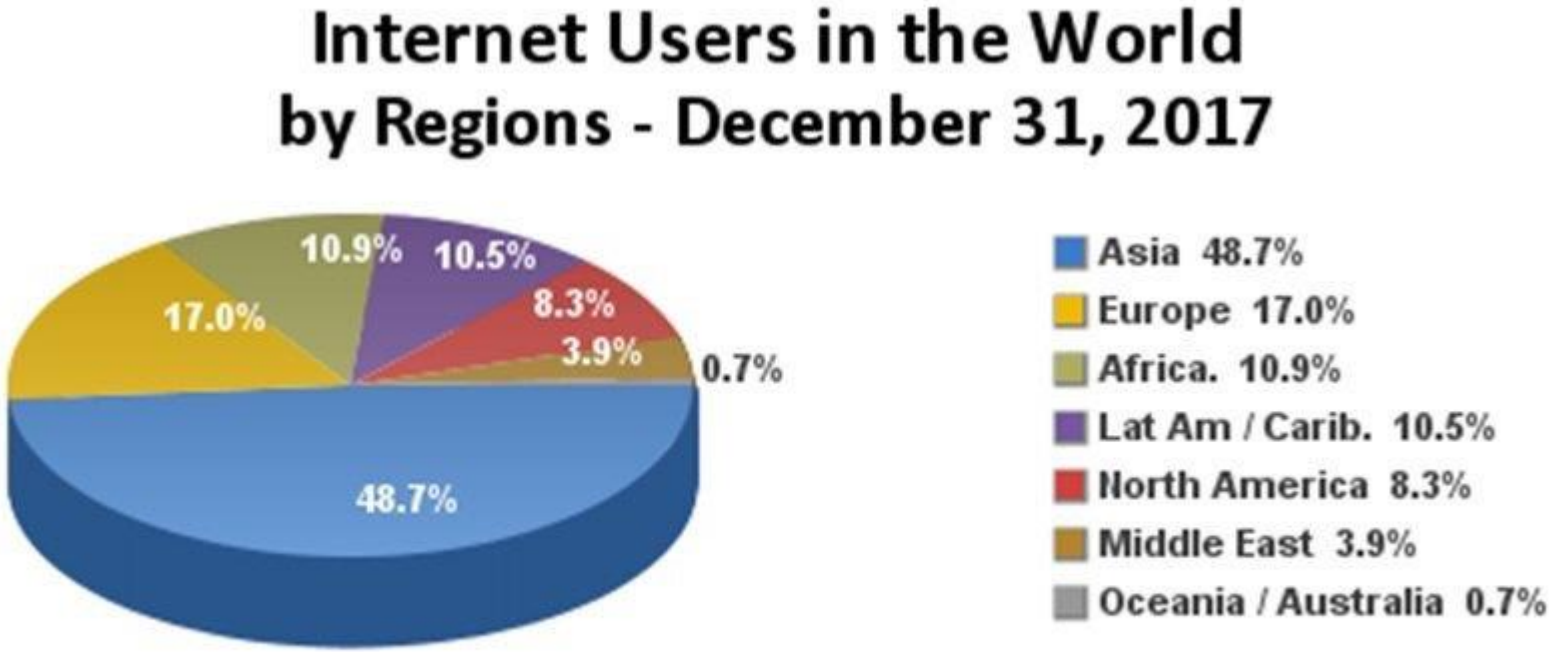
Copy:
0: copy only in first fragment
1: copy into all fragment

Class:
00: Datagram control
01: Reserved
10: Debugging and measurement
11: Reserved

Number:
00000: End of option
00001: No operation
00011: Loose source route
00100: Timestamp
00111: Record route
01001: Strict source route

Hạn chế của IPv4

- Internet sử dụng IPv4: 32 bits
  - Số địa chỉ IPv4 = 2^{32} địa chỉ



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,156,932,140 Internet users in December 31, 2017

IP Version Numbers

Decimal	Keyword	Version	References
0	Reserved		
1 - 3	Unassigned		
4	**IP**	**Internet Protocol**	**RFC 791**
5	ST	ST Datagram Mode	RFC 1190, JWF
6	**IPv6**	**RFC 1883**	
7	TP/IX	TP/IX: The Next Internet	
8	PIP	The P Internet Protocol	
9	TUBA	TCP and UDP over Bigger Addresses	
10 - 14	Unassigned		
15	Reserved		

Sự ra đời của IPv6

- Địa chỉ IP 128 bits
- Cung cấp nhiều cấp độ cho các cấu trúc phân cấp và tổng hợp định tuyến
- Tự động cấu hình địa chỉ IP dễ dàng hơn
- Quản lý địa chỉ IP dễ dàng hơn
- Áp dụng IPsec trên kết nối end-to-end

Địa chỉ IPv6

- **Dài 128 bits (hay 16 bytes) :** gấp 4 lần IPv4.
- **Số địa chỉ IPv6 = 2^{128}** : 340 tỉ tỉ tỉ tỉ địa chỉ
- **Cách viết địa chỉ IPv6:**
  - Địa chỉ IPv6 được viết bằng số hệ hexadecimal.
  - Các số này được chia làm 8 nhóm, mỗi nhóm 4 số.
  - Các nhóm được phân cách bởi dấu ":"

2001:0718:1c01:0016:020d:56ff:fe77:52a3

Địa chỉ IPv6 tương thích với địa chỉ IPv4

IPv4-compatible IPv6 address

0:0:IPv4 address

IPv6 - Luật bỏ số 0

Khi địa chỉ IPv6 chứa nhiều khối là 0 liên tục, các khối này sẽ bị giảm lược

Ví dụ:

link-local address

FE80:0:0:0:2AA:FF:FE9A:4CA2 → FE80::2AA:FF:FE9A:4CA2.

multicast address

FF02:0:0:0:0:0:0:2 → FF02::2

loopback address

0:0:0:0:0:0:0:1 → ::1

IPv6 - Luật bỏ số 0 (2)

Trường hợp số 0 là một phần của khối → KHÔNG được giảm lược

Ví dụ,

SAI FF02:30:0:0:0:0:5 → FF02:3::5

Đúng FF02:30::5

Tuy vậy, các số 0 ở đầu mỗi khối được giảm lược

2001:718:1c01:16:20d:56ff:fe77:52a3

Cách đọc địa chỉ IPv6 có giảm lược

Để xác định số số 0 đã giảm lược trong "::"

1. Đếm số khối
2. (-) Lấy 8 trừ số tính được ở #1
3. (*) Nhân kết quả của #2 với 16

Ví dụ

1. FF02::2
2. Số khối = 2 - "FF02" và "2".
3. The number of bits expressed by the "::" is 96 (96 = (8 – 2)×16).

Mạng con trong IPv6

Subnet mask trong IPv4 không dùng cho IPv6

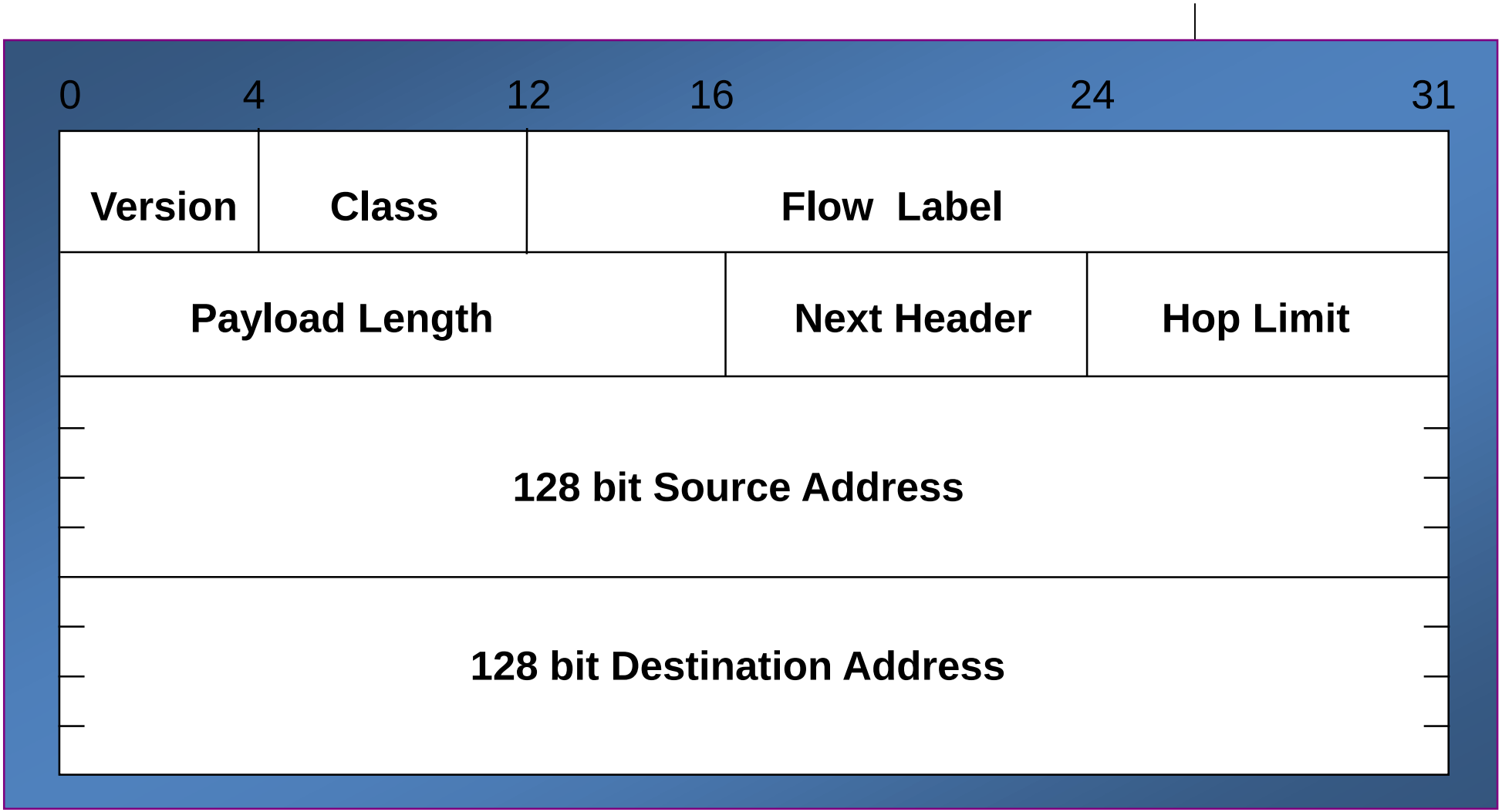
IPv6 sử dụng Classless Inter-Domain Routing (CIDR) tương tự như IPv4.

Ví dụ

21DA:D3::/48
21DA:D3:0:2F3B::/64

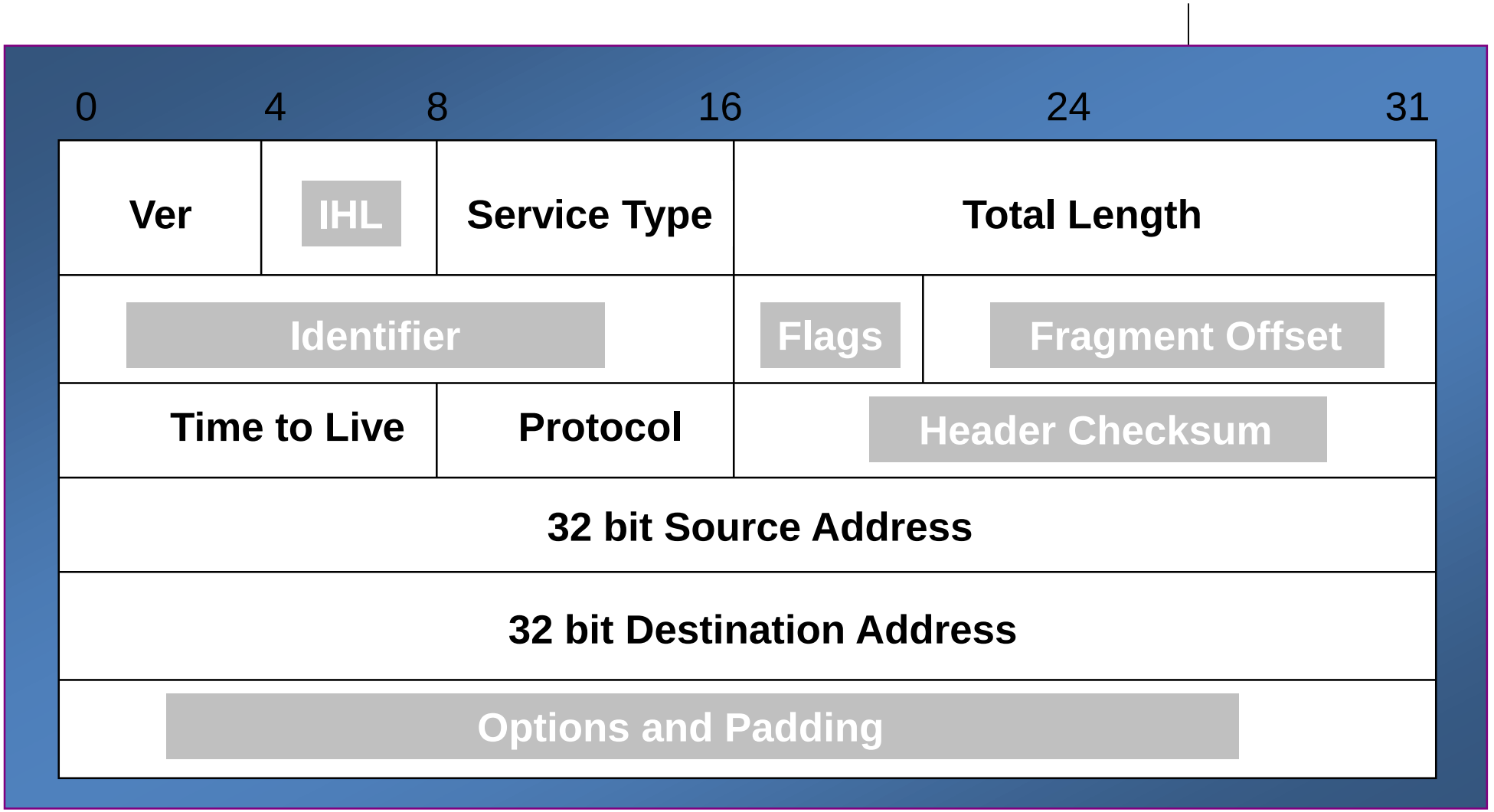
IPv6 Header

40 Octets, 8 fields



IPv4 Header

20 octets + options : 13 fields



Phần mờ là phần được lược bỏ so với IPv4

Thay đổi trong header IPv4 & IPv6

Sắp xếp lại

- Fragmentation fields moved out of base header
- IP options moved out of base header
- Header Checksum eliminated
- Header Length field eliminated
- Length field excludes IPv6 header
- Alignment changed from 32 to 64 bits

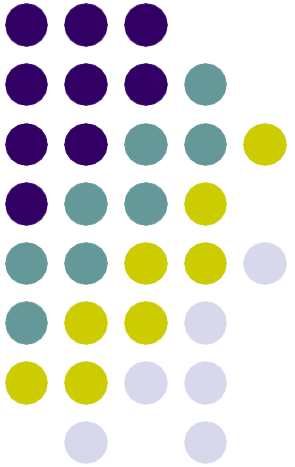
Chỉnh sửa

- Time to Live → Hop Limit
- Protocol → Next Header
- Precedence & TOS → Traffic Class
- Addresses increased 32 bits → 128 bits

Mở rộng

- Thêm Flow Label

Các thay đổi khác

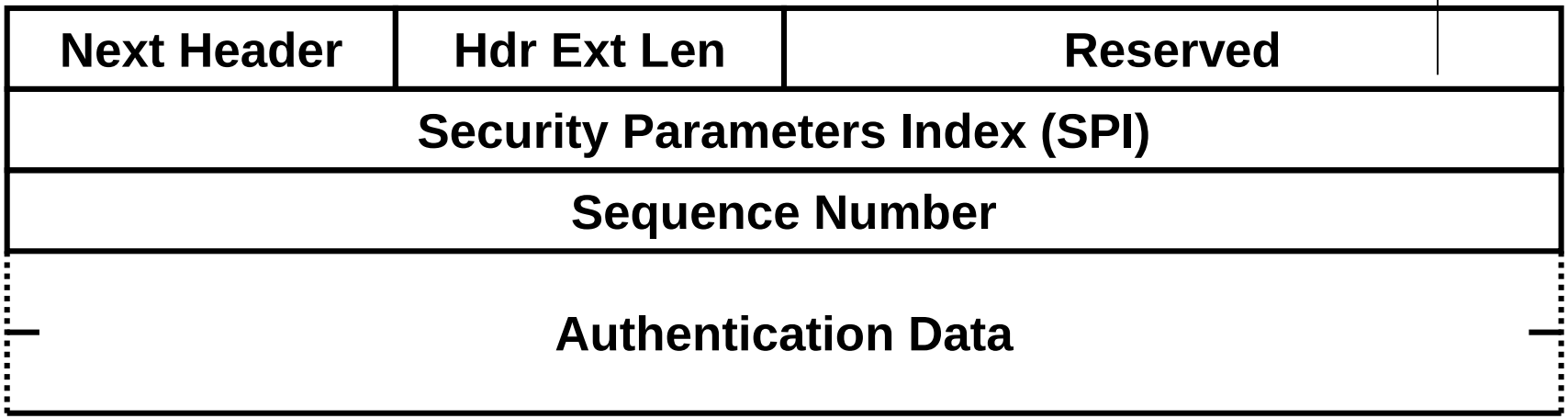


IPv6 Security

IPsec tropng IPv4 (tùy chọn)
→ IPsec tropng IPv6 (bắt buộc)
IPsec: authentication + encryption headers

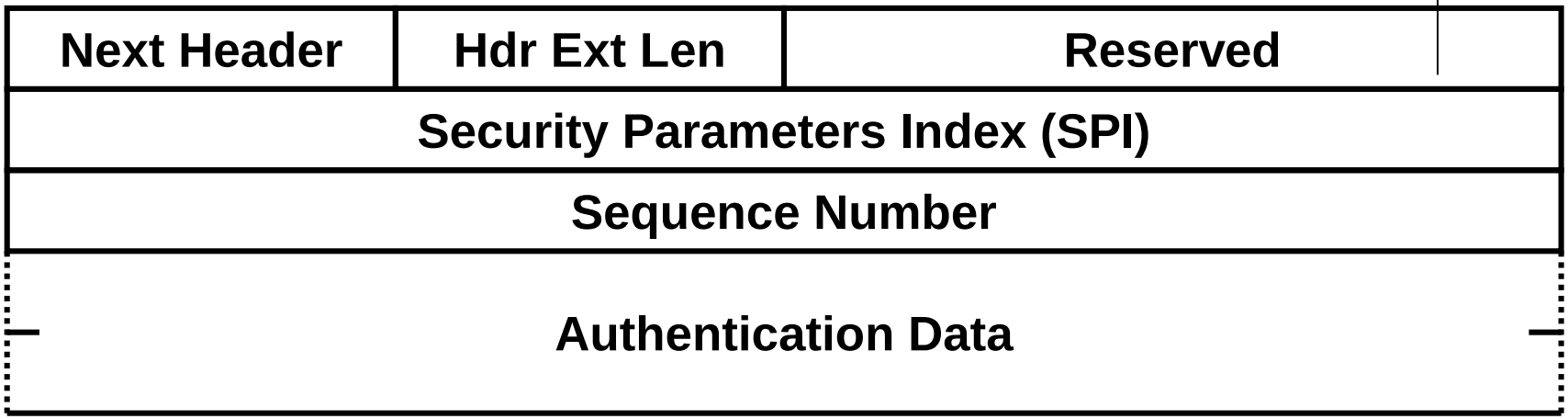
- **Các node IPv6 phải đáp ứng các đặc tả sau:**
  - **Security Architecture** for the Internet Protocol [RFC2401]
  - **IP Authentication Header** (AH) as defined in [RFC2402]
  - **IP Encapsulating Security** Payload (ESP) as defined in [RFC2406]

Authentication Header



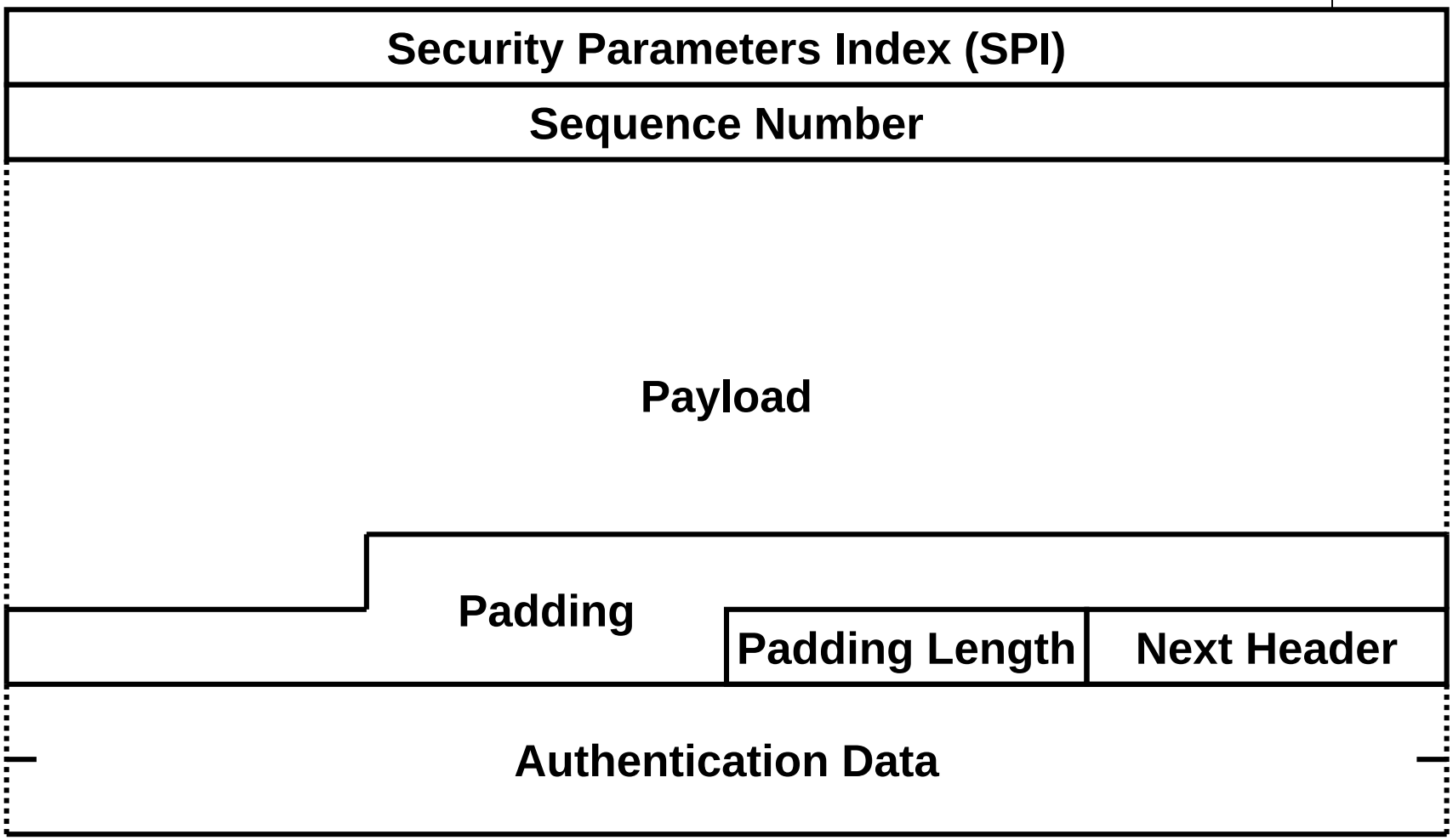
- SPI &địa chỉ IP đích xác định Security Association (SA) hình thành giữa bên gửi và bên nhận.
- SA định nghĩa phương thức xác thực áp dụng lên các packets được trao đổi giữa hai bên
- Thuật toán mặc định là Keyed MD5

Authentication Header (2)

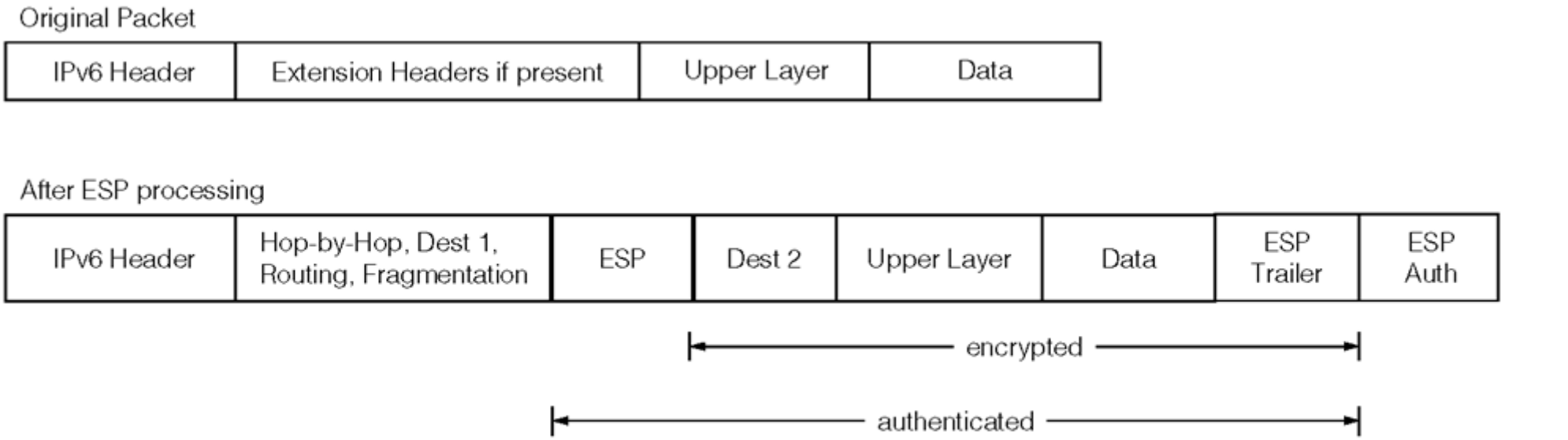


- Sequence Number (SN) Field dùng để tránh phát lại packets tấn công.
- Bên gửi sẽ tăng giá trị SN. Mỗi packet có một SN duy nhất ứng với một SA.
- SN_{max} = 232, giá trị SA mới được sử dụng khi SN đạt max

Encapsulating Security Payload (ESP)



Vị trí của ESP header

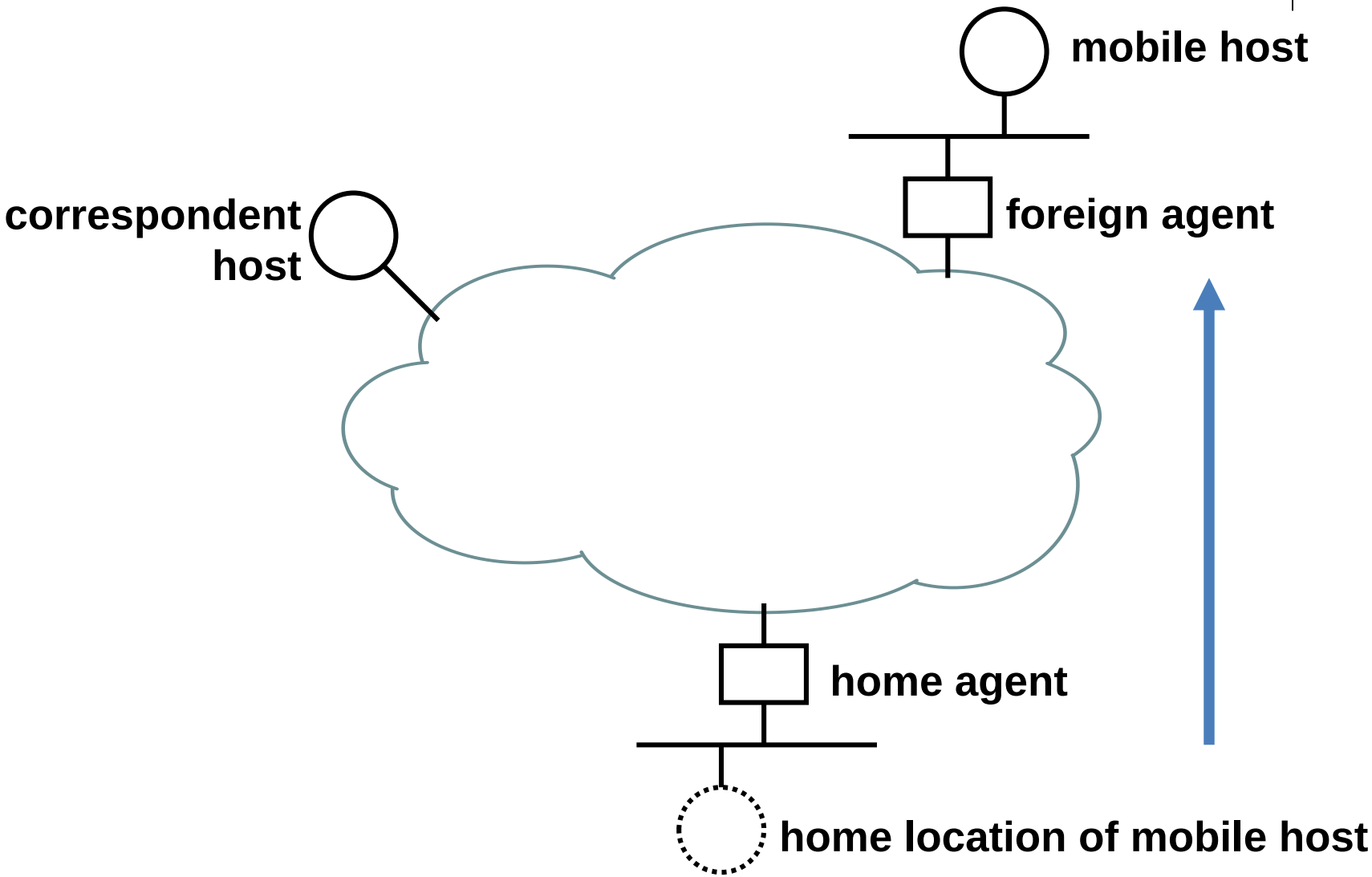


Insertion of the ESP header.

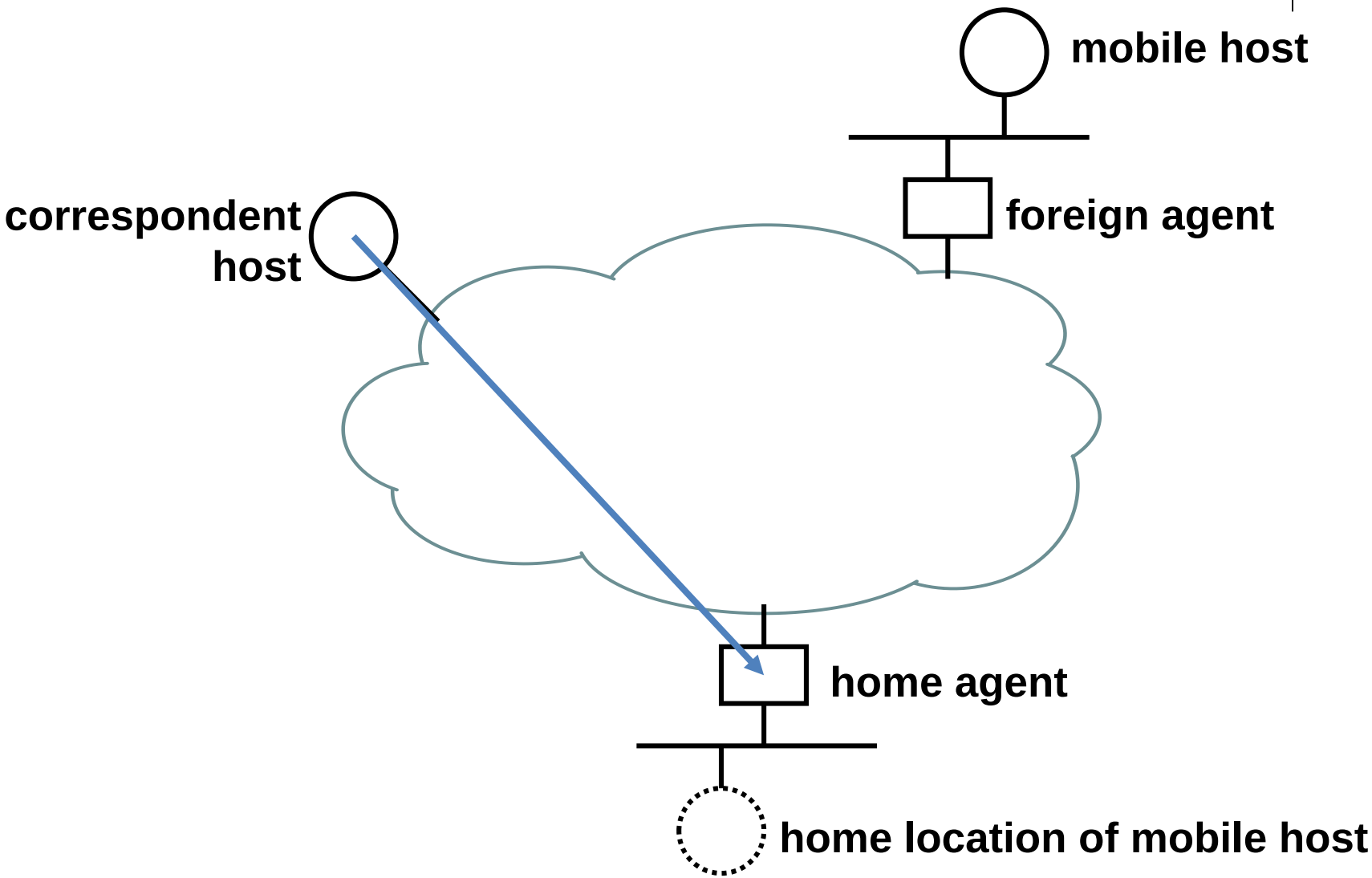
IPv6 Mobility

- Các máy trạm có một hoặc nhiều địa chỉ
- Khi máy trạm di chuyển từ mạng con (home subnet) này sang subnet khác (foreign address) máy trạm sẽ được gán một địa chỉ khách
- Việc gán địa chỉ hoàn toàn tự động
- Địa chỉ khách được gán phải đăng ký với home agent (ví dụ
  là router của mạng home subnet)
- Các packets được gửi đến địa chỉ nhà home address(es) được home agent chặn lại và chuyển tiếp tới địa chỉ khách, dùng phương thức đóng gói (encapsulation)

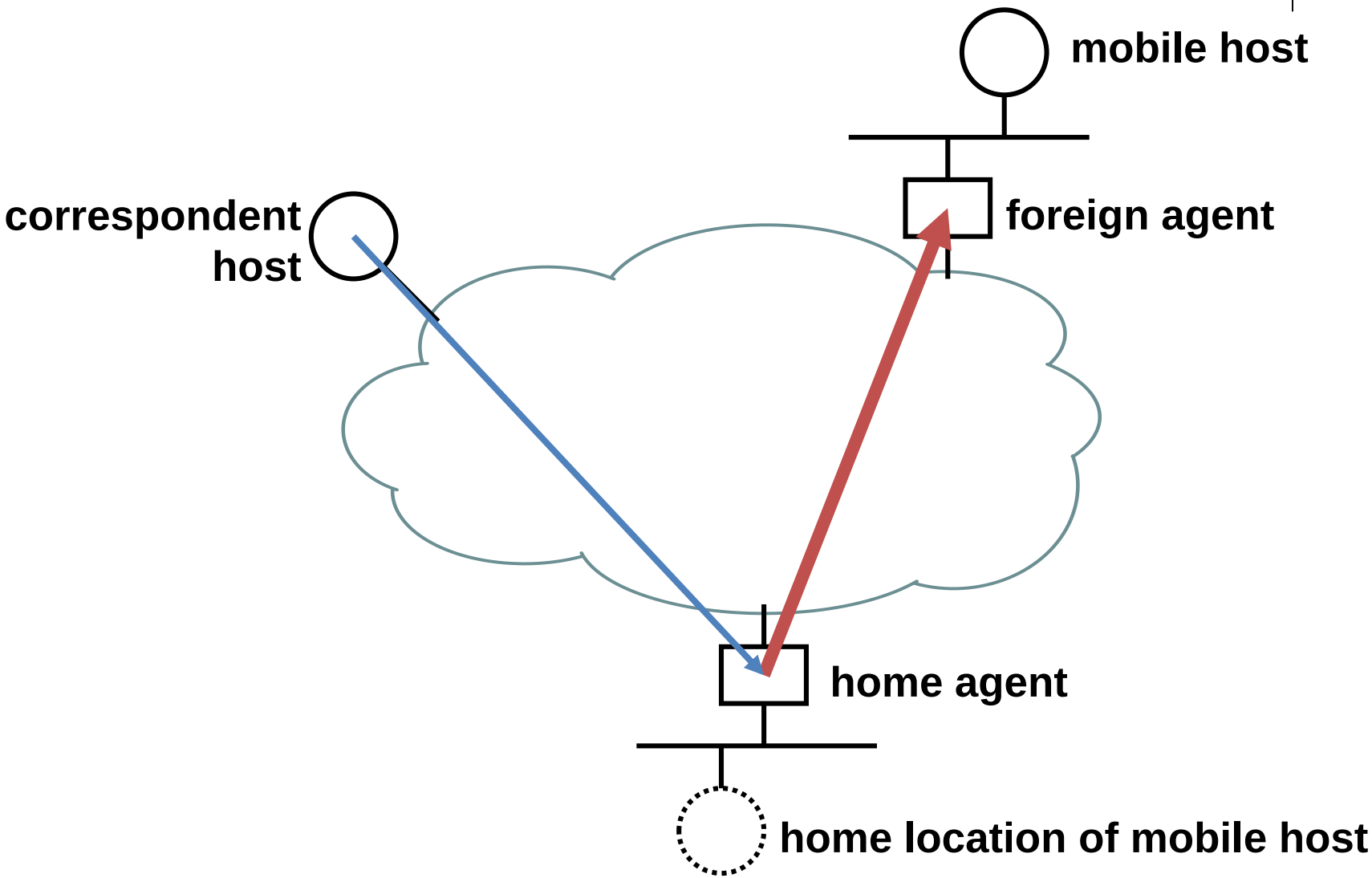
Mobile IP (v4 version)



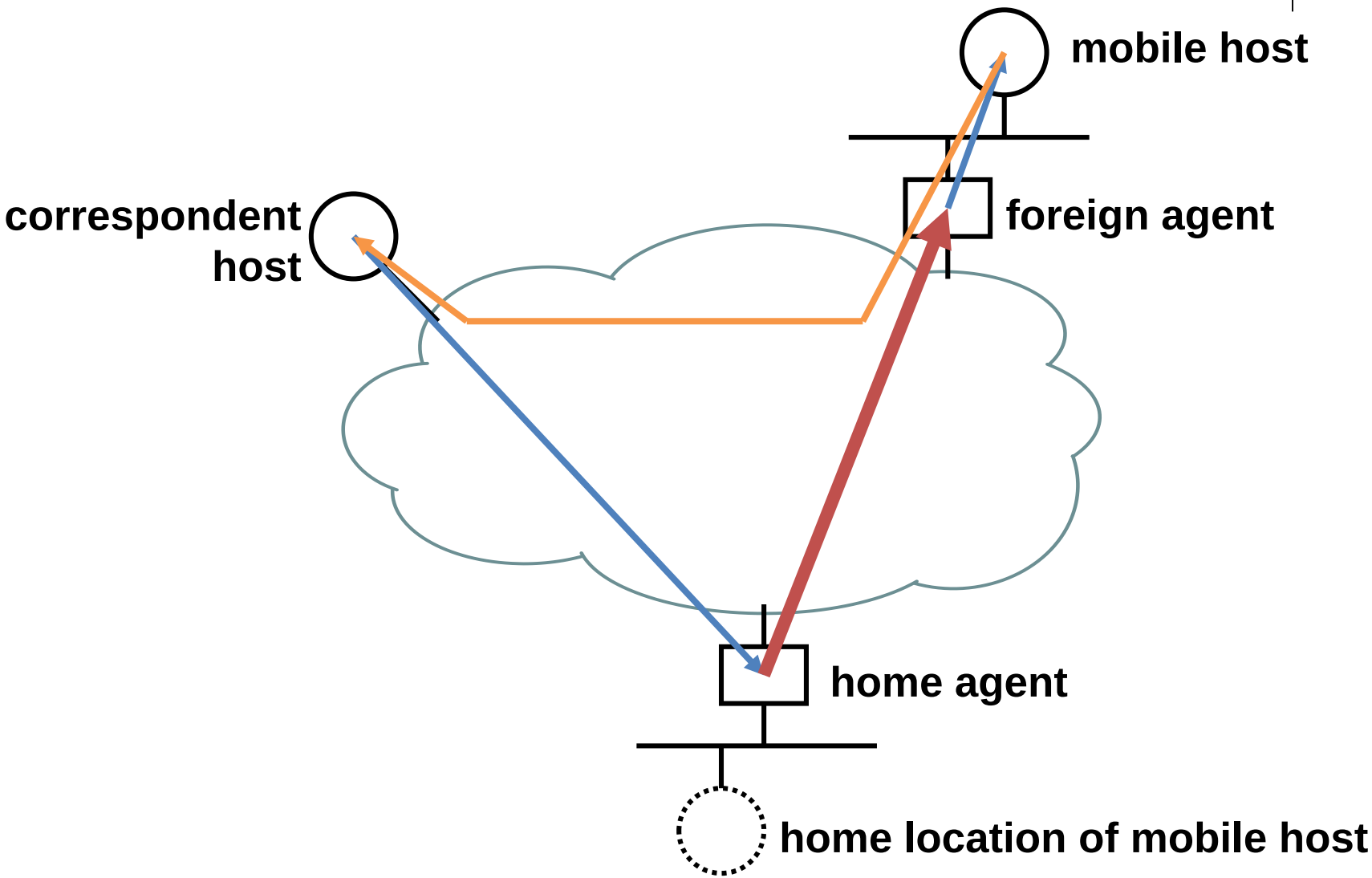
Mobile IP (v4 version)



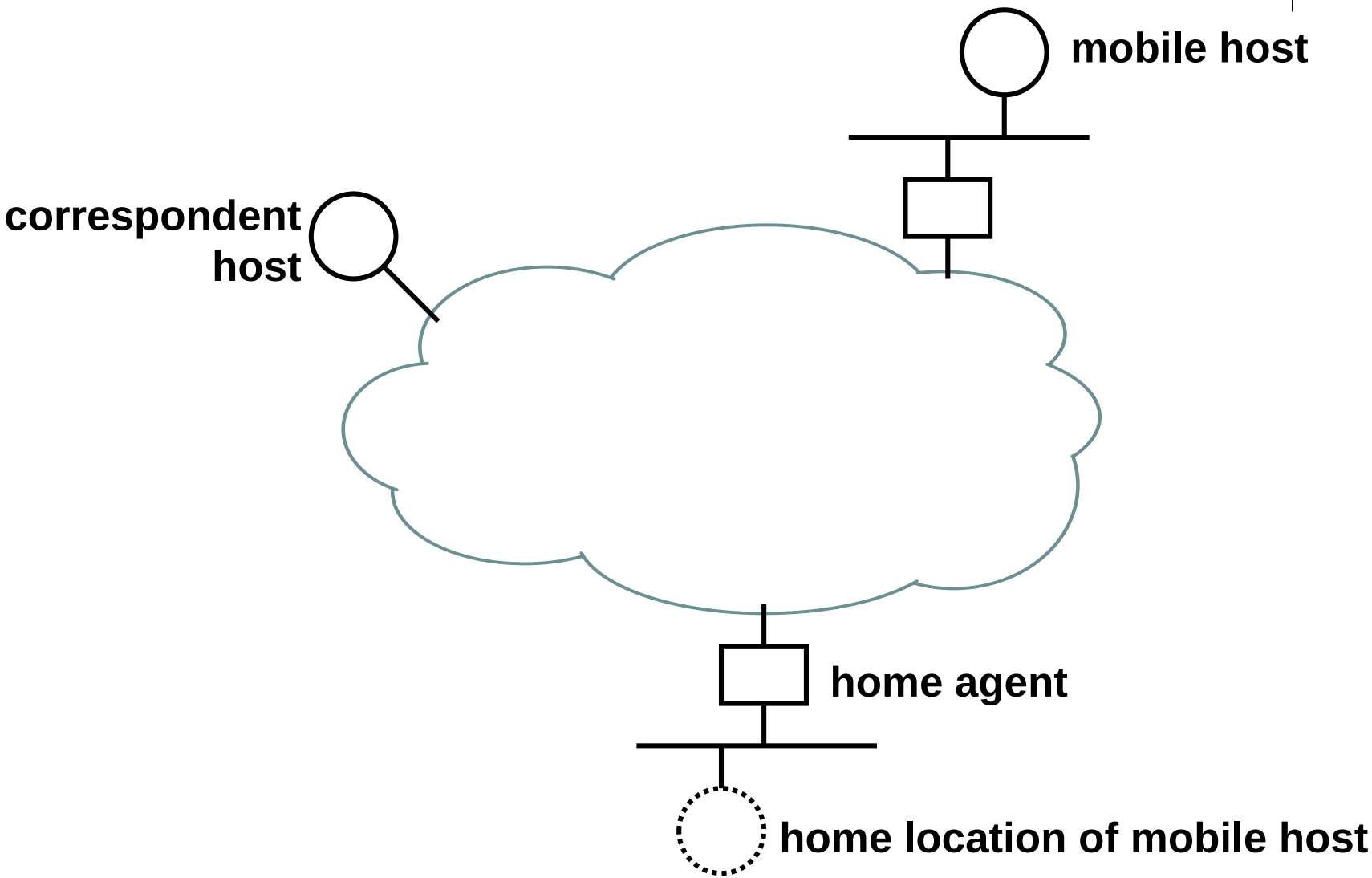
Mobile IP (v4 version)



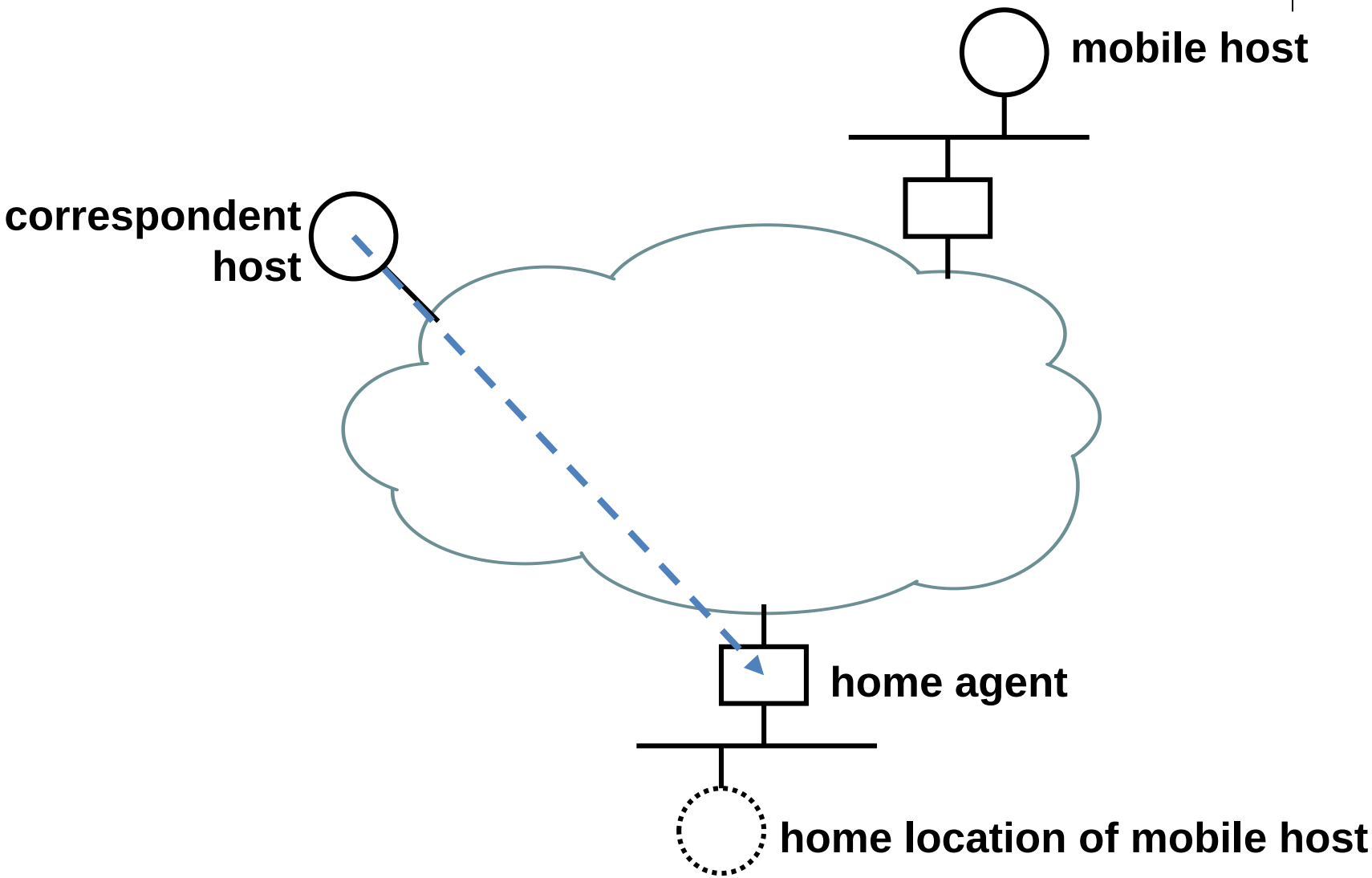
Mobile IP (v4 version)



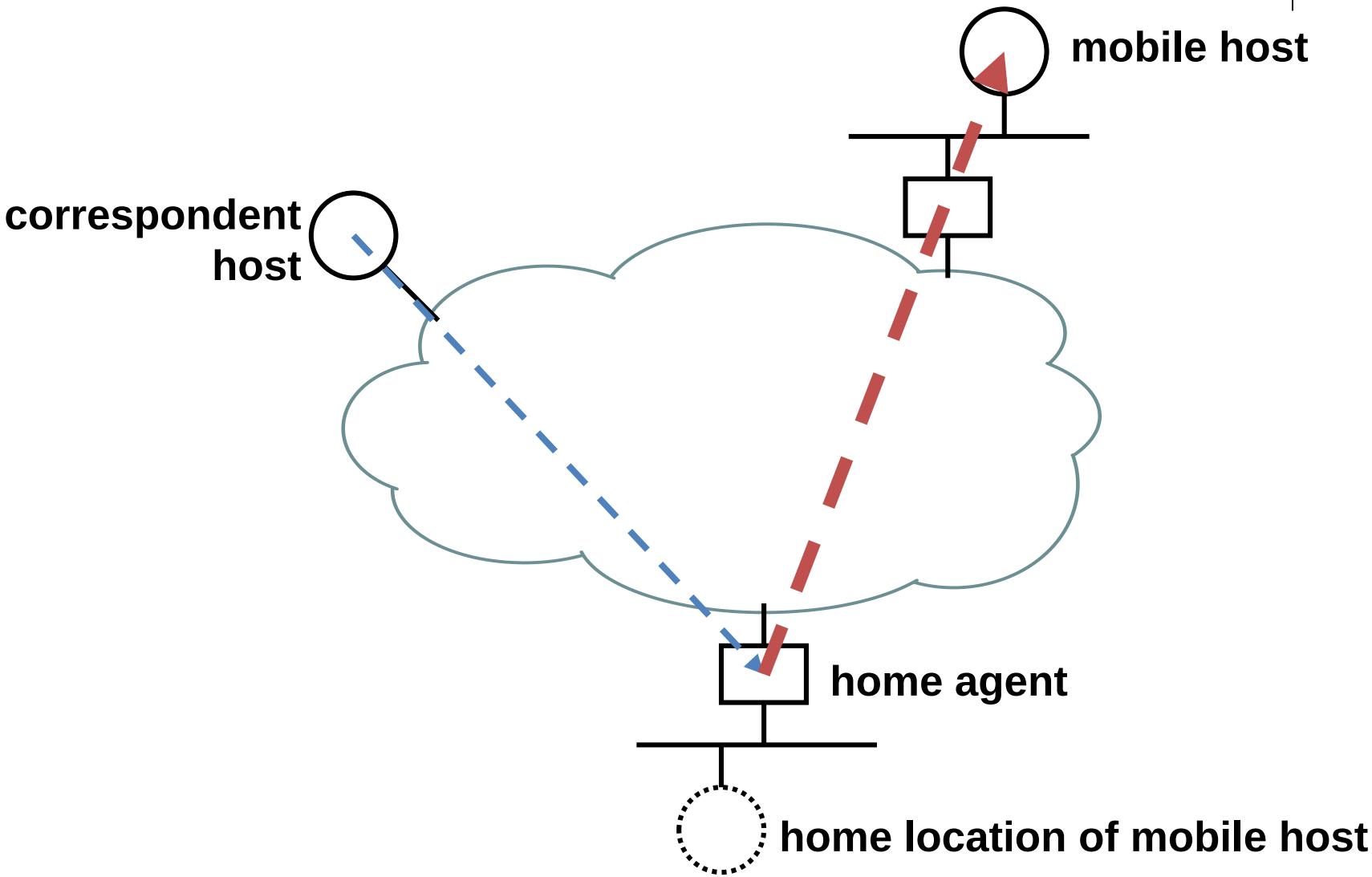
Mobile IPv6


mobile host
correspondent host
home agent
home location of mobile host

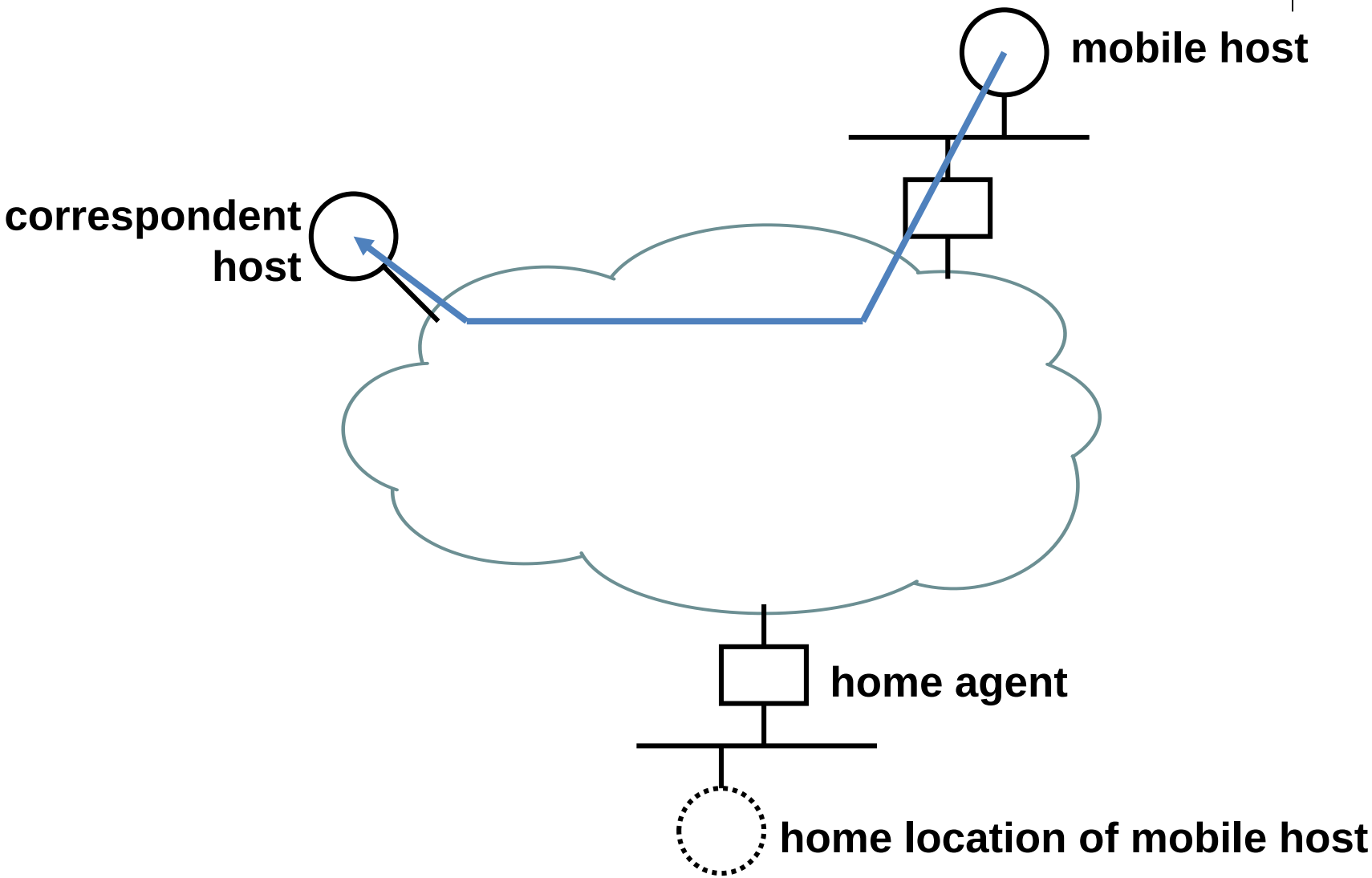
Mobile IP (v6 version)



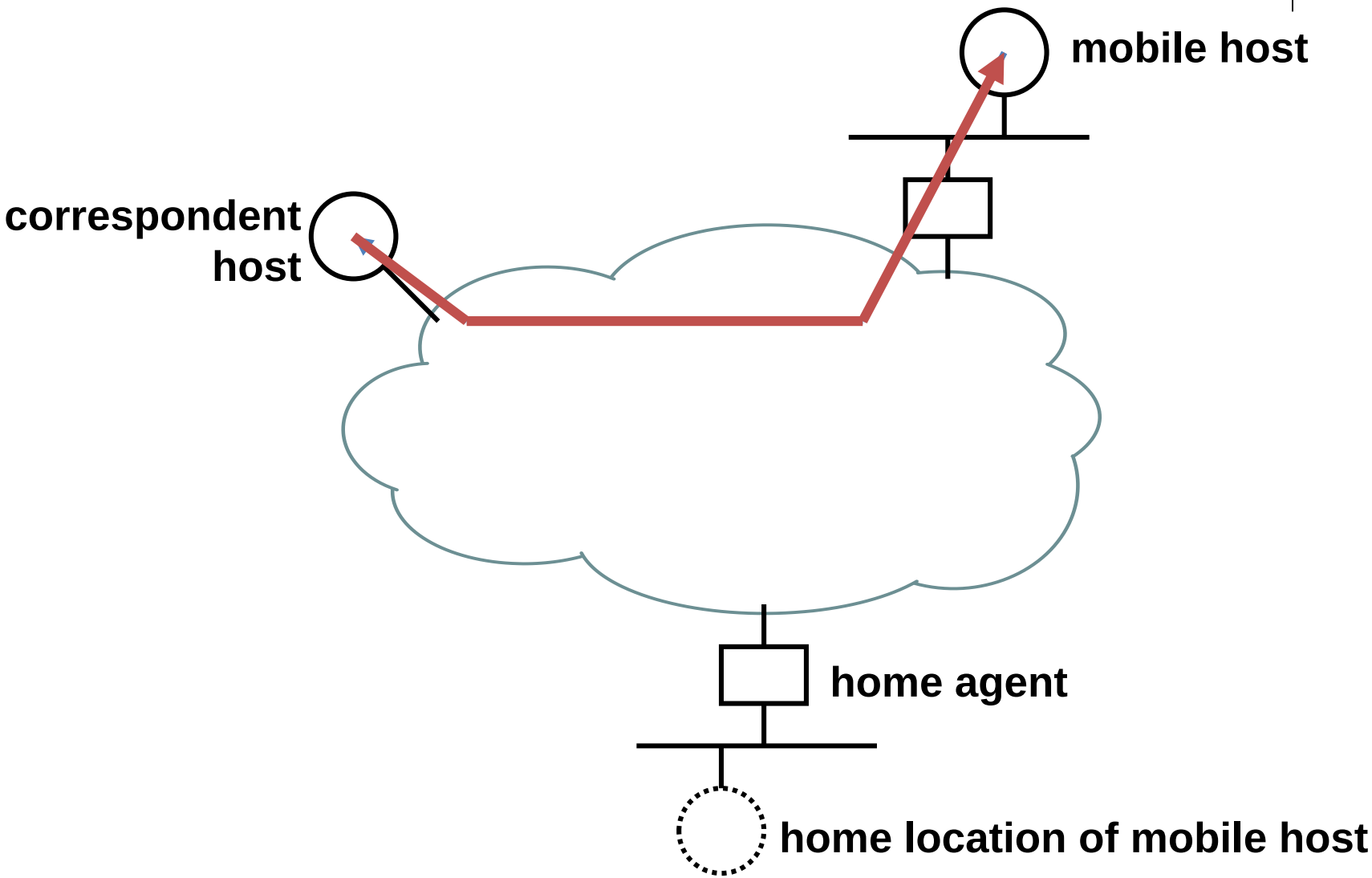
Mobile IP (v6 version)



Mobile IP (v6 version)



Mobile IP (v6 version)



Ảnh hưởng tới các lớp trên

- Thay đổi TCP/UDP checksum “pseudo-header”
- Ảnh hưởng tất cả các giao thức tầng trên trong việc đọc/ghi/lưu và chuyển tiếp địa chỉ IP
- Thời gian sống của Packet không còn bị giới hạn
  Chú ý khi tính kích thước tải lớn nhất do kích thước IP header lớn hơn
- Thêm loại bản ghi DNS : AAAA và A6

Địa chỉ IPv6 trong URL’s

Cần them cặp thẻ []

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

3ffe:2a00:100:7031::1

::192.9.5.5

2010:836B:4179::836B:4179

Khi gõ sẽ thành:

http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html

http://[3ffe:2a00:100:7031::1]

http://[::192.9.5.5]/ipng

http://[2010:836B:4179::836B:4179]

Gán địa chỉ IPv4?

Q: Làm thế nào để máy có địa chỉ IPv4?

- Do người quản trị gán trực tiếp
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: Giao thức cấu hình địa chỉ động
  - “plug-and-play”

DHCP: Dynamic Host Configuration Protocol

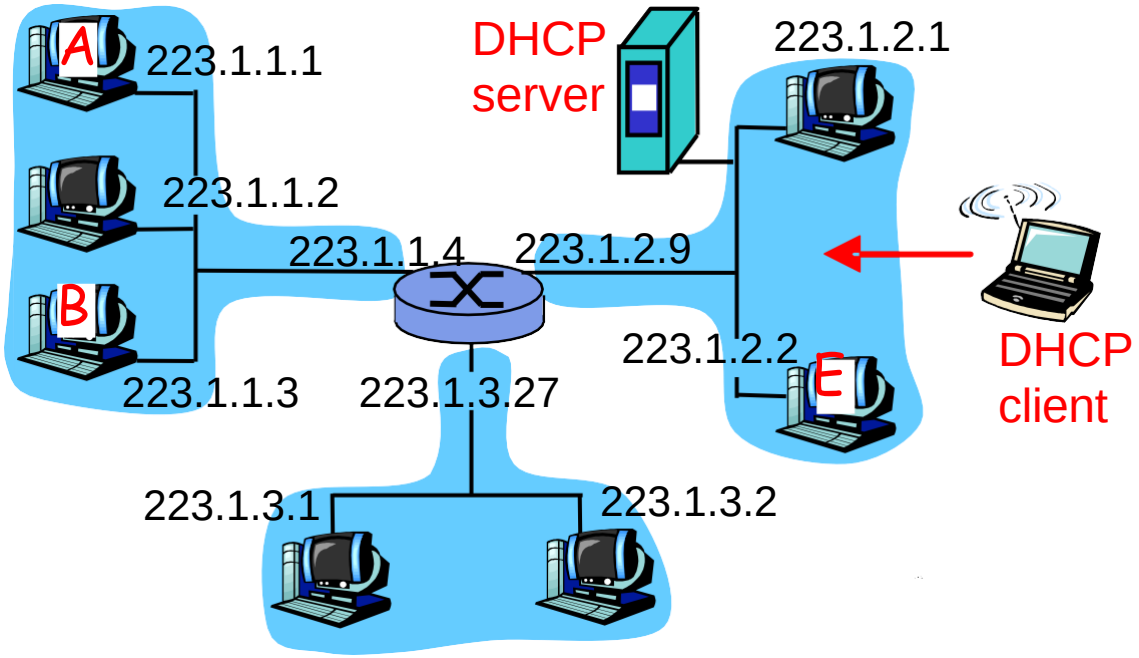
Máy chủ: Cần địa chỉ IP tĩnh vì các máy trạm thường xuyên truy cập

Router: Cần địa chỉ IP tĩnh để cung cấp định tuyến ổn định

Mục đích DHCP: Cho phép máy trạm nhận một địa chỉ IP động khi kết nối vào mạng

- Địa chỉ IP động do máy chủ DHCP quản lý và cung cấp
- Thường dùng cho các máy trạm cài phần mềm client

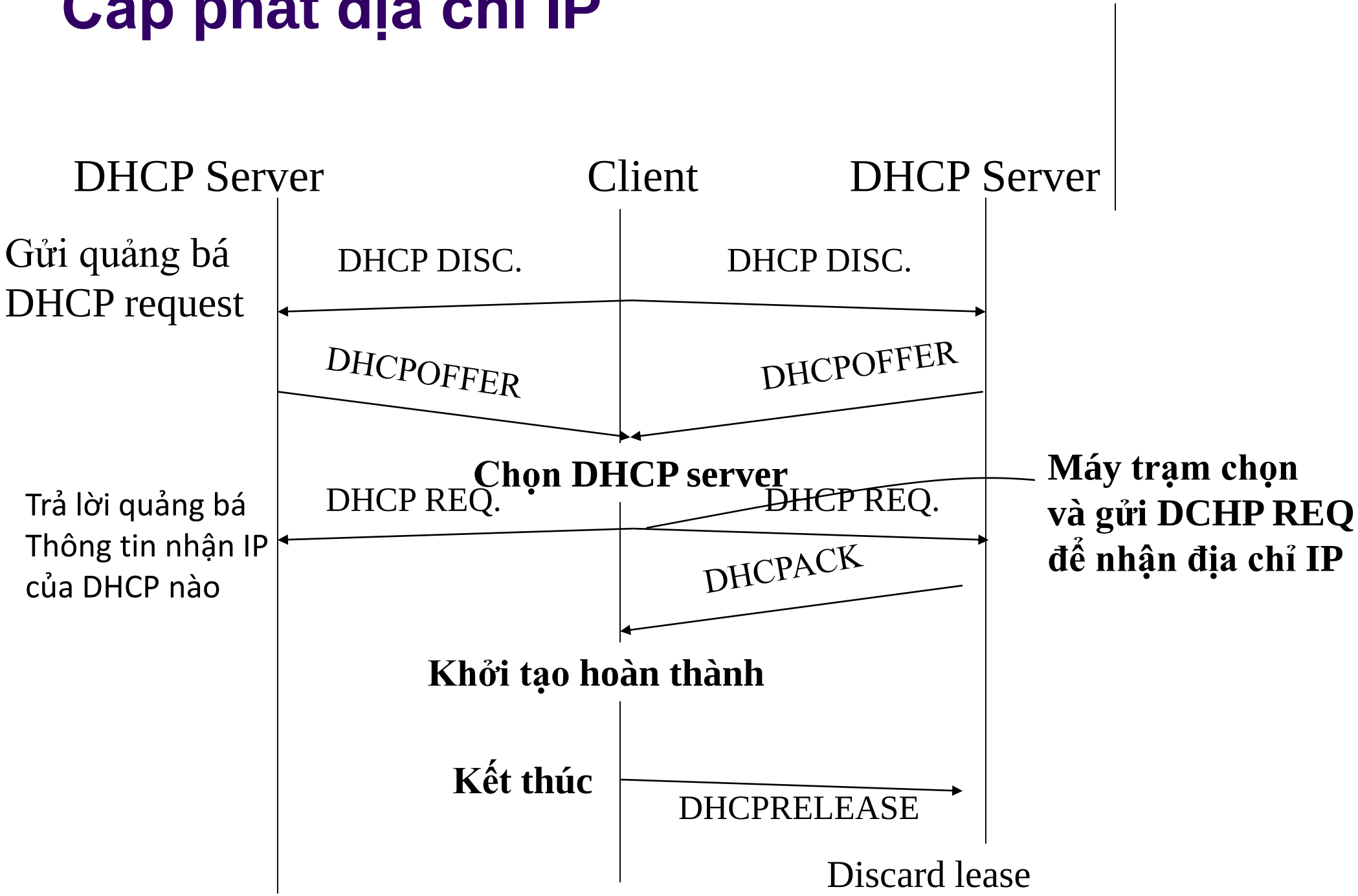
Các thành phần của DHCP



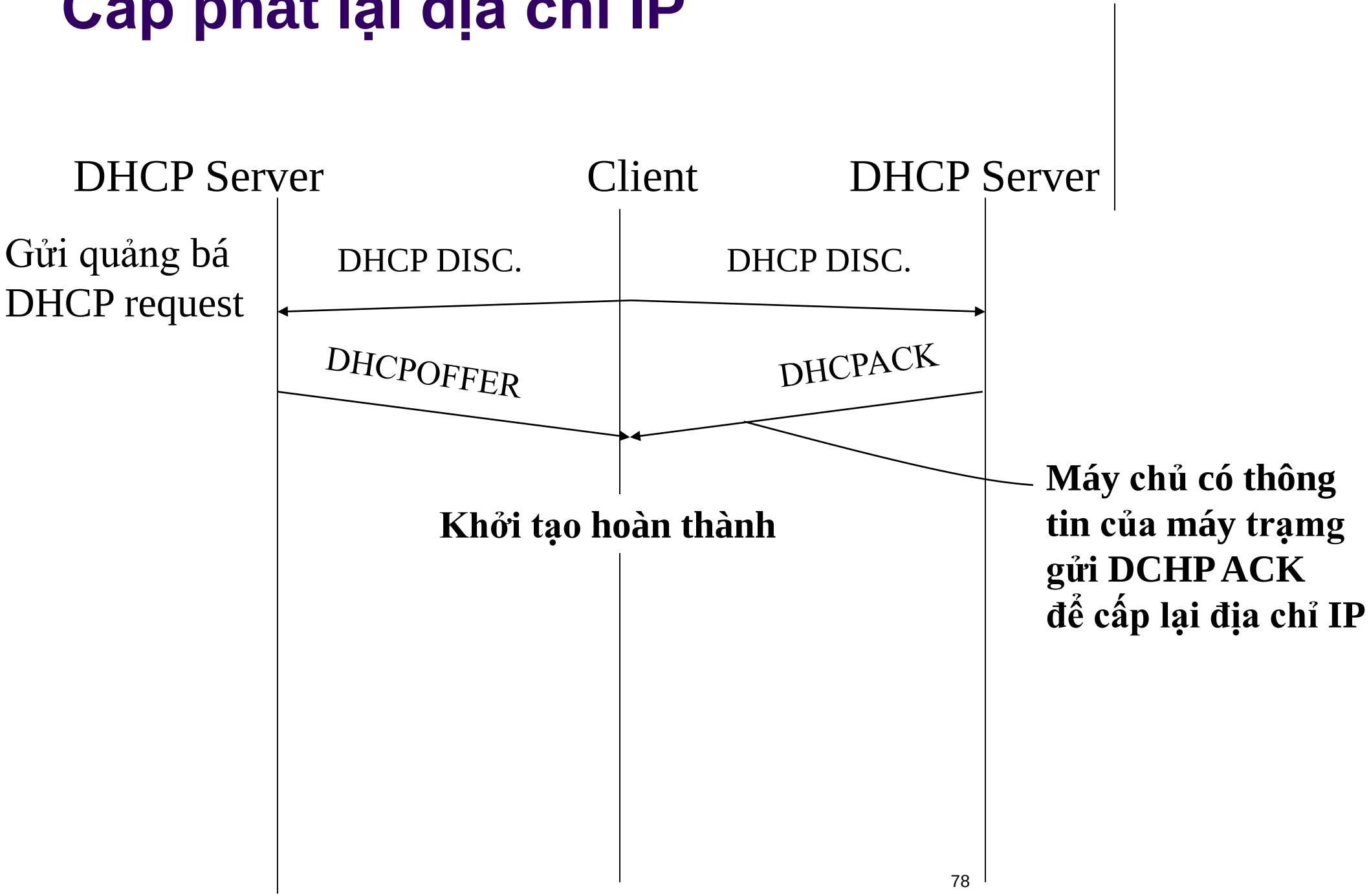
DHCP hoạt động thế nào?

1. Máy trạm quảng bá yêu cầu cấp địa chỉ IP.
2. Máy chủ DHCP nhận được yêu cầu, tiến hành tìm địa chỉ IP trong một khoảng thời gian (lease period) cho máy trạm.
3. Thông tin về địa chỉ IP và các thông tin cấu hình khác được gửi tới máy trạm.
4. Máy trạm xác nhận nhận được thông tin và tiến hành cài đặt.
5. Máy chủ DHCP không cấp địa chỉ IP mới trong khoảng thời gian lease period và cố gắng gán lại địa chi IP cho máy trạm mỗi khi có yêu cầu.

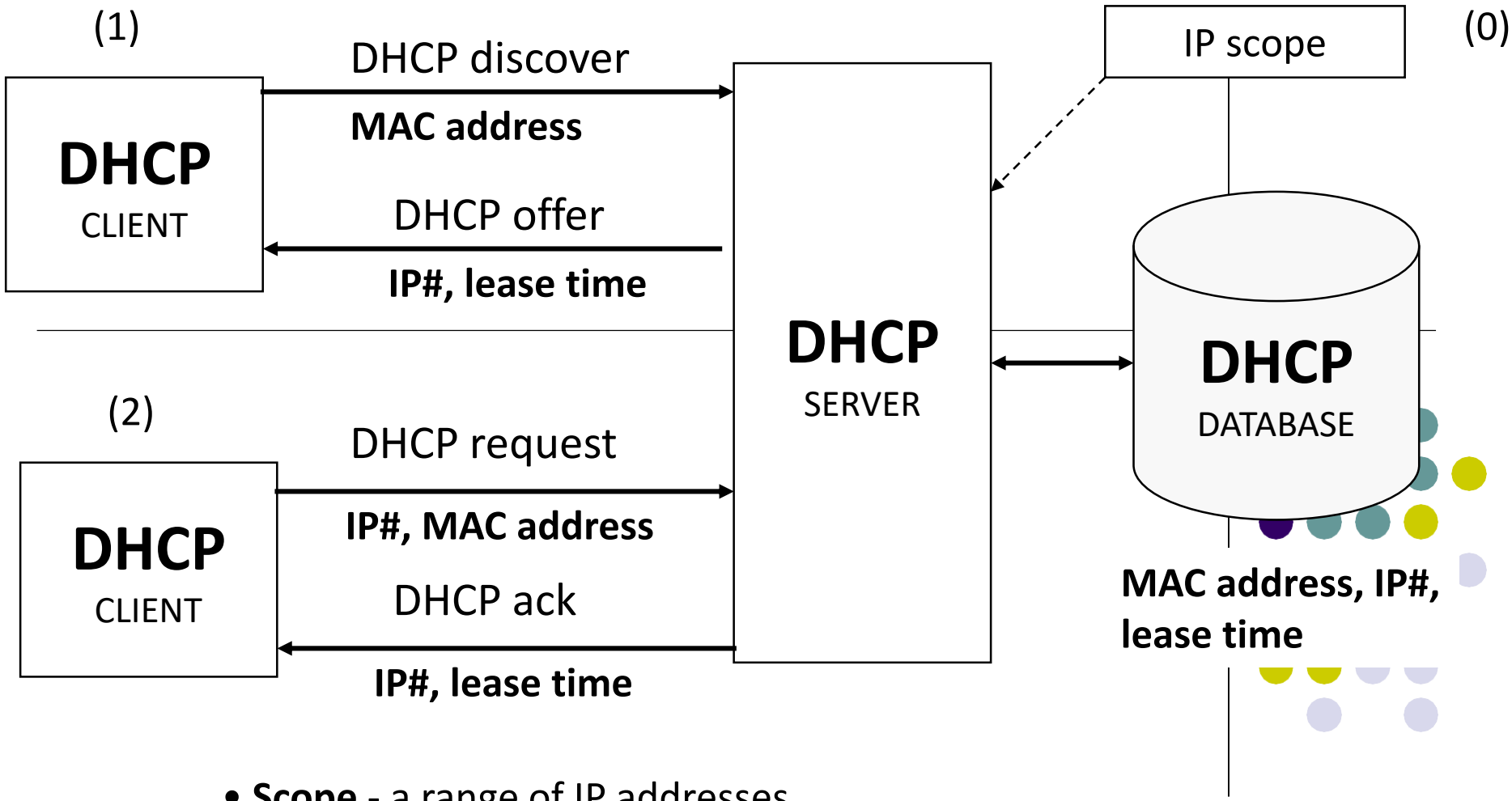
Cấp phát địa chỉ IP



Cấp phát lại địa chỉ IP



DHCP cấp lại IP thế nào?



- **Scope** - a range of IP addresses
- **IP lease** - the IP# is assigned temporarily
- **Reserved IP** - servers are assigned fixed IP addresses

Cấp địa chỉ IP cho mạng?

Q: Một mạng con lấy địa chỉ IP từ đâu?

A: Chia ra từ không gian địa chỉ của ISP (Internet Service Provider)

ISP's block	11001000 00010111 00010000	00000000	200.23.16.0/20
Organization 0	11001000 00010111 0001000**0**	00000000	200.23.16.0/23
Organization 1	11001000 00010111 0001001**0**	00000000	200.23.18.0/23
Organization 2	11001000 00010111 0001010**0**	00000000	200.23.20.0/23
...	.....	....	....
Organization 7	11001000 00010111 0001111**0**	00000000	200.23.30.0/23

Quản lý địa chỉ IP

Q: ISP lấy địa chỉ IP từ đâu ?

A: ICANN: Internet Corporation for Assigned Names and Numbers

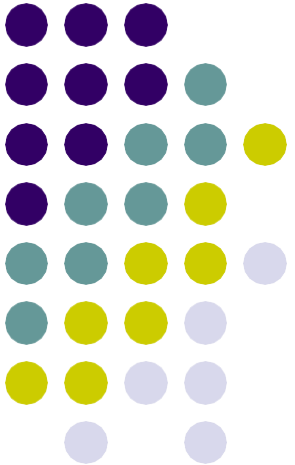
- Cấp phát địa chỉ
- Quản DNS….

Internet Control Message Protocol

Tổng quan

Khuôn dạng gói tin

Ping và Traceroute

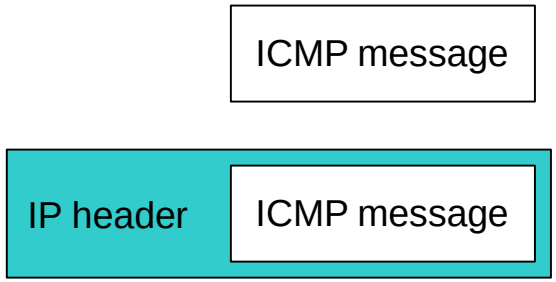


Tổng quan về ICMP (1)

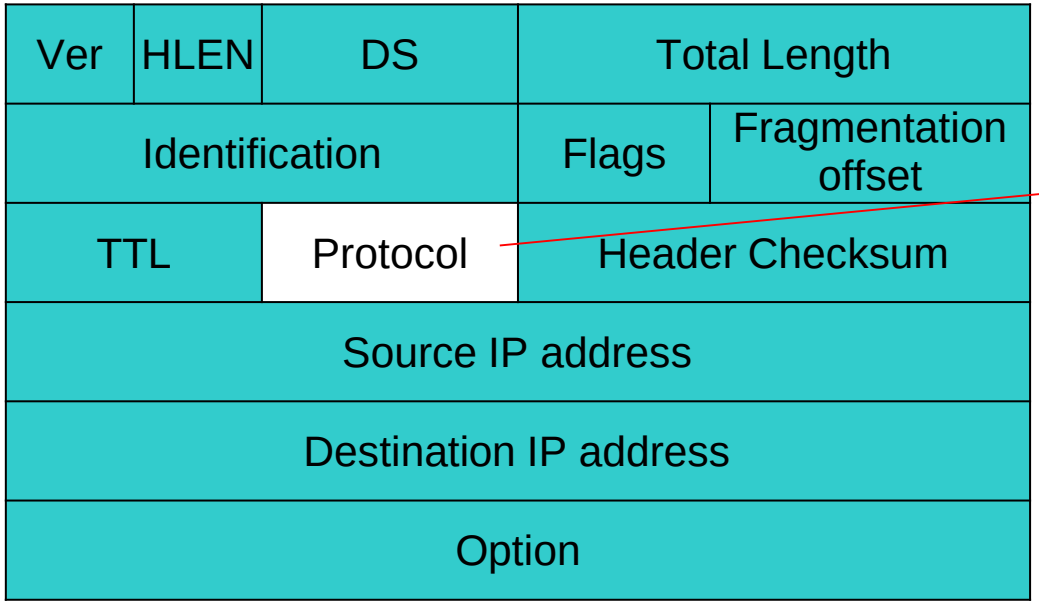
- IP là giao thức không tin cậy, không liên kết
  - Thiếu các cơ chế hỗ trợ và kiểm soát lỗi
- ICMP được sử dụng ở tầng mạng để trao đổi thông tin
  - Báo lỗi: báo gói tin không đến được một máy trạm, một mạng, một cổng, một giao thức.
  - Thông điệp phản hồi

Tổng quan về ICMP (2)

- Cũng là giao thức tầng mạng, song "phía trên" IP:
  - Thông điệp ICMP chứa trong các gói tin IP
- ICMP message: Type, Code, cùng với 8 bytes đầu tiên của gói tin IP bị lỗi



Nhắc lại: IP header và trường Protocol



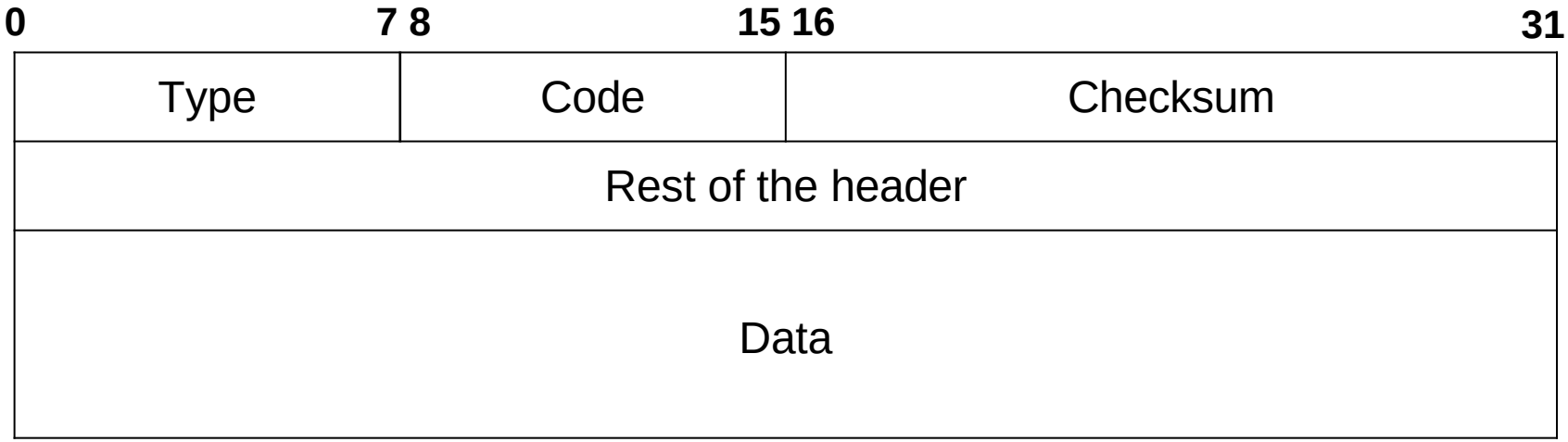
Protocol:
- 1: ICMP
- 2: IGMP
- 6: TCP
- 17: UDP
- 89: OSPF

Có thể xem số hiệu giao thức tại

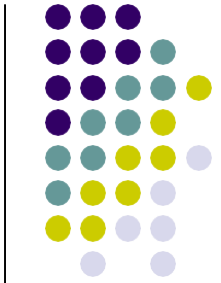
/etc/protocols
C:\WINDOWS\system32\drivers\etc\protocols

Khuôn dạng gói tin ICMP

- Type: dạng gói tin ICMP
- Code: Nguyên nhân gây lỗi
- Checksum
- Mỗi dạng có phần còn lại tương ứng



Một số dạng gói tin ICMP



ICMP Message Type	Error-reporting messages	3	Destination Unreachable
		4	Source quench
		5	Redirection
		11	Time exceeded
		12	Parameter problem
	Query messages	8 or 0	Echo reply or request
		13 or 14	Time stamp request or reply
		17 or 18	Address mask request or reply
		9 or 10	Router advertisement or solicitation

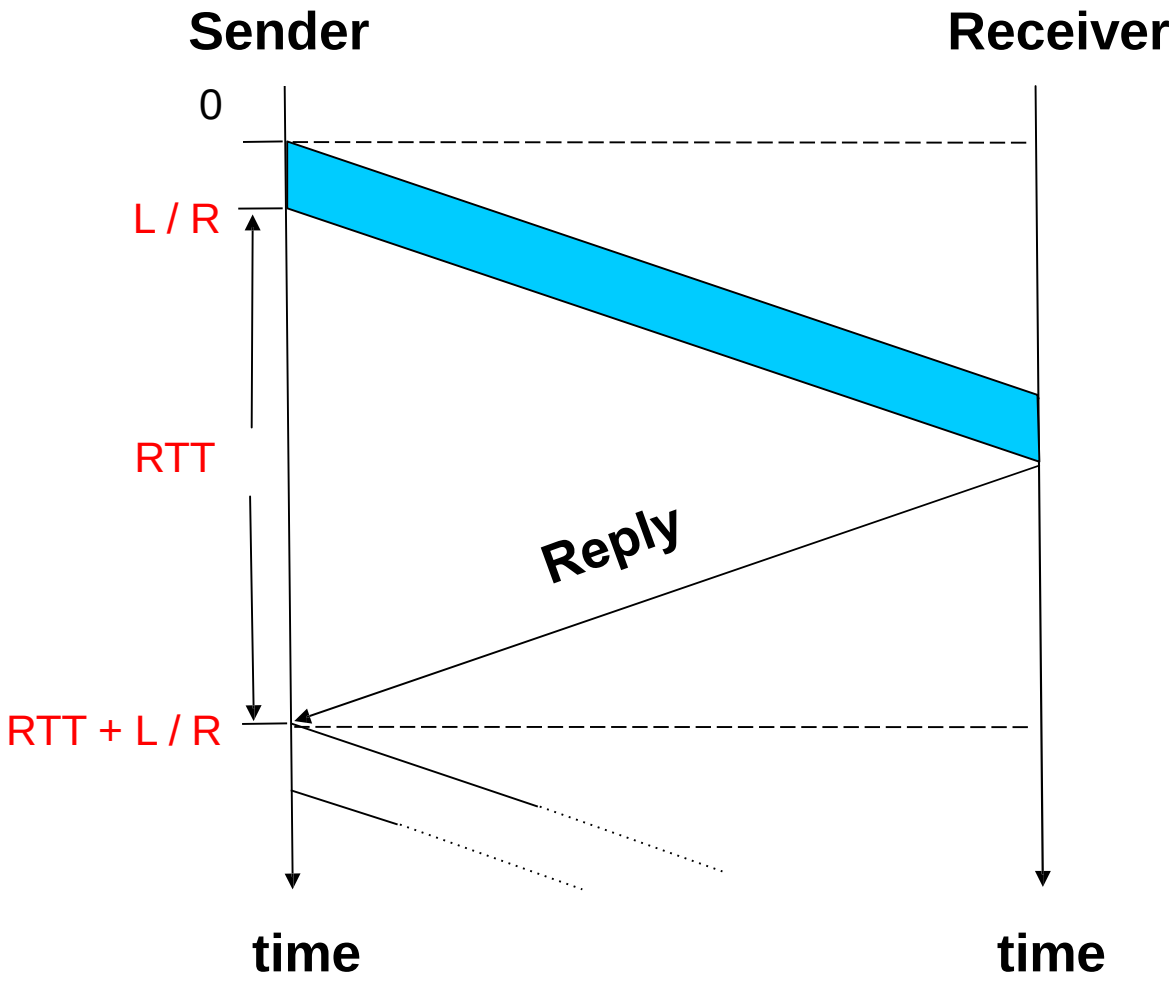
ICMP và các công cụ debug

- ICMP luôn hoạt động song trong suốt với người sử dụng
- NSD có thể sử dụng ICMP thông qua các công cụ debug
  - ping
  - traceroute

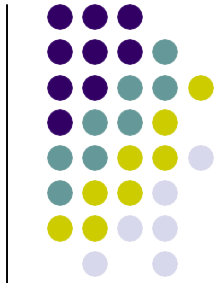
Ping và ICMP

- ping
  - Sử dụng để kiểm tra kết nối
  - Gửi gói tin “ICMP echo request”
  - Bên nhận trả về “ICMP echo reply”
- Mỗi gói tin có một số hiệu gói tin
- Trường dữ liệu chứa thời gian gửi gói tin
  - Tính được thời gian đi và về - RTT (round-trip time)

RTT (Round-Trip Time)



Ping: Ví dụ



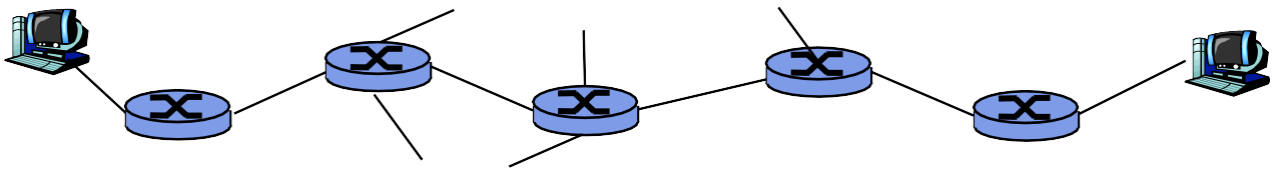
```
C:\Documents and Settings\hongson>ping www.yahoo.co.uk

Pinging www.euro.yahoo-eu1.akadns.net [217.12.3.11] with 32 bytes of data:

Reply from 217.12.3.11: bytes=32 time=600ms TTL=237
Reply from 217.12.3.11: bytes=32 time=564ms TTL=237
Reply from 217.12.3.11: bytes=32 time=529ms TTL=237
Reply from 217.12.3.11: bytes=32 time=534ms TTL=237

Ping statistics for 217.12.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 529ms, Maximum = 600ms, Average = 556ms
```

Traceroute: Công cụ dò vết đường đi

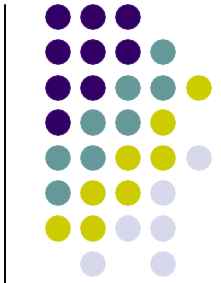
```
C:\Documents and Settings\hongson>tracert www.jaist.ac.jp

Tracing route to www.jaist.ac.jp [150.65.5.208]
over a maximum of 30 hops:

  1    1 ms    <1 ms    <1 ms 192.168.1.1
  2   15 ms    14 ms    13 ms  210.245.0.42
  3   13 ms    13 ms    13 ms  210.245.0.97
  4   14 ms    13 ms    14 ms 210.245.1.1
  5  207 ms   230 ms    94 ms pos8-2.br01.hkg04.pccwbtn.net [63.218.115.45]
  6    *      403 ms   393 ms 0.so-0-1-0.XT1.SCL2.ALTER.NET [152.63.57.50]
  7  338 ms   393 ms   370 ms 0.so-7-0-0.XL1.SJC1.ALTER.NET [152.63.55.106]
  8  402 ms   404 ms   329 ms POS1-0.XR1.SJC1.ALTER.NET [152.63.55.113]
  9  272 ms   288 ms   310 ms 193.ATM7-0.GW3.SJC1.ALTER.NET [152.63.49.29]
 10   205 ms   206 ms   204 ms wide-mae-gw.customer.alter.net [157.130.206.42]
 11   427 ms   403 ms   370 ms ve-13.foundry2.otemachi.wide.ad.jp [192.50.36.62]
 12   395 ms   399 ms   417 ms ve-4.foundry3.nezu.wide.ad.jp [203.178.138.244]
 13   355 ms   356 ms   378 ms ve-3705.cisco2.komatsu.wide.ad.jp [203.178.136.193]
 14   388 ms   398 ms   414 ms c76.jaist.ac.jp [203.178.138.174]
 15   438 ms   377 ms   435 ms www.jaist.ac.jp [150.65.5.208]

Trace complete.
```

Traceroute và ICMP: Cơ chế hoạt động

- Bên gửi truyền gói tin cho bên nhận
  - Gói thứ nhất có TTL =1
  - Gói thứ 2 có TTL=2, …
- Khi gói tin thứ n đến router thứ n:
  - Router hủy gói tin
  - Gửi trả lại một gói tin ICMP (type 11, code 0)
  - Có chứa tên và địa chỉ IP của router
- khi nhận được gói tin trả lời, bên gửi sẽ tính ra RTT

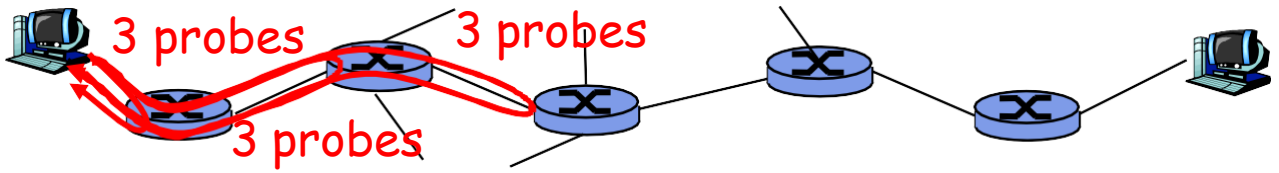


Traceroute và ICMP



Điều kiện kết thúc

- Gói tin đến được đích
- Đích trả về gói tin ICMP “host unreachable” (type 3, code 3)
- Khi nguồn nhận được gói tin ICMP này sẽ dừng lại
- Mỗi gói tin lặp lại 3 lần



Traceroute: Ví dụ

```
C:\Documents and Settings\hongson>tracert www.jaist.ac.jp

Tracing route to www.jaist.ac.jp [150.65.5.208]
over a maximum of 30 hops:

  1    1 ms    <1 ms    <1 ms 192.168.1.1
  2   15 ms    14 ms    13 ms  210.245.0.42
  3   13 ms    13 ms    13 ms  210.245.0.97
  4   14 ms    13 ms    14 ms 210.245.1.1
  5  207 ms   230 ms    94 ms pos8-2.br01.hkg04.pccwbtn.net [63.218.115.45]
  6    *      403 ms   393 ms 0.so-0-1-0.XT1.SCL2.ALTER.NET [152.63.57.50]
  7  338 ms   393 ms   370 ms 0.so-7-0-0.XL1.SJC1.ALTER.NET [152.63.55.106]
  8  402 ms   404 ms   329 ms POS1-0.XR1.SJC1.ALTER.NET [152.63.55.113]
  9  272 ms   288 ms   310 ms 193.ATM7-0.GW3.SJC1.ALTER.NET [152.63.49.29]
 10   205 ms   206 ms   204 ms wide-mae-gw.customer.alter.net [157.130.206.42]
 11   427 ms   403 ms   370 ms ve-13.foundry2.otemachi.wide.ad.jp [192.50.36.62]
 12   395 ms   399 ms   417 ms ve-4.foundry3.nezu.wide.ad.jp [203.178.138.244]
 13   355 ms   356 ms   378 ms ve-3705.cisco2.komatsu.wide.ad.jp [203.178.136.193]
 14   388 ms   398 ms   414 ms c76.jaist.ac.jp [203.178.138.174]
 15   438 ms   377 ms   435 ms www.jaist.ac.jp [150.65.5.208]

Trace complete.
```

Tổng kết

- Giao thức IP
  - Địa chỉ và khuôn dạng gói tin
  - Mạng con, mặt nạ mạng
- Giao thức ICMP
  - Khuôn dạng gói tin
  - Ping, Traceroute

Tuần tới: tiếp tục về tầng mạng

- Vấn đề chọn đường
- Bộ định tuyến, bảng chọn đường
- Chọn đường tĩnh và chọn đường động