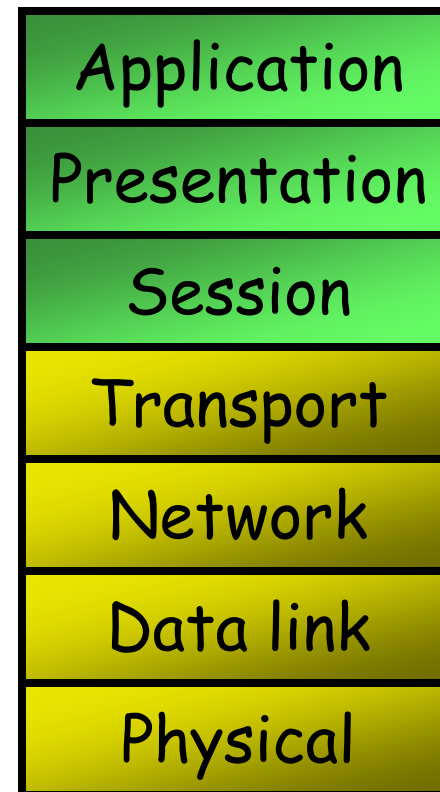




# Tầng Mạng

# MỤC TIÊU

- Thiết lập kết nối giữa 2 host để truyền dữ liệu từ host - host



# TẦNG MẠNG VS TẦNG VẬN CHUYỂN

- *Tầng mạng*: cung cấp kết nối logic giữa các host
- *Tầng vận chuyển*: cung cấp kết nối logic giữa các tiến trình
  - Dựa trên, mở rộng dịch vụ của tầng mạng

## Ví dụ:

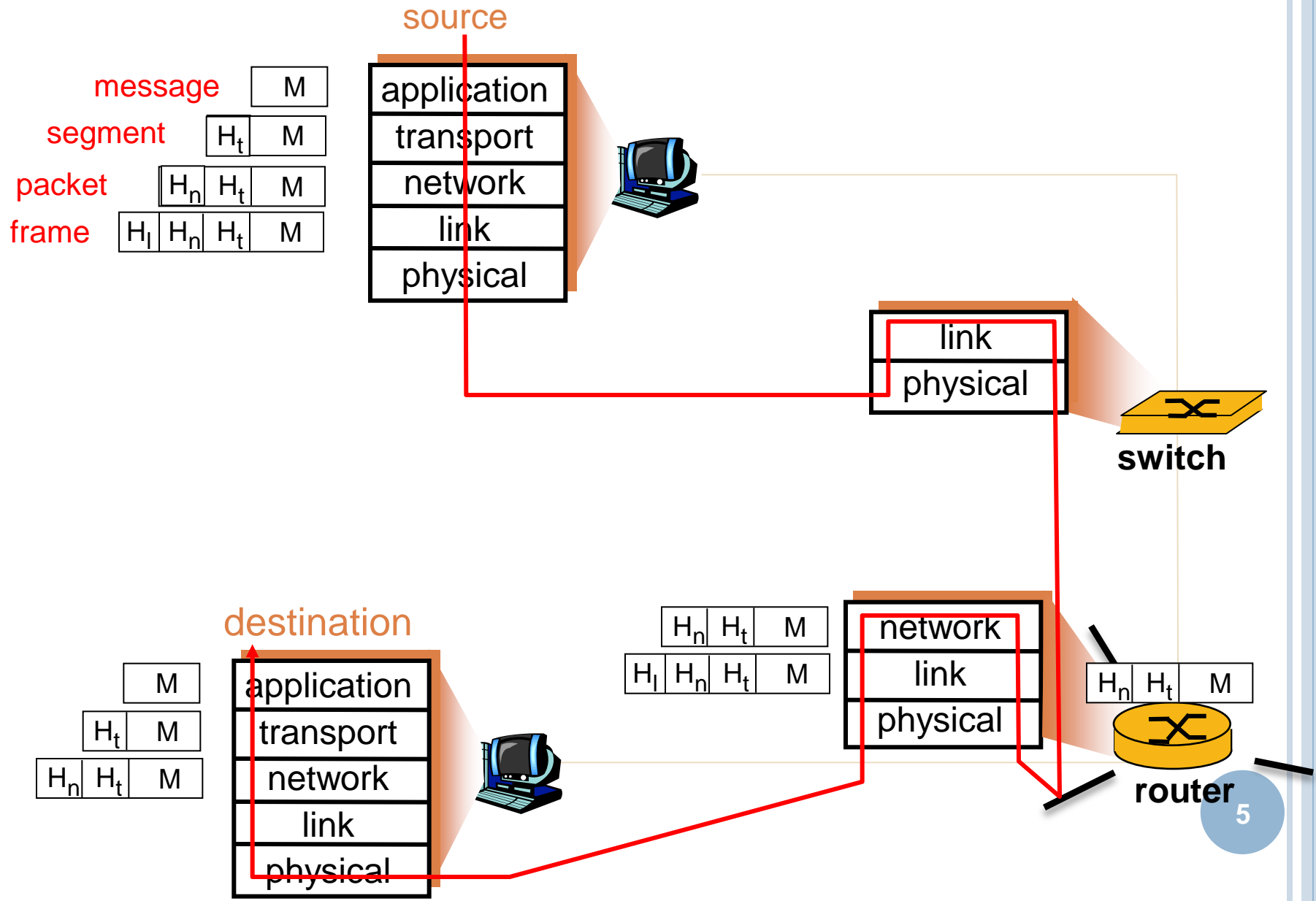
*A gửi B 1 bức thư qua đường bưu điện*

- processes = A, B
- app messages = bức thư
- hosts = nhà của A, nhà của B
- transport protocol ???
- network-layer protocol???

# NỘI DUNG

- Giới thiệu
- Định tuyến – chuyển tiếp
- Giao thức IP
- Giao thức ICMP
- Giao thức NAT

# NHẮC LẠI



# GIỚI THIỆU - 1

- Thực hiện chuyển các segment từ host gửi đến host nhận
- Tại host gửi:
  - Nhận các segment từ transport layer
  - Đóng gói thành các packet
- Tại host nhận:
  - Nhận các packet từ data link layer
  - Chuyển các segment lên transport layer
- Tại các router:
  - Dựa vào **thông tin đích đến** để chuyển các packet đến host nhận
    - Định tuyến: quyết định gói tin đi đường nào
    - Chuyển tiếp: chuyển gói tin từ interface nhận ra interface gửi

## GIỚI THIỆU - 2

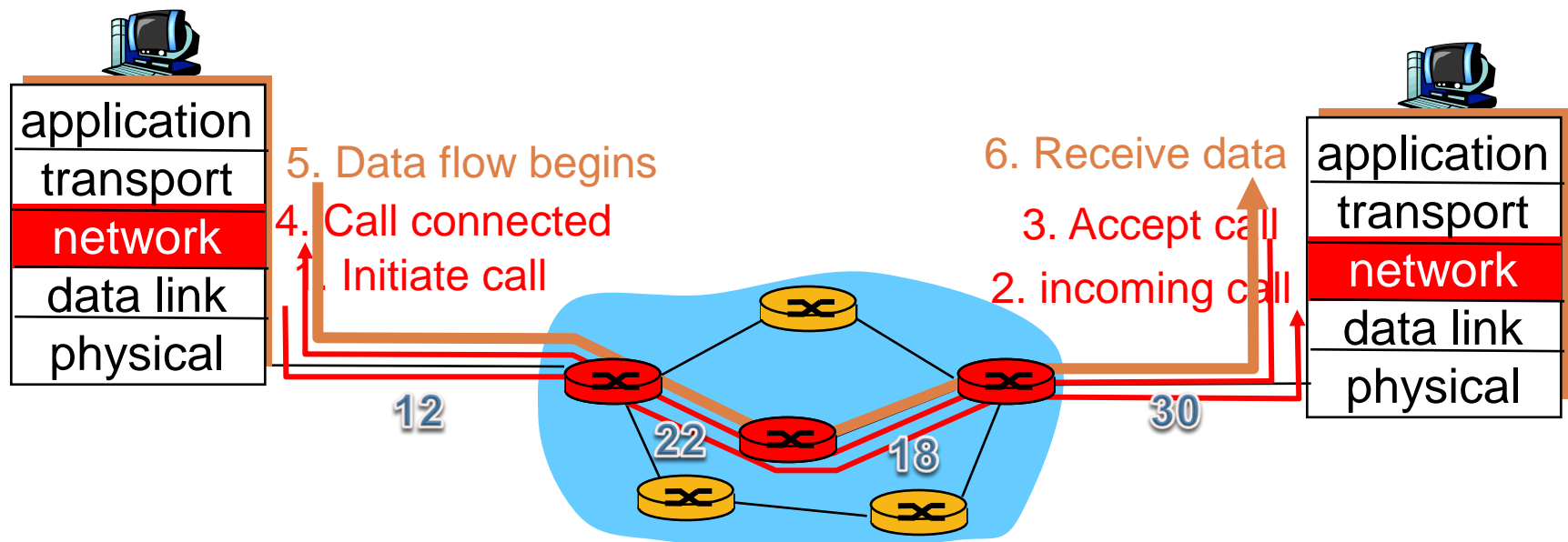
- Tầng mạng cung cấp 2 loại dịch vụ
  - Hướng kết nối (Connection)
    - Virtual Circuit
    - Trước khi truyền dữ liệu, 2 host phải thiết lập kết nối
  - Hướng không kết nối (Connectionless)
    - Datagram Network
    - Không cần thiết lập kết nối trước khi gửi
- Trong 1 kiến trúc mạng: chỉ hỗ trợ duy nhất 1 loại dịch vụ

# VIRTUAL CIRCUIT (VC) NETWORK - 1

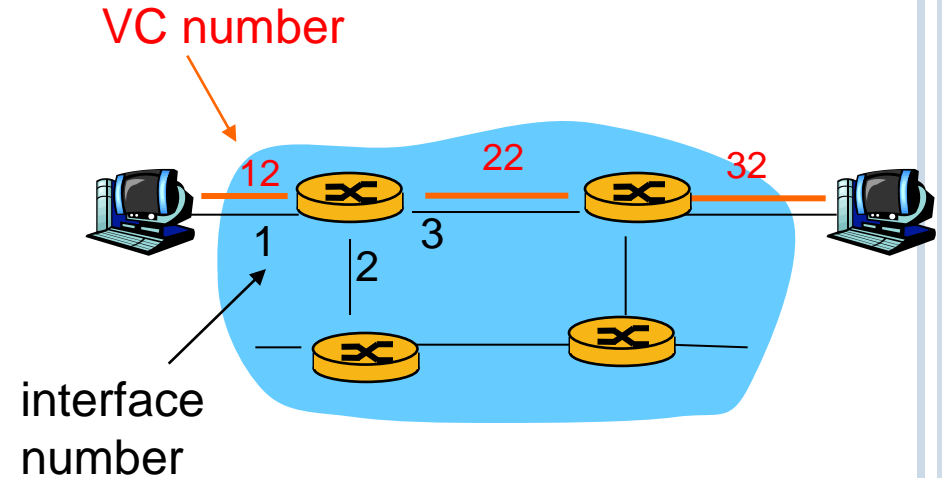
- Thiết lập, quản lý, duy trì mỗi kết nối khi truyền dữ liệu
  - 1 đường đi ảo khi truyền dữ liệu
    - Số hiệu VC (VC number)
      - Khác nhau trên mỗi link
  - Mỗi gói tin có một virtual circuit identifier (VC ID)
  - Các router duy trì trạng thái kết nối đi qua
    - bảng chuyển đổi VC ID
    - Thay thế thông tin VD ID của gói tin đi ngang qua router
- Thông tin định tuyến: Virtual Circuit number (VC ID)
- Dùng trong ATM, X.25, Frame-Relay,...



# VIRTUAL CIRCUIT (VC) NETWORK - 2



# VIRTUAL CIRCUIT NETWORK - 3



Cổng vào3	VC# vào	Cổng ra	VC# ra
1	12	3	22
2	63	1	18
3	7	2	17
1	97	3	87
...	...	...	...

Routers duy trì thông tin về trạng thái kết nối!

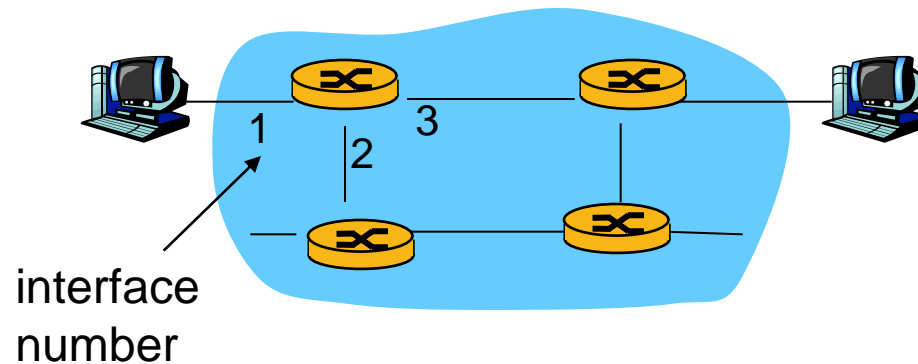
# DATAGRAM NETWORK - 1

- Không thiết lập kết nối trước khi truyền dữ liệu
  - Router không cần quản lý trạng thái kết nối
- Thông tin định tuyến: địa chỉ đích đến
  - Mỗi router duy trì một bảng định tuyến
- Dùng trong Internet

# DATAGRAM NETWORK - 2

200.245.60.45/24

210.245.10.5/24



Destination Network	Subnetmask	Out Interface	Nexthop
210.245.10.0	255.255.255.0	3	....
210.245.15.0	255.255.255.0	1	.....
210.245.15.192	255.255.255.192	2	.....
...	...	...	

# NỘI DUNG

- Giới thiệu
- Định tuyến – chuyển tiếp
- Giao thức IP
- Giao thức ICMP
- Giao thức NAT

# ĐỊNH TUYẾN - CHUYỂN TIẾP - 1

## ○ Định tuyến:

- Quyết định “lộ trình” mà gói tin di chuyển từ host nguồn đến host đích đến
- Sử dụng thông tin toàn cục

## ○ Chuyển tiếp:

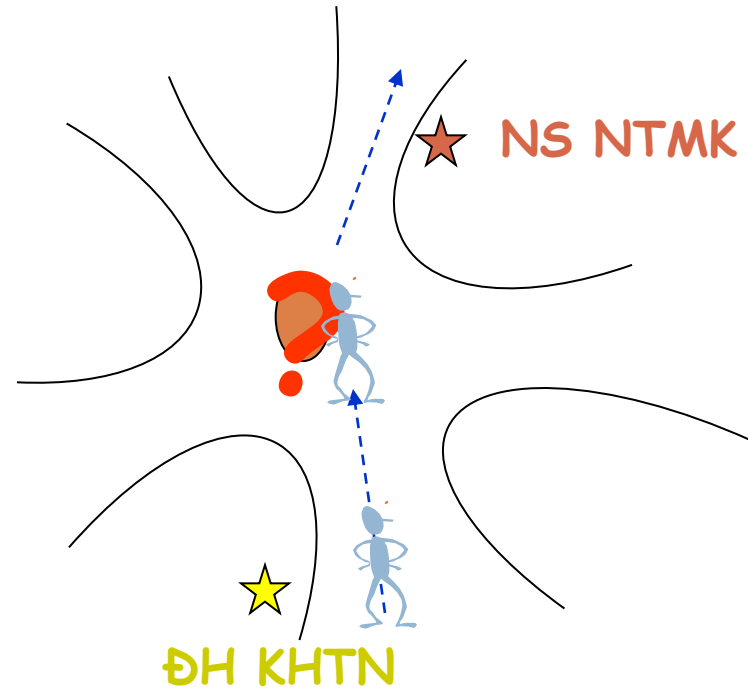
- Di chuyển gói tin từ cổng vào đến cổng ra
- Sử dụng thông tin cục bộ

# ĐỊNH TUYẾN - CHUYỂN TIẾP - 2

ĐH KHTN



NS NVCừ



Vạch ra lộ trình đi: NVCừ → NTMKhai

# ĐỊNH TUYẾN - 1

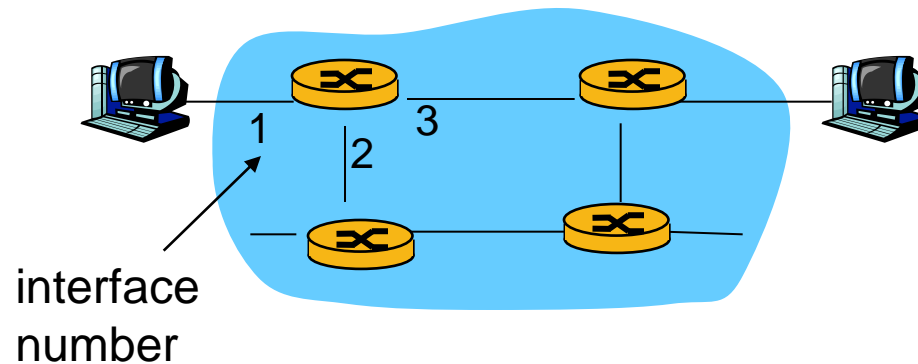
- Được thực hiện bởi các bộ định tuyến.
  - VD: router
- Dùng bảng định tuyến (routing/forwarding table)
  - destination/subnetmask
  - Out interface
  - next hop
  - chi phí
    - Hop count
    - Delay
    - Bandwidth
    - ...



# VÍ DỤ - ĐỊNH TUYẾN

200.245.60.45/24

210.245.10.5/24



Destination Network	Subnet mask	Nexthop	Out Interface
210.245.10.0	255.255.255.0	192.168.3.2	3
210.245.15.0	255.255.255.0	192.168.1.2	1
210.245.15.192	255.255.255.192	192.168.2.2	2
...	...		...

## ĐỊNH TUYẾN - 2

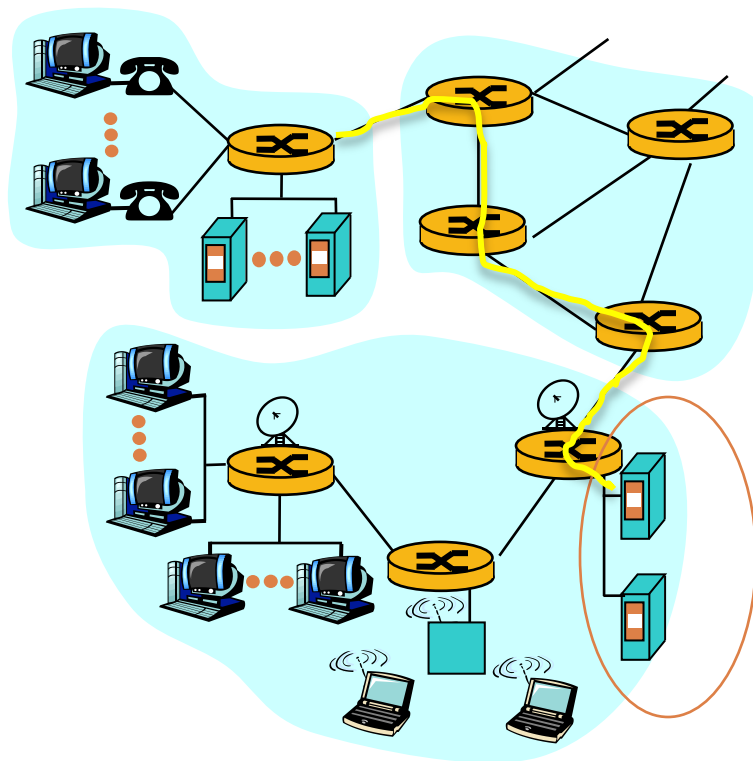
- Router định tuyến một gói tin như thế nào?
  - Dùng địa chỉ đích đến và bảng định tuyến
  - Thực hiện:
    - Tìm record thích hợp trong bảng định tuyến
      - Tính địa chỉ đường mạng giữa địa chỉ đích đến với subnetmask của từng record
      - So sánh destination network với địa chỉ đường mạng vừa tính
    - Gửi gói tin theo thông tin của record tìm được
- VD: R1 nhận gói tin có destination 210.245.10.5
  - 255.255.255.192
    - Net: 210.245.10.0 → không có record thoả
  - 255.255.255.0
    - Net: 210.245.10.0 → record số 1 thoả  
→ gói tin chuyển ra interface số 3 và nơi nhận gói tin tiếp theo là 192.168.3.2

# BẢNG ĐỊNH TUYẾN

- Xây dựng bảng định tuyến:
  - Tĩnh (static): con người tự thiết lập
  - Động (dynamic): học
    - Distance Vector:
      - Gửi theo định kỳ
      - Gửi toàn bộ bảng định tuyến
      - VD: RIP, IGRP, ...
    - Link State:
      - Gửi khi có thay đổi
      - Gửi tình trạng kết nối
      - VD: OSPF, ISIS, ...

# STATIC ROUTE

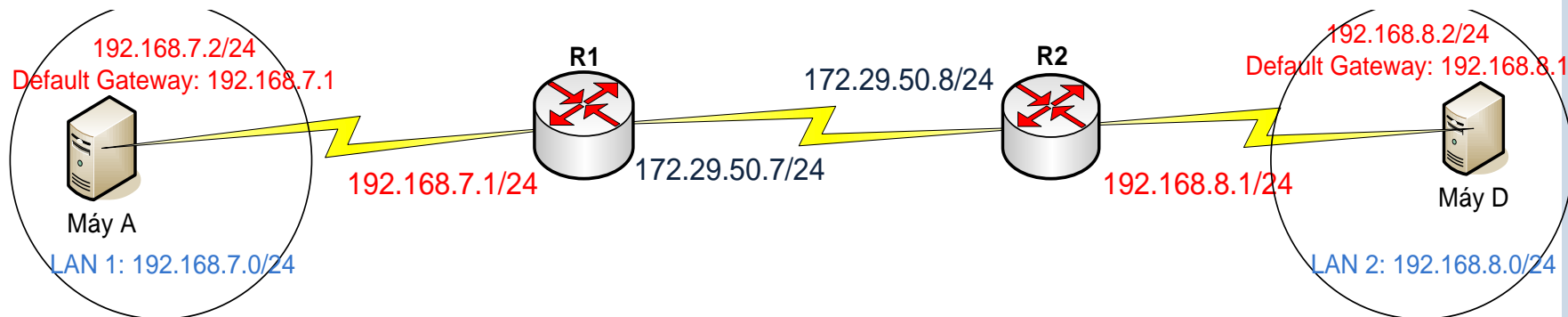
- Biết: Sơ đồ mạng
- Xây dựng:
  - Vẽ “đường đi” *tối ưu*
- Khi có thay đổi:
  - Tự cập nhật bằng tay



# DYNAMIC ROUTE

- Biết: không
- Xây dựng:
  - Sử dụng các giao thức định tuyến
    - Thông qua các gói tin “thu thập” thông tin
    - Thành phần:
      - Gửi và nhận thông tin từ các router khác
      - Tính đường đi tối ưu
      - Phản ứng khi có thay đổi
- Khi thay đổi
  - Cập nhật tự động

# STATIC ROUTE - VÍ DỤ - 1



**Yêu cầu:** cấu hình thông tin định tuyến cho R1 và R2 để các máy trong LAN1 có thể liên lạc với các máy trong LAN2

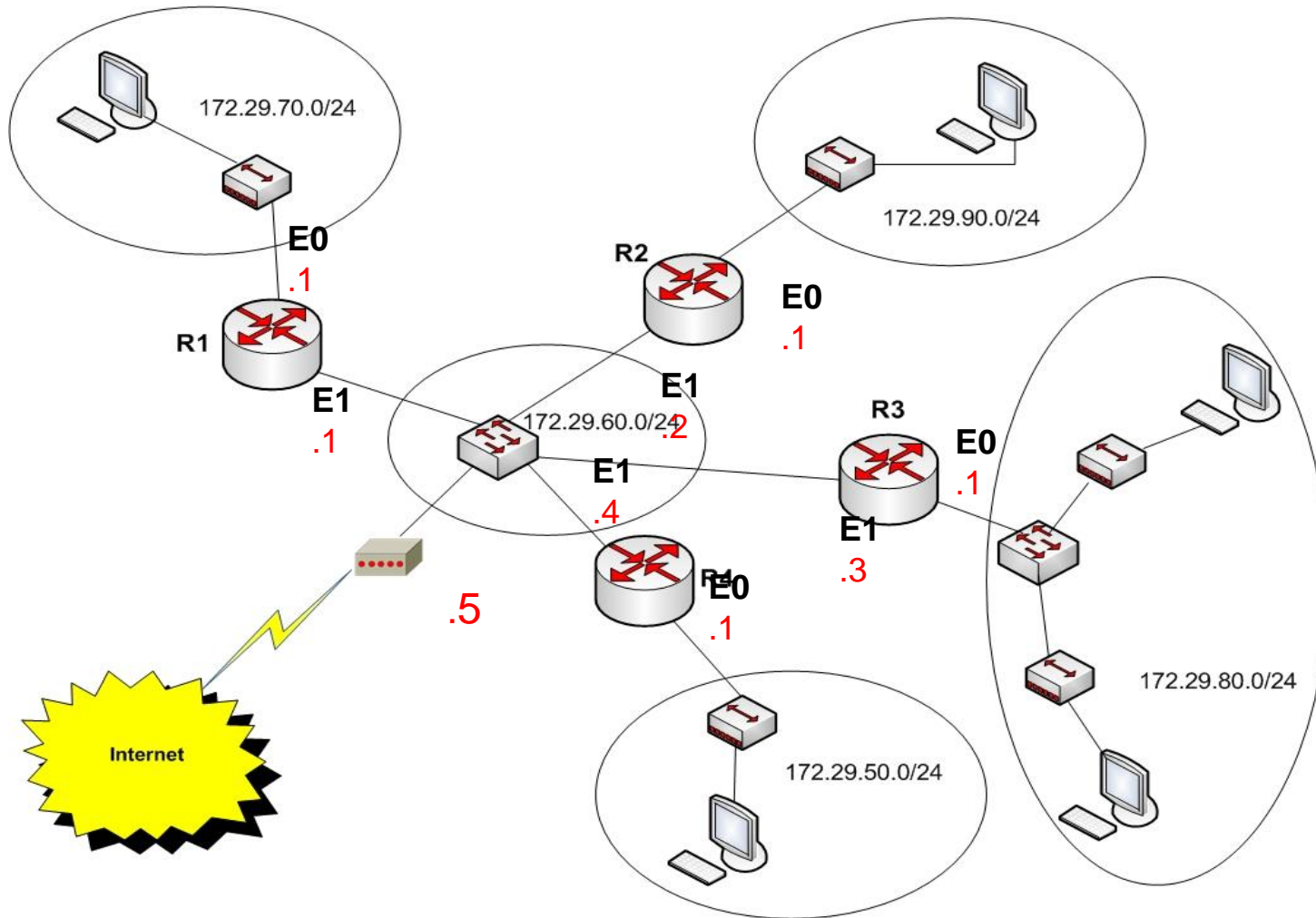
**Tại router R1:**

Destination network	Out interface	Next hop
192.168.8.0/24	172.29.50.7	172.29.50.8

**Tại router R2:**

Destination network	Out interface	Next hop
192.168.7.0/24	172.29.50.8	172.29.50.7

# STATIC ROUTE – VÍ DỤ 2



**Yêu cầu:** cấu hình thông tin định tuyến cho các router để tất cả các máy trong có thể liên lạc với nhau và có thể truy cập Internet

# STATIC ROUTE – VÍ DỤ 2

**Tại router R1:**

Destination network	Out interface	Next hop
172.29.90.0/24	E1	172.29.60.2
172.29.80.0/24	E1	172.29.60.3
172.29.50.0/24	E1	172.29.60.4
0.0.0.0	E1	172.29.60.5

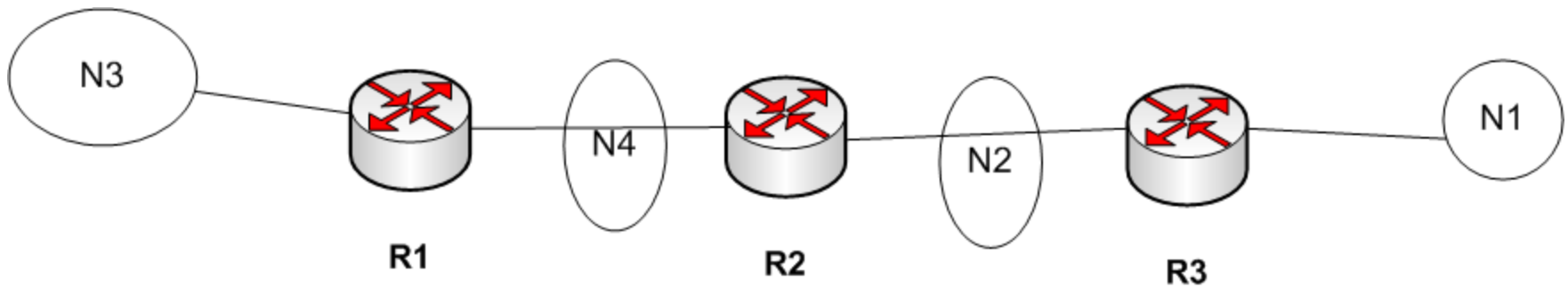
**Tại router R2:**

Destination network	Out interface	Next hop
172.29.70.0/24	E1	172.29.60.1
172.29.80.0/24	E1	172.29.60.3
172.29.50.0/24	E1	172.29.60.4
0.0.0.0	E1	172.29.60.5



# DYNAMIC ROUTE – VÍ DỤ

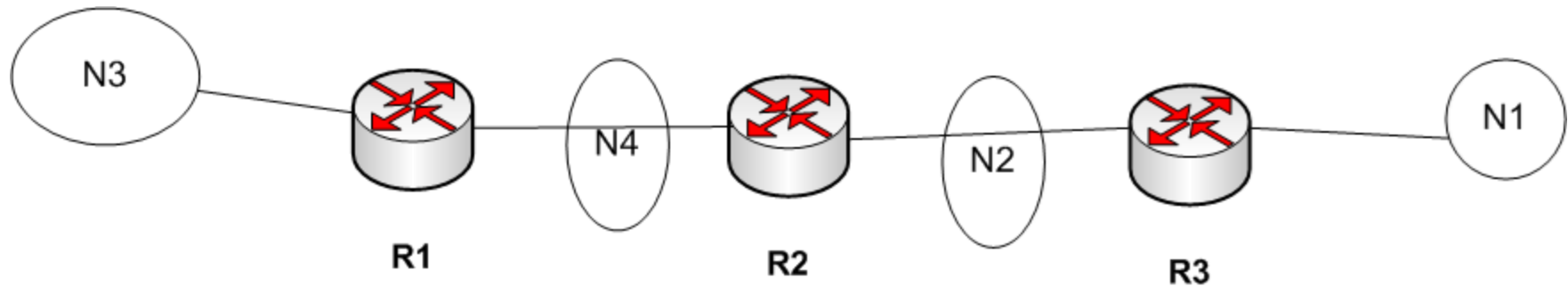
R2	
N2, N4	0 hop



R1	
N3, N4	0 hop

R3	
N1, N2	0 hop

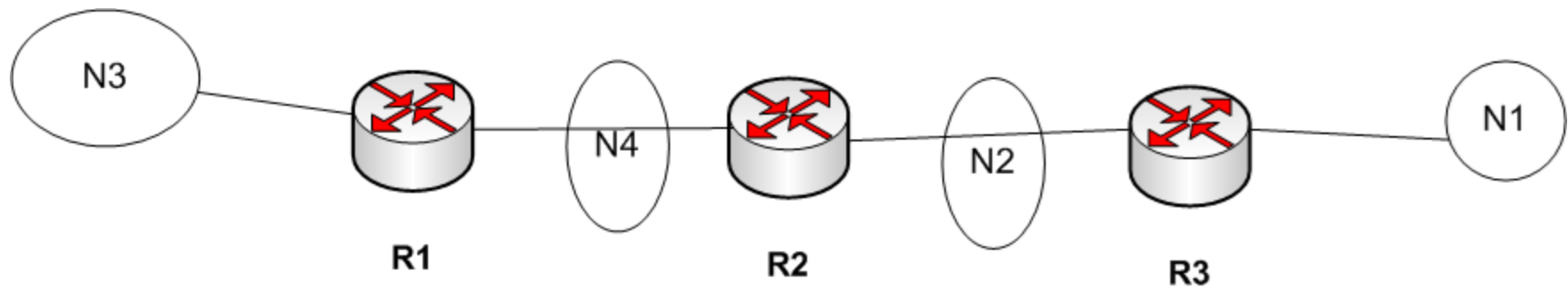
# DYNAMIC ROUTE – VÍ DỤ



R1: N3, **N4** – 0 hop

R2	
N2, <b>N4</b>	0 hop
N3	1 hop

# DYNAMIC ROUTE – VÍ DỤ

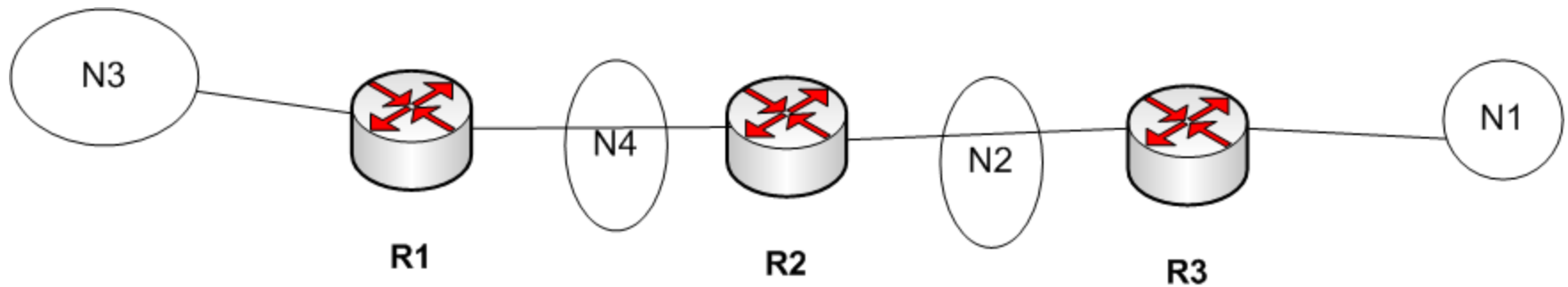


R2: N2, N4 – 0 hop  
**N3** – 1 hop

R3	
N1, N2	0 hop
N4	1 hop
N3	2 hops

# DYNAMIC ROUTE – VÍ DỤ

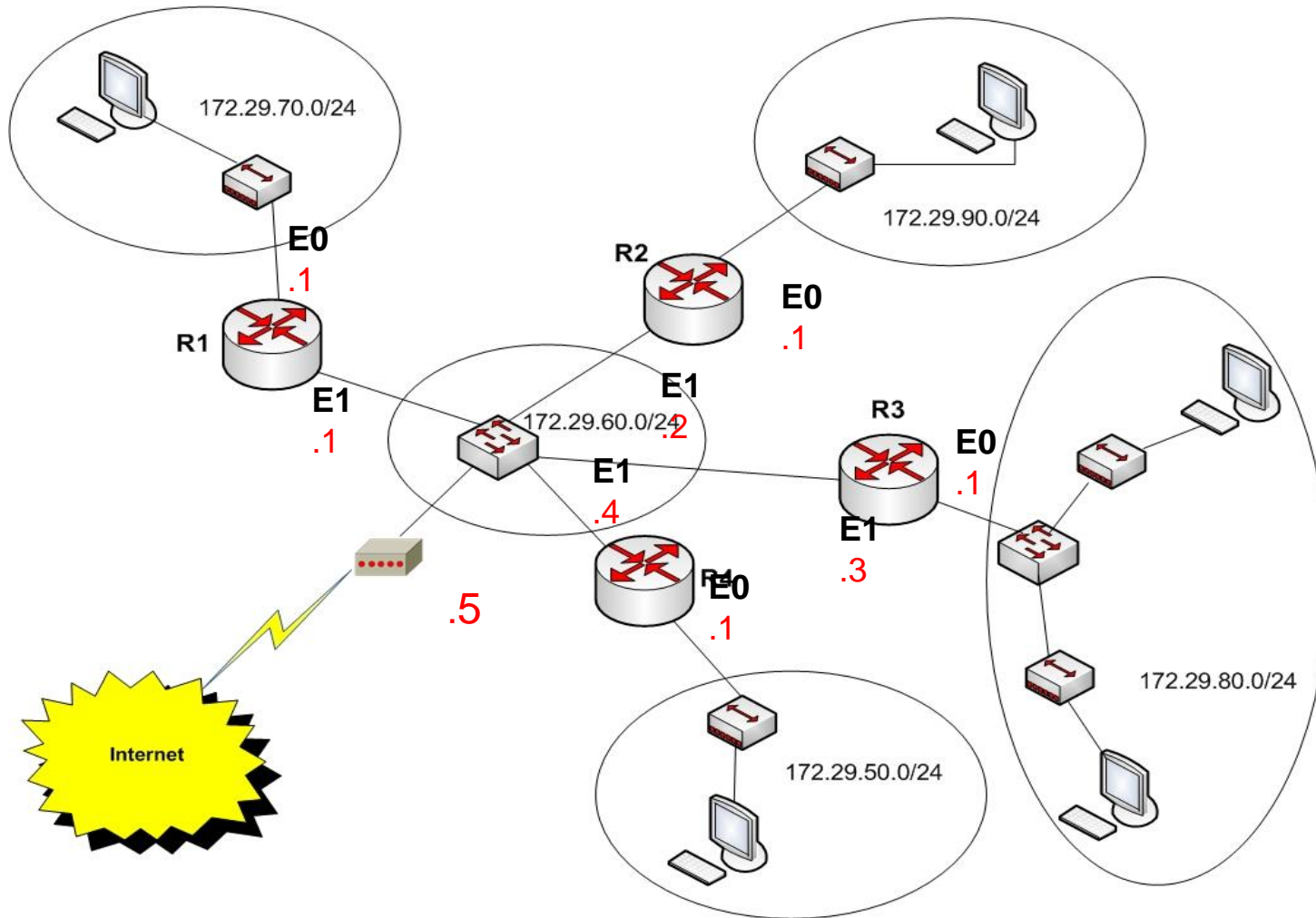
R2	
N2, N4	0 hop
N3, N1	1 hop



R1	
N3, N4	0 hop
N2	1 hop
N1	2 hops

R3	
N1, N2	0 hop
N4	1 hop
N3	2 hops

# DYNAMIC ROUTE – VÍ DỤ



**Yêu cầu:** cấu hình thông tin định tuyến cho các router để tất cả các máy trong có thể liên lạc với nhau và có thể truy cập Internet

# DYNAMIC ROUTE – VÍ DỤ

```
R1#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.29.0.0/24 is subnetted, 5 subnets  
O      172.29.50.0 [110/2] via 172.29.60.4, 00:00:15, FastEthernet0/0  
C      172.29.60.0 is directly connected, FastEthernet0/0  
C      172.29.70.0 is directly connected, FastEthernet0/1  
O      172.29.80.0 [110/2] via 172.29.60.3, 00:00:15, FastEthernet0/0  
O      172.29.90.0 [110/2] via 172.29.60.2, 00:00:46, FastEthernet0/0
```

# NỘI DUNG

- Giới thiệu
- Định tuyến – chuyển tiếp
- Giao thức IP
- Giao thức ICMP
- Giao thức NAT

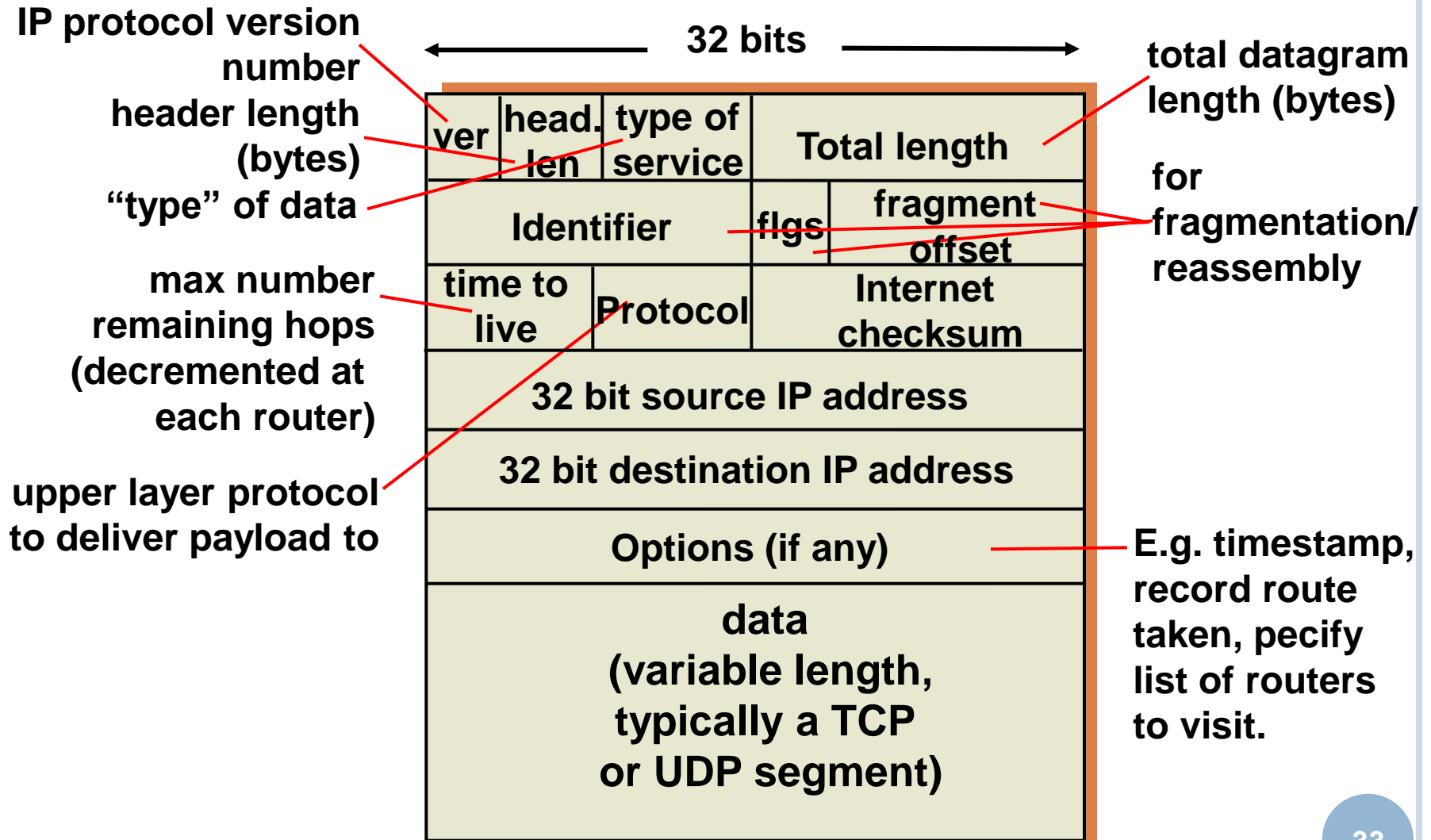
# ROUTED PROTOCOL - 1

- Giao thức được định tuyến (routed protocol):
  - qui định cách thức đóng gói dữ liệu truyền trên đường truyền
  - VD: IP (IPv4, IPv6), IPSec,...

Routing protocol	Routed protocol
Tạo bảng định tuyến	Đóng gói gói tin tại tầng mạng



# ROUTED PROTOCOL - 2



## ROUTED PROTOCOL - 3

- Version (4)
  - version của IP
- Header Length (4):
  - Chiều dài IP header (byte)
- Type of service (8)
  - Chứa định thông tin ưu tiên
  - Ít sử dụng
- Total length (16)
  - Tổng chiều dài của datagram (tính cả header) (byte)
- Identifier (16):
  - Khi một gói tin IP bị chia nhỏ ra thành nhiều đoạn, thì mỗi đoạn được gán cùng số ID
  - Dừng khi tổng hợp

# ROUTED PROTOCOL - 4

## ◦ Flag (3)



- DF

- Don't fragment, không chia nhỏ

- MF

- More fragment, còn gói tin nhỏ tiếp
- Khi 1 gói tin bị chia nhỏ, tất cả các gói nhỏ (trừ gói tin cuối cùng), bit này được bật lên

## ◦ Fragment offset (13)

- Vị trí gói nhỏ trong gói tin ban đầu

## ◦ Time to live – TTL (8)

- Thời gian sống của gói tin (hop count)
- Giảm mỗi khi gói tin đến 1 router mới
  - Khi hop count = 0 thì gói tin bị loại bỏ

# ROUTED PROTOCOL - 5

- Protocol (8)
  - Chỉ ra nghi thức nào ở tầng transport mà gói tin đang sử dụng
  - VD: TCP = 6, UDP = 17
- Internet (Header) checksum (16)
  - Kiểm tra tính đúng đắn nội dung của IP header
  - Không theo cách kiểm tra tuần tự
- Source and destination addr (32)
  - Địa chỉ IP của bên gửi và bên nhận
- Options (32)
  - Có thể dài đến 40 bytes
  - Dùng cho các tính năng mở rộng của IP
  - Vd: source routing, security, record route, ...
- Data:
  - Dữ liệu ở tầng transport gói xuống

# NỘI DUNG

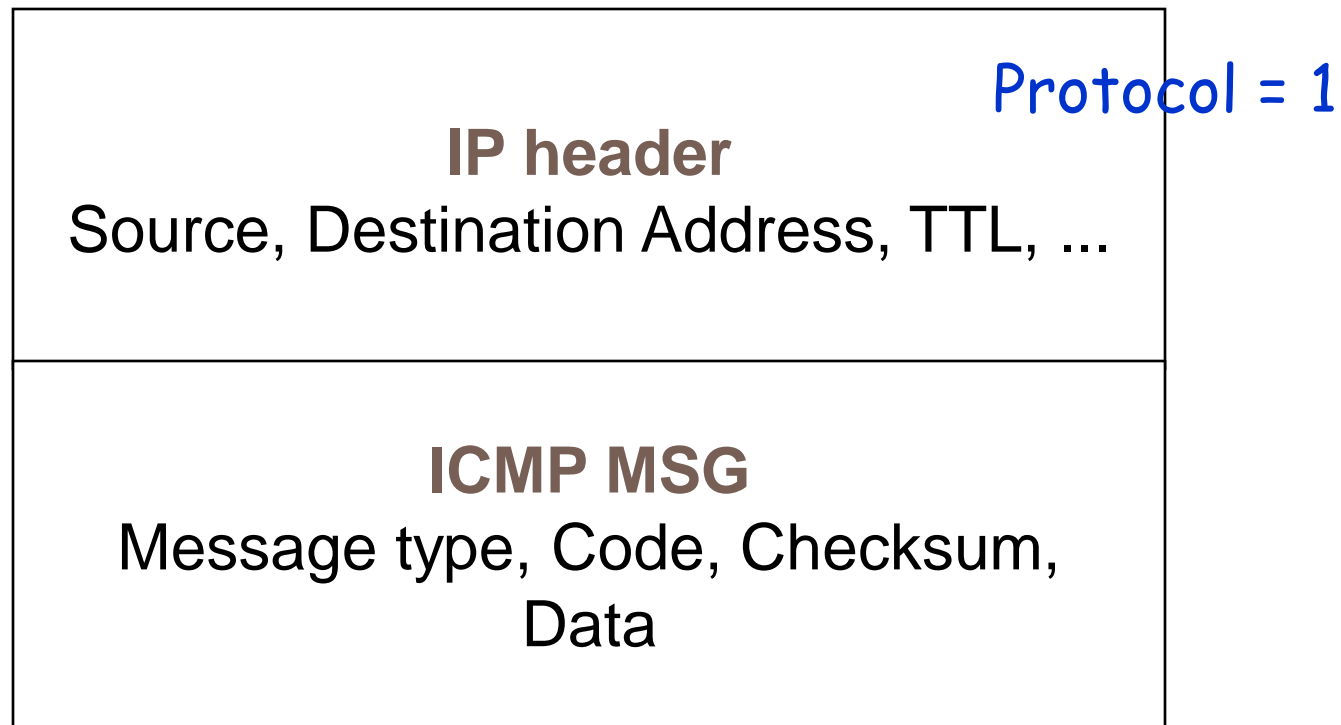
- Giới thiệu
- Định tuyến – chuyển tiếp
- Giao thức IP
- **Giao thức ICMP**
- NAT

# GIAO THỨC ICMP

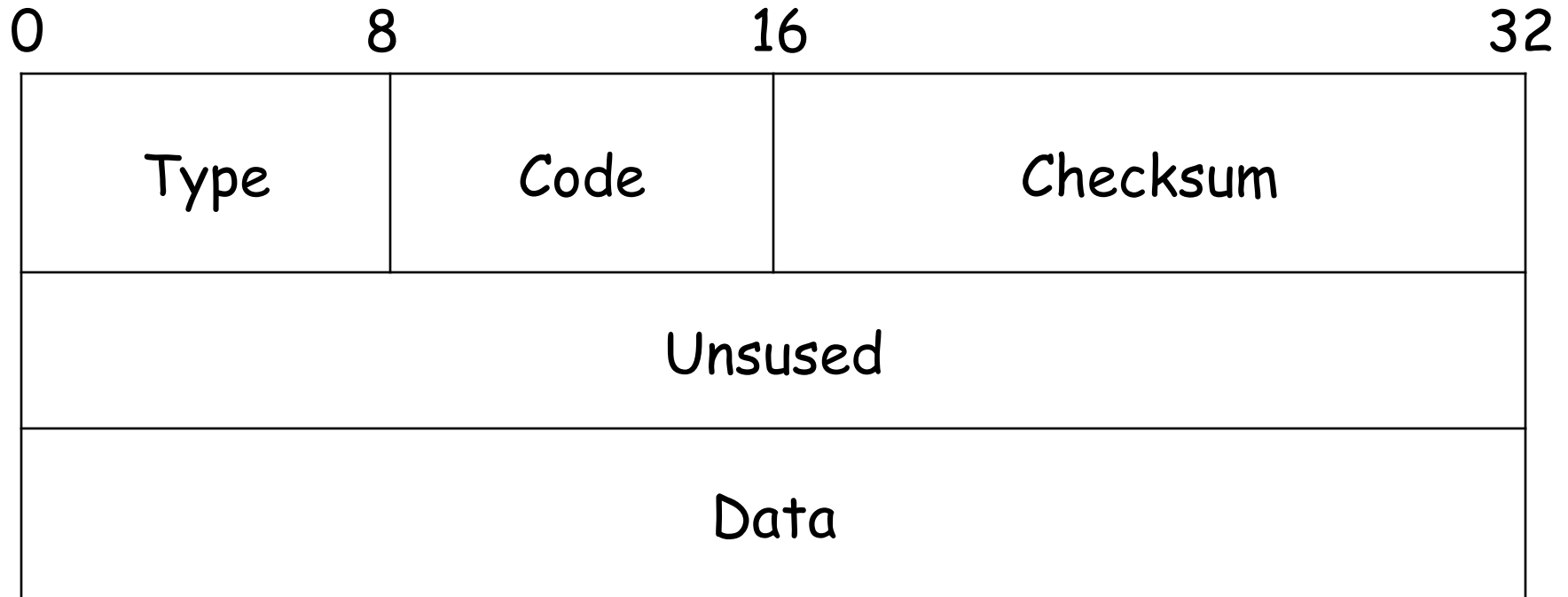
- ICMP (Internet Control Message Protocol)
- Được sử dụng bởi các host và router để trao đổi thông tin ở tầng mạng
  - Báo lỗi:
    - Mạng, host, protocol, port ... không vươn đến được
  - Báo mạng bị tắc nghẽn
  - Báo timeout
  - Echo request/reply (ping)

# GÓI TIN ICMP

- Thông điệp ICMP được đóng gói trong gói tin IP



# CẤU TRÚC THÔNG điệp ICMP - 1





## CẤU TRÚC THÔNG điệp ICMP - 2

ICMP Type	Code	Description
0	0	echo reply
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

# CẤU TRÚC THÔNG điệp ICMP - 3

## ○ Không đến được đích:

- Nguyên nhân: liên kết mạng bị đứt, đích đến không tìm thấy, ...
- Type = 3
- Code:
  - 0: unreachable network
  - 1: unreachable host
  - 2: unreachable protocol
  - 3: unreachable port
  - 4: không được phép fragment
  - 5: source route bị sai

# CẤU TRÚC THÔNG điệp ICMP - 4

- Quá hạn:
  - Nguyên nhân:
    - TTL = 0 trước khi đến đích
    - Quá hạn thời gian tái lắp ghép các fragment
  - Type = 11
  - Code:
    - 0: TTL
    - 1: hết thời gian tái lắp ghép

# GIAO THỨC ICMP

- Các trường hợp GỬI ICMP msg:
  - Datagram không đạt đến đích
  - Time out
  - Error xuất hiện trong header
  - Router/host bị tắt nghẽn
- Các trường hợp KHÔNG gửi ICMP msg:
  - Bản thân ICMP msg có lỗi
  - Broadcast, multicast (gói DL định tuyến)
  - Những fragment khác với fragment đầu tiên

# NỘI DUNG

- Giới thiệu
- Định tuyến – chuyển tiếp
- Giao thức IP
- Giao thức ICMP
- NAT

# NHẮC LẠI

## ○ Địa chỉ IP:

- Kích thước: 32 bits → không gian:  $2^{32}$  địa chỉ
  - 0.x.x.x/8, 127.0.0.0/8, lớp D, lớp E; không dùng
  - Số lượng node trên Internet “khổng lồ”
- Giải quyết:
  - dùng địa chỉ private trong mạng LAN
  - Dùng địa chỉ public khi giao tiếp bên ngoài Internet

## ○ Gửi dữ liệu giữa 2 host

- Địa chỉ host gửi
- Địa chỉ host nhận

# ĐẶT VẤN ĐỀ

## NAT

Private IP

Public IP

Src: 192.168.1.3  
Dest: 210.64.72.14

Src: 10.207.37.19  
Dest: 210.64.72.14

192.168.1.0/24

Src: 210.64.72.14  
Dest: 192.168.1.3

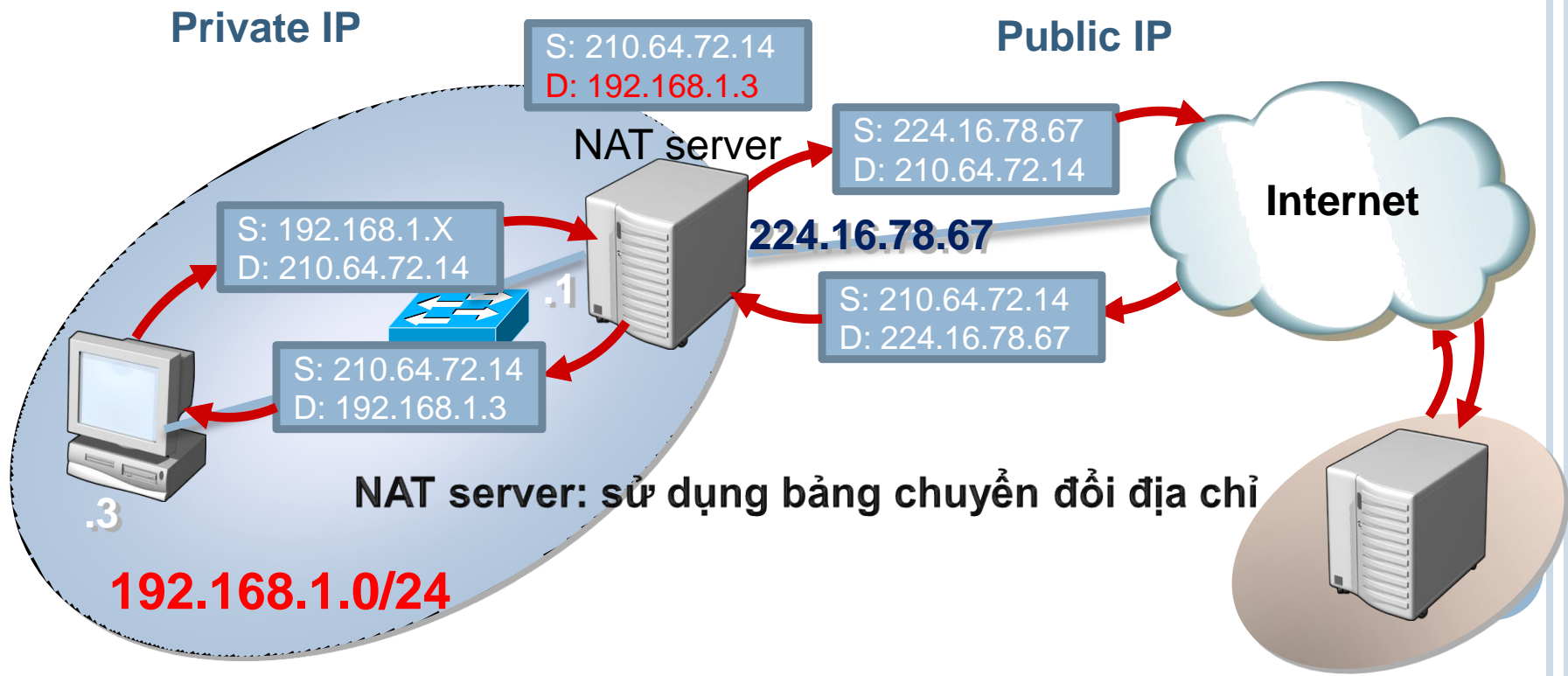
Src: 210.64.72.14  
Dest: 10.207.37.19

Src: 192.168.1.3  
Dest: 192.168.1.4

Internet

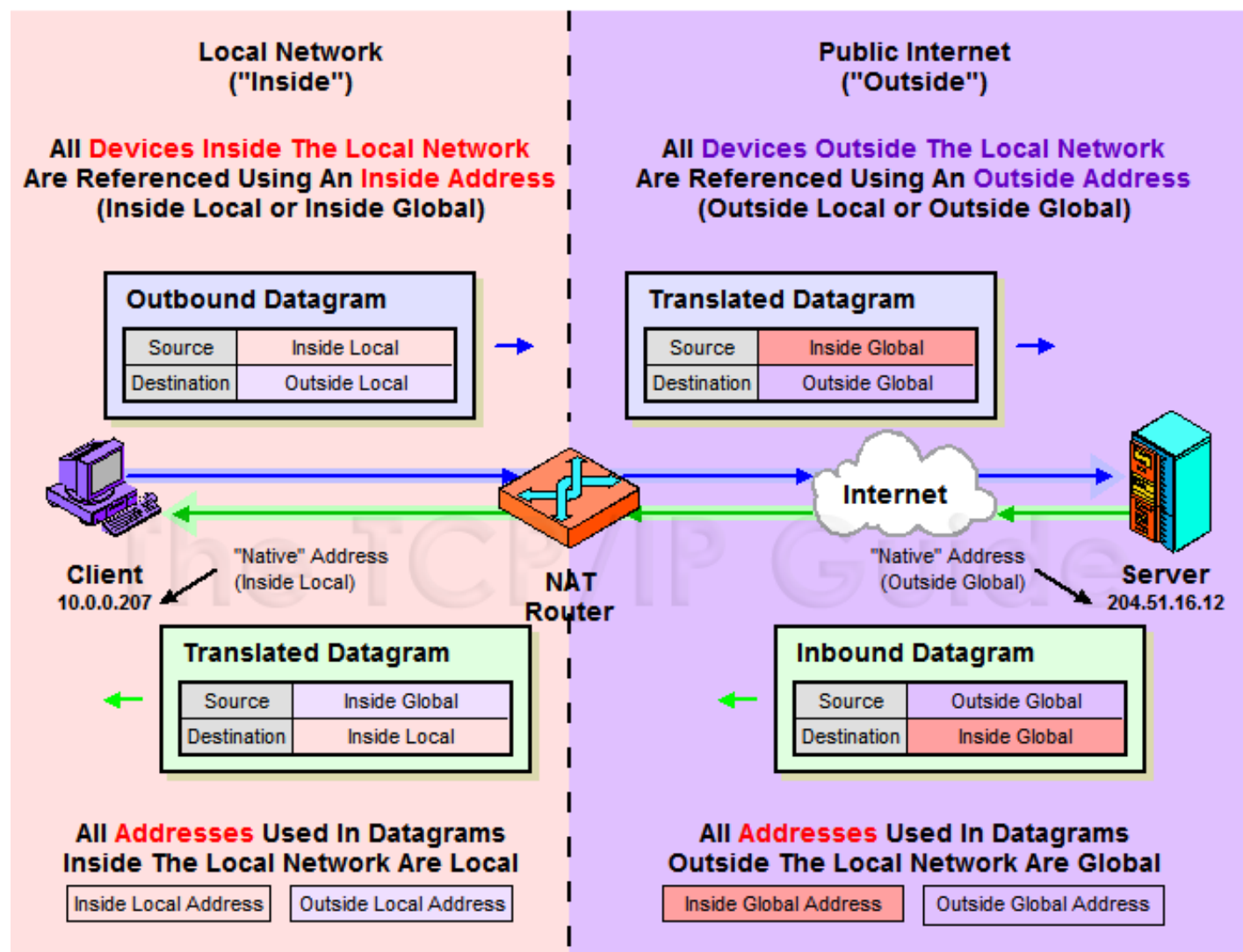
# NAT – GIỚI THIỆU

- NAT = Network Address Translation
- RFC 1631, 1918, 2663
- Chức năng: “thay đổi” địa chỉ
  - Incoming: thay đổi thông tin đích đến
  - Outgoing: thay đổi thông tin nguồn





# NAT – THUẬT NGỮ



# NAT – BẢNG CHUYỂN ĐỔI ĐỊA CHỈ

- Dùng chuyển đổi global <-> local
  - Thông tin cục bộ bên trong (Inside local)
  - Thông tin toàn cục bên trong (Inside global)
- Thông tin trong bảng chuyển đổi
  - Static
  - dynamic

# NAT – PHÂN LOẠI

## ○ Static

- Cố định: 1 local IP  $\Leftrightarrow$  1 global IP

## ○ Dynamic

- n local IP  $\Leftrightarrow$  m global IP
- NAT: chọn 1 global IP còn rảnh để NAT

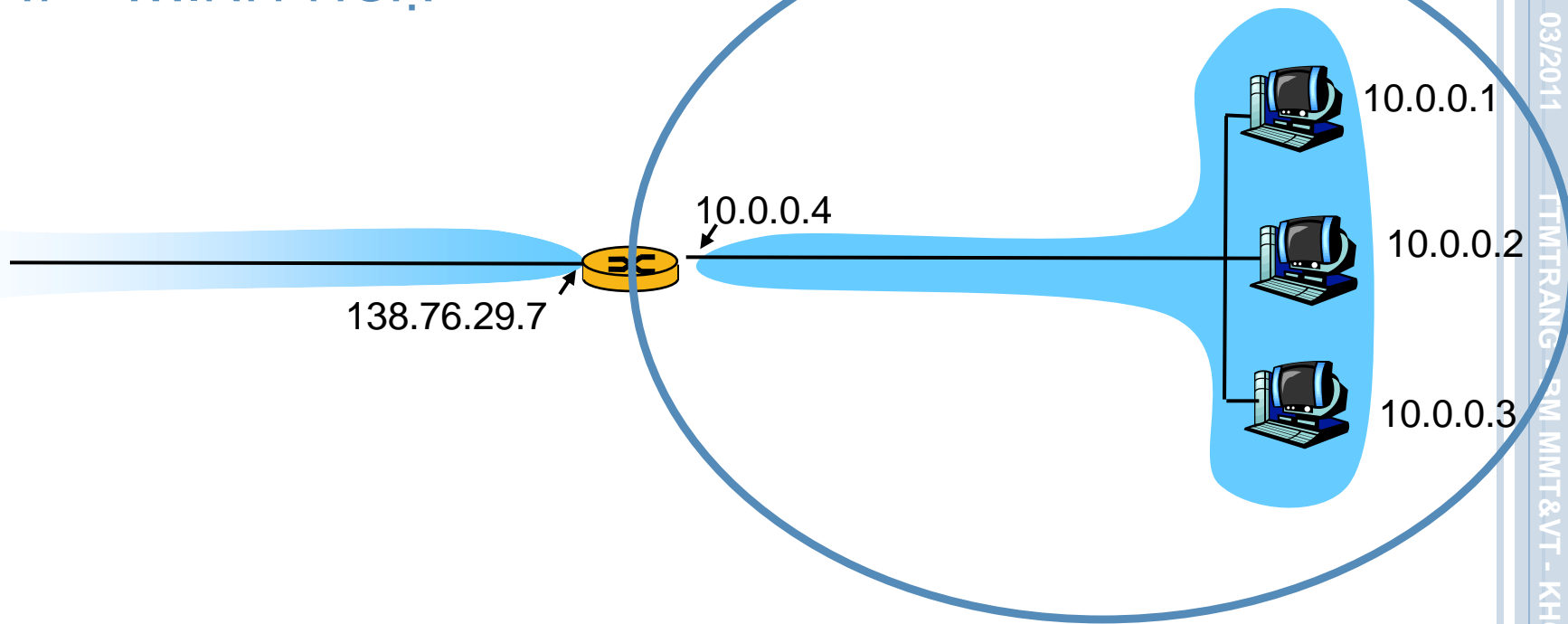
## ○ Overloading

- n local IP  $\Leftrightarrow$  1 global IP
- NAT: <local IP, local port>  $\Leftrightarrow$  <global IP, global port>

## ○ Overlapping

- Cố định: <local IP, *port*>  $\Leftrightarrow$  <global IP, *port*>

# NAT - MINH HOẠ



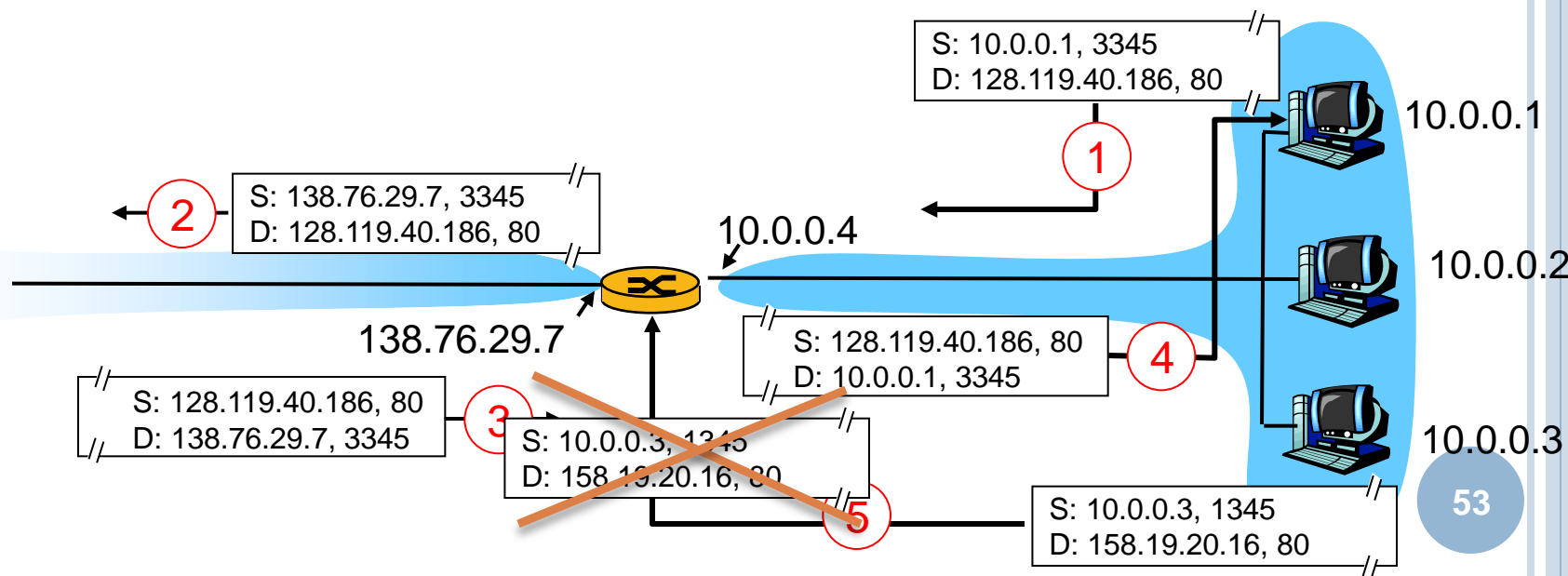
## ○ Thứ tự gửi các gói tin như sau:

- Máy 10.0.0.1 gửi 1 gói tin đến 128.119.40.186, 80 từ ứng dụng 3345
- Ứng dụng <128.119.40.186, 80> gửi lại gói tin phản hồi
- Máy 10.0.0.3 gửi 1 gói tin đến 158.19.20.16, 80 từ ứng dụng 1234
- Ứng dụng <120.11.40.18, 3345> gửi gói tin truy cập dịch vụ web tại máy 10.0.0.1

# STATIC NAT

- Cấu hình **cố định**: 1 local IP  $\Leftrightarrow$  1 global IP
  - Số máy kết nối ra ngoài bằng với số địa chỉ IP global
  - Bên ngoài (outside) có thể chủ động tạo kết nối với bên trong (inside)

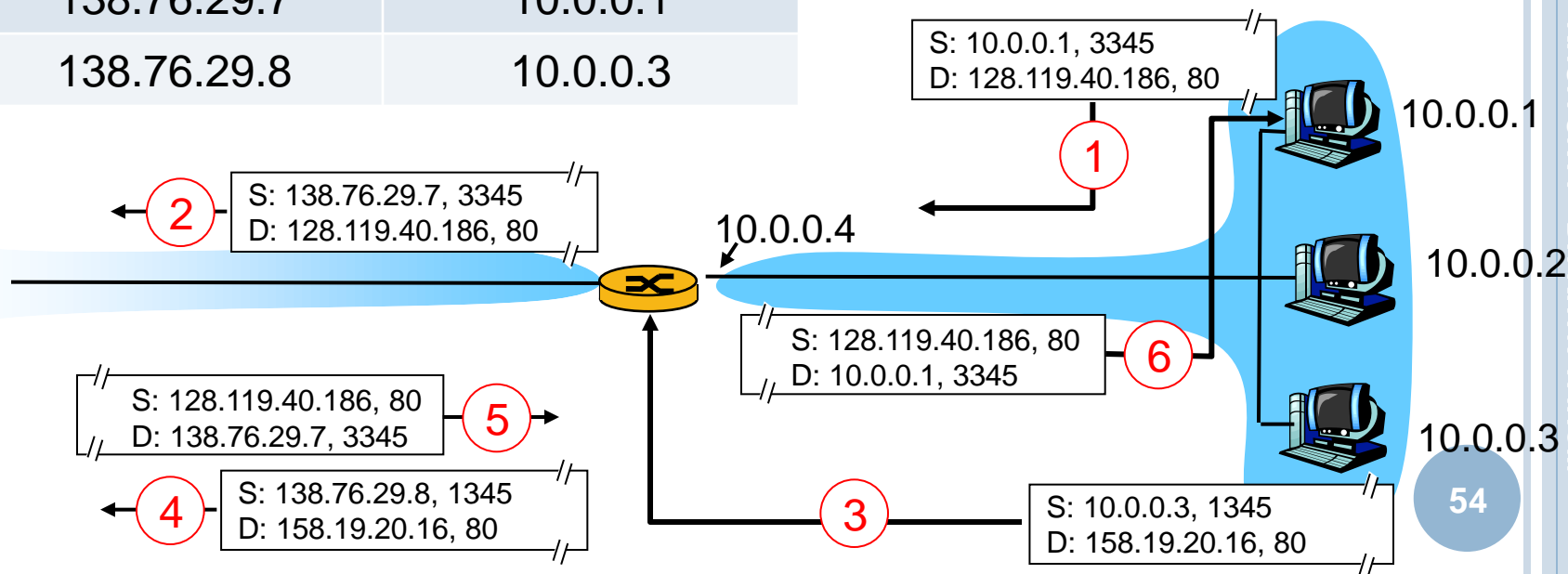
Global	Local
138.76.29.7	10.0.0.1



# DYNAMIC NAT

- Cấu hình:  $n$  local IP  $\Leftrightarrow$   $m$  global IP
  - Có  $m$  kết nối đồng thời
  - Bên ngoài (outside) **không** thể chủ động tạo kết nối với bên trong (inside)
- Ví dụ:  $10.0.0.0/24 \Rightarrow 138.76.29.7$  và  $138.76.29.8$

Global	Local
138.76.29.7	10.0.0.1
138.76.29.8	10.0.0.3

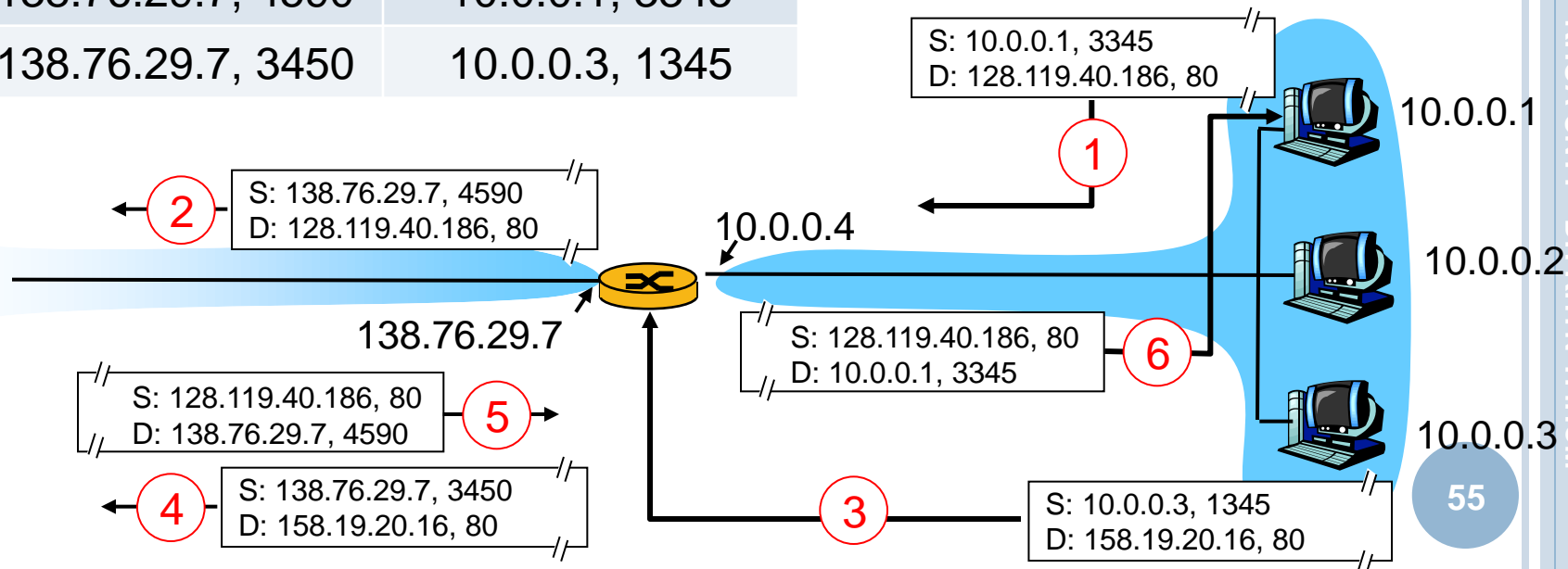


# OVERLOADING NAT

## ○ Cấu hình: n local IP $\Leftrightarrow$ 1 global IP

- NAT: <local IP, local port>  $\Leftrightarrow$  <global IP, global port>
- Có n kết nối đồng thời
- Bên ngoài (outside) **không** thể chủ động tạo kết nối với bên trong (inside)

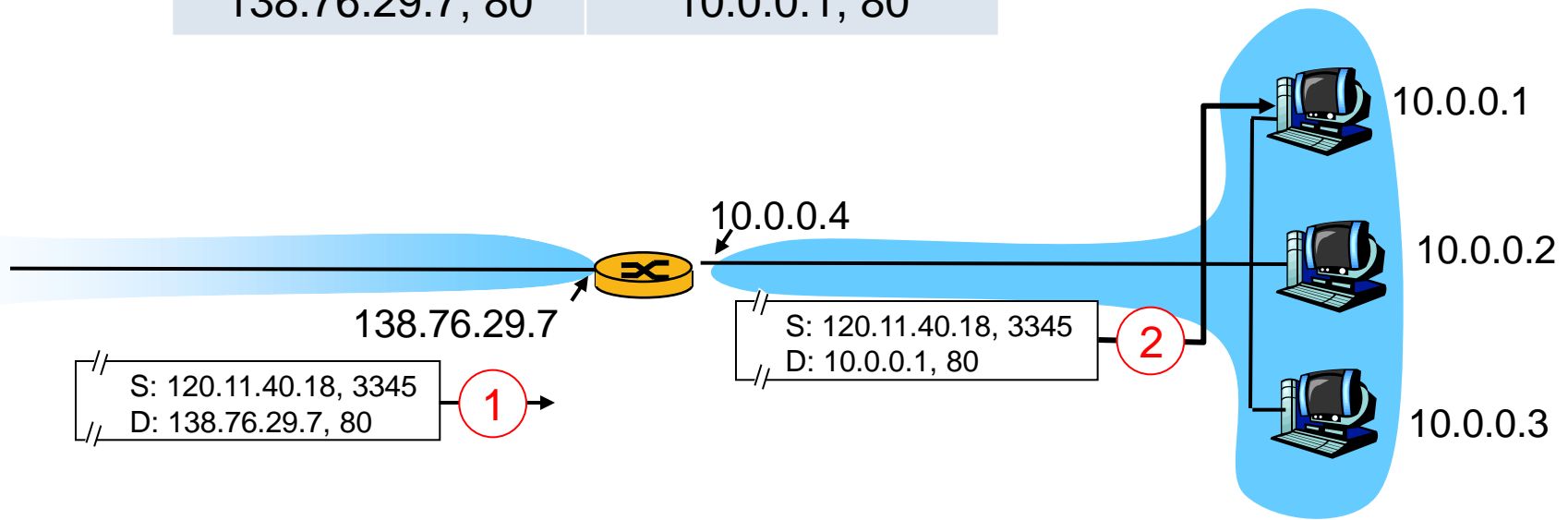
Global	Local
138.76.29.7, 4590	10.0.0.1, 3345
138.76.29.7, 3450	10.0.0.3, 1345



# OVERLAPING NAT

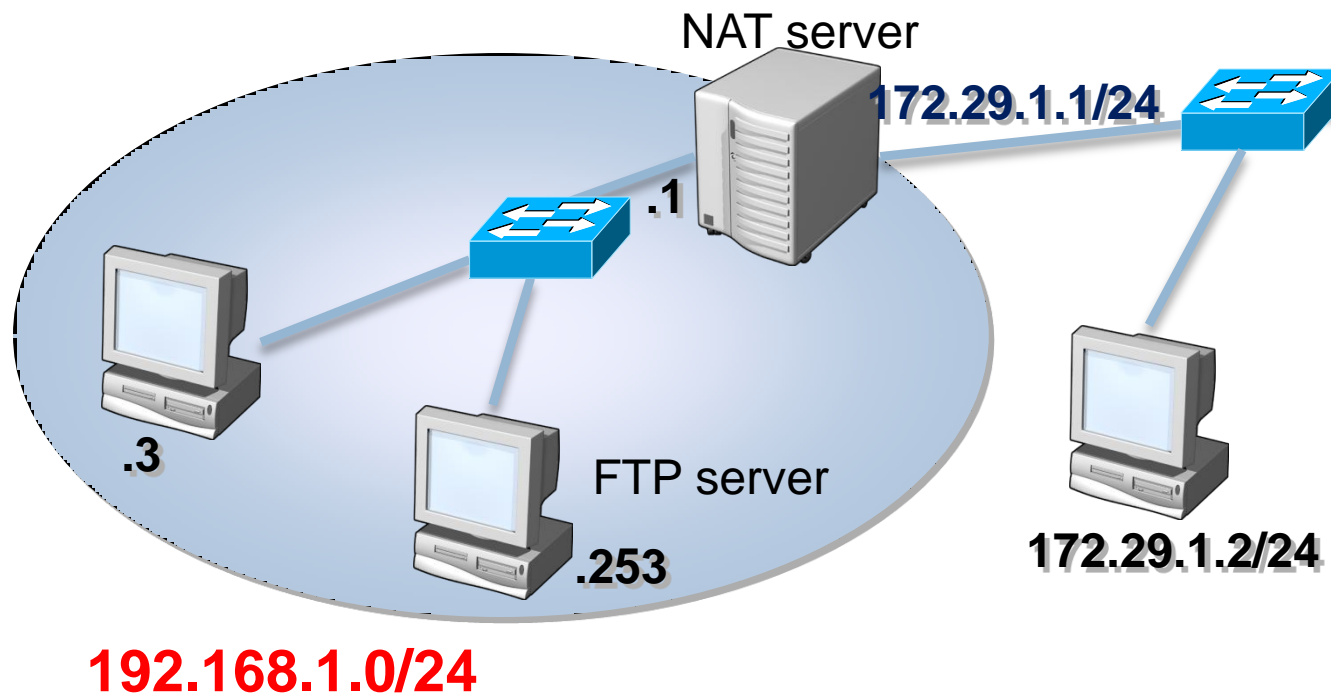
- Cấu hình **cố định**:  $\langle \text{local IP, port} \rangle \Leftrightarrow \langle \text{global IP, port} \rangle$ 
  - Bên ngoài (outside) có thể chủ động tạo kết nối với bên trong (inside)
  - Dùng để publish một dịch vụ ra *ngoài*

Global	Local
138.76.29.7, 80	10.0.0.1, 80





# NAT – MÔ TẢ BÀI TOÁN



## Yêu cầu:

- Các máy tính trong LAN: 192.168.1.0/24 có thể truy cập ra ngoài bằng IP: 172.29.1.1
- Bên ngoài có thể truy cập dịch vụ FTP trên máy 192.168.3.253

# NAT – CẤU HÌNH TRÊN WINS 2K3

- Chọn card public và private
  - Private: 192.168.1.1
  - Public: 172.29.1.1
- Chọn dịch vụ để publish (nếu có): Web
  - Local IP: 192.168.1.253
  - Incoming port: 80
  - Outcoming port: 80

# TÀI LIỆU THAM KHẢO

- Slide của J.F Kurose and K.W. Ross về Computer Networking: A Top Down Approach