



VIỆN ĐIỆN TỬ - VIỄN THÔNG

School of Electronics and Telecommunications

CHƯƠNG 3

NETWORK LAYER

TS. TRẦN QUANG VINH

Chức năng lớp Network

- IP addressing
- Datagram Format
- Routing
- Forwarding
- Provide error detection and diagnostic capability

Internet Protocol

- **Giao thức IP**

- Chuẩn hóa bởi IETF, RFC 791 (9/1981)
- Chuẩn hóa bởi DoD, MIL-STD-1777

- **Phương thức hoạt động**

- Connectionless:
 - Giao thức IP không chuyển các thông tin điều khiển trước khi truyền dữ liệu
- Unreliable
 - Giao thức IP không có khả năng phát hiện và khắc phục lỗi
 - Không quan tâm đến việc dữ liệu có đến đích một cách chính xác hay không
- Best effort delivery
 - Truyền các Datagram càng nhanh càng tốt

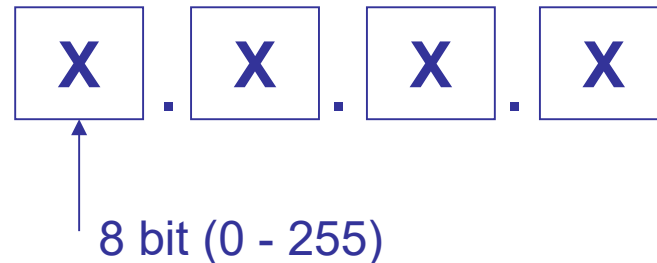
IP Addressing

▪ Hosts and Routers

- interface trên host và router đều có thể gửi và nhận IP datagram, nên mỗi giao diện phải có một IP address → IP Address có tính duy nhất!

▪ IP Address

- IPv4: 32 bit, IPv6: 128 bit
- Yêu cầu: phải có cấu trúc, cho phép định tuyến → địa chỉ IP gồm 2 phần thông tin:
 - Network address: địa chỉ mạng
 - Host address: địa chỉ máy trạm
- Biểu diễn:

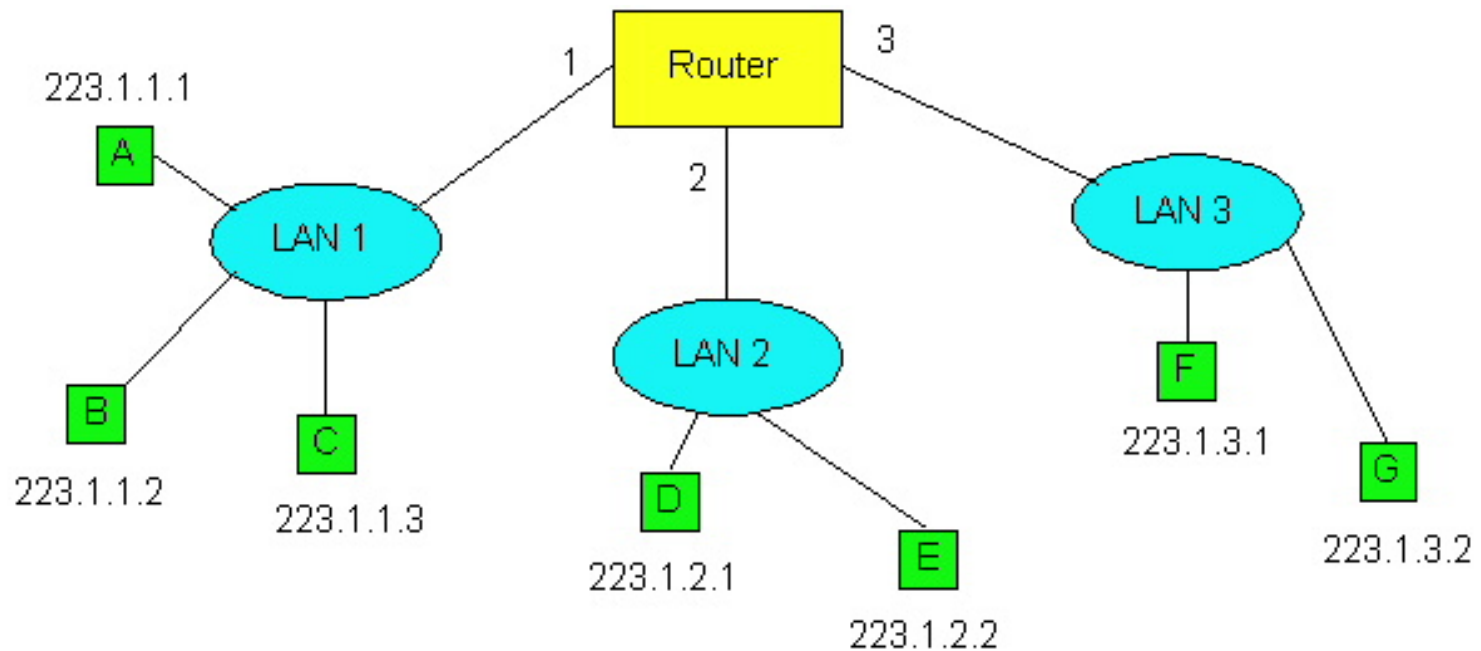


Binary:	11000000	10101000	00000001	00000001
Decimal:	192	168	1	1
	1st octet	2nd octet	3rd octet	4th octet

IP Addressing

■ Networks

Router Interface	IP Address
1	223.1.1.4
2	223.1.2.9
3	223.1.3.27



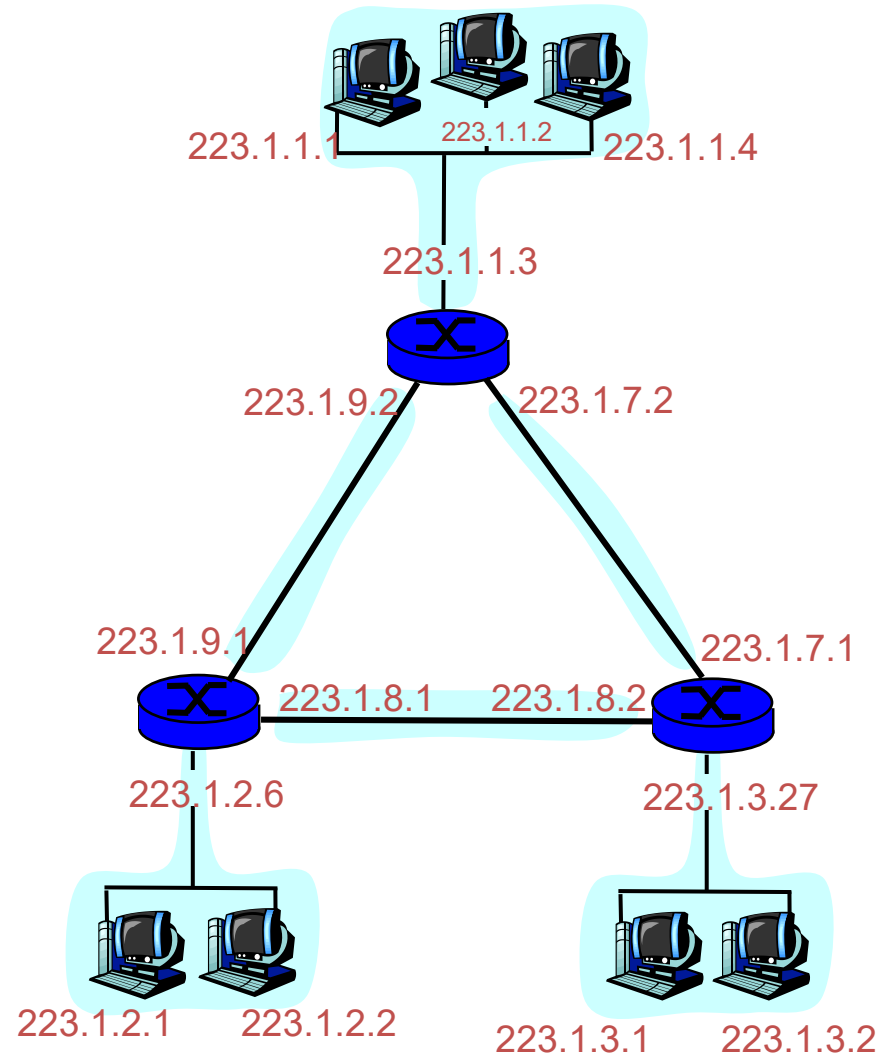
IP Addressing

■ Nguyên tắc đánh địa chỉ:

- Mỗi mạng LAN có địa chỉ mạng riêng biệt và được ngăn cách bởi router
- Các máy trạm (kể cả router) nằm trong một LAN có chung địa chỉ mạng, còn địa chỉ máy trạm khác nhau

■ Cách xác định Network

- Ngắt (detach) mỗi giao diện của router ra khỏi router và mỗi giao diện host ra khỏi host (ngắt các link giữa host và router)
- Mỗi isolated networks là một network



IP Addressing

IP Address Classing



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	$2^7=128$	2^{24}
Class B	$2^{14}=16384$	$2^{16}=65536$
Class C	2^{21}	$2^8=256$

	Range for first byte
Class A	0 - 127
Class B	128 - 191
Class C	192 - 223
Class D	224 - 239
Class E	240 - 255

IP Address Classifying

▪ Public IP Address

- IP thực và duy nhất, được quản lý bởi IANA

▪ Private IP Address

- sử dụng cho những host trong các mạng LAN

Class	Private IP Addresses (RFC 1918)	Default Subnet Mask	Number of Networks	Hosts per Network	Total Hosts
A	10.0.0.0 to 10.255.255.255	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0 to 172.31.255.255	255.255.0.0	16	65,534	1,048,544
C	192.168.0.0 to 192.168.255.255	255.255.255.0	256	254	65,024

▪ Loopback Address

Loopback address	127.0.0.1 / 127.1.*
Multicast address (RFC5771)	224.0.0.0~239.255.255.255

IP Address Classifying

▪ Multicast Address

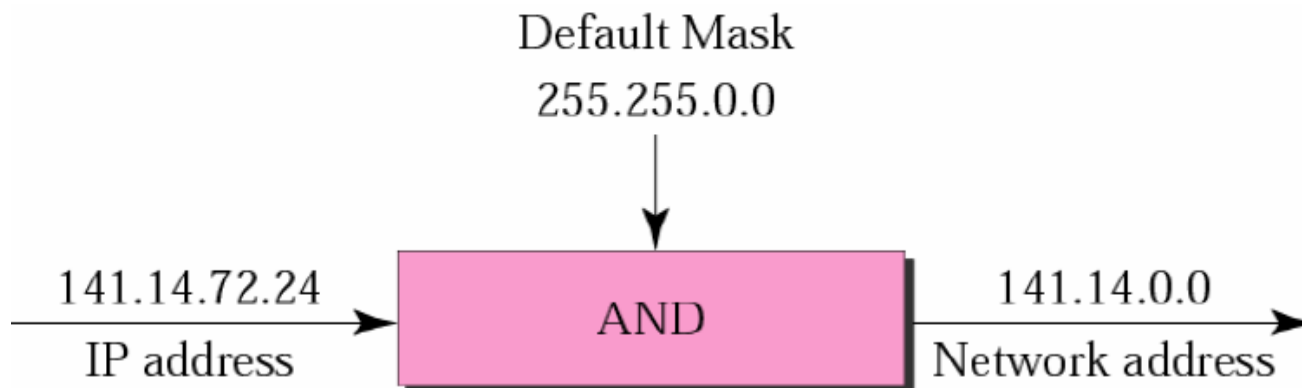
- Địa chỉ định danh (logic) cho một nhóm các host trên mạng máy tính có khả năng xử lý datagrams hoặc frames cho một số dịch vụ mạng được chỉ định

▪ Broadcast Address

- Địa chỉ có các bit phần HostID bằng 1
 - Sử dụng khi muốn phát quảng bá đến toàn bộ host trong cùng mạng
- Ví dụ: Mạng con: 180.13.0.0 sẽ có địa chỉ quảng bá: 180.13.255.255

▪ Default Mask/Subnet mask

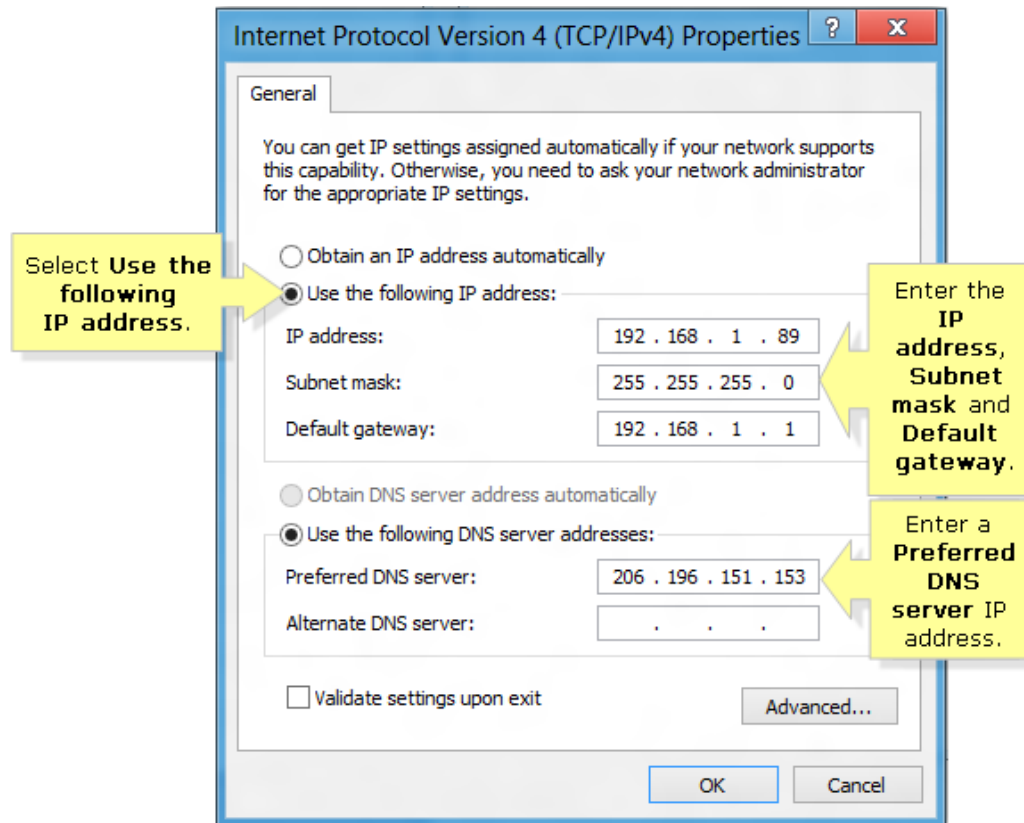
- Địa chỉ dùng để che phần host ID của địa chỉ IP → để xác định network ID



Assigning Addresses

■ Manual configuration

- IP address is configured into the host by the system administrator
- Windows: control panel → network → configuration → tcp/ip → properties
- UNIX: /etc/rc.config



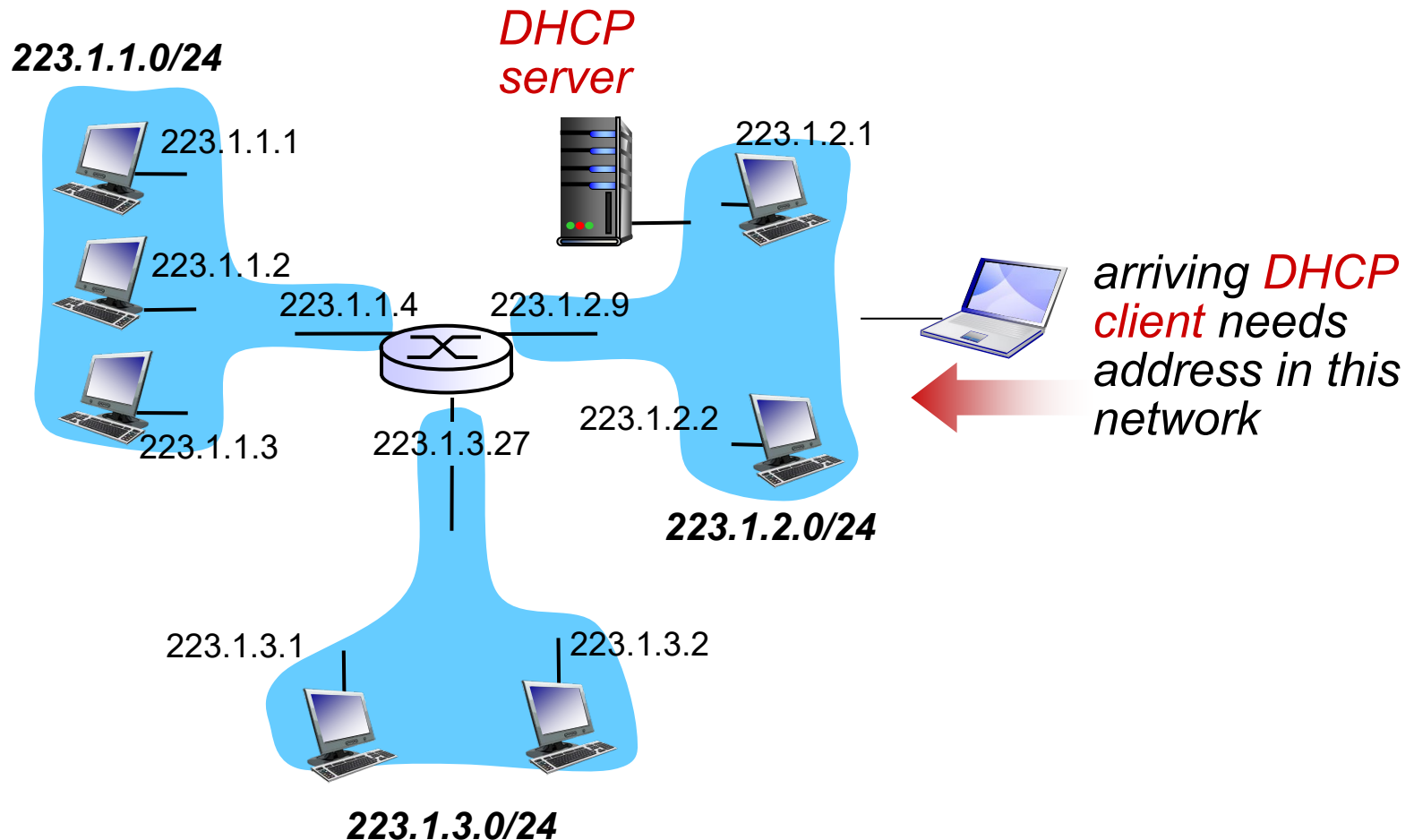
Assigning Addresses

▪ Dynamic Host Configuration Protocol (DHCP)

- Giao thức cấu hình địa chỉ động [RFC 2131]
- “plug-and-play”: Cho phép host nhận một địa chỉ IP động khi kết nối mạng



DHCP client-server scenario



DHCP client-server scenario

DHCP server: 223.1.2.5



DHCP discover

src : 0.0.0.0, 68
dest.: 255.255.255.255, 67
yiaddr: 0.0.0.0
transaction ID: 654

arriving
client



DHCP offer

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP request

src: 0.0.0.0, 68
dest.: 255.255.255.255, 67
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP: Wireshark output (home LAN)

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

.....

request

reply

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."

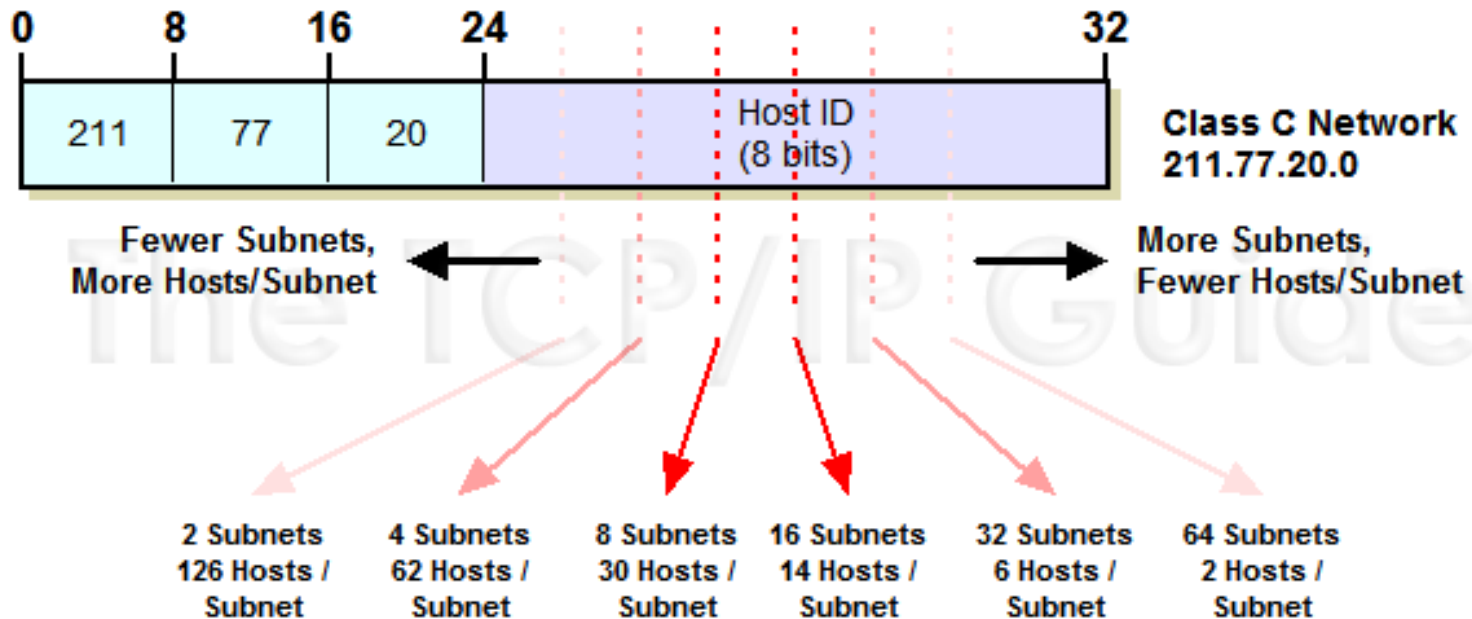
Nhận xét

- **Đánh địa chỉ có phân lớp có một số nhược điểm**
 - Cứng nhắc, lớp C quá nhỏ, lớp B quá lớn → không tận dụng hiệu quả miền địa chỉ
 - Các router trong mạng nội bộ cần phải có địa chỉ mạng (network ID.) riêng biệt cho từng giao diện
- **Cách giải quyết**
 - CIDR: Classless Inter Domain Routing
 - Phần địa chỉ mạng sẽ có độ dài bất kỳ

Classless Inter-Domain Routing (CIDR)

■ CIDR notation

- Địa chỉ IP: a.b.c.d/x, trong đó a.b.c.d là địa chỉ mạng, x (mặt nạ mạng) là số lượng bit trong phần ứng với địa chỉ mạng
- Ví dụ: 128.211.168.0/21



Classless Inter-Domain Routing (CIDR)

- **Phân chia mạng con (Subnetting)**

- Mở rộng địa chỉ mạng sang các bit của địa chỉ host

- **Ví dụ:**

- IP class C: 203.160.9.0 và subnet mask: 255.255.255.0 (địa chỉ mạng 24 bits)
 - Chia thành 4 mạng con → lấy thêm 2 bit cho địa chỉ mạng (26 bits)
 - 203.160.9.0/26

Subnetting: 203.160.9.0/26

Địa chỉ mạng 1 :	203	160	9	0
	11001011	10100000	00001001	00000000

Địa chỉ mạng 2 :	203	160	9	64
	11001011	10100000	00001001	01000000

Địa chỉ mạng 3 :	203	160	9	128
	11001011	10100000	00001001	10000000

Địa chỉ mạng 4 :	203	160	9	192
	11001011	10100000	00001001	11000000

Mặt nạ của các mạng con này là : 255.255.255.192

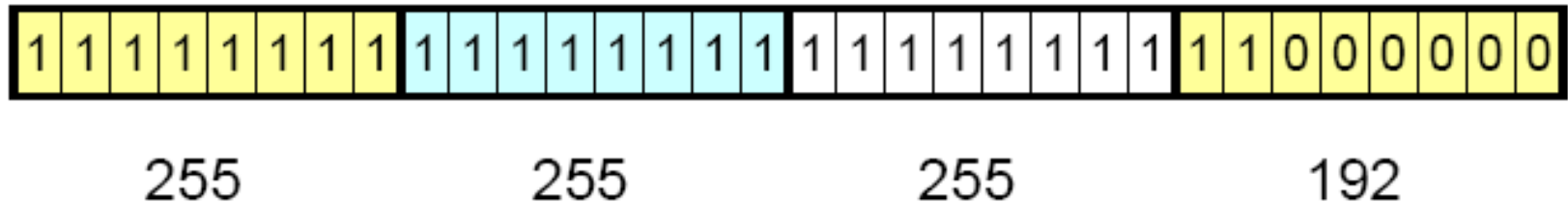
255	255	255	192
11111111	11111111	11111111	11000000

- **Subnet mask**

- 19

Subnetting

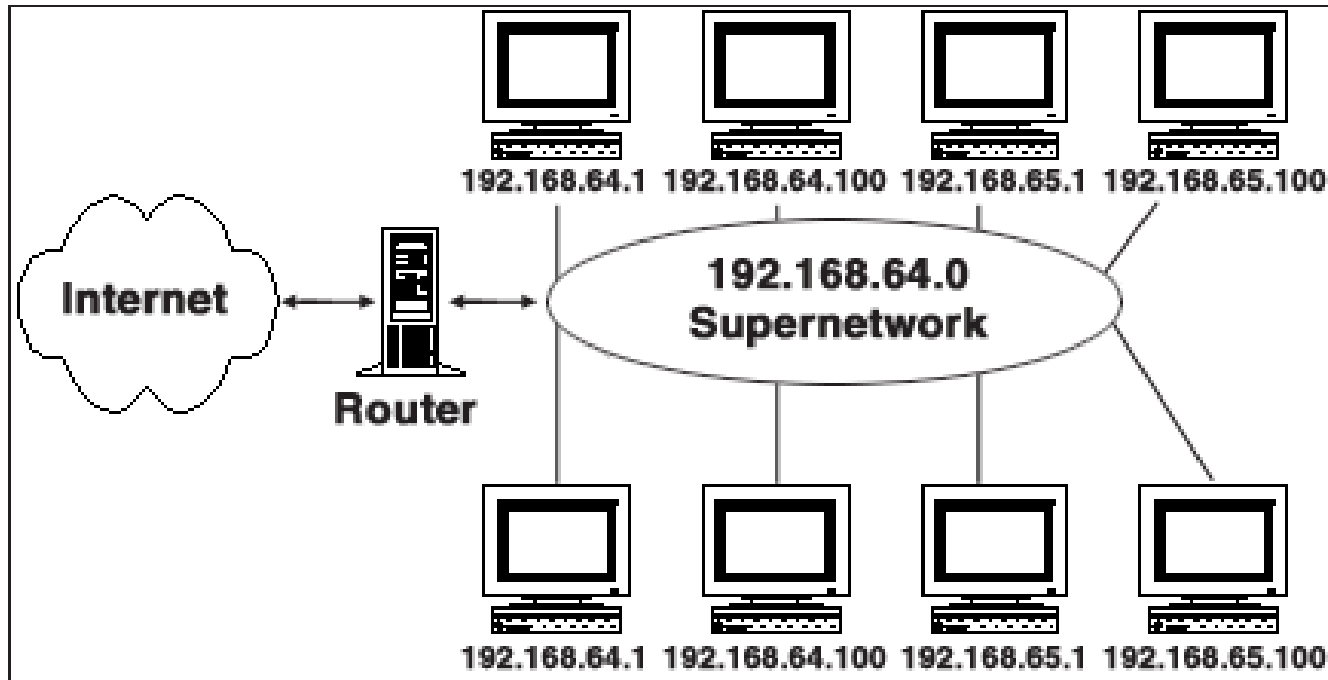
▪ Kích thước mạng



- 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

Supernetting

- **Nhóm nhiều segment → segment lớn hơn**
 - Tiết kiệm vùng địa chỉ
 - Giảm số bản ghi trong bảng định tuyến
 - summarized route



Four separate Class C networks may be combined to create one large supernetwork

Classless Inter-Domain Routing (CIDR)

▪ Example 1:

- Một ISP được cấp một địa chỉ mạng: 192.10.64.0/19
- Tìm mặt nạ mạng, địa chỉ đầu tiên và địa chỉ cuối cùng trong giải địa chỉ, địa chỉ broadcast và số lượng host cho mạng trên.

▪ Solution

- Network address:

11000000 00001010 010|00000 00000000 = 192.10.64.0/19

- Net mask:

11111111 11111111 111|00000 00000000 = 255.255.224.0

- The network address: 010|00000 00000000 = 192.10.64.0/19

- The first host address: 010|00000 00000001 = 192.10.64.1

- Broadcast address: 010|11111 11111111 = 192.10.95.255

- The last host address: 010|11111 11111110 = 192.10.95.254

- There are 213 host addresses ($32 - 19 = 13$) in this range. So the ISP can allocate $8192 - 2 = 8190$ host addresses

Classless Inter-Domain Routing (CIDR)

▪ Example 2:

- Một ISP được gán dải địa chỉ: **194.160.0.0 – 194.175.255.255**
- Tìm địa chỉ mạng, prefix length, địa chỉ đầu, địa chỉ cuối, địa chỉ quảng bá.

▪ Solution:

$$160_{10} = 1010|0000_2$$

$$175_{10} = 1010|1111_2$$

→ Prefix length = 12 (8 bits from 1st byte + 4 bits from 2nd byte)

Network address is: 194.160.0.0/12

Network mask is: 255.240.0.0

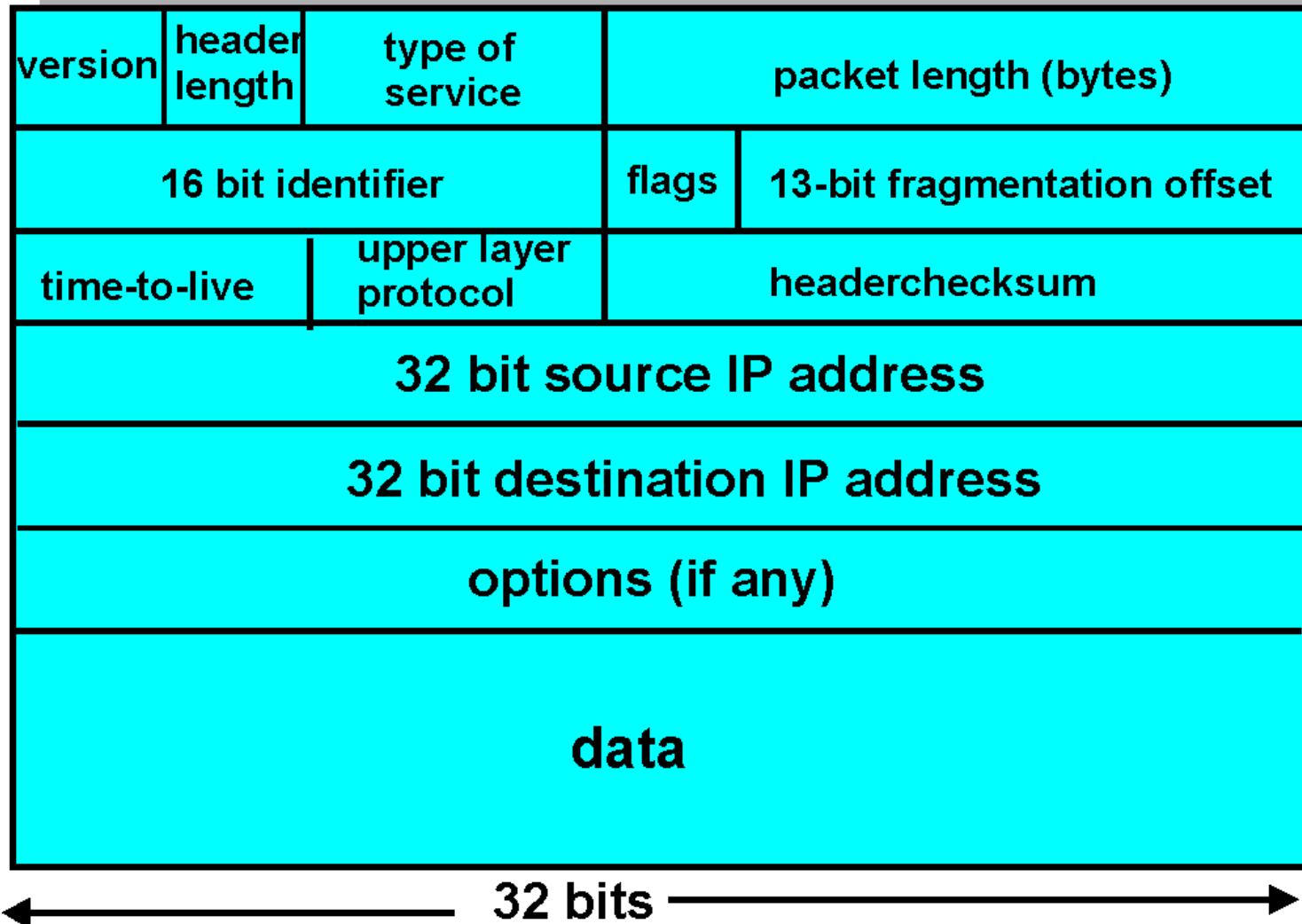
First host address is: 194.160.0.1

Last host address is: 194.175.255.254

Broadcast address is: 194.175.255.255

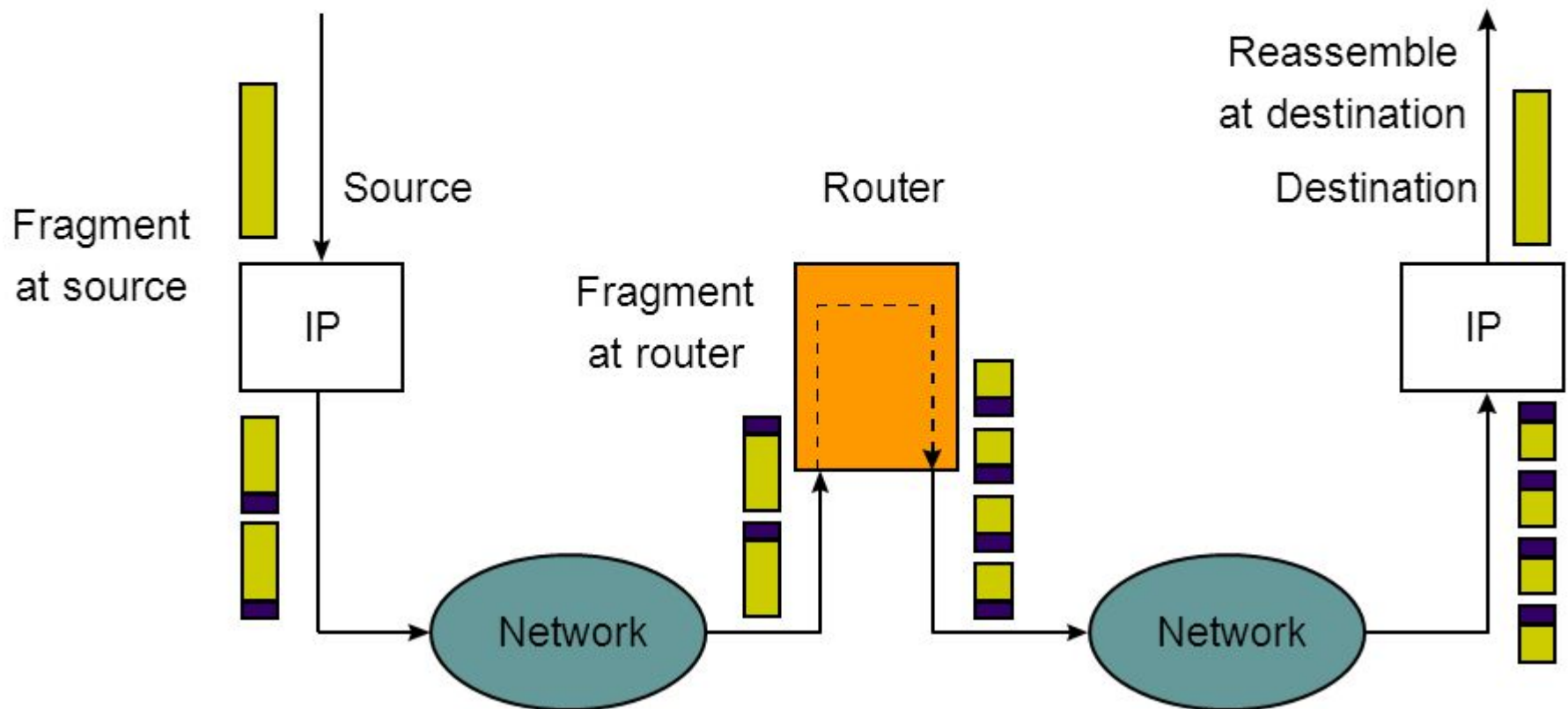
Total Host addresses: $2^{(32-12)} - 2 = 1,048,574$ addresses

IP header



IP Fragmentation and Reassembly

- **Identification** identifies a particular packet
- **Flags** = (unused, don't fragment/DF, more fragment/MF)
- **Fragment offset** identifies the location of a fragment within a packet



IP Fragmentation and Reassembly

▪ Fragmentation

- Phân mảnh sử dụng các trường: identification, flags, fragment offset
 - **Identification**: 16 bit - các offset của cùng 1 gói lớn có cùng một ID.
 - **Flags**: 3 bit
 - + #1 bit: không sử dụng
 - + #2 bit – Don't fragment (DF) bit:
 - » DF=1: Không được phép phân mảnh
 - » DF=0: Được phép phân mảnh
 - + #3 bit – More fragment (MF) bit: nếu DF=0
 - » MF=1: hãy còn phân mảnh tiếp theo
 - » MF=0: phân mảnh cuối cùng
- **Offset**: 13 bit
 - Vị trí của gói tin phân mảnh trong gói tin ban đầu
 - Theo đơn vị 8 bytes

Ví dụ

▪ Ví dụ 1:



Example

- ❑ 4000 byte datagram
- ❑ MTU = 1500 bytes

	length	ID	fragflag	offset	
	=4000	=x	=0	=0	

One large datagram becomes several smaller datagrams

1480 bytes in data field

offset =
 $1480/8$

	length	ID	fragflag	offset	
	=1500	=x	=1	=0	

	length	ID	fragflag	offset	
	=1500	=x	=1	=185	

	length	ID	fragflag	offset	
	=1040	=x	=0	=370	

Homework:

1. ARP (Address Resolution Protocol), RARP
2. ICMP
3. NAT
4. IPv6

ICMP

- **ICMP – Internet Control Message Protocol**
- **RFC 792**
- **ICMP được sử dụng ở tầng mạng để trao đổi thông tin**
 - Báo lỗi: báo gói tin không đến được một máy trạm, số chặng vượt quá giới hạn cho phép (TTL=0), kích thước gói tin quá dài .v.v.
 - Thông tin phản hồi
- **ICMP được sử dụng ở tầng mạng, “phía trên” IP**
 - Thông điệp ICMP chứa trong gói tin IP

Ver	HLEN	DS	Total Length	
Identification			Flags	Fragmentation offset
TTL	Protocol		Header Checksum	
Source IP address				
Destination IP address				
Option				

Protocol:

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

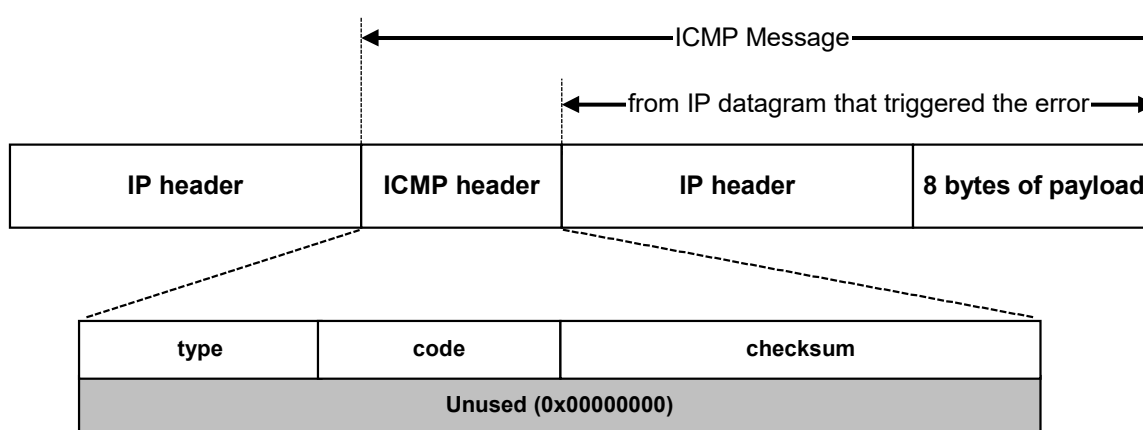
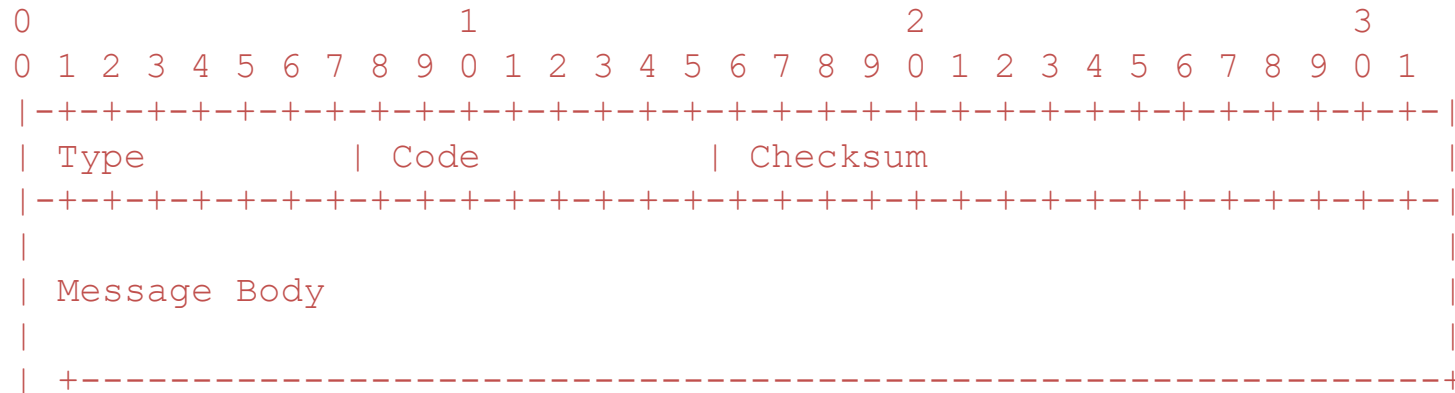
ICMP (tiếp)

- **Định dạng bản tin ICMP:**
 - Type: dạng gói tin ICMP
 - Code: nguyên nhân gây lỗi
 - Rest of the header: 8 bytes đầu tiên của gói tin IP bị lỗi
- **ICMP luôn hoạt động, xong “trong suốt” với user**
- **User có thể sử dụng ICMP qua các công cụ debug**
 - ping
 - traceroute

Type	Code	Checksum
Rest of the header		
Data		

ICMP (tiếp)

■ ICMP Error message



- ICMP error messages include the complete IP header and the first 8 bytes of the payload

- **Một số dạng bản tin ICMP:**

<u>Type</u>	<u>Code</u>	<u>description</u>
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

■ 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)
- Cú pháp: **ping [địa chỉ IP/tên host]**
 - ping www.google.com

▪ Traceroute

- Tìm đường đi (các router trung gian) từ nguồn tới đích
- Cú pháp:
 - Linux: `traceroute` [địa chỉ IP/tên host]
 - Windows: `tracert` [địa chỉ IP/tên host]

