IPv4 Addressing

Computer Networks

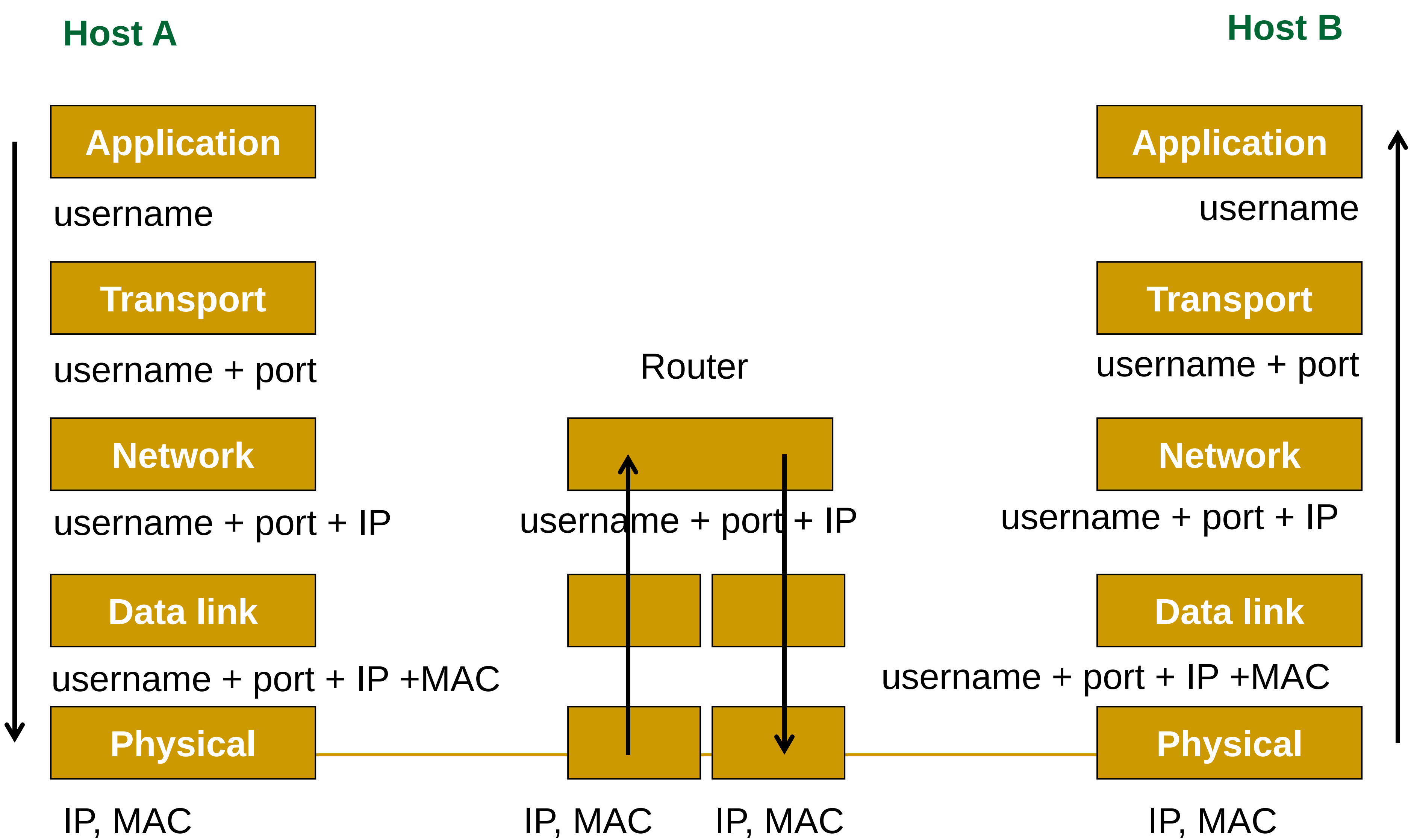
Faculty of Information Technology
Hanoi University

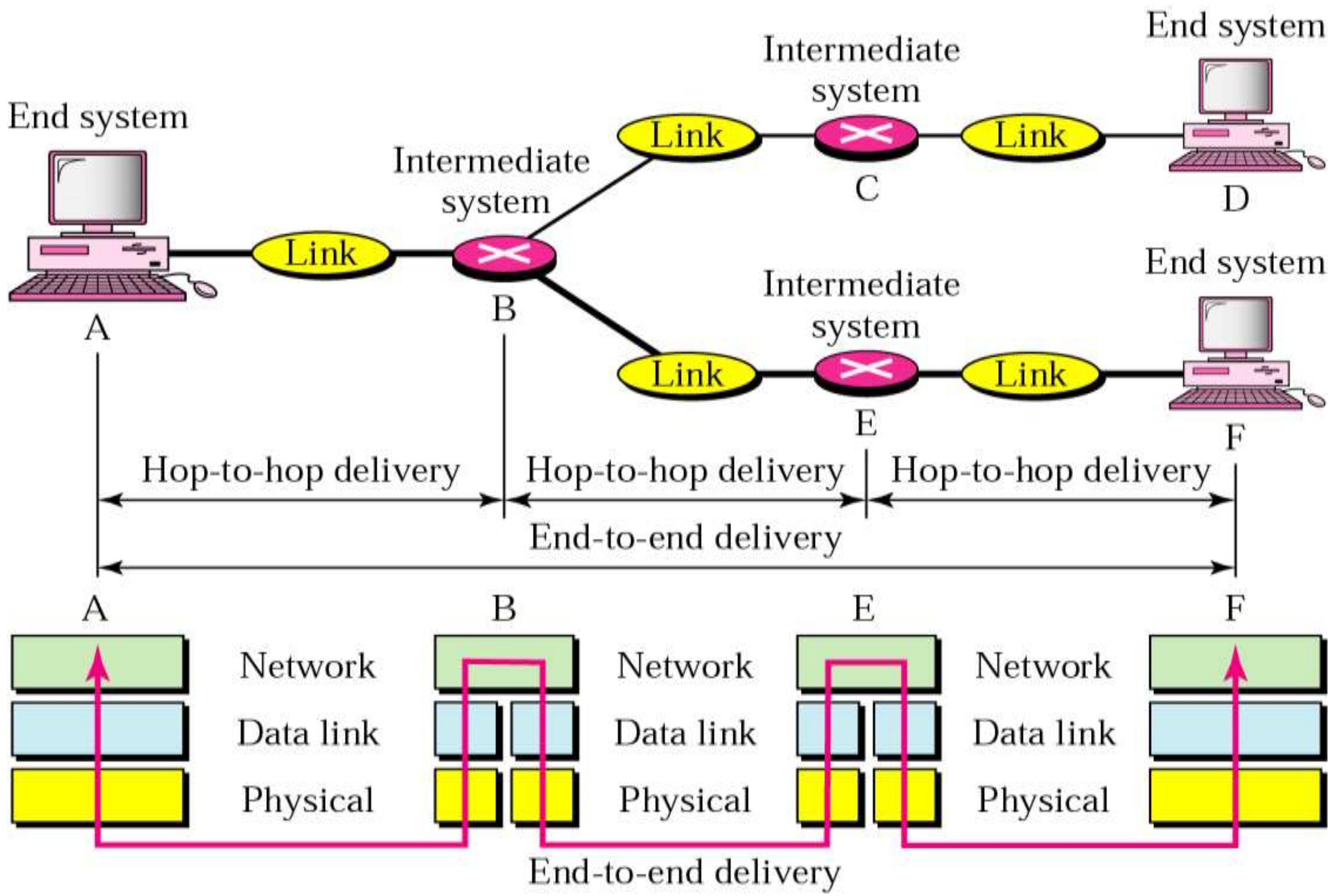
Content

1. Introduction
2. IPv4 Classful addressing
3. IPv4 CIDR
4. NAT

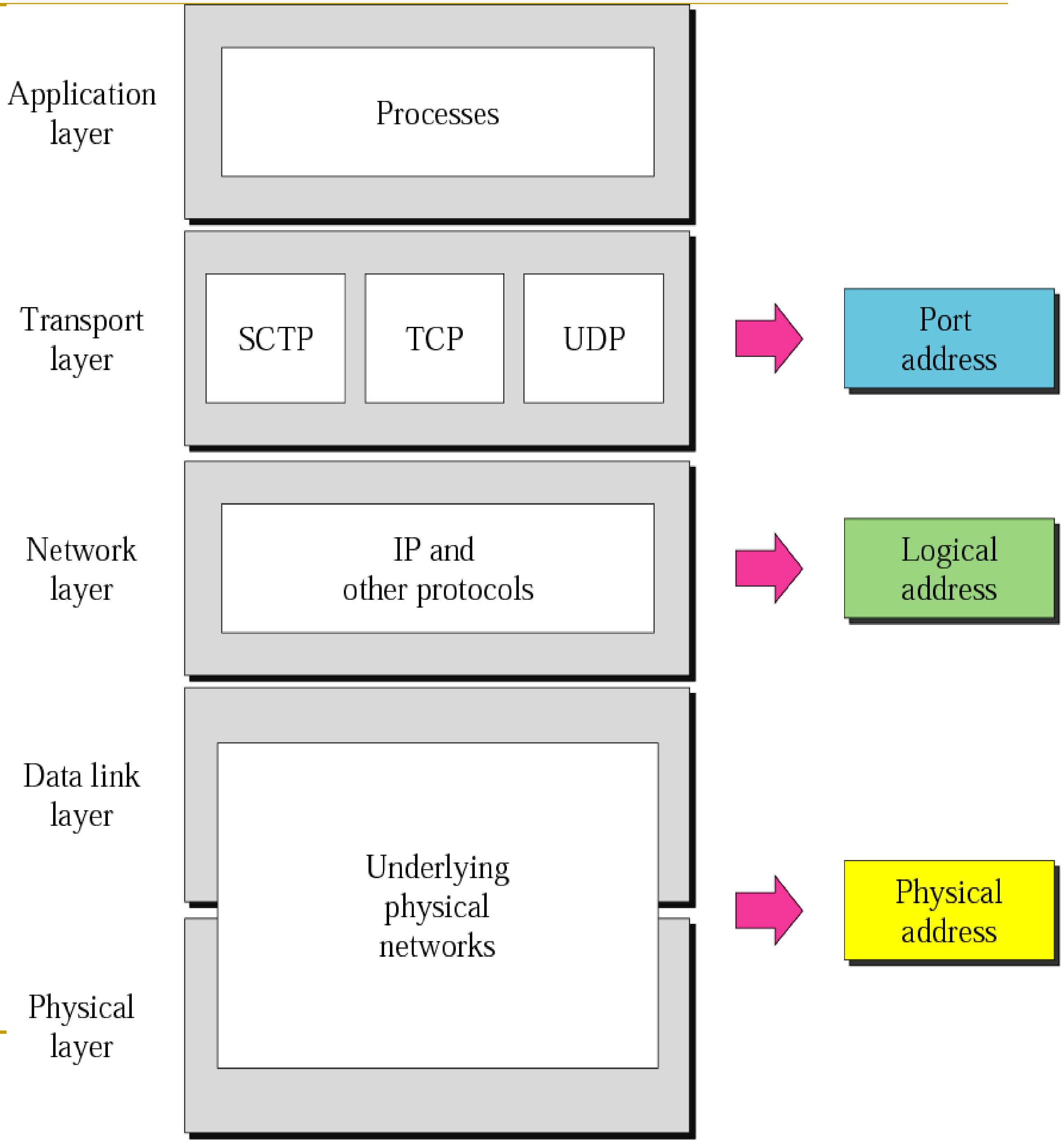
1. Introduction to IPv4

TCP/IP Model


Host A
Host B
Application
username
Transport
username + port
Network
username + port + IP
Data link
username + port + IP +MAC
Physical
IP, MAC
Router
username + port + IP
IP, MAC
IP, MAC
Application
username
Transport
username + port
Network
username + port + IP
Data link
username + port + IP +MAC
Physical
IP, MAC

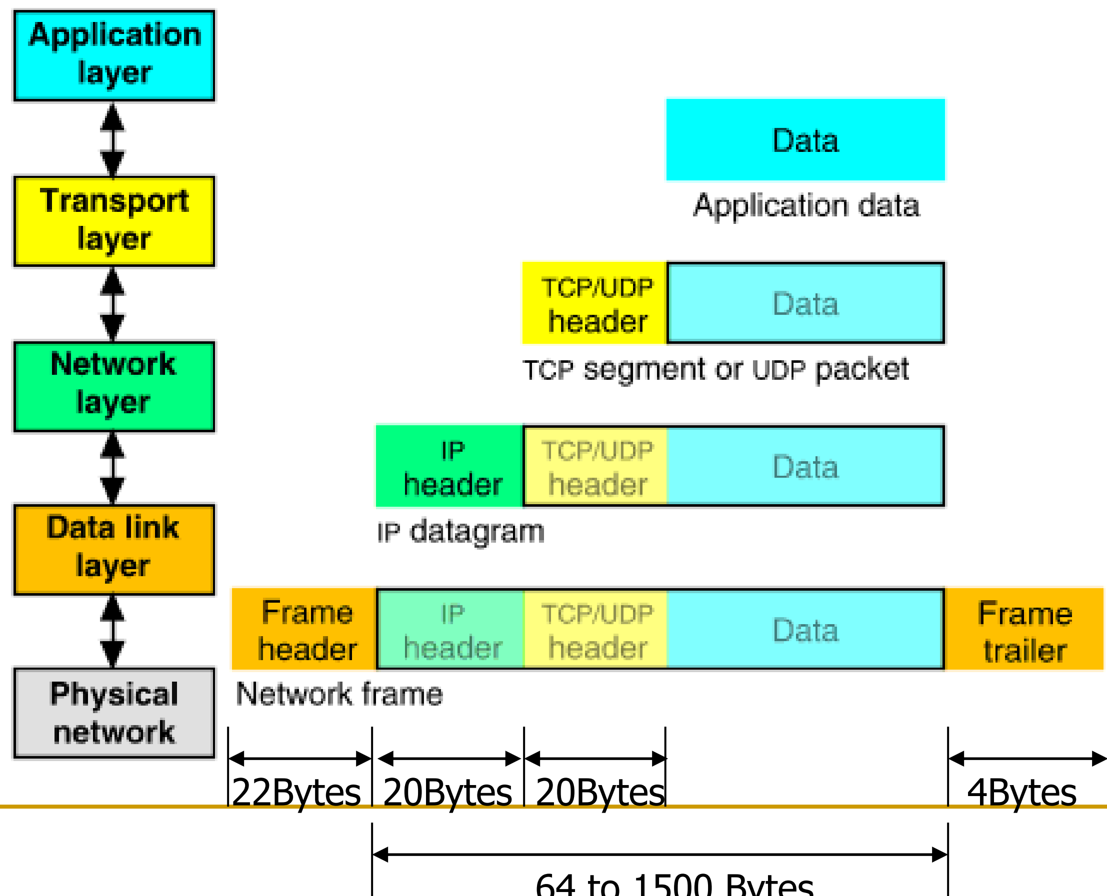

End system
Intermediate system
Intermediate system
End system
Link
Link
Link
Link
Link
A
B
C
D
Intermediate system
End system
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
End-to-end delivery
A
B
E
F
Network
Data link
Physical
Network
Data link
Physical
Network
Data link
Physical
End-to-end delivery

Logical Addressing

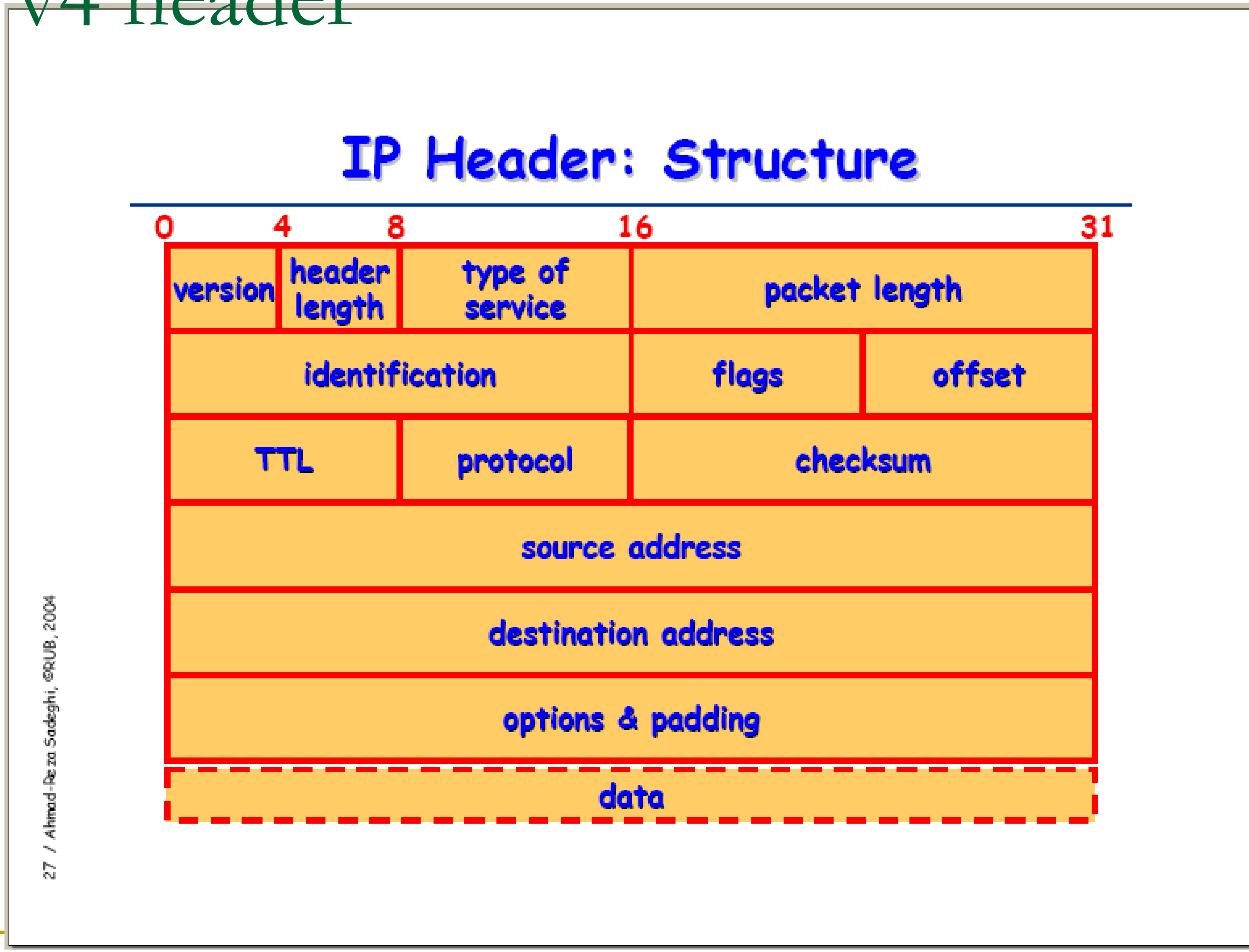


IPv4: Packet Encapsulation

- The data is sent down the protocol stack
- Each layer adds to the data by prepending headers



IPv4 header

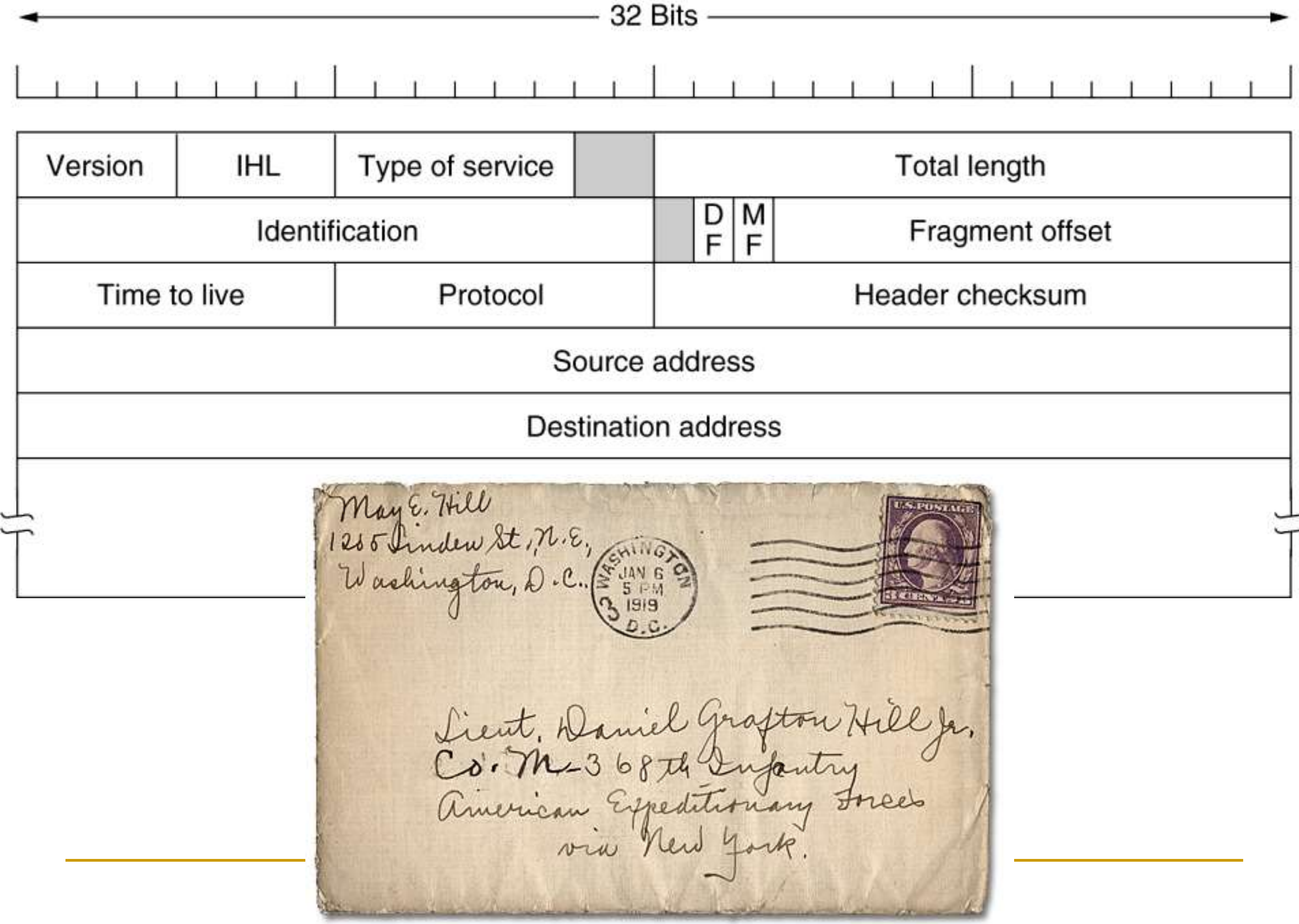

IP Header: Structure
0
4
8
16
31
version
header length
type of service
packet length
identification
flags
offset
TTL
protocol
checksum
source address
destination address
options & padding
data
27 / Ahmad-Reza Sadeghi, ©RUB, 2004

IP Header: Individual Fields

Version	IP Version
Header length	Important for receiver
Type of service	Importance of package
Packet length	Between 72 and 8192 bytes
Identification	Unique identification number
Flags	Controls packet fragmentation
TTL	Lifetime of a packet (15-30 s)

IP Header: Individual Fields

Offset	Relative position to first packet
Protocol	Type of superimposed protocol (TCP/UDP)
Checksum	Integrity of header
Addresses	Identification of nodes by logical addresses
Options	Security, routing information, time stamps

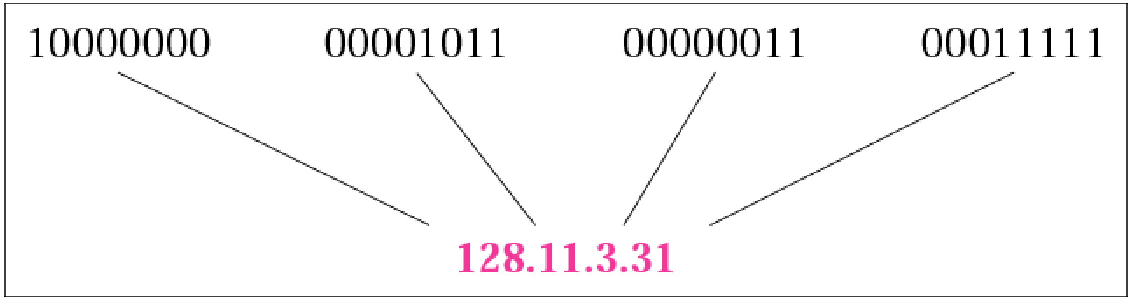

32 Bits
Version
IHL
Type of service
Total length
Identification
DF
MF
Fragment offset
Time to live
Protocol
Header checksum
Source address
Destination address
May E. Hill
1205 Linden St, N.E.,
Washington, D.C.
WASHINGTON
JAN 6
5 PM
1919
D.C.
U.S. POSTAGE
Lieut. Daniel Grafton Hill Jr.
Co. M - 368th Infantry
American Expeditionary Forces
via New York.

Example

Envelope	data length
To	dst IP add
From	src IP add
	time to live
	version
Stamp	service type
Book	protocol type
	Header check sum
	options
	fragment

IPv4 Addresses

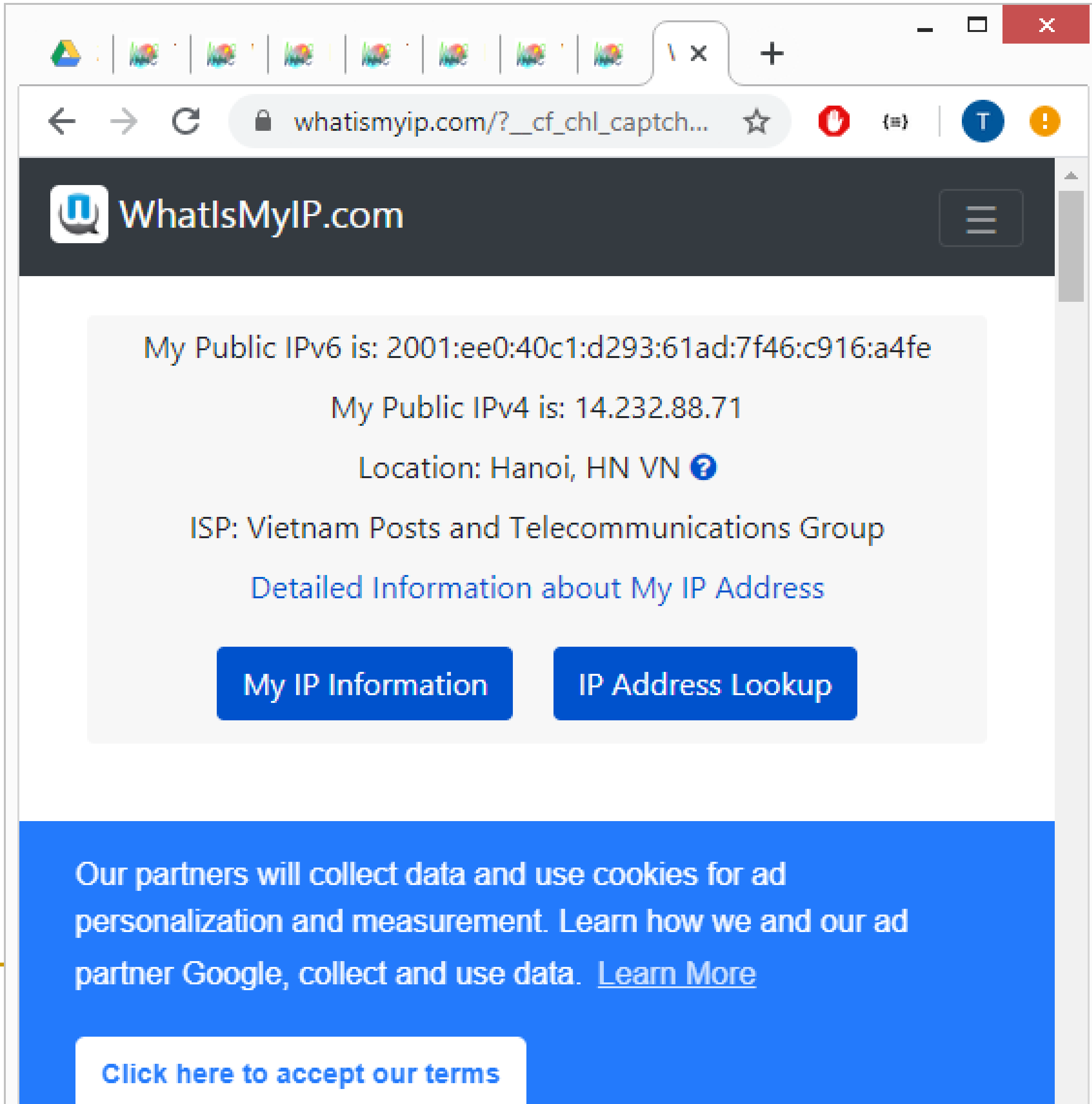
- 32-bit Address
- Uniquely and universally identifies a host
- **Address space** is the total number of addresses used by the protocol
  - 2^{32} = 4,294,967,296 addresses
- Notation
  - Binary
  - Dotted decimal



What is the IP address of fit.hanu.vn?

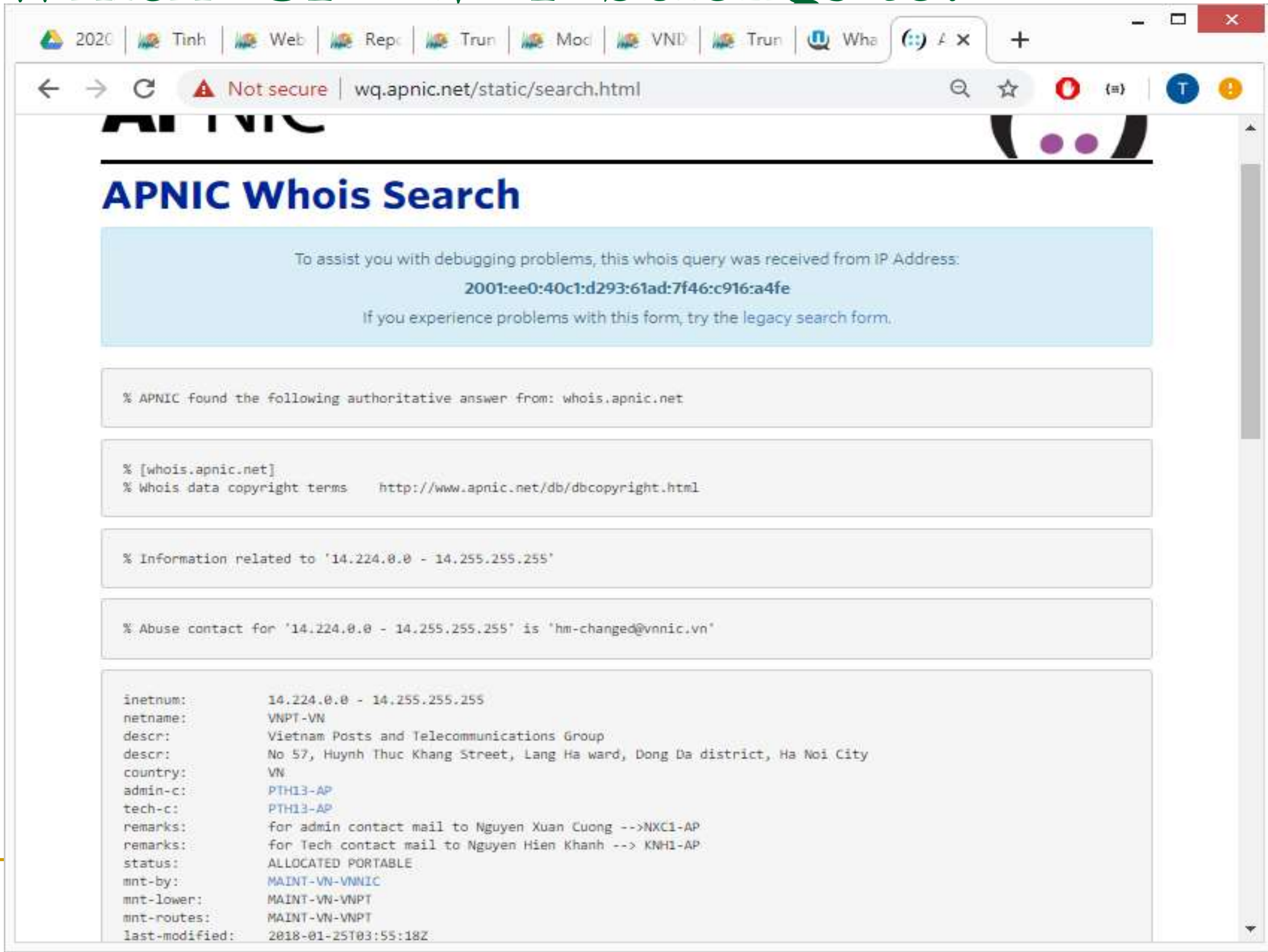
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:¥Documents and Settings¥Tran Quang Anh>nslookup fit.hanu.vn
*** Can't find server name for address 10.0.0.2: Server failed
*** Default servers are not available
Server:  UnKnown
Address:  10.0.0.2

Non-authoritative answer:
Name:    fit.hanu.vn
Address:  202.151.161.173
```

What is my IP?



whatismyip.com/?__cf_chl_captch...
WhatIsMyIP.com
My Public IPv6 is: 2001:ee0:40c1:d293:61ad:7f46:c916:a4fe
My Public IPv4 is: 14.232.88.71
Location: Hanoi, HN VN
ISP: Vietnam Posts and Telecommunications Group
Detailed Information about My IP Address
My IP Information
IP Address Lookup
Our partners will collect data and use cookies for ad personalization and measurement. Learn how we and our ad partner Google, collect and use data. Learn More
Click here to accept our terms

Which ISP my IP belongs to?

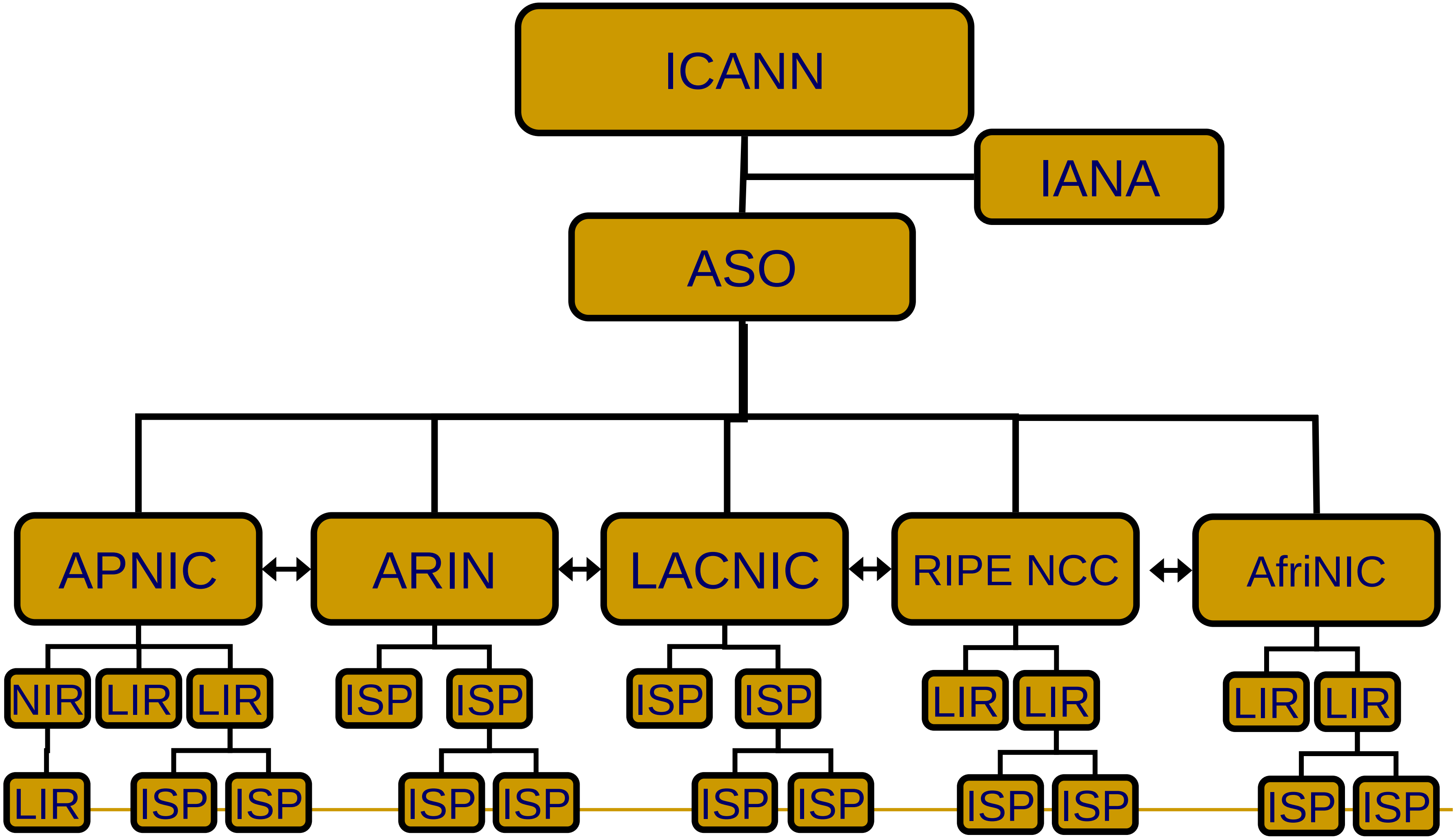


How many IP address in Vietnam?

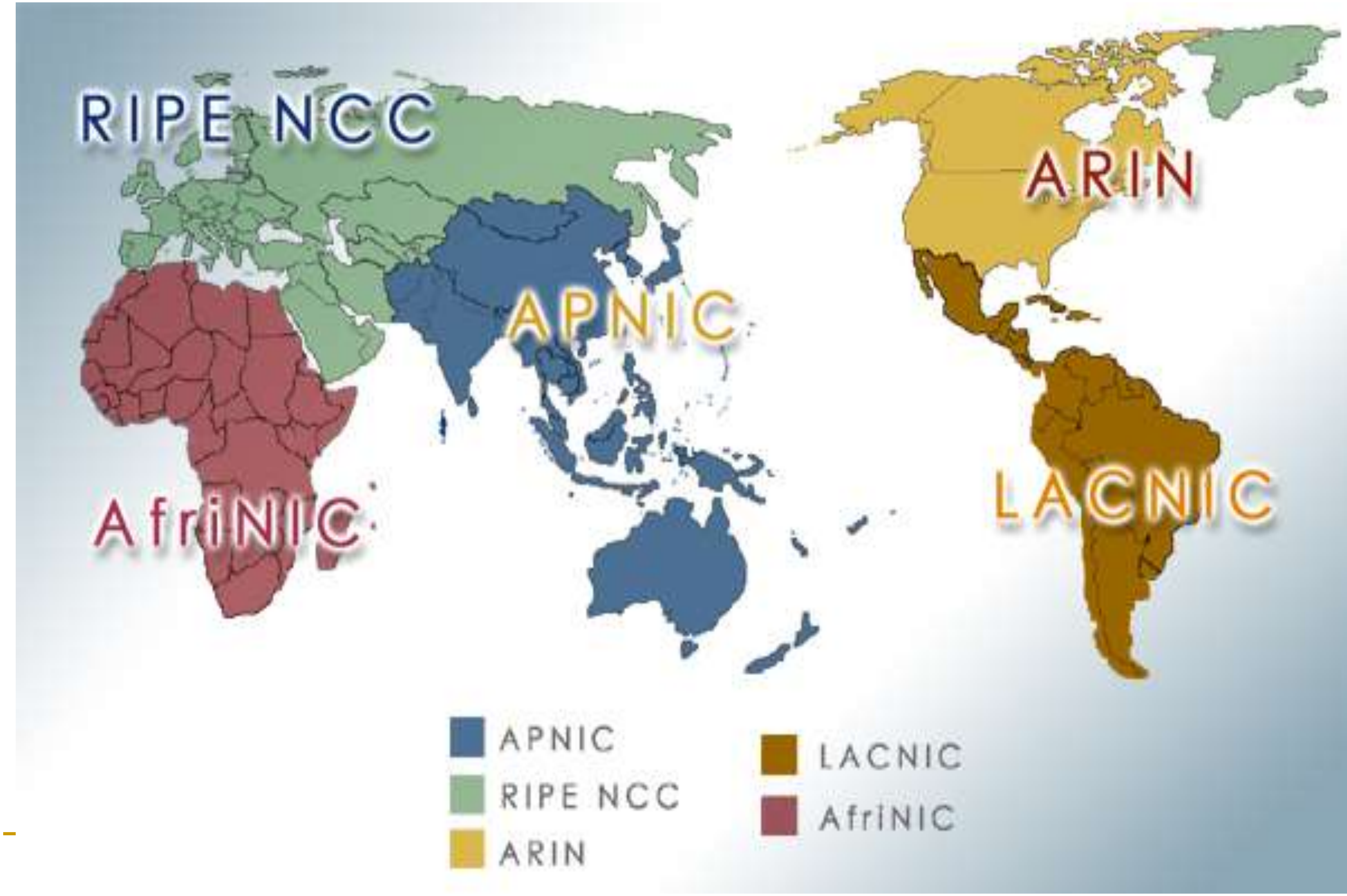
- Allocated IP address (VNNIC) (March 2020)
  - **IPv4: ~16 million**
  - **IPv6: 408 billion/64**

(https://www.thongkeinternet.vn/jsp/trangchu/index.jsp)

Internet Registry Structure



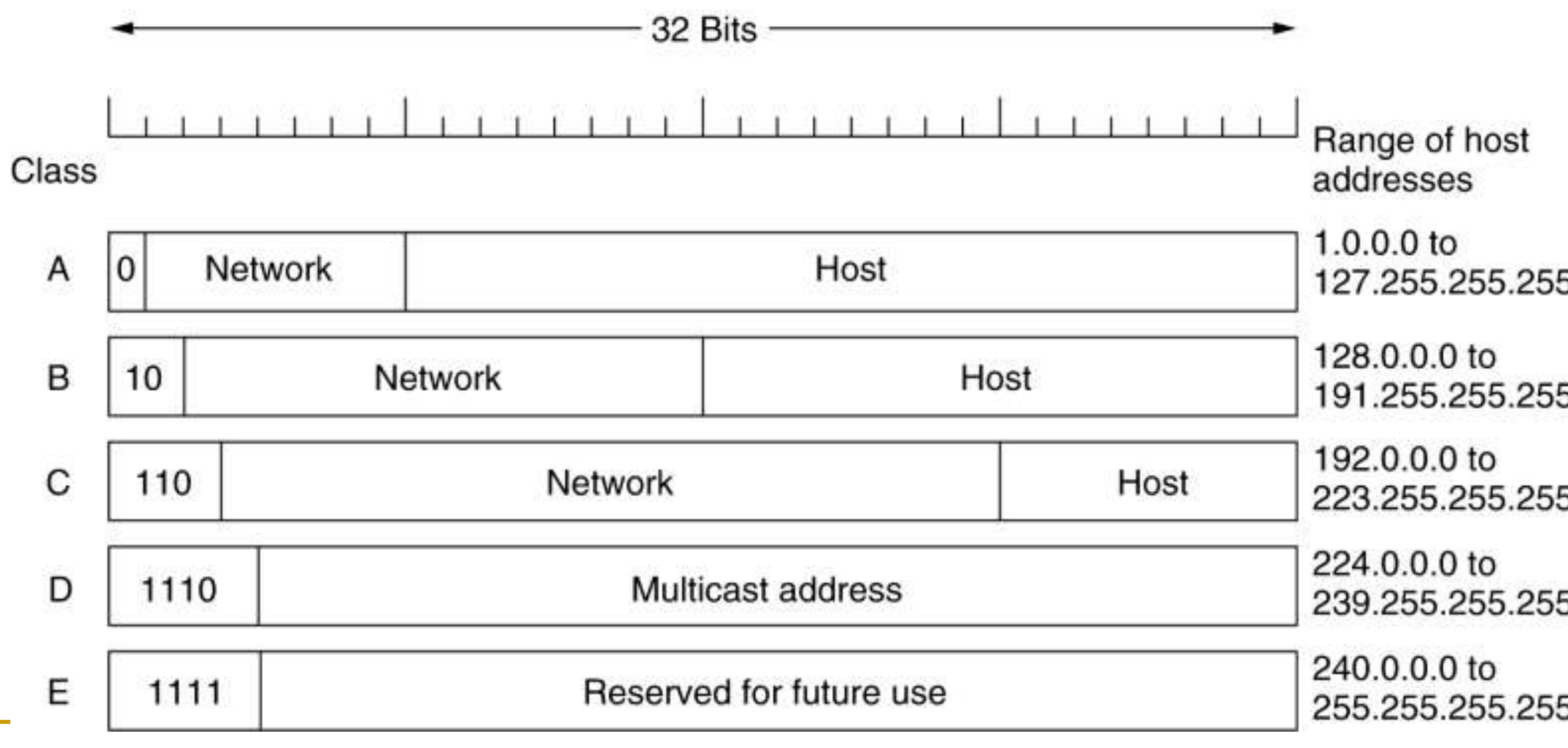
Internet Registry Structure



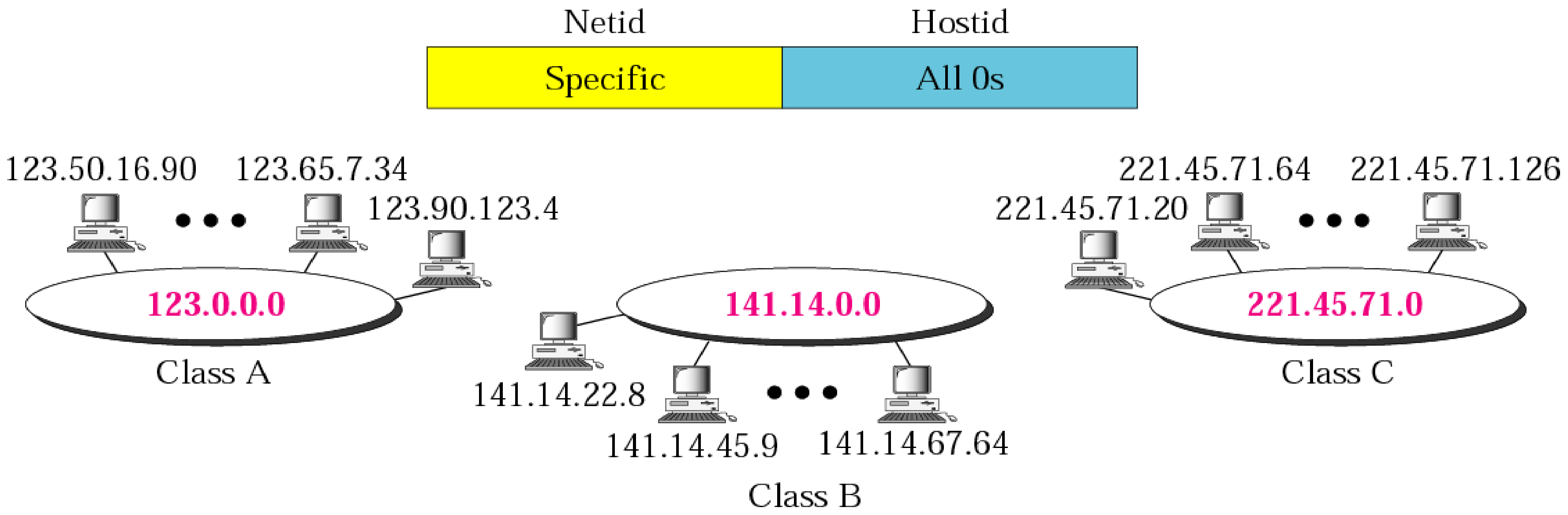
2. IPv4 classful addressing

Classful Addressing

- Five classes; A, B, C, D and E
  - Each class occupies some part of the address space



Network Address & Default Mask

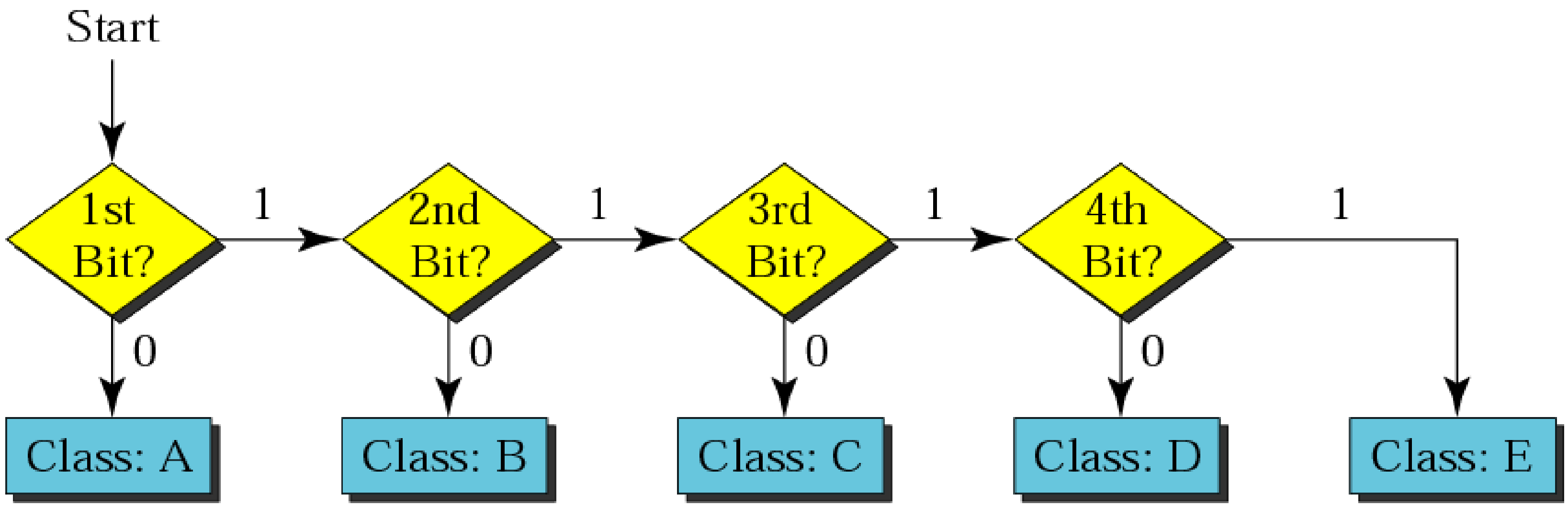


Class	*Mask in binary*	*Mask in dotted-decimal*
A	**11111111** 00000000 00000000 00000000	**255.**0.0.0
B	**11111111 11111111** 00000000 00000000	**255.255.**0.0
C	**11111111 11111111 11111111** 00000000	**255.255.255.**0

Why do we need Mask?

- Mask together with an IP defines the range of IP block.
- Example 1
  - IP: 192.168.5.7
  - Mask: 255.255.255.0
  - => IP block: 192.168.5.0 – 192.168.5.255
  - IP range from 192.168.5.1 – 192.168.5.254
- Example 2
  - IP 18.202.1.6
  - Mask: 255.0.0.0
  - What is the IP block? 18.0.0.0-18.255.255.255

Finding the class



	First byte	Second byte	Third byte	Fourth byte
Class A	**0 to 127**			
Class B	**128 to 191**			
Class C	**192 to 223**			
Class D	**224 to 239**			
Class E	**240 to 255**			

Network address

- Network address is the first address in the block
- We don’t use the first and the last address of the block for real host.
- Given the whole address, can we find the network address?
  1. Find the class
  2. Apply the default mask
  3. We have the network address !

Example 3

Given the network address 220.34.76.0, find the class, the block, and the range of the addresses.

Solution

The class is C because the first byte is between 192 and 223. The block has a netid of 220.34.76. The addresses range from 220.34.76.0 to 220.34.76.255.

Host range: 220.34.76.1 to 220.34.76.254

Address in binary: 11011100 00100010 01001100 00000000
C-mask: 11111111 11111111 11111111 00000000
IP block : 11011100 00100010 01001100 00000000 (220.34.76.0)

- 11011100 00100010 01001100 11111111 (220.34.76.255)

The center of the Internet based on IPv4

- MIT owns one Class A (18.*.*.*)
- China owns 3 Class A
- Vietnam owns 64 Class B

Problem with Classfull Addressing (IPv4)

- Major Problem: Running out of addresses

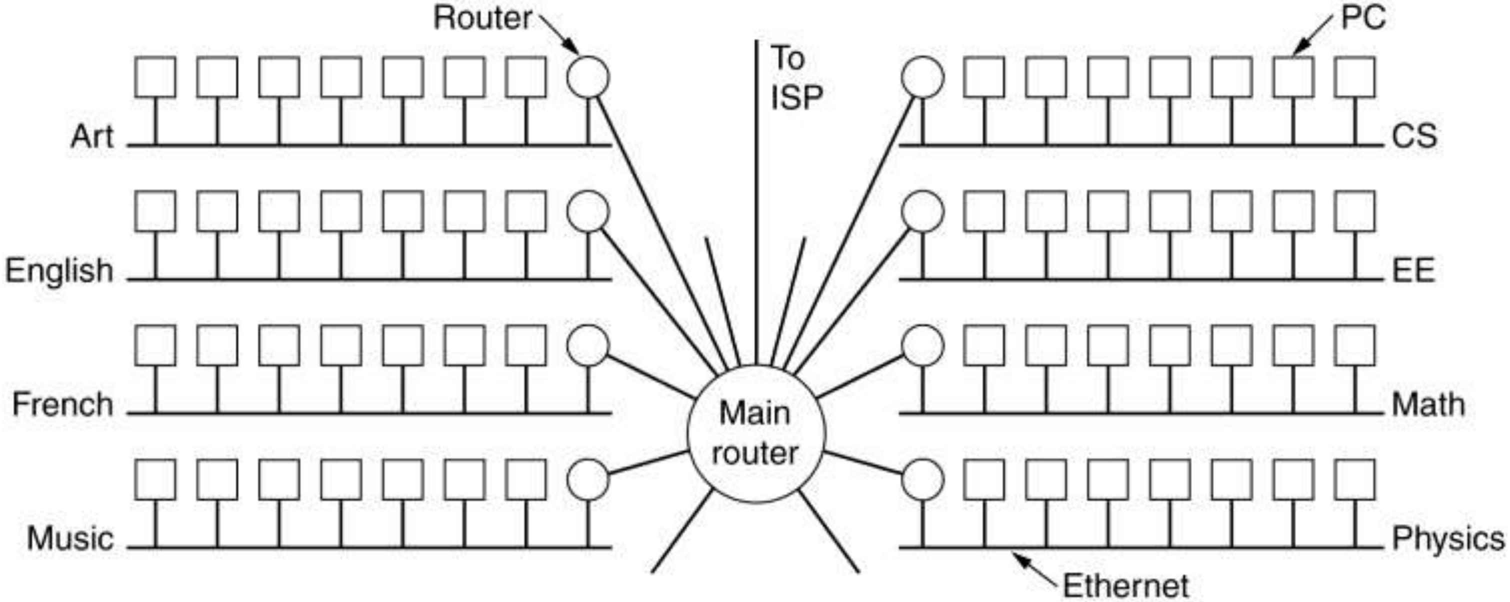
Class	Max. networks	Max. hosts/network
A	126	16,777,214
B	16,382	65,536
C	2,097,150	254

  - Class C is too small, class B widely used, but host size too large
- Temporary solutions
  - NAT (Network Address Translation)
  - CIDR (Classless Inter Domain Routing)
- The best Solutions is IPv6.

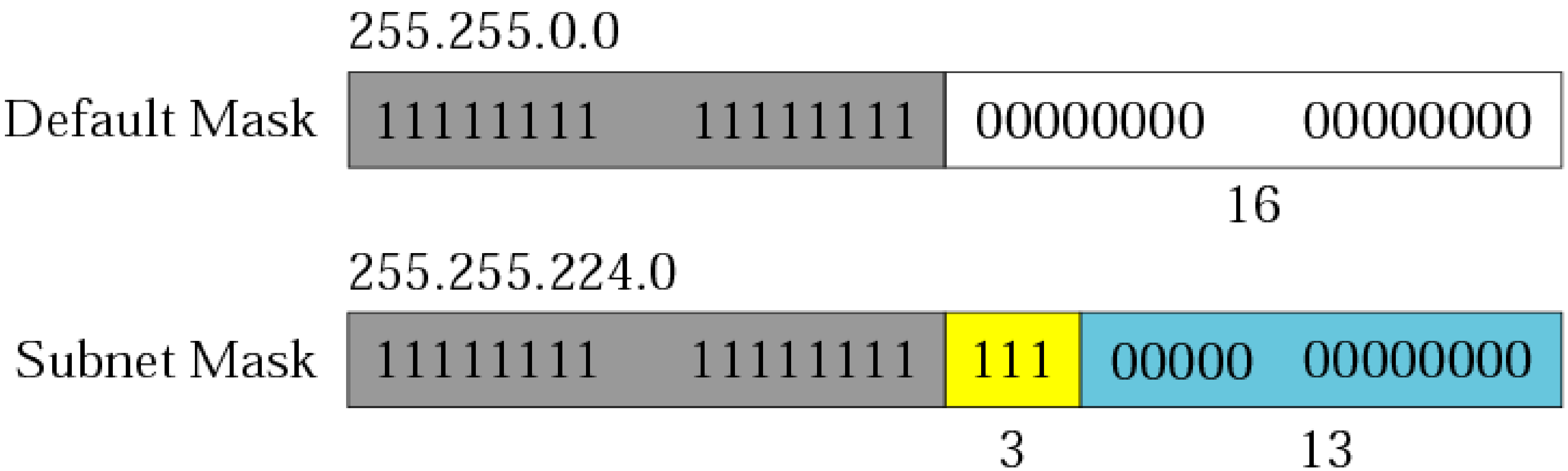
3. CIDR
(Classless Inter Domain Routing)

CIDR / Subnets

- Use a single network address for the entire organization, and internally divide the host address space into a **subnet address** and a **host id**



Subnetting and Subnet Mask



- Number of subnets = 2^3
- Number of addresses per subnet = 2^{13}

Terminology

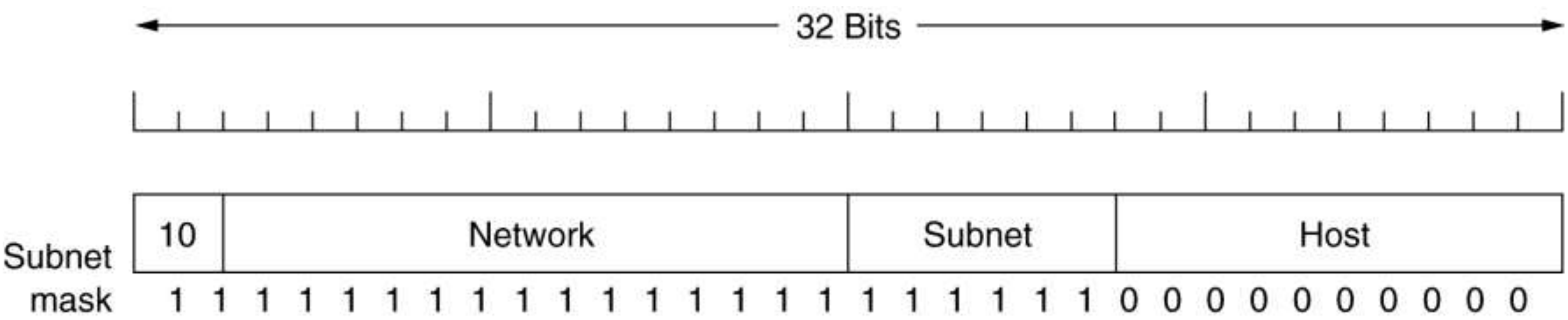
- Prefix = netID
  - The common part of the address
- Prefix Length = length (# of bits) of the prefix
  - denoted by */n*
- Suffix = hostID
- Suffix length = length (# of bits) of the suffix
  - calculated by (32 - *n*)

Prefix Lengths

/n	Mask	/n	Mask	/n	Mask	/n	Mask
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

Subnet Masks

a class B network subnetted into 64 subnets



Address: 130.50.15.6/22

Subnet Mask: 255.255.252.0

CIDR/Subnetting

A set of IP address assignments

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

$$
\begin{array}{lll}
(194.24.17.4 \& \& 255.255.248.0) \neq 194.24.0.0 & & \surd \\
(194.24.17.4 \& \& 255.255.240.0) = 194.24.16.0 & & OK \\
(194.24.17.4 \& \& 255.255.252.0) \neq 194.24.8.0 & & \surd
\end{array}
$$

Finding the Address block

- Given the address and the mask, we can find
  - the first address
  - the last address
  - the number of addresses

Example 4: Finding the first address

What is the first address in the block if one of the addresses is 140.120.84.24/20?

Solution

The prefix length is 20, which means that we must keep the first 20 bits as is and change the remaining bits (12) to 0's. The following shows the process:

Address in binary: ***10001100 01111000 01010100 00011000***
Keep the left 20 bits: ***10001100 01111000 01010000 00000000***
Result in CIDR notation: 140.120.80.0/20

Finding the last address in the block : 3 ways

1. Keep constant n first bits, change 32-n last bits to all 1 (best way)
2. add the number of addresses to the 1^{st} address, minus one
3. Add the first address to the complement of the mask

Remember:

We don't use the first and the last address for real host

Example 4

Find the number of addresses in the block if one of the addresses is 140.120.84.24/20.

Solution 1:

The prefix length is 20, which means that we must keep the first 20 bits as is and change the remaining bits (12) to 0's. The following shows the process:

Address in binary: 10001100 01111000 01010100 00011000
Keep the left 20 bits: 10001100 01111000 01011111 11111111
Result in CIDR notation: 140.120.95.255/20

Example 4

Find the number of addresses in the block if one of the addresses is 140.120.84.24/20.

Solution 2:

The prefix length is 20. The number of addresses in the block is 2^{32-20} or 2^{12} or 4096

Example 4

Find the last address in the block if one of the addresses is 140.120.84.24/20.

Solution 2

We found in the previous examples that the first address is 140.120.80.0/20 and the number of addresses is 4096. To find the last address, we need to add 4095 (4096 − 1) to the first address (last one is the broadcast address):

Example 4

Solution 2

To keep the format in dotted-decimal notation, we write 4095 as 15.255. We then add the first address to this number (in base 255) to obtain the last address as shown below:

```
140 . 120 .  80 .    0
              15  .  255
-------------------------
140 . 120 .  95 .  255
```

The last address is 140.120.95.255/20.

Example 4

Find the last address in the block if one of the addresses is 140.120.84.24/20.

Solution 3:

The mask has twenty 1s and twelve 0s. The complement of the mask has twenty 0s and twelve 1s. In other words, the mask complement is

00000000 00000000 00001111 11111111

or 0.0.15.255. We add the mask complement to the beginning address to find the last address.

Example 4

Find the last address in the block if one of the addresses is 140.120.84.24/20.

Solution 3:

140 . 120 . 80 . 0
15 . 255
----
140 . 120 . 95 . 255

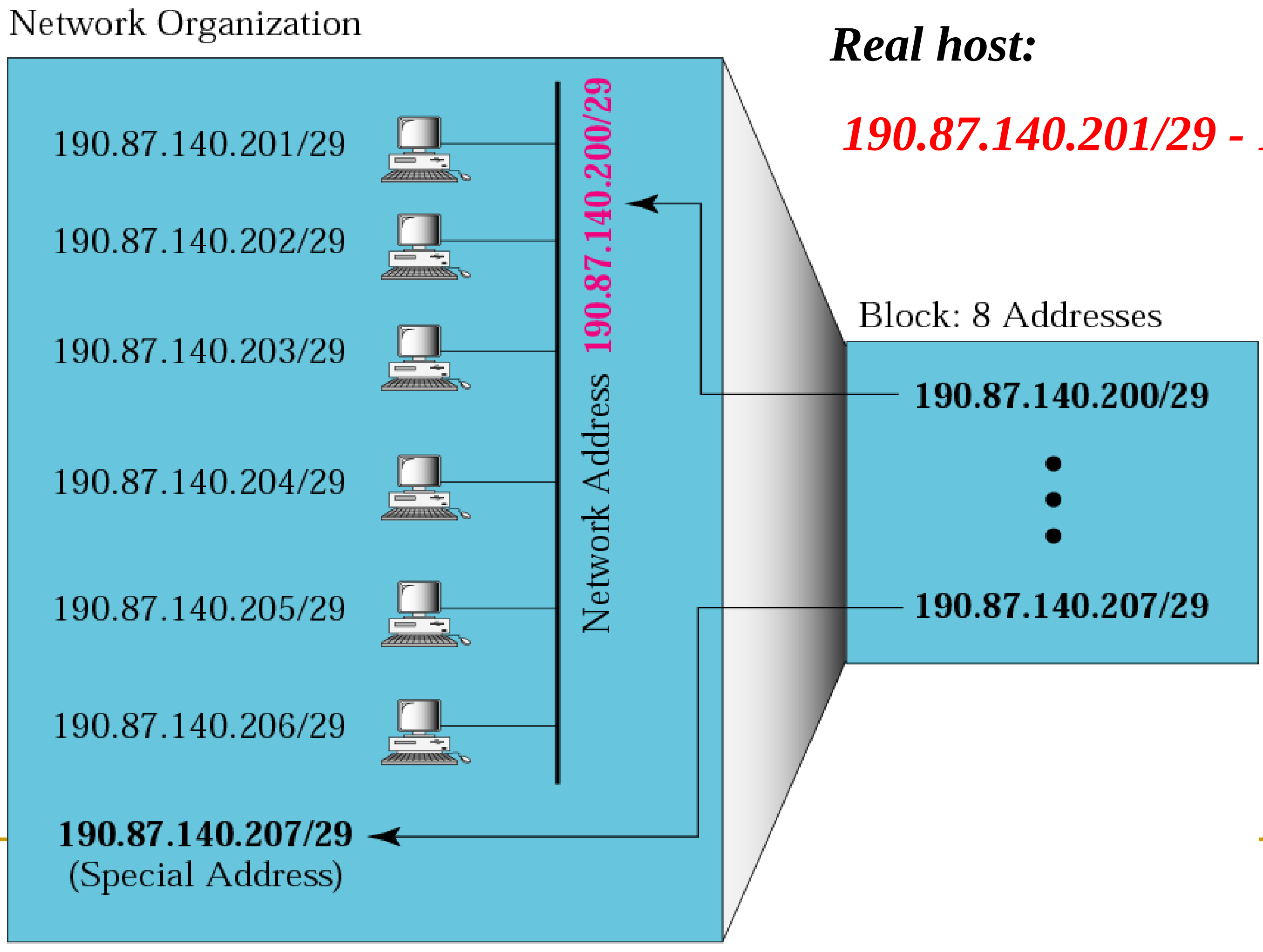
The last address is 140.120.95.255/20.

Example 5

- ***Find the block if one of the addresses is 190.87.140.202/29***

Example 5

The first address is 190.87.140.200/29, the last address is 190.87.140.207/29. There are only 8 addresses in this block.



Real host:

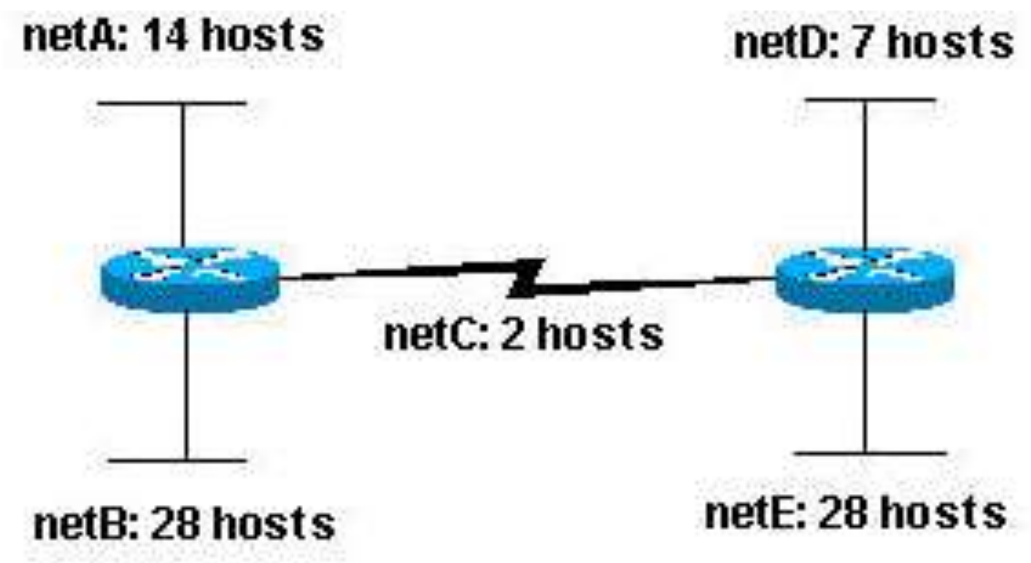
190.87.140.201/29 - 190.87.140.206/29

Creating Subnets

- **Network formula**
  - 2^x, where *x* is the number of 1s added to the subnet mask from the previous or default subnet mask
- **Hosts formula**
  - $2^y - 2$, where *y* is the number of 0s in the subnet mask , y = 32-n

Example 6

Given the Class C network of 204.15.5.0/24, subnet the given network



Example 6

Solution 1:

A: 204.15.5.0/27 (255.255.255.224)

host address range 204.15.5.1 to 204.15.5.30

B: 204.15.5.32/27 (255.255.255.224)

host address range 204.15.5.33 to 204.15.5.62

C: 204.15.5.64/27 (255.255.255.224)

host address range 204.15.5.65 to 204.15.5.94

D: 204.15.5.96/27 (255.255.255.224)

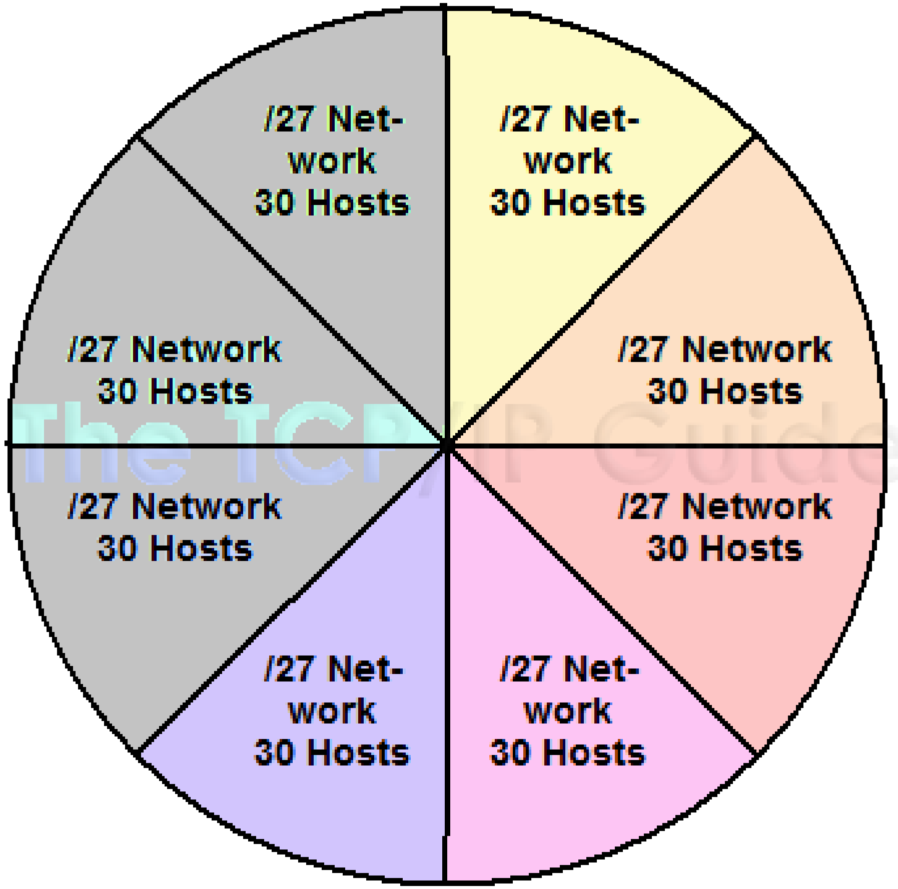
host address range 204.15.5.97 to 204.15.5.126

E: 204.15.5.128/27 (255.255.255.224)

host address range 204.15.5.129 to 204.15.5.158

Solution 1:

- **Class C (/24) Network (254 hosts) Split Into 8 Subnets /27 (32 IPs - 30 hosts)**



Another solution: VLSM (Variable Length Subnet Masks)

- VLSM allows using different masks for each subnet, thereby using address space efficiently

- CIDR/VLSM network addresses are now used throughout the public Internet

Example 6

Solution 2:

- A (14 hosts): 204.15.5.0/28 (255.255.255.240)
  host address range 204.15.5.1 - 204.15.5.14
- D (7 hosts): 204.15.5.16/28 (255.255.255.240)
  host address range 204.15.5.17 - 204.15.5.30
- B (28 hosts): 204.15.5.32/27 (255.255.255.224)
  host address range 204.15.5.33 - 204.15.5.62
- E (28 hosts): 204.15.5.64/27 (255.255.255.224)
  host address range 204.15.5.65 - 204.15.5.94
- C (2 hosts): 204.15.5.96/30 (255.255.255.252)
  host address range 204.15.5.97 - 204.15.5.98

Example 6

Solution 3: The easiest way to assign the subnets is to assign the largest first

- B: 204.15.5.0/27 (255.255.255.224)

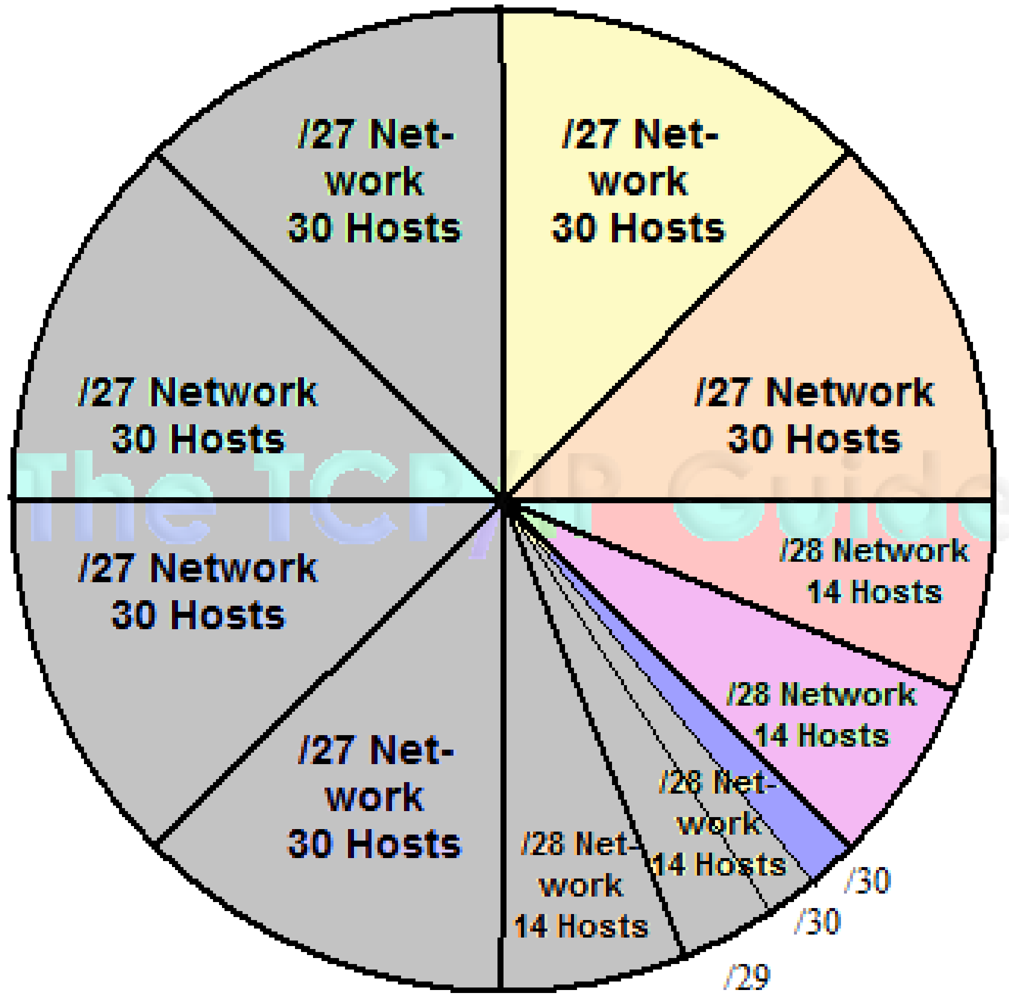
  host address range 204.15.5.1 to 204.15.5.30
- E: 204.15.5.32/27 (255.255.255.224)

  host address range 204.15.5.33 to 204.15.5.62
- A: 204.15.5.64/28 (255.255.255.240)

  host address range 204.15.5.65 to 204.15.5.78
- D: 204.15.5.80/28 (255.255.255.240)

  host address range 204.15.5.81 to 204.15.5.94
- C: 204.15.5.96/30 (255.255.255.252)

  host address range 204.15.5.97 to 204.15.5.98



/27 Net-
work
30 Hosts
/27 Net-
work
30 Hosts
/27 Network
30 Hosts
/27 Network
30 Hosts
/27 Network
30 Hosts
/28 Network
14 Hosts
/28 Network
14 Hosts
/27 Net-
work
30 Hosts
/28 Net-
work
14 Hosts
/28 Net-
work
14 Hosts
/30
/30
/29
The TCP/IP Guide

Example 6

- Solution 1:

  204.15.5.0-204.15.5.159 => good not the best solution

- Solution 2 & 3:

  204.15.5.0-204.15.5.99 => better than solution 1. IP address space can be used economically.

The best way to solve this problem is to

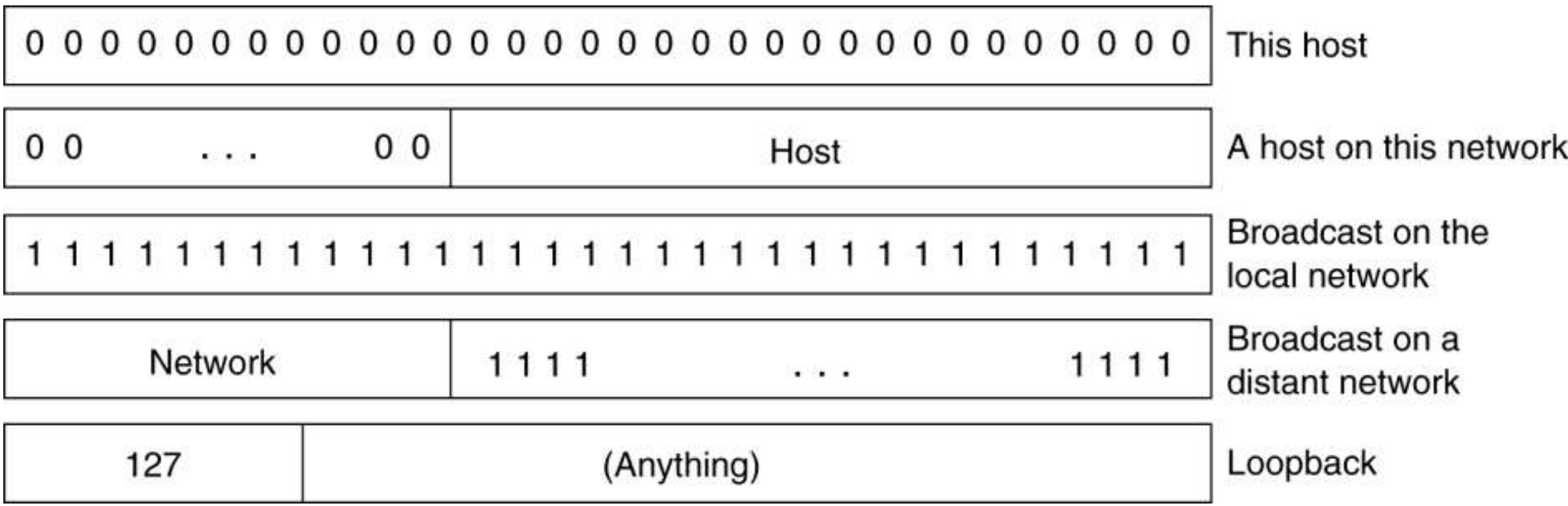
assign IP addresses the largest network first

(Follow solution 3)

CIDR

- The advantages of CIDR over the classful IP addressing are:
  - CIDR can be used to effectively manage the available IPv4 address space
    - As a result of the deployment of CIDR/VLSM, it is now estimated that IPv4 addresses would be depleted around 2008
  - CIDR reduces the number of routing table entries by creating a 3-level hierarchy

Special IP Addresses



Loopback address

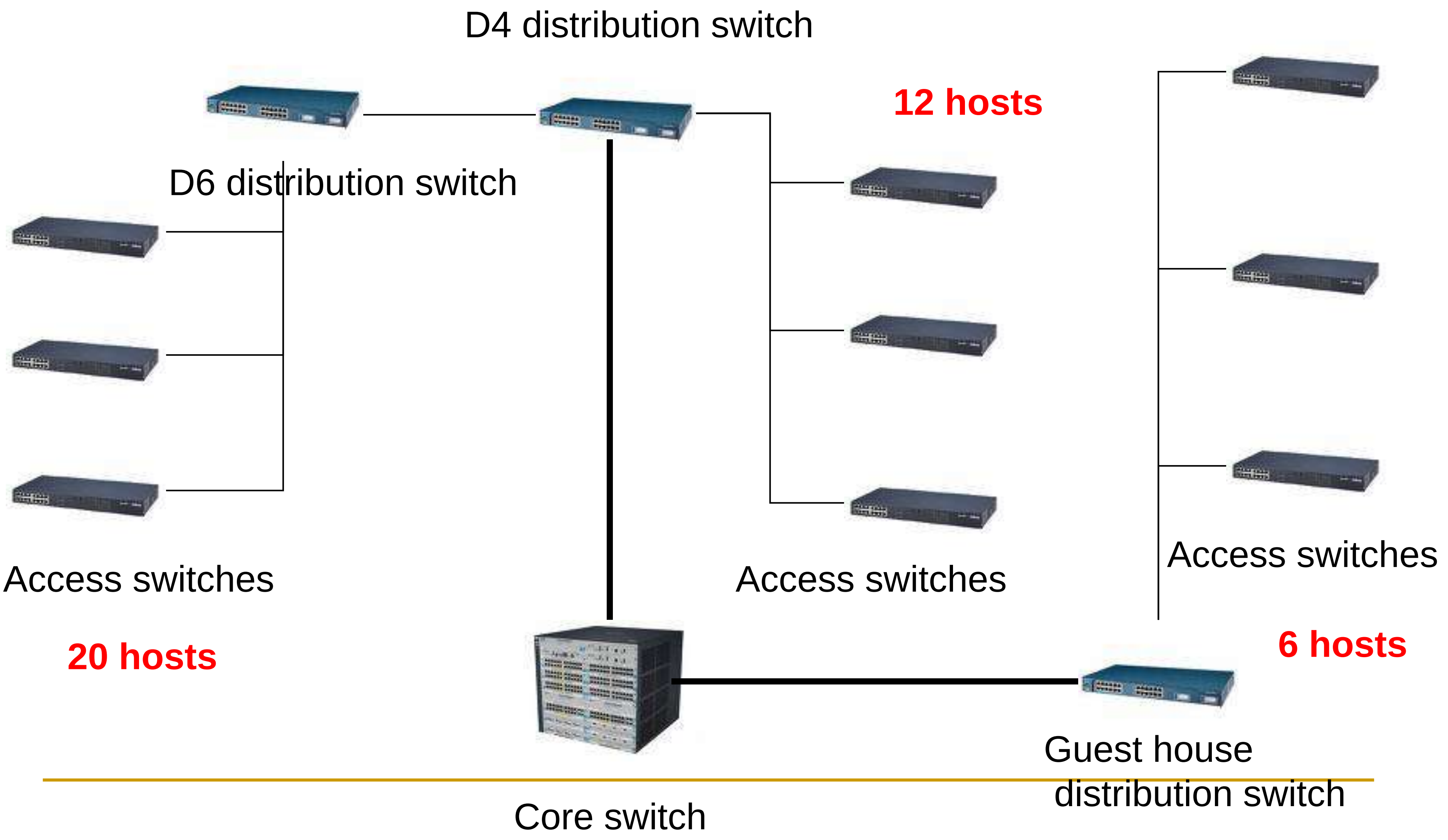
- A **loopback address** is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 though 127.255.255.255 is the broadcast address for 127.0.0.0/8.
- The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets.
- The loopback address 127.0.0.1 is generally known as localhost.

Loopback interface

- A **loopback interface** is a virtual interface in our network device that is always up and active after it has been configured.
- Like our physical interface, we assign a special IP address which is called a loopback address or loopback IP address.

How to assign IP for KTX Network ?

202.151.161.128/26



IP block 202.151.161.128/26
First:202.151.161.128/26 – last: 202.151.161.191/26

- D6 (20 hosts): 255.255.255. 224

  202.151.161.128/27 - **202.151.161.159/27**
- **D4** (12 hosts): 255.255.255. 240

  202.151.161.160/28 - 202.151.161.175/28
- **GH** (6 hosts): 255.255.255. 248

  202.151.161.176/29 - 202.151.161.183/29

Internet Multicasting

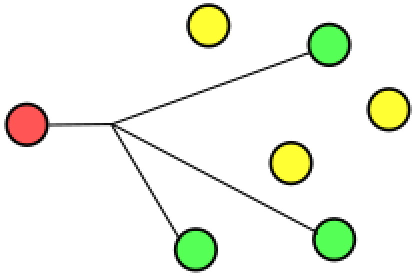
- Ability to send IP datagram's to a large no. of receivers simultaneously
  - Updating replicated databases
  - Transmitting stock quotes to multiple brokers
  - Multiparty video conferencing
- Class D addresses
  - 224.0.0.0 – 239.255.255.255
  - The 28 bits after the leading “1110” in the IP address define the *multicast group address* (2^{28} groups)
  - There is no specific concept of a network ID and host ID as in classes A, B and C

Internet Multicasting

- Two kinds of group addresses are supported
  - Permanent addresses
    - No need to set up permanent addresses
      - Range is from 224.0.0.0 – 224.0.0.255
        - 224.0.0.0 Reserved; not used
        - 224.0.0.1 All systems on a LAN
        - 224.0.0.2 All routers on a LAN
        - 224.0.0.3 Reserved
        - 224.0.0.4 All routers using DVMRP
        - 224.0.0.5 All OSPF routers on a LAN
        - 224.0.0.6 Designated routers using OSPF
        - 224.0.0.9 Designated routers using RIP-2
        - 224.0.0.11 Mobile agents (for Mobile IP)
        - 224.0.0.12 DHCP Server / Relay Agent

Internet Multicasting

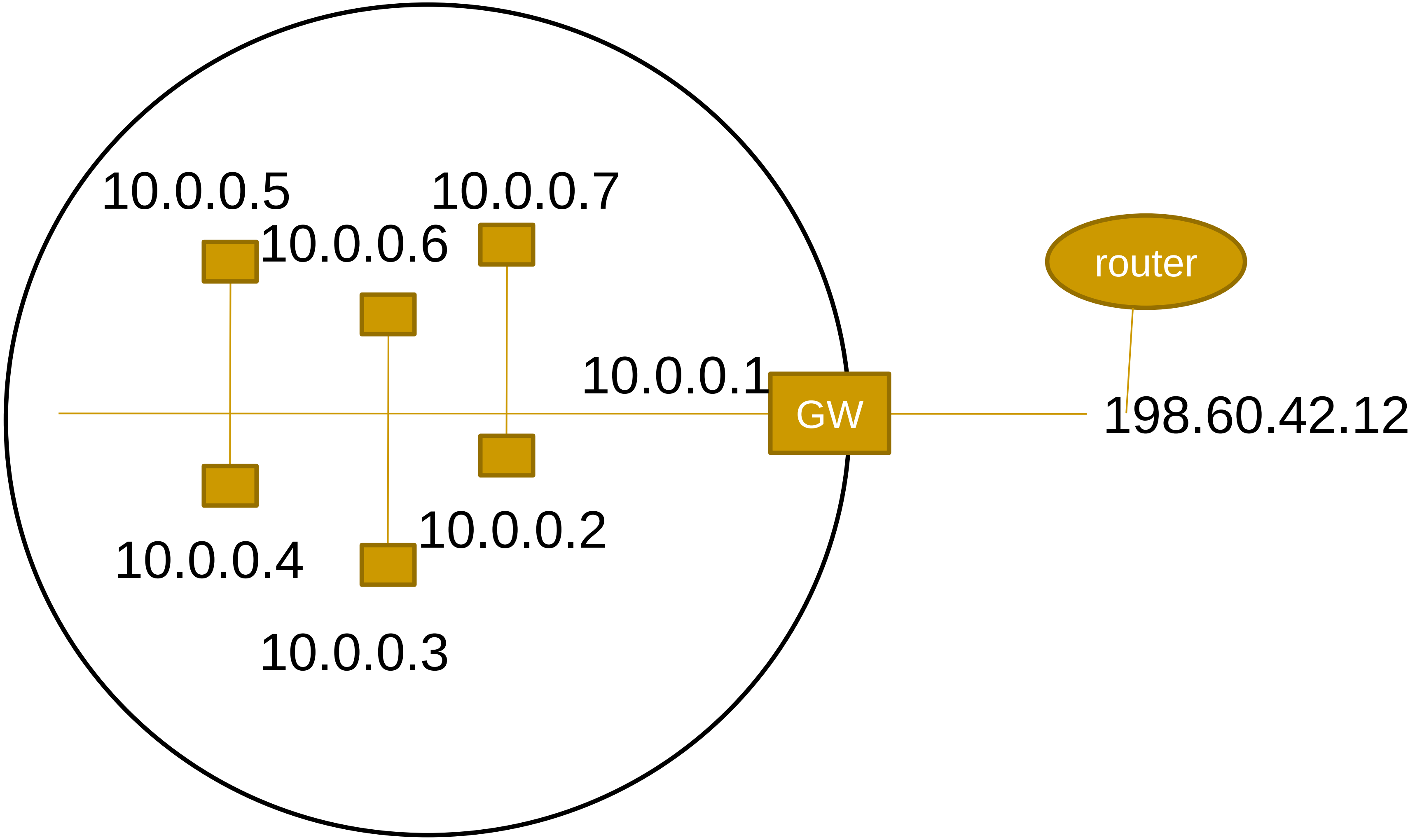
- Temporary addresses
  - Globally-scoped multicast addresses
- Multicasting is implemented by special multicast routers, using a special protocol IGMP (Internet Group Management Protocol)



4. NAT
(Network Address Translation)

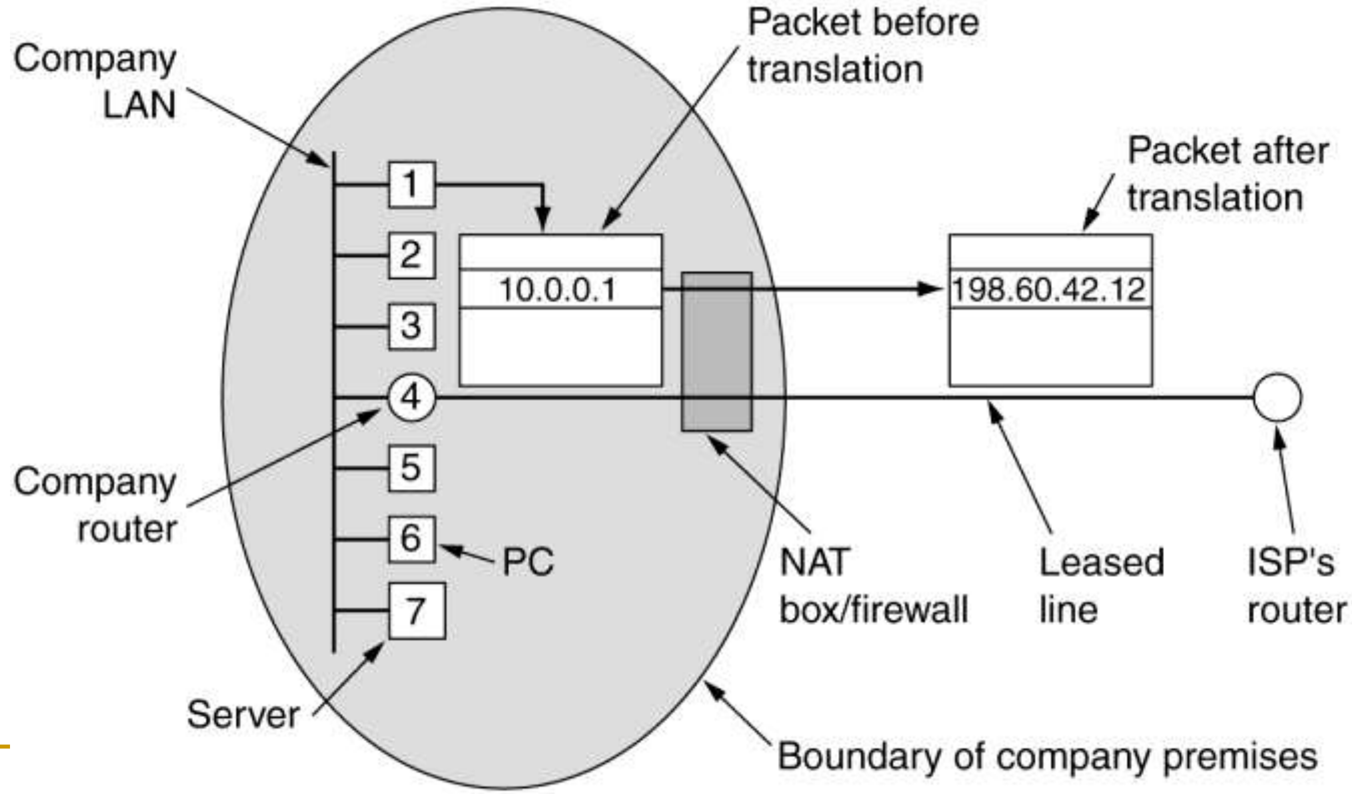
NAT – Network Address Translation

- Reserve a single IP address for local networks that operate behind a special router (which can also operate as a firewall), and allow only **outgoing** connections
  - To make this scheme possible, 3 ranges of IP addresses have been declared private
    - 10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
    - 172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
    - 192.168.0.0 – 192.168.255.255/16 (65,536 hosts)


10.0.0.5
10.0.0.7
10.0.0.6
router
10.0.0.1
GW
198.60.42.12
10.0.0.2
10.0.0.4
10.0.0.3

NAT – Network Address Translation

Placement and operation of a NAT box.



NAT – Network Address Translation

Drawbacks and advantages of NAT:

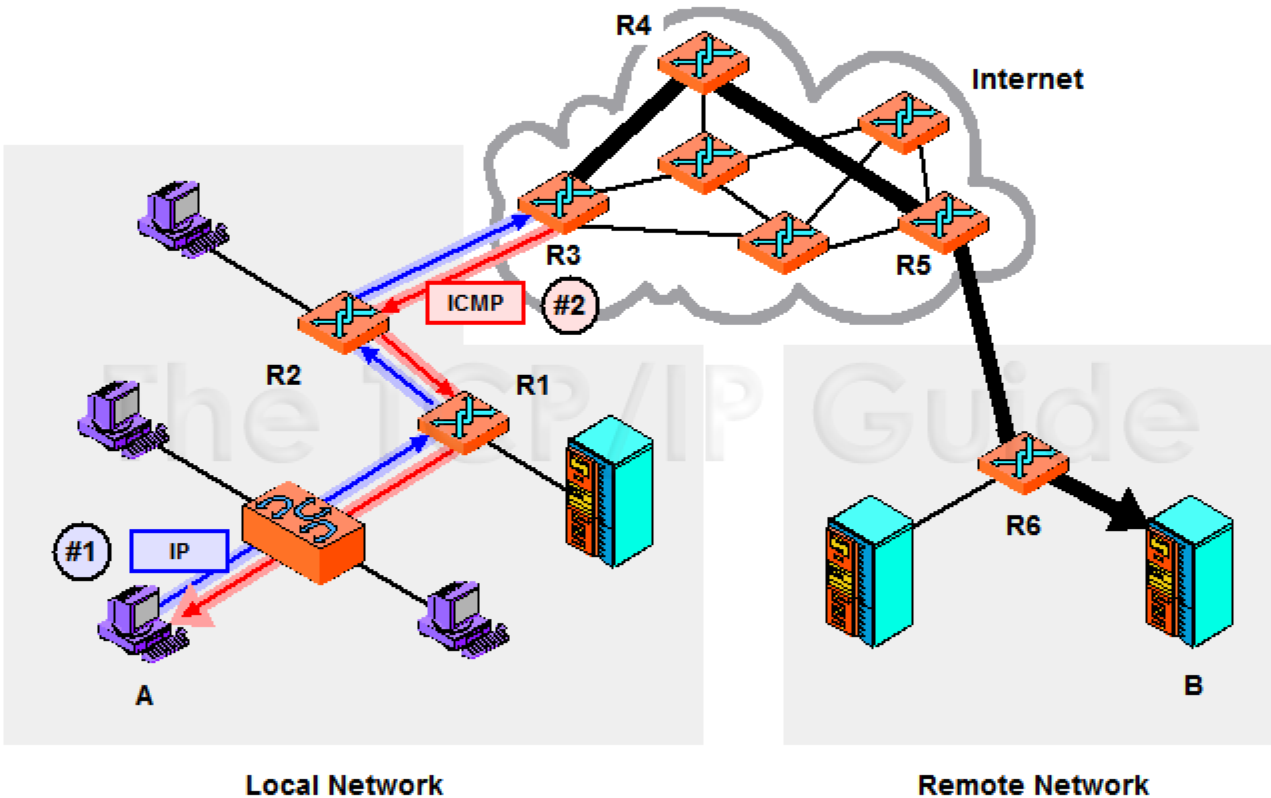
What do you think?

5. Some protocols

ICMP

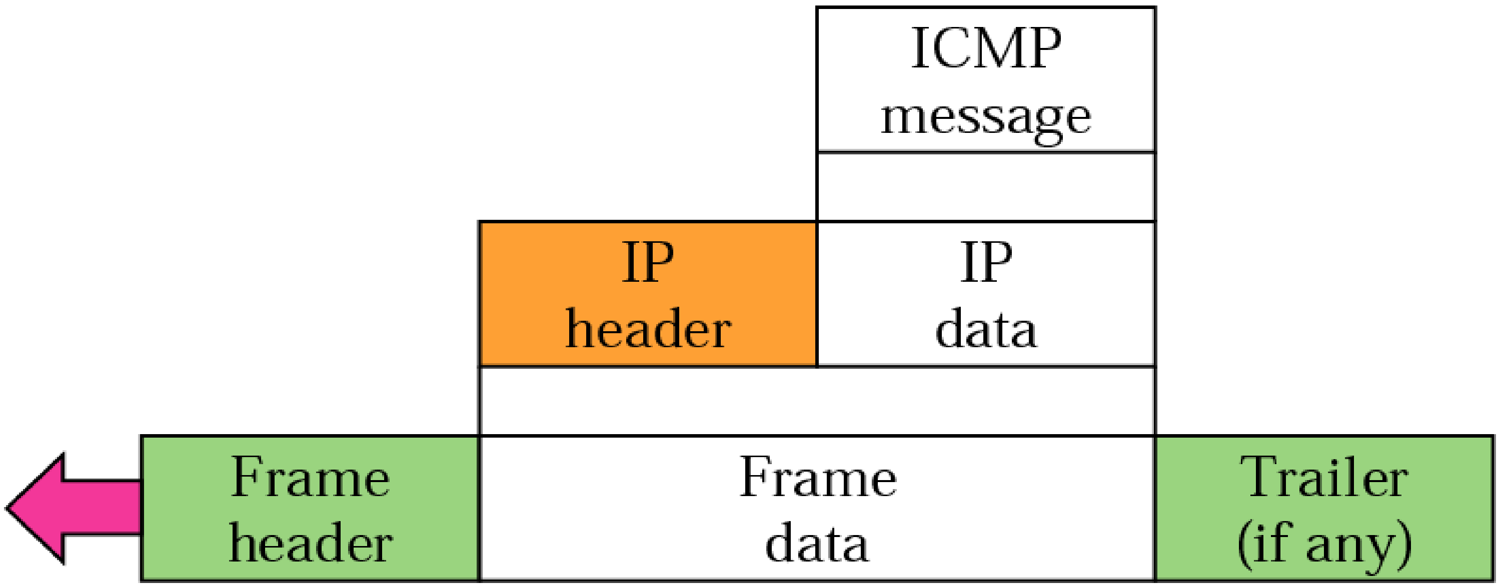
ICMP (Internet Control Message Protocol)

- We need to inform hosts and routers when things go wrong, or, likewise, should be able to send queries to get status information



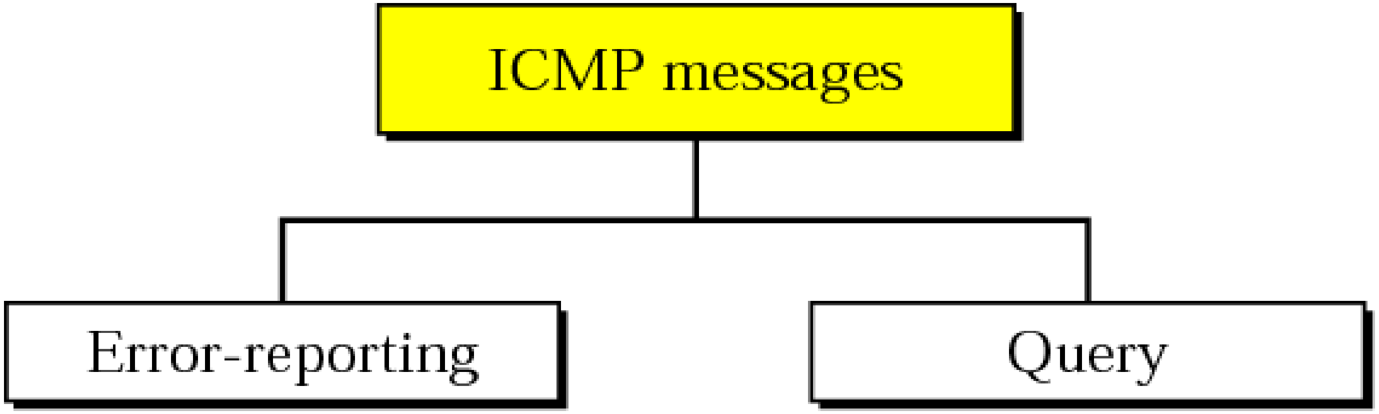
R3 only sends the ICMP message back to *A*, not to *R2* or *R1*

ICMP Encapsulation

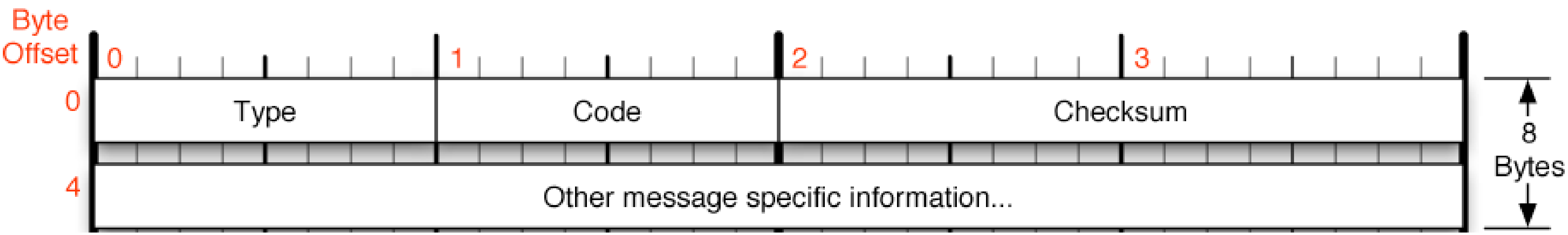


ICMP Message Types

- Each individual kind of message in ICMP is given its own unique *Type* and *Code* values, which are put into the 8 bit fields in the ICMP common message format



ICMP Header



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited

Type	Code/Name
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
	0 TTL Exceeded in Transit
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer indicates the error
	1 Missing a Required Option
	2 Bad Length

Type	Code/Name
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

- Ping
- Nmap
- tracert

ICMP Echo

No.	Time	Source	Destination	Protocol	Info
607	122.229553	192.168.8.135	192.168.8.130	ICMP	Echo (ping) request
608	122.229577	192.168.8.130	192.168.8.135	ICMP	Echo (ping) reply
612	123.229625	192.168.8.135	192.168.8.130	ICMP	Echo (ping) request
613	123.229650	192.168.8.130	192.168.8.135	ICMP	Echo (ping) reply

```
⊞ Frame 607 (98 bytes on wire, 98 bytes captured)
⊟ Ethernet II, Src: Intel_2d:1a:5c (00:11:11:2d:1a:5c), Dst: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
    ⊞ Destination: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
    ⊞ Source: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
      Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.8.135 (192.168.8.135), Dst: 192.168.8.130 (192.168.8.130)
      Version: 4
      Header length: 20 bytes
    ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      Total Length: 84
      Identification: 0x0000 (0)
    ⊞ Flags: 0x04 (Don't Fragment)
      Fragment offset: 0
      Time to live: 1
      Protocol: ICMP (0x01)
    ⊞ Header checksum: 0xe74f [correct]
      Source: 192.168.8.135 (192.168.8.135)
      Destination: 192.168.8.130 (192.168.8.130)
⊟ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x25e3 [correct]
      Identifier: 0x330a
      Sequence number: 5 (0x0005)
      Data (56 bytes)
```

ICMP Echo Reply

No.	Time	Source	Destination	Protocol	Info
607	122.229553	192.168.8.135	192.168.8.130	ICMP	Echo (ping) request
608	122.229577	192.168.8.130	192.168.8.135	ICMP	Echo (ping) reply
612	123.229625	192.168.8.135	192.168.8.130	ICMP	Echo (ping) request
613	123.229650	192.168.8.130	192.168.8.135	ICMP	Echo (ping) reply

```
⊞ Frame 608 (98 bytes on wire, 98 bytes captured)
⊟ Ethernet II, Src: Micro-St_ee:54:6f (00:11:09:ee:54:6f), Dst: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
    ⊞ Destination: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
    ⊞ Source: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
      Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.8.130 (192.168.8.130), Dst: 192.168.8.135 (192.168.8.135)
      Version: 4
      Header length: 20 bytes
    ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      Total Length: 84
      Identification: 0xd5fe (54782)
    ⊞ Flags: 0x04 (Don't Fragment)
      Fragment offset: 0
      Time to live: 128
      Protocol: ICMP (0x01)
    ⊞ Header checksum: 0x9250 [correct]
      Source: 192.168.8.130 (192.168.8.130)
      Destination: 192.168.8.135 (192.168.8.135)
⊟ Internet Control Message Protocol
      Type: 0 (Echo (ping) reply)
      Code: 0
      Checksum: 0x2de3 [correct]
      Identifier: 0x330a
      Sequence number: 5 (0x0005)
      Data (56 bytes)
```

ICMP Echo with TTL = 1

No.	Time	Source	Destination	Protocol	Info
3	2.237394	192.168.8.130	10.10.4.65	ICMP	Echo (ping) request
4	2.237867	192.168.8.2	192.168.8.130	ICMP	Time-to-live exceeded (Time to live exceeded in transit

```
⊞ Frame 3 (74 bytes on wire, 74 bytes captured)
⊟ Ethernet II, Src: Micro-St_ee:54:6f (00:11:09:ee:54:6f), Dst: Cisco_1a:de:c7 (00:14:a8:1a:de:c7)
  ⊞ Destination: Cisco_1a:de:c7 (00:14:a8:1a:de:c7)
  ⊞ Source: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.8.130 (192.168.8.130), Dst: 10.10.4.65 (10.10.4.65)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0xd649 (54857)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0x0c03 [correct]
    Source: 192.168.8.130 (192.168.8.130)
    Destination: 10.10.4.65 (10.10.4.65)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x405c [correct]
    Identifier: 0x0200
    Sequence number: 2816 (0x0b00)
    Data (32 bytes)
```

ICMP TTL Exceeded

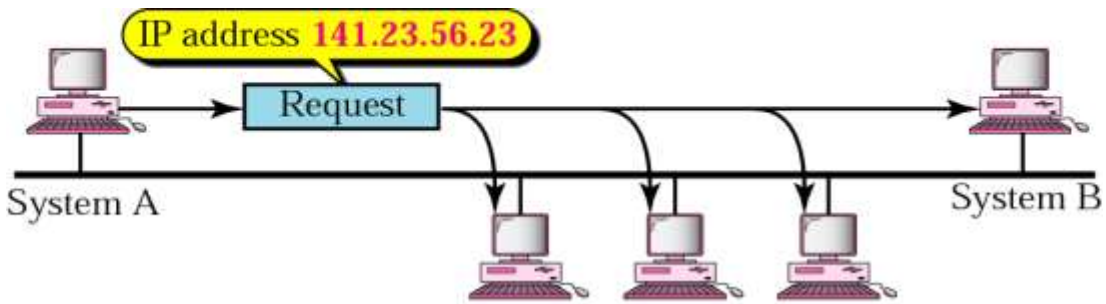
No.	Time	Source	Destination	Protocol	Info
3	2.237394	192.168.8.130	10.10.4.65	ICMP	Echo (ping) request
4	2.237867	192.168.8.2	192.168.8.130	ICMP	Time-to-live exceeded (Time to live exceeded in transit

```
⊞ Frame 6 (70 bytes on wire, 70 bytes captured)
⊞ Ethernet II, Src: Cisco_1a:de:c7 (00:14:a8:1a:de:c7), Dst: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
⊞ Internet Protocol, Src: 192.168.8.2 (192.168.8.2), Dst: 192.168.8.130 (192.168.8.130)
⊟ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x9fa3 [correct]
```

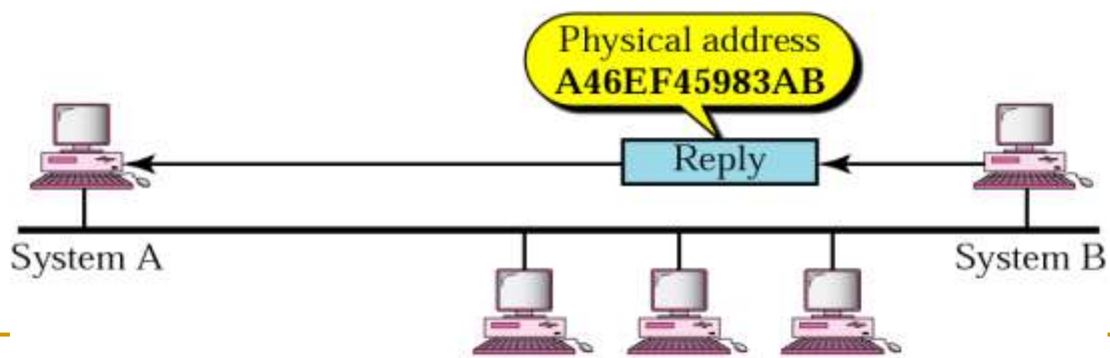
ARP

ARP (Address Resolution Protocol)

- Problem: Logical-to-Physical address mapping
  - Static Solution: a mapping database
  - Dynamic Solution: ARP
    - Broadcast request/Unicast reply



a. ARP request is broadcast



b. ARP reply is unicast

ARP Broadcast Request

No.	Time	Source	Destination	Protocol	Info
9	2.959786	Intel_2d:1a:5c	Broadcast	ARP	Who has 192.168.8.130? Tell 192.168.8.135
10	2.959794	Micro-St_ee:54:6f	Intel_2d:1a:5c	ARP	192.168.8.130 is at 00:11:09:ee:54:6f

```
⊞ Frame 9 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: Intel_2d:1a:5c (00:11:11:2d:1a:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ⊞ Source: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
     Type: ARP (0x0806)
     Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
     Hardware type: Ethernet (0x0001)
     Protocol type: IP (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: request (0x0001)
     Sender MAC address: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
     Sender IP address: 192.168.8.135 (192.168.8.135)
     Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
     Target IP address: 192.168.8.130 (192.168.8.130)
```

ARP Unicast Reply

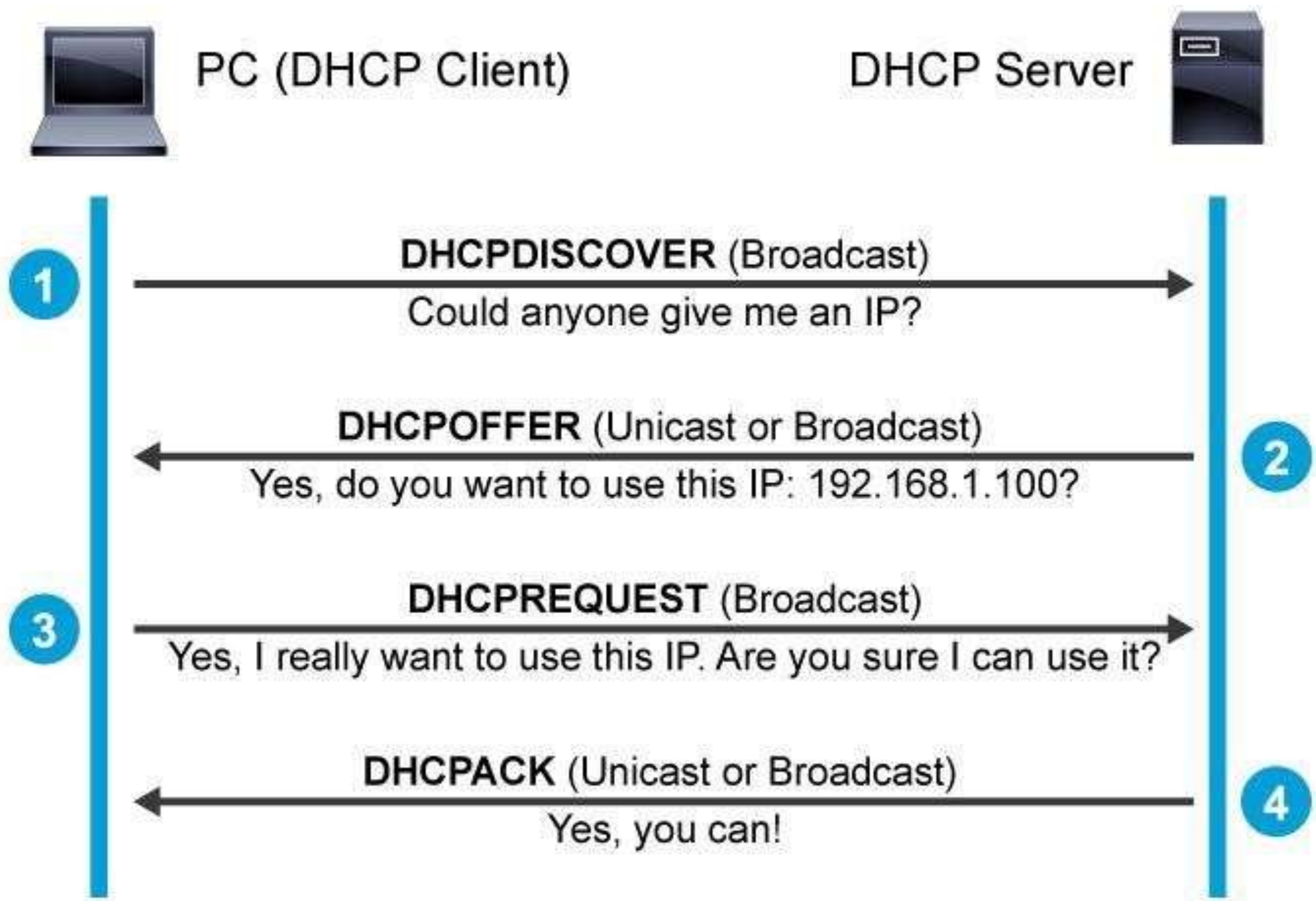
No.	Time	Source	Destination	Protocol	Info
9	2.959786	Intel_2d:1a:5c	Broadcast	ARP	Who has 192.168.8.130? Tell 192.168.8.135
10	2.959794	Micro-St_ee:54:6f	Intel_2d:1a:5c	ARP	192.168.8.130 is at 00:11:09:ee:54:6f

```
⊞ Frame 10 (42 bytes on wire, 42 bytes captured)
⊟ Ethernet II, Src: Micro-St_ee:54:6f (00:11:09:ee:54:6f), Dst: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
  ⊞ Destination: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
  ⊞ Source: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: Micro-St_ee:54:6f (00:11:09:ee:54:6f)
    Sender IP address: 192.168.8.130 (192.168.8.130)
    Target MAC address: Intel_2d:1a:5c (00:11:11:2d:1a:5c)
    Target IP address: 192.168.8.135 (192.168.8.135)
```

DHCP

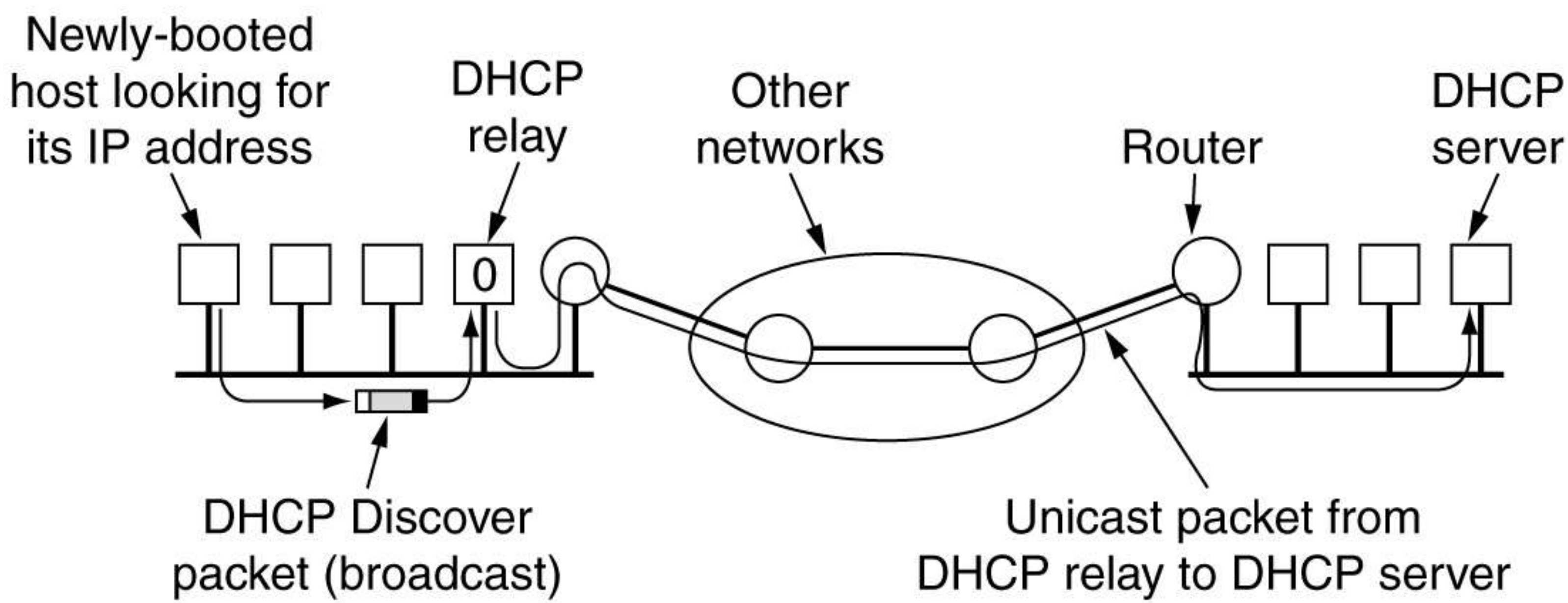
Dynamic Host Configuration Protocol

- DHCP allows both manual and automatic address assignments



Dynamic Host Configuration Protocol

- DHCP may not be reachable by broadcasting, so a DHCP Relay Agent is needed on each LAN



Dynamic Host Configuration Protocol

- DHCP may not be reachable by broadcasting, so a DHCP Relay Agent is needed on each LAN