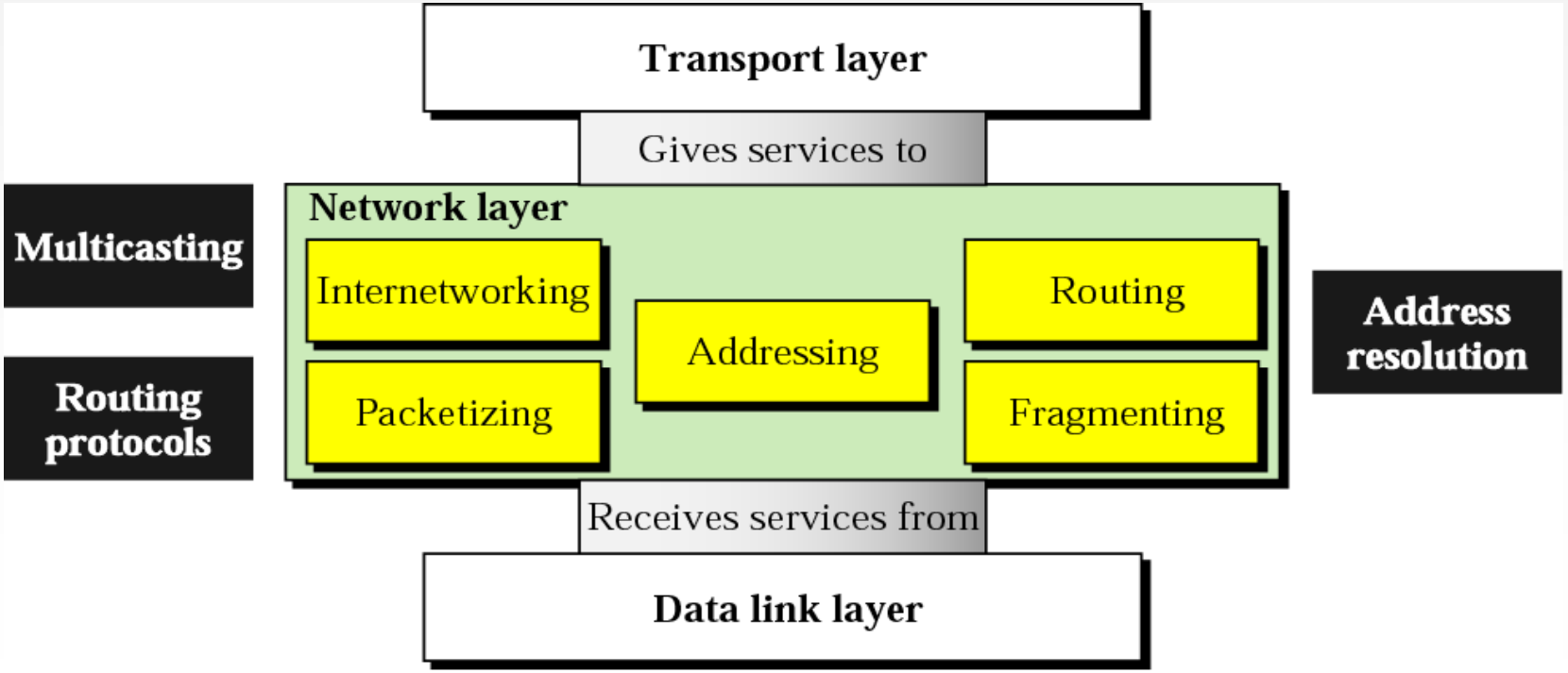
Network Layer

Position of Network Layer

- The network layer is responsible for the delivery of individual packets from the source to the destination host



Network Layer (Internetwork Protocol: IP)

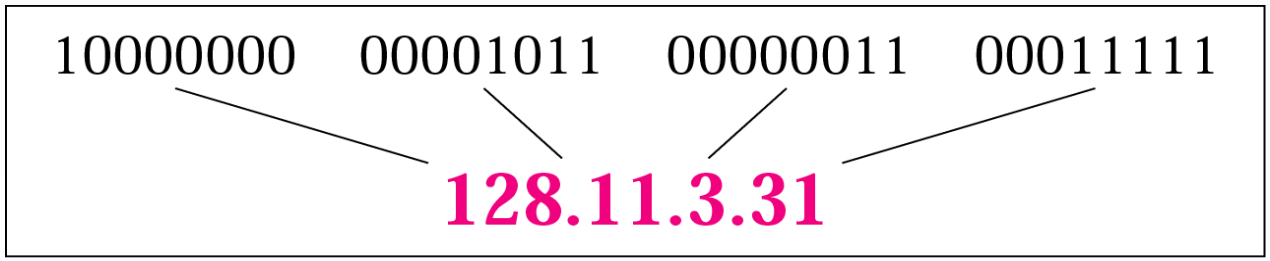
- IP is transmission mechanism for TCP/IP protocols.
  - Unreliable
  - Connectionless datagram protocol
  - No error checking and tracking (of whole data packet)
  - Best effort to destine a packet, but no guarantee
  - For reliability, paired with TCP

IP Datagram:

- Packets at IP layer are called datagrams
- IP datagrams:
  - Transported separately
  - May travel along different routes
  - May arrive out of sequence
  - As a connectionless, no call set up is required
  - Variable length (up to 65536 bytes)
    - 20 to 40 bytes header

IPv4 Addresses:

- An IP address is a 32-bits long
- The IP addresses are unique and universal
- The address space of IPv4 is 2^{32} or 4,294,967,296
- Binary notation: e.g. 01110101 10010101 00011101 00000010
- Dotted-decimal notation: 117.149.29.2



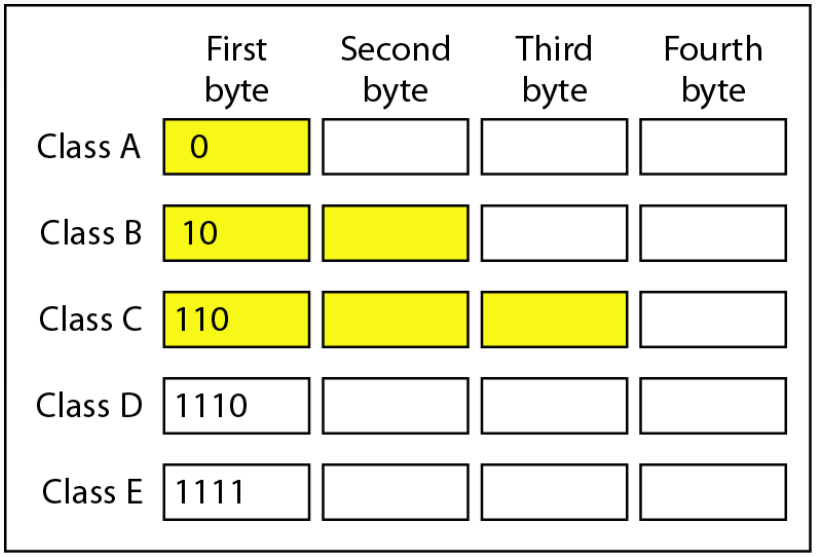
Example

- Change the following IP addresses from binary notation to dotted-decimal notation.
    a. 10000001 00001011 00001011 11101111
    b. 11111001 10011011 11111011 00001111

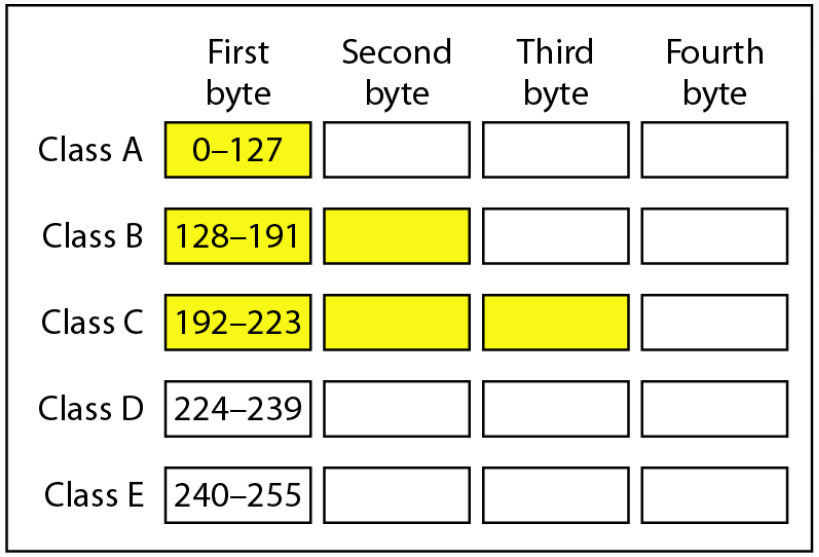
- We replace each group of 8 bits with its equivalent decimal number and add dots for separation:
    a. 129.11.11.239
    b. 249.155.251.15

Classful Addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, E
- A new architecture, called classless addressing was introduced in the mid-1990s

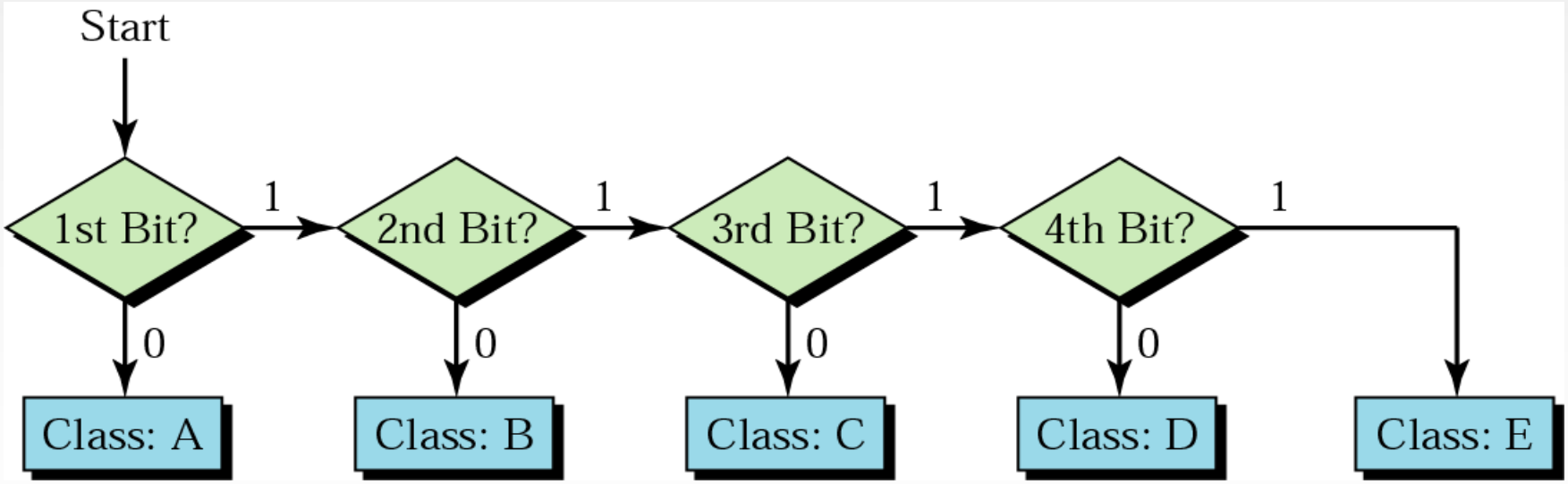


a. Binary notation

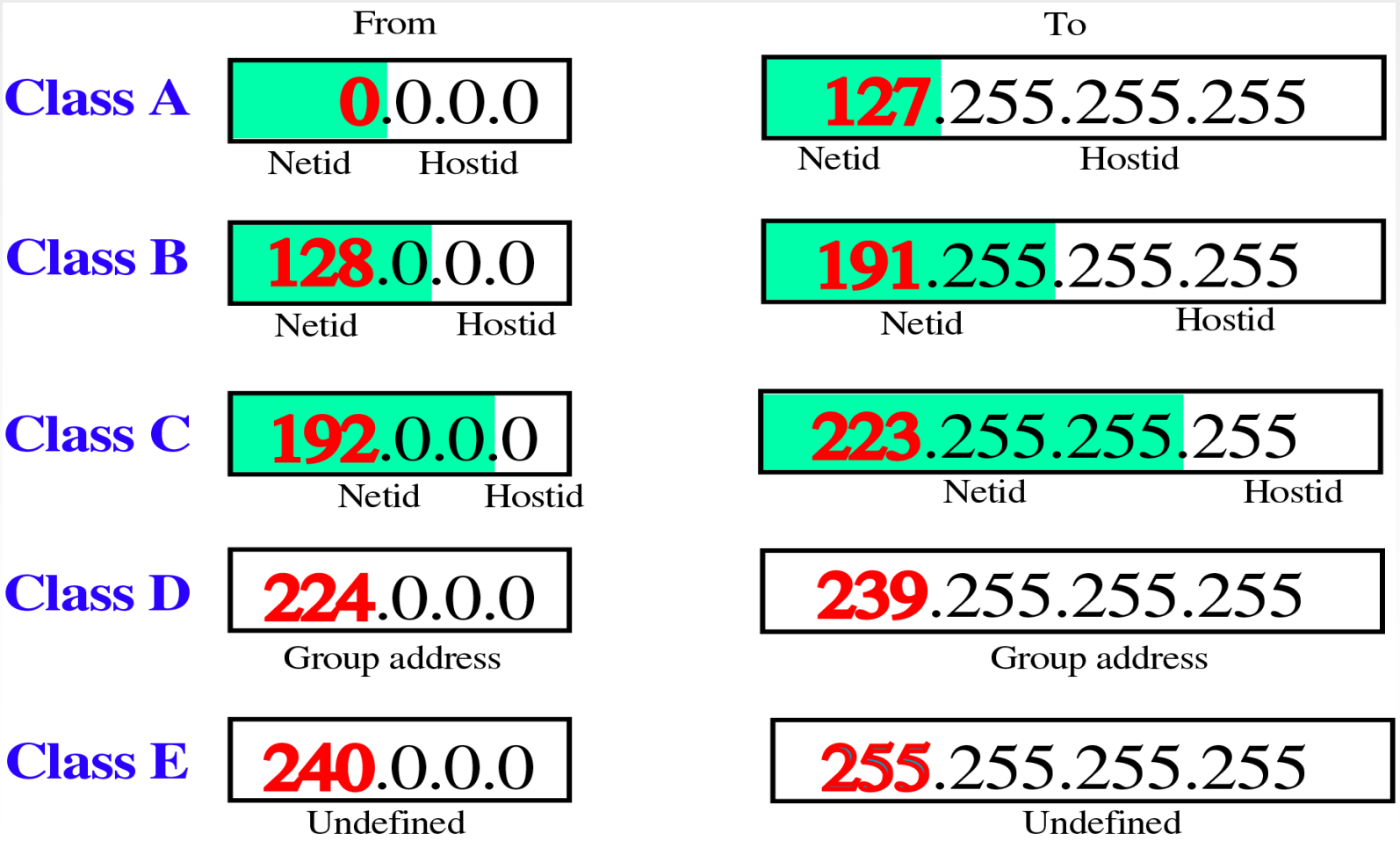


b. Dotted-decimal notation

Finding the address class



Class Ranges of Internet Addresses:

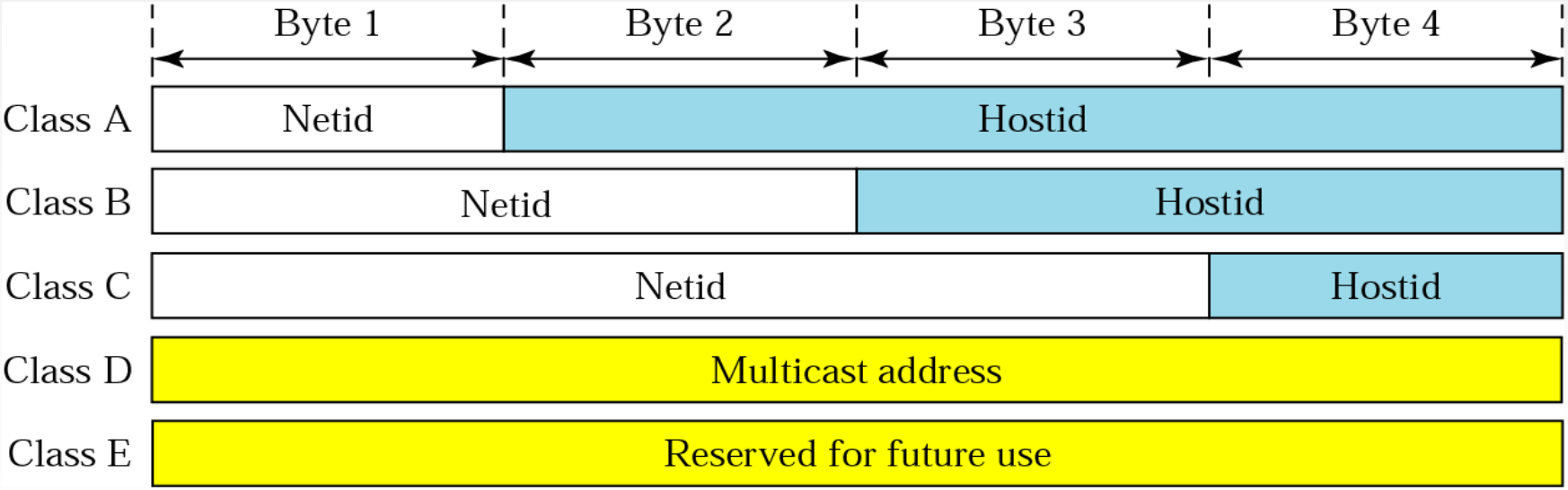


Classful Addressing: Example

- Find the class of each address.
  a. 00000001 00001011 00001011 11101111
  b. 11000001 10000011 00011011 11111111
  c. 14.23.120.8
  d. 252.5.15.111
- Solution
  a. The first bit is 0. This is a class A address.
  b. The first 2 bits are 1; the third bit is 0. This is a class C address.
  c. The first byte is 14; the class is A.
  d. The first byte is 252; the class is E.

Netid and Hostid

- IP address in classes A, B, and C is divided into netid and hostid



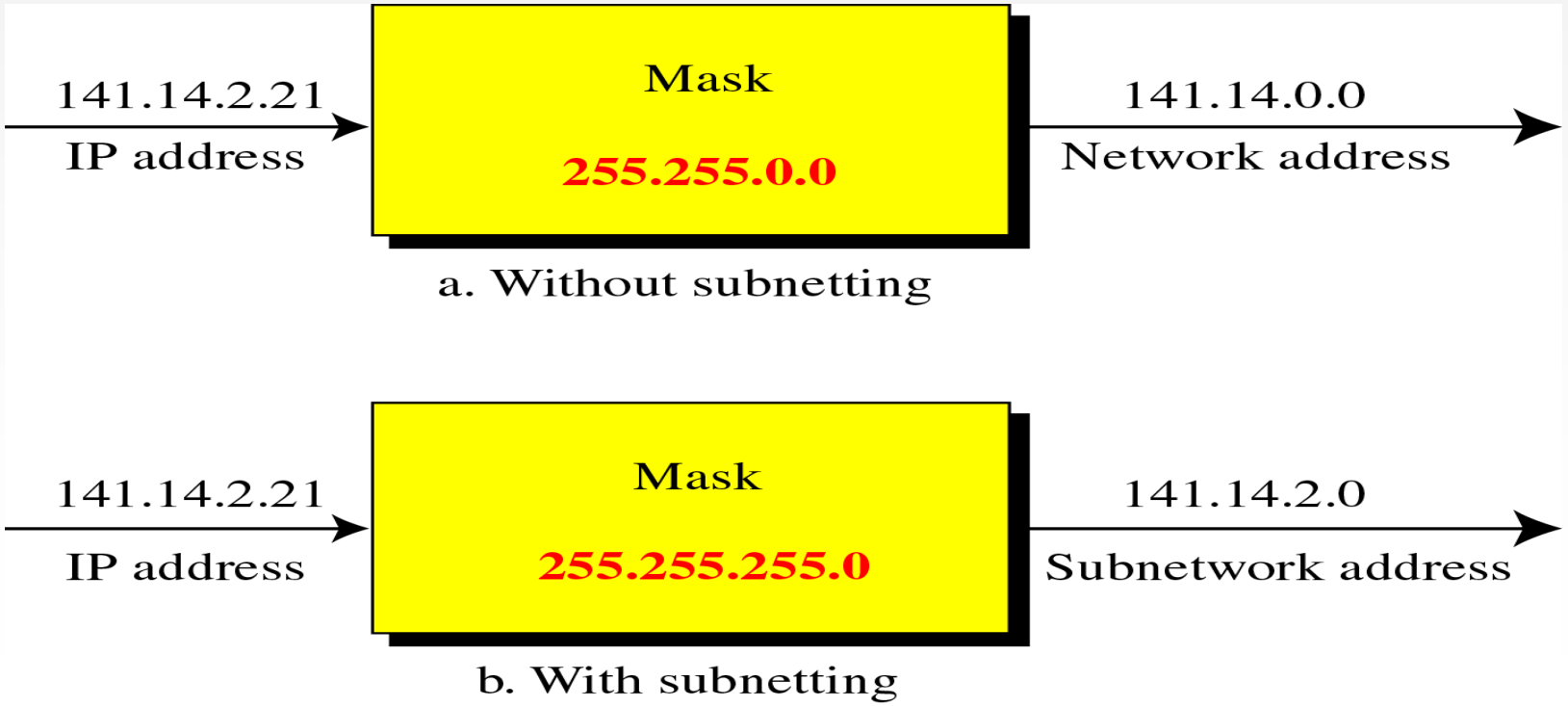
Class Ranges of Internet Addresses:

- All 0's and all 1's are reserved for special functions

Class	Number of Networks	Number of Hosts
A	$2^{7}-1=127$	$2^{24}-2=16,777,214$
B	$2^{14}=16,384$	$2^{16}-2=65,534$
C	$2^{21}=2,097,152$	$2^{8}-2=254$
D, E	Not applicable	Not applicable

Masking:

- A process that extracts the address of the actual network from IP address



Masking:

- Boundary Level Masking:
  - Mask numbers are either 0 or 255
- No boundary Level Masking:
  - Any number between 0 and 255
  - Finding the subnetwork address involves bit wise AND operation

IP Address:	45.123.21.8
Mask:	255.192.0.0
Subnetwork Address:	45.64.0.0

- Classless Inter Domain Routing (CIDR):
  - a.b.c.d/x, x = No. bits in netid

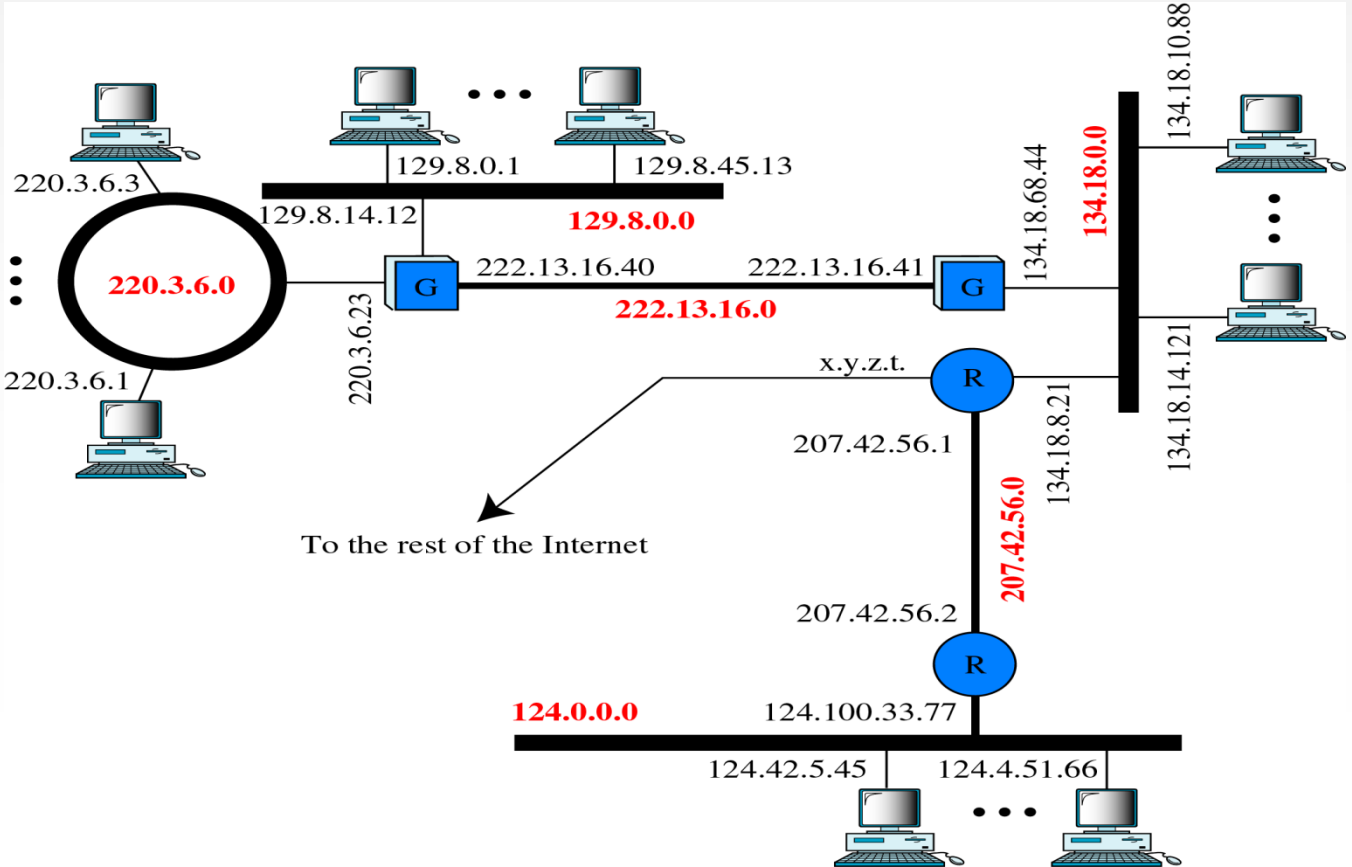
Mask: Default Mask

- The length of the netid and hostid is predetermined in classful addressing
- Default masking
- CIDR notation

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	**11111111** 00000000 00000000 00000000	**255**.0.0.0	/8
B	**11111111 11111111** 00000000 00000000	**255.255**.0.0	/16
C	**11111111 11111111 11111111** 00000000	**255.255.255**.0	/24

Network and Host Addresses:

- Any device connected to more than one network/router, must have more than one IP address



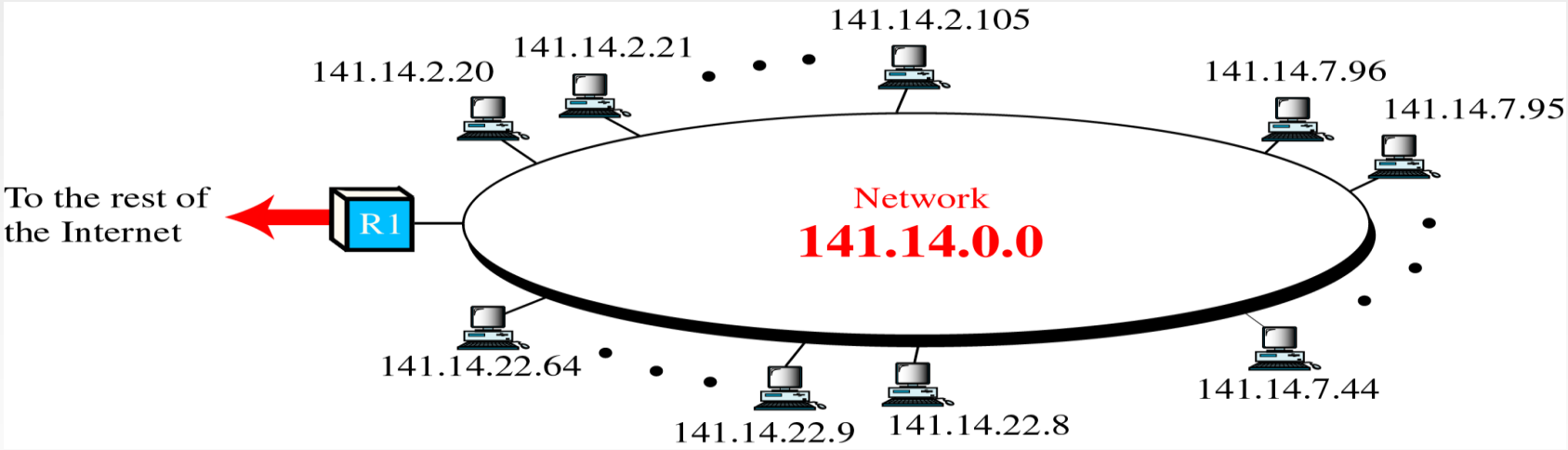
Subnetting

- Divide a large block of addresses into several contiguous groups and assign each group to smaller networks called subnets
- Increase the number of 1s in the mask

Network Address

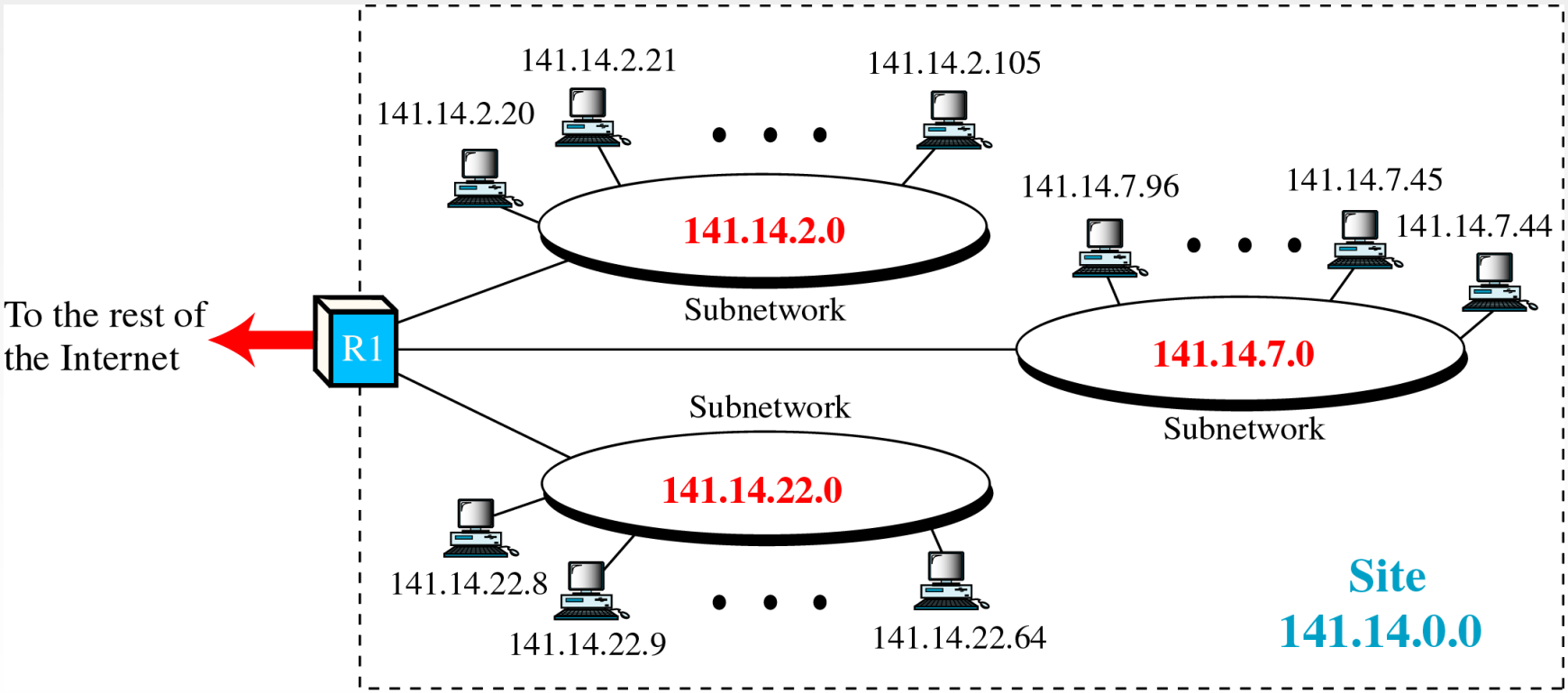
- The first address in a block is normally not assigned to any device
- It is used as the network address that represents the organization to the rest of the world

Two-Level Hierarchy: No Subnetting

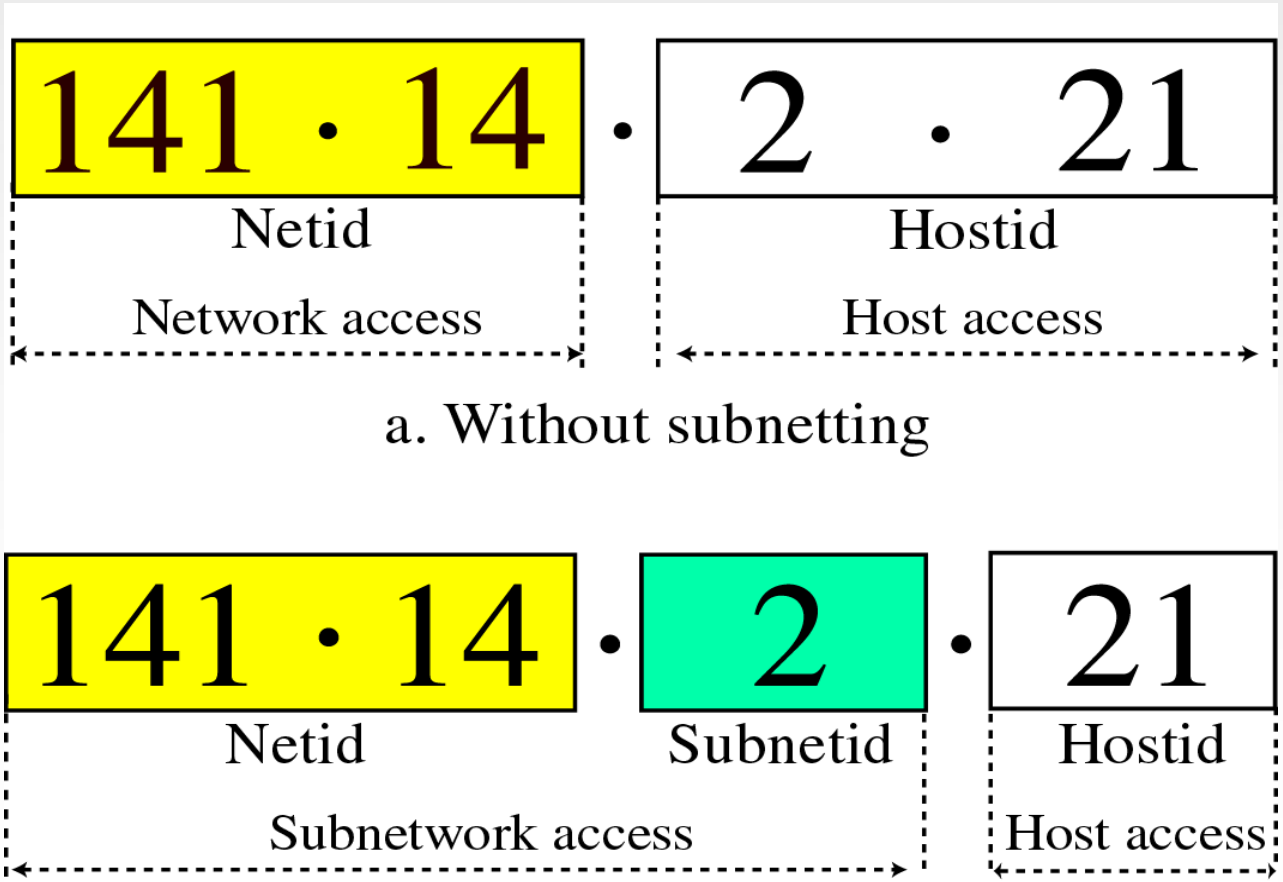


- Only one network (141.14.0.0)
- No grouping/level
- In many cases, two level hierarchy is not enough.

A Network with Three Levels of Hierarchy:
(With Subnetting)



Addresses with and without Subnetting:



IP Addressing:

- A software address (not hardware like NIC)
- Allows to communicate a host on network to host on different network
- Network address: e.g. 10.0.0.0, 172.16.0.0, 192.168.0.0
- Broadcast address: To send a message to all the hosts in that network. e.g.
  - 255.255.255.255 for broadcasting to all host on internet
  - 172.16.255.255 for broadcasting to all host on 172.16.0.0
  - 10.255.255.255 for broadcasting to all host on 10.0.0.0

Private IP Addresses:

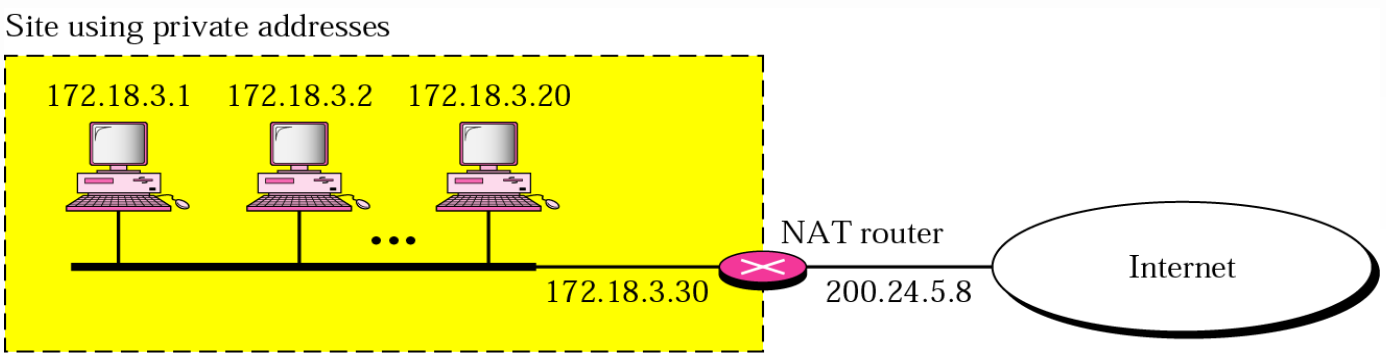
- Can be used in private networks but are not routable through the Internet
- Network Address translation (NAT) is used to convert private IP addresses to public IPs, which are acceptable on Internet.
- Private IPs:
  - Class A: 10.0.0.0 through 10.255.255.255
  - Class B: 172.16.0.0 through 172.31.255.255
  - Class C: 192.168.0.0 through 192.168.255.255

Network Address Translation: NAT

- NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

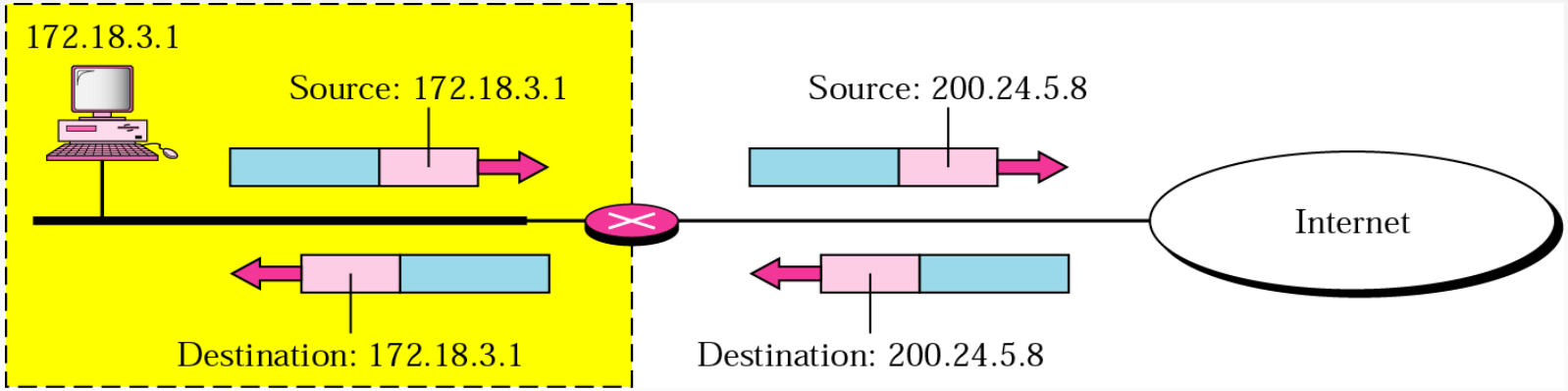
Addresses for private networks

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}



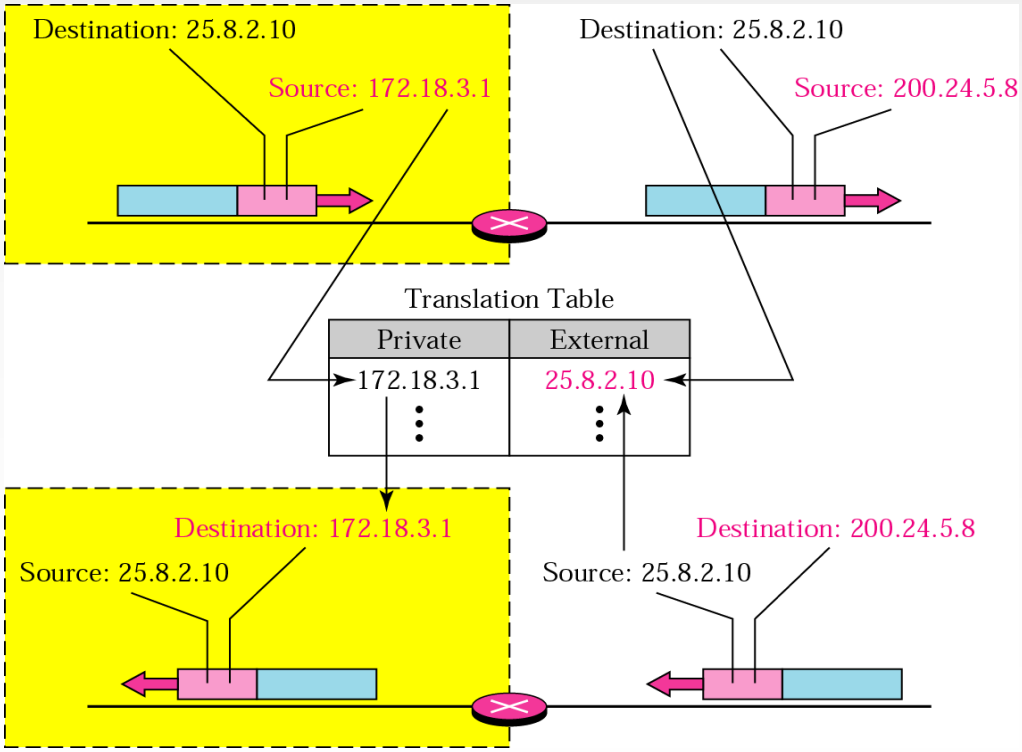
Addresses Translation

- Address translation for source address of outgoing packet and for destination address of incoming packet



Translation Table

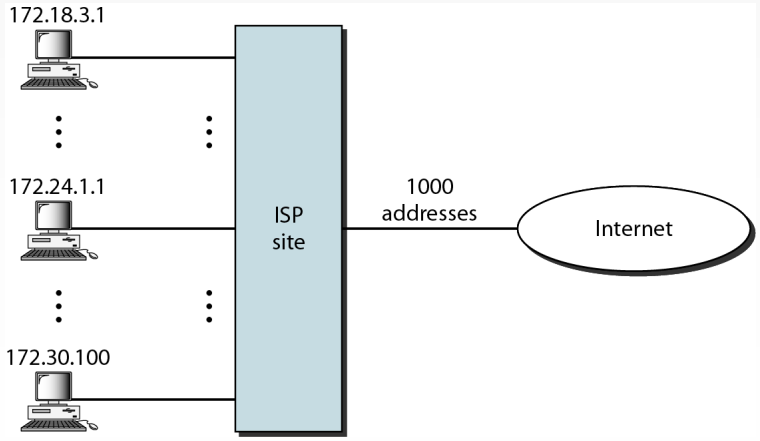
- Using (1) one IP address, (2) a pool of IP address, and (3) both IP addresses and port numbers



Five-Column Translation Table

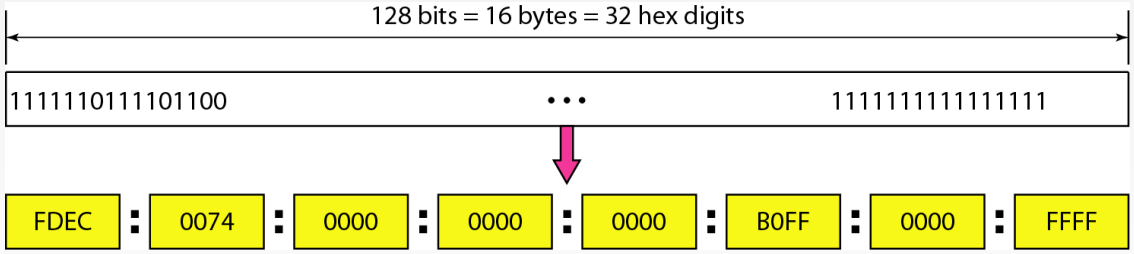
Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
. . .	. . .	. . .	. . .	. . .

ISP and NAT

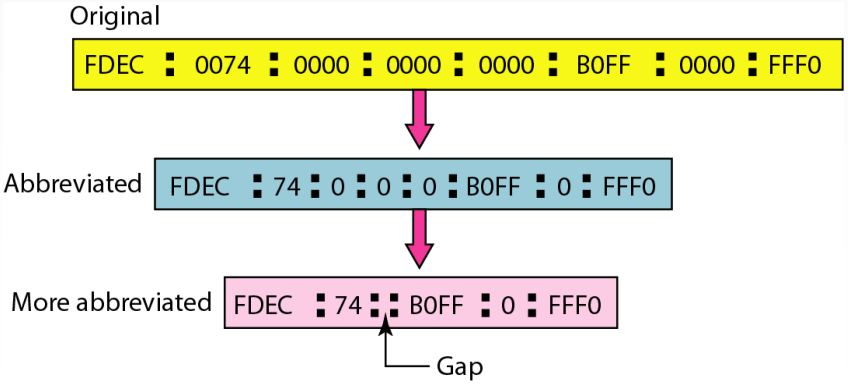


IPv6 Addresses

- Despite all short-term solutions, such as classless addressing, DHCP (Dynamic Host Configuration Protocol), and NAT, still address-hungry
- An IPv6 address is 128 bits long
- Hexadecimal colon notation:

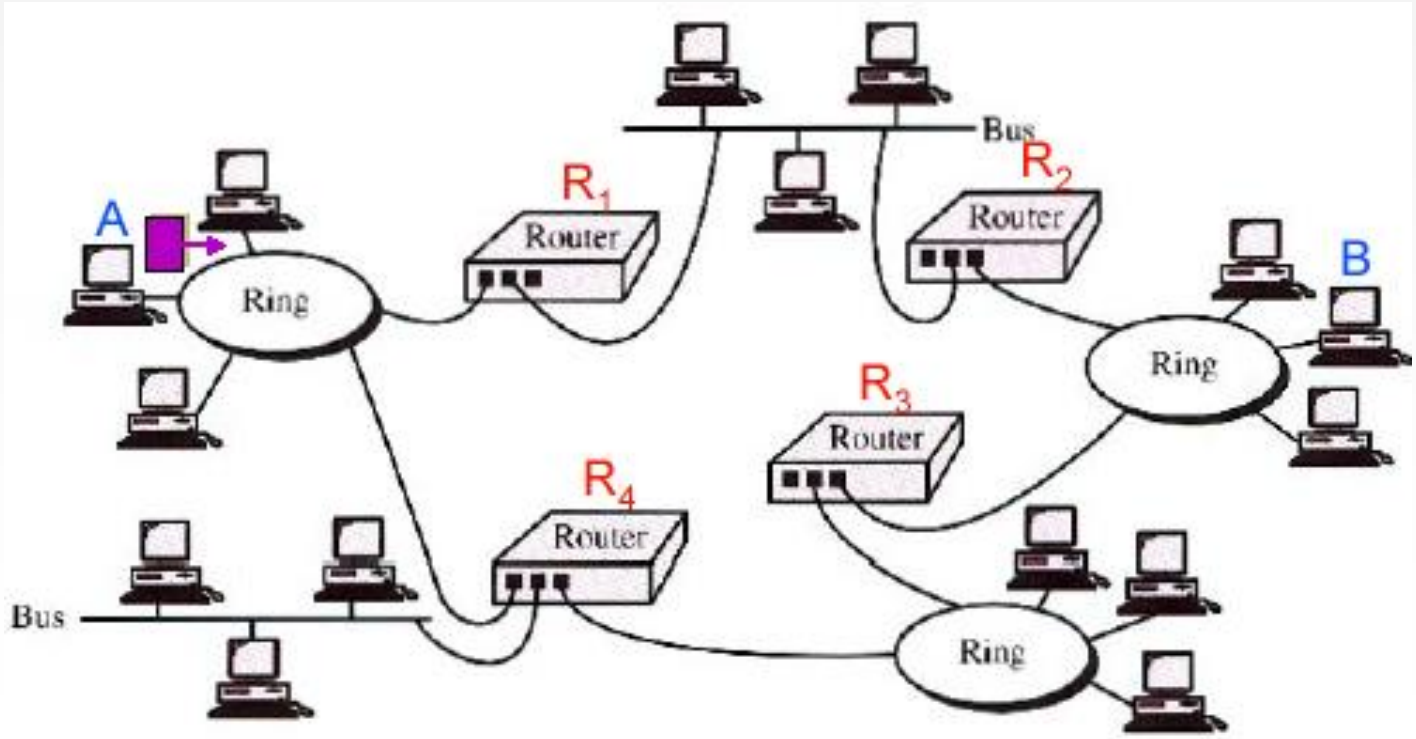


- Abbreviation:

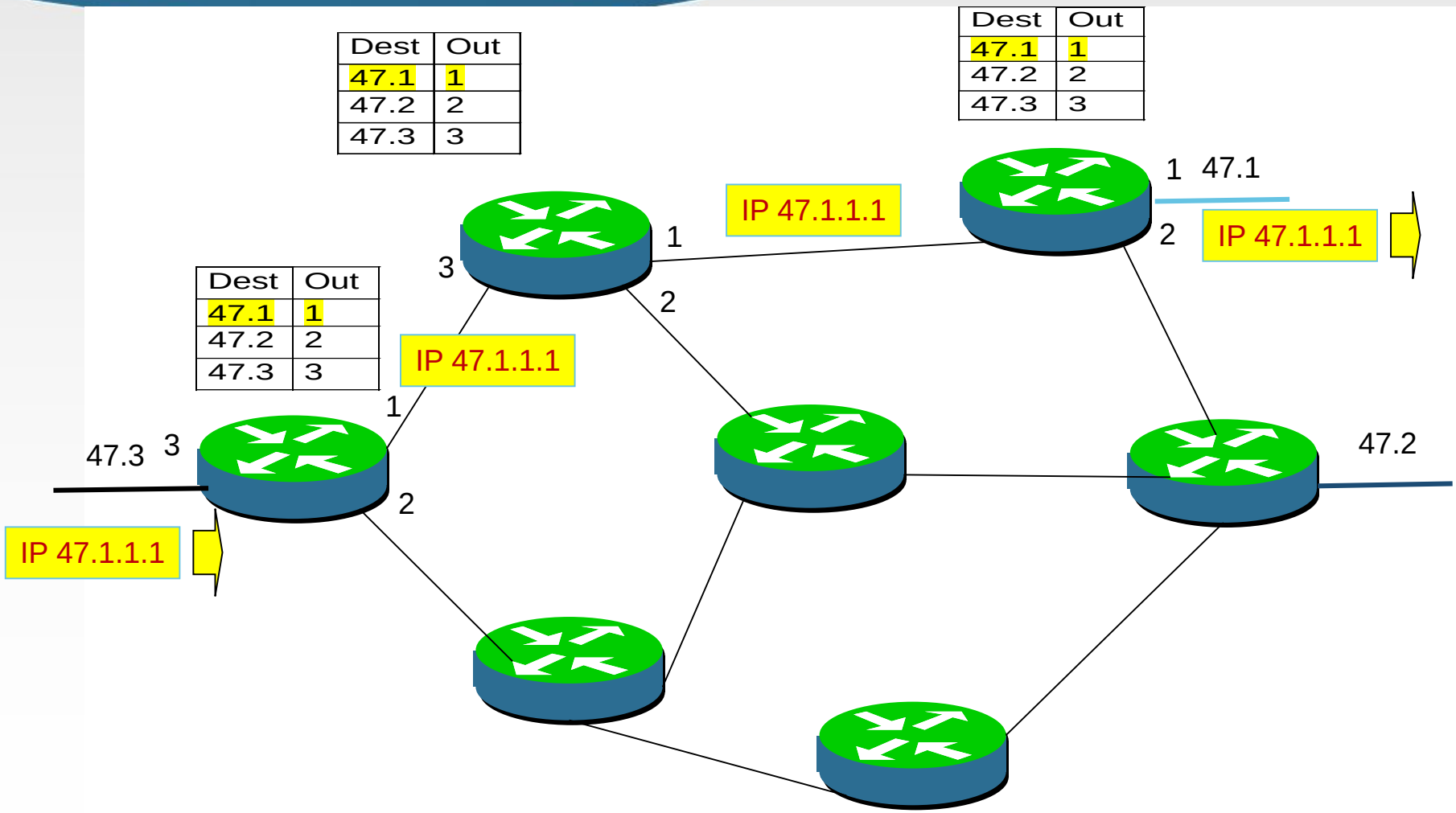


Routing:

- Process of moving packets from one network to another along the path from source to the destination.



IP Routing:


Dest
Out
47.1
1
47.2
2
47.3
3
Dest
Out
47.1
1
47.2
2
47.3
3
Dest
Out
47.1
1
47.2
2
47.3
3
1
47.1
2
IP 47.1.1.1
IP 47.1.1.1
3
1
2
IP 47.1.1.1
1
47.3
3
2
47.2
IP 47.1.1.1

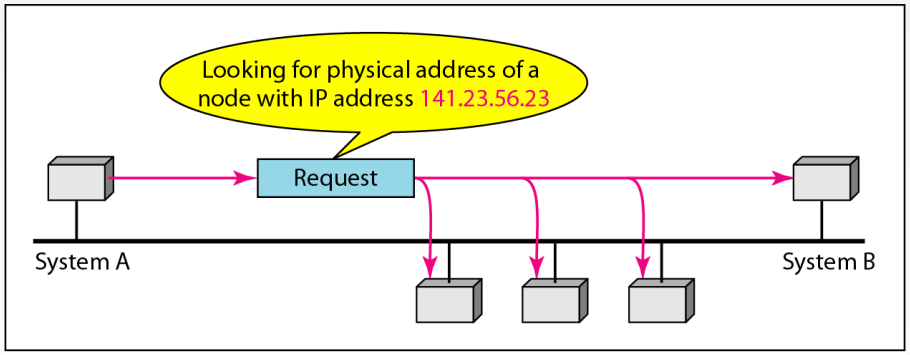
Network Layer: Address Mapping, Error Reporting, and Multicasting

Address Resolution Protocol (ARP)

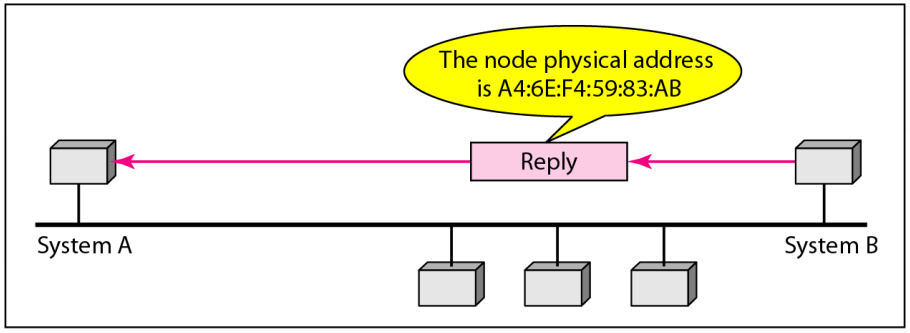
- Two levels of addresses: Physical address (local address: MAC address) and Logical address (network address: IP address)
- Need to be able to map an IP address to its corresponding MAC address
- Two types of mapping : static and dynamic
- Static mapping has some limitations
- Dynamic mapping: ARP and RARP
- ARP: mapping IP address to a MAC address
- RARP (replaced by DHCP): mapping a MAC address to an IP address

ARP operation

- ARP associates an IP address with its MAC addresses
- An ARP request is broadcast; an ARP reply is unicast.
- ARP Cache



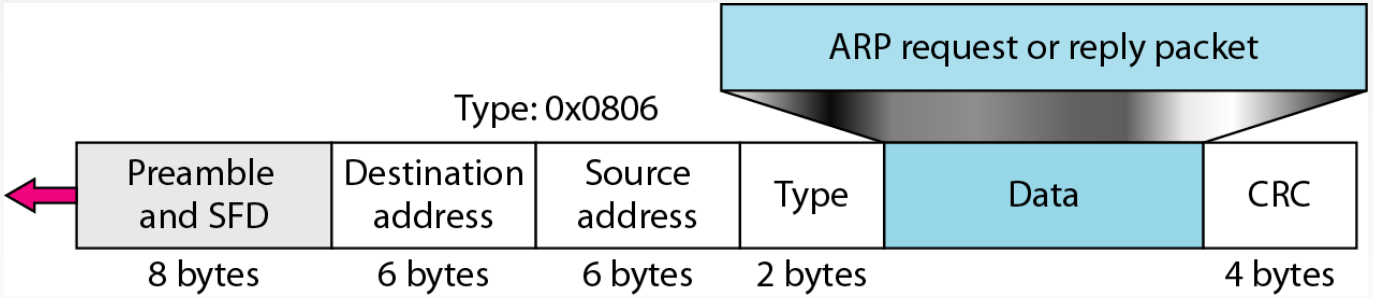
a. ARP request is broadcast



b. ARP reply is unicast

Encapsulation of ARP packet

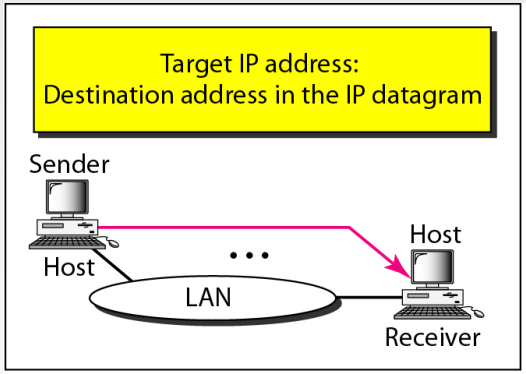
- ARP packet is encapsulated directly into a data link frame (example: Ethernet frame)



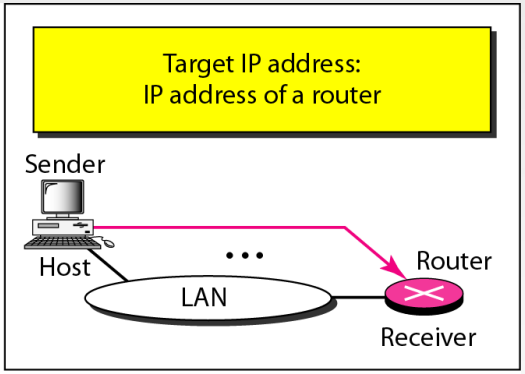
ARP Operation

- The sender knows the IP address of the target
- IP asks ARP to create an ARP request message
- The message is encapsulated in a frame (destination address = broadcast address)
- Every host or router receives the frame. The target recognizes the IP address
- The target replies with an ARP reply message (unicast with its physical address)
- The sender receives the reply message knowing the physical address of the target
- The IP datagram is now encapsulated in a frame and is unicast to the destination

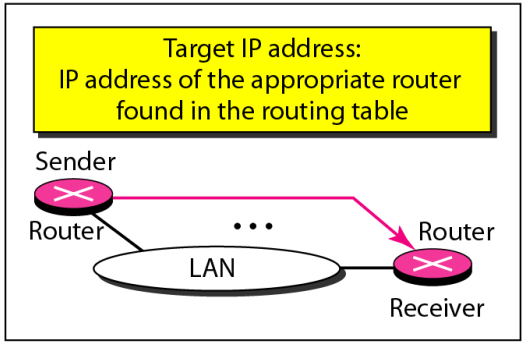
Four different cases using ARP



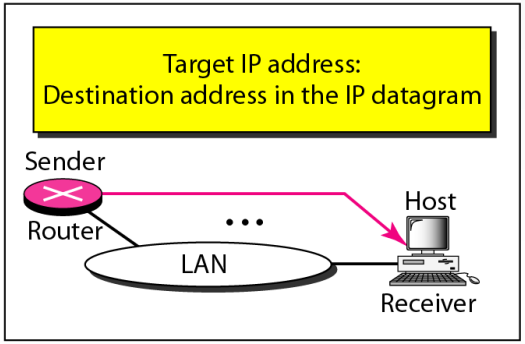
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.



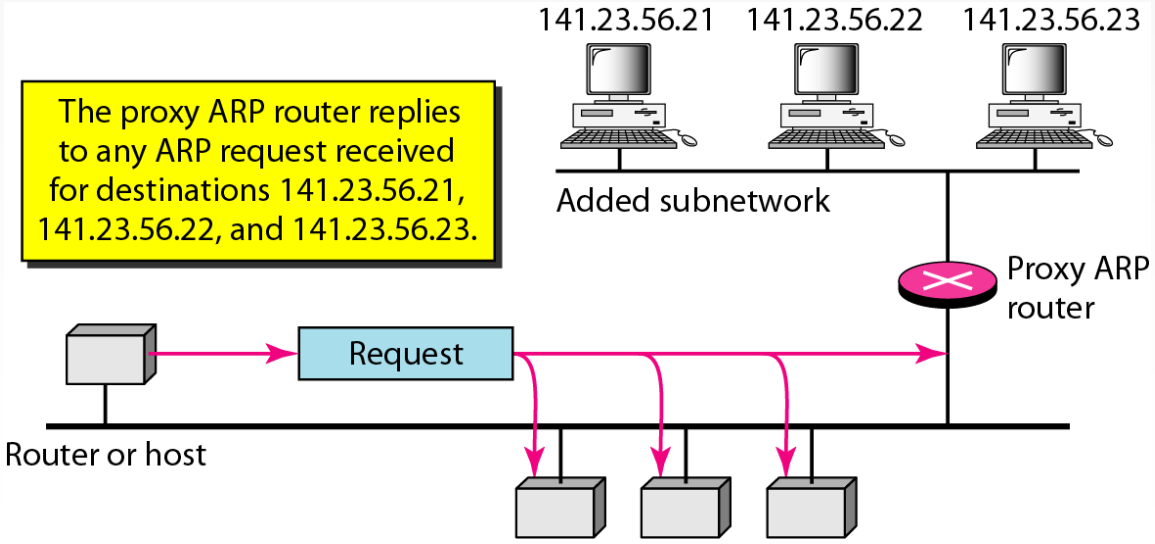
Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



Case 4. A router receives a packet to be sent to a host on the same network.

Proxy ARP

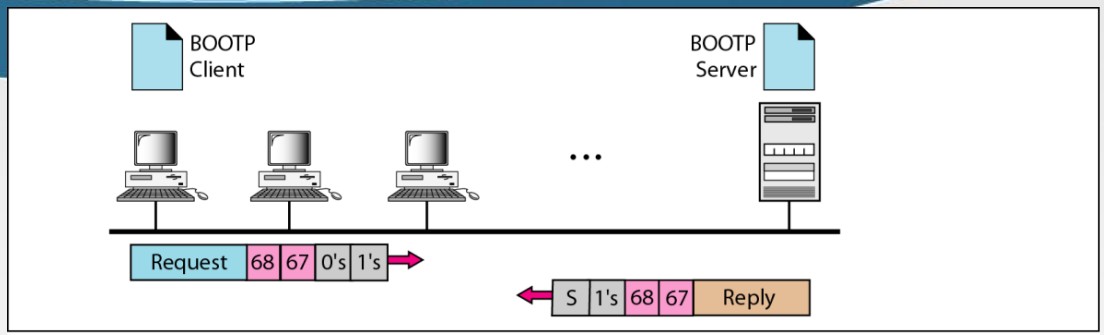
- A technique used to create a subnetting effect
- An ARP that acts on behalf of a set of hosts
- When enquired to a router, it send its own physical address on behalf of host.



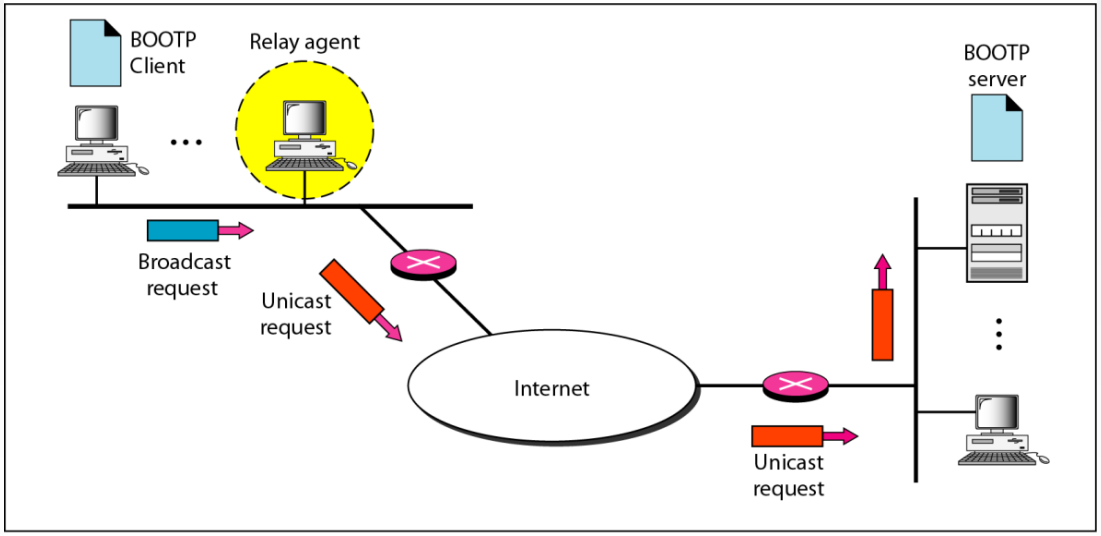
Mapping Physical to Logical Address

- Diskless station just booted
- Organizations does have not sufficient IP addresses
- RARP, BOOTP, and DHCP
- RARP(Reverse ARP):
  - Serious problem due to broadcasting at the data link layer. RARP server required for each network or subnet.
- BOOTP and DHCP are replacing RARP
- BOOTP (Bootstrap Protocol) is a client/server protocol designed to provide IP address (statistically mapped MAC to IP address)
  - Is an application layer protocol
  - Is not a dynamic configuration protocol

BOOTP Client and Server



a. Client and server on the same network

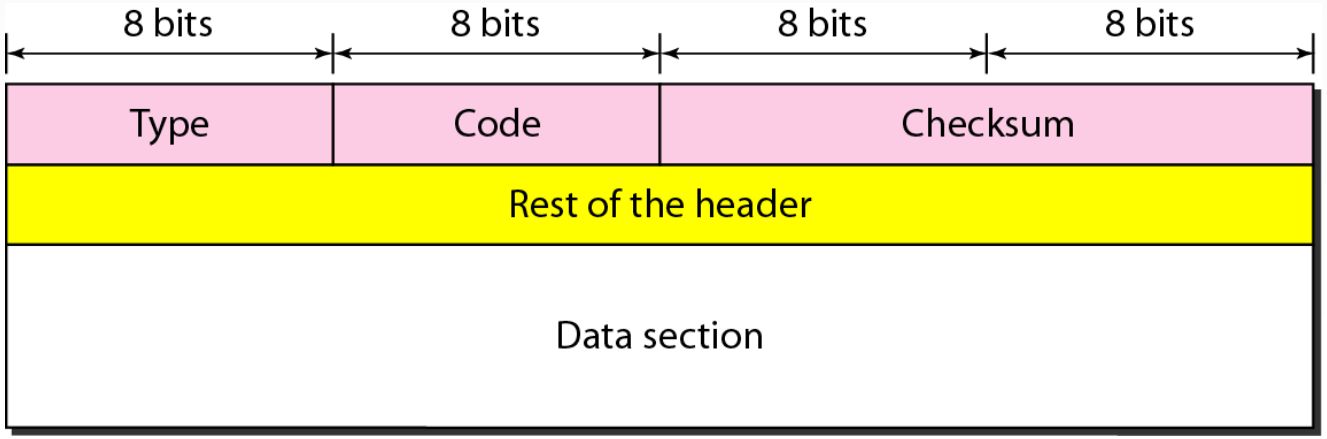


b. Client and server on different networks

- **DHCP (Dynamic Host Configuration Protocol)** provides static and dynamic address allocation that can be manual or automatic

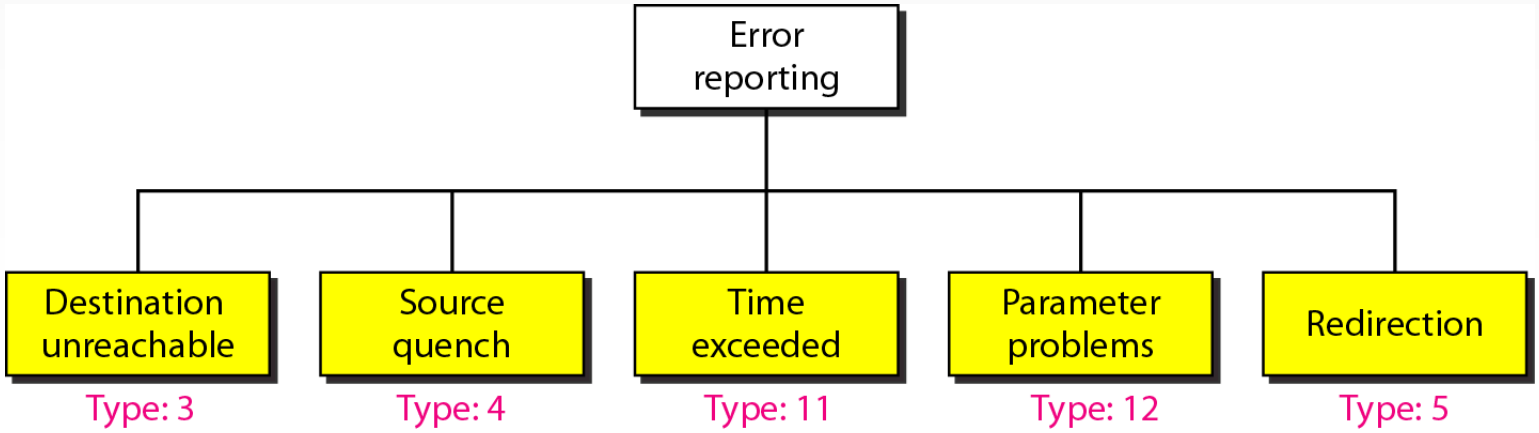
ICMP

- IP has no error-reporting or error-correcting mechanism
- IP also lacks a mechanism for host and management queries
- Internet Control Message Protocol (ICMP) is designed to compensate for two deficiencies, which is a companion to the IP
- Two types messages: error-reporting messages and query messages



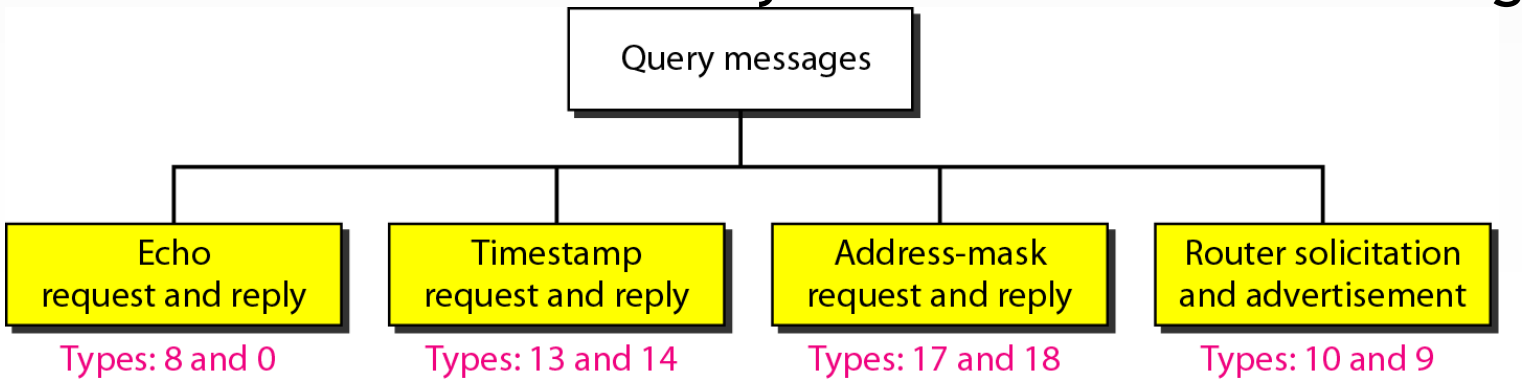
Error Reporting

- ICMP always reports error messages to the original source.
- Source quench: There is no flow control or congestion control mechanism in IP.
- Time exceed: (1) TTL related, (2) do not receive all fragments with a certain time limit
- Redirection: To update the routing table of a host



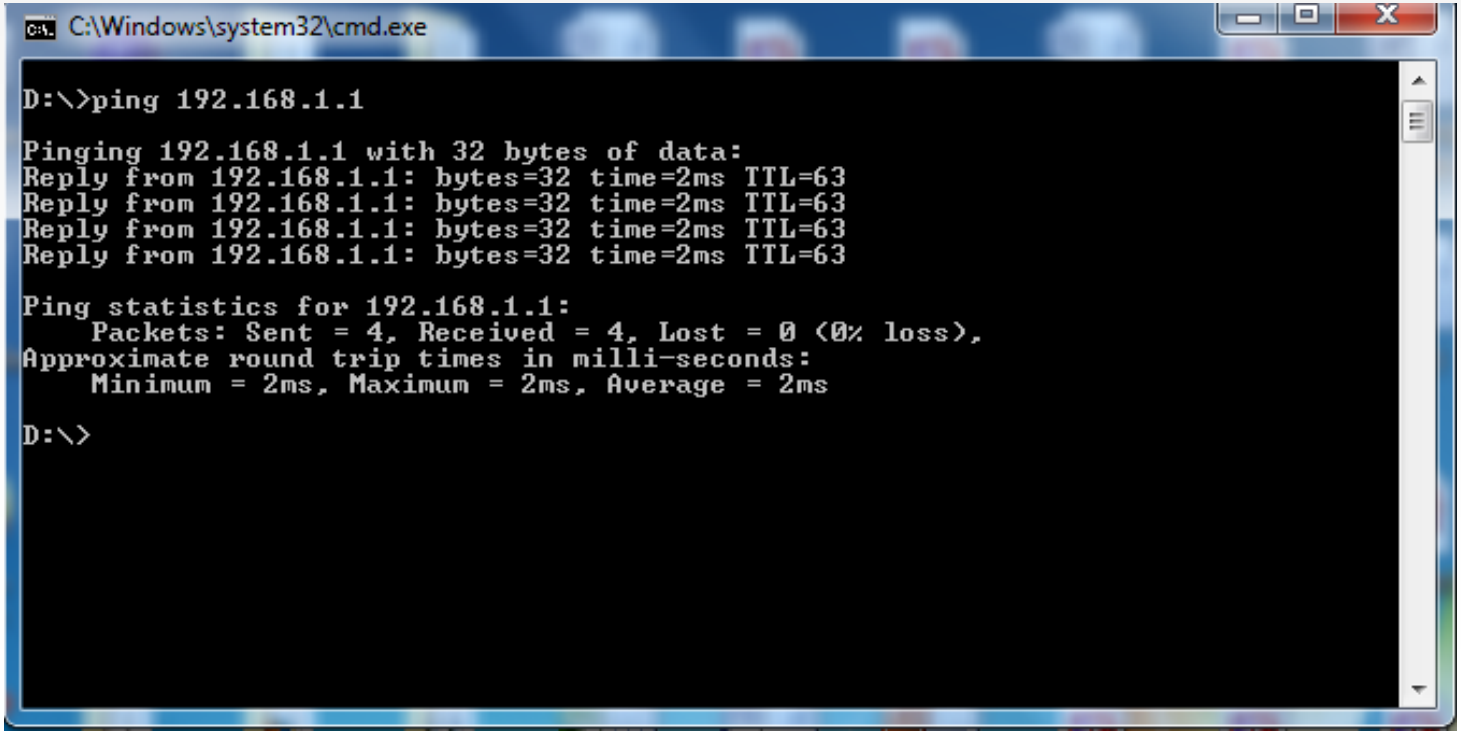
Query messages

- To diagnose some network problems
- A node sends a message that is answered in a specific format by the destination node
- Echo for diagnosis; Time-stamp to determine RTT or synchronize the clocks in two machines; Address mask to know network address, subnet address, and host id; Router solicitation to know the address of routers connected and to know if they are alive and functioning



Debugging Tools

- Two tools that use ICMP for debugging or tracing the route of a packet: ping and traceroute
- Ping: ICMP echo-request message and echo-reply message



Debugging Tools: Traceroute

- Traceroute can be used to trace the route of a packet from the source to the destination