Chapter 18

Internet Protocols

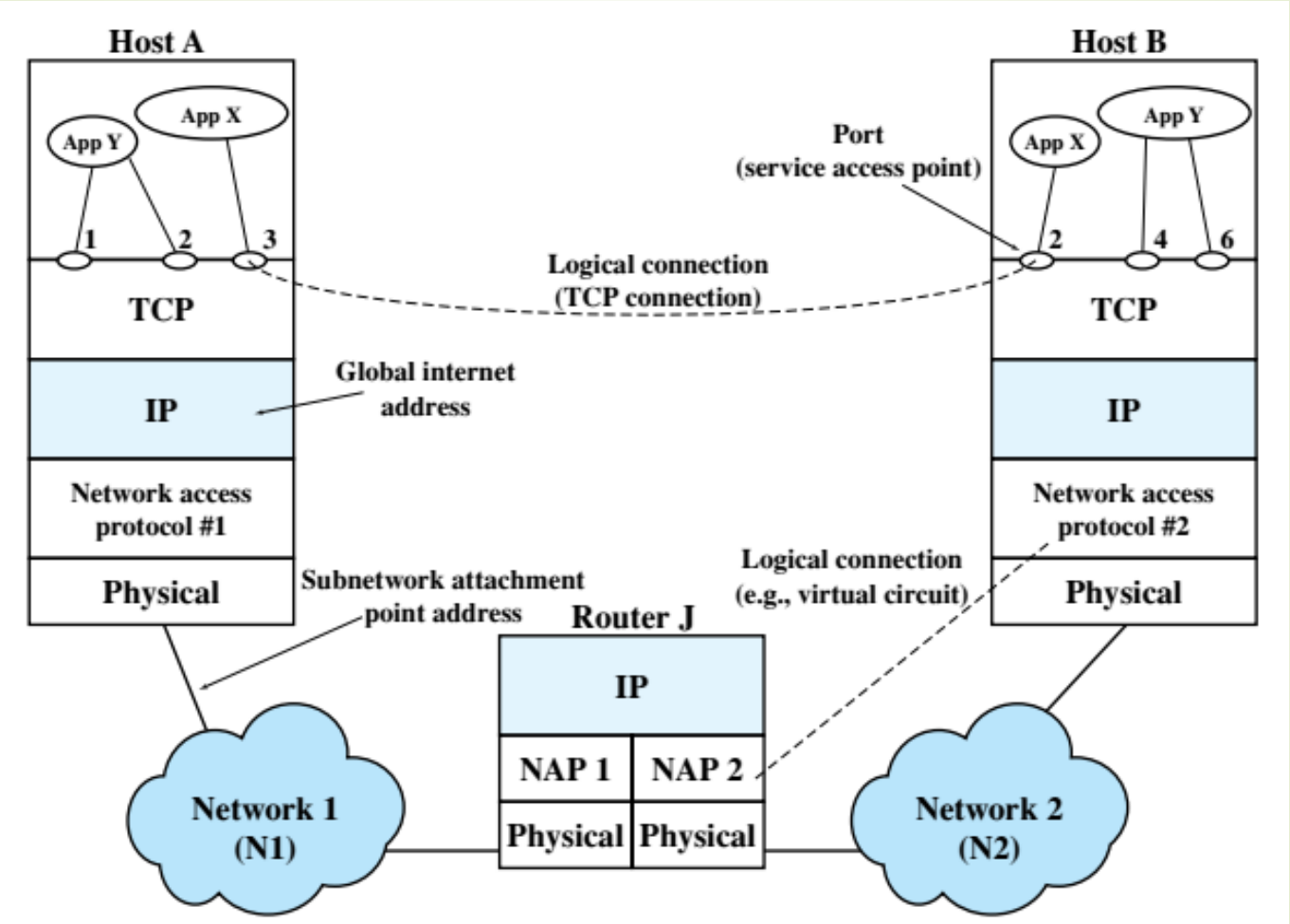
Reading Materials

- **Data and Computer Communications**, William Stallings

Contents

- Topologies
- Bridges & switches
- Ethernet
- Token ring
- CSMA/CD

TCP/IP Concepts



Internetworking Terms

Communication Network
A facility that provides a data transfer service among devices attached to the network.

Internet
A collection of communication networks interconnected by bridges and/or routers.

Intranet
An internet used by a single organization that provides the key Internet applications, especially the World Wide Web. An intranet operates within the organization for internal purposes and can exist as an isolated, self-contained internet, or may have links to the Internet.

Subnetwork
Refers to a constituent network of an internet. This avoids ambiguity because the entire internet, from a user's point of view, is a single network.

End System (ES)
A device attached to one of the networks of an internet that is used to support end-user applications or services.

Intermediate System (IS)
A device used to connect two networks and permit communication between end systems attached to different networks.

Bridge
An IS used to connect two LANs that use similar LAN protocols. The bridge acts as an address filter, picking up packets from one LAN that are intended for a destination on another LAN and passing those packets on. The bridge does not modify the contents of the packets and does not add anything to the packet. The bridge operates at layer 2 of the OSI model.

Router
An IS used to connect two networks that may or may not be similar. The router employs an internet protocol present in each router and each end system of the network. The router operates at layer 3 of the OSI model.

Design Issues

- Routing
- Datagram lifetime
- Fragmentation and reassembly
- Error control
- Flow Control

Routing

- End systems and routers maintain routing tables
  - Indicate next router to which datagram should be sent
  - Static
    - May contain alternative routes
  - Dynamic
    - Flexible response to congestion and errors
- Source routing
  - Source specifies route as sequential list of routers to be followed
  - Security
  - Priority
- Route recording

Datagram Lifetime

- Datagrams could loop indefinitely
  - Consumes resources
  - Transport protocol may need upper bound on datagram life
- Datagram marked with lifetime
  - Time-To-Live field in IP
  - Once lifetime expires, datagram discarded (not forwarded)
  - Hop count
    - Decrement time to live on passing through a each router
  - Time count
    - Need to know how long since last router

Fragmentation and Re-assembly

- Different packet sizes
- When to re-assemble
  - At destination
    - Results in packets getting smaller as data traverses internet
  - Intermediate re-assembly
    - Need large buffers at routers
    - Buffers may fill with fragments
    - All fragments must go through same router
      - Inhibits dynamic routing

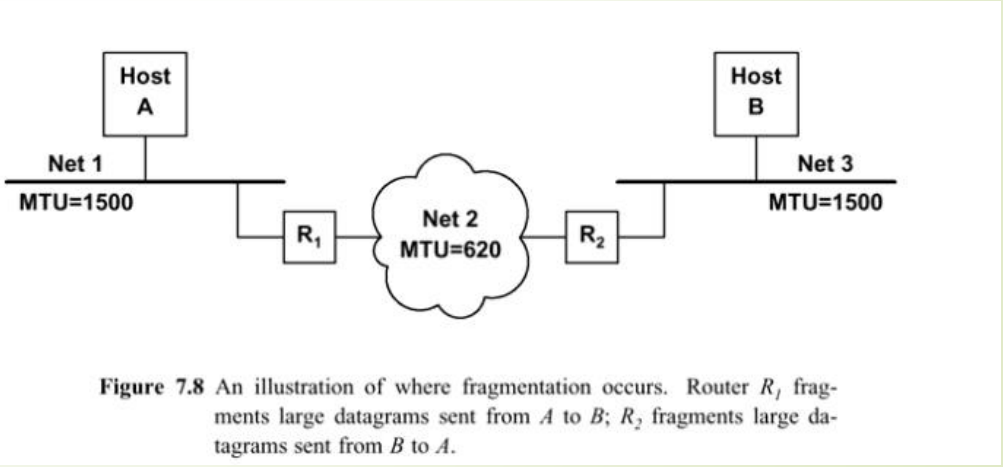
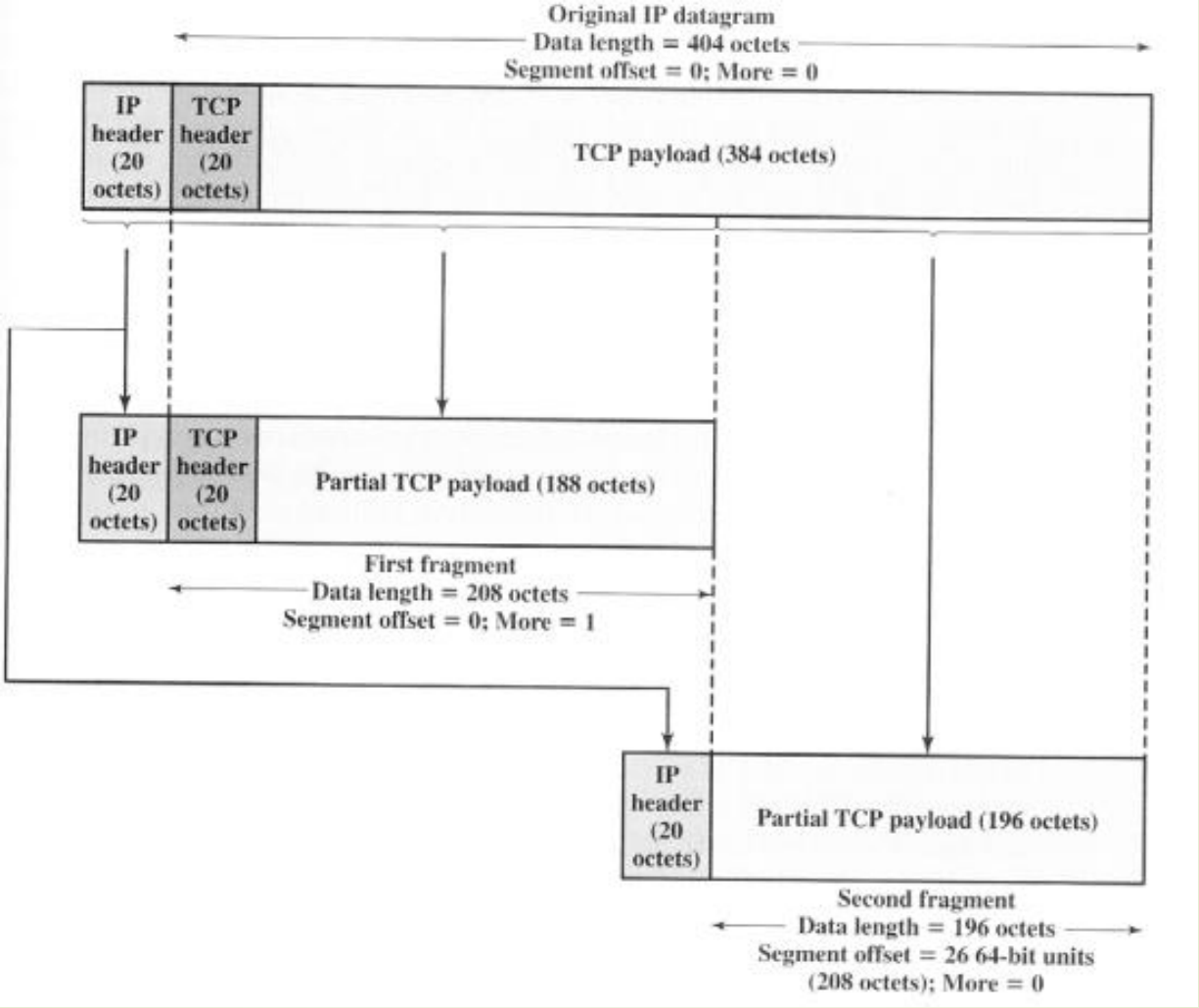


Figure 7.8 An illustration of where fragmentation occurs. Router R_1 fragments large datagrams sent from A to B; R_2 fragments large datagrams sent from B to A.

IP Fragmentation

- IP re-assembles at destination only
- Three fields in the datagram header control fragmentation and reassembly of datagrams.
  - IDENTIFICATION
    - Computers sending IP datagrams must generate a unique value
      for the IDENTIFICATION field for each datagram.
  - FLAGS
    - (more) Indicates that this is not the last fragment
    - (do not fragment)
  - FRAMMENT OFFSET
    - Position of fragment of user data in original datagram
    - In multiples of 64 bits (8 octets)

Fragmentation Example



Dealing with Failure

- Re-assembly may fail if some fragments get lost
- Need to detect failure
- Re-assembly timeout
  - Assigned to first fragment to arrive
  - If timeout expires before all fragments arrive, discard partial data received
- Use packet lifetime (time-to-live in IP)
  - If time-to-live runs out, kill partial data

Error Control

- Not guaranteed delivery
- Router should attempt to inform source if packet discarded
  - e.g. for time-to-live expiring
- Source may modify transmission strategy
- May inform high layer protocol
- Datagram identification needed
- (Look up ICMP)

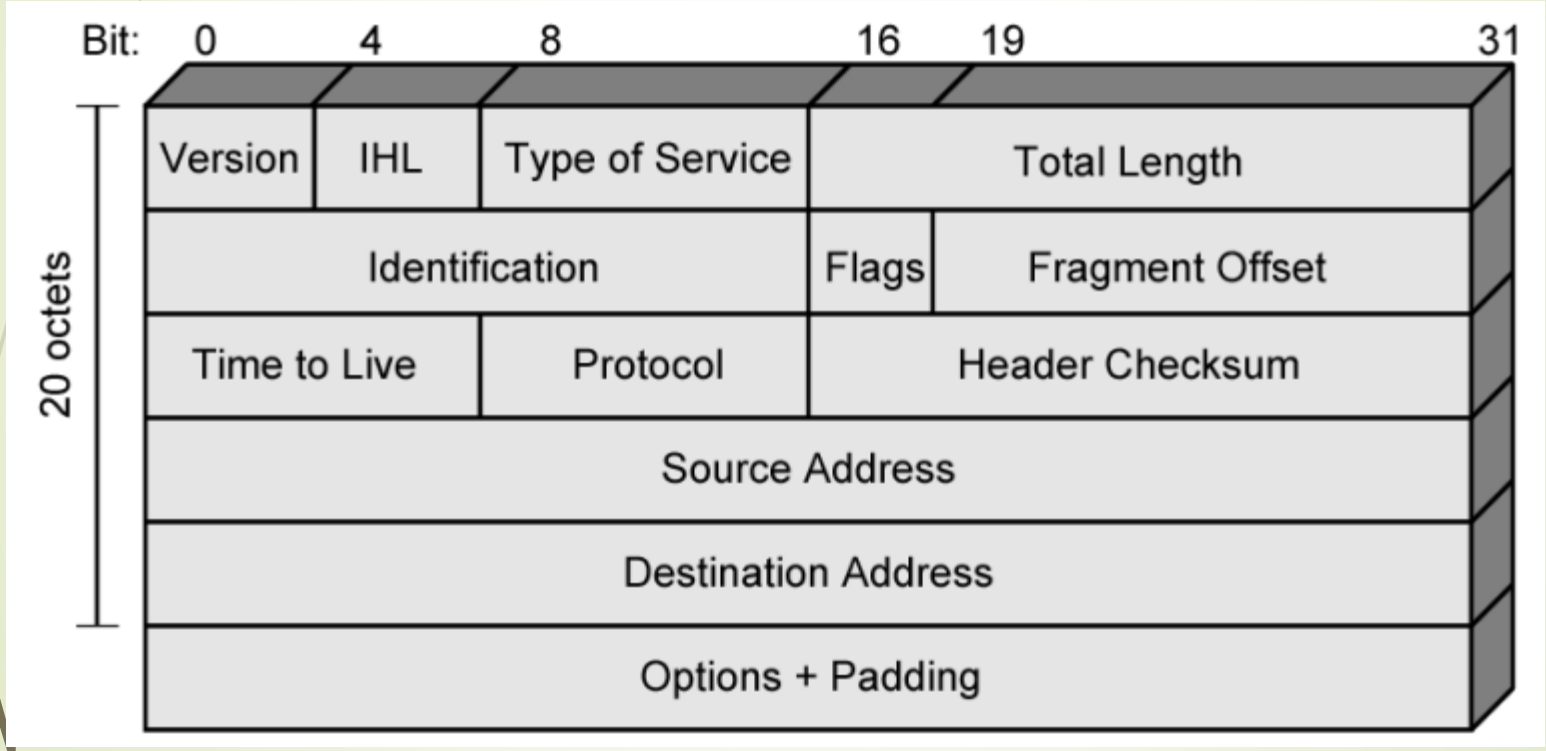
Flow Control

- Allows routers and/or stations to limit rate of incoming data
- Limited in connectionless systems
- Send flow control packets
  - Requesting reduced flow
- e.g. ICMP

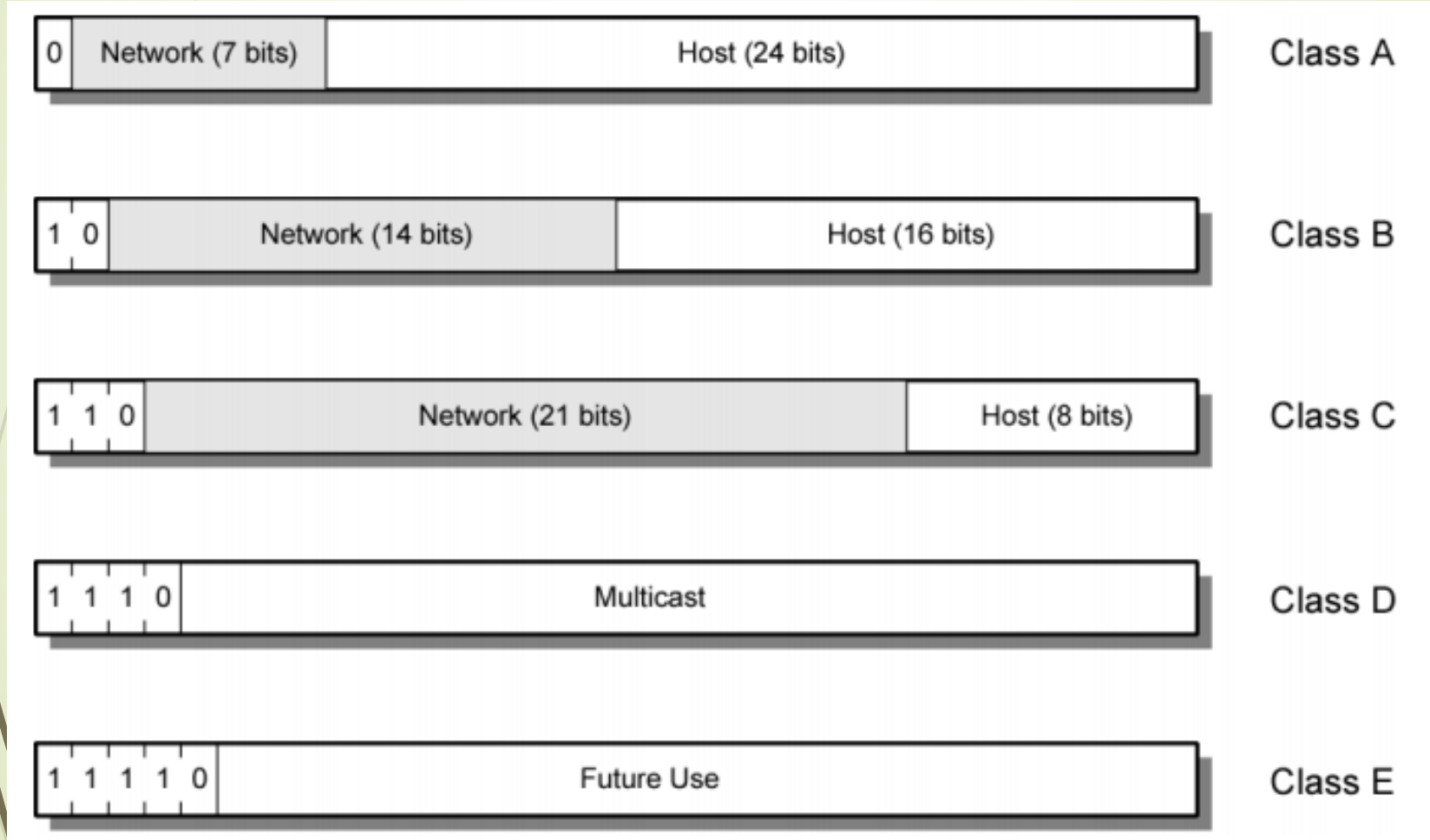
Internet Protocol (IP) Version 4

- Part of TCP/IP
  - Used by the Internet
- Specifies interface with higher layer
  - e.g. TCP
- Specifies protocol format and mechanisms
- RFC 791
- Will (eventually) be replaced by IPv6 (see later)

IPv4 Header


Bit:
0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + Padding
20 octets

IPv4 Address Formats



IP Addresses - Class A

- 32 bit global internet address
- Network part and host part
- Dotted decimal
  - (e.g. 10000000 00001010 00000010 00011110 ↔ 128.10.2.30)
- Class A
  - Start with binary 0
  - All 0 reserved
  - 01111111 (127) reserved for loopback
  - Range 1.x.x.x to 126.x.x.x
  - All allocated

IP Addresses - Class B

- Start with binary 10
- Range 128.x.x.x to 191.x.x.x
- Second Octet also included in network address
- $2^{14} = 16{,}384$ class B addresses
- All allocated

IP Addresses - Class C

- Start with binary 110
- Range 192.x.x.x to 223.x.x.x
- Second and third octet also part of network address
- $2^{21} = 2{,}097{,}152$ addresses
- Nearly all allocated
  - See IPv6

Subnets and Subnet Masks

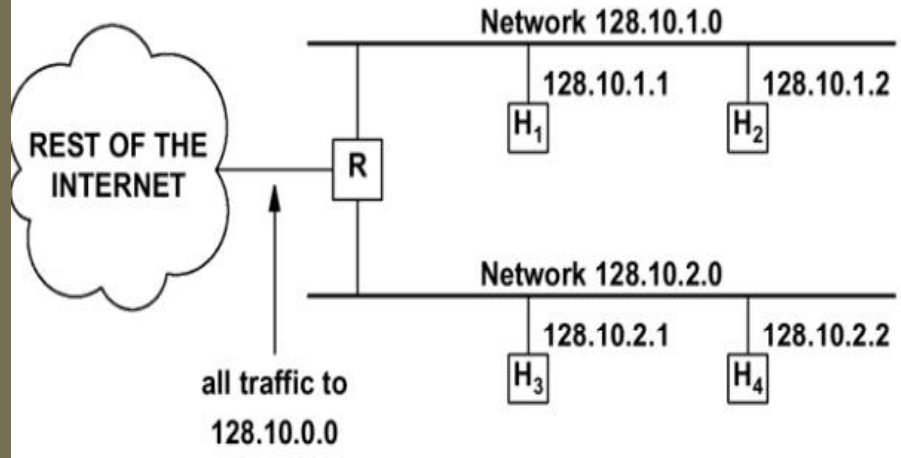


Figure 10.3 A site with two physical networks using subnet addressing to label them with a single class *B* network address. Router *R* accepts all traffic for net 128.10.0.0 and chooses a physical network based on the third octet of the address.

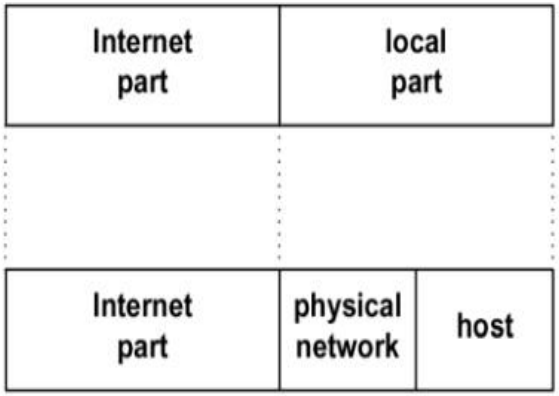
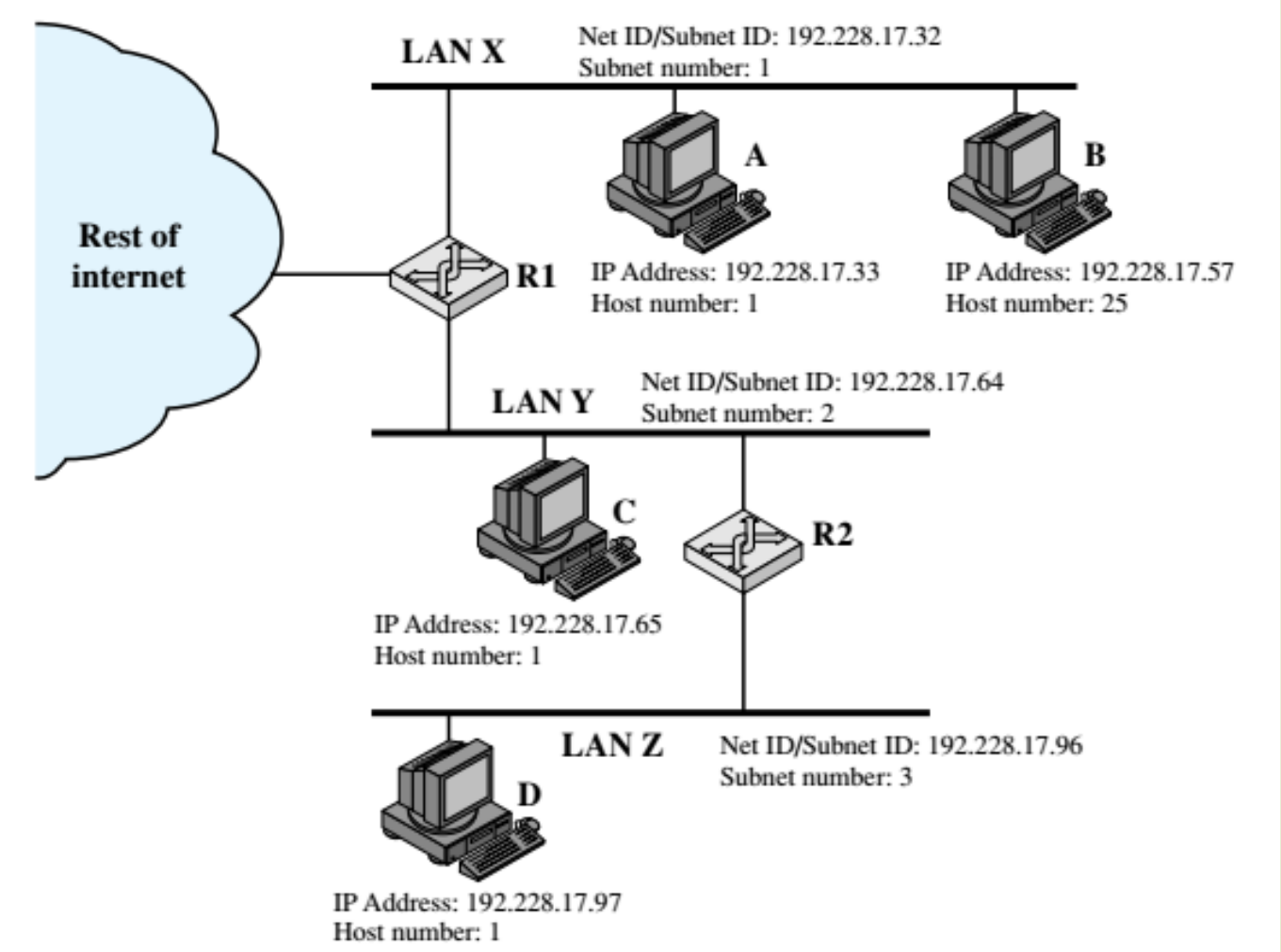
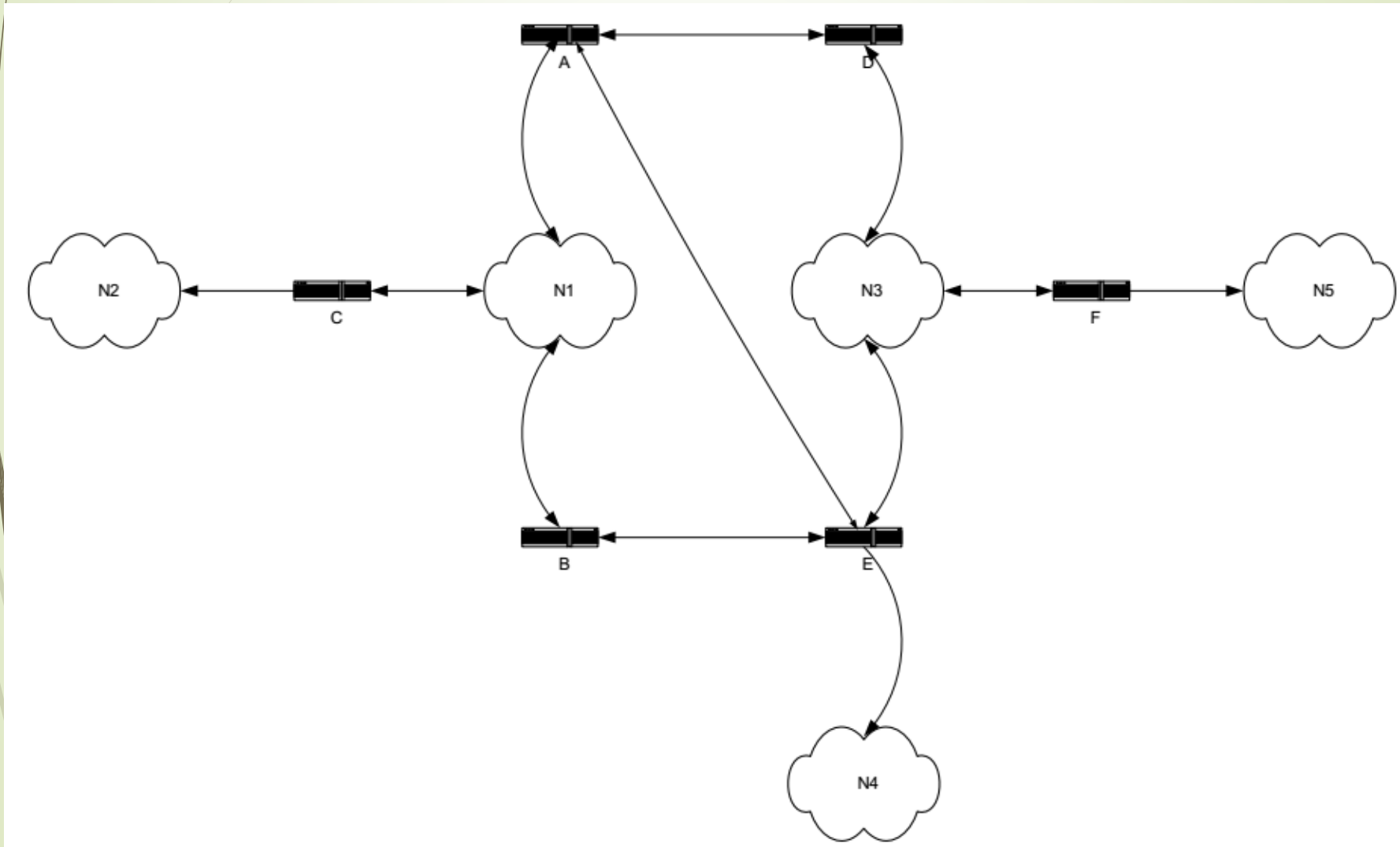


Figure 10.4 (a) Conceptual interpretation of a 32-bit IP address in the original IP address scheme, and (b) conceptual interpretation of addresses using the subnet scheme shown in Figure 10.3. The local portion is divided into two parts that identify a physical network and a host on that network.

Routing using Subnets

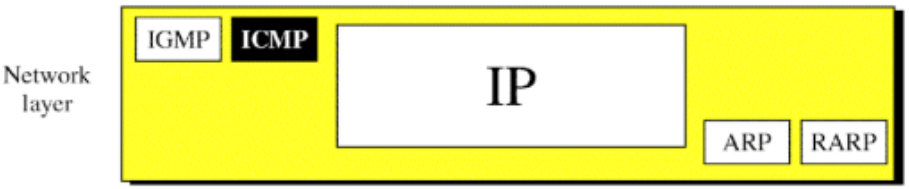


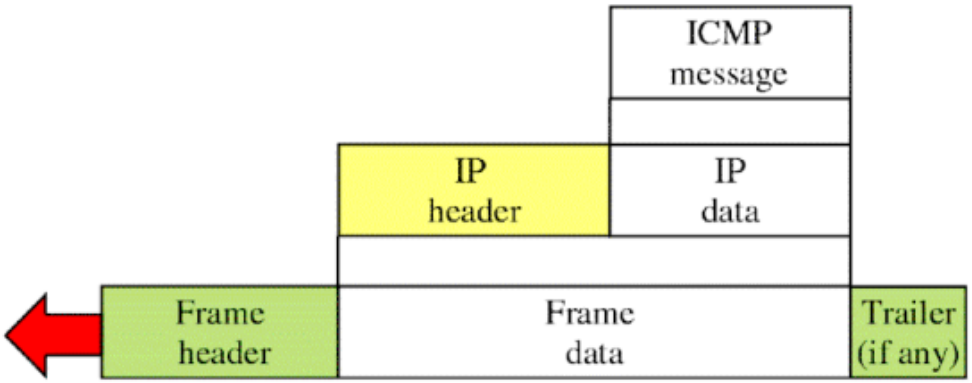
- In the following figure, there are eight (8) sub-networks belonging to a company. The company has Class C addresses, 192.121.152.0. Help the company partition the network into the needed number of sub-networks, by identifying the subnet mask, assigning addresses to each of the sub-networks, assigning needed IP addresses to routers and computers. Suppose that there are two computers on each sub-network.



ICMP

- Internet Control Message Protocol
- Transfer of (control) messages from routers and hosts to hosts
- Feedback about problems
  - e.g. time-to-live expired
- Encapsulated in IP datagram
  - Not reliable





Courtesy

- Professor Jiying Zhao, University of Ottawa