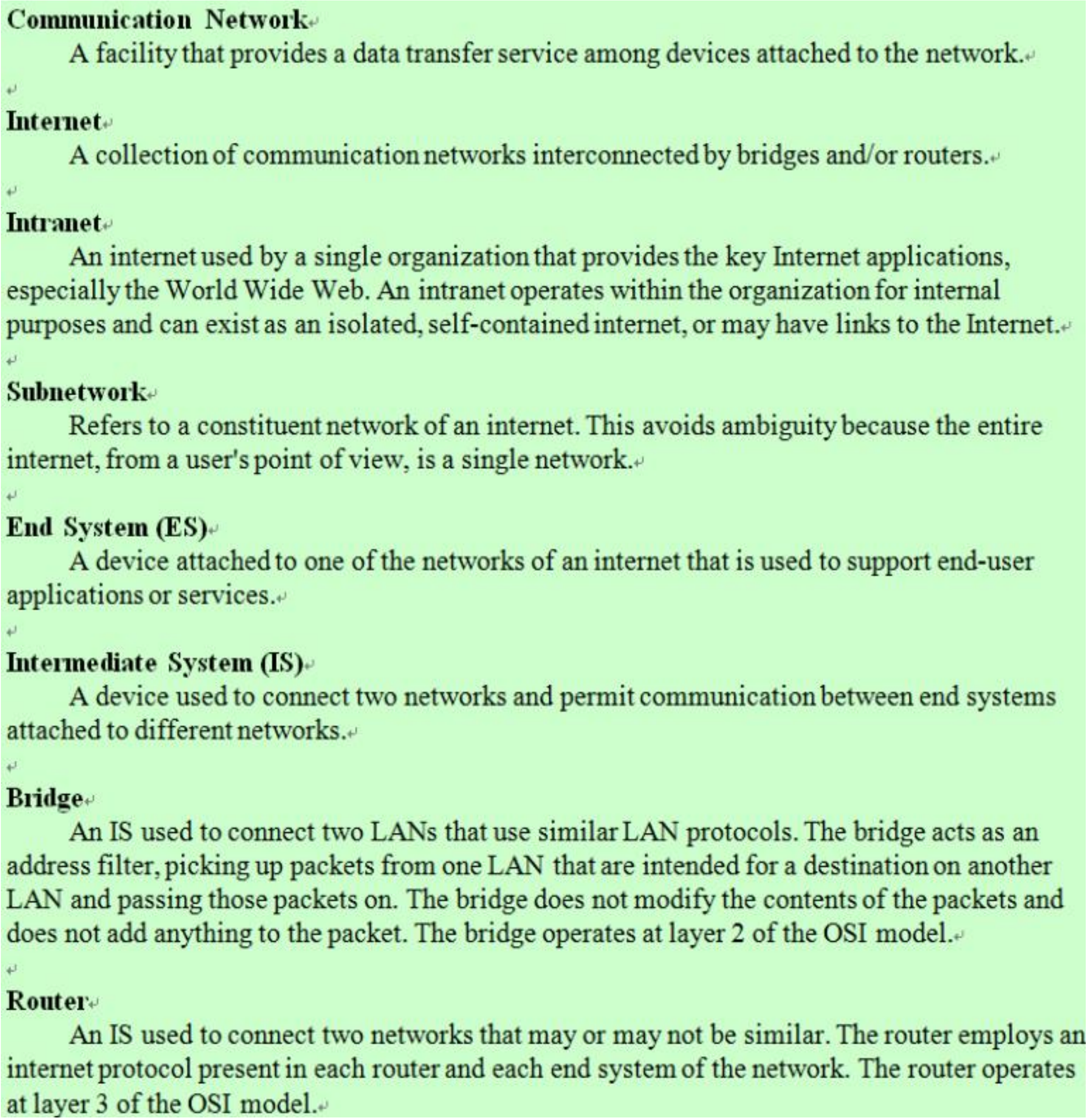
Network : Internet Protocol (1)

Jae Hyeon Kim

Reference

William Stalling, Data and Computer Communications 10/E, Prentice Hall

– Internet Protocol



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.

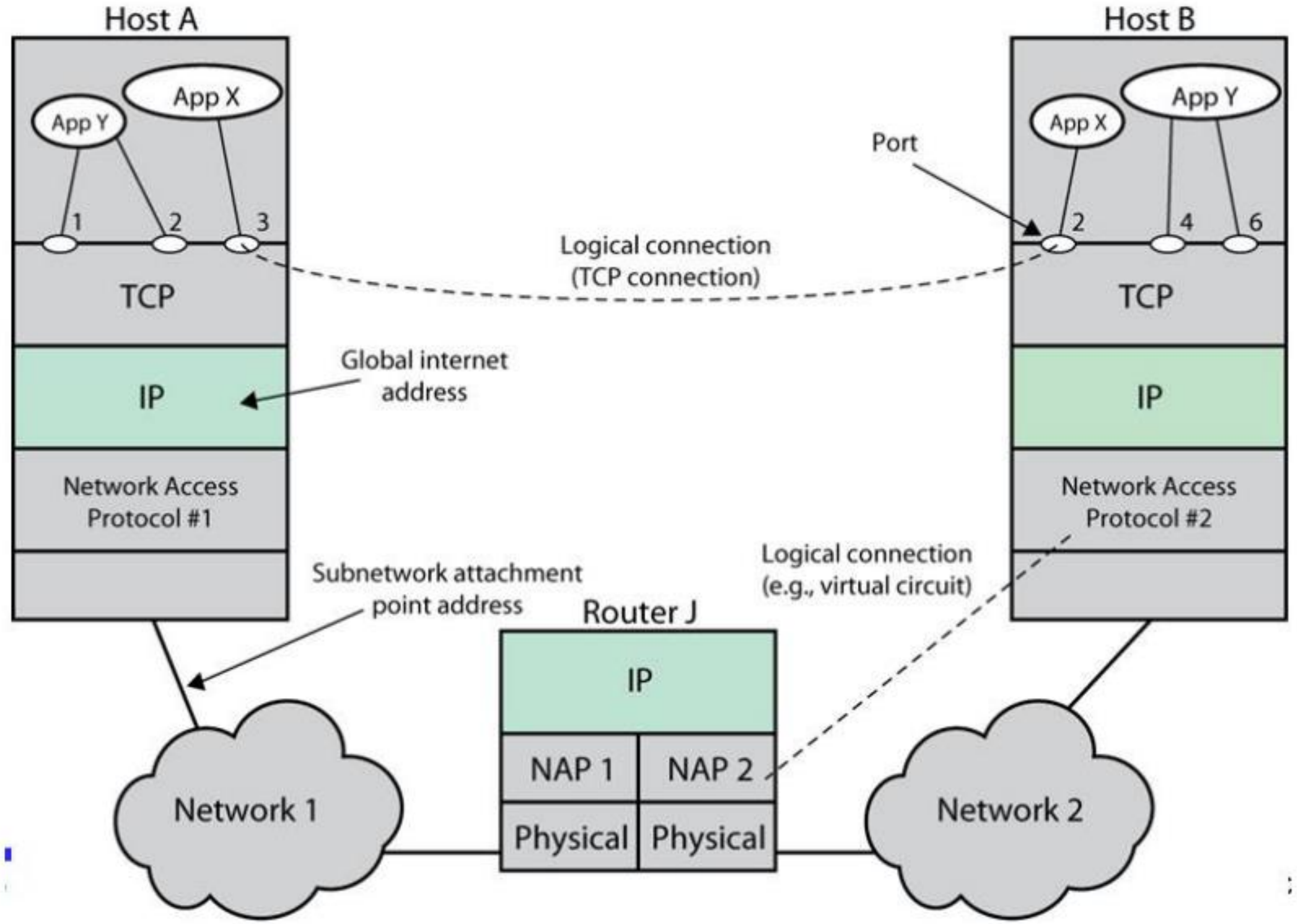
Bridge

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.

– TCP/IP Concepts

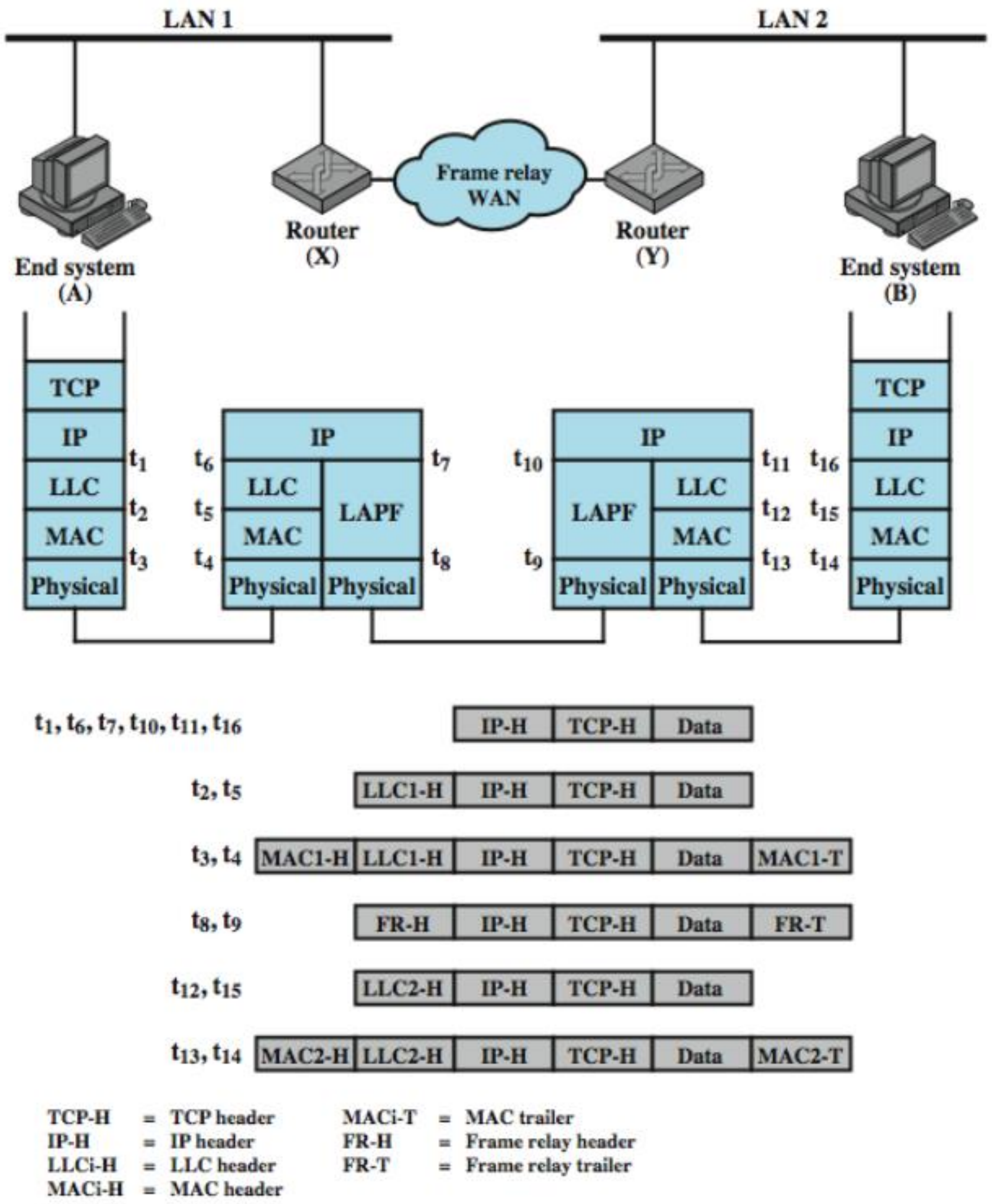


Host A
App Y
App X
1
2
3
TCP
IP
Network Access Protocol #1
Global internet address
Logical connection (TCP connection)
Port
Host B
App X
App Y
2
4
6
TCP
IP
Network Access Protocol #2
Subnetwork attachment point address
Logical connection (e.g., virtual circuit)
Router J
IP
NAP 1
NAP 2
Physical
Physical
Network 1
Network 2

Connectionless Operation

- Internetworking involves connectionless operation at the level of the Internet Protocol
- IP provides a connectionless service
    - Initially developed for the DARPA Internet project
    - Protocol is needed to access a particular network
- Connectionless Internet facility
    - Is flexible
    - Can be made robust
    - Does not impose unnecessary overhead

– IP Operation


LAN 1
LAN 2
End system (A)
Router (X)
Frame relay WAN
Router (Y)
End system (B)
TCP
IP
LLC
MAC
Physical
LAPF
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 t_{10} t_{11} t_{12} t_{13} t_{14} t_{15} t_{16}

$t_1, t_6, t_7, t_{10}, t_{11}, t_{16}$: IP-H | TCP-H | Data

t_2, t_5: LLC1-H | IP-H | TCP-H | Data

t_3, t_4: MAC1-H | LLC1-H | IP-H | TCP-H | Data | MAC1-T

t_8, t_9: FR-H | IP-H | TCP-H | Data | FR-T

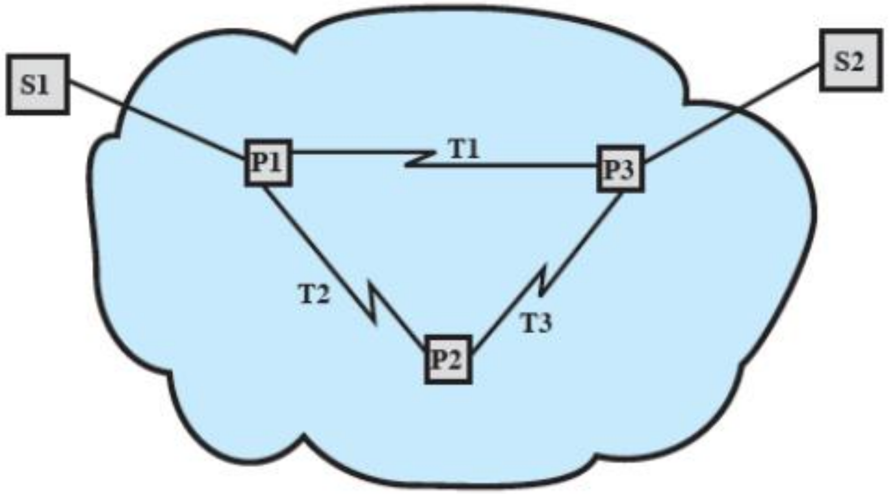
t_{12}, t_{15}: LLC2-H | IP-H | TCP-H | Data

t_{13}, t_{14}: MAC2-H | LLC2-H | IP-H | TCP-H | Data | MAC2-T

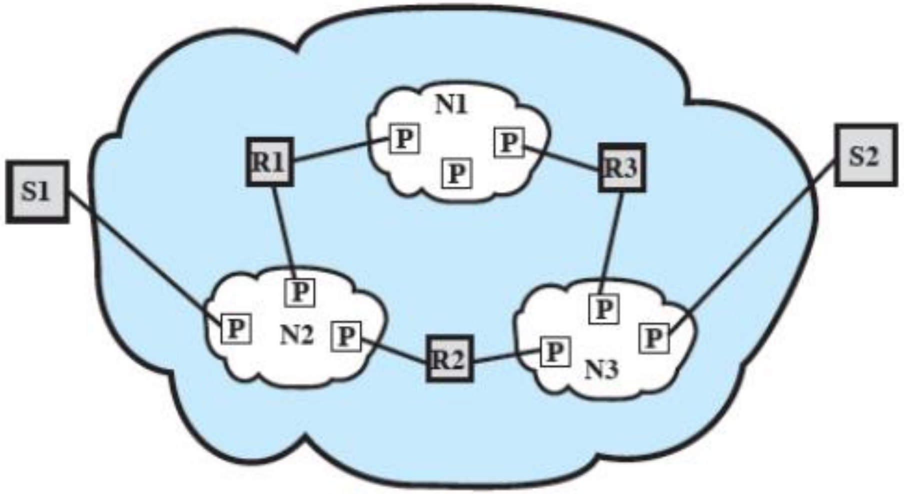
TCP-H = TCP header		MACi-T = MAC trailer	
IP-H = IP header		FR-H = Frame relay header	
LLCi-H = LLC header		FR-T = Frame relay trailer	
MACi-H = MAC header			

IP Design Issues

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



(a) Packet-switching network architecture



(b) Internetwork architecture

Routing

- ES/router maintain routing tables
  - The table indicate next to which datagram is sent
  - It can be static or dynamic
- Router decides the next router to which the internet datagram should be sent : see next in detail
  - Source routing : source specifies route to be followed and can be useful for security and priority
  - Route recording : each router appends its Internet address to a list of addresses in the datagram, useful for testing and debugging

Datagram Lifetime

- Datagrams could loop indefinitely, possibly with making use of incorrect routing information
  - Consumes resources
  - IP may need upper bound on lifetime of a datagram
- IP lifetime
  - Specified in lifetime, so Time to Live (8 bits), TTL in IP header
  - Initially, it is assigned in the sender's OS, as 64 or 128
  - Every router that processes a datagram must decreases the TTL by at least one, so the TTL is similar to a hop count
  - In addition, the router decrease the time, in seconds, that a datagram is stayed in the router

Fragmentation and Re-assembly (1)

- Lower-level protocols may need to break data up into smaller blocks, called fragmentation
- Reasons for fragmentation
  - Network only accepts blocks of a certain size
  - More efficient error control & smaller retransmission units
  - Fairer access to shared facilities
  - Smaller buffers
- Disadvantages
  - Greater overhead with more percentage of control information
  - More interrupts & processing time

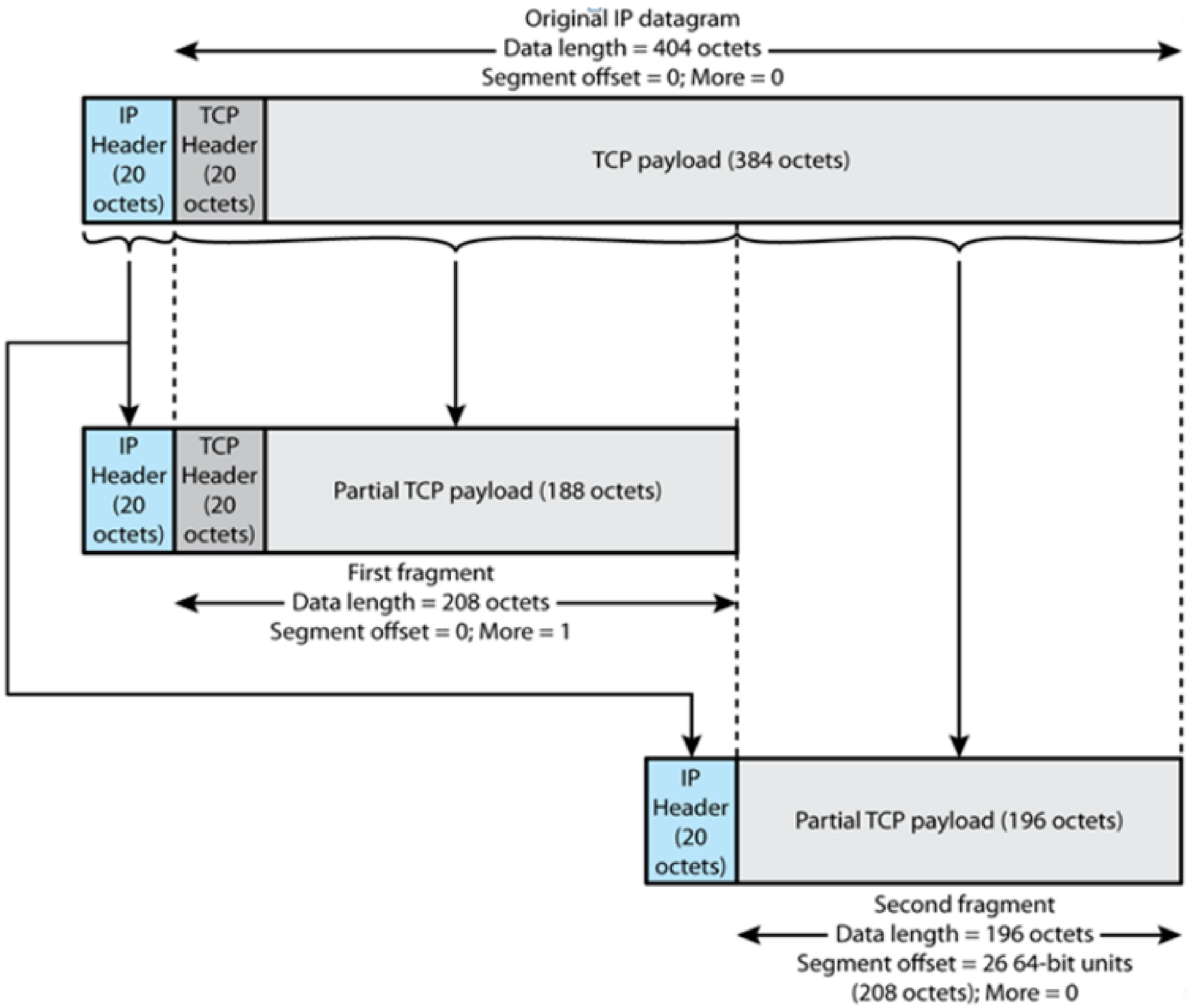
Fragmentation and Re-assembly (2)

- Issue of when to re-assemble
  - At destination : packet get smaller ad data traverses Internet
  - At intermediate node (router) : need large buffers at routers, buffer may fill with fragments, all fragments must go through same router

IP Fragmentation

- IP re-assembles at destination only
- Make use of fields in header
  - Data unit identifier (ID) : identifies end system originated datagram
  - Data length : length of user data in octets
  - Offset : position of fragment of user data in original datagram
  - More flag : indicates that this is not the last fragment

– Fragmentation Example



Error and Flow Control

- Error control
  - Discarded datagram
  - So, identification is needed
  - Reasons for discarded datagrams include : lifetime expiration, congestion, FCS error
- Flow control
  - Allows routers to limit the rate they receive data
  - Send flow control packets requesting reduced data flow
- Error and flow control takes place in station to station
  - That is, TCP have the role

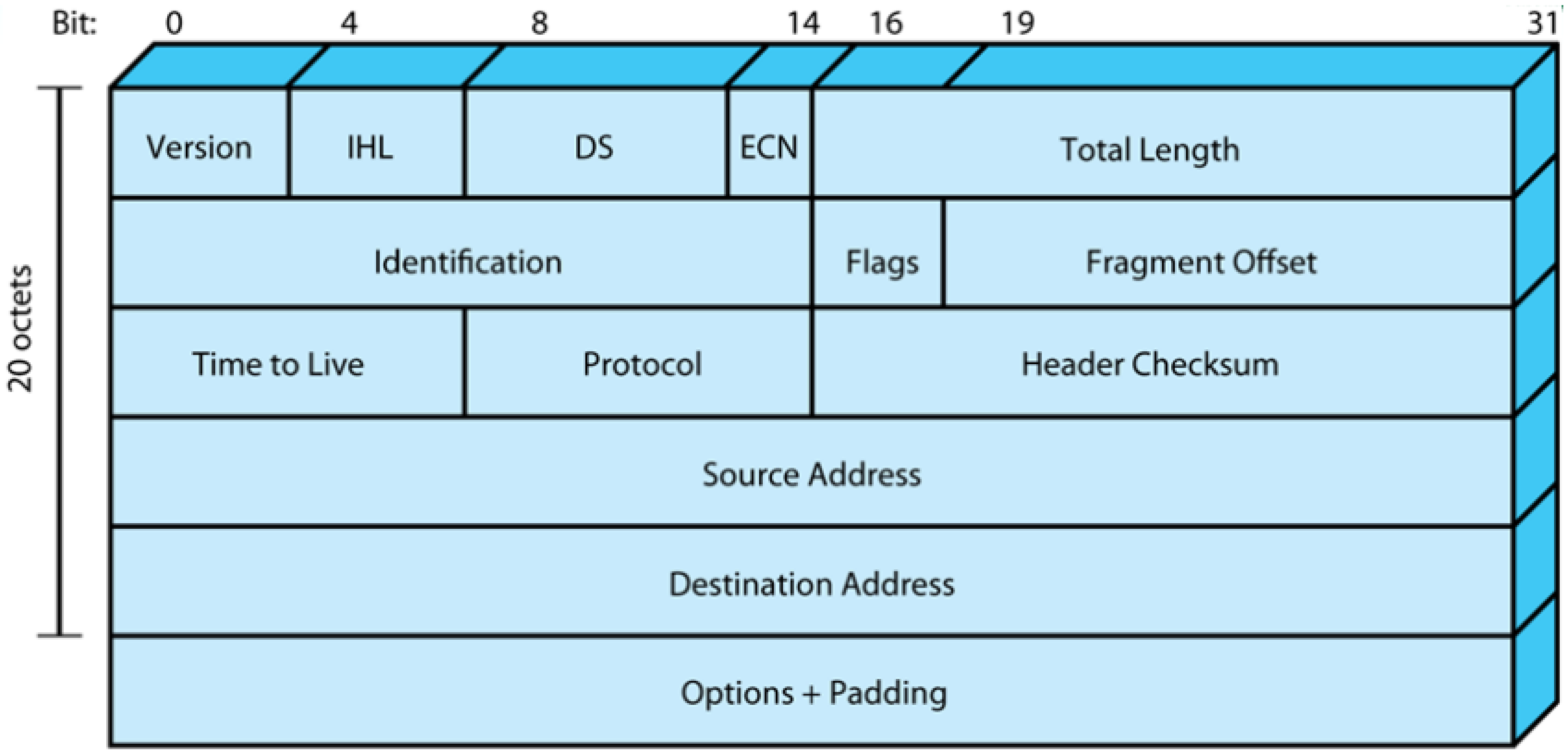
Internet Protocol (IP) v4

- IPv4 is defined in RFC 791 as a part of TCP/IP suite
- It consists of two parts
  - Specification of interface with a higher layer
  - Specification of actual protocol format and mechanisms
- IP services
  - Primitives : specifies functions to be performed, the actual form of a primitive is implementation dependent
  - Parameters : used to pass data and control information

IP Parameters

- Source address and destination address
- Protocol
- Type of Service
- Identification
- Fragment indicator {More bit | Don’t fragment bit}
- Time to live
- Data length
- Option data (security, source routing, route recording, stream identification..)
- User data

IPv4 Header



Bit: 0 4 8 14 16 19 31

20 octets

Version | IHL | DS | ECN | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

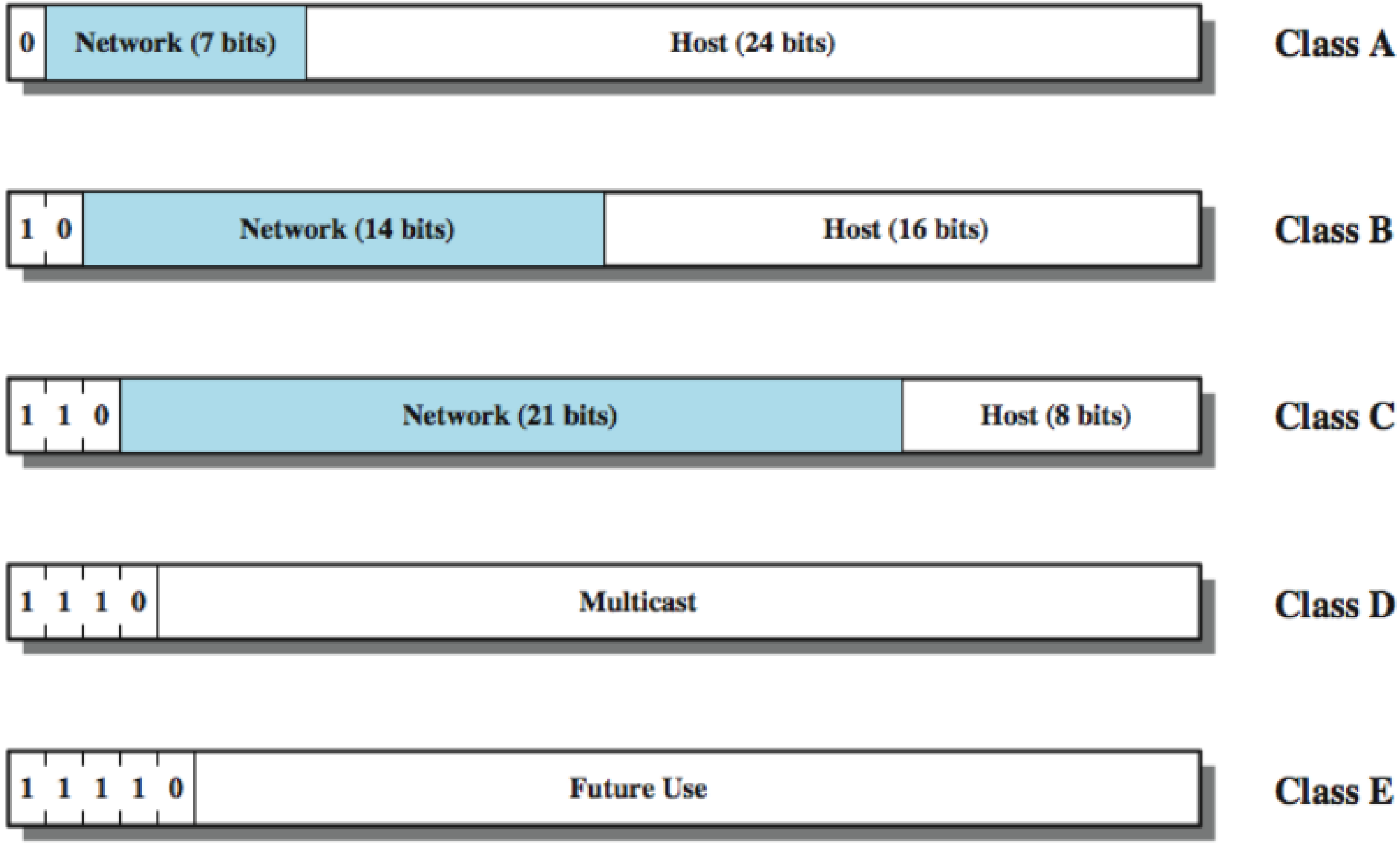
Destination Address

Options + Padding

DS : Differentiated Services (delivery priority, drop precedence) see IPv6's DS in Chap. 20
ECN : Explicit Congestion Notification (01 or 10 by sender to notify ECN-capable, 11 by router to indicate a congestion)
Protocol : (TCP=6, UDP=17)

IPv4 Address Formats

- Two-level addressing



0 | Network (7 bits) | Host (24 bits) — Class A

1 0 | Network (14 bits) | Host (16 bits) — Class B

1 1 0 | Network (21 bits) | Host (8 bits) — Class C

1 1 1 0 | Multicast — Class D

1 1 1 1 0 | Future Use — Class E

IP Addresses

- Class A
    - Start with binary 0, range 1.x.x.x to 126.x.x.x
    - All 0 reserved, 01111111 (127) reserved for loopback
- Class B
    - Start with binary 10, range 128.x.x.x to 191.x.x.x
- Class C
    - Start with binary 110, range 192.x.x.x to 223.x.x.x
- Private address (vs. public address)
    - Range as 10.x.x.x, 172.16.x.x, 192.168.x.x
    - Mapped by a Network Address Translation (NAT) box