Network Model

- OSI model and TCP/IP model -

Sogang University

Jaewoo So

서강대학교
SOGANG UNIVERSITY

학습에 앞서

■학습개요

- 네트워크 모델에 대하여 이해하고, OSI-7 계층 모델과 TCI/IP 계층 모델의 구성을 학습한다.

■학습목표

- 네트워크 모델의 필요성과 개념을 설명할 수 있어야 한다.
- 네트워크 계층 모델에서 각 계층의 역할과 동작을 설명할 수 있어야 한다.

1. Layered Tasks

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

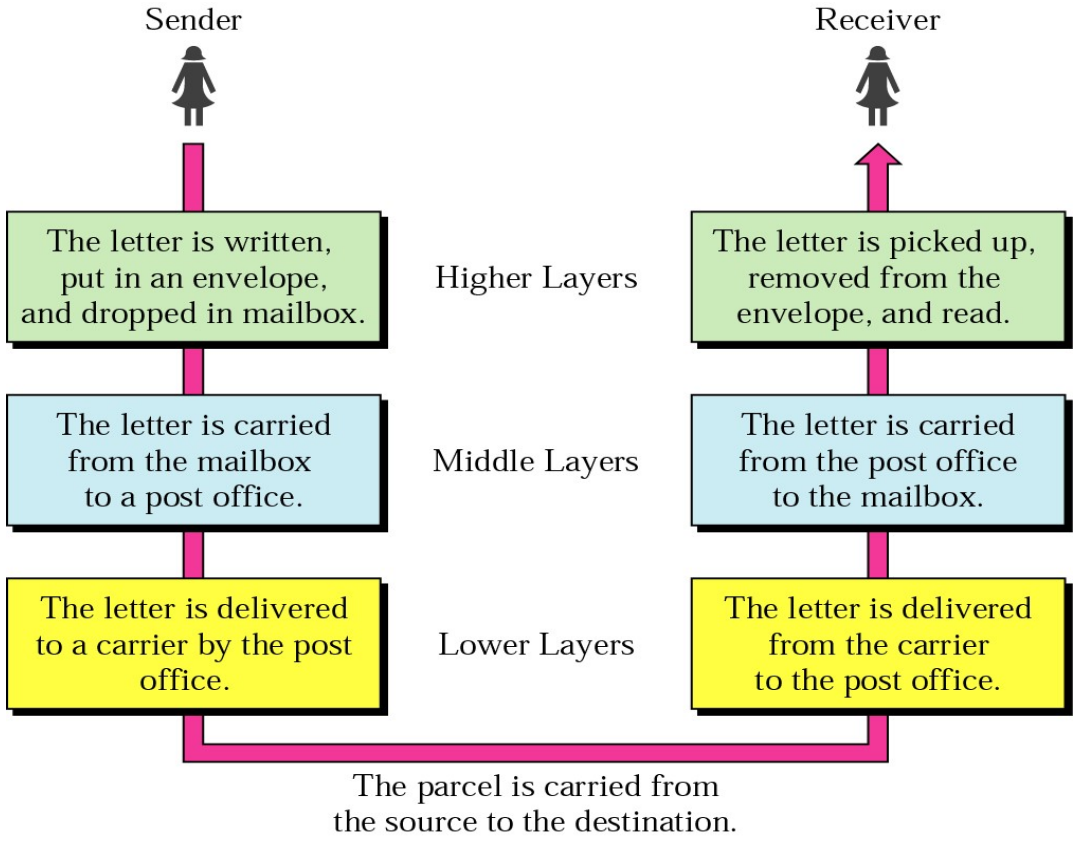
Topics discussed in this section:

Sender, Receiver, and Carrier
Hierarchy

1. Layered Tasks

- We use the concept of layers in our daily life
  - ex : postal mail
- Sender, Receiver, and Carrier
  - needs three components
  - there is a hierarchy of tasks

- Hierarchy
  - letter must be written and dropped in the mailbox before being picked up by the letter carrier at the sender
  - letter must be dropped in the recipient mailbox before being picked up by the recipient
- Services
  - each layer at the sending site uses the services of the layer immediately below it



2. The OSI Model

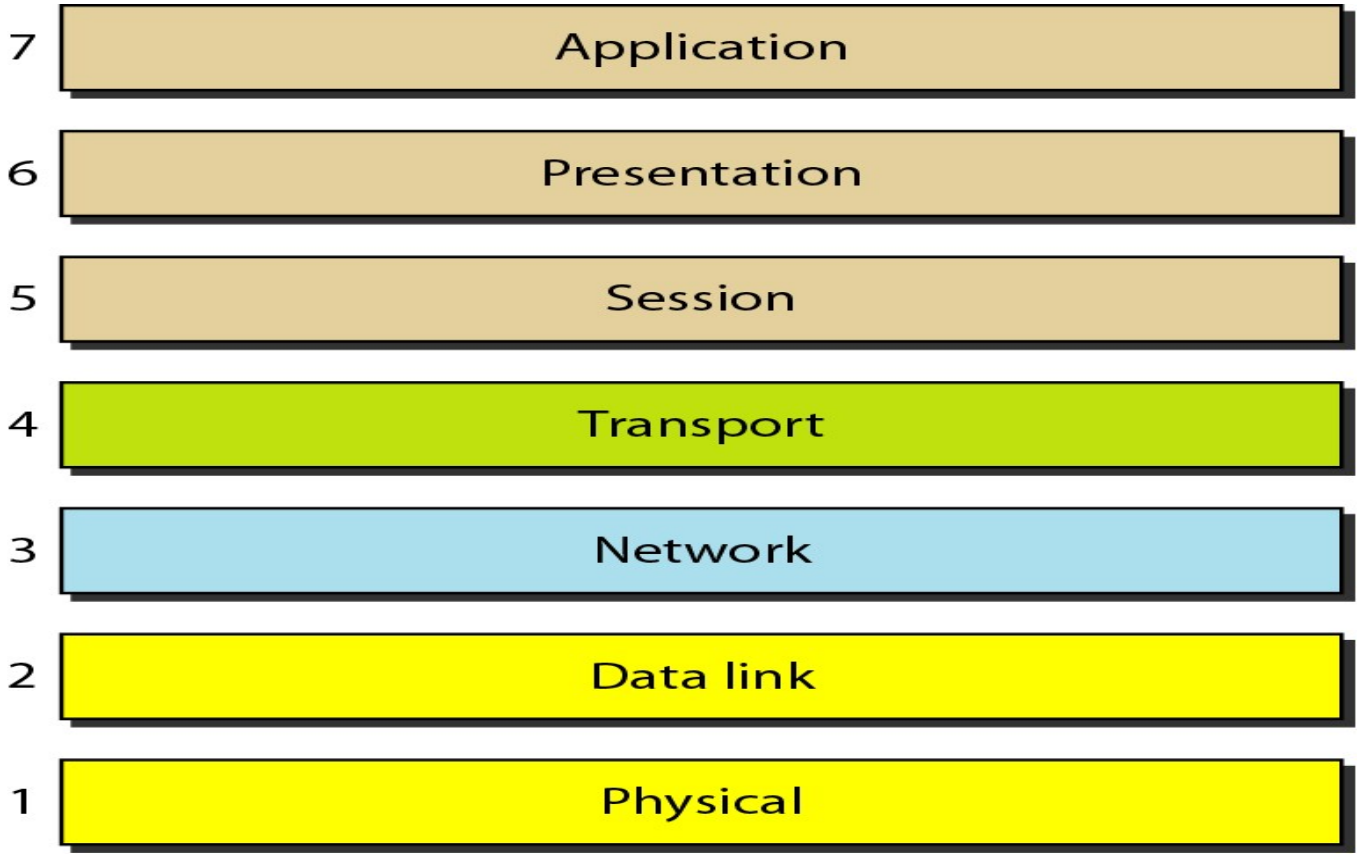
Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Topics discussed in this section:

Layered Architecture
Peer-to-Peer Processes
Encapsulation

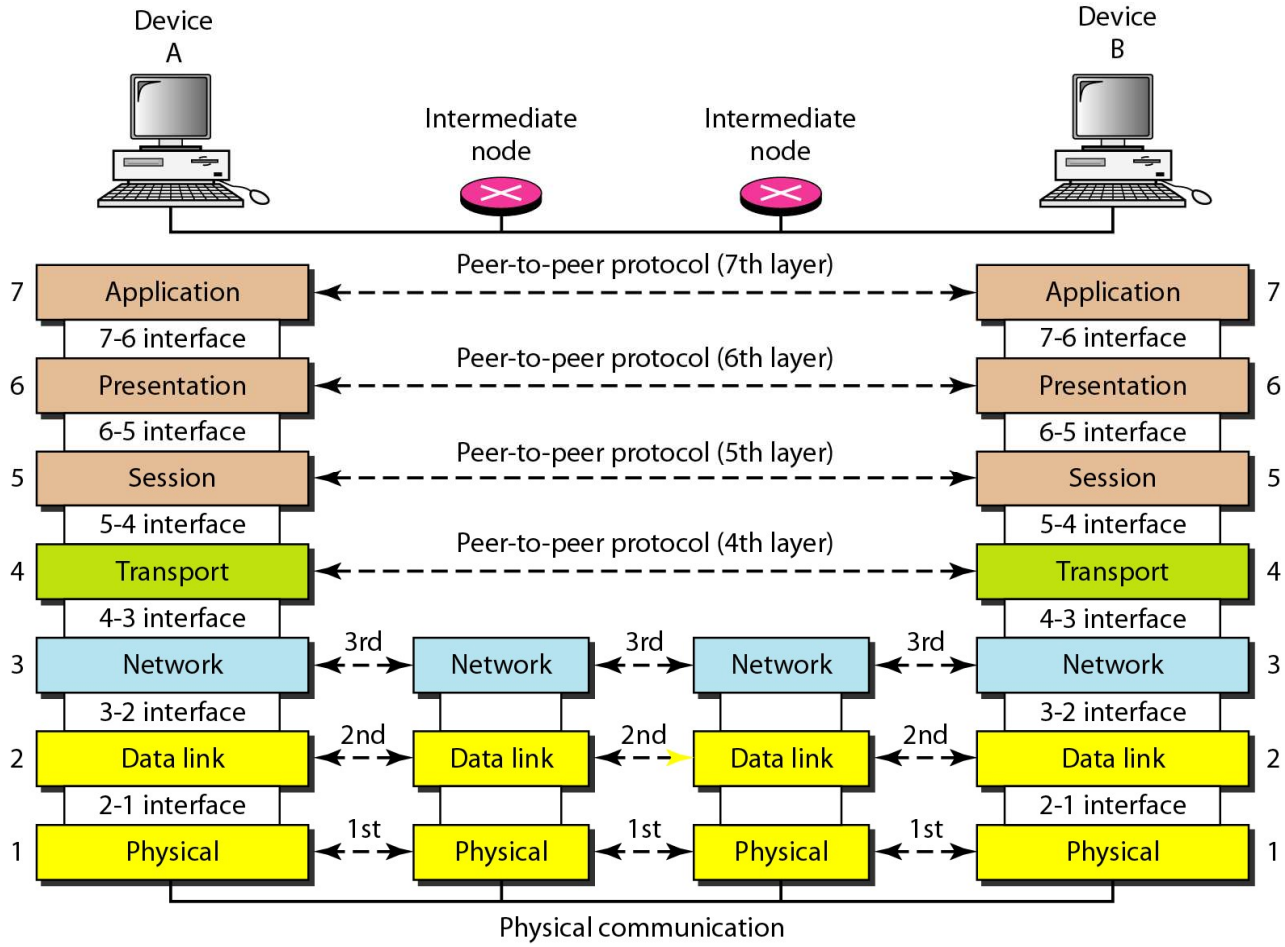
2. The OSI Model

- The International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement of international standards.
  - 7 layer
  - Layer defines a segment of the process of moving information across a network

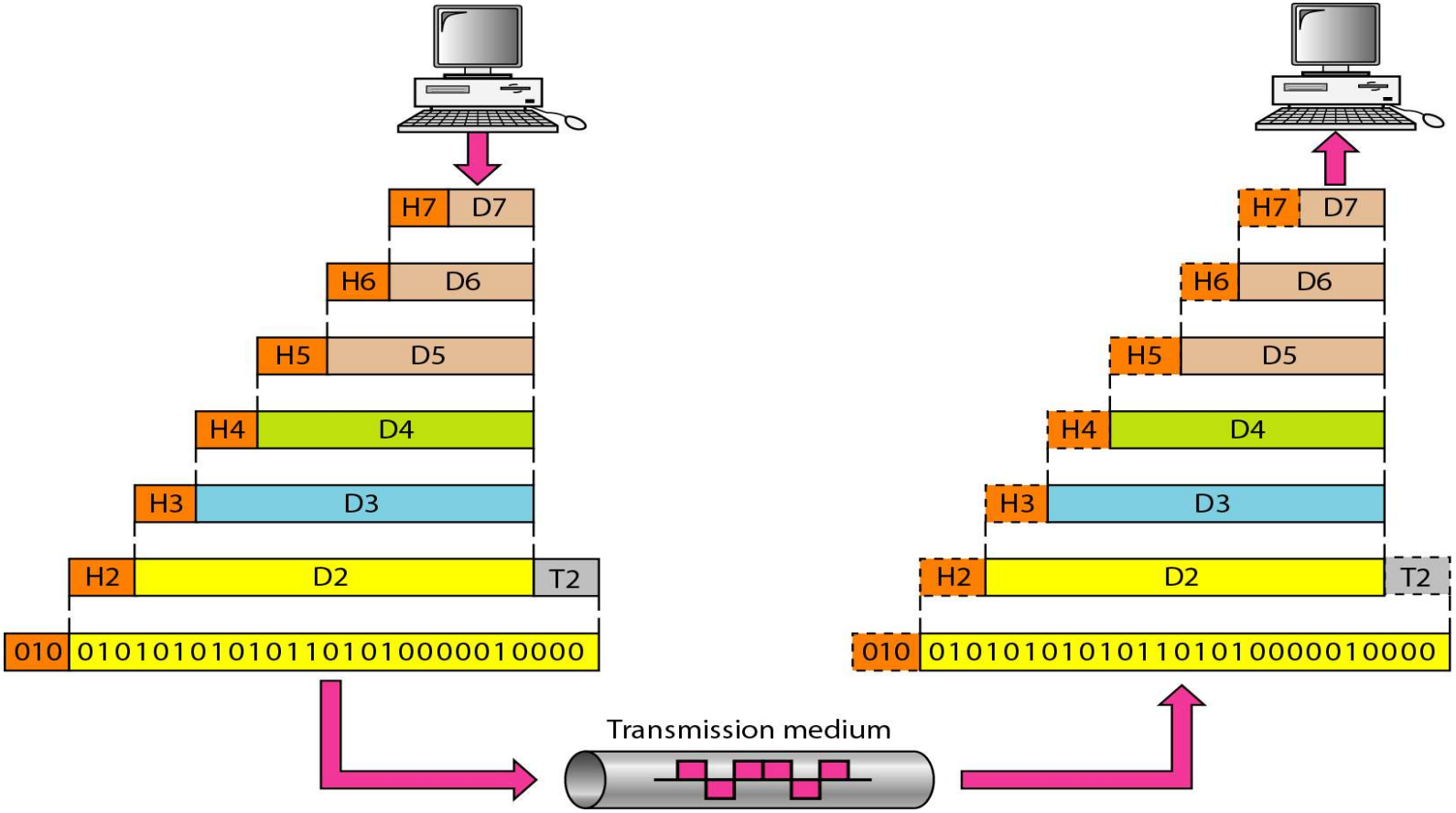


Network Models

- Layers involved when a message is sent from device A to device B
  - may pass through many intermediate nodes
  - intermediate nodes usually involve only the first three layers of the model



Peer-to-Peer Process



2. The OSI Model

Network Models

- interfaces between layers
  - data passing is made possible by an interface between each pair of adjacent layers
  - defines what information and services a layer must provide for above layer
  - provide modularity → specific implementation of a layer's functions can be modified or replaced without requiring changes to the surrounding layers
- organization of the layers
  - L1, 2, and 3 → network support layer
    - deal with the physical aspects of moving data from device to another
    - such as electrical specifications, physical connections, physical addressing, transport timing and reliability
  - L5, 6, and 7 → user support layer
    - allows interoperability among unrelated software system
  - L4 → links the two subgroups
    - ensures end-to-end reliable data transmission
  - header can be added at each layer
    - trailer is added at layer 2
    - at the receiver, the headers(trailers) attached at the corresponding layer are removed, and action appropriate to that layer are taken

3. Layers In the OSI Models

In this section we briefly describe the functions of each layer in the OSI model.

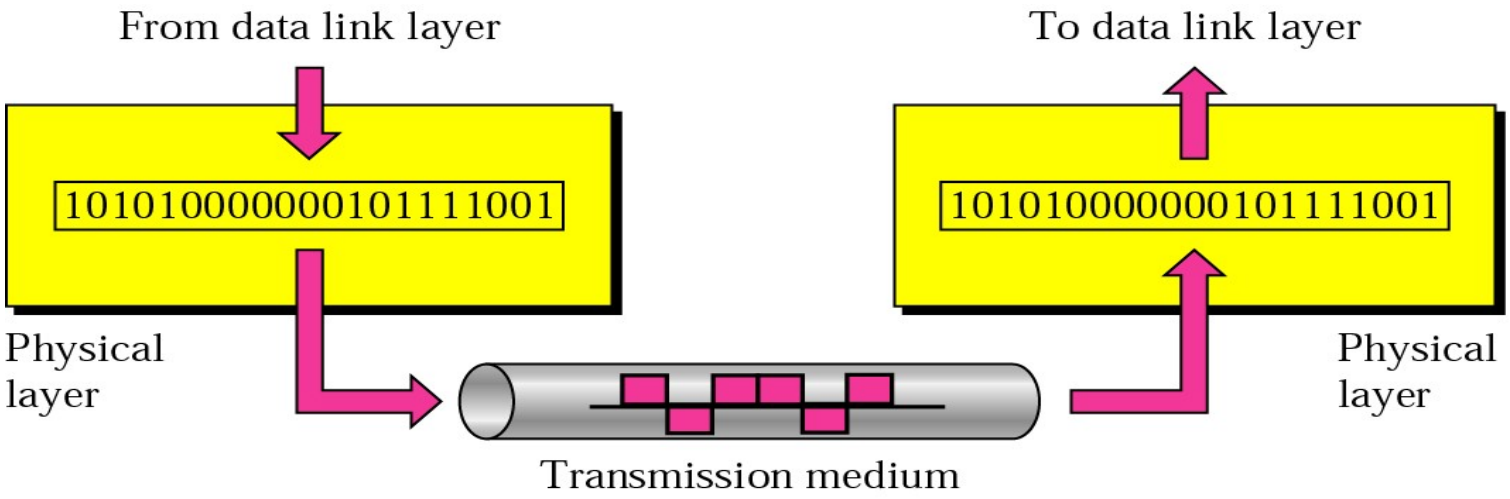
Topics discussed in this section:

Physical Layer
Data Link Layer
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer

3. Layers In the OSI Models

1) Physical Layer

- coordinates the functions required to transmit a bit stream over a physical medium



– Characteristics of interfaces and medium
  - physical, electrical, procedural, and functional characteristics of the interface between the devices and the transmission medium
  - defines the type of the transmission medium

– Representation of bits
  - defines the type of encoding
  - how 0s and 1s are changed to signals – electrical or optical

3. Layers In the OSI Models

1) Physical Layer

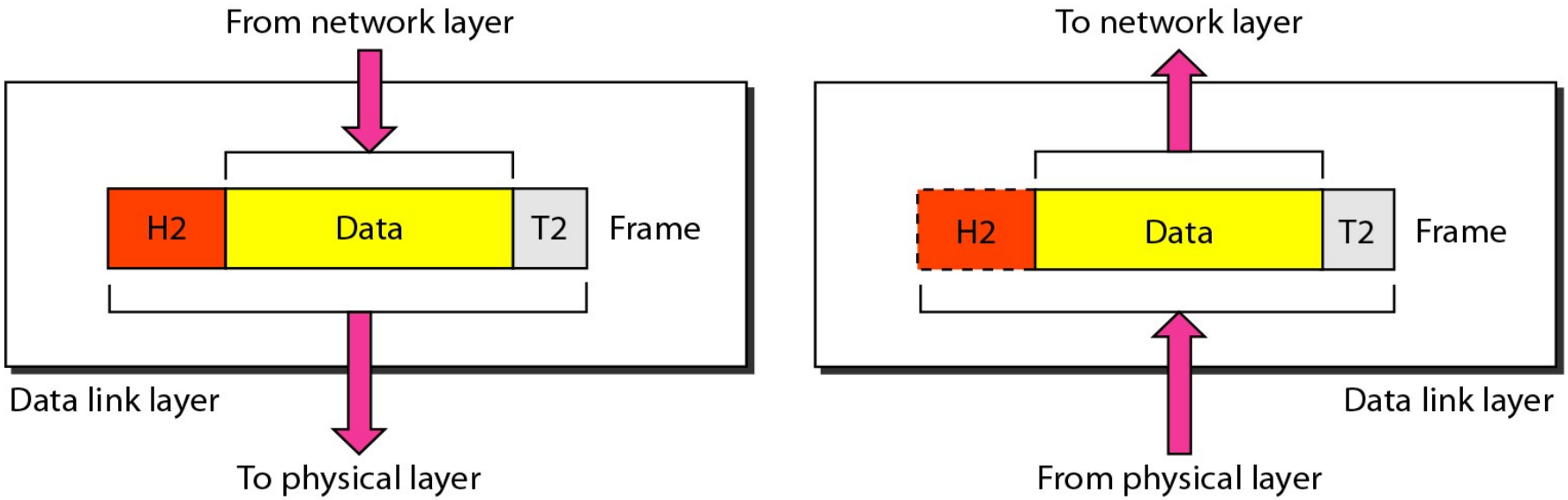
- Data rate, transmission rate : the number of bits sent each seconds
  - defines the duration of a bit
- Synchronization of bits
  - sender and receiver clocks must be synchronized
- Line configuration
  - The physical layer is concerned with the connection of device to the media
- Physical topology
  - The physical topology defines how devices are connected to make a network.
- Transmission mode
  - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

3. Layers In the OSI Models

2) Data Link Layer

- makes the physical layer appear error-free to the upper (network) layer

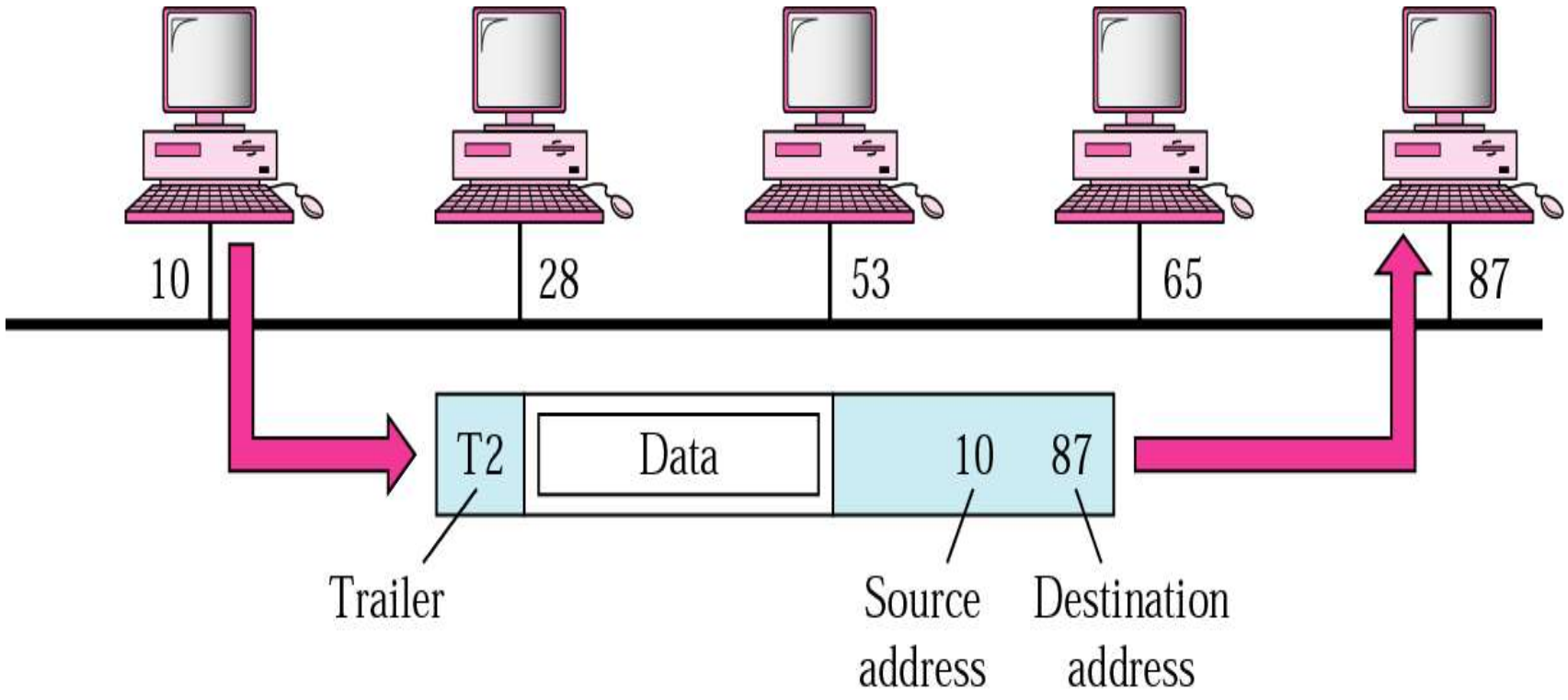


2) Data Link Layer

- responsible for node-to-node delivery
  - framing
    - divides the data stream into manageable data unit → frame
    - detection of frame at the receiver
  - physical addressing
    - adds a header to define the sender (source address) and/or receiver (destination address)
    - distribute frames to different systems on the sender's network
    - receiver address is the address of the devices that connects one network to the next if the frame is intended for a system outside the sender's network
  - flow control : necessary when data is being sent faster than it can be processed by receiver
  - error control
    - detect and retransmit damaged or lost frames to add reliability to the physical layer
    - also prevent duplication of frames
    - normally achieved through a trailer added to the end of the frames
  - access control : determines which device has control over the link at any given time when two or more devices are connected to the same link

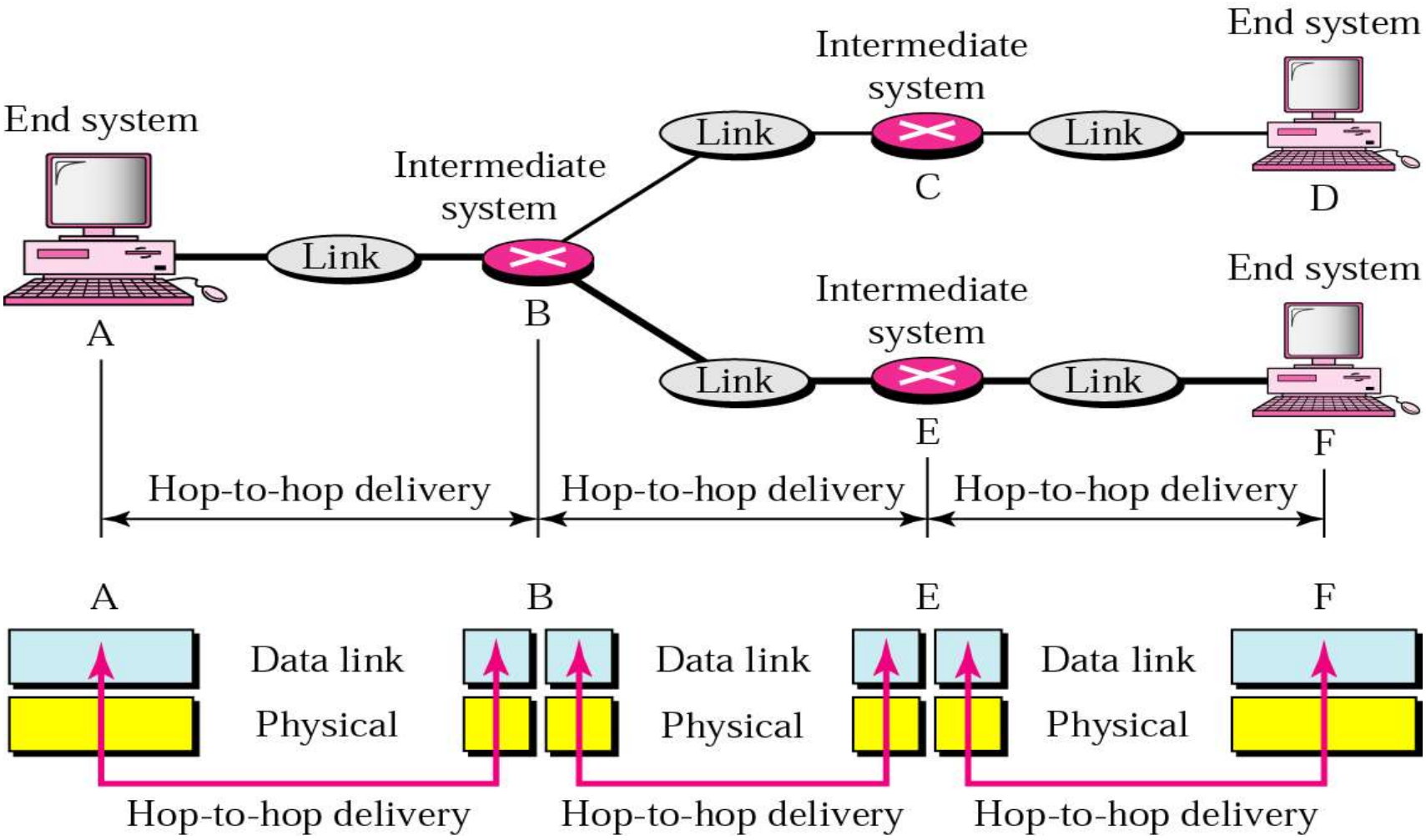
2) Data Link Layer

- Example.



2) Data Link Layer

- hop-by-hop (node-to-node) delivery concept by the data link layer



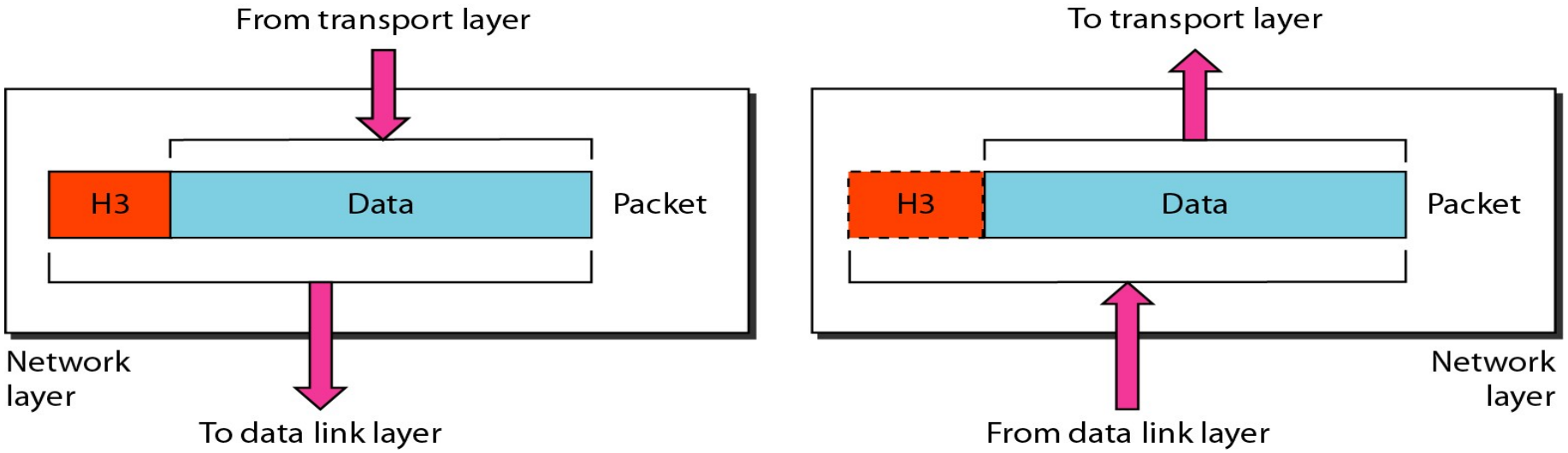
2) Data Link Layer

Note

The data link layer is responsible for moving frames from one hop (node) to the next.

3. Layers In the OSI Models

3) Network Layer

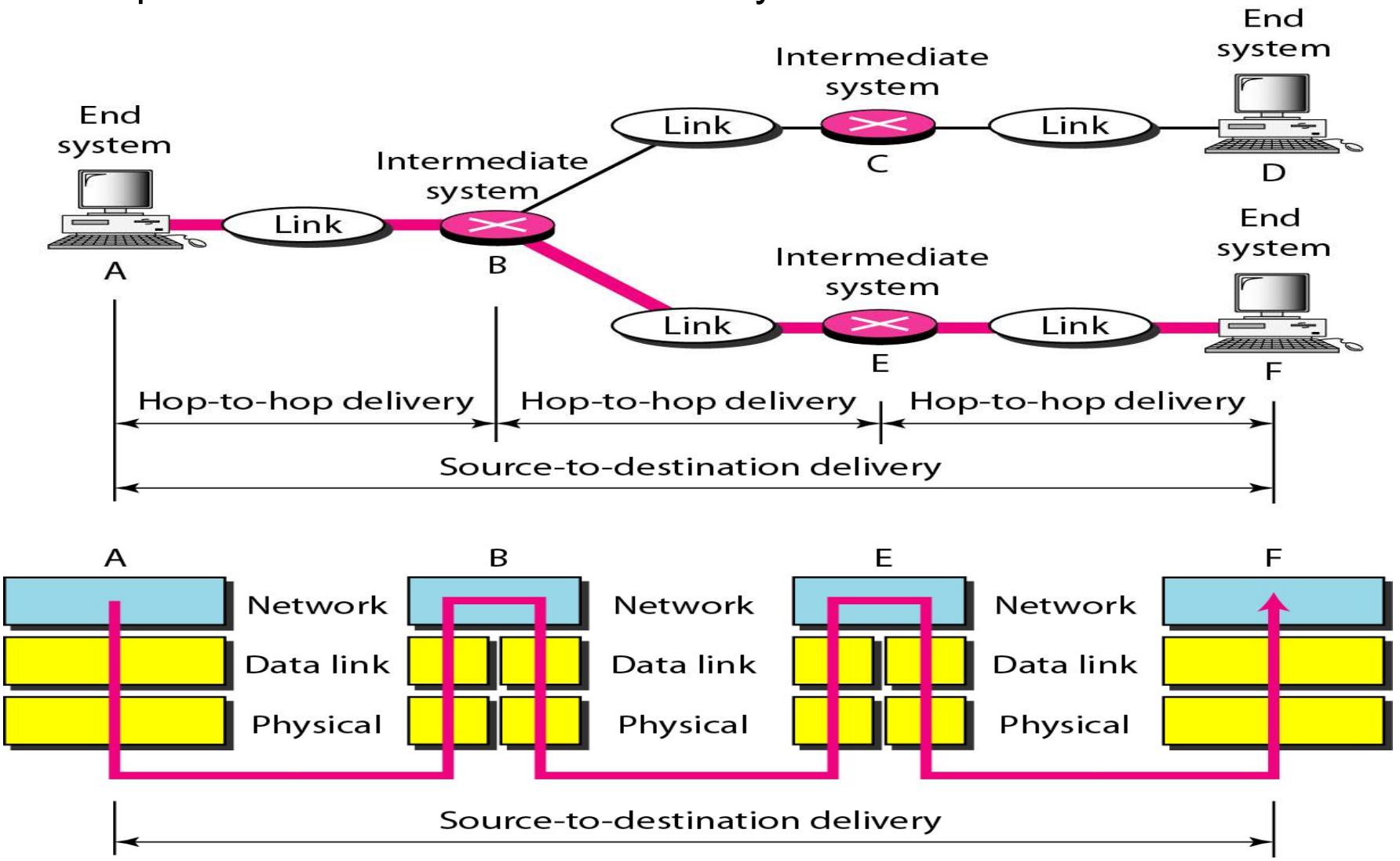


- responsible for the delivery of packets from the original source to the final destination possibly across multiple networks (links)
  - logical addressing
    - If a packet passes the network boundary, we need it to help distinguish the source and destination systems
  - routing
    - in the internet, connecting devices (called routers or switches) route or switch the packets to their final destination

3. Layers In the OSI Models

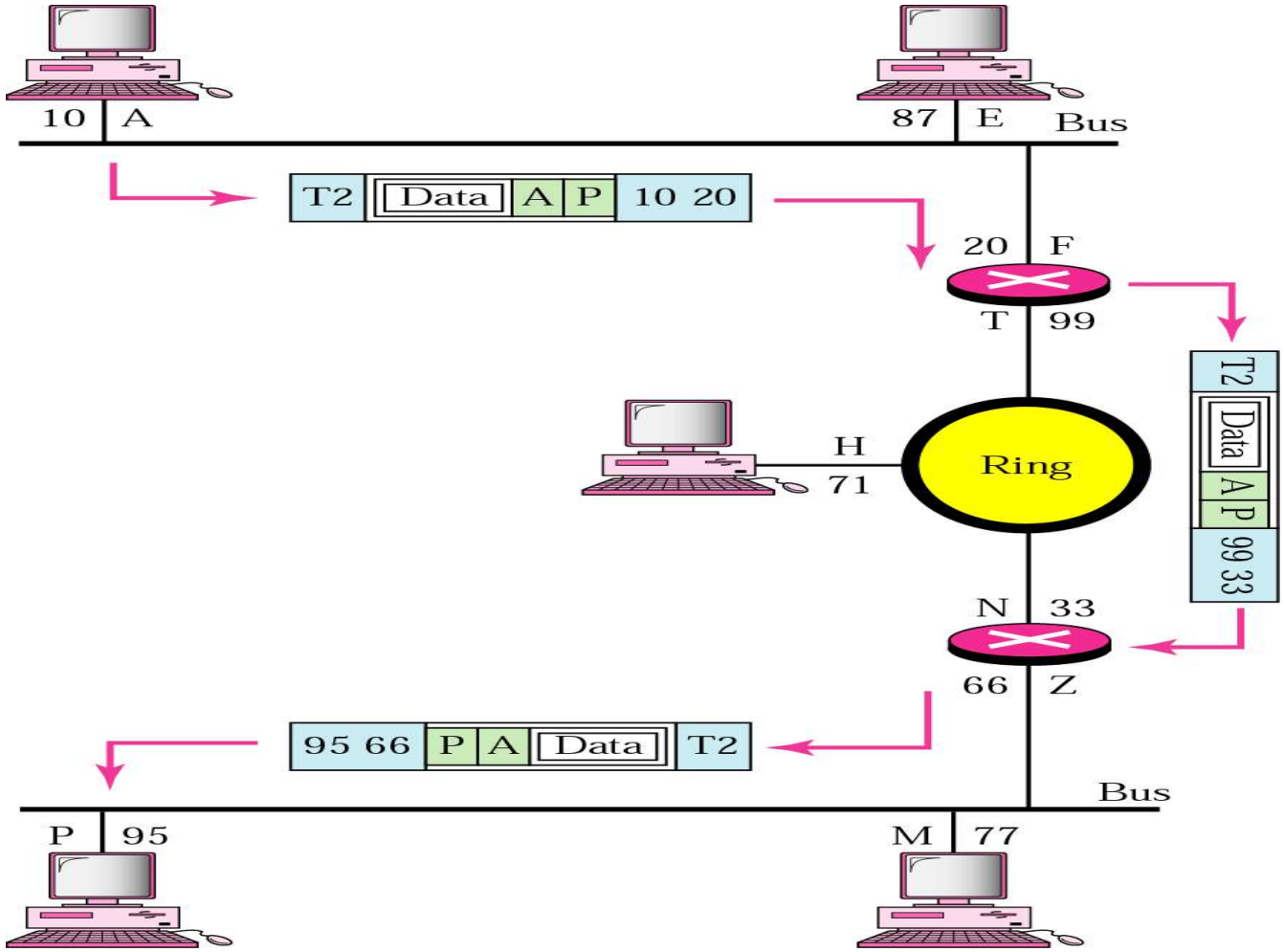
3) Network Layer

- concept of source-to-destination delivery



3) Network Layer

- Example.



3) Network Layer

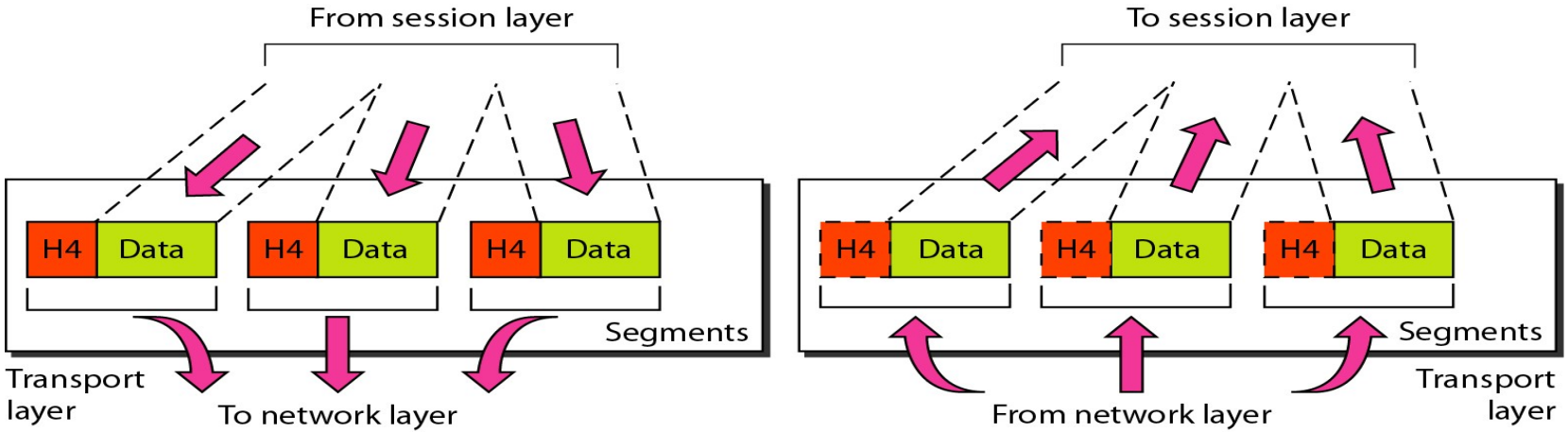
Note

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

3. Layers In the OSI Models

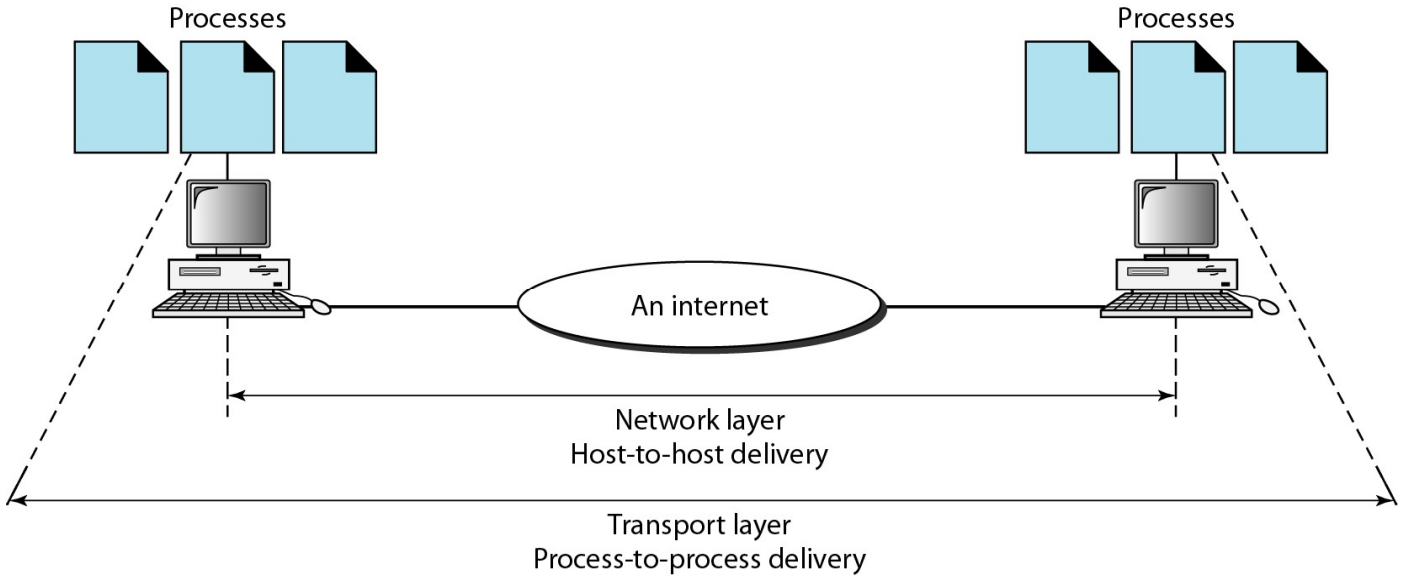
4) Transport Layer

- responsible for process-to-process delivery of the entire message
  - treats each packet independently
  - ensures that the whole message arrives intact and in order
  - use both error control and flow control at the source-to-destination level
- port addressing
  - computers often run several processes (running program) at the same time
  - process-to-process delivery means delivery to a specific process
  - header must therefore include a type of address called port address
- segmentation and reassembly
  - a message is divided into transmittable segments at the sender
  - reassemble the message correctly upon arriving at the receiver



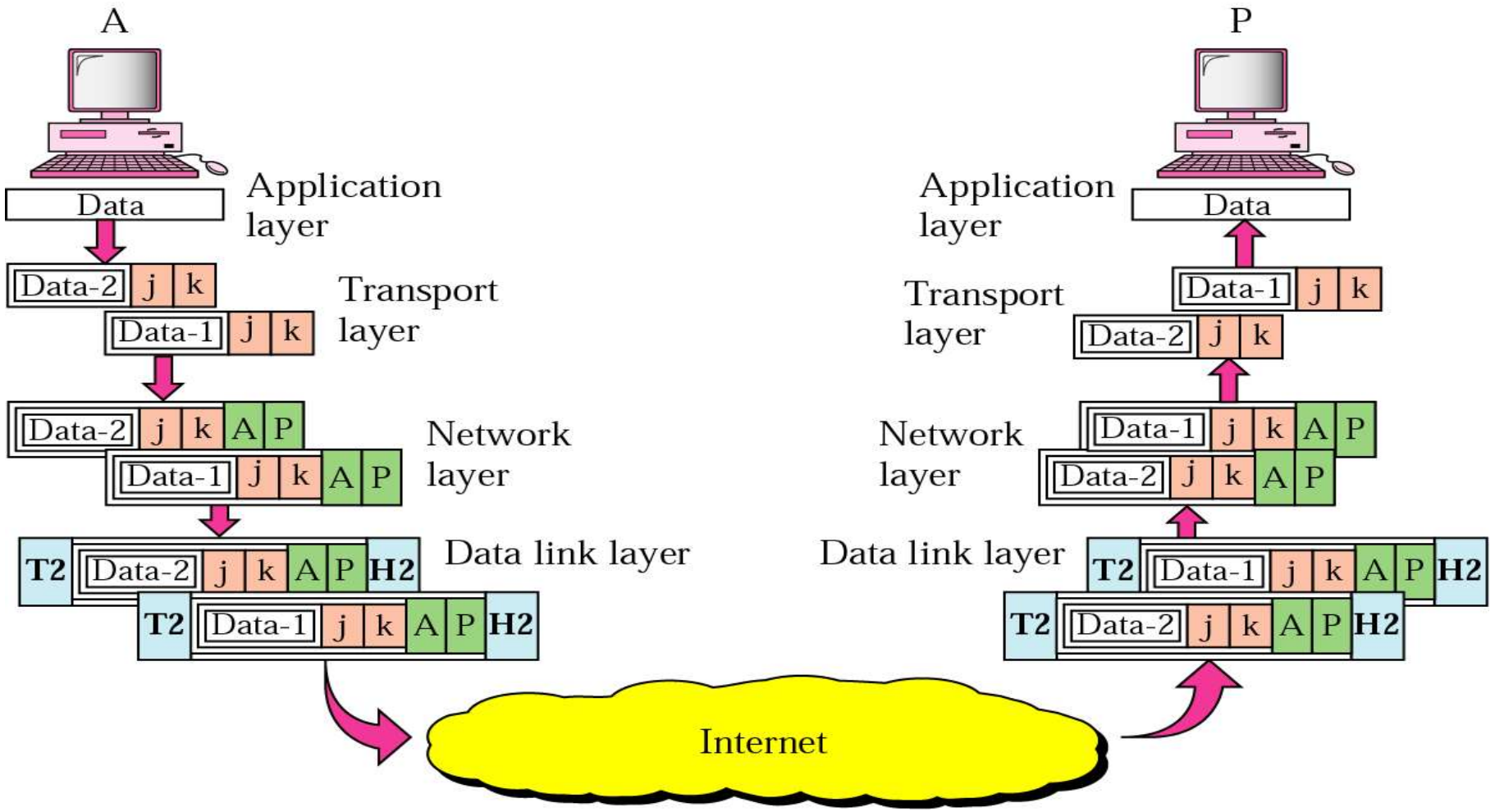
4) Transport Layer

- connection control
  - connectionless mode : treats each segment as an independent packet
  - connection-oriented mode : needs connection control
    - make a connection with the transport layer at the destination machine before delivering the packets
    - after all the data are transferred, the connection is terminated
    - has more control over sequencing, flow and error control
- flow control : end-to-end flow control rather than across a single link
- error control : end-to-end error control rather than across a single link



4) Transport Layer

- Example



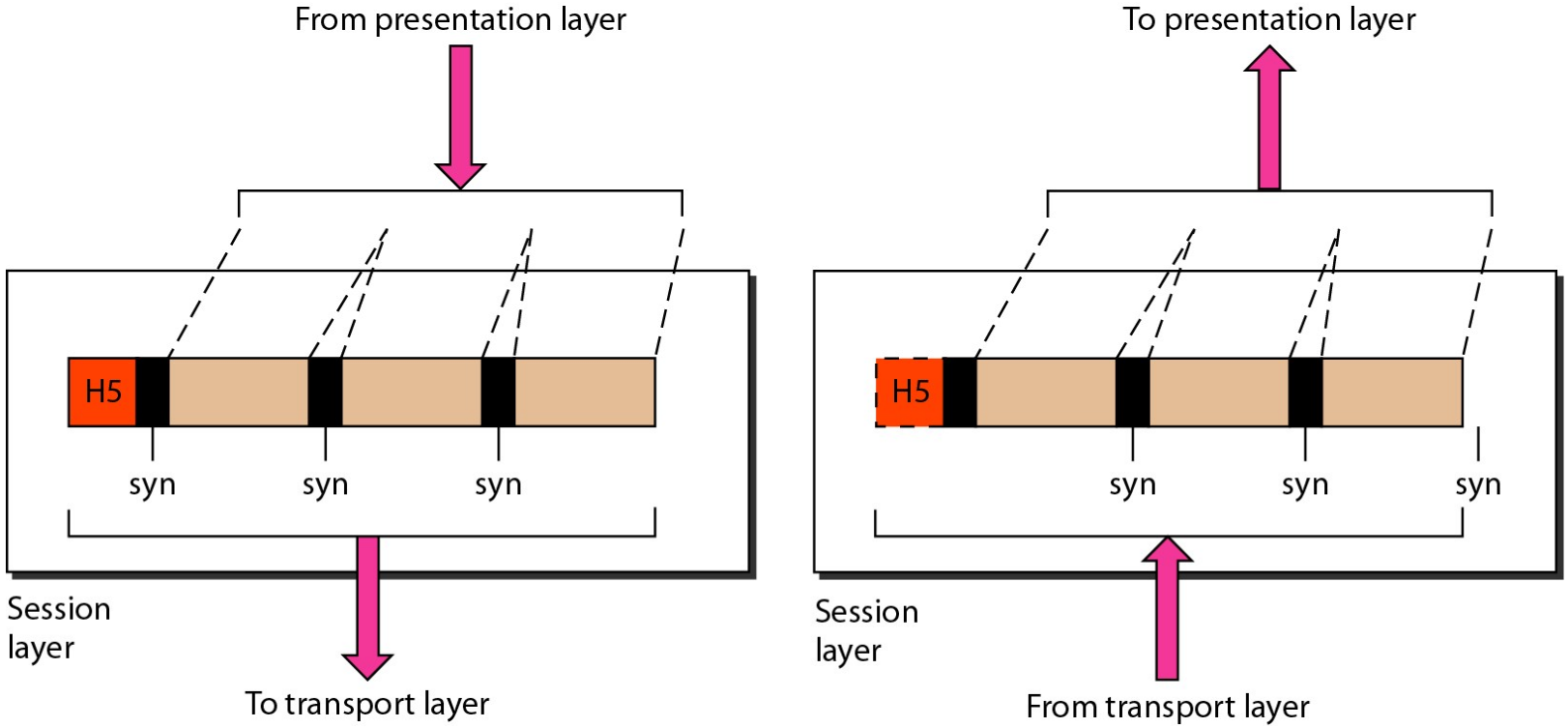
4) Transport Layer

Note

The transport layer is responsible for the delivery of a message from one process to another.

5) Session Layer

- the session layer is responsible for dialog control and synchronization.
- Dialog control : the Session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex
- Synchronization : the Session layer allows a process to add checkpoints, or synchronization points, to a stream of data.



5) Session Layer

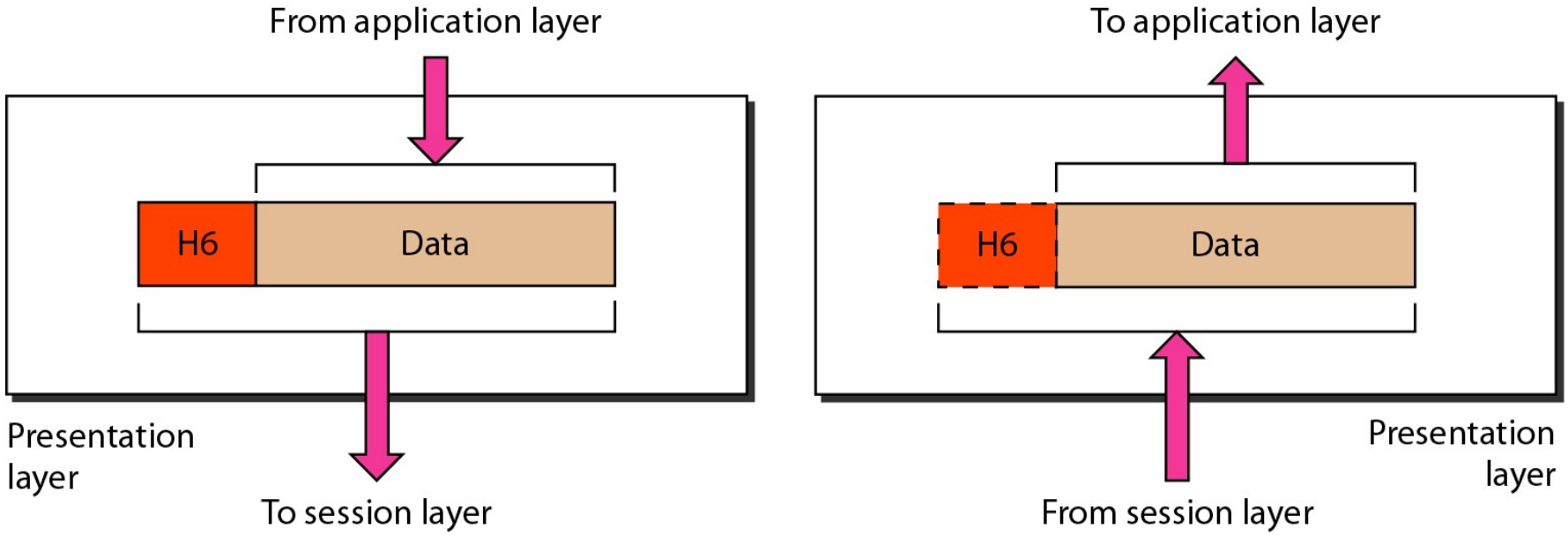
Note

The session layer is responsible for dialog control and synchronization.

3. Layers In the OSI Models

6) Presentation Layer

- responsible for translation, compression, and encryption.
- Translation : the processes in two systems are usually exchanging information in the form of character string, number, and so on.
- Encryption : to carry sensitive information, a system must be able to ensure privacy.
- Compression : Data compression reduces the number of bits contained in the information



6) Presentation Layer

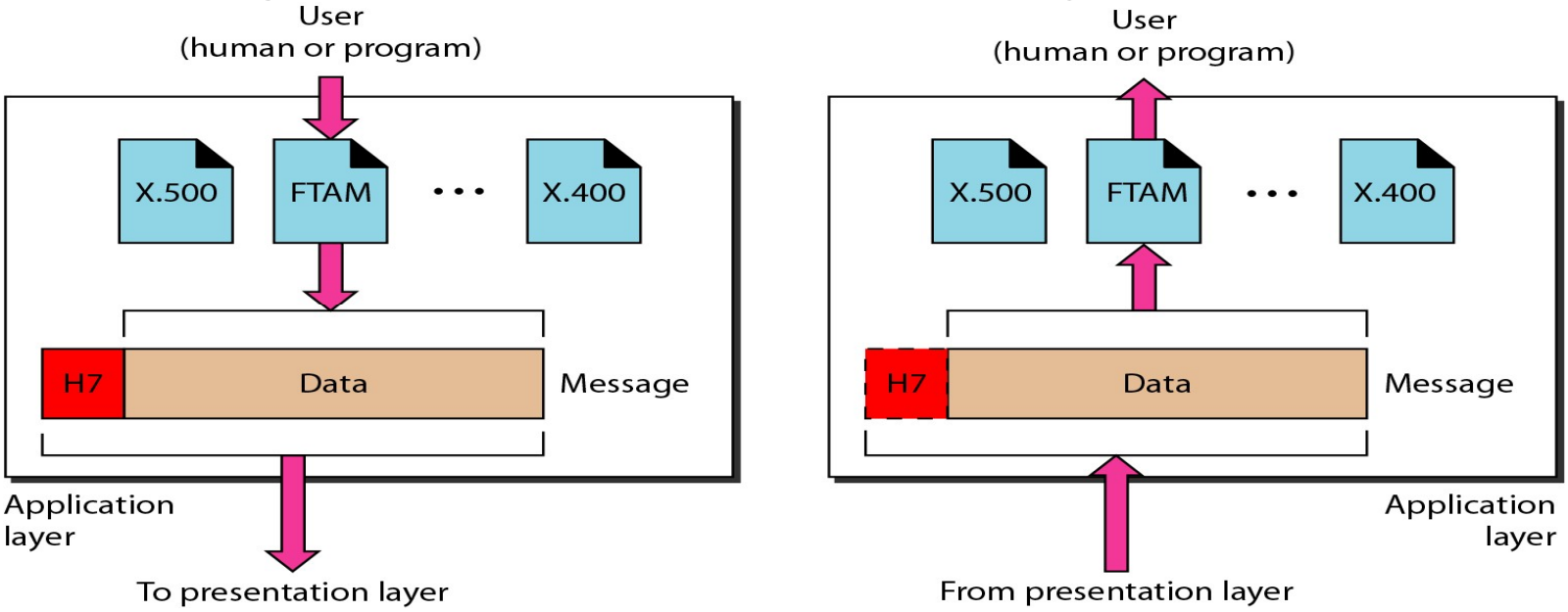
Note

The presentation layer is responsible for translation, compression, and encryption.

3. Layers In the OSI Models

7) Application Layer

- responsible for providing services to the user.
- **Network virtual terminal** : a network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File transfer, access, and management** : this application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally
- **Mail services** : this application provides distributed database sources and access for global information about various objects and services.



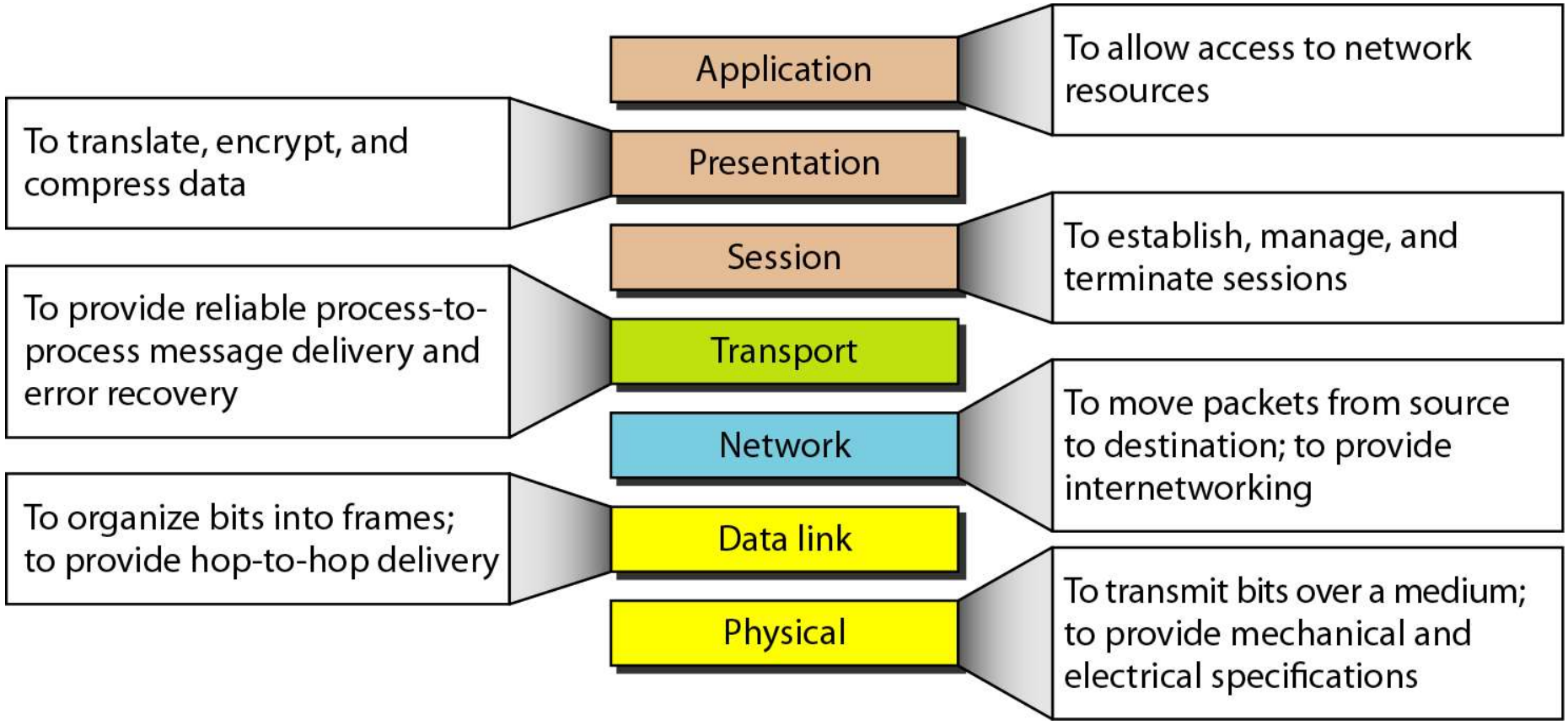
7) Application Layer

Note

The application layer is responsible for providing services to the user.

3. Layers In the OSI Models

Summary of Layers



4. TCP/IP Protocol Suite

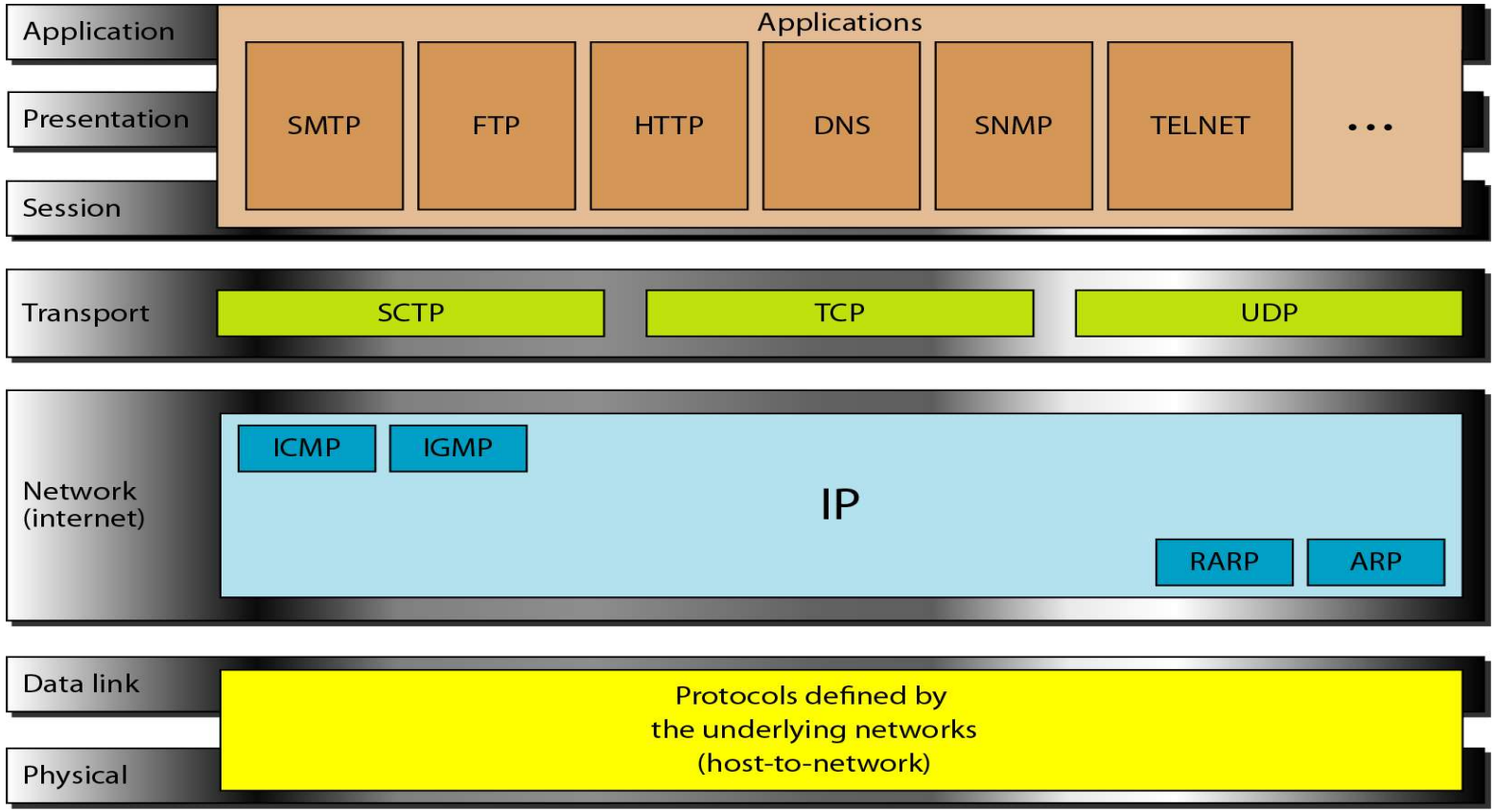
The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

Topics discussed in this section:

Physical and Data Link Layers
Network Layer
Transport Layer
Application Layer

4. TCP/IP Protocol Suite

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.



4. TCP/IP Protocol Suite

- Physical and Data Link Layers
  - At the physical and data link layer, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols.

- Network layer
  - Supports the Internetworking Protocol. IP, in turn, uses four supporting protocols, ARP, RARP, ICMP, and IGMP.
  - Internetworking Protocol (IP)
    - the transmission mechanism used by the TCP/IP protocols.
    - an unreliable and connectionless protocol - a best-effort delivery service.
    - IP transports data in packets called datagrams
    - The limited functionality of IP should not be considered a weakness, however IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.
  - Address Resolution Protocol (ARP)
    - ARP is used to associate a logical address with a physical address
    - ARP is used to find the physical address of the node when its Internet address is known.

4. TCP/IP Protocol Suite

- Reverse Address Resolution Protocol (RARP)
  - RARP allows a host to discover its Internet address when it knows only its physical address.

- Internet Control Message Protocol (ICMP)
  - ICMP is a mechanism used by host and gateways to send notification of datagram problems back to the sender.

- Internet Group Message Protocol (IGMP)
  - IGMP is used to facilitate the simultaneous transmission of a message to group of recipients.

4. TCP/IP Protocol Suite

- Transport layer
  - Represented in TCP/IP by two protocols : TCP and UDP
  - IP is a host-host protocol, it can deliver a packet from one physical device to another.
  - TCP and UDP are transport level protocols responsible for delivery of a message from a process to another process.
  - User Datagram Protocol (UDP)
    - UDP is the simpler of the two standard TCP/IP transport protocols
    - A process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.
  - Transmission Control Protocol (TCP)
    - TCP provides full transport-layer services to applications.
    - TCP is a reliable stream transport protocol. Cf. The term stream means a connection-oriented.
  - Stream Control Transmission Protocol (SCTP)
    - SCTP provides support for newer applications such as voice over the Internet protocol (VoIP).

4. TCP/IP Protocol Suite

- Application Layer
  - The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.
  - Many protocols are defined at this layer.

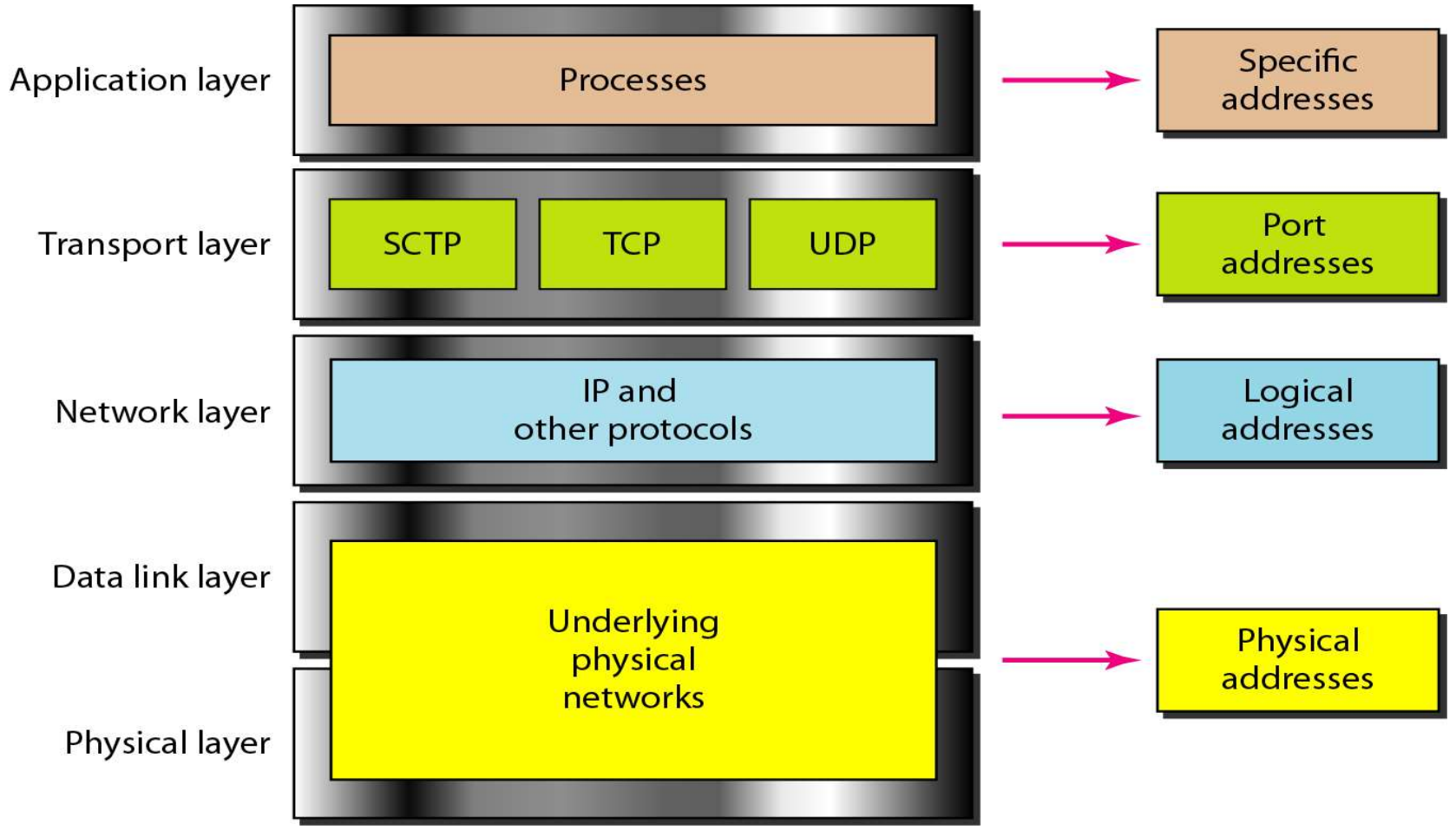
Summary

- The OSI-7 model defines seven layers: physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.
- The physical layer coordinates the functions required to transmit a bit stream over a physical medium.
- The data link layer is responsible for delivering data units from one station to the next without errors.
- The network layer is responsible for the source-to-destination delivery of a packet across multiple network links.
- The transport layer is responsible for the process-to-process delivery of the entire message.
- The application layer enables the users to access the network.

Appendix

- TCP/IP model -

1) Addresses in TCP/IP Model



2) Ethernet

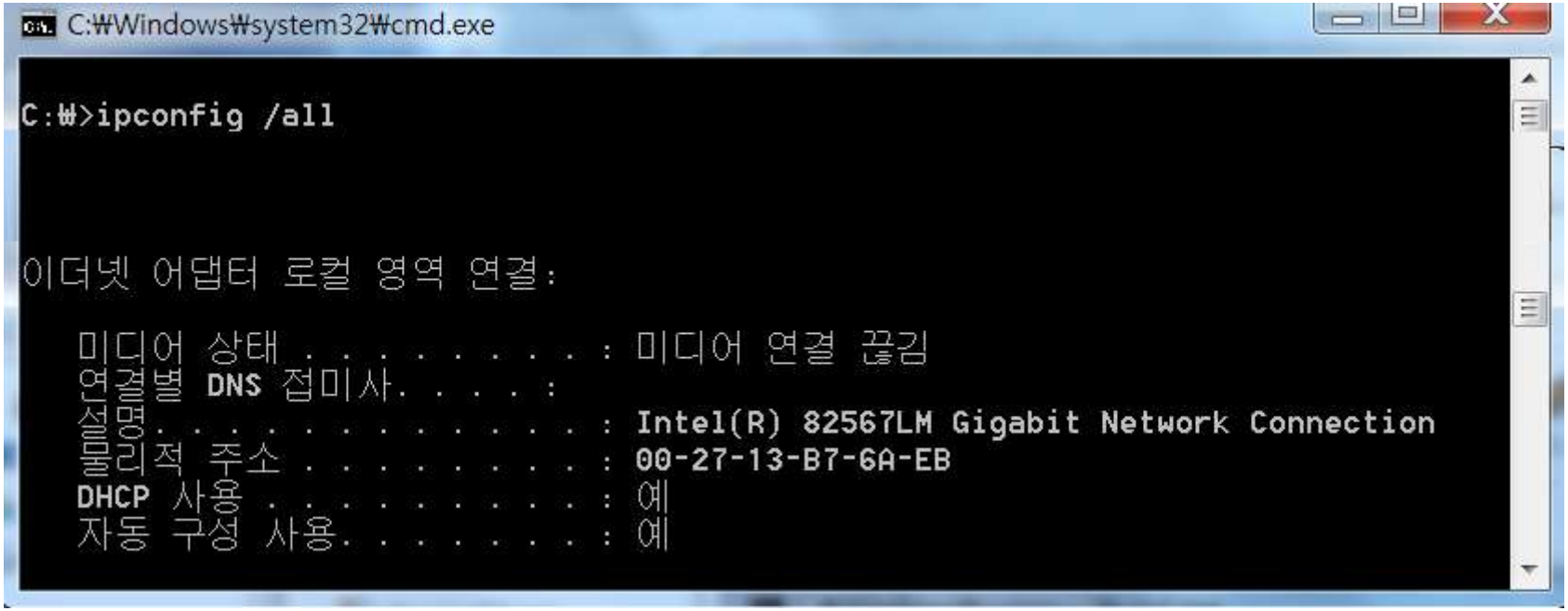
- A frame-based networking technologies for local area networks (LAN).
- Standardization of LAN: IEEE 802.3
- Speed: 10Mbps → 100Mbps → 1Gbps → 10Gbps → 40Gbps/100Gbps
- IEEE 802.3 Ethernet frame structure

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype or length	Payload	Cyclic redundancy check	Interframe gap
7 octets of 10101010	1 octet of 10101011	6 octets	6 octets	(4 octets)	2 octets	46–1500 octets	4 octets	12 octets
		64–1522 octets						
72–1530 octets								
84–1542 octets								

Physical Address

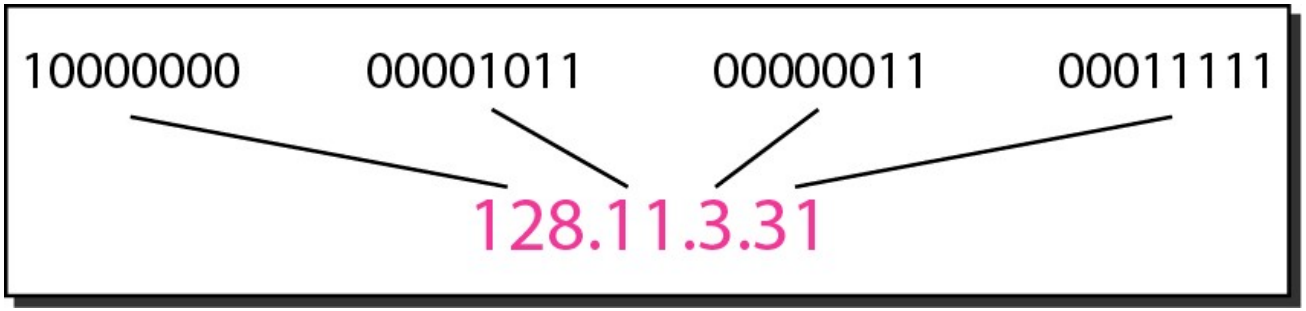
- Physical Address = Ethernet Address
  - The address of a node as defined by its LAN.
  - 48-bit (6-byte) physical address written as 12 hexadecimal digits; as shown below:

00-27-13-B7-6A-EB



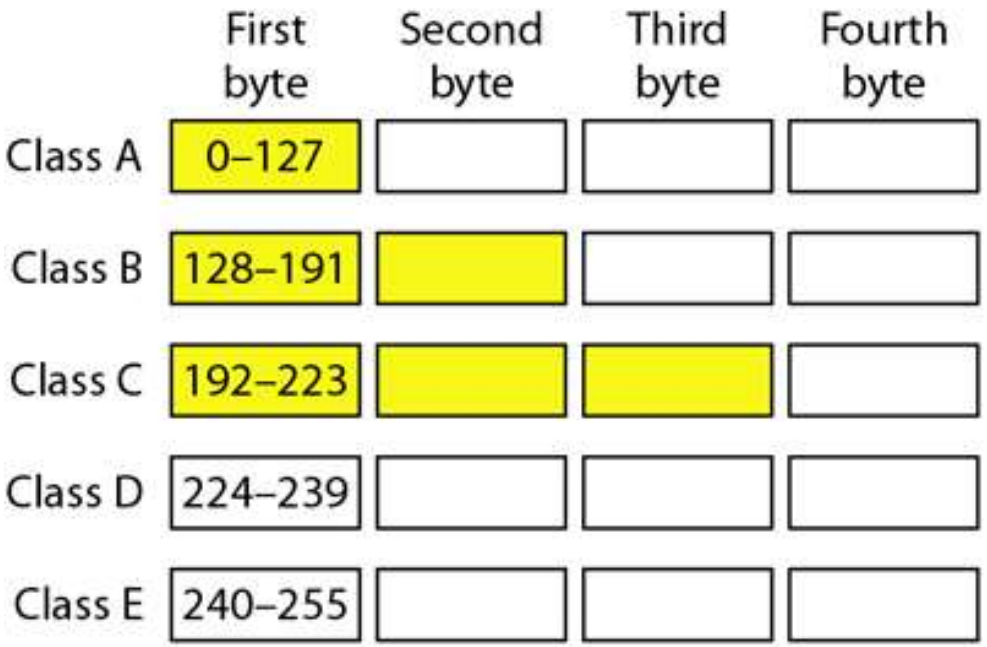
3) IP (Internet Protocol)

- The transmission mechanism used by the TCP/IP protocols.
- An unreliable and connectionless protocol - a best-effort delivery service.
- IP transports data in packets called datagrams.
- The IPv4 addresses are unique and universal.
  - IPv4: 32 bits (4 byte), 2^{32} or 4,294,967,296.
  - IPv6: 128 bits (16 byte): 2^{128}



IP Address

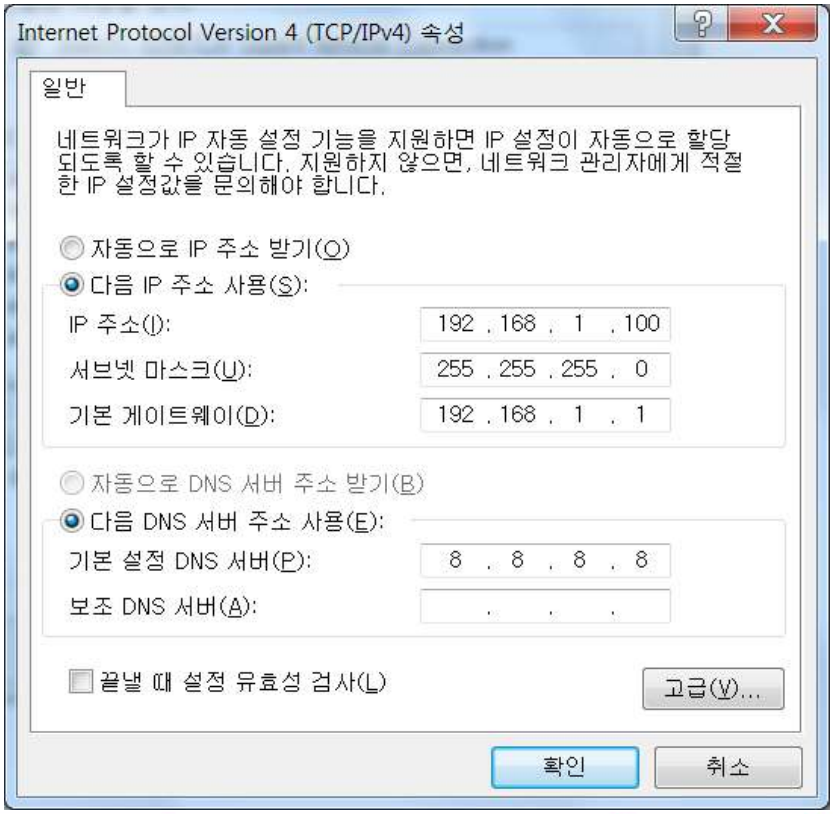
- The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations.



- Class A: large organizations.
- Class B: midsize organizations.
- Class C: small organizations.
- Class D: multicasting.
- Class E: reserved for future use.

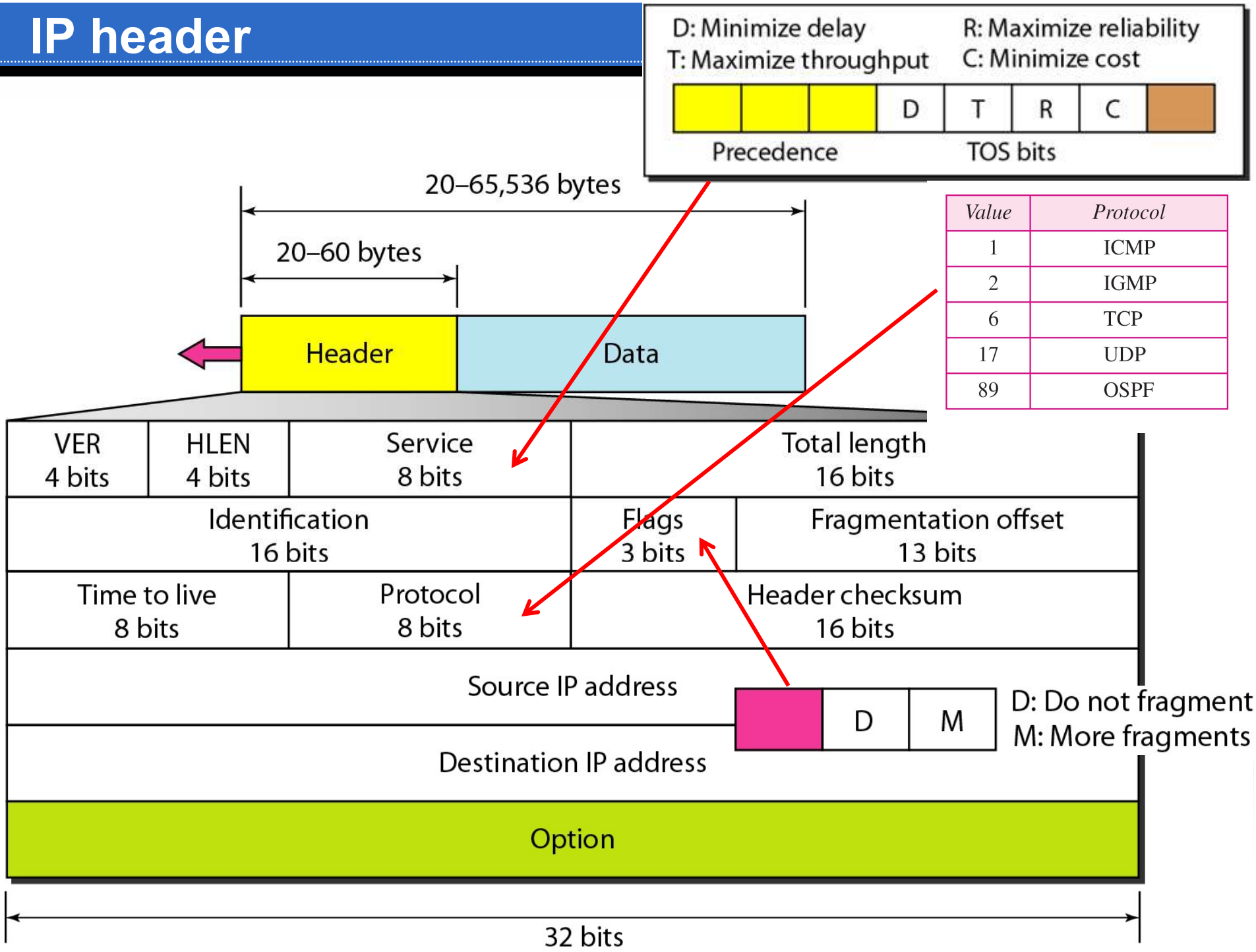
Subnet Mask

- Network part: ‘1’ of subnet mask
- Host part: ‘0’ of subnet mask



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

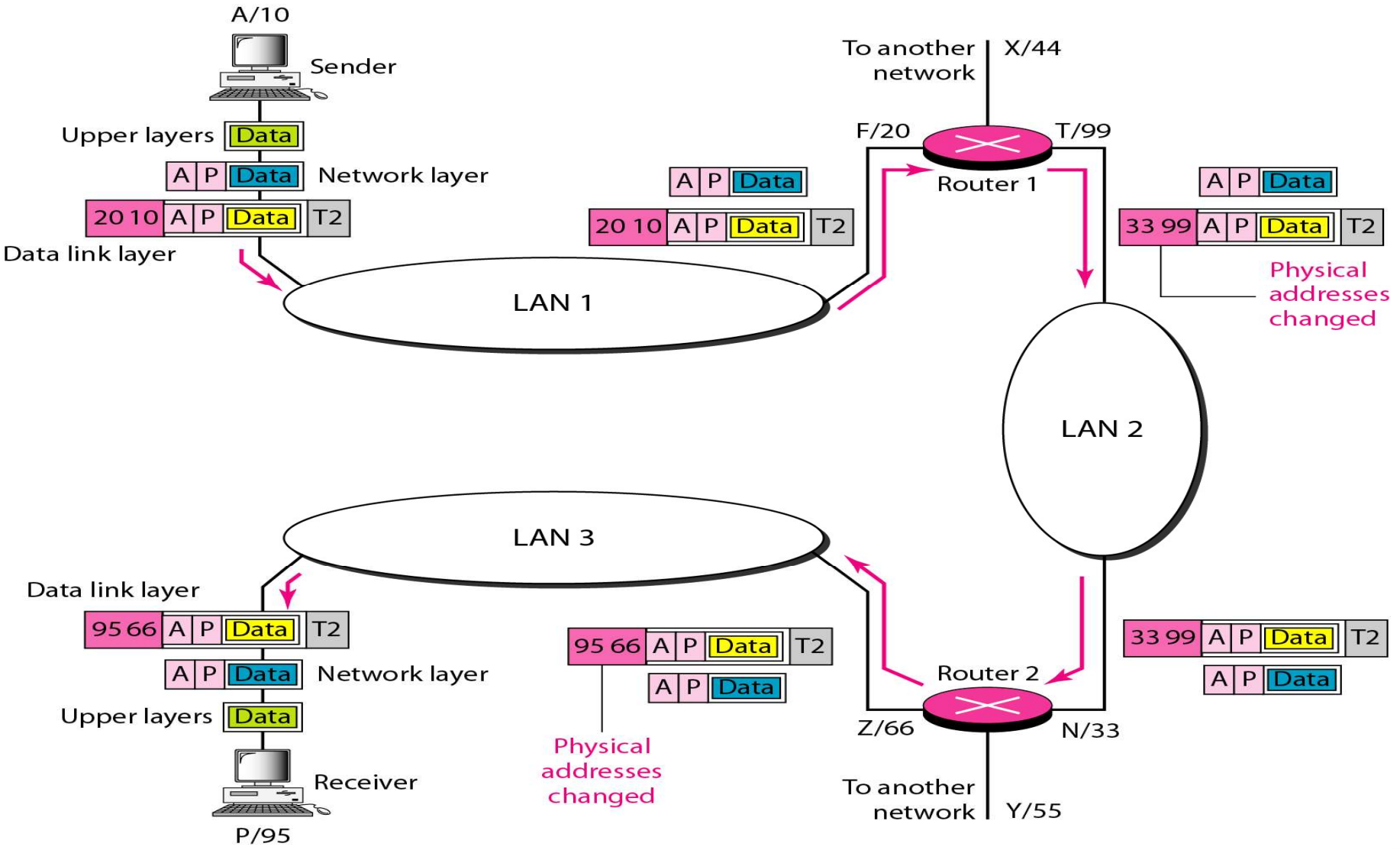
IP header



Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

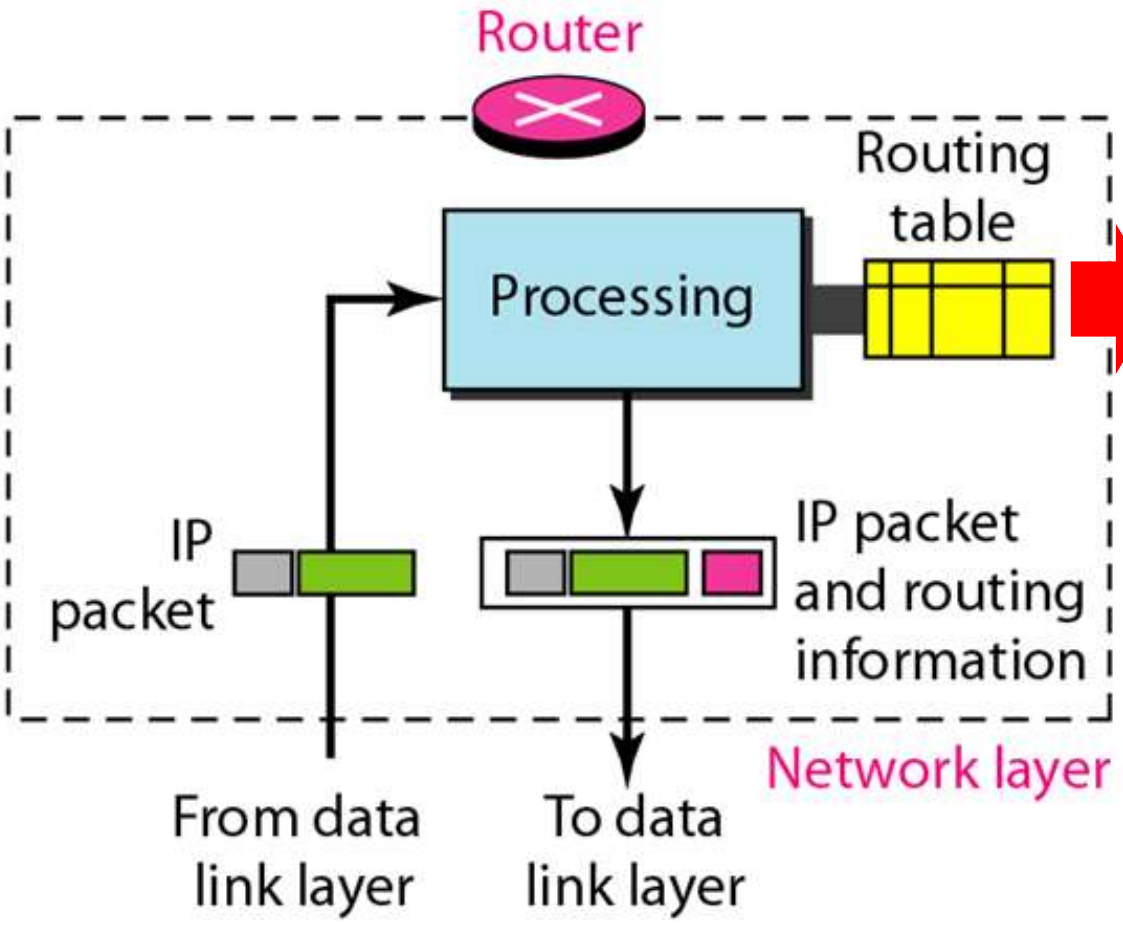
Packet Delivery (1/2)

- The physical addresses will change form hop to hop, but the logical addresses usually remain the same.



Packet Delivery (2/2)

- Router at the Network layer



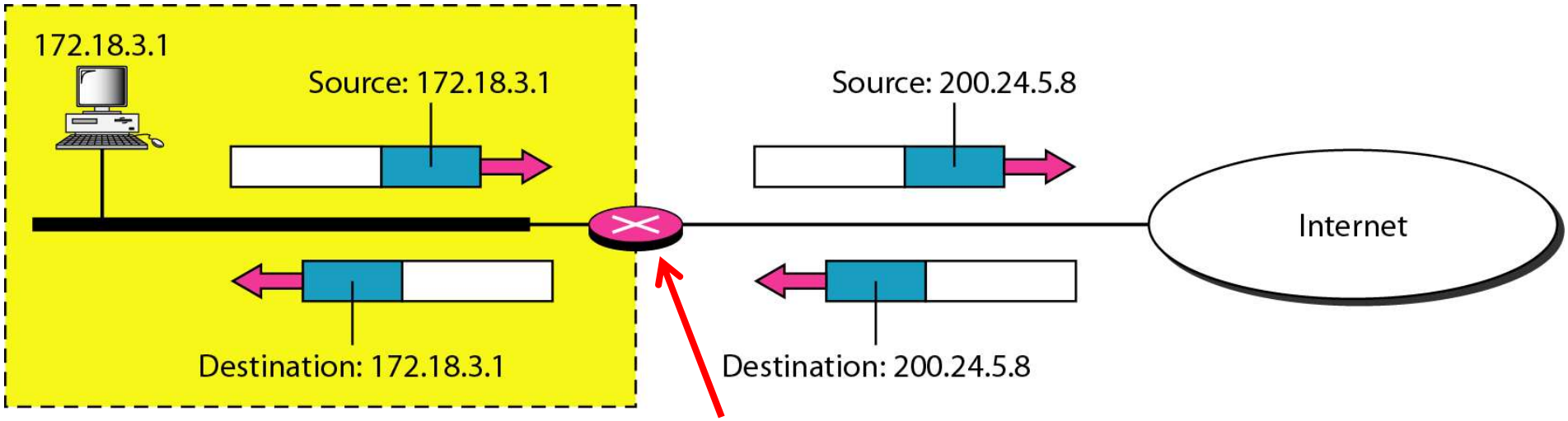
Mask (/n)	Network address	Next-hop address	Interface
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

Routing protocols

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)

NAT (Network Address Translation)

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

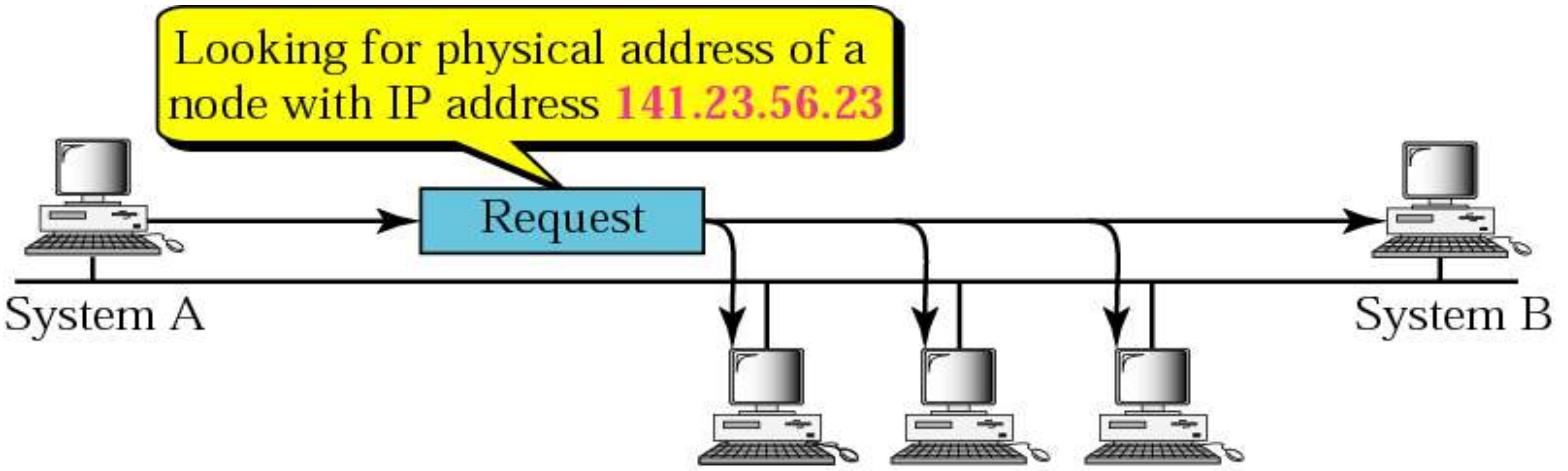


Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
. . .	. . .	. . .	. . .	. . .

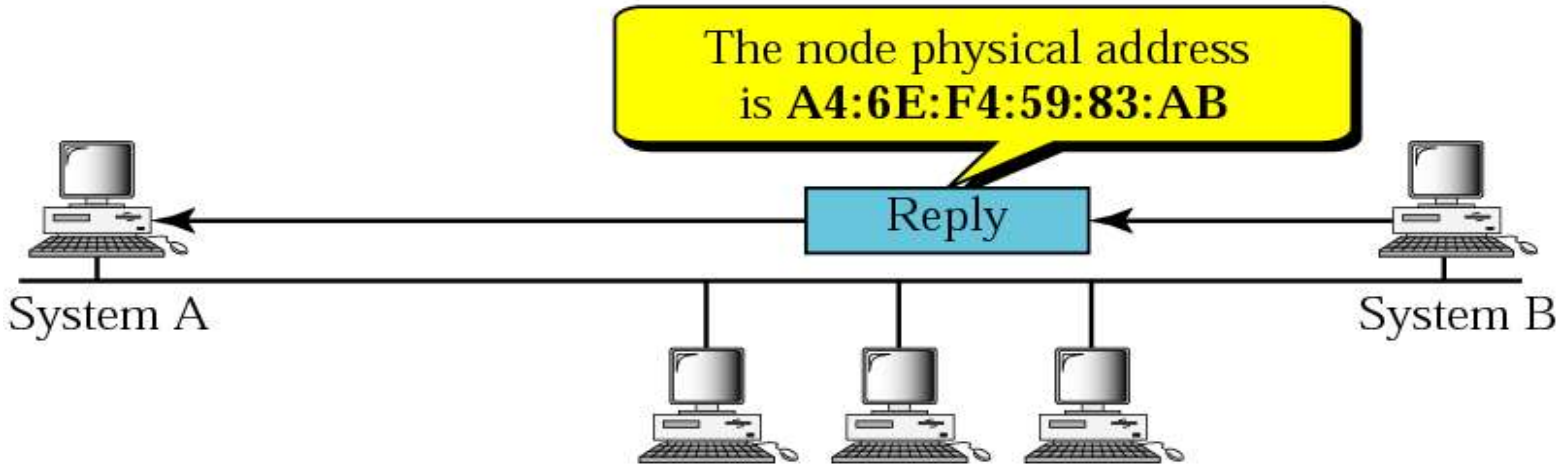
ARP, RARP, ICMP, IGMP

- Address Resolution Protocol (ARP)
  - ARP is used to find the physical address of the node when its Internet address is known.
- Reverse Address Resolution Protocol (RARP)
  - RARP allows a host to discover its Internet address when it knows only its physical address.
- Internet Control Message Protocol (ICMP)
  - ICMP is a mechanism used by host and gateways to send notification of datagram problems back to the sender.
- Internet Group Message Protocol (IGMP)
  - IGMP is used to facilitate the simultaneous transmission of a message to group of recipients.

ARP (1/2)



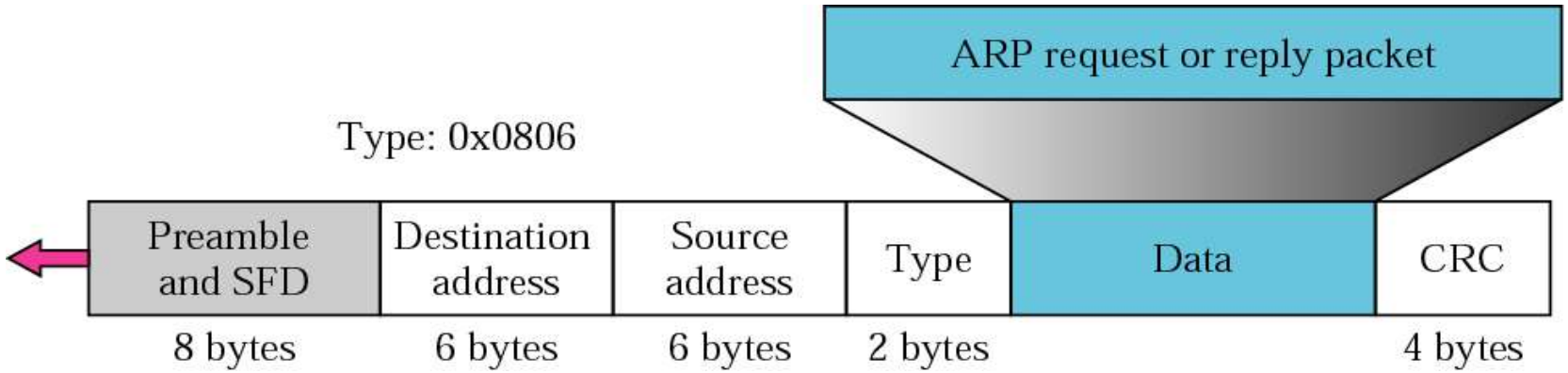
a. ARP request is broadcast



b. ARP reply is unicast

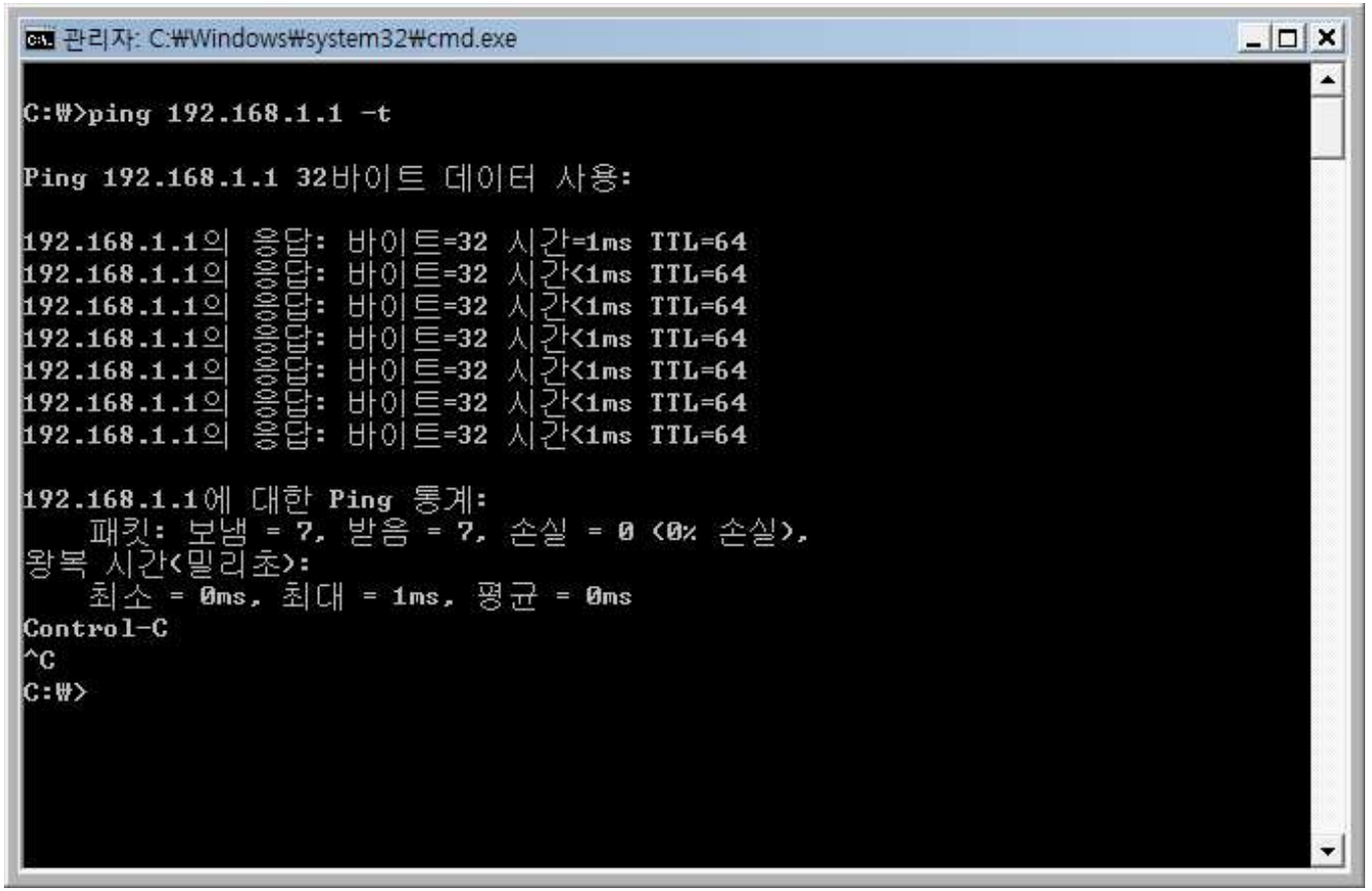
ARP (2/2)

Hardware Type Ethernet (1)		Protocol Type IPv4 (0800)
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

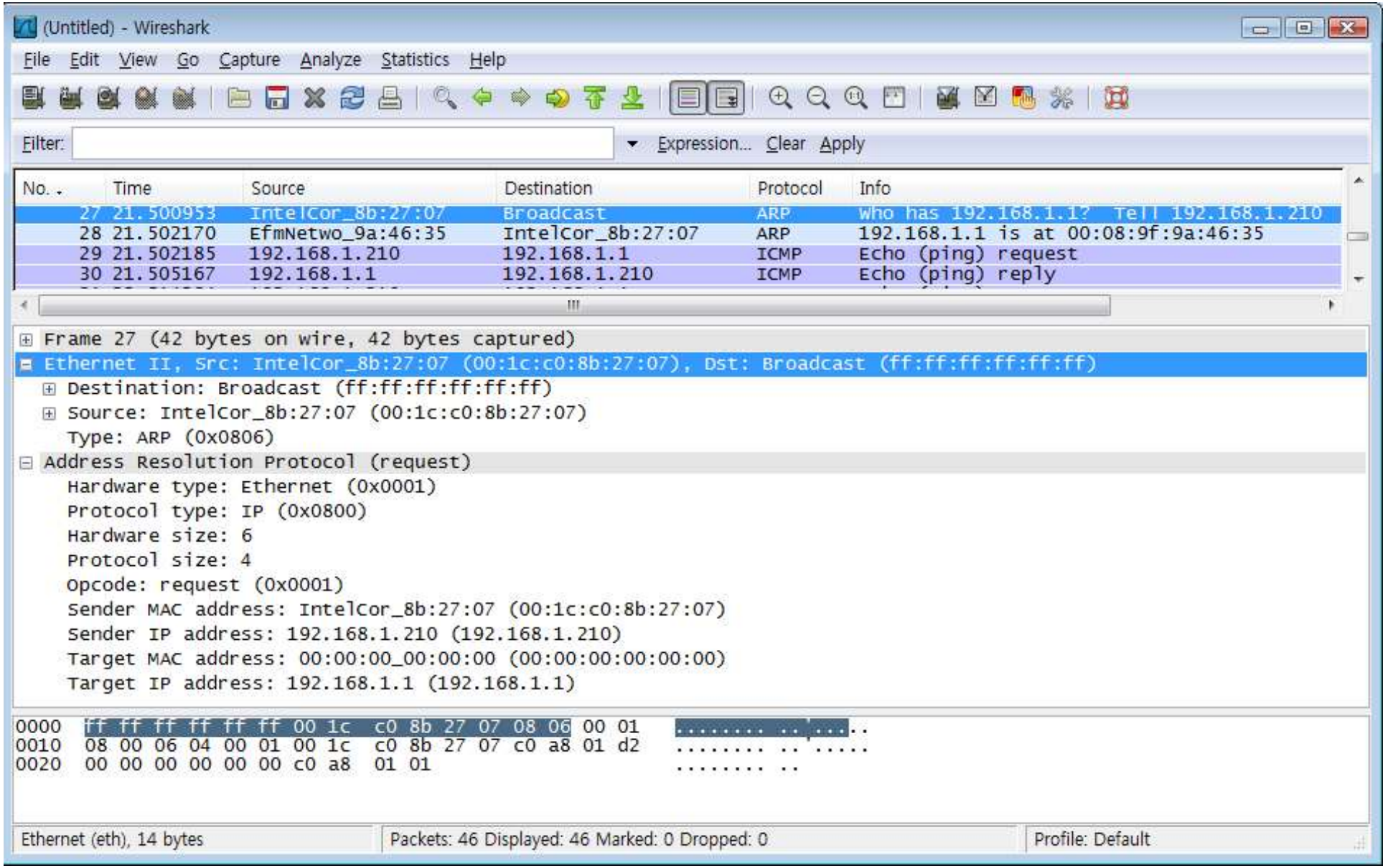


Example: Packet Sniffer

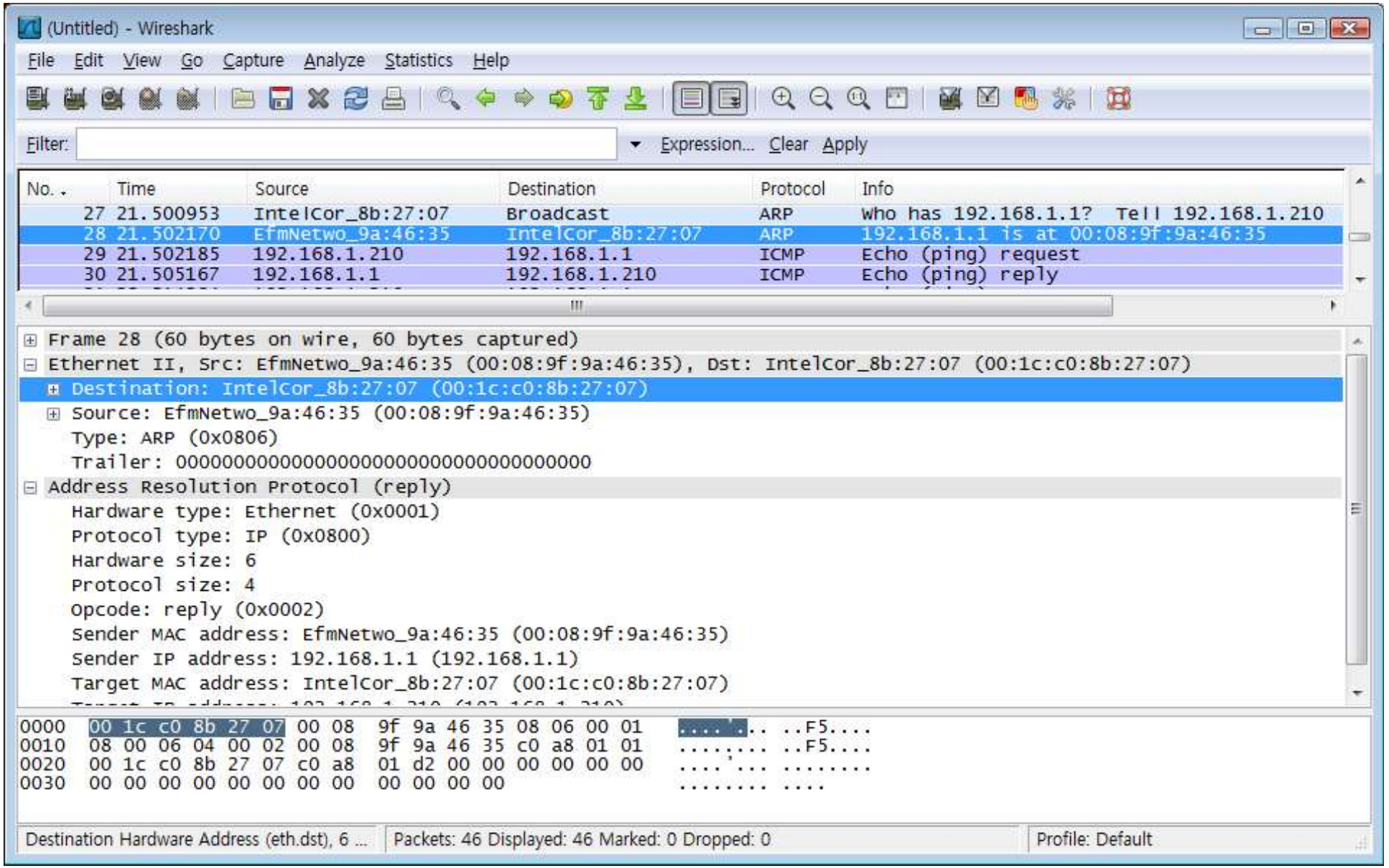
- Wireshark (Ethereal) is a famous network protocol analyzer.
- Test: ping 192.168.1.1 -t



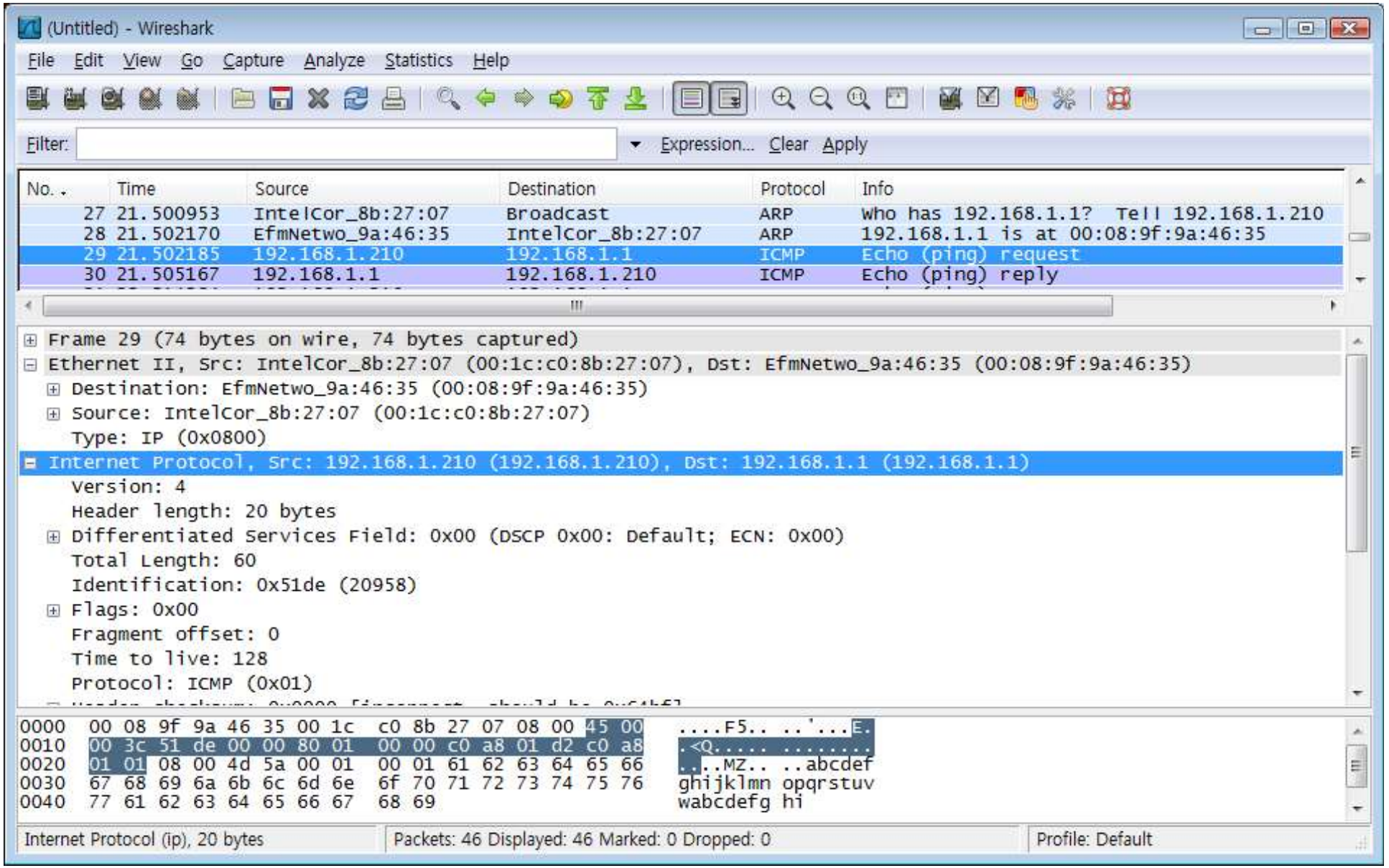
ARP request


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
27 21.500953 IntelCor_8b:27:07 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.210
28 21.502170 EfmNetwo_9a:46:35 IntelCor_8b:27:07 ARP 192.168.1.1 is at 00:08:9f:9a:46:35
29 21.502185 192.168.1.210 192.168.1.1 ICMP Echo (ping) request
30 21.505167 192.168.1.1 192.168.1.210 ICMP Echo (ping) reply
Frame 27 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: IntelCor_8b:27:07 (00:1c:c0:8b:27:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: IntelCor_8b:27:07 (00:1c:c0:8b:27:07)
Type: ARP (0x0806)
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: IntelCor_8b:27:07 (00:1c:c0:8b:27:07)
Sender IP address: 192.168.1.210 (192.168.1.210)
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1 (192.168.1.1)
0000 ff ff ff ff ff ff 00 1c c0 8b 27 07 08 06 00 01
0010 08 00 06 04 00 01 00 1c c0 8b 27 07 c0 a8 01 d2
0020 00 00 00 00 00 00 c0 a8 01 01
Ethernet (eth), 14 bytes
Packets: 46 Displayed: 46 Marked: 0 Dropped: 0
Profile: Default

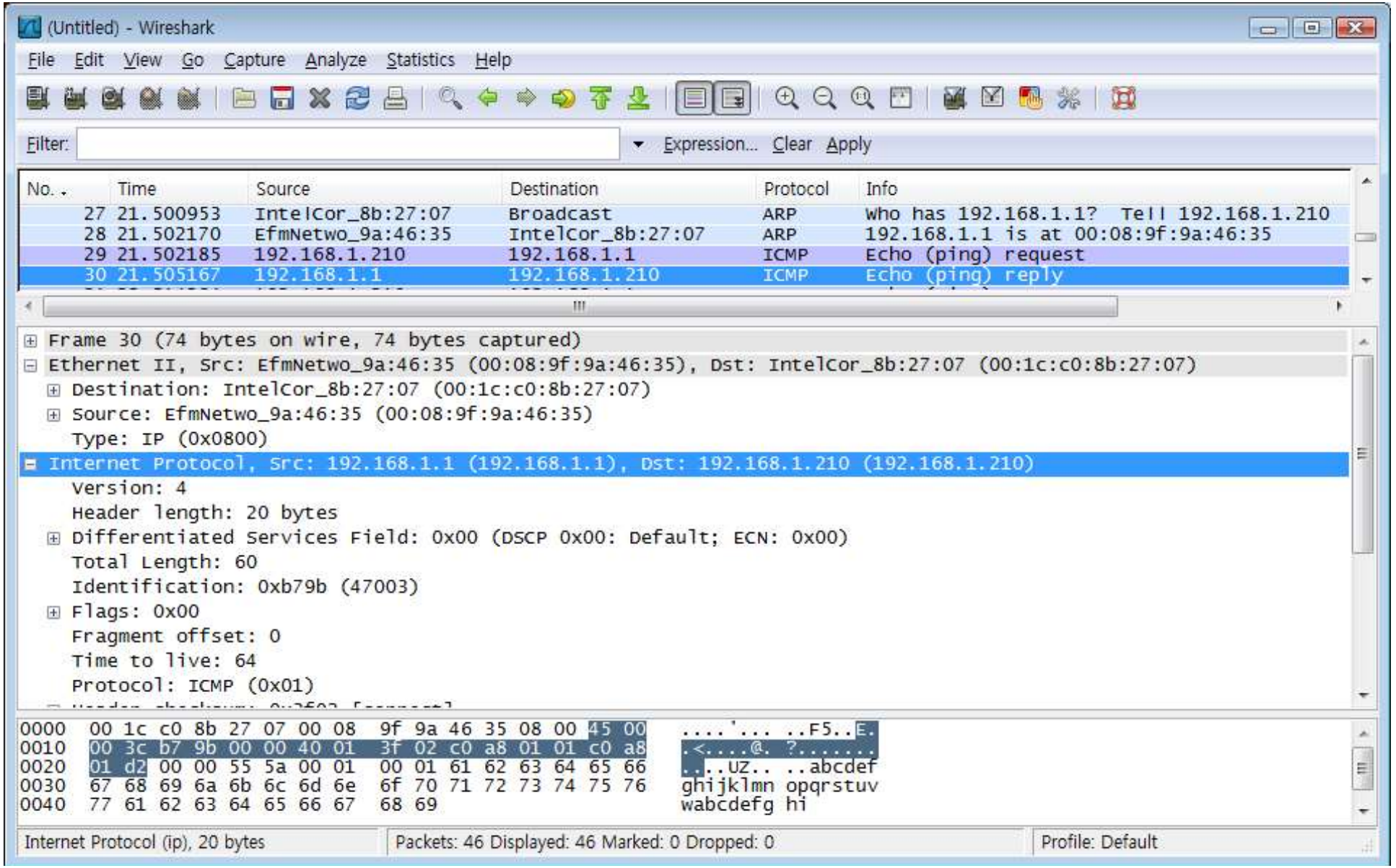
ARP reply


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
27 21.500953 IntelCor_8b:27:07 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.210
28 21.502170 EfmNetwo_9a:46:35 IntelCor_8b:27:07 ARP 192.168.1.1 is at 00:08:9f:9a:46:35
29 21.502185 192.168.1.210 192.168.1.1 ICMP Echo (ping) request
30 21.505167 192.168.1.1 192.168.1.210 ICMP Echo (ping) reply
Frame 28 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: EfmNetwo_9a:46:35 (00:08:9f:9a:46:35), Dst: IntelCor_8b:27:07 (00:1c:c0:8b:27:07)
Destination: IntelCor_8b:27:07 (00:1c:c0:8b:27:07)
Source: EfmNetwo_9a:46:35 (00:08:9f:9a:46:35)
Type: ARP (0x0806)
Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender MAC address: EfmNetwo_9a:46:35 (00:08:9f:9a:46:35)
Sender IP address: 192.168.1.1 (192.168.1.1)
Target MAC address: IntelCor_8b:27:07 (00:1c:c0:8b:27:07)
0000 00 1c c0 8b 27 07 00 08 9f 9a 46 35 08 06 00 01
0010 08 00 06 04 00 02 00 08 9f 9a 46 35 c0 a8 01 01
0020 00 1c c0 8b 27 07 c0 a8 01 d2 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Destination Hardware Address (eth.dst), 6 ...
Packets: 46 Displayed: 46 Marked: 0 Dropped: 0
Profile: Default

ICMP (ping request)



ICMP (ping reply)

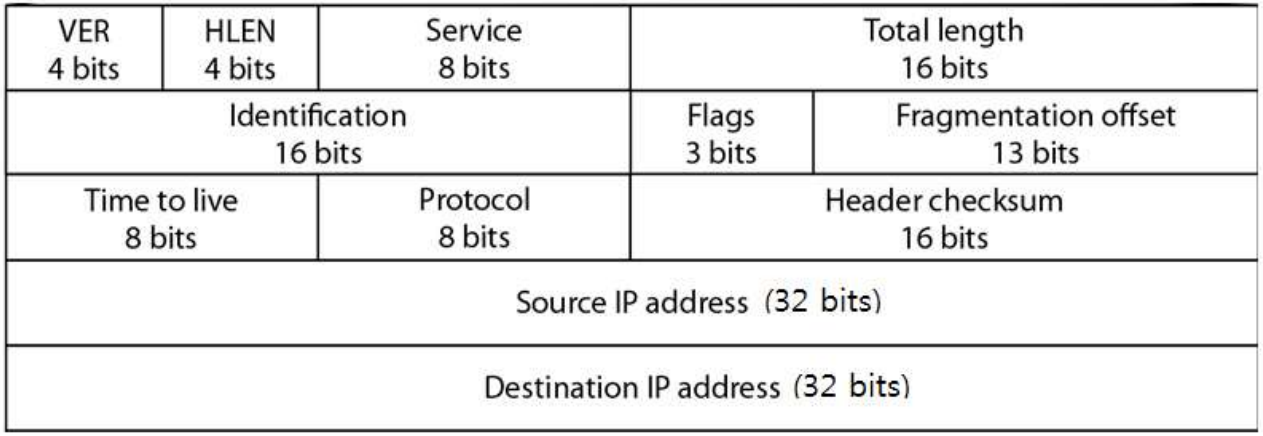


Quiz

- What is the source IP address of the packet?

```
0000   00 08 9f 9a 46 35 00 24   54 30 e8 1f 08 00 45 00
0010   05 74 02 22 20 00 80 01   00 00 c0 a8 01 05 c0 a8
0020   01 01 08 00 e4 4b 00 01   01 9e 61 62 63 64 65 66
0030   67 68 69 6a 6b 6c 6d 6e   6f 70 71 72 73 74 75 76
0040   77 61 62 63 64 65 66 67   68 69 6a 6b 6c 6d 6e 6f
0050   70 71 72 73 74 75 76 77   61 62 63 64 65 66 67 68
0060   69 6a 6b 6c 6d 6e 6f 70   71 72 73 74 75 76 77 61
0070   62 63 64 65 66 67 68 69   6a 6b 6c 6d 6e 6f 70 71
```

Answer: ?

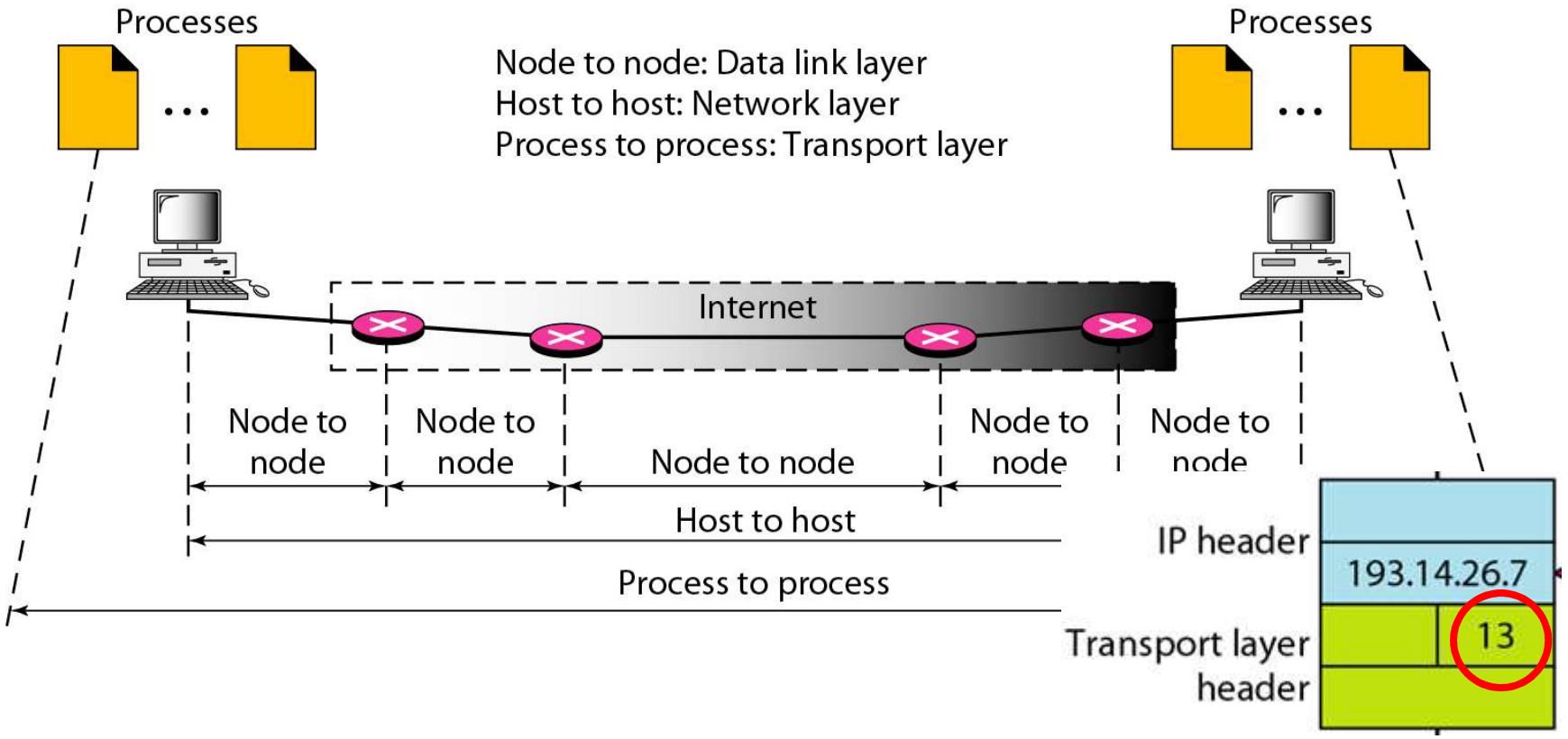


4) TCP/UDP

- Responsible for delivery of a message from a process to another process.

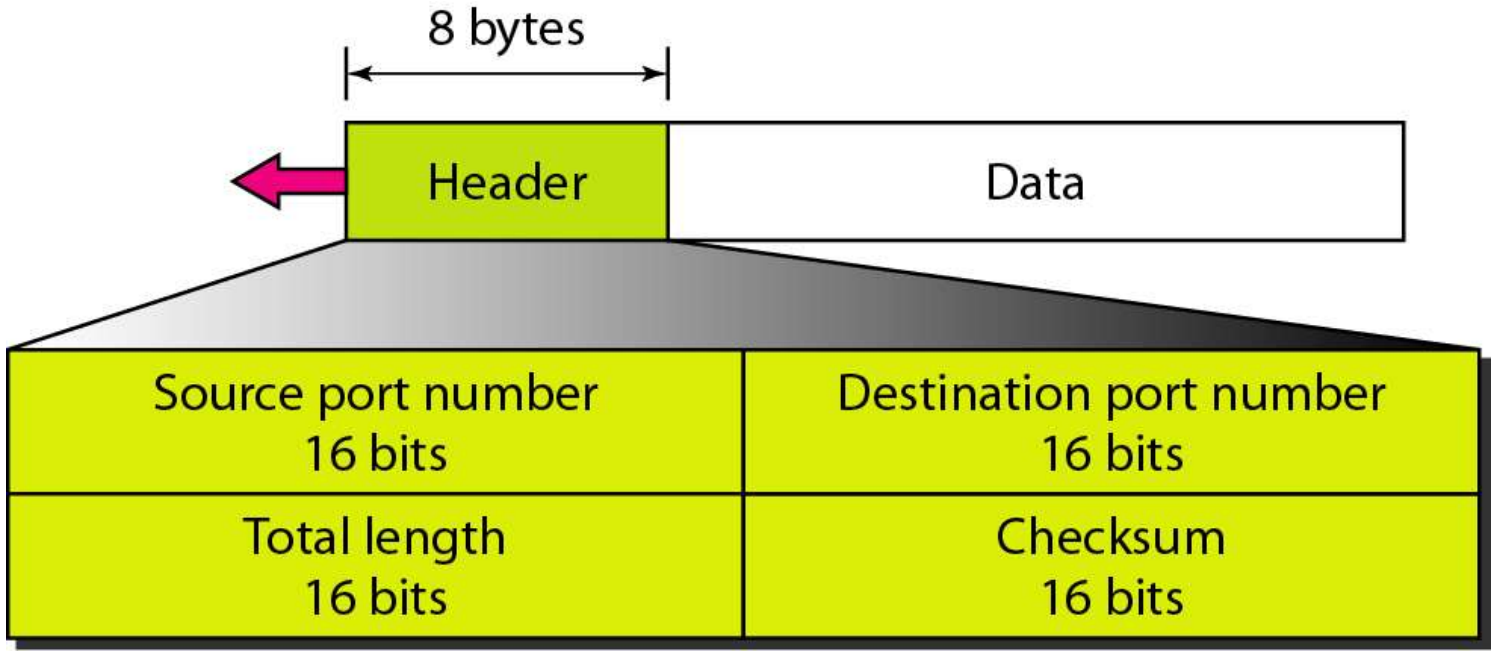
- User Datagram Protocol (UDP)
  - UDP is the simpler of the two standard TCP/IP transport protocols
- Transmission Control Protocol (TCP)
  - TCP is a reliable stream transport protocol.
  - Connection-oriented protocol.
- Stream Control Transmission Protocol (SCTP)
  - SCTP provides support for newer applications such as voice over the Internet protocol (VoIP).

Port Address



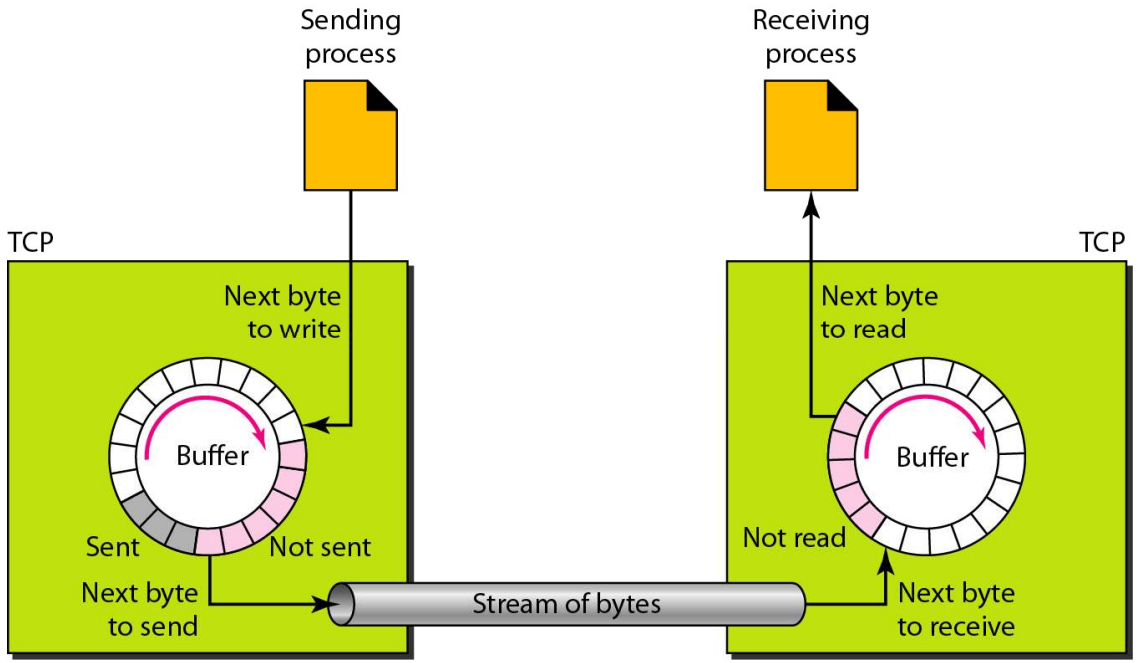
UDP

- The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol.
- Protocol: Echo (7), BOOTPs/c (67, 68), TFTP (69), NTP (123), SNMP (161), SNMP trap(162)

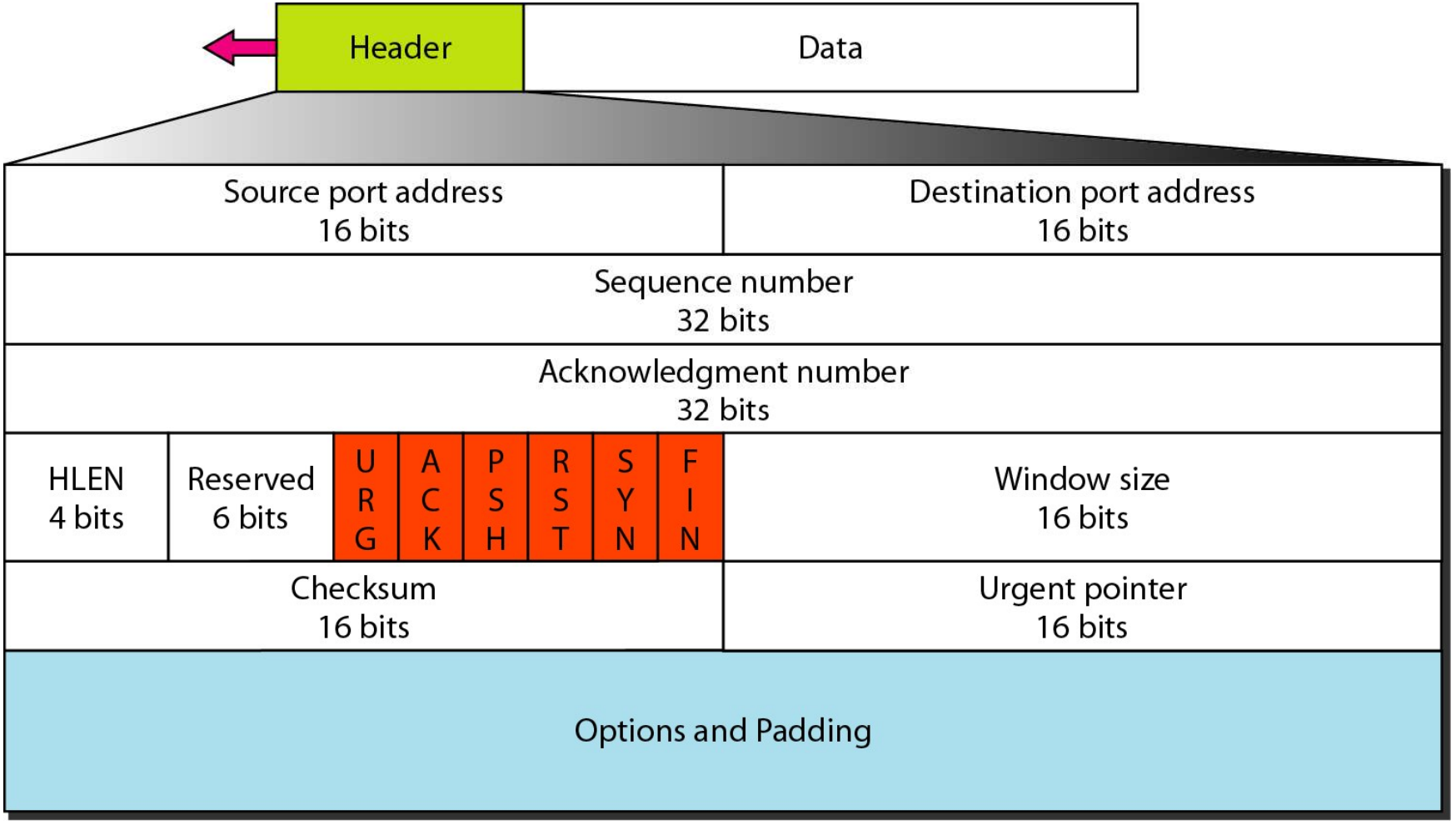


TCP

- Connection-oriented protocol.
- TCP creates a virtual connection between two TCPs to send data.
- Congestion control: Slow start, Reno, Vegas, ...
- Protocol: FTP (21), TELNET (23), SMTP (25), DNS (53), BOOTP (67), HTTP (80)



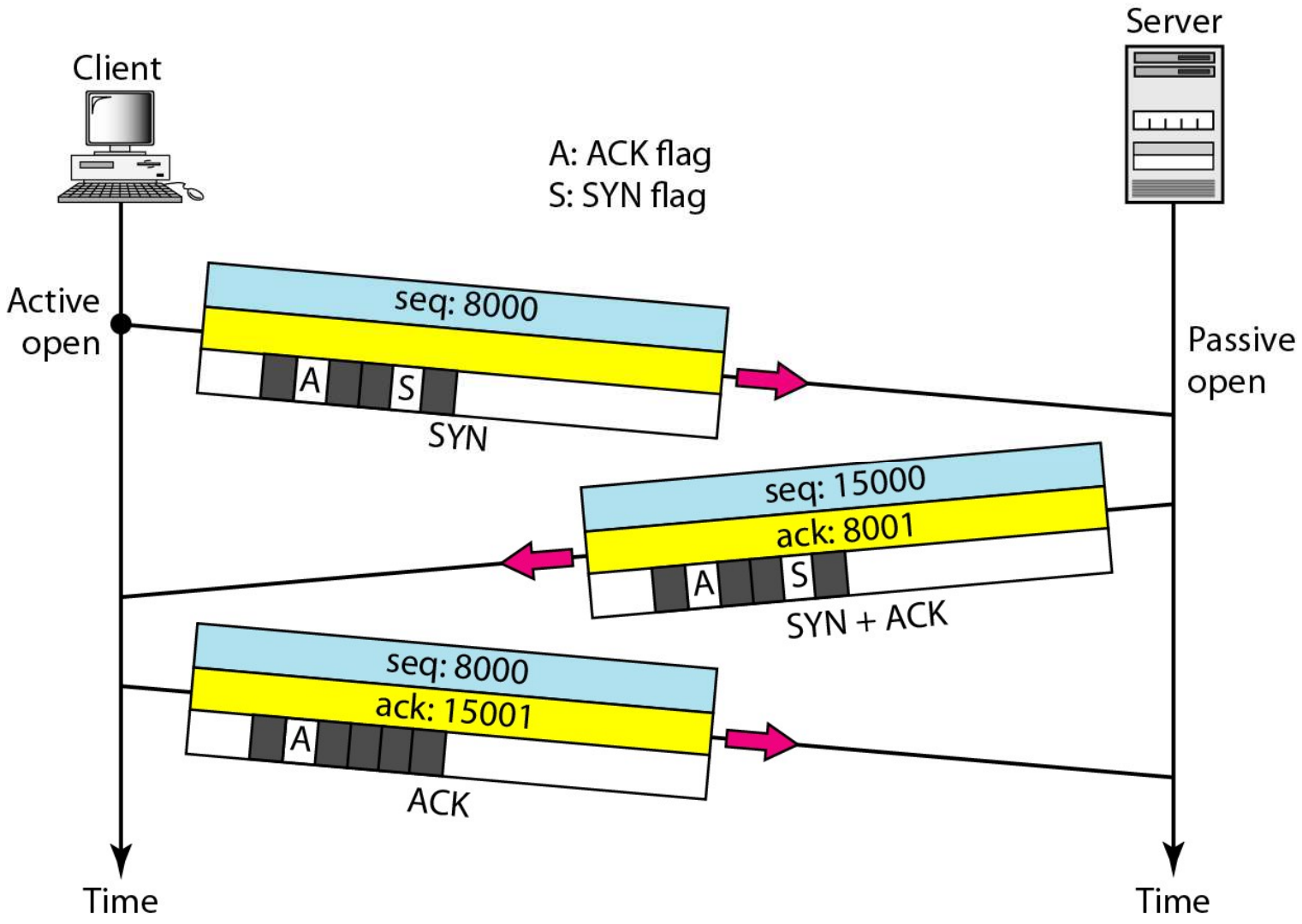
TCP Header



URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push

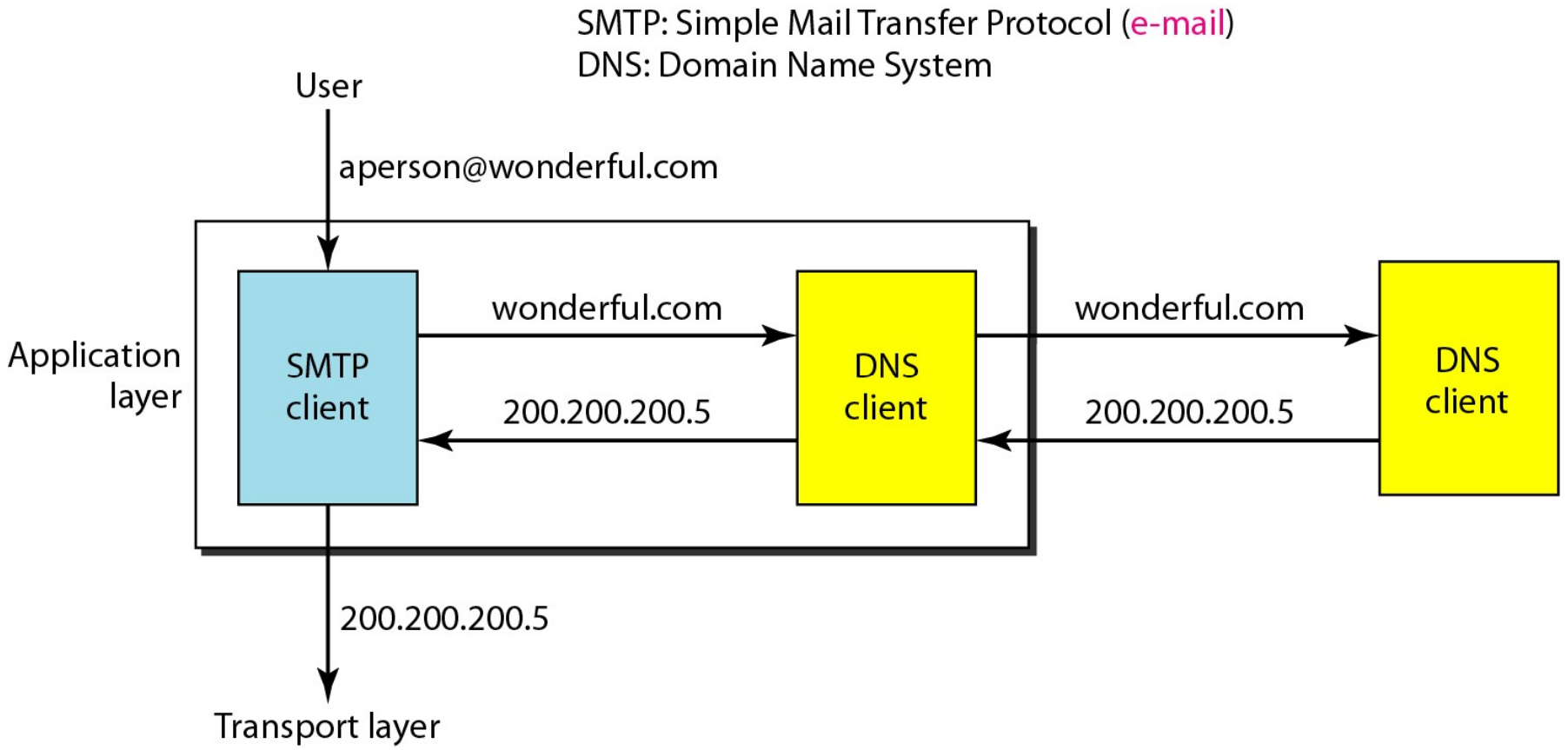
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection

TCP: Connection Establishment



5) DNS, HTTP

- DNS Service



Architecture of WWW