5 TCP/IP Protocol Suite
Part 1

Most slides are from the instructor resources of the following books:
1. Data communications and networking, 4th edition, Forouzan, McGrawHill
2. Computer networks, 4th edition, Tanenbaum, Prentice Hall
3. Textbook

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.

ISO is the organization.
OSI is the model.

Topics discussed in this section:

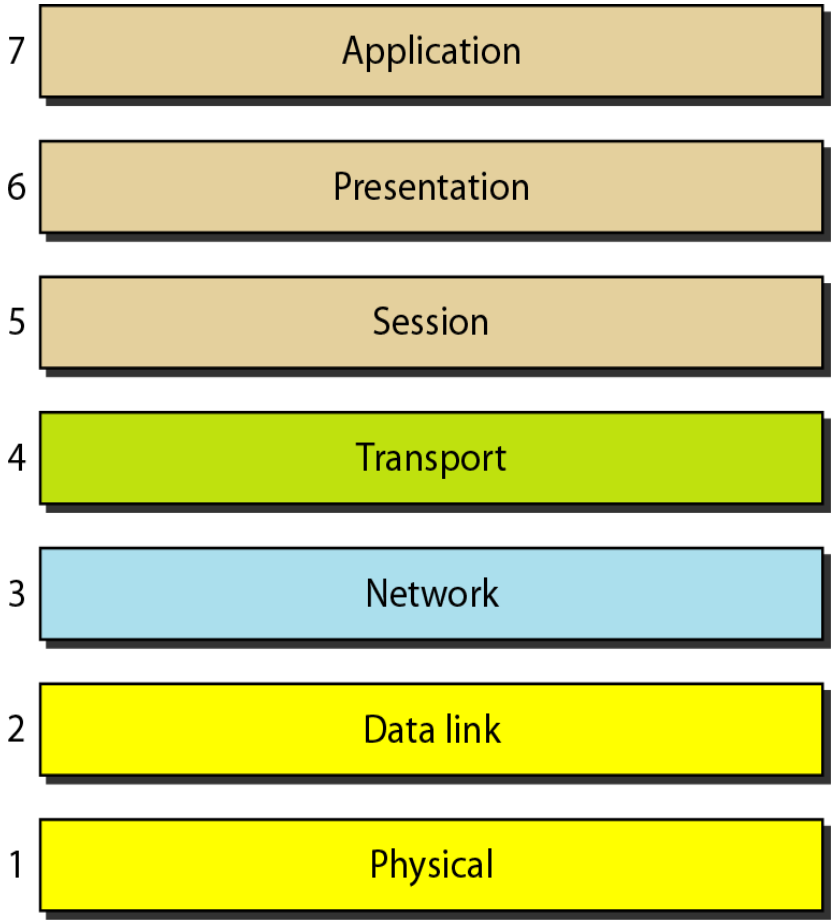
Layered Architecture
Peer-to-Peer Processes
Encapsulation

Layered Architecture

- The OSI model is composed of seven layers ;
  - Physical (layer1), Data link (layer2), Network (layer3)
  - Transport (layer4), Session (layer5), Presentation (layer6)
  - Application (layer7)
- Layer
  - Designer identified which networking functions had related uses and collected those functions into discrete groups that became the layers.
  - The OSI model allows complete interoperability between otherwise incompatible systems.
  - Each layer uses the services of the layer immediately below it.

Layered Architecture (cont'd)

Seven layers of the OSI model

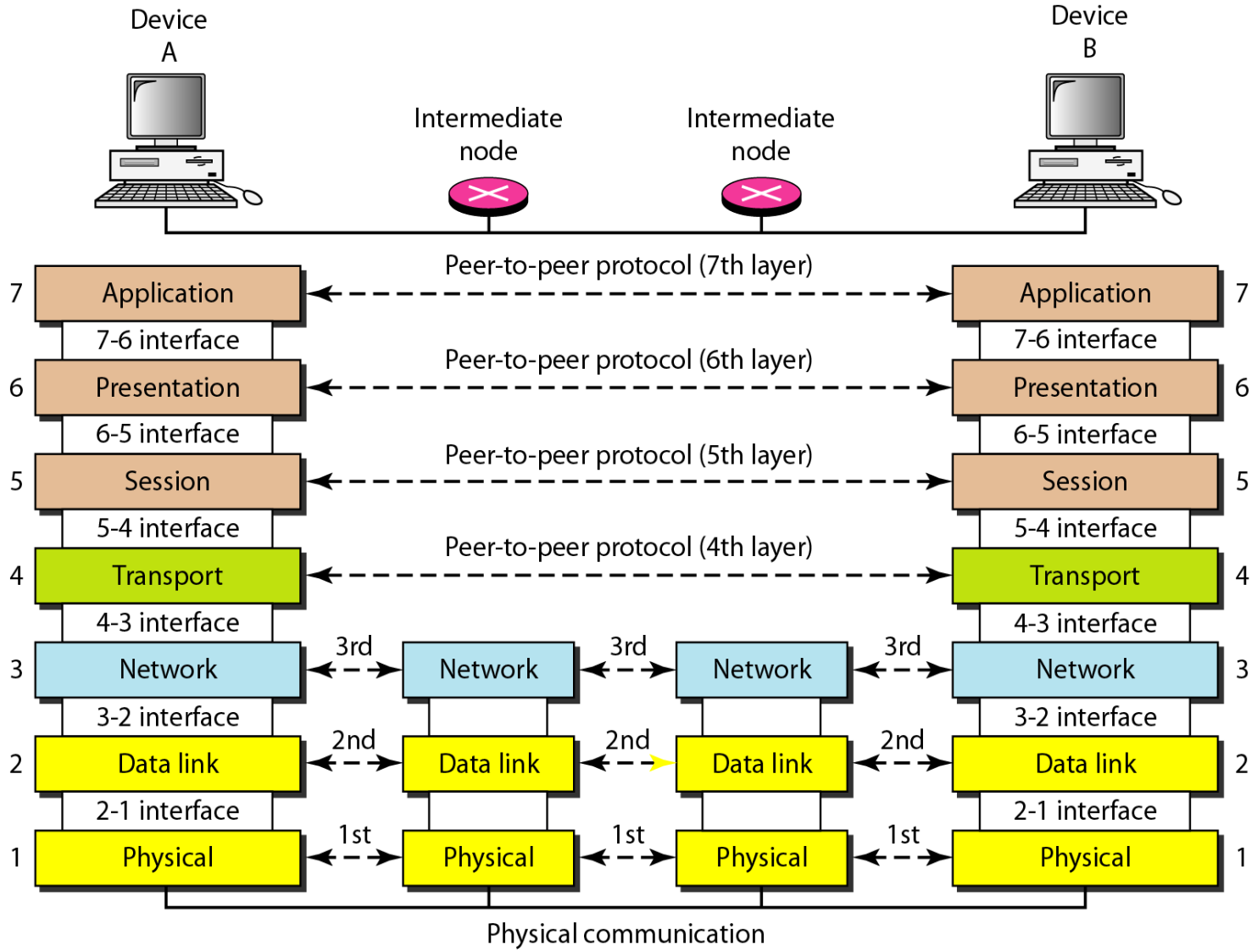


Peer-to-peer Processes

- Layer x on one machine communicates with layer x on another machine - called Peer-to-Peer Processes.
- Interfaces between Layers
  - Each interface defines what information and services a layer must provide for the layer above it.
  - Well defined interfaces and layer functions provide modularity to a network
- Organizations of the layers
  - Network support layers : Layers 1, 2, 3
  - User support layer : Layer 5, 6, 7
    - It allows interoperability among unrelated software systems
  - Transport layer (Layer 4) : links the two subgroups

Peer-to-peer Processes (cont'd)

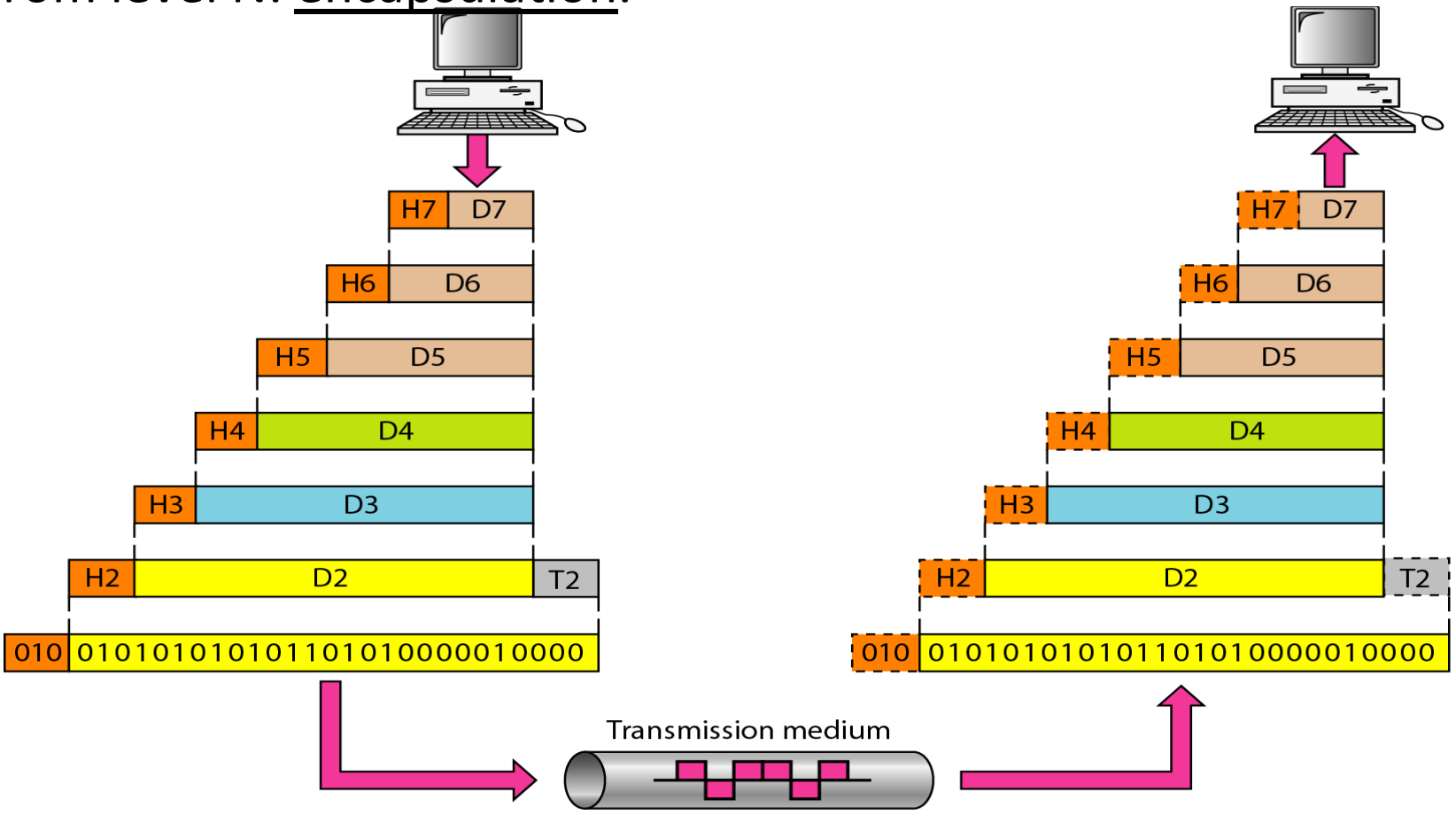
The interaction between layers in the OSI model



Peer-to-peer Processes (cont'd)

An exchange using the OSI model

Data portion of a packet at level N-1 carries the whole packet from level N: encapsulation.



LAYERS IN THE OSI MODEL

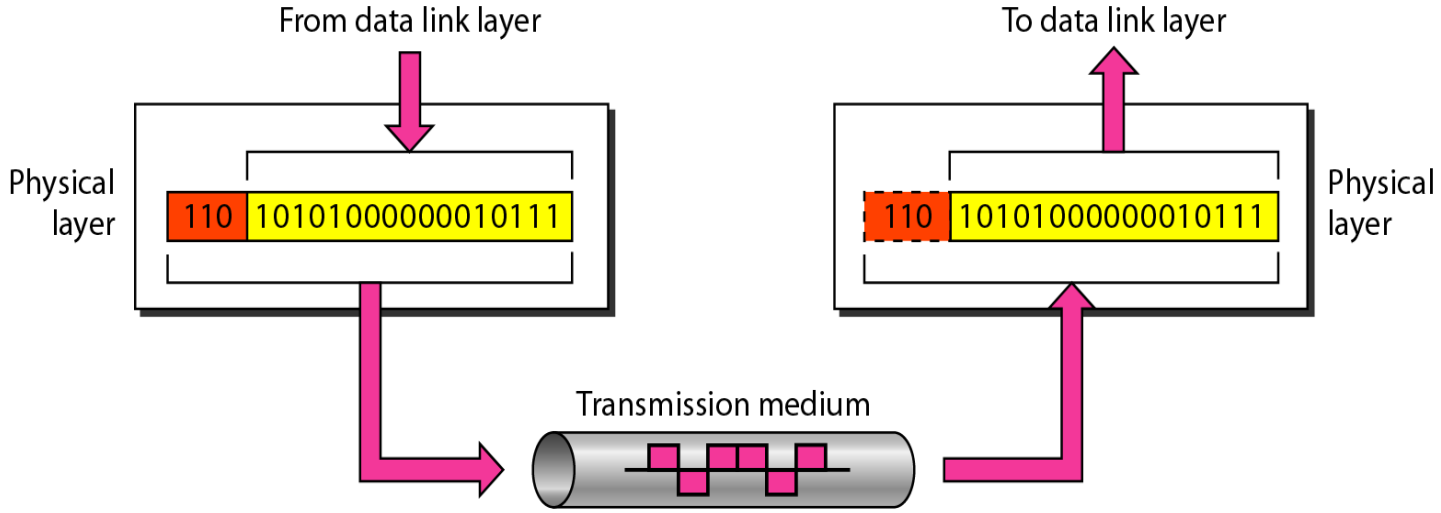
In this section we briefly describe the functions of each layer in the OSI model.

Topics discussed in this section:

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

Physical Layer

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

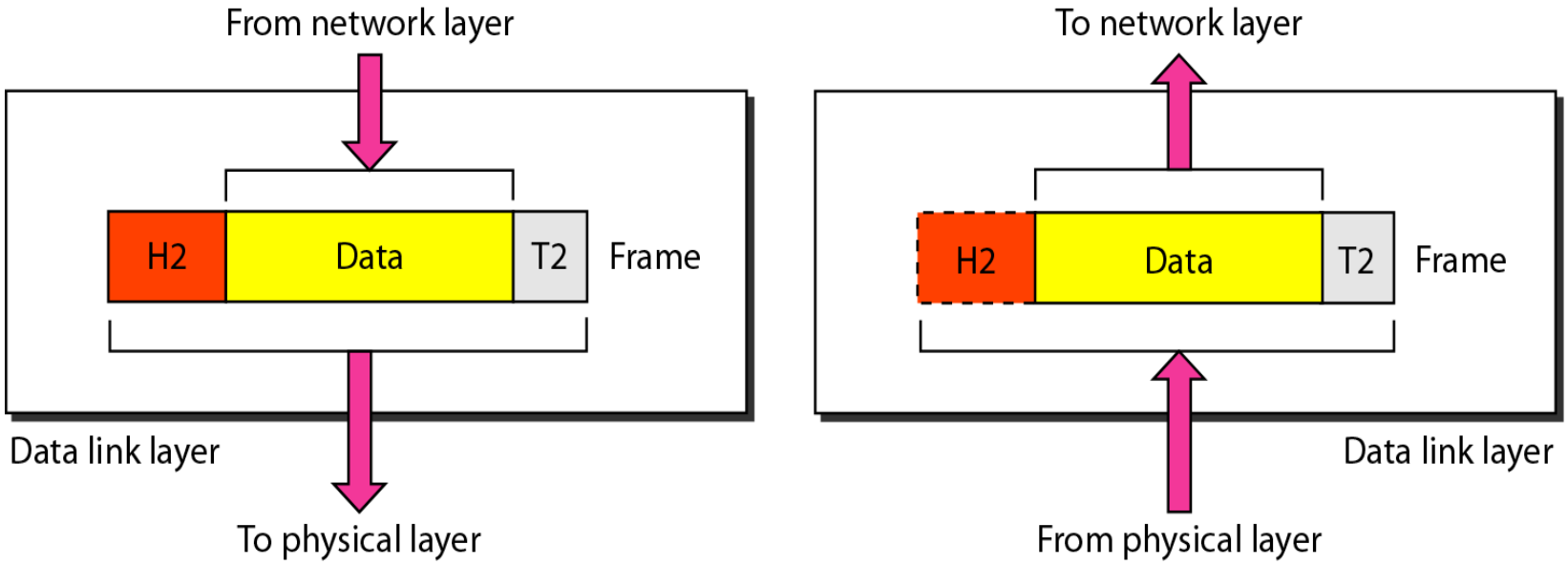


- The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Physical Layer

- Physical layer is concerned with the following: (deal with the mechanical and electrical specification of the primary connections: cable, connector)
  - Physical characteristics of interfaces and medium
  - Representation of bits
  - Data rate (=transmission rate)
  - Synchronization of bits
  - Line configuration
  - Physical topology
  - Transmission mode

Data Link Layer

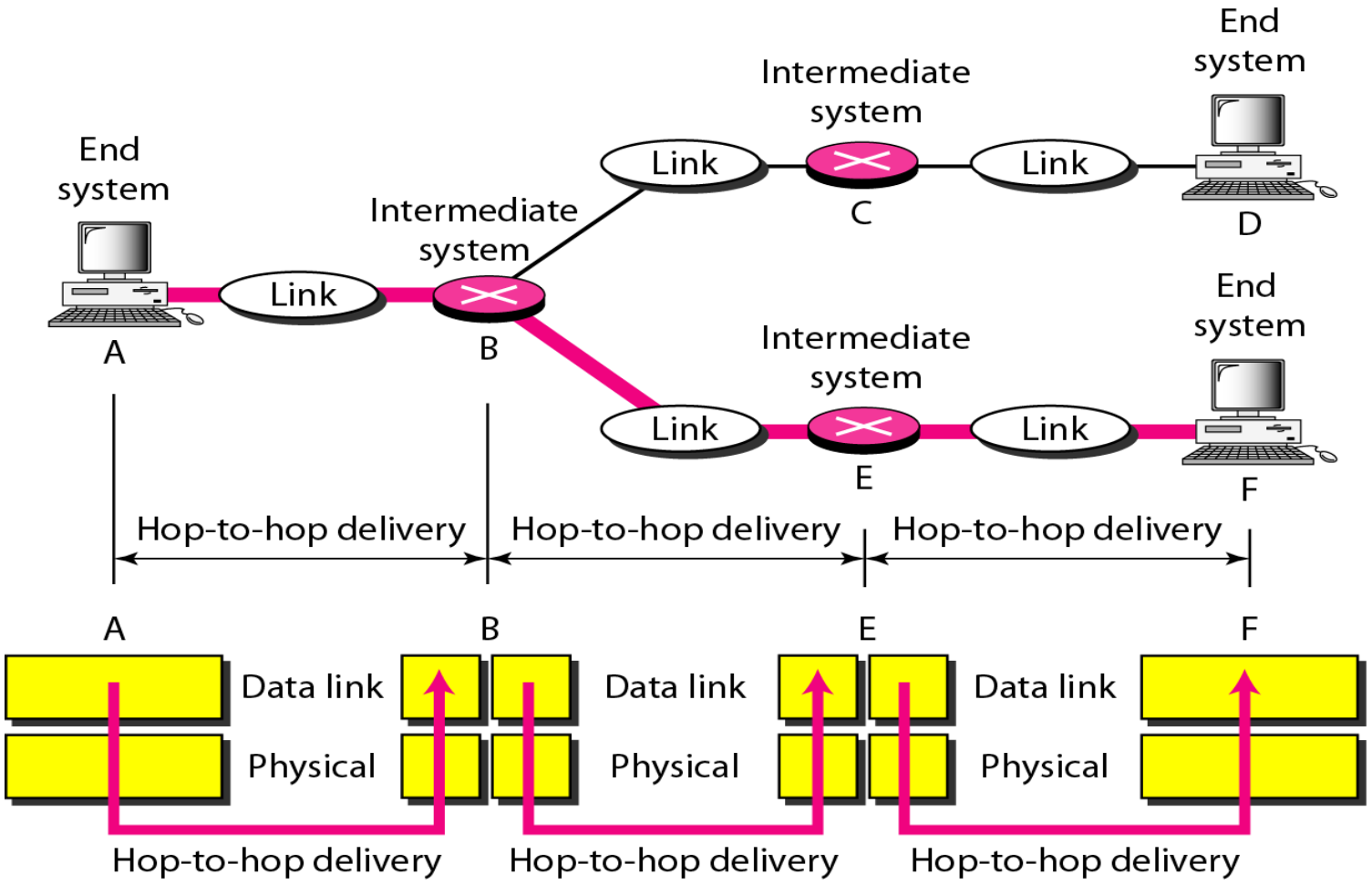


Data Link Layer

- Major duties
  - Framing
  - Physical addressing
  - Flow control
  - Error control
  - Access control

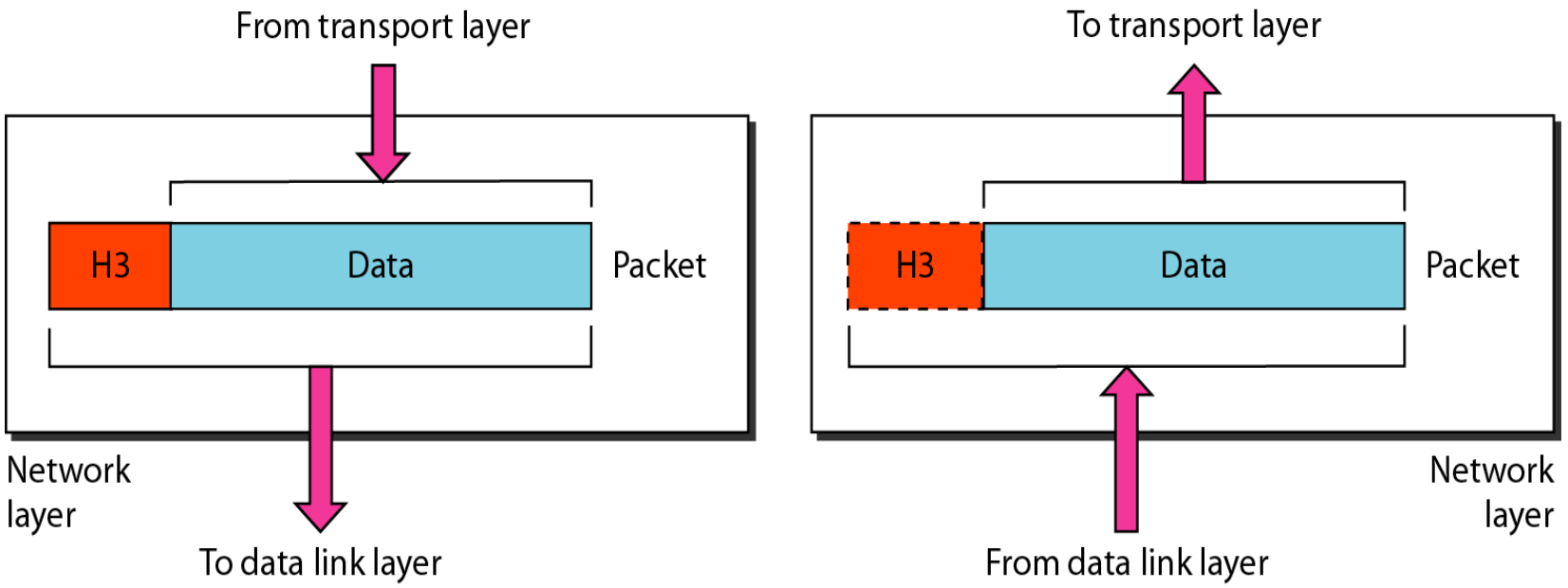
Data Link Layer

- **Hop-to-hop** (**node-to-node**) delivery



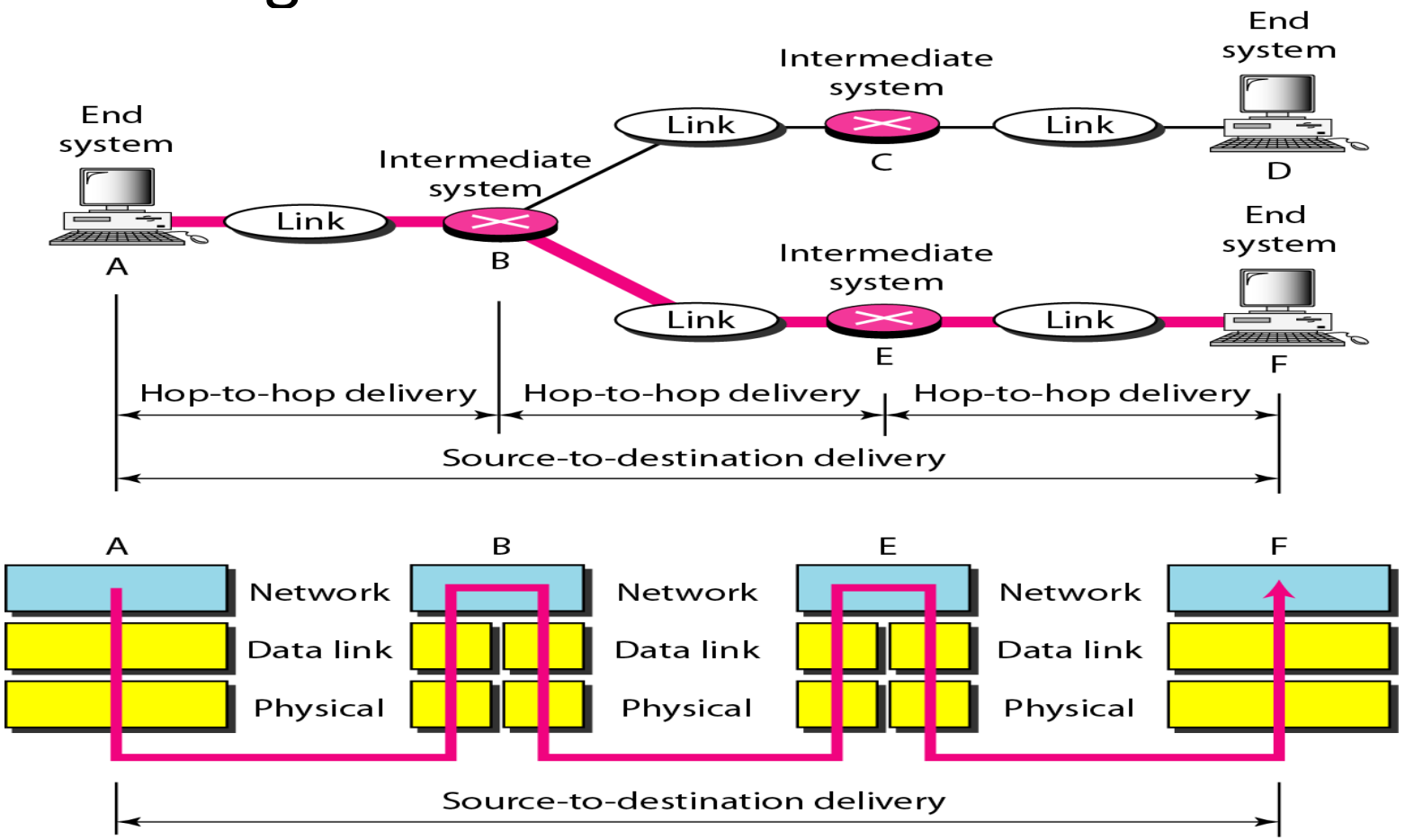
Network Layer

- Network layer is responsible for the delivery of individual packets from the source host to the destination host. (**source-to-destination** delivery)



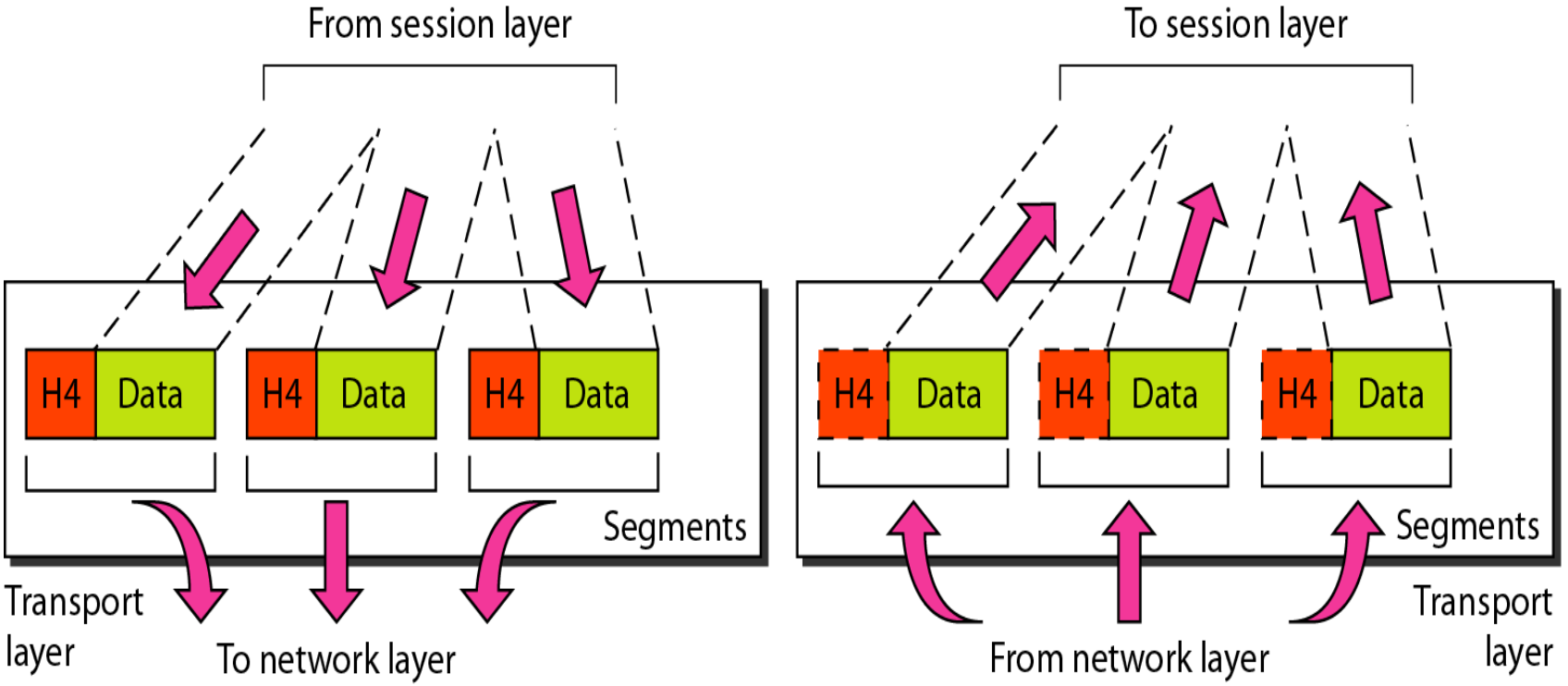
Network Layer

- Logical addressing
- Routing

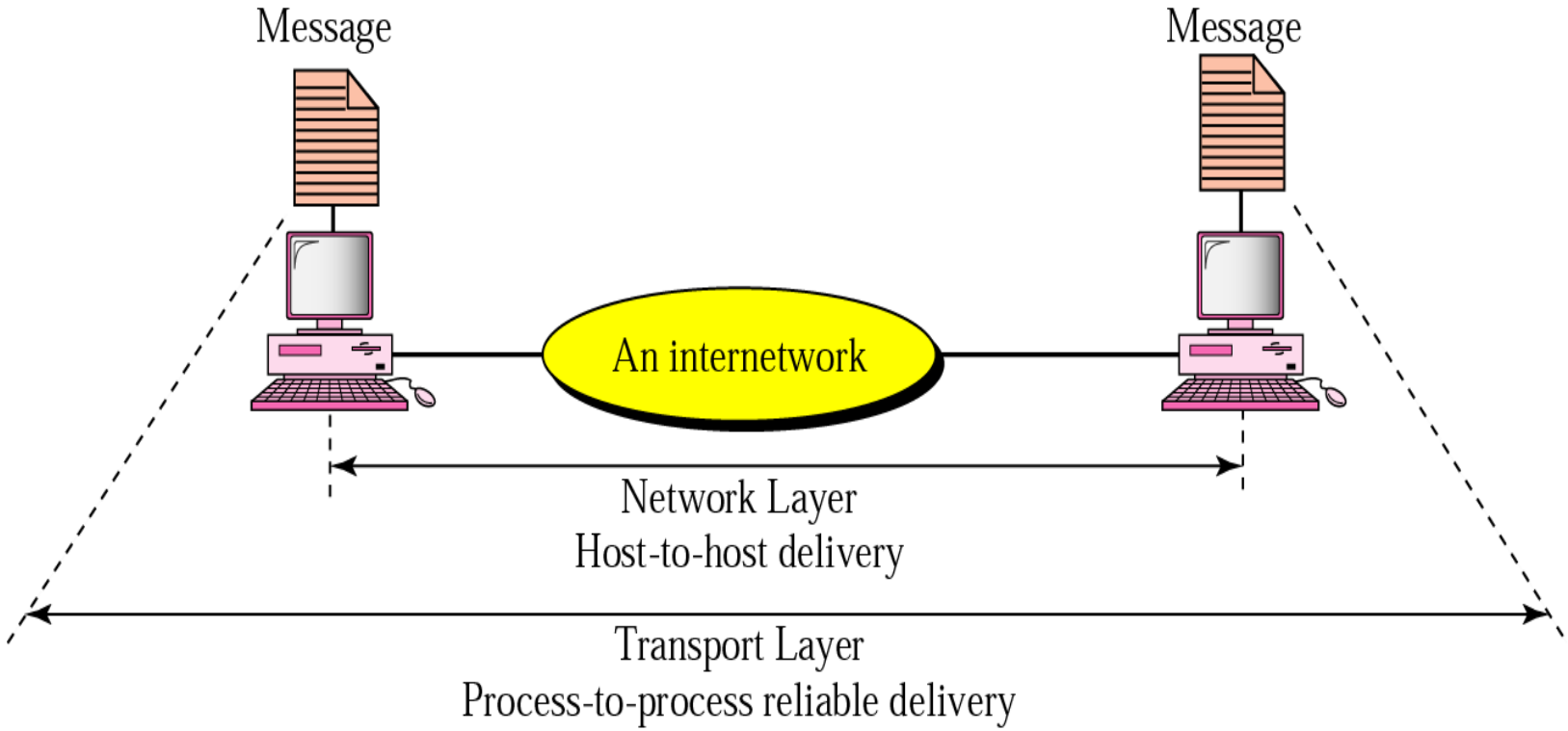


Transport Layer

Transport layer is responsible for the delivery of a message from one process to another. (**process-to-process** delivery)



Transport Layer

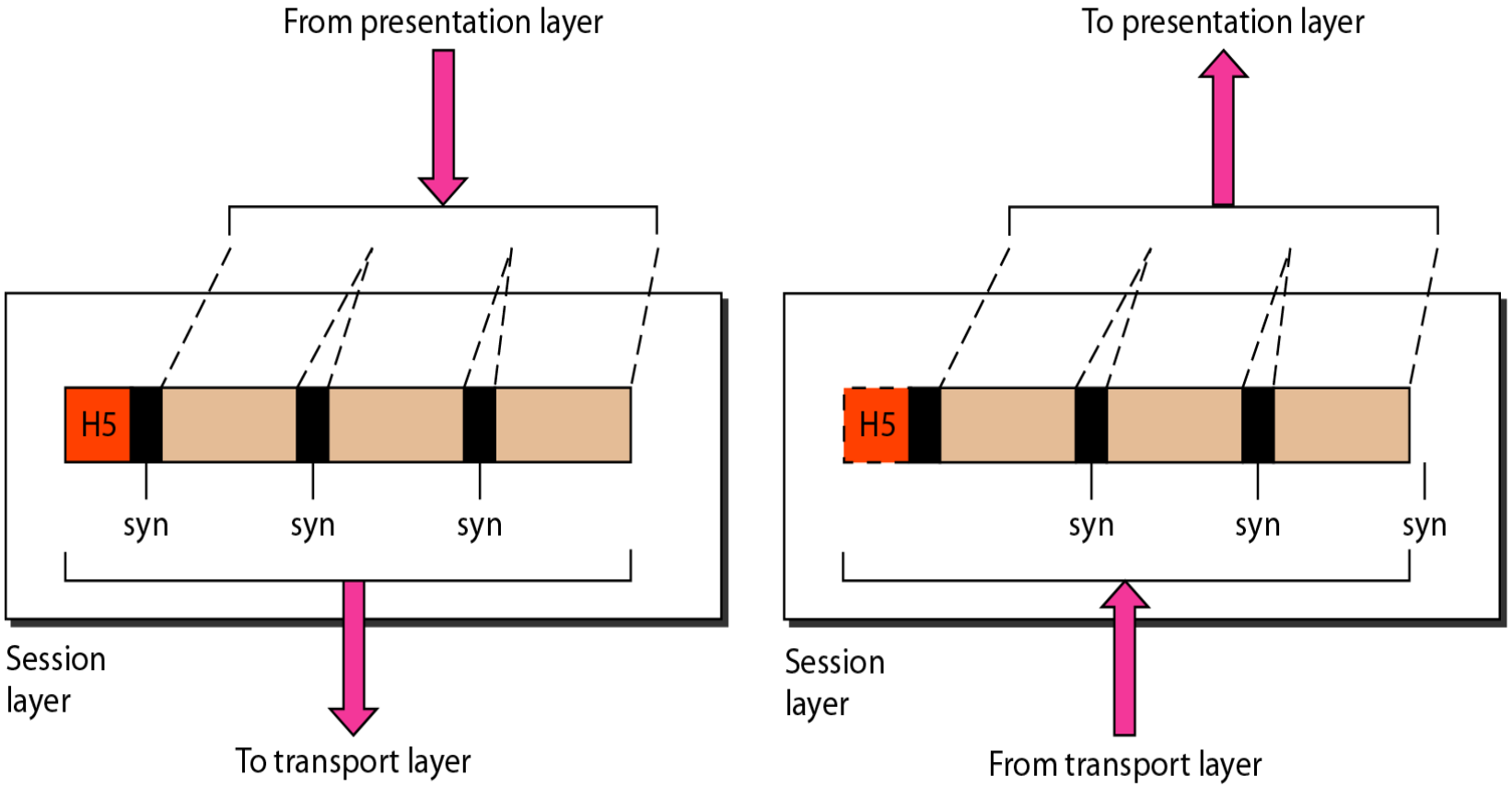


Transport Layer

- Service-port (point) addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control

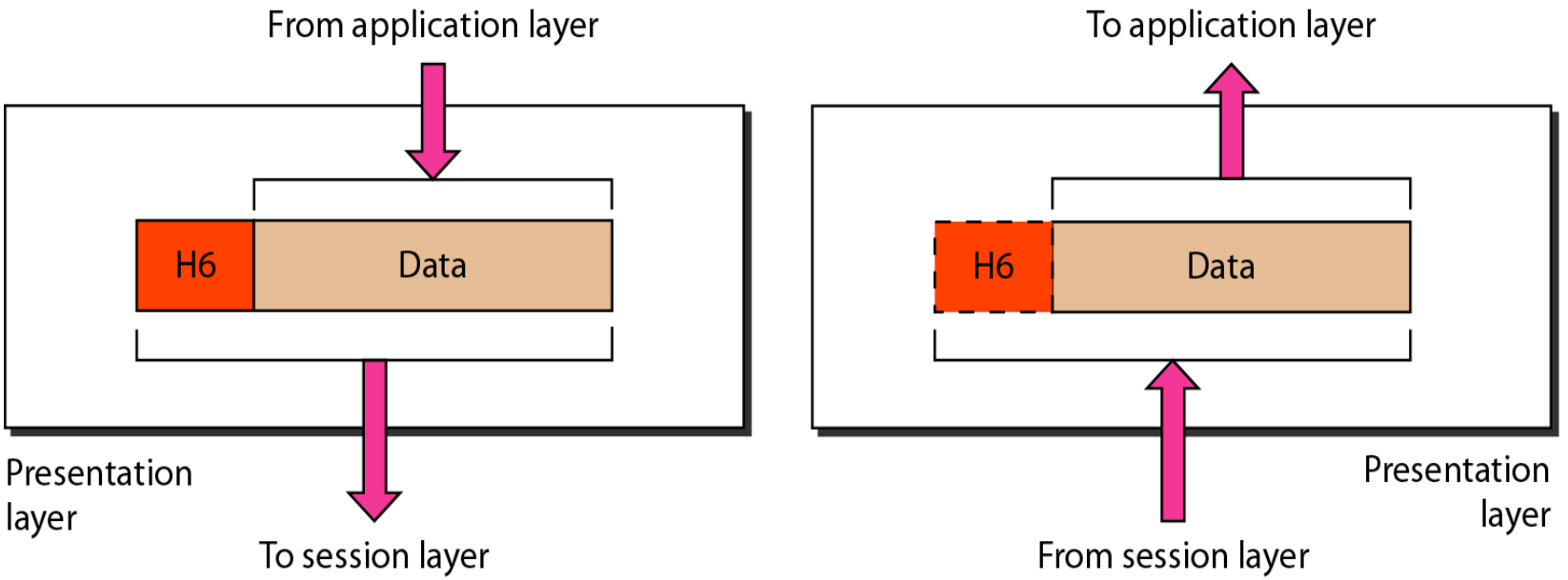
Session Layer

Session layer is responsible for dialog control and synchronization.



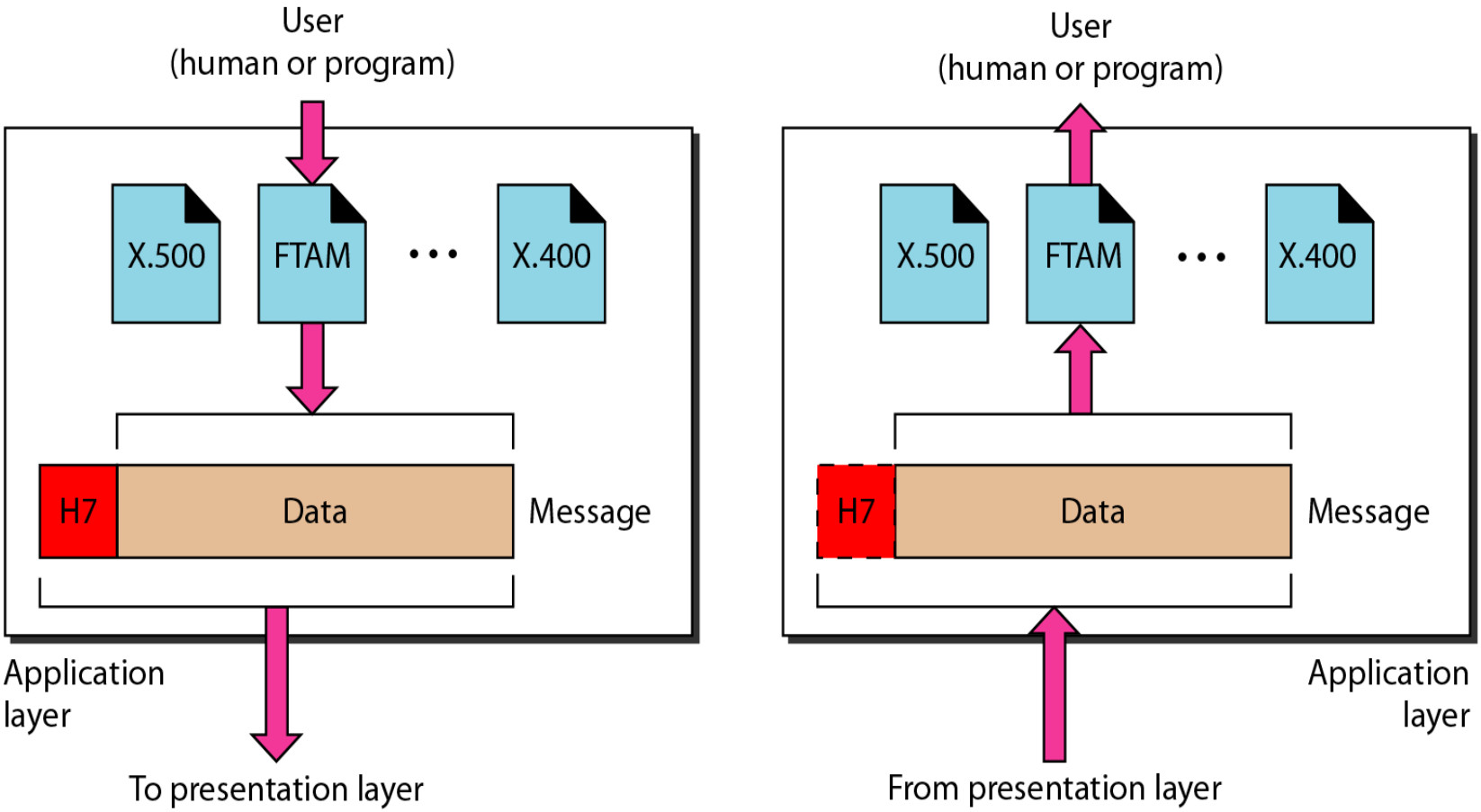
Presentation Layer

Presentation layer is responsible for translation, compression, and encryption



Application Layer

Application layer is responsible for providing services to the user.

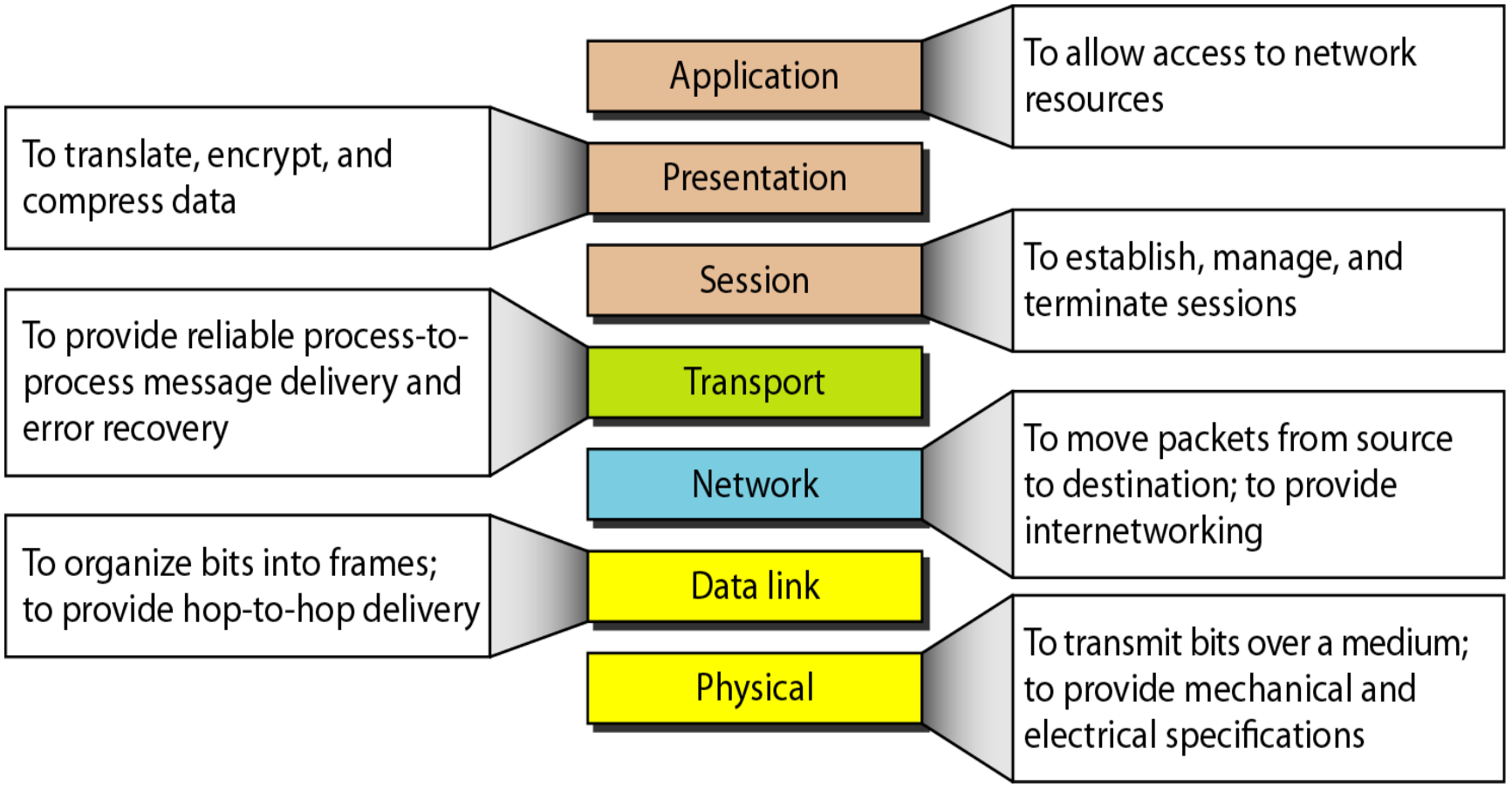


Application Layer

- The major duties of the application
  - Network virtual terminal
  - File transfer, access, and management
  - Mail services
  - Directory services

Summary of Layers

Summary of layers



TCP/IP PROTOCOL SUITE

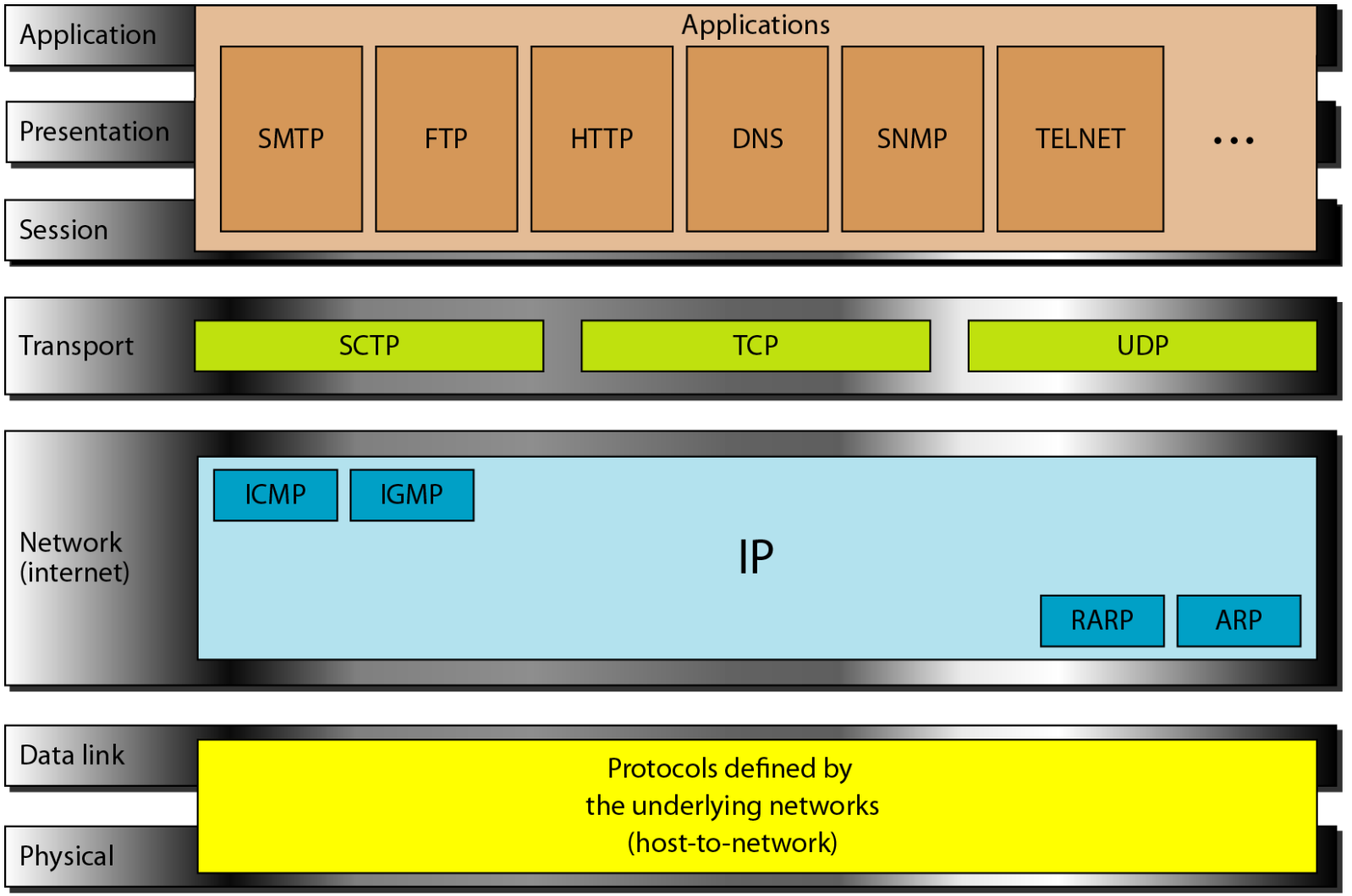
The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made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

TCP/IP Protocol Suite

TCP/IP and OSI model



Physical and Data Link Layers

- At the physical and data link layers, TCP/IP does not define any specific protocol.
- It supports all the standard and proprietary protocols.
- A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Network Layer (=internetwork layer)

- TCP/IP supports the Internetworking Protocol.
- IP uses four supporting protocols : ARP, RARP, ICMP, and IGMP.
  - IP (Internetworking Protocol)
  - ARP (Address Resolution Protocol)
  - RARP (Reverse Address Resolution Protocol)
  - ICMP (Internet Control Message Protocol)
  - IGMP (Internet Group Message Protocol)

Transport Layer

- The transport layer was represented in TCP/IP by two protocols : TCP and UDP.
  - IP is a host-to-host protocol
  - TCP and UDP are transport level protocols responsible for delivery of a message from a process to another process.
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- SCTP (Stream Control Transmission Protocol)

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.

Comparing OSI and TCP/IP Models

Concepts central to the OSI model

- Services
- Interfaces
- Protocols

A Critique of the OSI Model and Protocols

Why OSI did not take over the world

- Bad timing
- Bad technology
- Bad implementations

A Critique of the TCP/IP Reference Model

Problems:

- Service, interface, and protocol not distinguished
- Not a general model
- Host-to-network “layer” not really a layer
- No mention of physical and data link layers
- Minor protocols deeply entrenched, hard to replace

2-5 ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
Specific Addresses

Figure 2.17 *Addresses in TCP/IP*

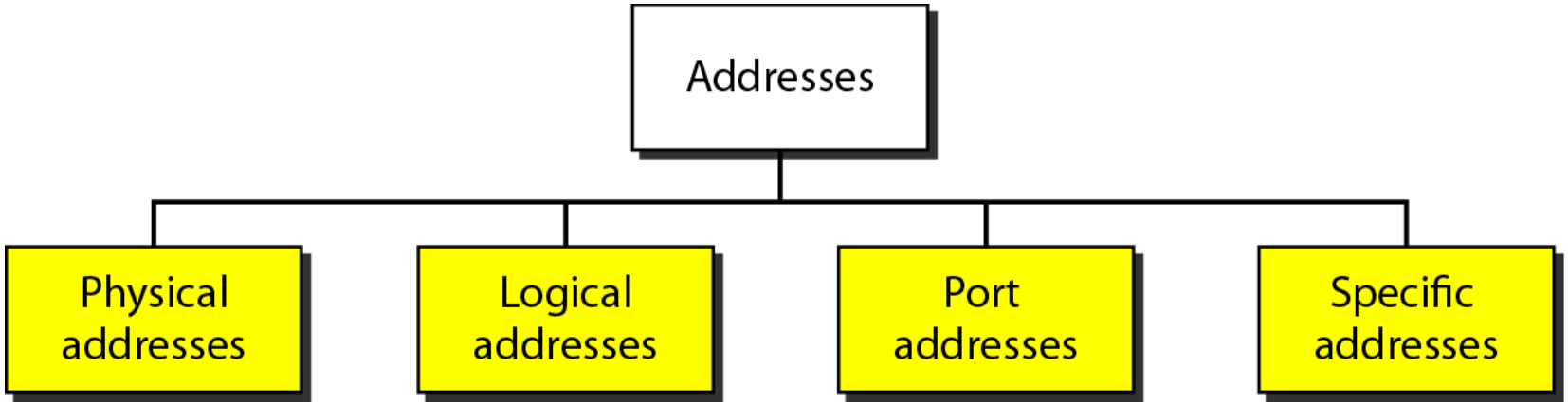
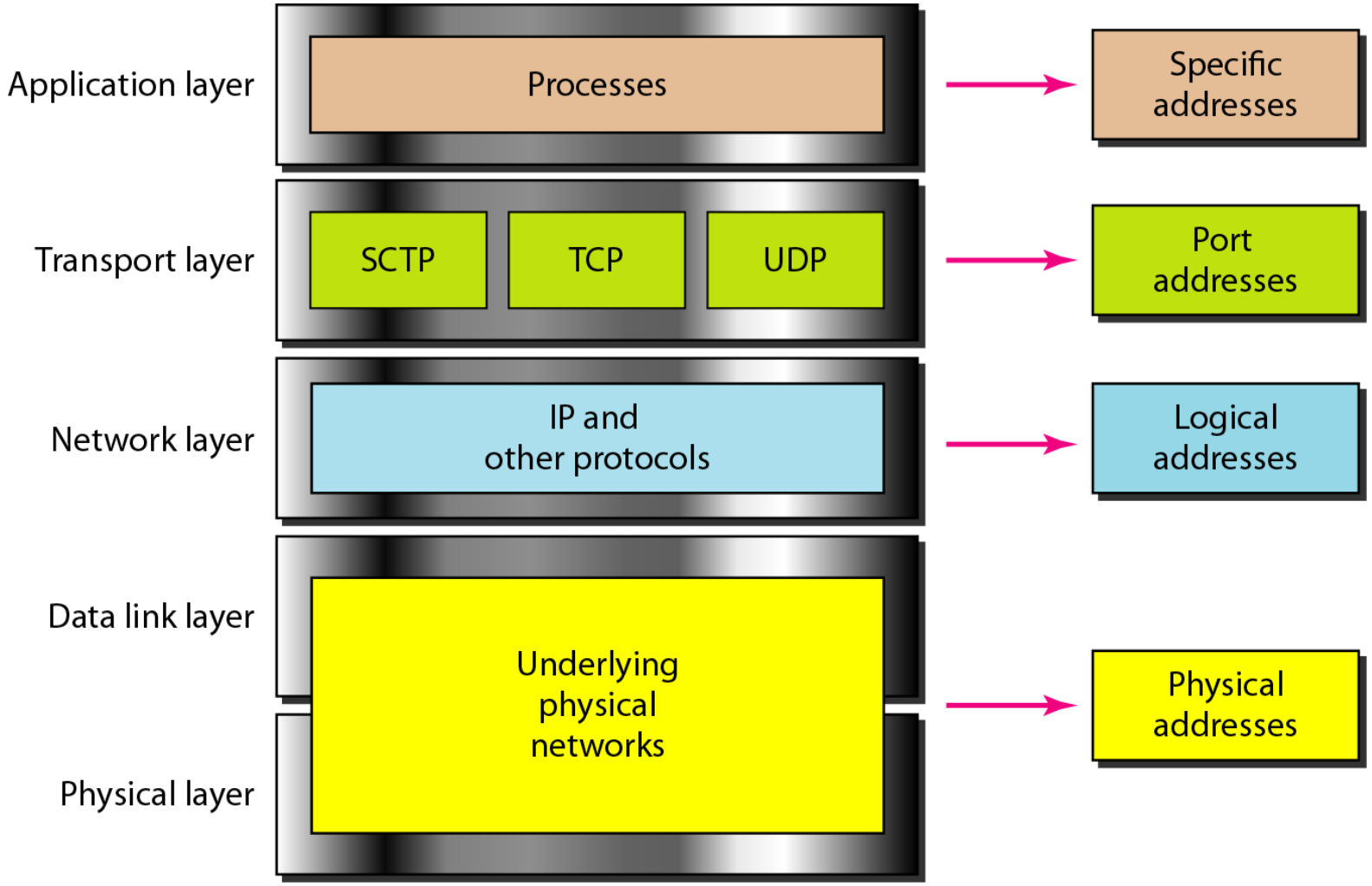
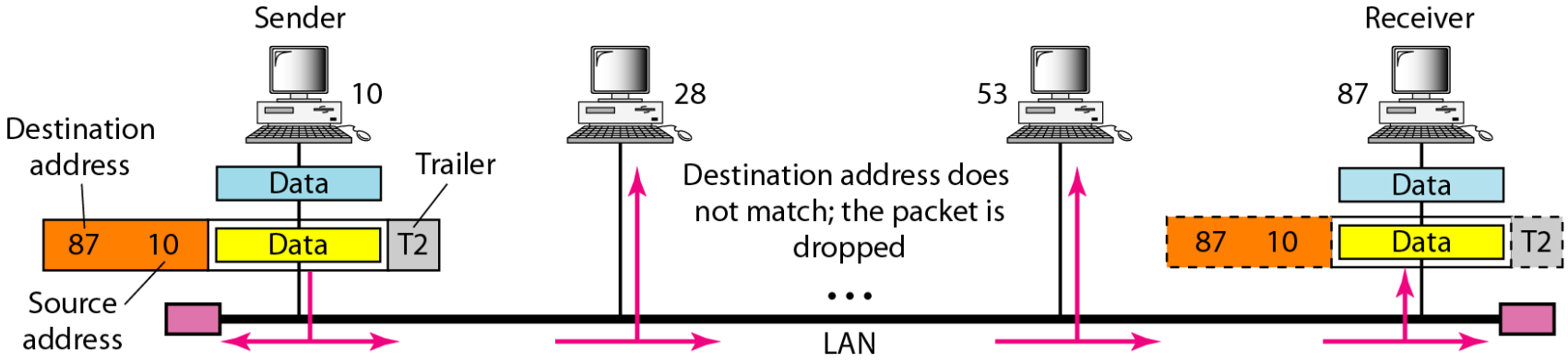


Figure 2.18 *Relationship of layers and addresses in TCP/IP*



Example 2.1

A node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.



Example 2.2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

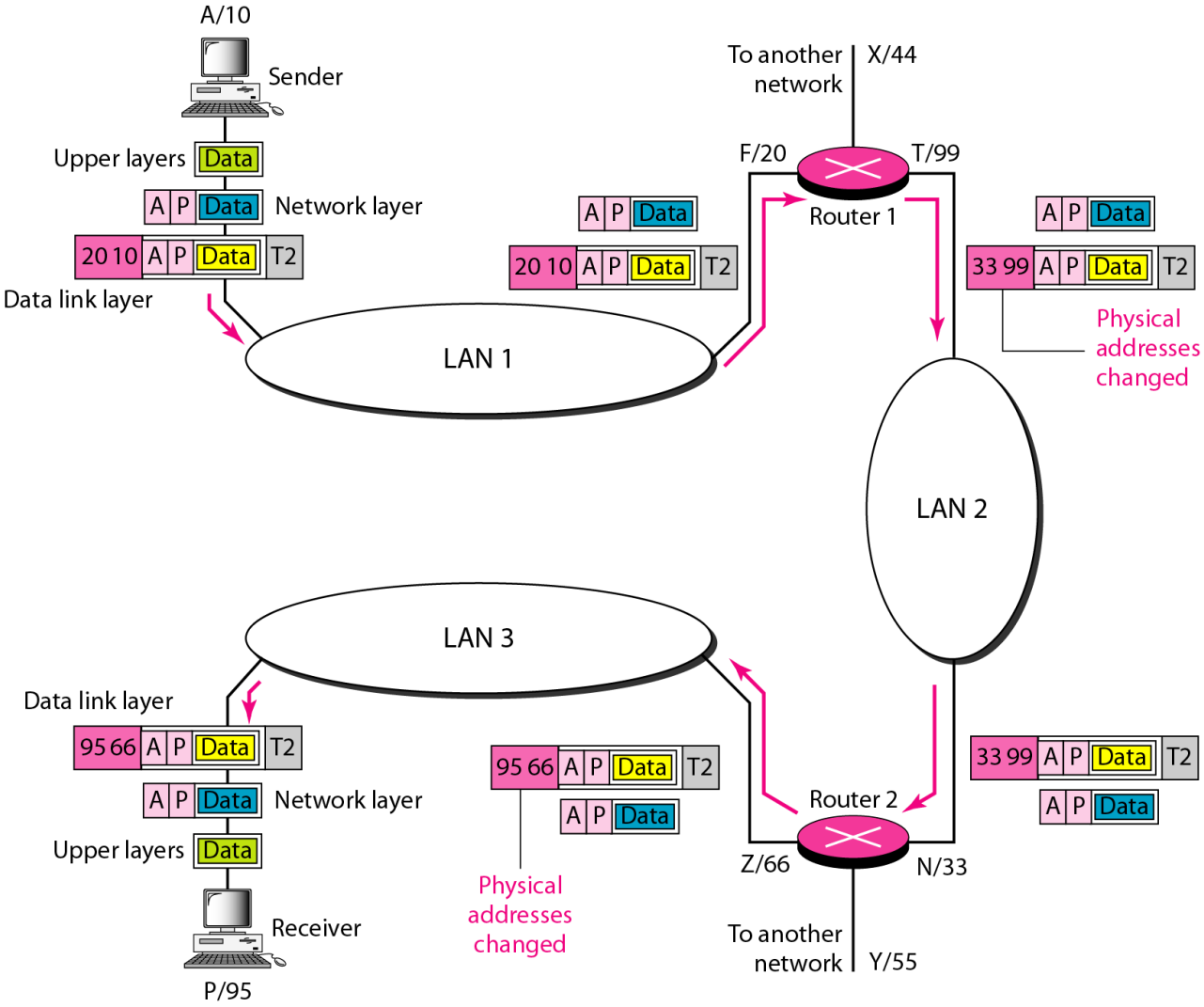
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Example 2.3

Part of an internet with two routers connecting three LANs is shown. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

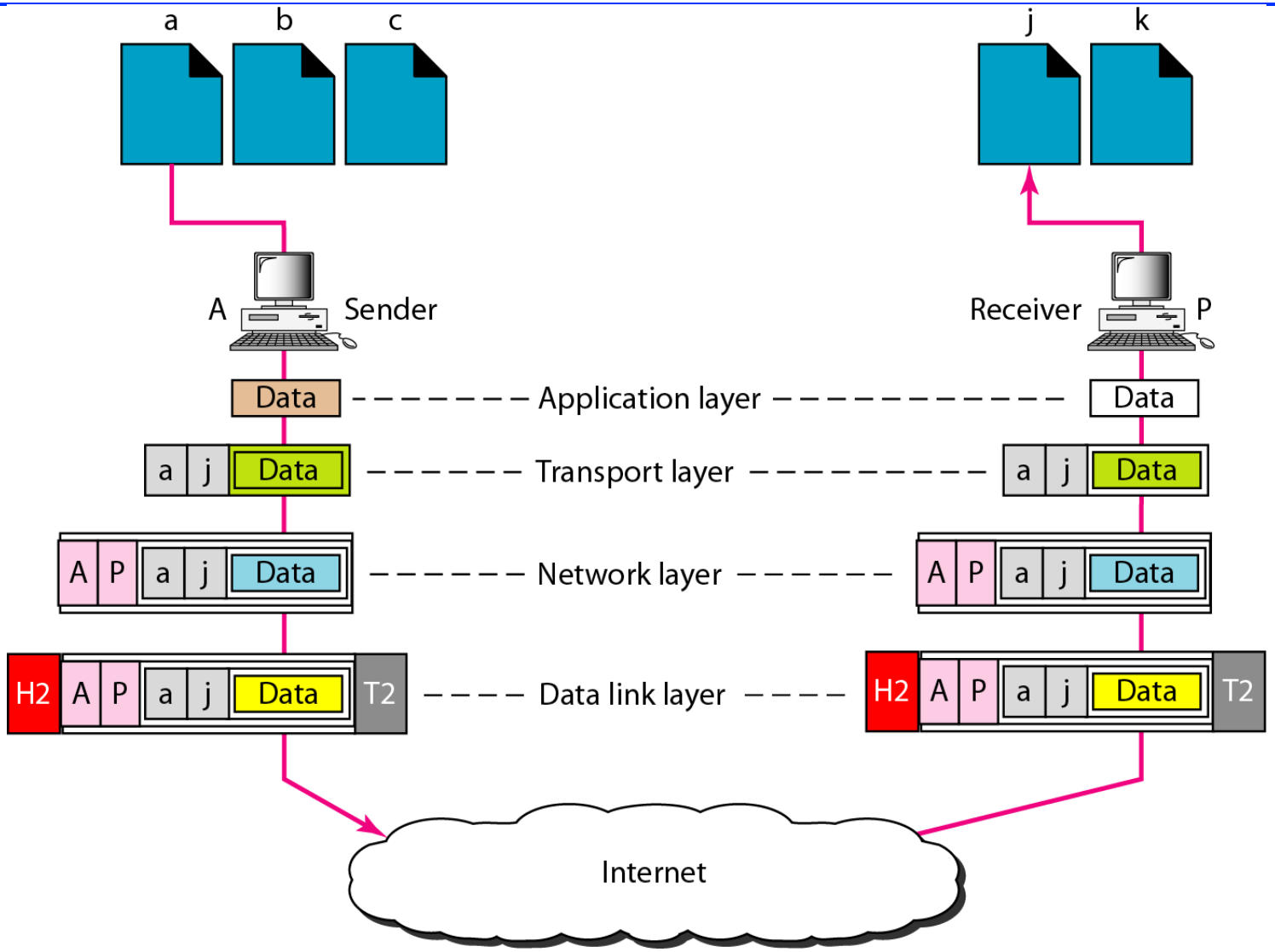
IP addresses



Example 2.4

Two computers are communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Port addresses



Note

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

Example 2.5

A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented
as one single number.

Note

The physical addresses change from hop to hop,
but the logical and port addresses usually remain the same.

Network Layer:
Internet Protocol

Ch20: Data communications and networking, Forouzan

5.3: Textbook

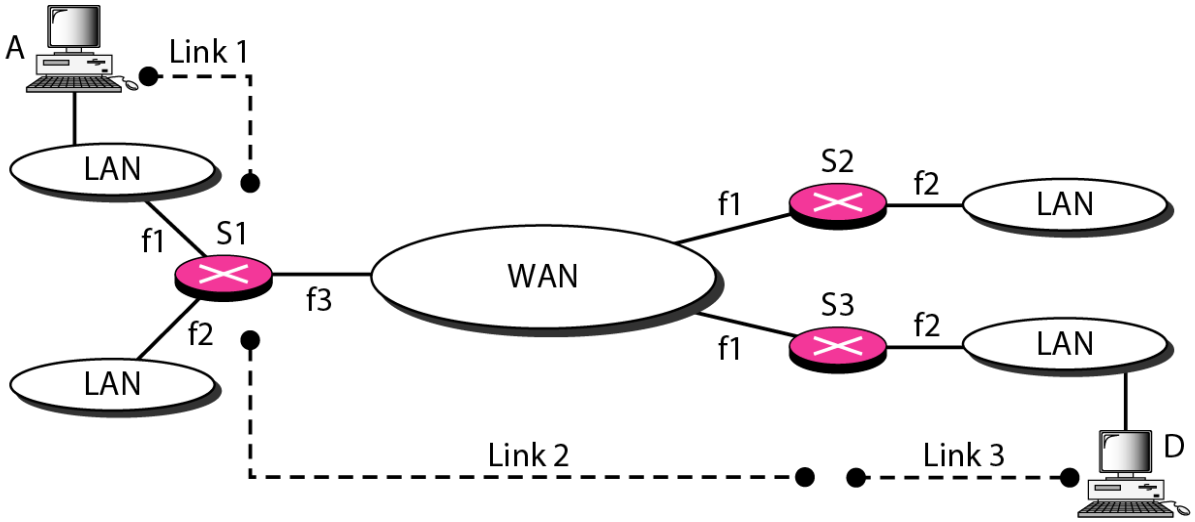
INTERNETWORKING

In this section, we discuss internetworking, connecting networks together to make an internetwork or an internet.

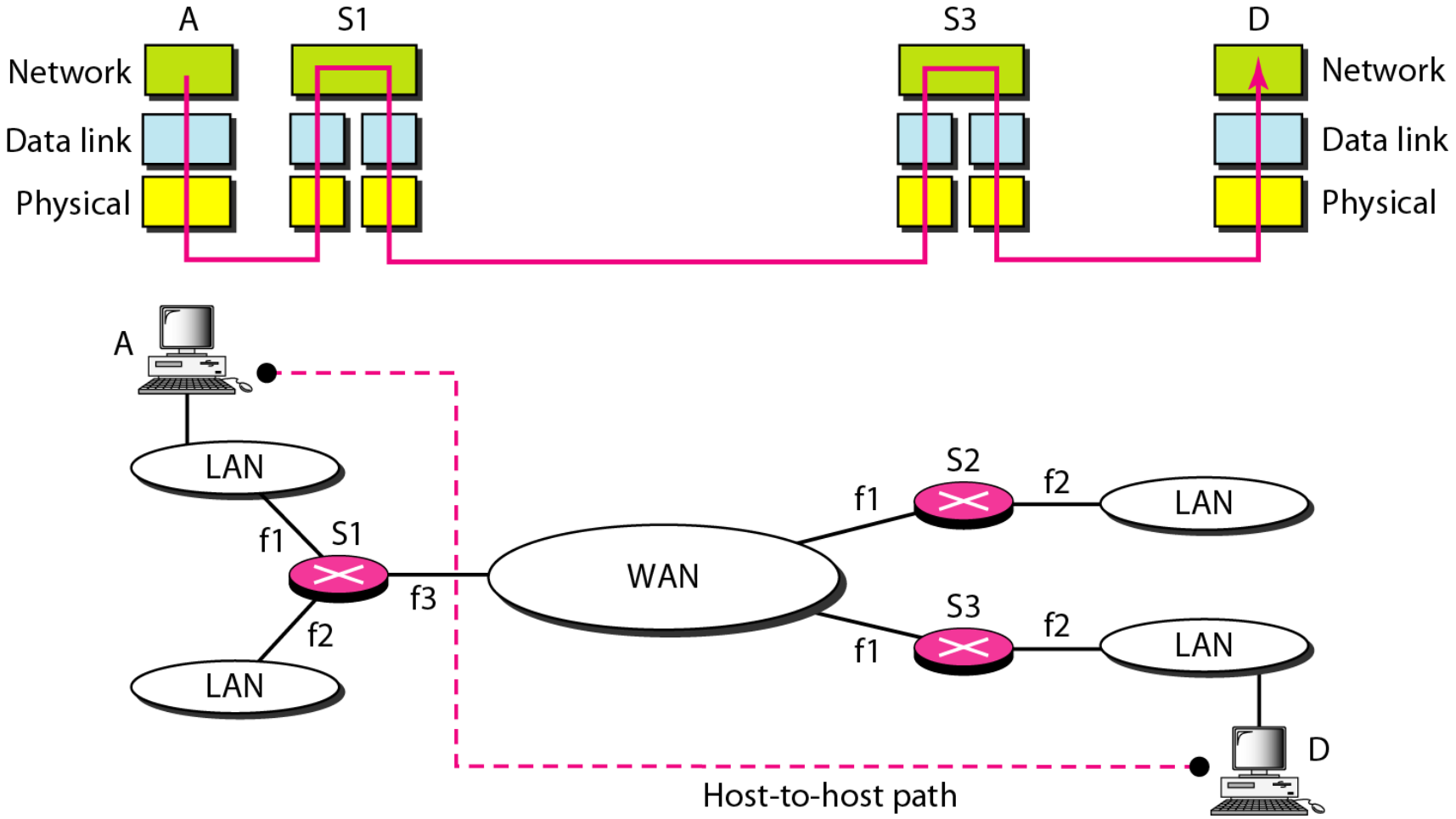
Topics discussed in this section:

Need for Network Layer
Internet as a Datagram Network
Internet as a Connectionless Network

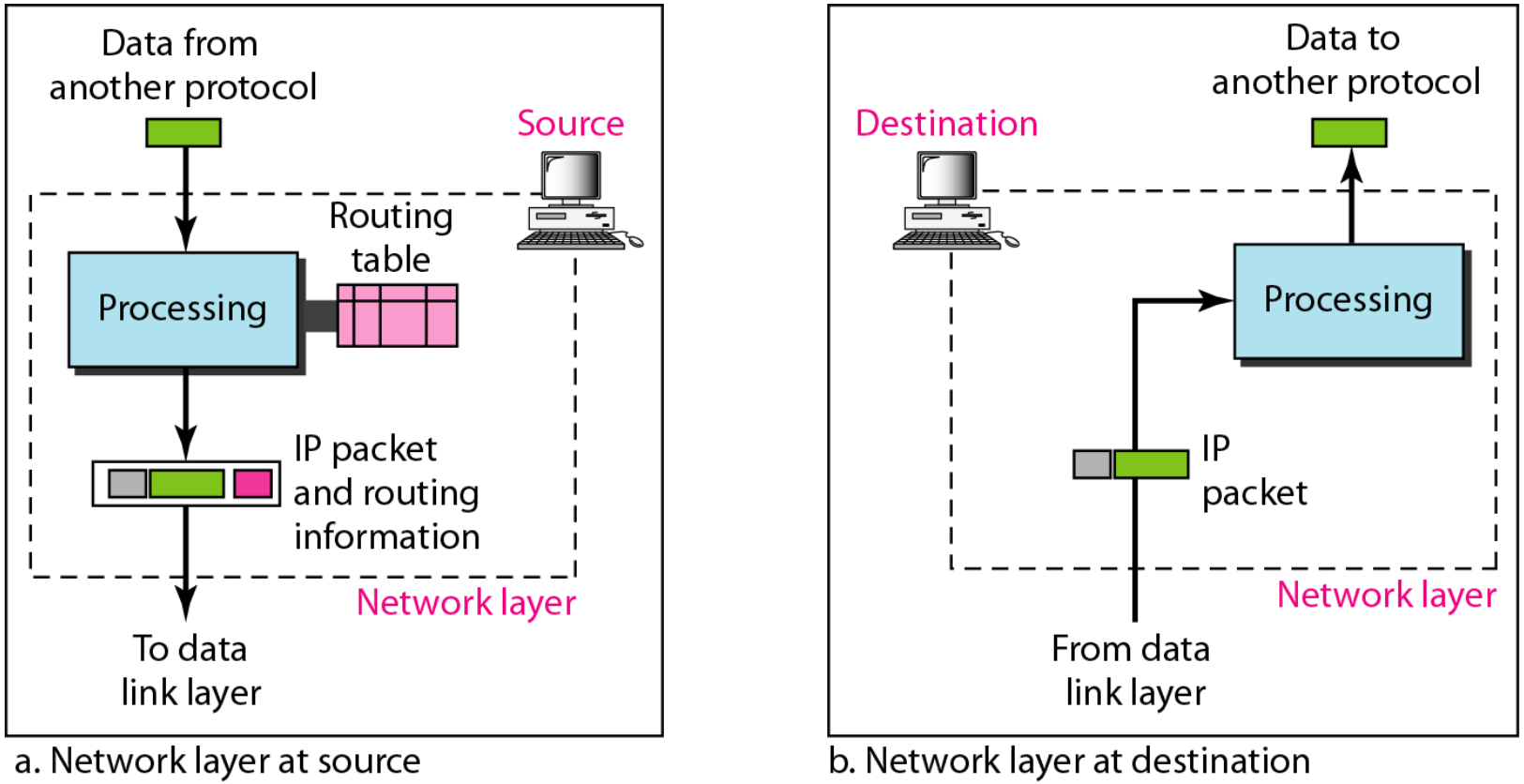
Links between two hosts



Network layer in an internetwork



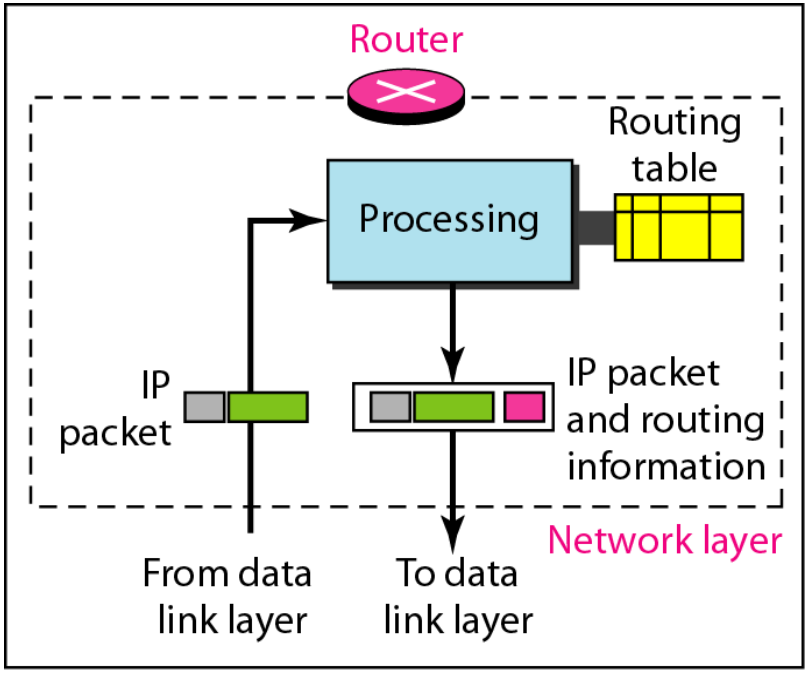
Network layer at the source, router, and destination



a. Network layer at source

b. Network layer at destination

Network layer at the source, router, and destination (continued)



c. Network layer at a router

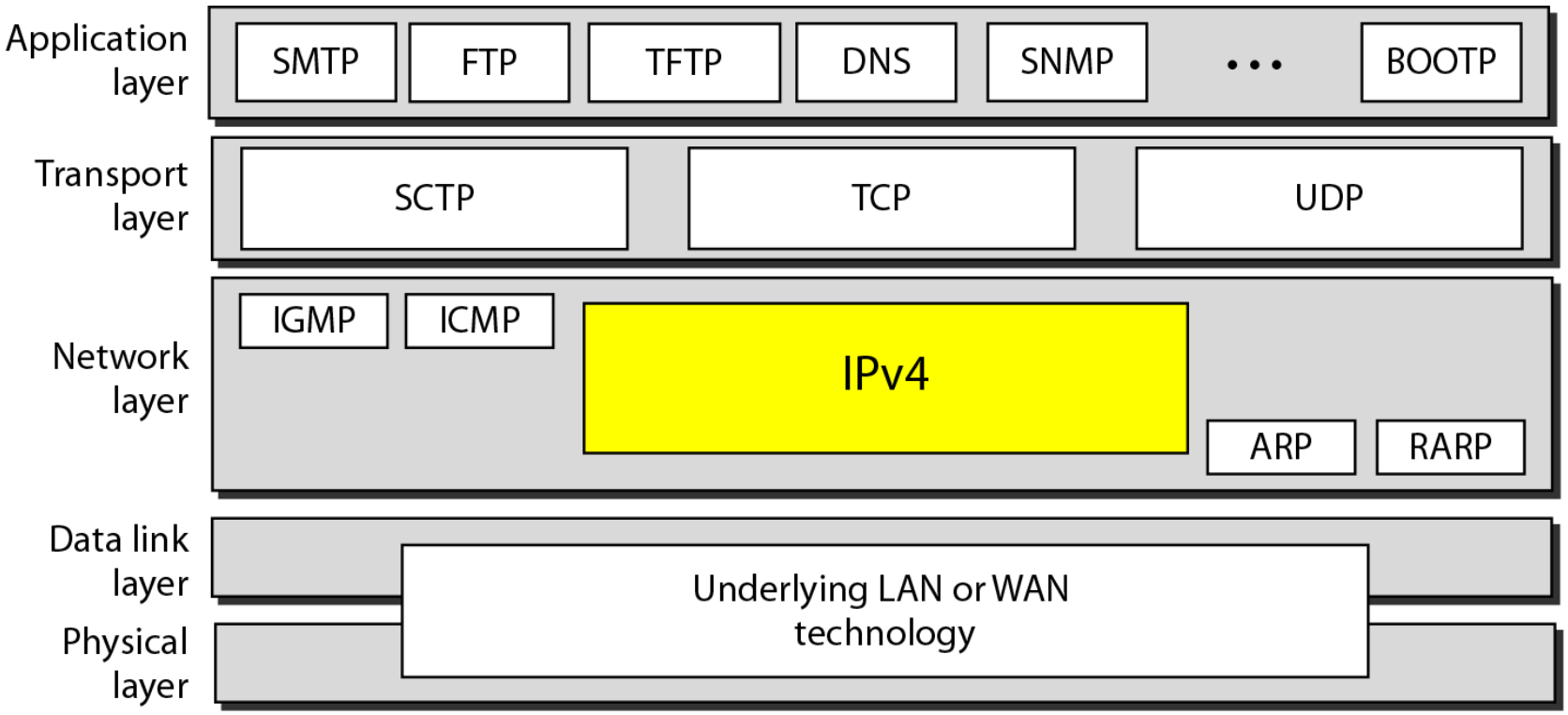
IPv4

The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.

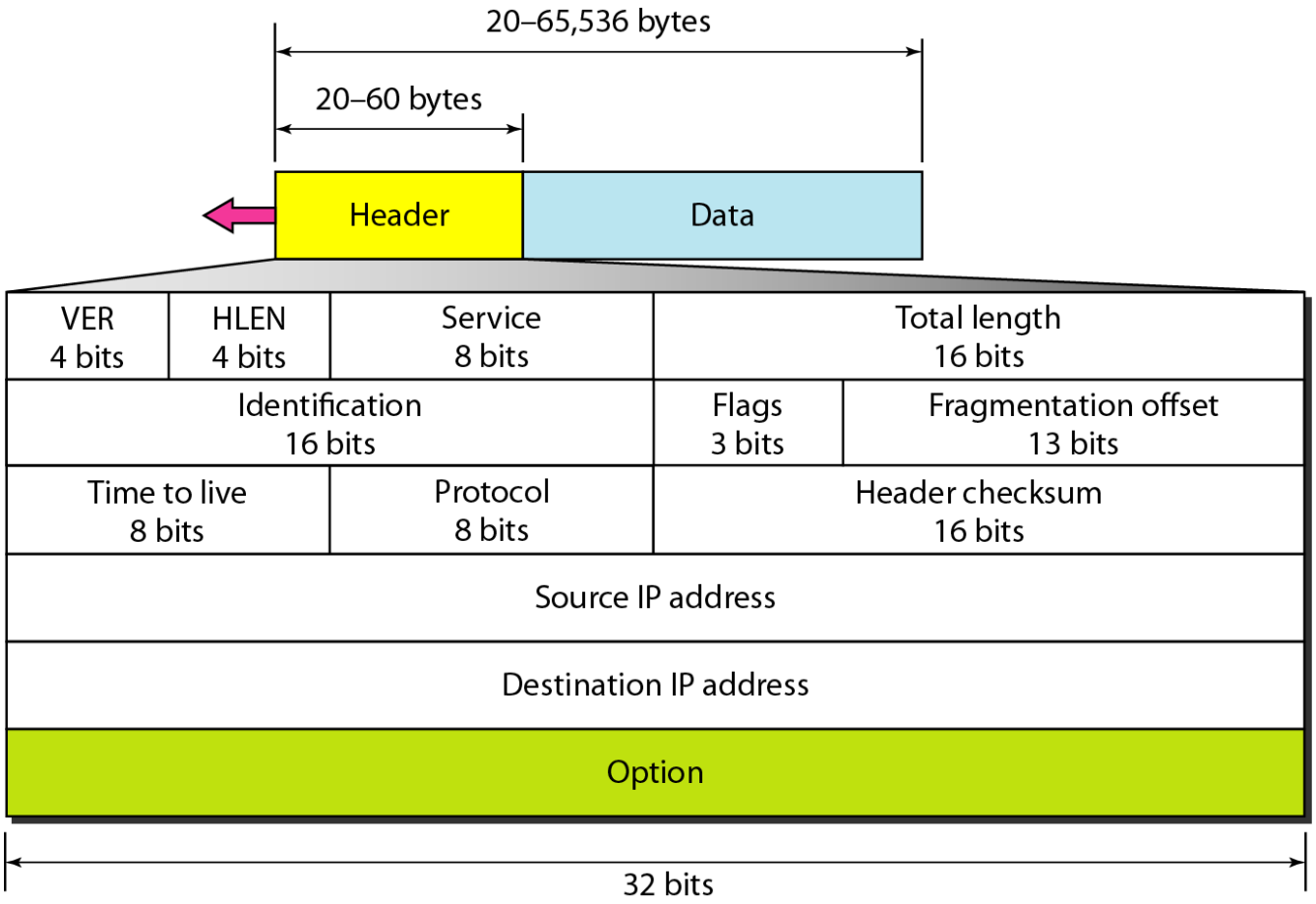
Topics discussed in this section:

Datagram
Fragmentation
Checksum
Options

Position of IPv4 in TCP/IP protocol suite

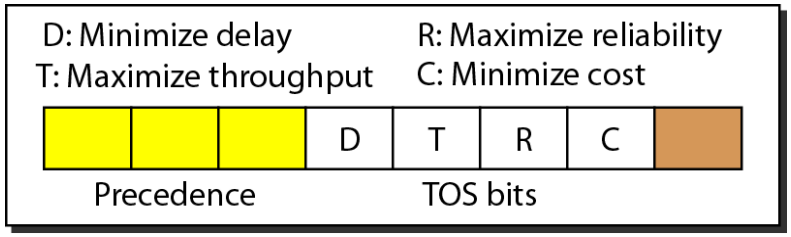


IPv4 datagram format

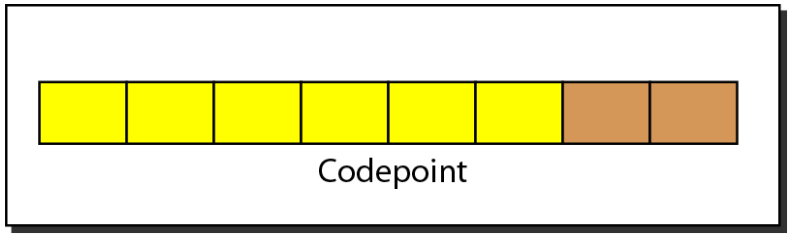


- VER (Version): defines the version of IPv4 protocol
- HLEN (Header Length): total length of the datagram header in 4-byte words. Default: 20 bytes (value = 5)

Service type or differentiated services



Service type



Differentiated services

Service type -> Differentiated services

Differentiated services (8 bit):

compatible with "Precedence" bits

Types of service

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Default types of service

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

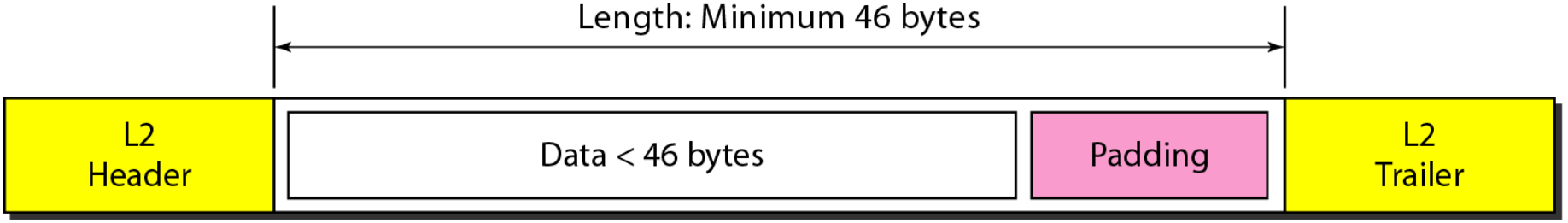
Values for codepoints

Category	Codepoint	Assigning authority
1	xxxxx0	Internet
2	xxxx11	Local
3	xxxx01	Temporary or experimental

Note

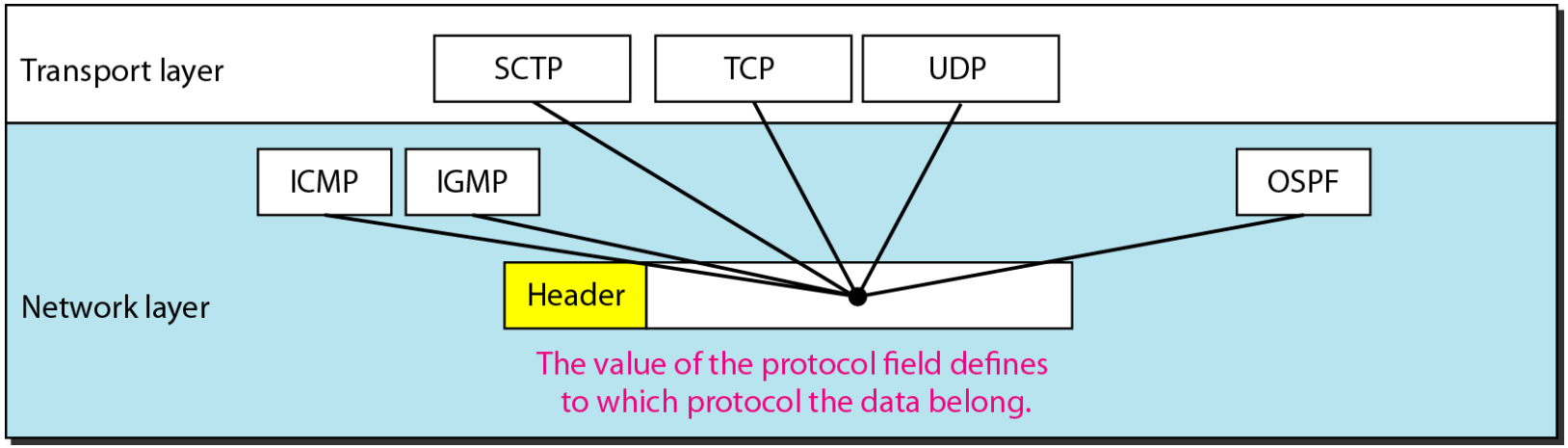
The total length field (16-bit) defines the total length of the datagram including the header.
Length of Data = total length – header length

Encapsulation of a small datagram in an Ethernet frame



Time to live field (8-bit): to control maximum number of hops (routers) visited by the datagram

Protocol field (8-bit) and encapsulated data



Protocol values

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

Example 1

An IPv4 packet has arrived with the first 8 bits as shown:

01000010

The receiver discards the packet. Why?

Solution

There is an error in this packet. The 4 leftmost bits (0100) show the version, which is correct. The next 4 bits (0010) show an invalid header length ($2 \times 4 = 8$). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Example 2

In an IPv4 packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?

Solution

The HLEN value is 8, which means the total number of bytes in the header is 8 × 4, or 32 bytes. The first 20 bytes are the base header, the next 12 bytes are the options.

Example 3

In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is 0x0028. How many bytes of data are being carried by this packet?

Solution

The HLEN value is 5, which means the total number of bytes in the header is 5 × 4, or 20 bytes (no options). The total length is 40 bytes, which means the packet is carrying 20 bytes of data (40 – 20).

Example 4

An IPv4 packet has arrived with the first few hexadecimal digits as shown.

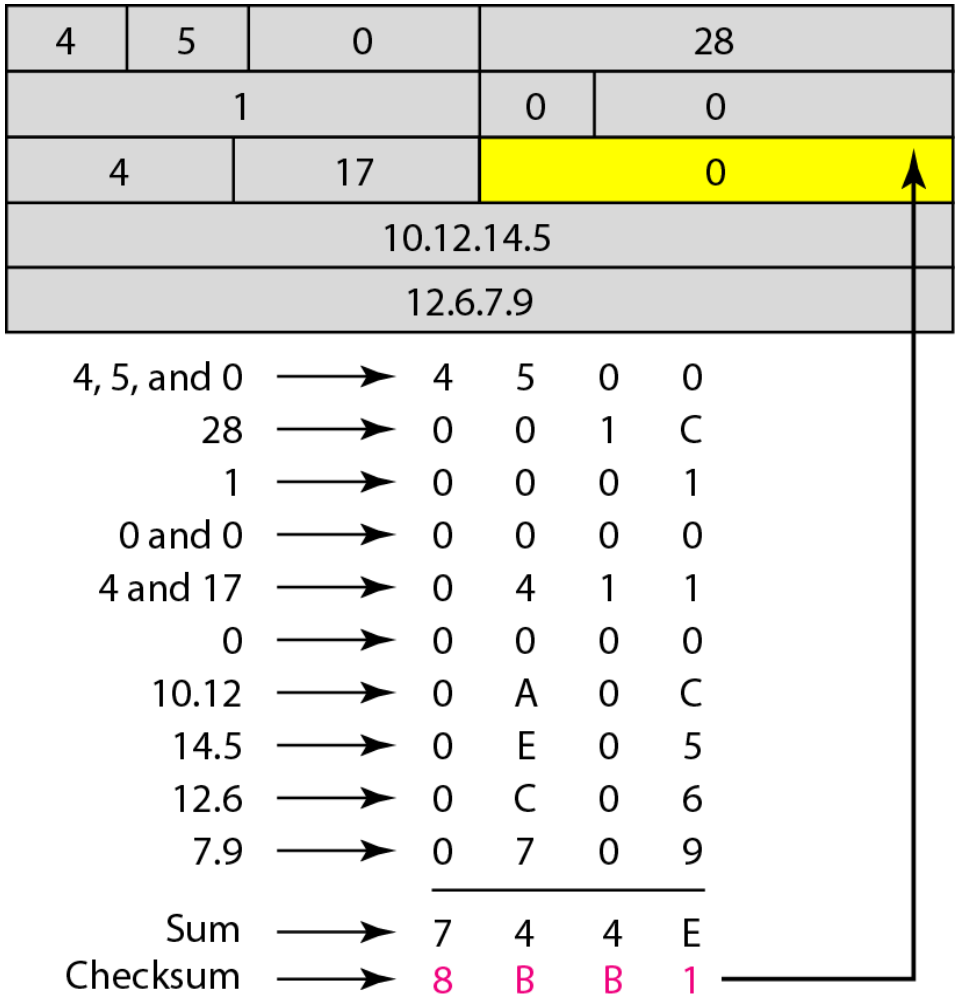
0x45000028000100000102 . . .

How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?

Solution

To find the time-to-live field, we skip 8 bytes. The time-to-live field is the ninth byte, which is 01. This means the packet can travel only one hop. The protocol field is the next byte (02), which means that the upper-layer protocol is IGMP.

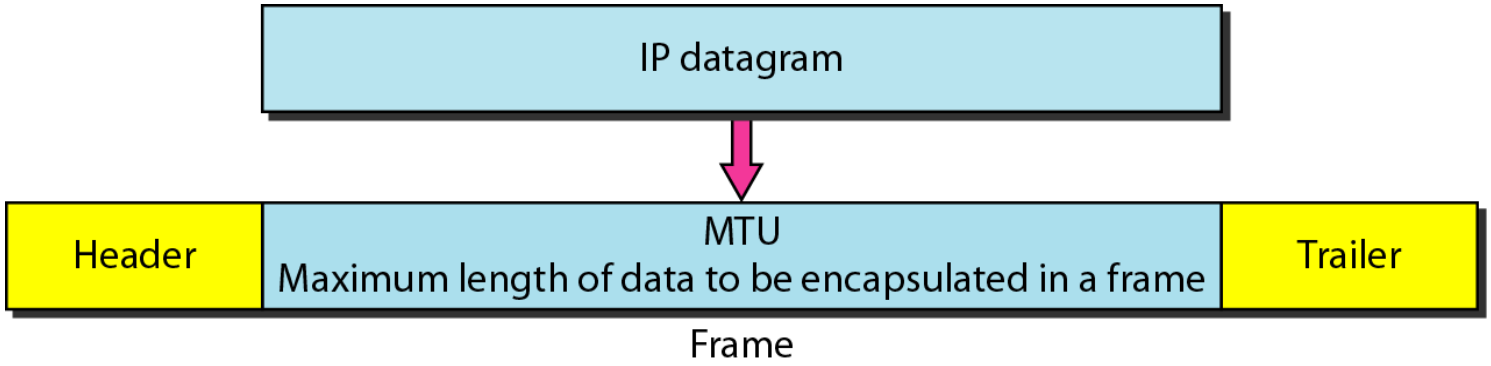
Example of checksum (16-bits) calculation in IPv4



Source address (32-bit): defines IPv4 address of the source

Destination address (32-bit): defines IPv4 address of the destination

Maximum transfer unit (MTU)



MTUs for some networks

Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

Fields related to fragmentation

Identification (16-bit): identifies a datagram originating from the source host

Flag (3-bit): do not fragment or more fragments

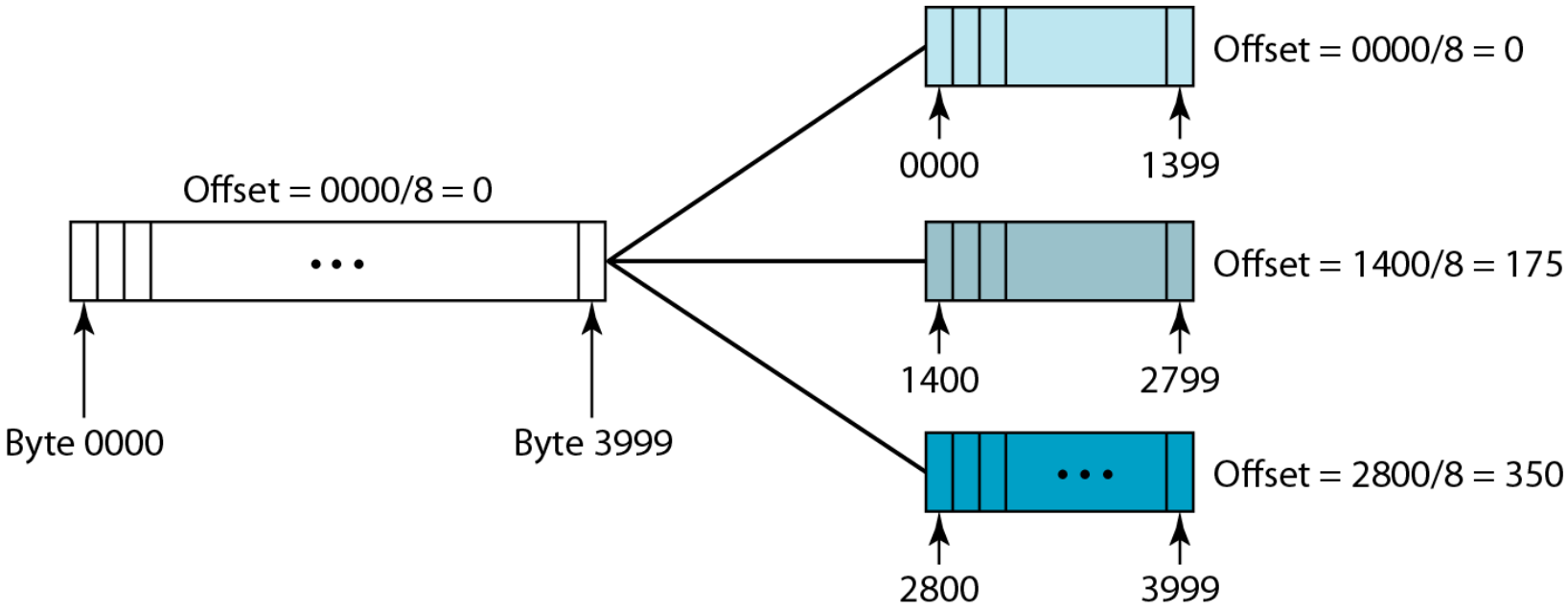
Fragmentation offset (13-bit): shows the relative position of this fragment; measured in units of 8 bytes

Options (maximum of 40 bytes): used for network testing and debugging

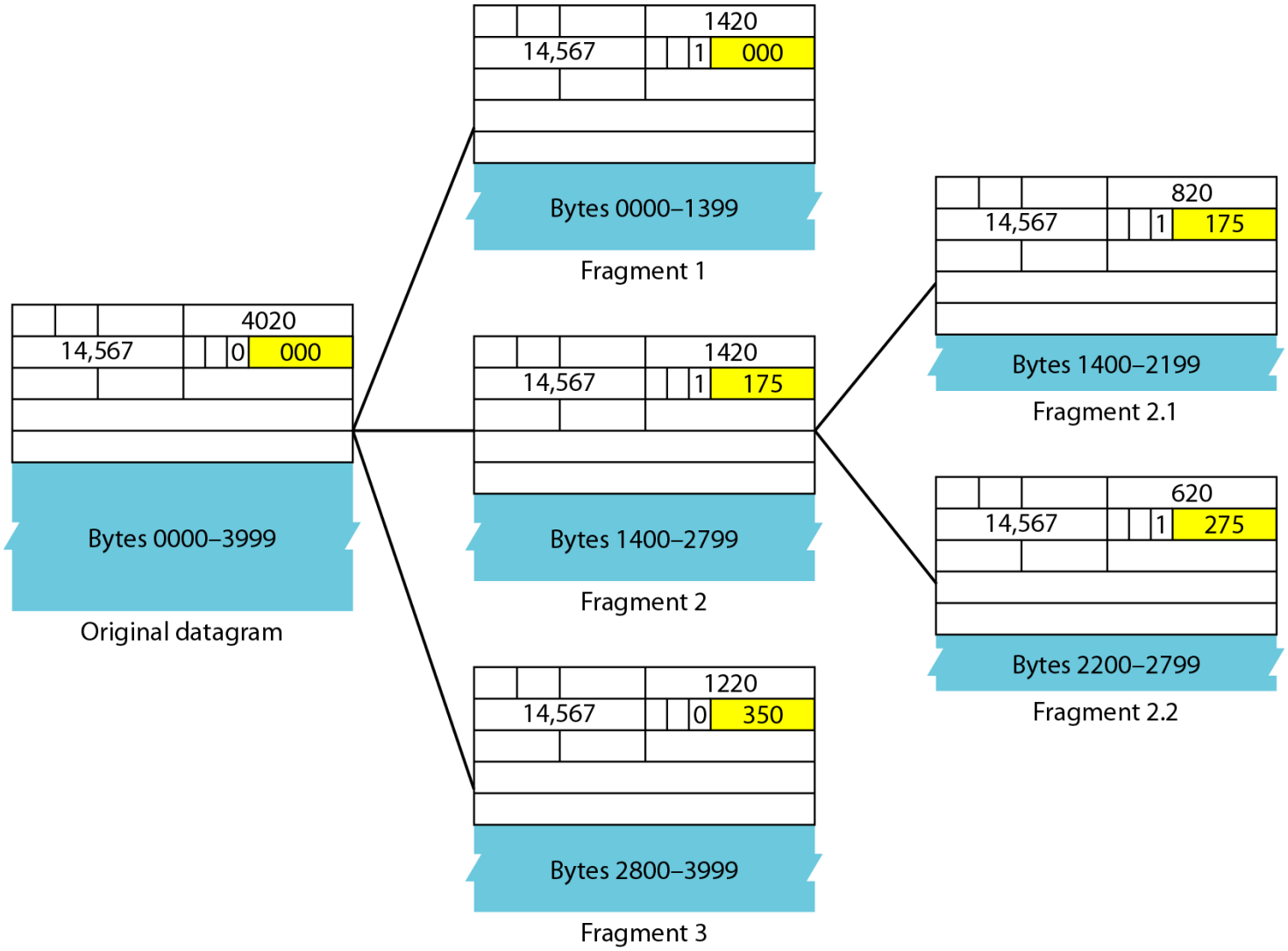
Flags used in fragmentation

D: Do not fragment
M: More fragments

Fragmentation example



Detailed fragmentation example



Example 5

A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 0, it means that there are no more fragments; the fragment is the last one. However, we cannot say if the original packet was fragmented or not. A non-fragmented packet is considered the last fragment.

Example 6

A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 1, it means that there is at least one more fragment. This fragment can be the first one or a middle one, but not the last one. We don't know if it is the first one or a middle one; we need more information (the value of the fragmentation offset).

Example 7

A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

Solution

Because the M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0, it is the first fragment.

Example 8

A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Solution

To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length.

Example 9

A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?

Solution

The first byte number is 100 × 8 = 800. The total length is 100 bytes, and the header length is 20 bytes (5 × 4), which means that there are 80 bytes in this datagram. If the first byte number is 800, the last byte number must be 879.

IPv6

The network layer protocol in the TCP/IP protocol suite is currently IPv4. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 has some deficiencies that make it unsuitable for the fast-growing Internet.

Topics discussed in this section:

Advantages
Packet Format
Extension Headers

Advantages

-larger address space

-better header format

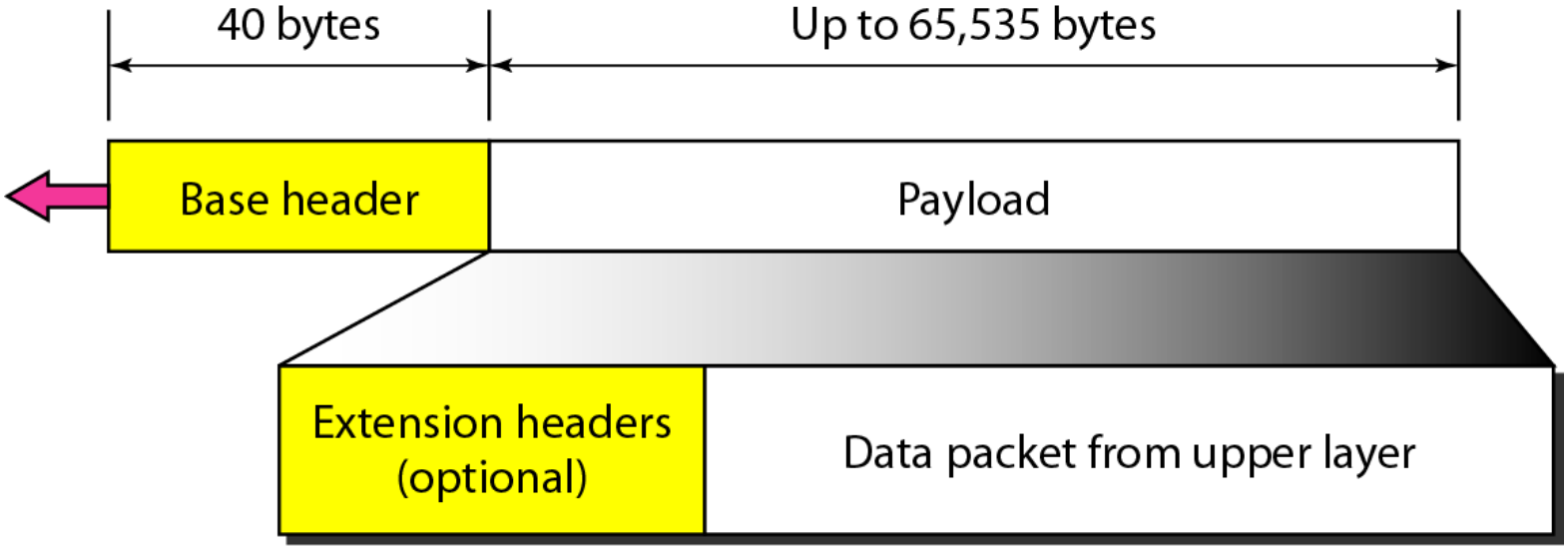
-new options

-allowance for extension

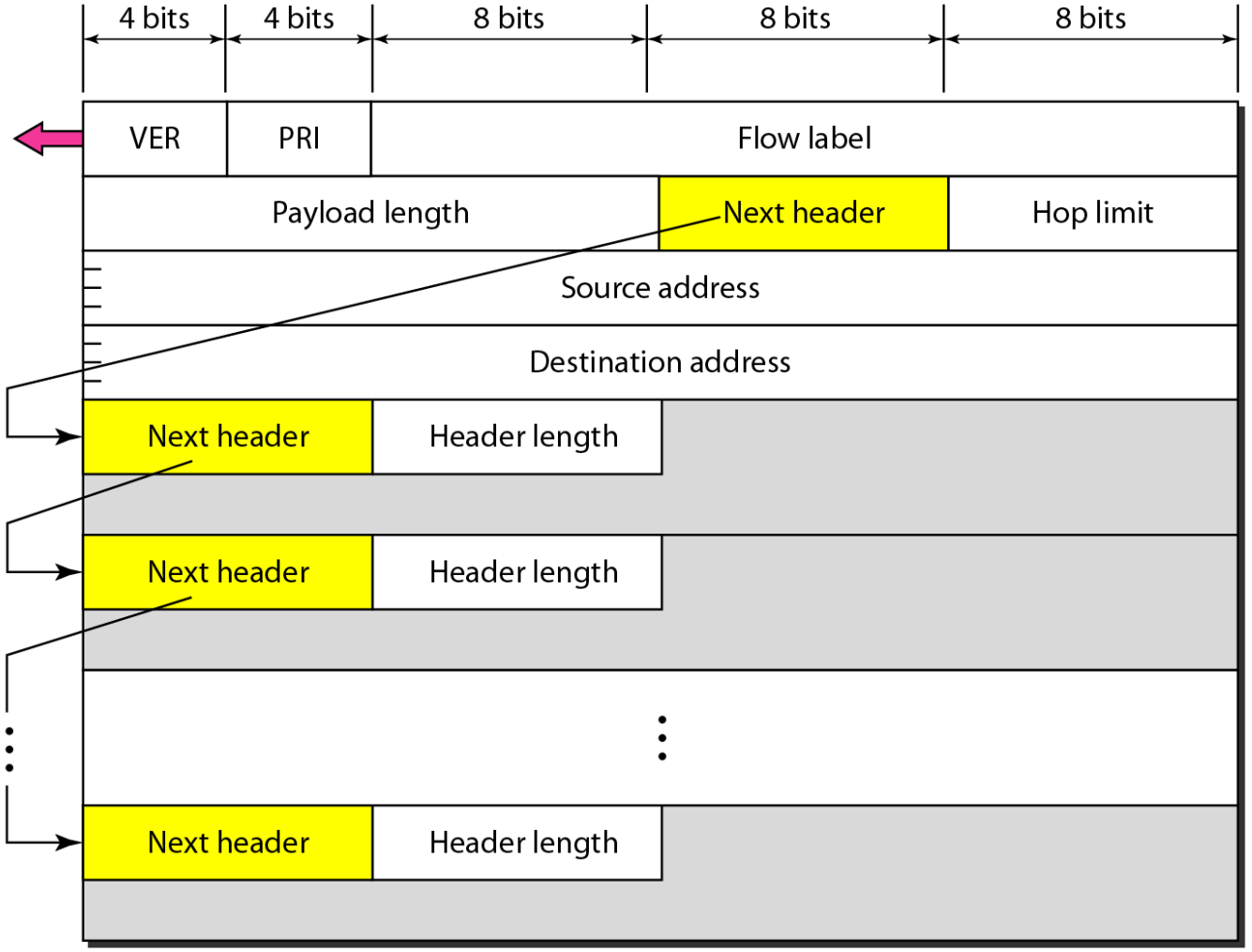
-support for resource allocation

-support for more security

IPv6 datagram header and payload



Format of an IPv6 datagram



Version (4-bit): value is 6.

Priority (4-bit): defines the priority of the packet with respect to traffic congestion.

Flow label (24-bit): to provide special handling for a particular flow of data

Payload length (16-bit): defines the length of IP datagram excluding the base header

Next header (8-bit): defines the header following the based header in the datagram (=protocol in IPv4)

Hop limit (8-bit): (=TTL in IPv4)

Source address (128-bit)

Destination address (128-bit)

Next header codes for IPv6

Code	*Next Header*
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no next header)
60	Destination option

Priorities for congestion-controlled traffic

Priority	*Meaning*
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

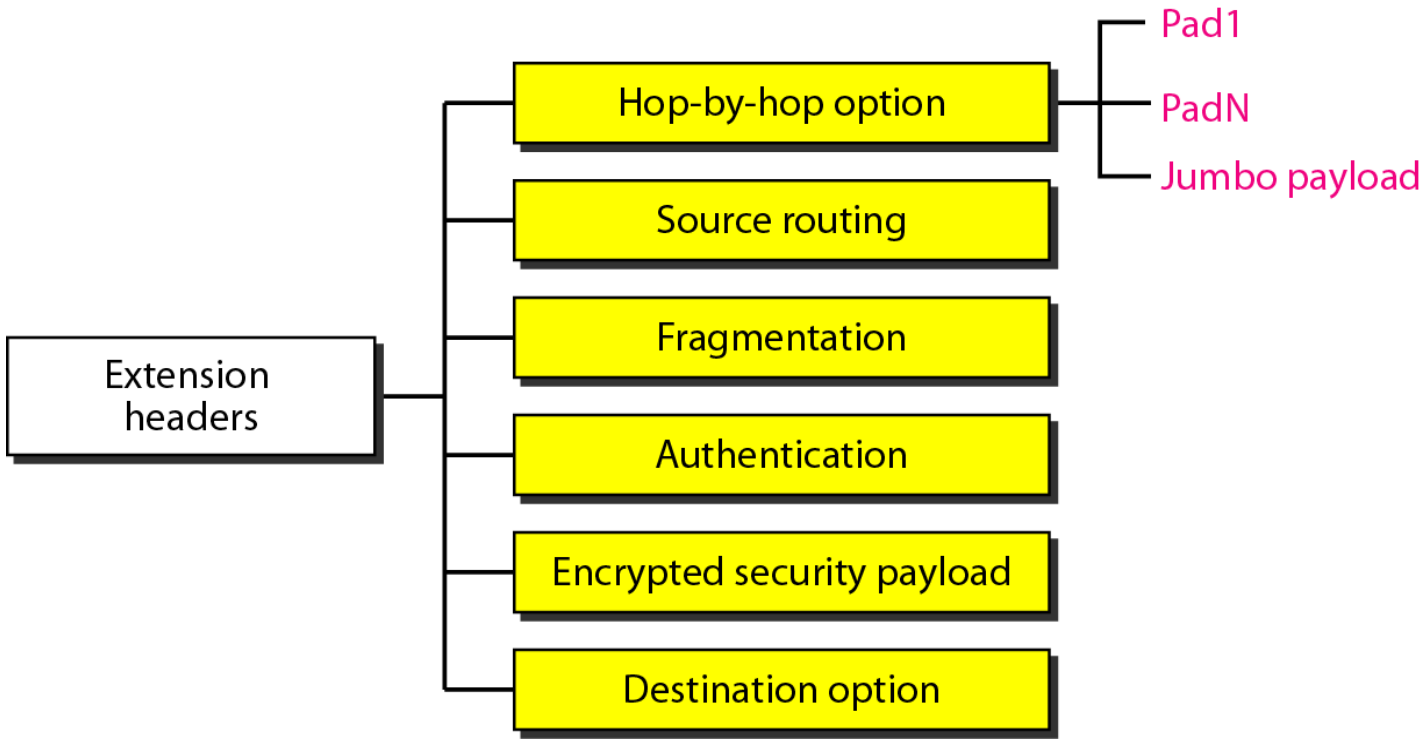
Priorities for noncongestion-controlled traffic

Priority	*Meaning*
8	Data with greatest redundancy
. . .	. . .
15	Data with least redundancy

Comparison between IPv4 and IPv6 packet headers

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Extension header types



Comparison between IPv4 options and IPv6 extension headers

Comparison
1. The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
2. The record route option is not implemented in IPv6 because it was not used.
3. The timestamp option is not implemented because it was not used.
4. The source route option is called the source route extension header in IPv6.
5. The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
6. The authentication extension header is new in IPv6.
7. The encrypted security payload extension header is new in IPv6.

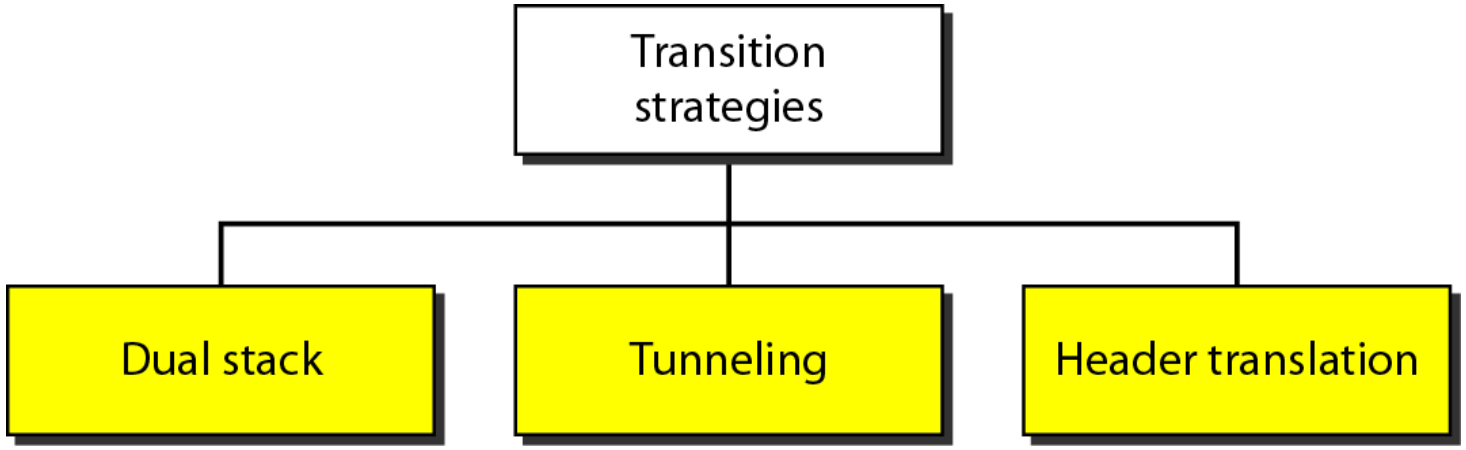
TRANSITION FROM IPv4 TO IPv6

Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems.

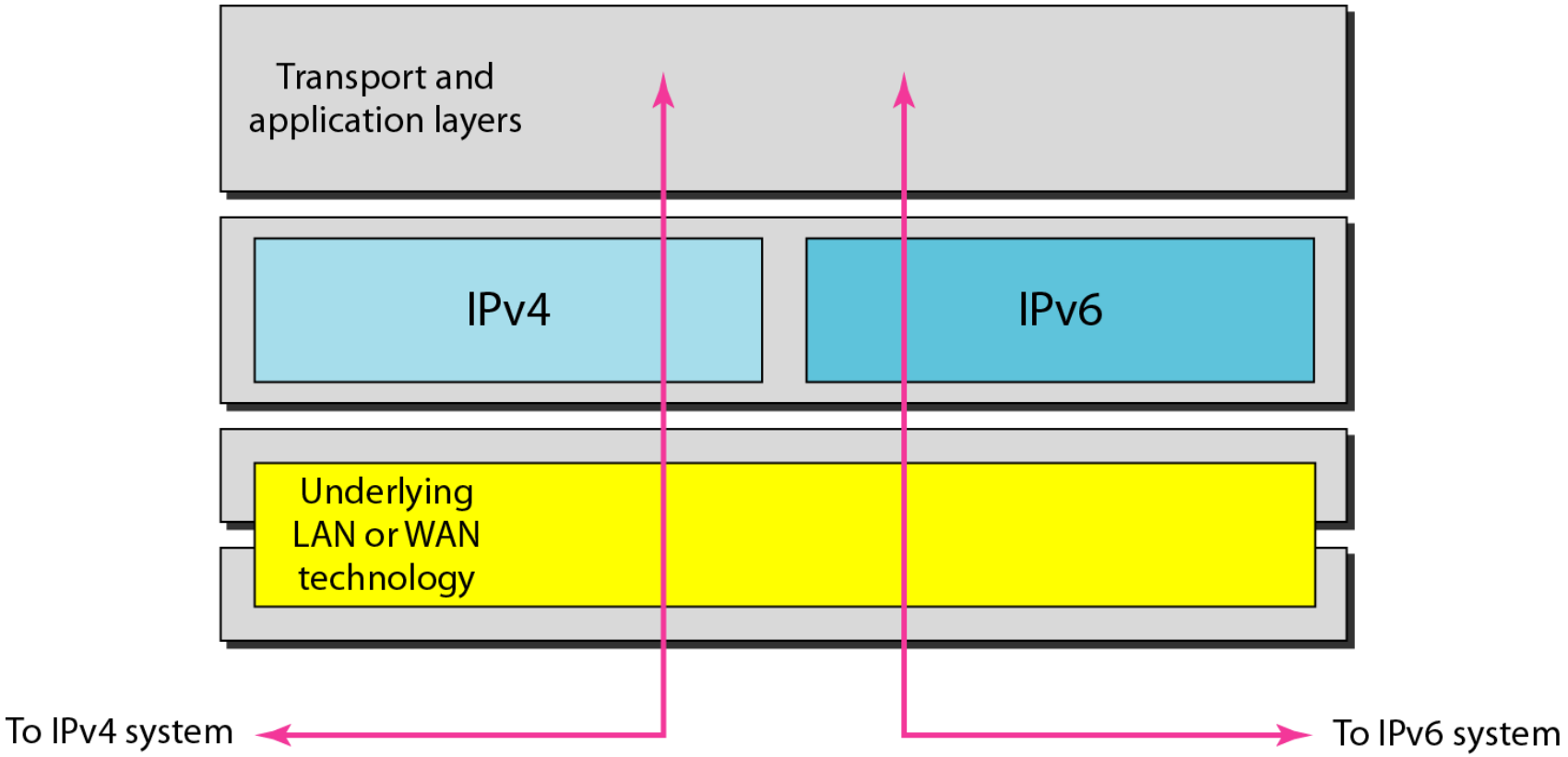
Topics discussed in this section:

Dual Stack
Tunneling
Header Translation

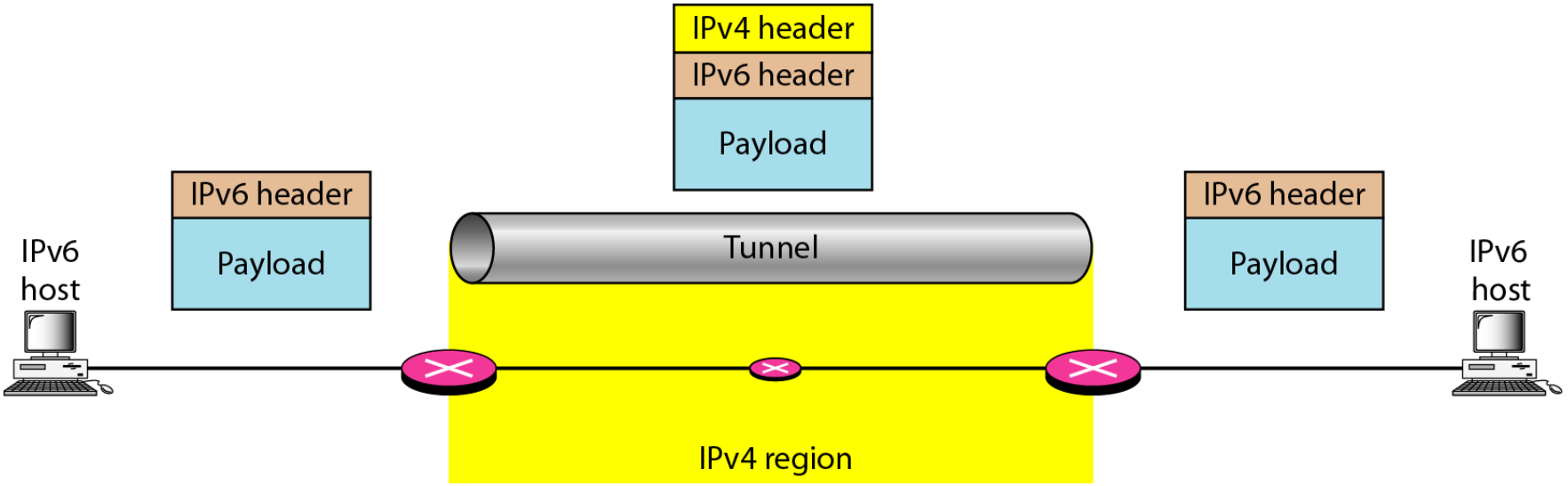
Three transition strategies



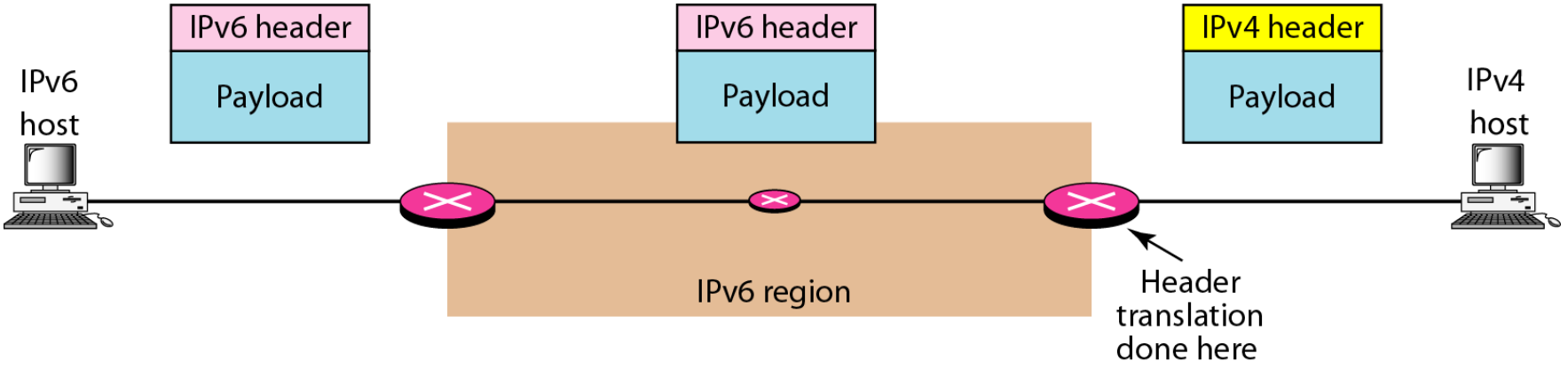
Dual stack


Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

Tunneling strategy



Header translation strategy



For more details,

www.ietf.org/rfc.html

IPv4: 760, 781, 791, 815, 1025, 1063, 1071, 1141, 1190, 1191, 1624, 2113

IPv6: 1365, 1550, 1678, 1682, 1683, 1686, 1688, 1726, 1752, 1826, 1883, 1884, 1886, 1887, 1955, 2080, 2373, 2452, 2463, 2465, 2466, 2472, 2492, 2545, 2590