

Chapter 3: Networking and Internetworking

From **Coulouris, Dollimore, Kindberg and Blair**
Distributed Systems: Concepts and Design

Edition 5, © Addison-Wesley 2012

From **Andrew S. Tanenbaum and David J. Wetherall**
Computer Networks

Edition 5, © Prentice Hall 2011

Outlines

- **Types of Networks**
- **Network Principles**
- **Internet Protocols**
- **Network Issues for Distributed Systems**

Types of Networks

- **PANs:** Personal Area Networks

- PANs are a subcategory of local networks in which the various digital devices carried by a user are connected by a low-cost, low-energy network.
- Small area in square meters.
- Example (Bluetooth Wireless PAN).
- Wired PANs are irrelevant: Too much wires on a person.

- **LANs:** Local Area Networks

- Spans Small Space (Usually a building or several close by buildings).
- Services to small number of people.
- Several segments can be distributed between building floor and connected via switches.

- **MANs:** Metropolitan Area Networks

- Connects two or more LANs.
- Spans larger area than LAN (Usually a city).

- **WANs:** Wide Area Networks

- Spans large geographical areas.
- The best example is the internet.

Figure 3.1 Network Performance

	<i>Example</i>	<i>Range</i>	<i>Bandwidth (Mbps)</i>	<i>Latency (ms)</i>
<i>Wired:</i>				
LAN	Ethernet	1–2 kms	10–10,000	1–10
WAN	IP routing	worldwide	0.010–600	100–500
MAN	ATM	2–50 kms	1–600	10
Internetwork	Internet	worldwide	0.5–600	100–500
<i>Wireless:</i>				
WPAN	Bluetooth (IEEE 802.15.1)	10–30m	0.5–2	5–20
WLAN	WiFi (IEEE 802.11)	0.15–1.5 km	11–108	5–20
WMAN	WiMAX (IEEE 802.16)	5–50 km	1.5–20	5–20
WWAN	3G phone	cell: 1–5	348–14.4	100–500

Networks Principles

Packet transmission:

- Before a message is transmitted it is subdivided into packets. The simplest form of packet is a sequence of binary data (an array of bits or bytes) of restricted length, together with addressing information sufficient to identify the source and destination computers.
- Packets of restricted length are used:
 - So that each computer in the network can allocate sufficient buffer storage to hold the largest possible incoming packet.
 - To avoid the undue delays that would occur in waiting for communication channels to become free if long messages were transmitted without subdivision.

Networks Principles

Data streaming:

- The transmission and display of audio and video in real time is referred to as streaming.
- It requires much higher bandwidths than most other forms of communication in distributed systems.

Switching schemes:

- To transmit information between two arbitrary nodes, a switching system is required.
- We define **four types of switching** that are used in computer networking:
 1. **Broadcast**
 2. **Circuit switching**
 3. **Packet switching**
 4. **Frame relay**

Networks Principles

1. **Broadcast** is a transmission technique that involves no switching. Everything is transmitted to every node. Some LAN technologies, including Ethernet, are based on broadcasting. Wireless networking is based on broadcasting.
2. **Circuit switching** such as telephone networks (telecommunication networks). When a caller dialed a number, the pair of wires from his/her phone to the local exchange was connected by an automatic switch at the exchange to the pair of wires connected to the other party's phone.
3. **Packet switching** is a store-and-forward network that forwards packets from their source to their destination. There is a computer at each switching node. Each packet arriving at a node is first stored in memory at the node and then processed by a program that transmits it on an outgoing circuit, which transfers the packet to another node that is closer to its ultimate destination.

Networks Principles

- In packet switching it takes anything from a few tens of microseconds to a few milliseconds to switch a packet through each network node in a store-and-forward network.
- This switching delay depends on:
 - Packet size.
 - Hardware speed.
 - Quantity of other traffic.
- But delay's lower bound is determined by the network bandwidth.
- Since the entire packet must be received before it can be forwarded to another node. Thus, the Internet is based on store-and-forward switching.

Networks Principles

4. Frame relay

- Depends on smaller size units called frames.
- Unlike packet-switching, a frame is not stored on intermediate nodes. This way delay is minimized.
- A node relays (forwards) a frame by examining the first few bits of a frame.
- It is sufficient to streaming application because delay degrades the service.

Networks Principles

Protocols:

The term protocol is used to refer to a set of rules and formats to be used for communication between processes in order to perform a given task.

The definition of a protocol has two parts to it:

- A specification of the sequence of messages that must be exchanged.
 - Example: Acknowledgment: Reply that a message is received.
 - Example: Negative acknowledgment: Reply that message is not received.
- A specification of the format of the data in the messages.
 - Example: A message has information related to length of message, etc., then followed by the actual message.

Figure 3.2 Conceptual layering of protocol software

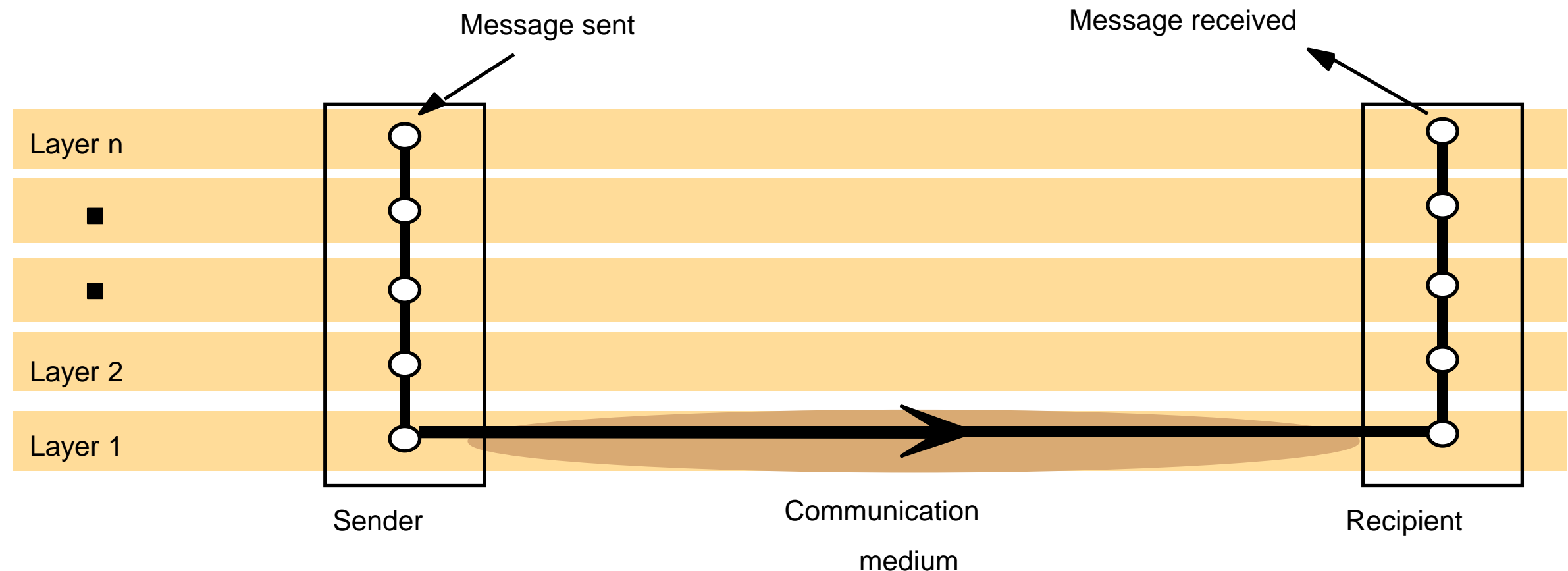


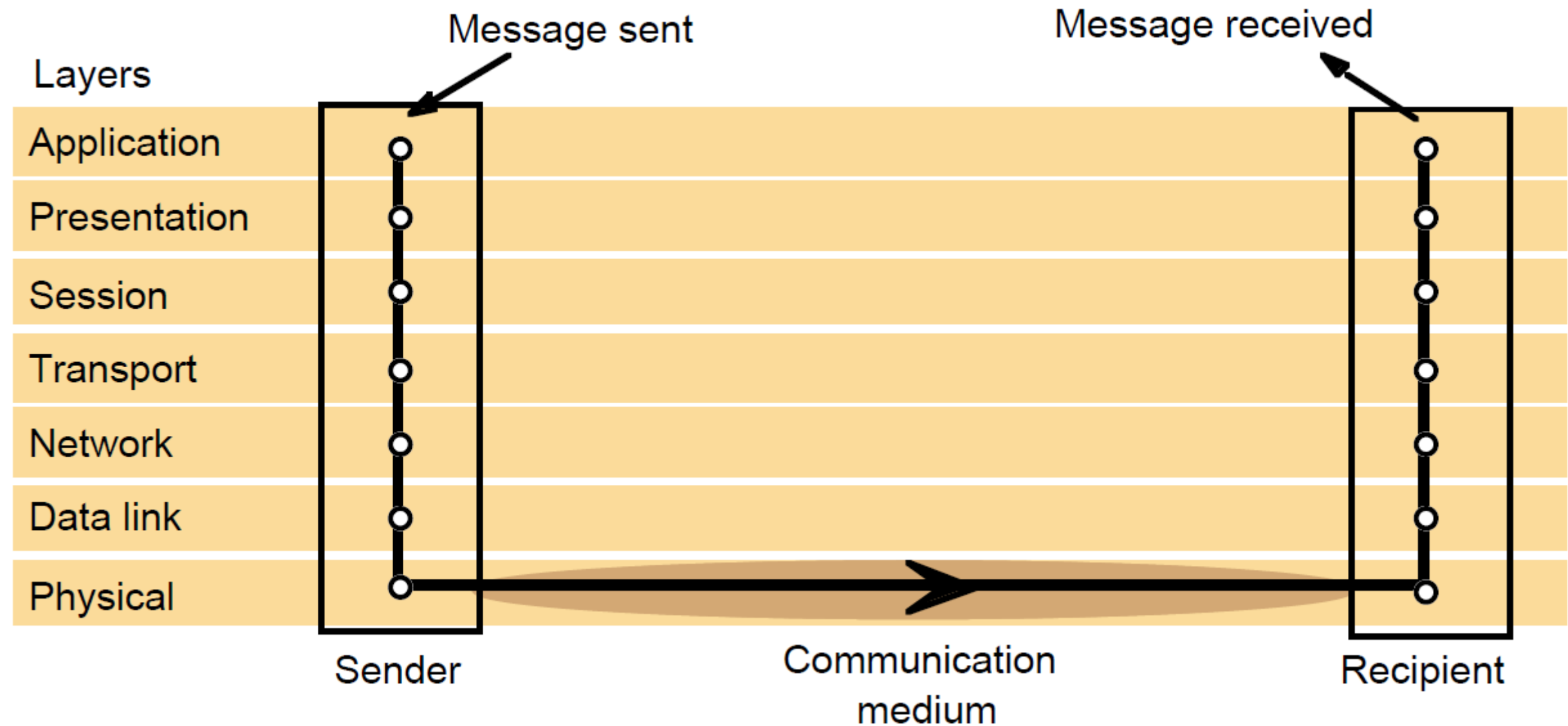
Figure 3.2 Illustrates the structure and the flow of data when a message is transmitted using a layered protocol. Thus, each layer of network software communicates by local procedure calls with the layers above and below it.

OSI Reference Model

- The **Open System Interconnection (OSI) Reference Model** is a description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative. It divides network architecture into seven layers which are, from top to bottom, the ***Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers***. It is therefore often referred to as the **OSI Seven Layer Model**.
- A **layer** is a collection of similar functions that provide services to the layer above it and receives service from the layer below it.

Figure 3.4

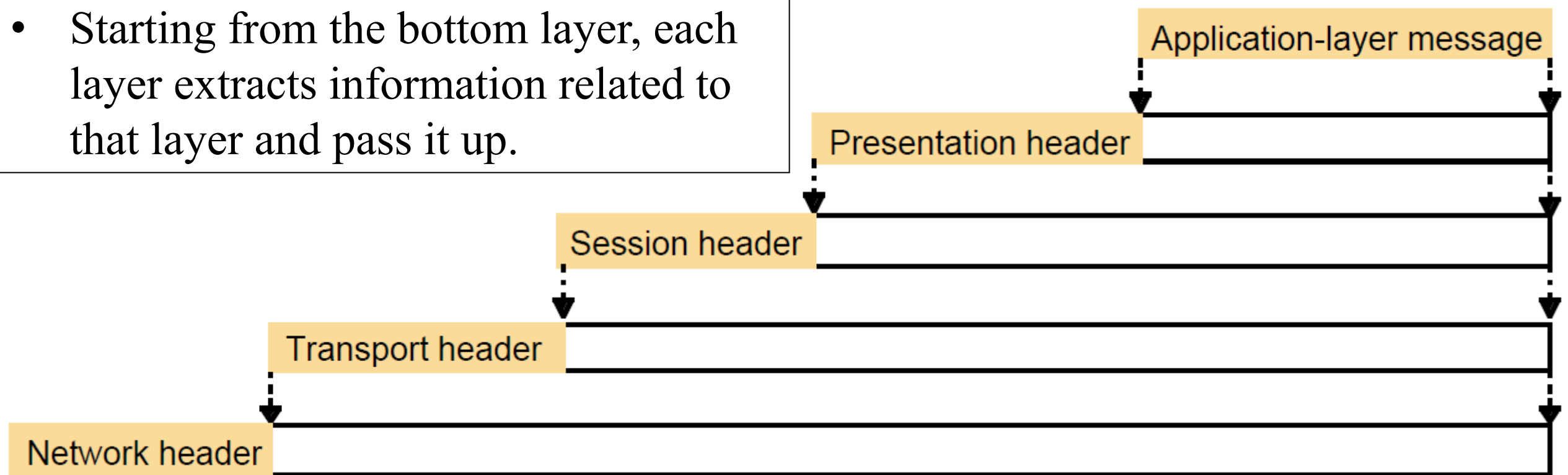
Protocol layers in the Open Systems Interconnection (OSI) model adapted by the International Organization for Standardization (ISO)



OSI Network Layers

Figure 3.3 Encapsulation as it is applied in layered protocols

- Starting from the top layer, each layer adds information related to that layer and pass it down.
- Starting from the bottom layer, each layer extracts information related to that layer and pass it up.



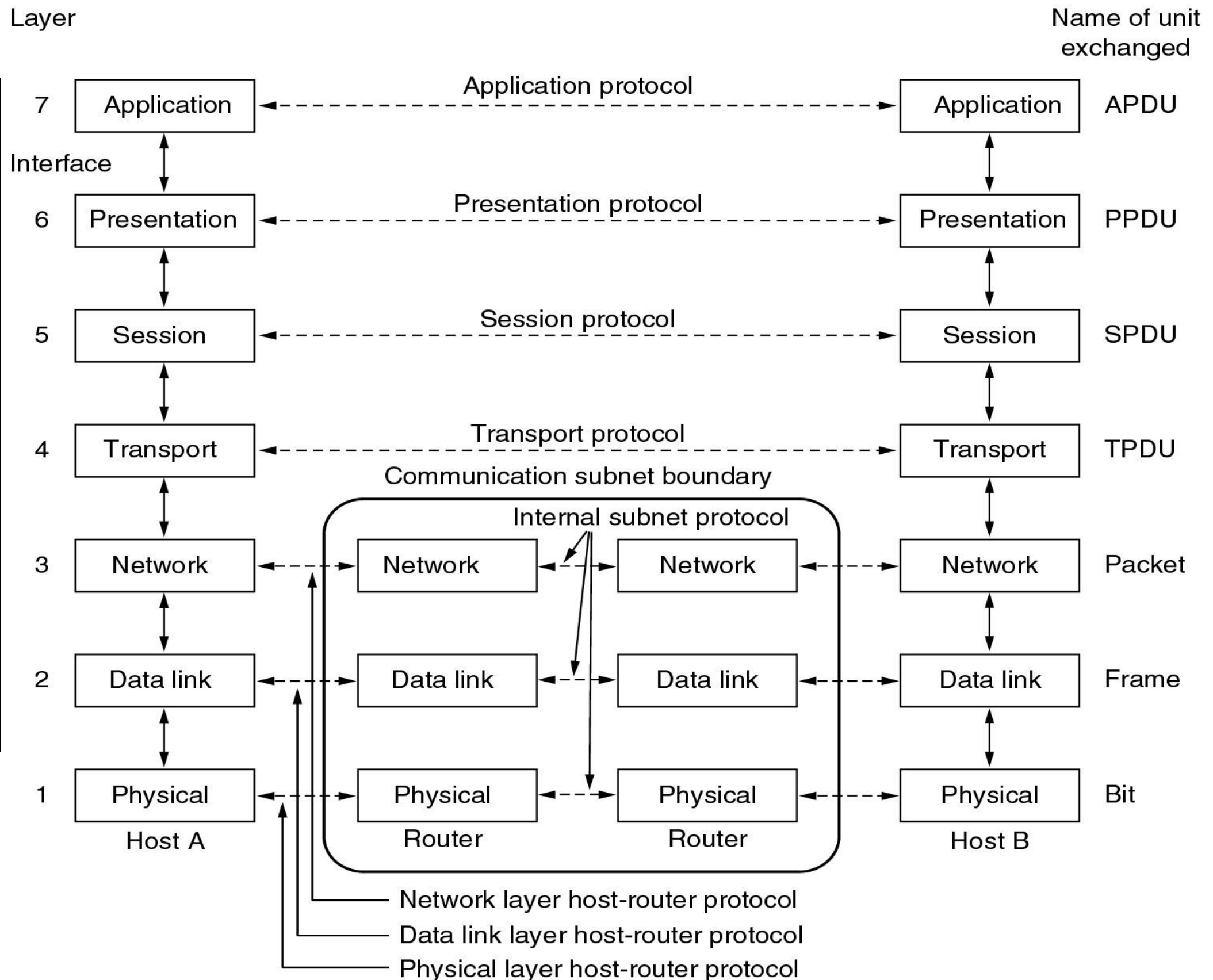
On the sending side, each layer (except the topmost, or application layer) accepts items of data in a specified format from the layer above it and applies transformations to encapsulate the data in the format specified for that layer before passing it to the layer below for further processing. **Figure 3.3** illustrates this process as it applies to the top four layers of the OSI protocol suite.

OSI Reference Model

Data unit	Layer	Function
Data	7. Application	Network process to application
	6. Presentation	Data representation and encryption
	5. Session	Host-to-host communication
Segment	4. Transport	End-to-end connections and reliability
Packet	3. Network	Path determination and logical addressing
Frame	2. Data Link	Physical addressing
Bit	1. Physical	Media, signal, and binary transmission

OSI Reference Model

- **PDU: Protocol Data Unit.**
- A protocol is used to communicate between similar layers at different hosts.
- An interface is used to communicate between different layers at the same host.



Layer 7: Application Layer

It is a service layer that provides the following functions (services):

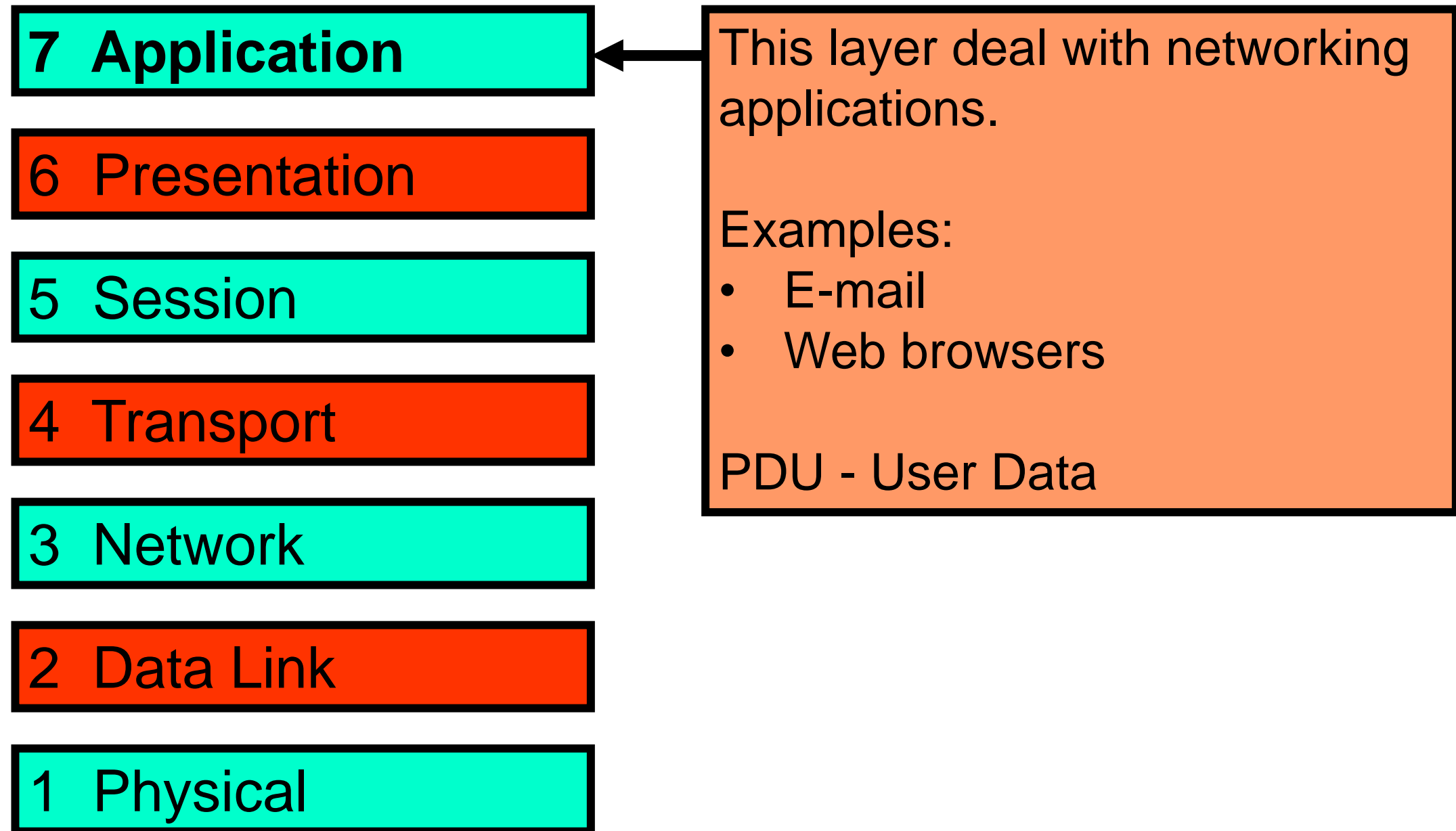
Main Function:

- Allows applications to use the network.
- Interface between the user & the computer (Applications & Gateways).
- Provides services that directly support user applications, such as the USER INTERFACE, E-MAIL, FILE TRANSFER, TERMINAL EMULATION, DATABASE ACCESS.

Other Functions:

- Message authentication for either the sent message or received message.
- Makes sure that necessary communication resources exist.
- Determines protocol and data syntax rules at the application level.
- Handles network access, flow control, and error recovery.

Layer 7: Application Layer



Layer 6: Presentation Layer

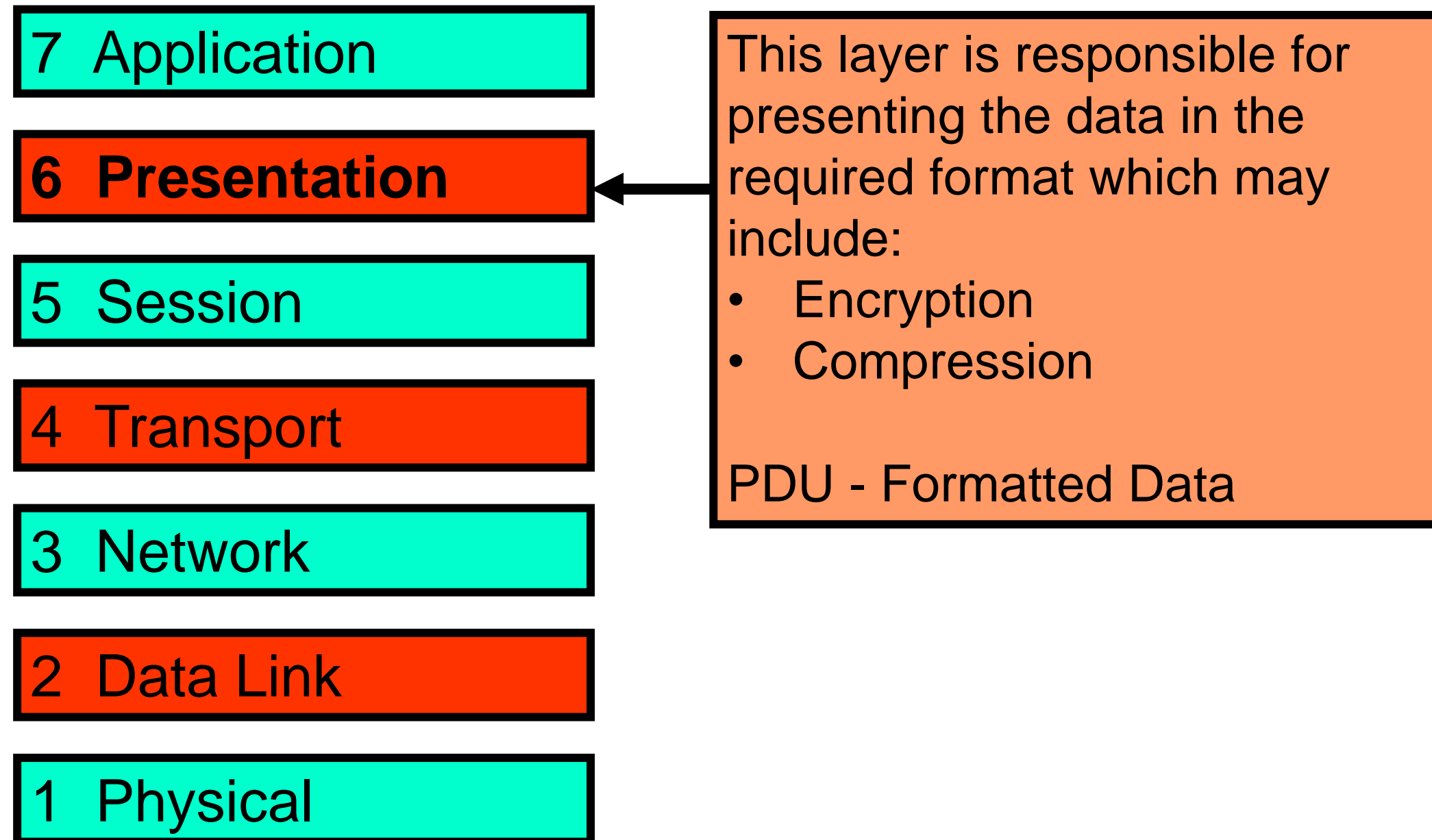
The **Presentation layer** enables translation between Application layer entities, in which higher-layer entities can use different syntax and semantics, as long as, the Presentation Service understands both and the mapping between them.

- In other words, many applications entities (instances of programs and software) can be hosted on different nodes, and they require using the network to send data to each other. Since they are considered applications, then they deal with the application layer.
- Notice that an application is usually designed differently than other applications in terms of data format or protocols used. Therefore, the application layer works as an intermediate step that unifies the way these applications interact with the network via having a clear mapping between applications in application layer and the layer underneath it (Presentation Layer).

Layer 6: Presentation Layer

- This layer formats and encrypts data to be sent across a network.
- The presentation service data units are then encapsulated into Session Protocol Data Units and moved to the lower layer.
- Translation of data into understandable format for transmission (into a form usable by the application layer, that is translates data between the formats the network requires, and the computer expects).
- Handles character encoding, bit order and byte order issues, and encodes and decodes data.
- Data compression and encryption takes place at this layer.
- Generally, determines the structure of data.

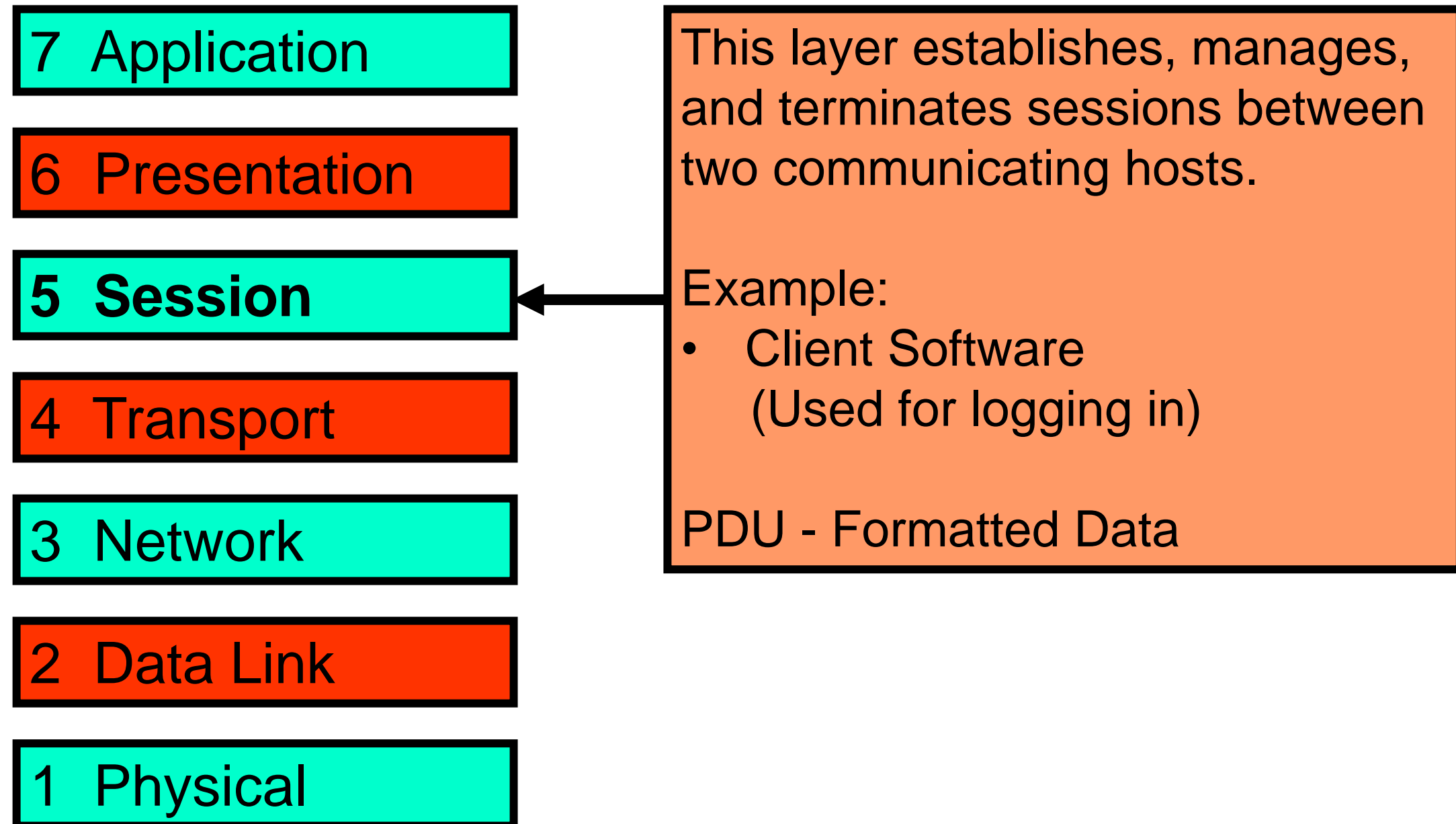
Layer 6: Presentation Layer



Layer 5: Session Layer

- The **Session layer** controls the dialogues (connections) between computers.
- It establishes, manages, and terminates the connections between the local and remote application.
- It provides full-duplex, half-duplex, or simplex operation.
 - **Simplex**: One direction only from fixed source “A” to fixed destination “B”.
 - **Half-duplex**: Bidirectional, one operation at a time. “A” can send and “B” receive or the other way around.
 - **Full-duplex**: Bidirectional, that is, two operations can happen simultaneously.
So, “A” sends and “B” receives and at the same time “B” sends and “A” receives.
- Provides synchronization between communicating computers (nodes), messages are sent between layers (i.e., Manages upper layer errors).
- Places checkpoints in the data flow, so that if transmission fails, only the data after the last checkpoint needs to be retransmitted.

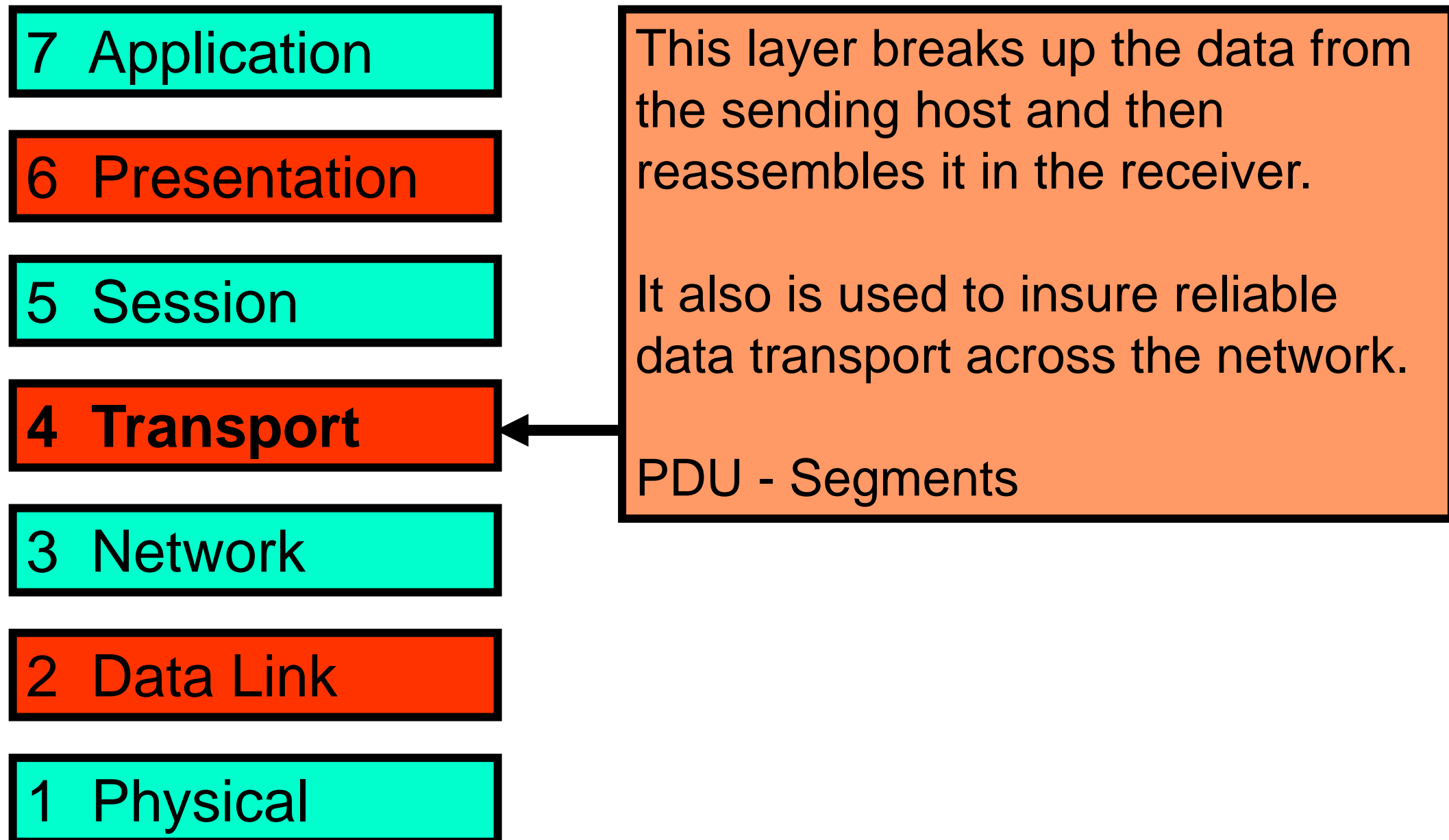
Layer 5: Session Layer



Layer 4: Transport Layer

- The **Transport Layer** provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.
- Responsible for PACKET HANDLING. Ensures error free delivery. Repackages messages, divides messages into smaller packets (fragments and reassembles data), and handles error handling.
- Ensures proper sequencing and without loss and duplication.
- Takes action to correct faulty transmissions.
- Controls flow of data.
- Acknowledges successful receipt of data.
- **TCP (Transmission Control Protocol):** Connection oriented communication for applications to ensure error free delivery.
- **UDP (User Datagram Protocol):** Connectionless communications and does not guarantee packet delivery between transfer points.

Layer 4: Transport Layer



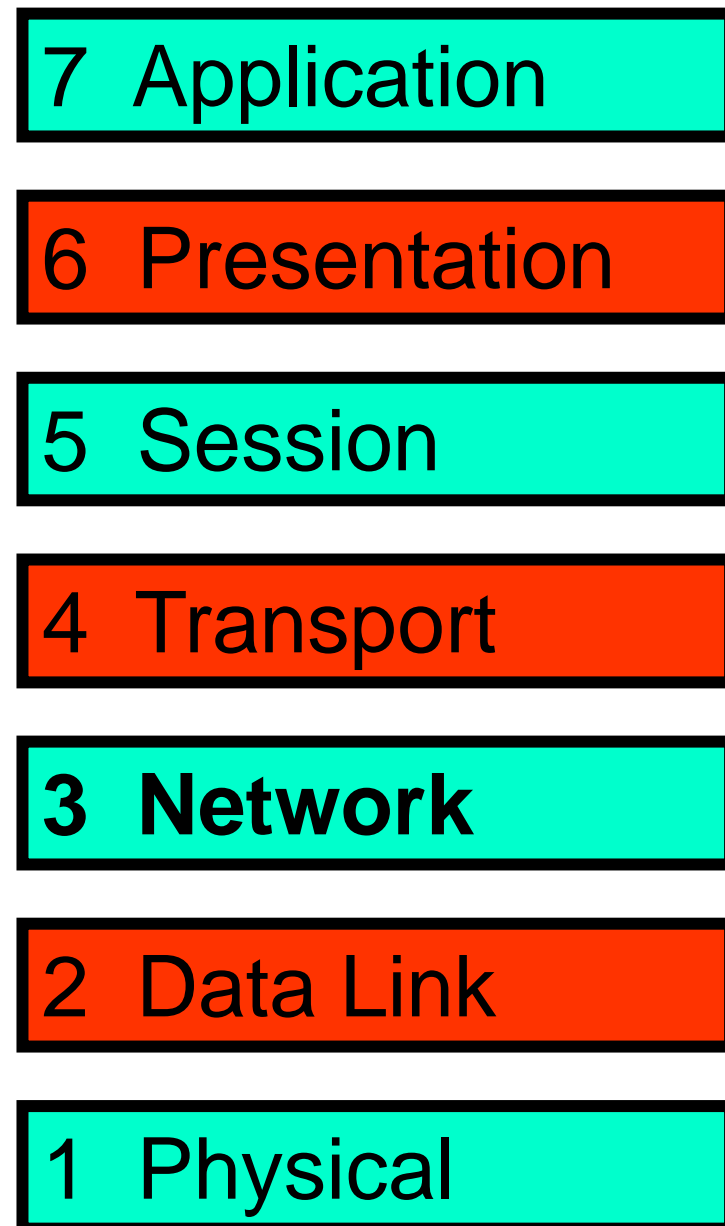
Layer 3: Network Layer

- The **Network Layer** provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks. The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.
- A well-known example of the network layer protocol is Internet Protocol (IP).
- Logical addressing: software addresses to hardware addresses are resolved (**ARP/RARP**).
- Determining the best route (Makes routing decisions & forwards packets).

ARP (Address Resolution Protocol): Mapping a logical IP address to physical MAC (Media Access Control) address.

RARP (Reverse Address Resolution Protocol): Mapping physical MAC address to logical IP address.

Layer 3: Network Layer



Sometimes referred to as the
“Cisco Layer”.

Makes “Best Path Determination”
decisions based on logical
addresses (usually IP addresses).

PDU - Packets

Layer 2: Data Link Layer

- The **Data Link Layer** provides the functional and procedural means to transfer data between network entities and to detect and correct errors that may occur in the Physical Layer.
- **Data link layer** arrange bits, from the Physical Layer, into logical sequences called frames.

Layer 2: Data Link Layer

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

This layer provides reliable transmit of data across a physical link.

Makes decisions based on physical addresses (usually MAC addresses).

PDU - Frames

Layer 1: Physical Layer

- The **Physical Layer** defines the electrical and physical specifications for devices. This includes the layout of pins, voltages, cable specifications, Hubs, repeaters, network adapters, etc.
- The Physical Layer will tell one device how to transmit to the communication medium, and another device how to receive from it.
- The **major functions and services** of the Physical Layer are:
 - Establishment and termination of a connection to a communication medium.
 - Flow control.
 - Modulation (conversion between the representation of digital data) (Analog signals to digital data (0 & 1) and vice versa). These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Layer 1: Physical Layer

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

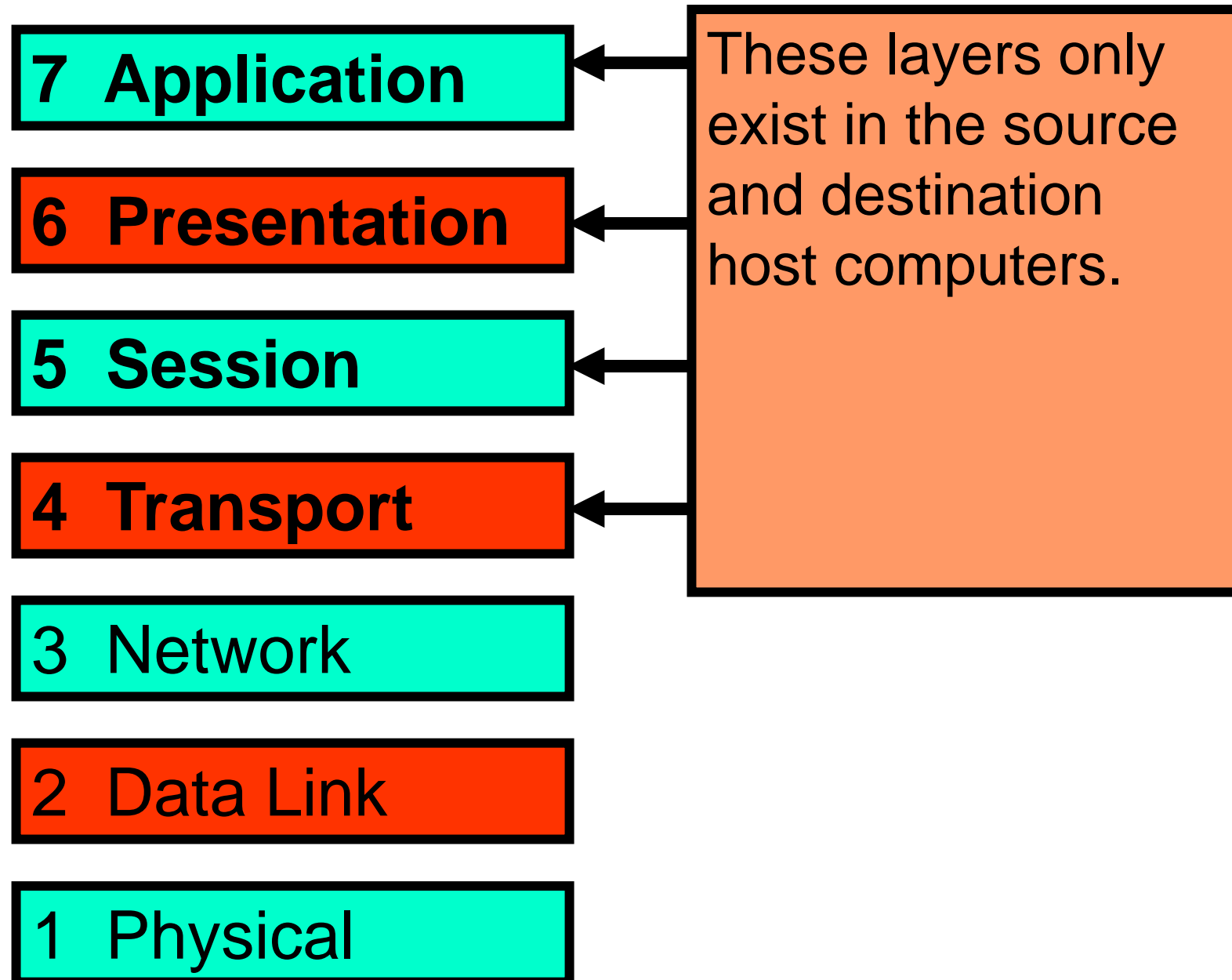
This is the physical media through which the data, represented as electronic signals, is sent from the source host to the destination host.

Examples:

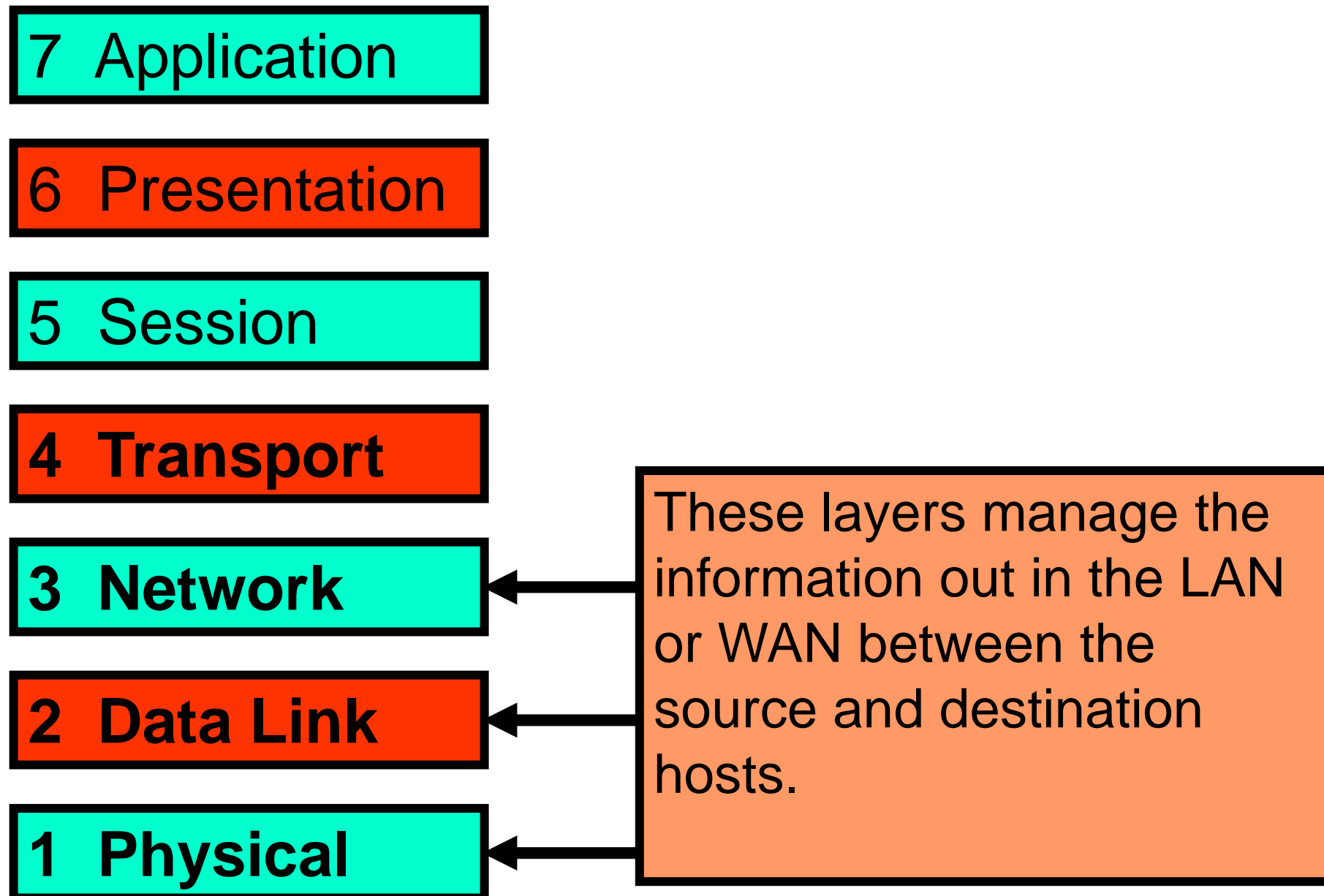
- CAT5 (what we have)
- Coaxial (like cable TV)
- Fiber optic

PDU - Bits

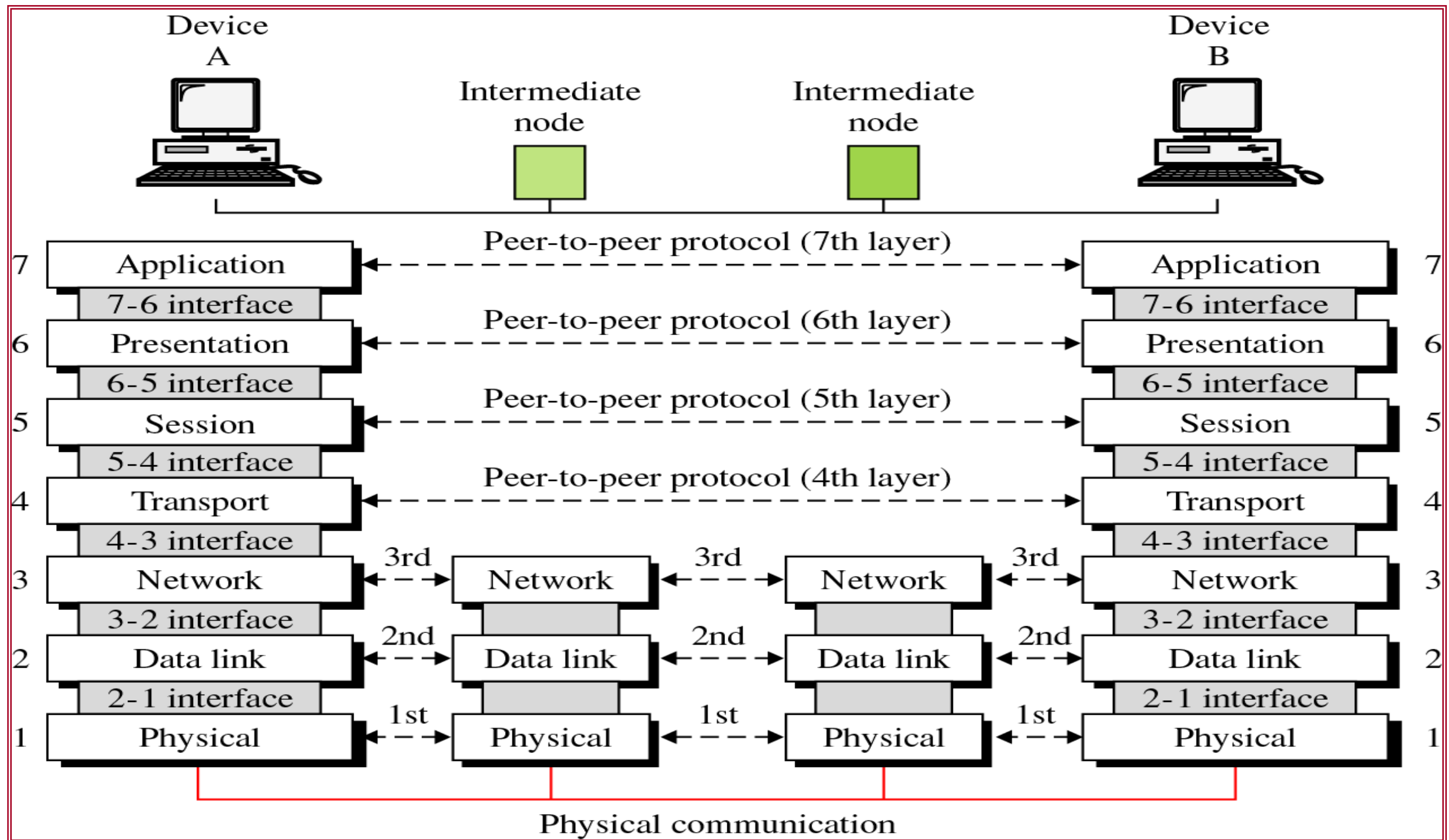
Host Layers



Media Layers



OSI Layers Communications




TCP/IP Reference Model: Why Another Model?

Although the OSI reference model is universally recognized, the historical and technical open standard of the Internet is Transmission Control Protocol / Internet Protocol (TCP/IP).

The TCP/IP reference model and the TCP/IP protocol stack make data communication possible between any two computers, anywhere in the world, at nearly the speed of light.

The U.S. Department of Defense (DoD) created the TCP/IP reference model because it wanted a network that could survive any conditions, even a nuclear war.



They created the first Internet: Advanced Research Projects Agency Network (ARPANET)

Don't be confused between the models

OSI Model

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

TCP/IP Model

Application

Transport

Internet

Network Access

Network Access Layer

Application

Transport

Internet

Network
Access

The **network access layer** is also called the **host-to-network** layer. It is the layer that is concerned with all of the issues that an IP packet requires to actually make a physical link to the network media. It includes LAN and WAN details, and all the details contained in the OSI physical and data-link layers. NOTE: ARP & RARP work at both the Internet and Network Access Layers.

- Ethernet
- Fast Ethernet
- SLIP & PPP
- FDDI
- ATM, Frame Relay & SMDS
- ARP
- Proxy ARP
- RARP

Network Access Layer: General Definitions

Ethernet: A network for connecting devices within a LAN by cables such as coaxial cables.

SLIP (Serial Line Internet Protocol): A communication protocol for devices directly connected to each other.

PPP (Point-to-Point Protocol): A newer version of SLIP.

FDDI (Fiber Distributed Data Interface): A protocol for data transmission over fiber optics lines in a LAN.

ATM (Asynchronous Transfer Mode): A network for sending audio and video data.

Frame Relay: A cost effective network that enables devices to virtually be connected in a point-to-point pattern.

SMDS (Switched Multimegabit Data Service): A service that allows organization to exchange large amount of data over telephone network.

ARP (Address Resolution Protocol): Mapping a logical IP address to physical MAC address.

Proxy ARP: Same as ARP but, the sender and receiver are separated by a router.

RARP (Reverse Address Resolution Protocol): Mapping physical MAC address to logical IP address.

Internet Layer



The purpose of the **Internet layer** is to select the best path through the network for packets to travel. The main protocol that functions at this layer is the Internet Protocol (IP). Best path determination and packet switching occur at this layer.

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

Address Resolution Protocol (ARP)

Reverse Address Resolution Protocol (RARP)

ICMP: A protocol to handle error and control messages

TCP/IP Reference Model: Internet Layer

- The ability to connect multiple networks in a seamless way known as the **TCP/IP Reference Model**, the name came from its two primary protocols (TCP and IP protocols).
- The **internet layer** is a connectionless internetwork layer. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.
- The **internet layer** defines an official packet format and protocol called **IP (Internet Protocol)**. The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer. The following figure shows this correspondence.

OSI

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data link
1	Physical

TCP/IP

Application
Transport
Internet
Host-to-network

Not present
in the model

Application

Transport

Internet

Network
Access

Transport Layer

Transmission Control Protocol (TCP)

Connection-Oriented

User Datagram Protocol (UDP)

Connectionless

The **transport layer** provides transport services from the source host to the destination host.

Transport Layer

The layer above the internet layer in the TCP/IP model is called the **transport layer**. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here:

- 1) TCP (Transmission Control Protocol)
- 2) UDP (User Datagram Protocol)

Application Layer

- The TCP/IP model does not have session or presentation layers. On top of the transport layer is the **application layer**. It contains all the **higher-level protocols**. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).
- ✓ The **virtual terminal protocol** allows a user on one machine to log onto a distant machine and work there.
- ✓ The **file transfer protocol** provides a way to move data efficiently from one machine to another.
- ✓ **Electronic mail** was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it.
- Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

Host-to-Network Layer

- **The Host-to-Network Layer (Network Access Layer):** The host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host-to-host and network-to-network.
- However, for comparison's sake between OSI model and TCP/IP model, we can say that Host-to-Host layer job is equivalent to the job performed by the Data Link layer and the Physical Layer.

Types of Connections

The protocols that use TCP include:

- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Telnet

1) Connection-Oriented

- One connection is established between client and server.
- Data flows in the communication channel in a continuous stream.
- Packets arrive in order.
- Low probability of packet loss.
- **TCP (Transmission Control Protocol)** is used for connection establishment and data transfer.
- In Java, this type of communication is programmed using “Sockets”.



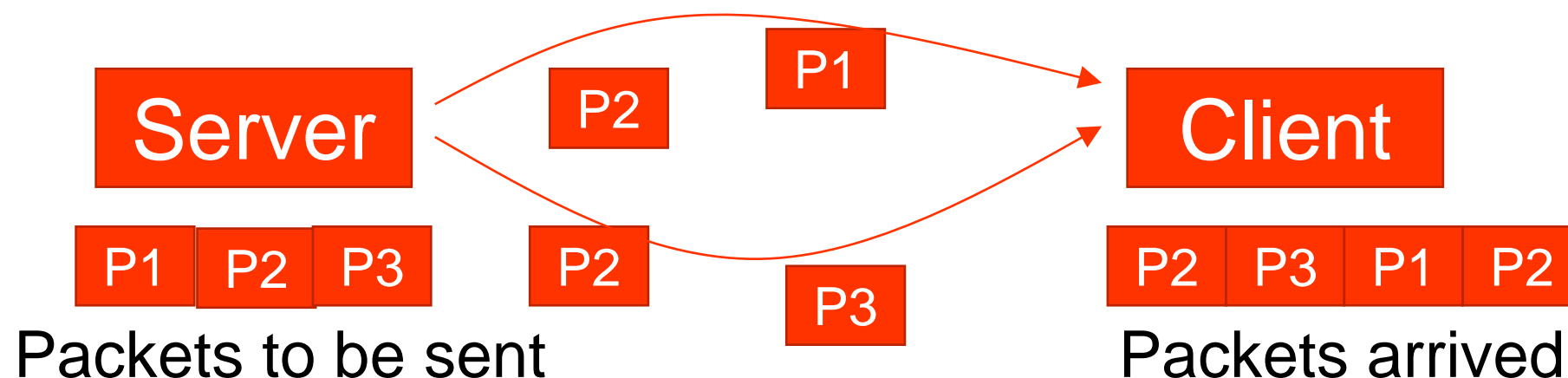
Types of Connections

2) Connectionless

The protocols that use UDP include:

- TFTP (Trivial File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- DHCP (Dynamic Host Control Protocol)
- DNS (Domain Name System)

- Packets can go through different communication channels.
- Packets are not guaranteed to arrive in order.
- Packets can be lost or duplicated.
- Protocol used is **UDP (User Datagram Protocol)**.
- In Java, such type of communication is programmed using “Datagrams”.
- This type of communication is used in applications where error checking and reliability of TCP is not needed.



- Order is not right.
- Duplication can happen if packets are resubmitted, and they arrive from multiple paths.

Connection-Oriented and Connectionless

- Connectionless applications are more efficient than Connection-oriented applications because connectionless applications do not generate the overhead of:
 - No data loss.
 - In order arrival guarantee.

Internet Protocols

TCP features:

- The **TCP layer** includes additional mechanisms (implemented over IP) to meet the reliability guarantees.
- These are sequencing, flow control, retransmission, buffering, and checksum.
- **Sequencing:**
 - A **TCP** sending process divides the stream into a sequence of data segments and transmits them as IP packets.
 - A **sequence number** is attached to each TCP segment.
 - The **receiver** uses the sequence numbers to order the received segments before placing them in the input stream at the receiving process.
 - No **segment** can be placed in the input stream until all lower-numbered segments have been received and placed in the stream, so segments that arrive out of order must be held in a buffer until their predecessors arrive.

Internet Protocols

➤ Flow control:

- Whenever a receiver successfully receives a segment, it records its sequence number.
- From time to time the receiver sends an **acknowledgement** to the sender, giving the sequence number of the highest-numbered segment in its input stream together with a window size.
- If there is a reverse flow of data, **acknowledgements** are carried in the normal data segments; otherwise, they travel in acknowledgement segments.
- The **window size field** in the acknowledgement segment specifies the quantity of data that the sender is permitted to send before the next acknowledgement.

➤ Retransmission:

- The sender records the sequence numbers of the segments that it sends.
- When it receives an acknowledgement, it notes that the segments were successfully received, and it may then delete them from its outgoing buffers.
- If any segment is not acknowledged within a specified timeout, the sender retransmits it.

Internet Protocols

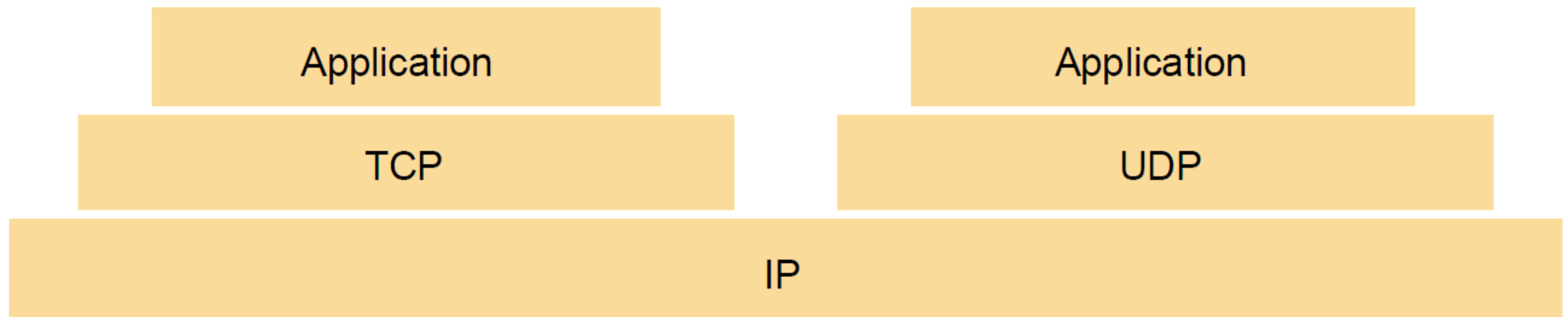
➤ Buffering:

- The incoming buffer at the receiver is used to balance the flow between the sender and the receiver.
- If the receiving process issues receive operations more slowly than the sender issues send operations, the quantity of data in the buffer will grow.
- It is extracted from the buffer before it becomes full, but ultimately the buffer may overflow, and when that happens incoming segments are simply dropped without recording their arrival.
- Their arrival is therefore not acknowledged, and the sender is obliged to retransmit them.

➤ Checksum:

- Each segment carries a **checksum** covering the header and the data in the segment.
- If a received segment does not match its checksum, the segment is dropped.

Figure 3.14 The programmer's conceptual view of a TCP/IP Internet

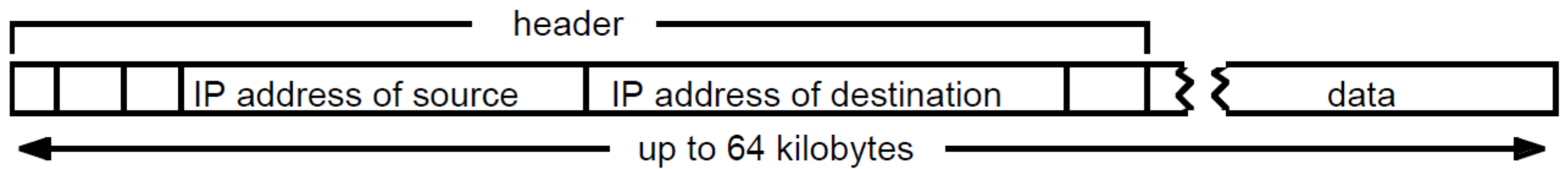


Internet Protocols

IP Protocol:

- The **IP protocol** transmits datagrams from one host to another via intermediate routers.
- The full IP packet format is complex, but **Figure 3.17** shows the main components.
- There are several header fields, not shown in the diagram, that are used by the transmission and routing algorithms.

Figure 3.17 IP packet layout



Port Number

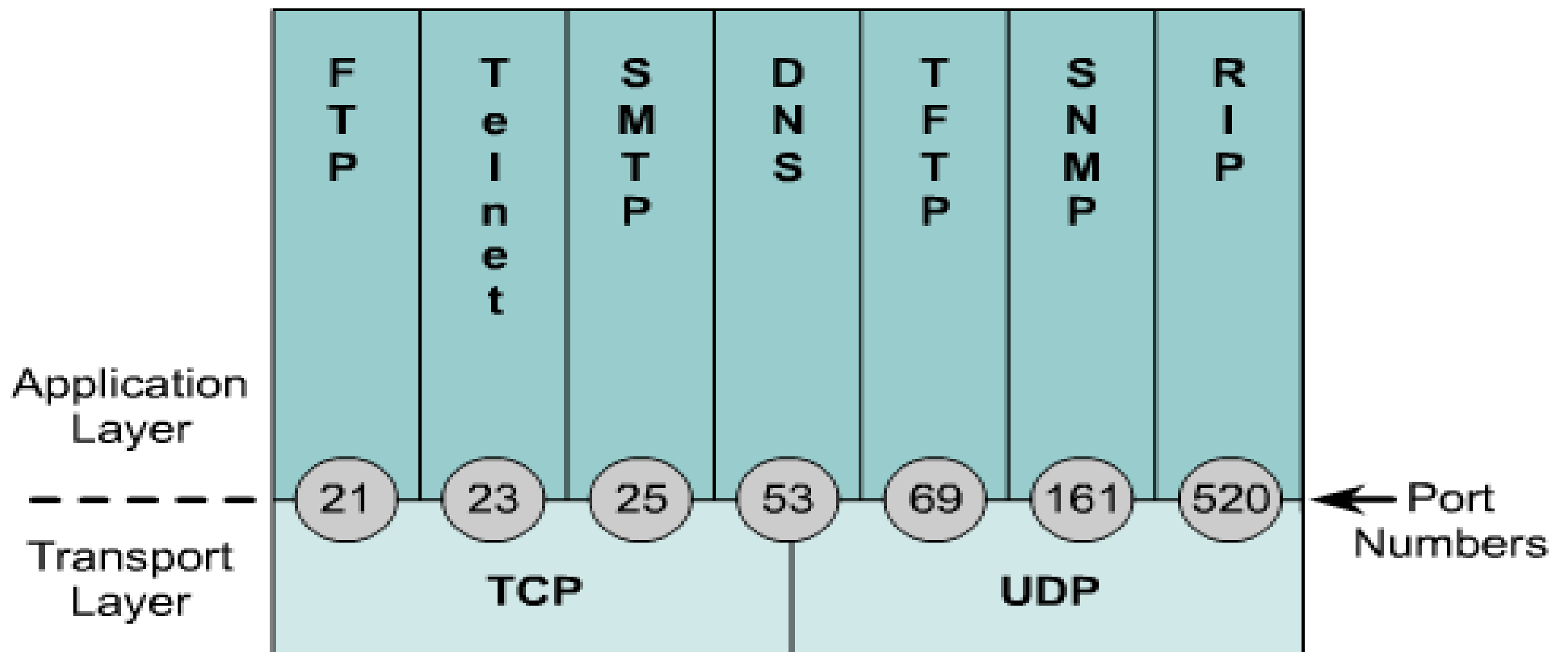
- **Port numbers** are used for addressing messages to processes within a particular computer and are valid only within that computer.
- A **port number** is a 16-bit integer.
- Once an **IP packet** has been delivered to the destination host, the TCP- or UDP-layer software dispatches it to a process via a specific port at that host.

Well Known Port Numbers

The following port numbers should be memorized:

NOTE:

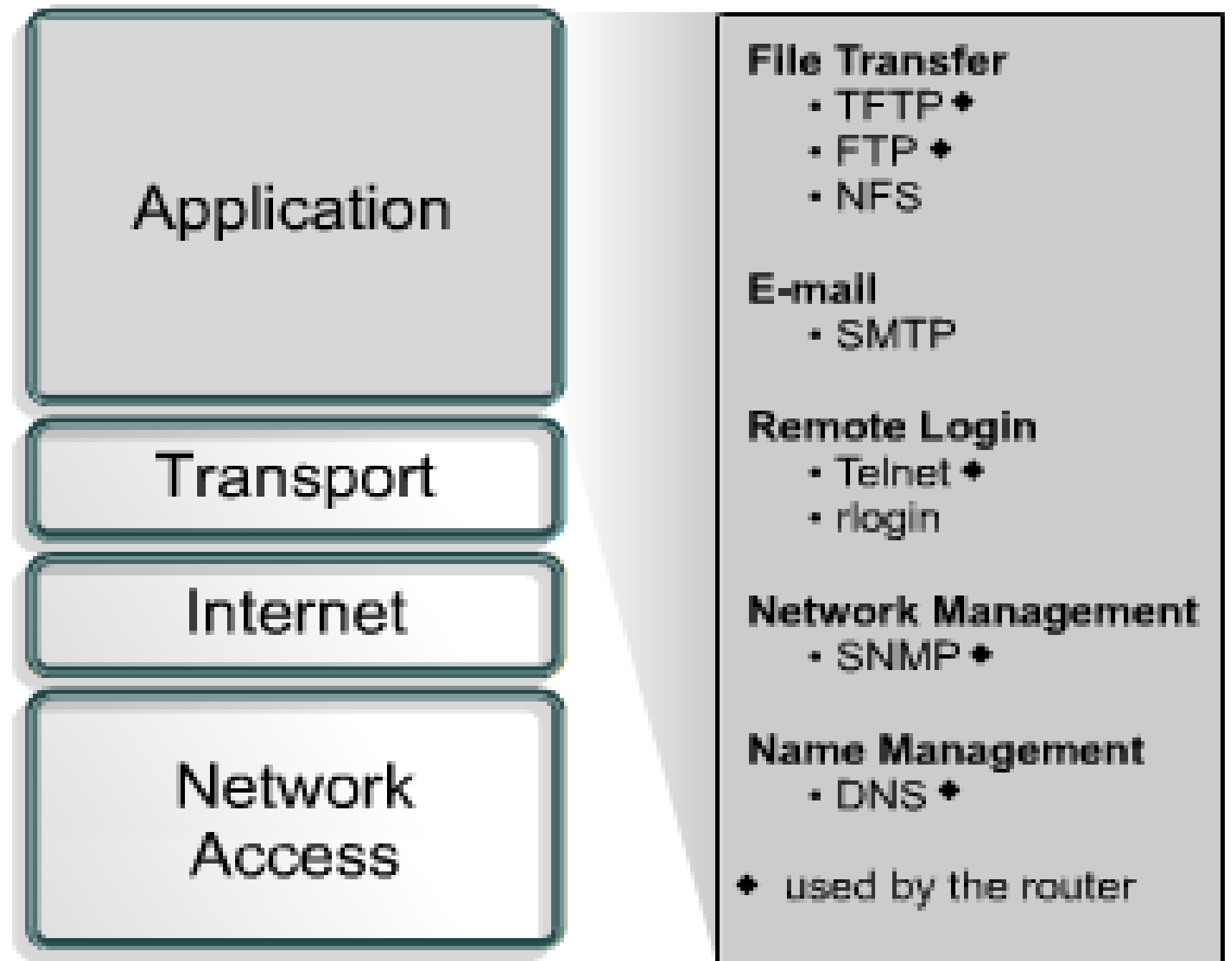
- The curriculum forgot to mention one of the most important port numbers.
- **Port 80** is used for **HTTP** or **WWW** protocols (Essentially access to the internet).



RIP (Routing Information Protocol): A protocol for exchanging network topology in terms of number of hops to find best path from sender to receiver.

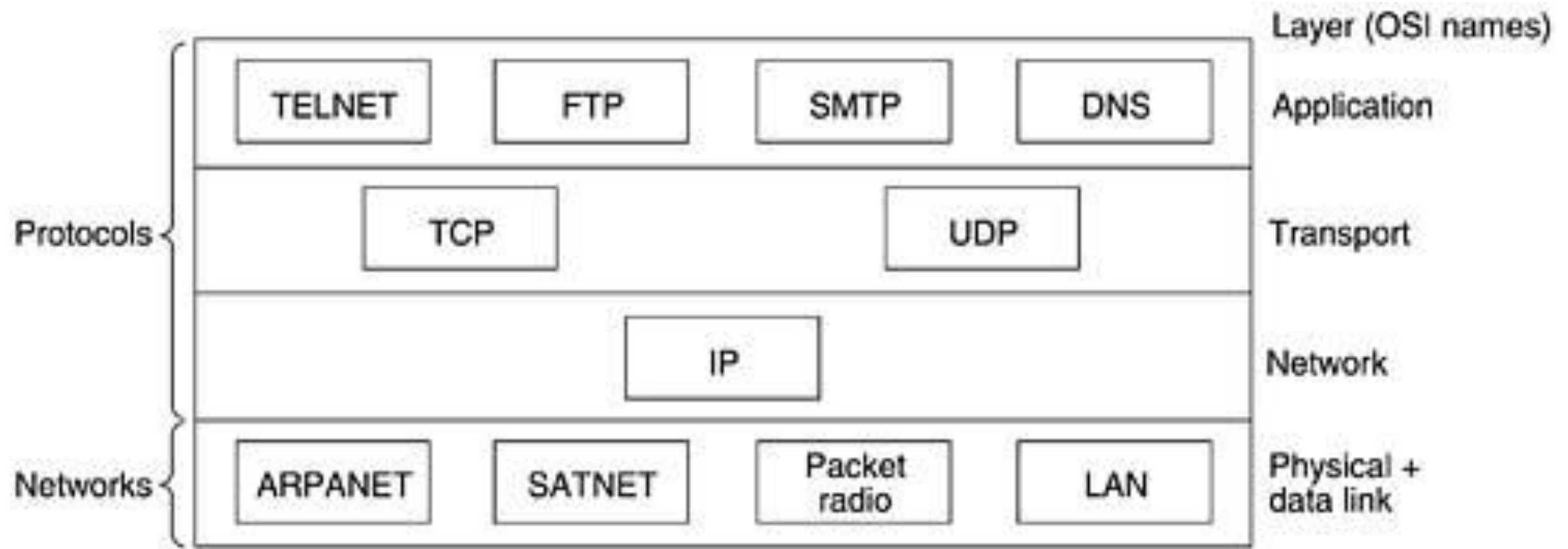
Application Layer

The **application layer** of the TCP/IP model handles high-level protocols, issues of representation, encoding, and dialog control.



NFS (Network File System): A protocol that allows a host to remotely deals with File systems and drives on a remote machine.

Protocols and Networks in the TCP/IP Model



SATNET(Atlantic Packet Satellite Network):

A network that used satellites to connect areas of USA to areas in Europe.

Networks Principles

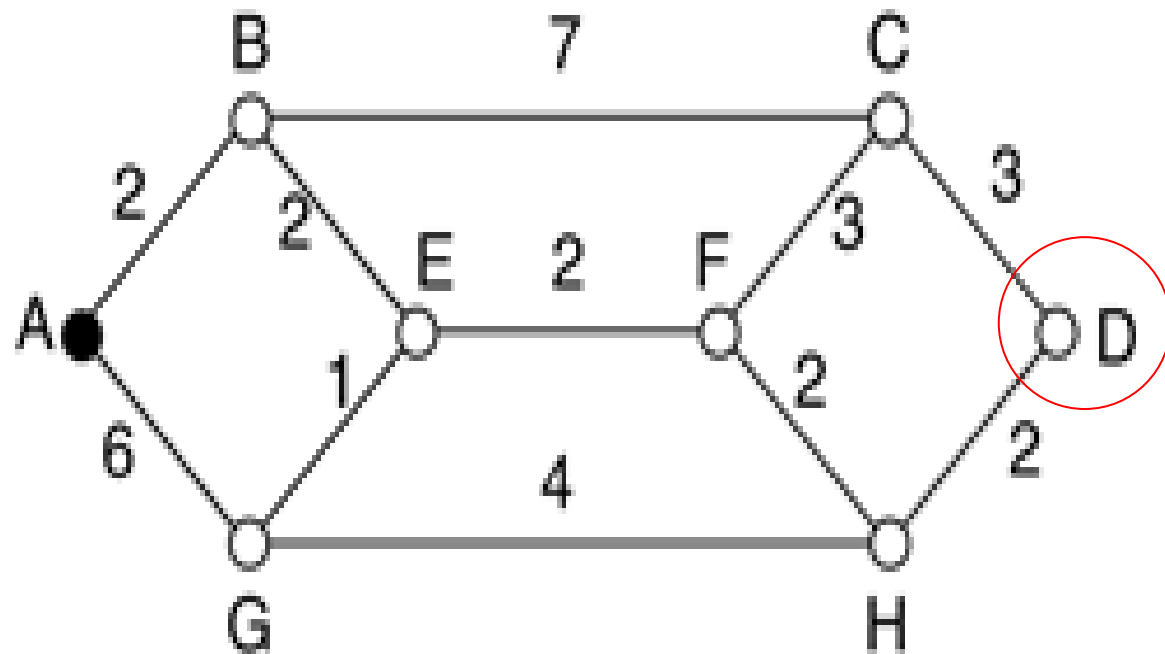
Routing:

- Routing is a function that is required in all networks except those LANs, such as Ethernets, that provide direct connections between all pairs of attached hosts.
- In large networks, adaptive routing is employed: the best route for communication between two points in the network is re-evaluated periodically, taking into account the current traffic in the network and any faults such as broken connections or routers.
- The determination of routes for the transmission of packets to their destinations is the responsibility of a routing algorithm implemented by a program in the network layer (OSI Model) or internet layer (TCP/IP Model) at each node.

How to use a Routing Table

Example:

- Each host has a routing table.
- Shortest distance starting from “A” to all other vertices.



Routing table at host “A”

Vertex	Shortest Distance from A	Through Vertex
A	0	
B	2	A
C	9	B
D	10	H
E	4	B
F	6	E
G	5	E
H	8	F

Traverse the table to know the shortest path from A to D:

A **D** H
A **H** F
A **F** E
A **E** B
A **B** A

So: Path is **B E F H D** Length is 10

Figure 3.7 Routing in a wide area network

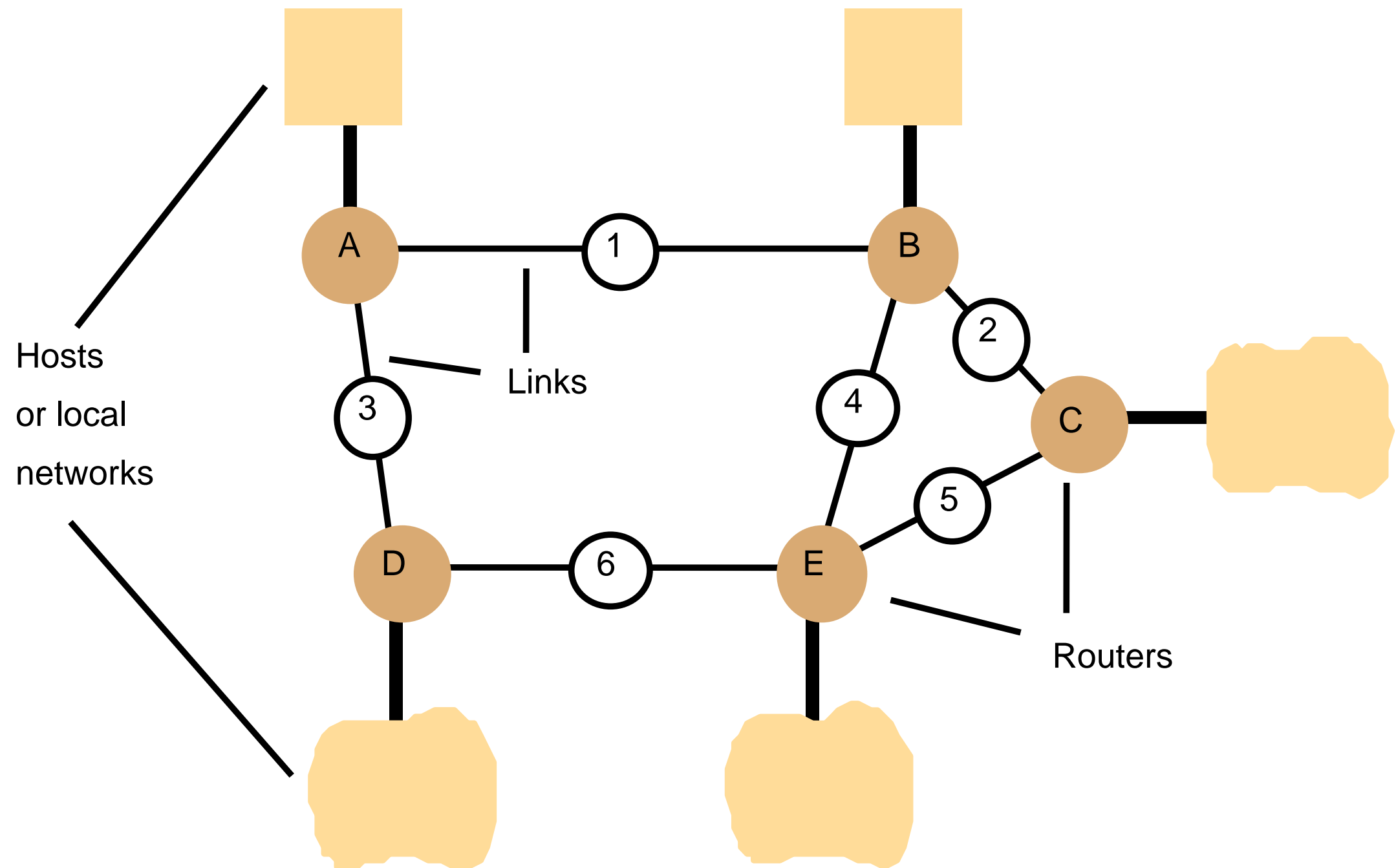


Figure 3.8 Routing tables for the network in Figure 3.7

Another type of routing tables

Cost is number of hops to destination

Routings from A

<i>To</i>	<i>Link</i>	<i>Cost</i>
A	local	0
B	1	1
C	1	2
D	3	1
E	1	2

Routings from B

<i>To</i>	<i>Link</i>	<i>Cost</i>
A	1	1
B	local	0
C	2	1
D	1	2
E	4	1

Routings from C

<i>To</i>	<i>Link</i>	<i>Cost</i>
A	2	2
B	2	1
C	local	0
D	5	2
E	5	1

Routings from D

<i>To</i>	<i>Link</i>	<i>Cost</i>
A	3	1
B	3	2
C	6	2
D	local	0
E	6	1

Routings from E

<i>To</i>	<i>Link</i>	<i>Cost</i>
A	4	2
B	4	1
C	5	1
D	6	1
E	local	0

Route a packet from host “A” to host “C”:

- 1) From “A” to “C” via link “1” with total cost “2”
- 2) This leads us to host “B”
- 3) From “B” to “C” via link “2”

So, path is A→B→C, and total cost is 2

Networks Principles

Congestion control:

- The **capacity** of a network is limited by the performance of its communication links and switching nodes.
- When the load at any link or node approaches its capacity, queues will build up at hosts trying to send packets and at intermediate nodes holding packets whose onward transmission is blocked by other traffic.
- If the load continues at the same high level, the queues will continue to grow until they reach the limit of available buffer space.
- Once this state is reached at a node, the node has no option but to drop further incoming packets.
- When the load on a network exceeds 80% of its capacity, the total throughput tends to drop as a result of packet losses unless usage of heavily loaded links is controlled.

Networks Principles

Congestion control:

- Instead of allowing packets to travel through the network until they reach over-congested nodes, where they will have to be dropped, it would be better to hold them at earlier nodes until the congestion is reduced.
- This will result in increased delays for packets but will not degrade the total throughput of the network. This technique is called **congestion control**.
- **Congestion control** is achieved by informing nodes along a route that congestion has occurred and that their rate of packet transmission should therefore be reduced.
- For **intermediate nodes**, this will result in the buffering of incoming packets for a longer period.
- For **hosts** that are sources of the packets, the result may be to queue packets before transmission or to block the application process that is generating them until the network can handle them.

Networks Principles

Internetworking:

- There are many **network technologies** with different network-, link- and physical-layer protocols.
- **Local networks** are built with Ethernet technologies.
- **Wide area networks** are built over analogue and digital telephone networks of various types, satellite links and wide area Asynchronous Transfer Mode (ATM) networks.
- **Individual computers** and **local networks** are linked to the Internet or intranets by modems and by wireless and Digital Subscriber Line (DSL) connections.
- So, **Internetworking** is the process of connecting different types of networks together in a way that facilitates communication between hosts even the hosts belong to different networks.

Networks Principles

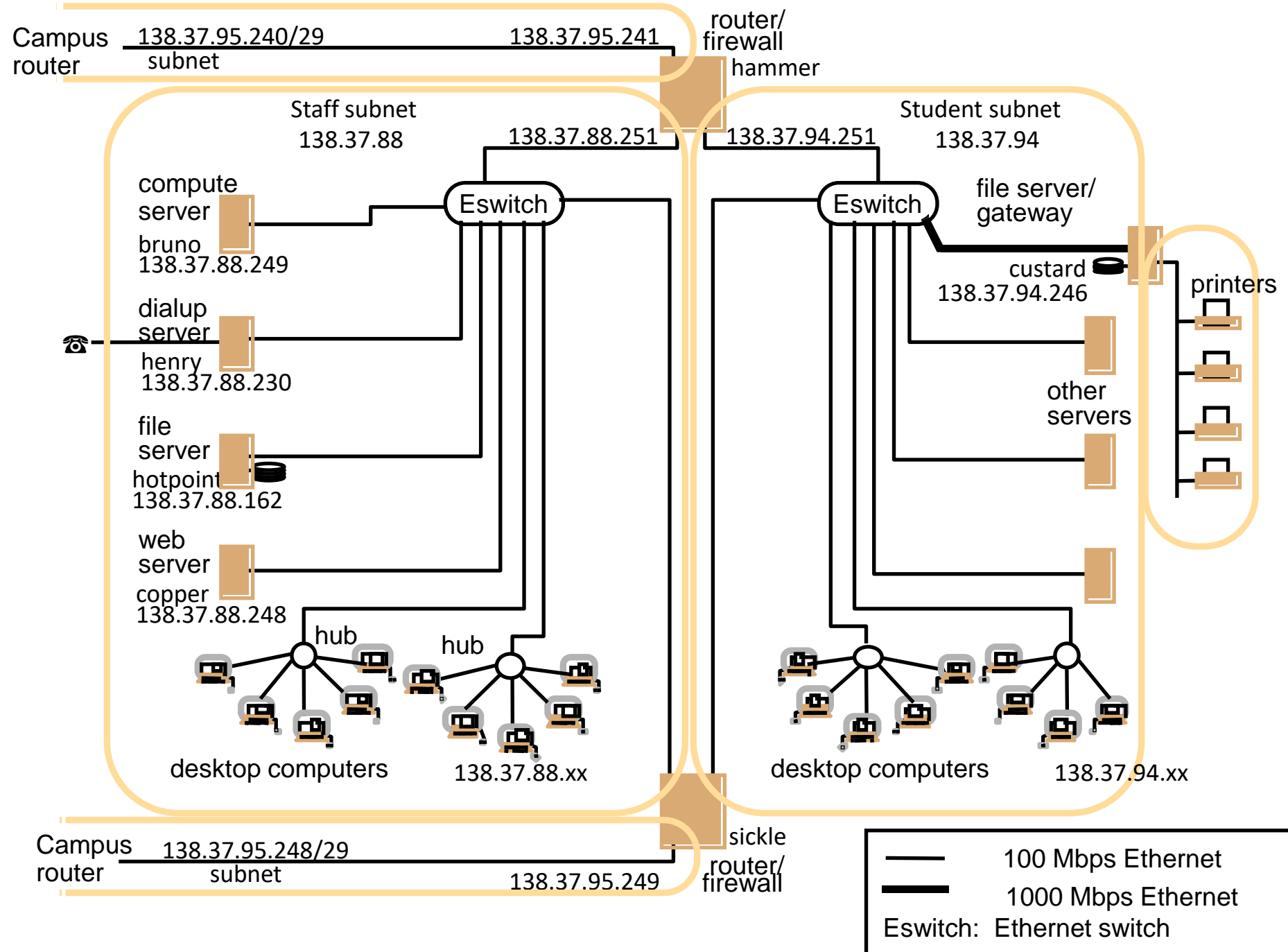
Internetworking:

- To build an **integrated network (internetwork)** we must integrate many subnets, each of which is based on one of the mentioned network technologies. Thus, the following are needed:
 1. A unified internetwork addressing scheme that enables packets to be addressed to any host connected to any subnet (**How IP addresses are formed**).
 2. A protocol defining the format of internetwork packets and giving rules according to which, they are handled.
 3. Interconnecting components that route packets to their destinations in terms of internetwork addresses, transmitting the packets using subnets with a variety of network technologies.
- **Figure 3.10** shows a small part of the campus intranet at a British university, where there are five subnets.

Figure 3.10 Simplified view of part of a university campus network

IP addresses in a way that forms different networks (Subnetting).

Devices needed to forward messages such as hubs, switches, and routers.



Forwarding and Routing Devices

1) Hub

- It is a repeater. That is, it repeats messages coming through it.
- It operates on the physical layer.
- If a hub receives a message, it simply forwards the message to all devices connected to the hub (Not Smart).
- Usually used to directly connect devices in one given network.

Forwarding and Routing Devices

2) Switch

- It operates on the Data Link layer.
- It relies on MAC addresses for routing messages.
 - **How does it work?**
 - * First, a switch works as a hub. So, it forwards a message to all other devices connected to it.
 - * But the switch starts learning about the devices connected to it.
 - **For example:**
 - * Host “A” sends a message to host “B” via a switch.
 - * The switch does not know anything about “A” and “B” yet.
 - * So, the switch sends the message to all devices connected to it including “B”.
 - * Now, the switch knows the path to reach “A”.
 - * So, the next time a message is sent to “A”, the switch will forward the message only to “A” via the right path (No need to send it to all devices).
 - * Usually used to connect devices in one given network.

Forwarding and Routing Devices

3) Router

- The smartest of them.
- Operates on the Network Layer Level (OSI Model).
- It relies on IP addresses for routing.
- It performs more complicated work such as keeping routing tables and error control.
- Most likely used to connect distinct networks together.

Internet Protocols

Unregistered Addresses and Network Address Translation (NAT):

- Not all of the computers and devices that access the Internet need to be assigned globally unique IP addresses.
- Computers that are attached to a local network and access to the Internet through a NAT-enabled router can rely upon the router to redirect incoming UDP and TCP packets for them.
- **Figure 3.18** illustrates a typical home network with computers and other network devices linked to the Internet through a NAT-enabled router.
- The network includes Internet-enabled computers that are connected to the router by a wired **Ethernet** connection as well as others that are connected through a **WiFi** access point.
- Some **Bluetooth-enabled** devices are shown, but these are not connected to the router and hence cannot access the Internet directly.
- The home network has been allocated a single registered IP address (83.215.152.95) by its **Internet Service Provider (ISP)**.
- The approach described here is suitable for any organization wishing to connect computers without registered IP addresses to the Internet.

Figure 3.18 A typical NAT-based home network

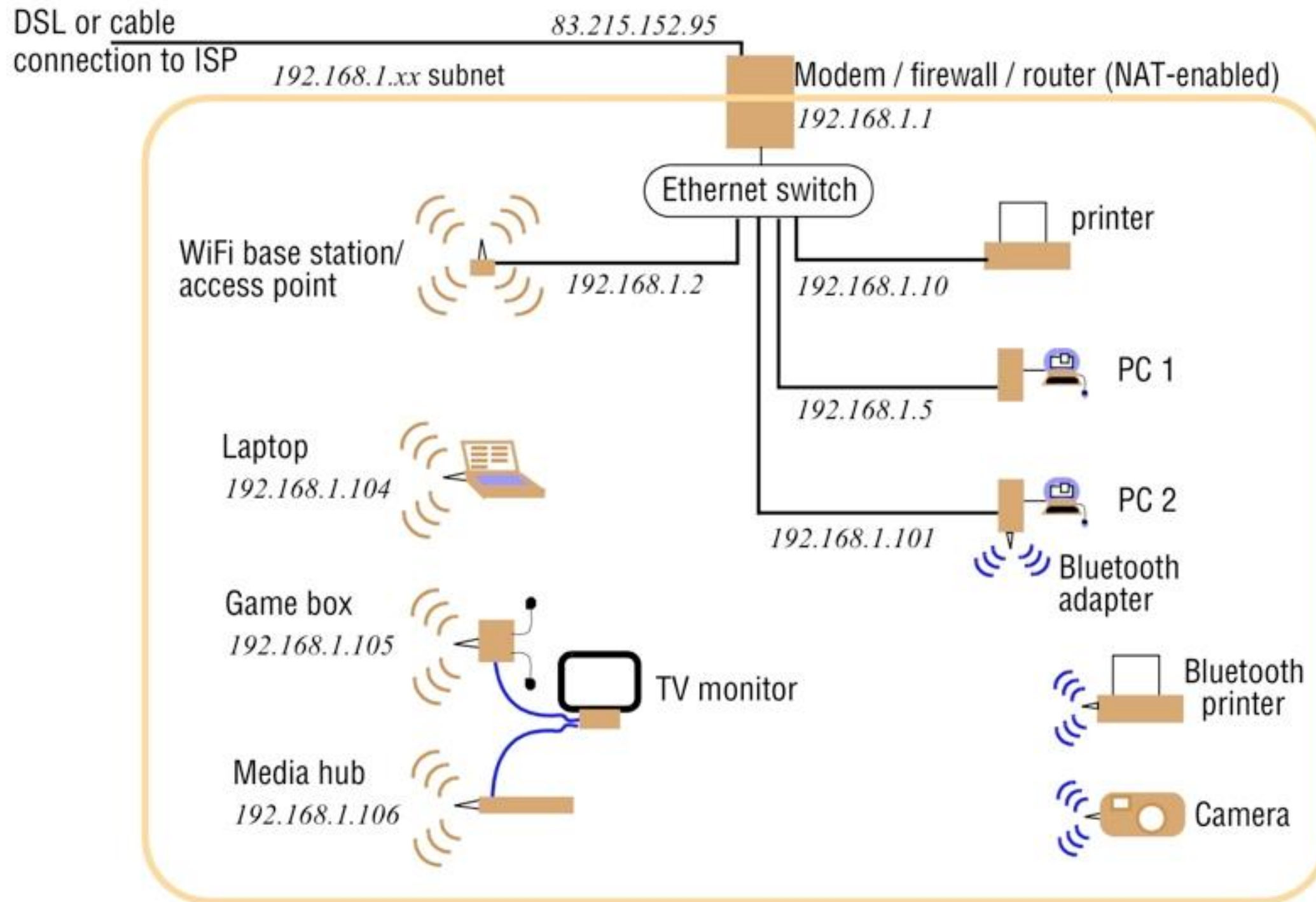


Figure 3.22 IEEE 802 network standards

<i>IEEE No.</i>	<i>Name</i>	<i>Title</i>	<i>Reference</i>
802.3	Ethernet	CSMA/CD Networks (Ethernet) Carrier Sense Multiple Access with Collision Detection	[IEEE 1985a]
802.4		Token Bus Networks	[IEEE 1985b]
802.5		Token Ring Networks	[IEEE 1985c]
802.6		Metropolitan Area Networks	[IEEE 1994]
802.11	WiFi	Wireless Local Area Networks	[IEEE 1999]
802.15.1	Bluetooth	Wireless Personal Area Networks	[IEEE 2002]
802.15.4	ZigBee	Wireless Sensor Networks	[IEEE 2003]
802.16	WiMAX	Wireless Metropolitan Area Networks	[IEEE 2004a]

Internet Protocols

- **Baseband transmission** sends only one signal at a time, and it uses digital signals.
- **Broadband transmission** sends multiple signals at a time, and it uses analog signals.

Figure 3.23 Ethernet ranges and speeds

	<i>10Base5</i>	<i>10BaseT</i>	<i>100BaseT</i>	<i>1000BaseT</i>
Data rate	10 Mbps	10 Mbps	100 Mbps	1000 Mbps
<i>Max. segment lengths:</i>				
Twisted wire (UTP)	100 m	100 m	100 m	25 m
Coaxial cable (STP)	500 m	500 m	500 m	25 m
Multi-mode fibre	2000 m	2000 m	500 m	500 m
Mono-mode fibre	25000 m	25000 m	20000 m	2000 m

Notes:

- Base means Baseband
- Notice that when bandwidth increases, range decreases

<R><L> Where: *R* = data rate in Mbps
B = medium signalling type (baseband or broadband)
L = maximum segment length in metres/100 or T
 (twisted pair cable hierarchy)

Network Issues for Distributed Systems

Performance:

- The general speed of data delivery in the network in addition to how often packet loss is experienced in the network.

Latency:

- The delay that occurs after a send operation is executed and before data starts to arrive at the destination computer. It can be measured as the time required to transfer an empty message (measured in *milliseconds*).

Data Transfer Rate (Network Speed):

- The actual speed at which data can be transferred between two computers (point-to-point) in the network once transmission has begun, usually quoted in *bits per second* (It depends on sender and receiver and data link).

Network Issues for Distributed Systems

Bandwidth:

- The theoretical total capacity of information that can be transmitted over a network link in a given time.

Throughput:

- The actual total amount of information that can be transmitted over a network link in a given time. It is not dependent on sender and receiver.

Scalability:

- The ability of network to handle increases in number of hosts, increases in volume of data, and having variety of devices.

Reliability:

- How often the network fails. Less failure means high reliability.

Network Issues for Distributed Systems

Security:

- How secure is the data sent/received via the network.

Mobility:

- What if some of the hosts in the network are mobile? Would that affect the service of the network. For example, it is largely dependent on wireless communication, so, what if wireless quality degrades? What if a node goes out of range?

QoS:

- Quality of Service (e.g., Fast Network, Reliable Network, etc.)
- **Unicasting:** Send to one destination in a given network.
- **Multicasting:** Send to several destinations in a given network.
- **Broadcasting:** Send to all destinations in a given network.

Transmission Time to Send a Packet

Packet Transmission Time = Latency + Length / Data Transfer Rate

Example:

- Latency = 3 milliseconds
- Suppose packet size = 100bits
- Data transfer rate = 50 bits per second
- Message transmission time = $3 + (100/50) = 5$ milliseconds

If a message is larger than packet size, then it will be broken into several packets.