20CS2007
Computer Communication Networks

GCR code: c4e3ucp

Course Outcomes

- The student will be able to

understand the components and layered architecture of communication networks

identify the protocols and services of data link layer.

analyze the different LAN technologies for building networks.

describe the wireless WAN technologies for wireless transmission.

design network model and determine the routing protocols for different applications.

construct communication networks for supporting different applications.

Module 1: Foundation of Networking

Physical layout of network components for personal and business networks.
Data Communication, Networks, OSI model, Layers in the OSI Model, TCP/IP Protocol Suite, Addressing.

Module 2: Data Links and Transmission

Medium selection for installing cables, Reliable data delivery in industrial environment.
Transmission media, Error detection and correction, block codes, linear block codes, cyclic codes, checksum, Data link control-Framing, Flow and error control, Channels, HDLC and PPP.

Module 3: Local Area Networks

Design Café and residential networks, Setup Wi-Fi networks, Traffic confinement with VLAN.
LANs and Basic Topologies, LAN Protocols, MAC/IP Address Conversion Protocols, Wired LAN, Wireless LAN, Virtual LAN, IEEE 802.11 Wireless LAN Standard.

Module 4: Wireless Wide Area Networks and LTE Technology

Design Private and public leased networks. Video conferencing, television and radio broadcast transmissions.

Wireless WAN, Cellular Networks, Mobile IP Management in Cellular Networks, Long-Term Evolution (LTE) Technology, Wireless Mesh Networks (WMNs) with LTE, Characterization of Wireless Channels.

Module 5: Routing and Internetworking

Address assignment for campus and enterprise networks, Transmission/Stream data delivery to single and multiple recipients.

Logical addressing, Internet Protocol, Address mapping and Error reporting, Delivery and forwarding, Unicast and multicast routing protocols.

Module 6: Transport and Application Protocols

Browsing E-commerce website, Remote access to server from workstation, Chat application.

Process-to-process delivery, UDP, TCP, Mobile Transport Protocols, Congestion control, DNS, TELNET, HTTP.

Text Books:

1. **Behrouz A. Foruzan, "Data communication and Networking", Tata McGraw-Hill, 4th Edition, 2017, ISBN-10: 9780070634145, ISBN-13: 978-0070634145.**
2. **Nader F. Mir, "Computer and Communication Networks",Pearson Education, Second Edition, 2015, ISBN-13: 978-0133814743, ISBN-10: 0133814742**

Reference Books:

1. William Stallings, "Data and Computer Communications", Pearson Education India, tenth edition, 2014, ISBN-10: 0133506487, ISBN-13: 978-0133506488
2. James F. Kurose and Keith W. Ross, "Computer Networking A Top-Down Approach", Pearson Education, Sixth edition, 2017, ISBN-10: 9789332585492, ISBN-13: 978-9332585492
3. Tanenbaum. A.S, "Computer Networks", Pearson, 5th edition, 2013, ISBN-10: 9332518742, ISBN-13: 978-9332518742

1-1 DATA COMMUNICATIONS

- The term telecommunication means communication at a distance.

  includes telephony, telegraphy, and television, (tele is Greek word for "far")
- The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- Data communications is the exchange of data between two devices via some form of transmission medium such as a wire cable.

Effectiveness of a data communications

- The effectiveness of a data communications system depends on **four fundamental characteristics**: **delivery, accuracy, timeliness, and jitter**.

1. **Delivery:** The system must **deliver data to the correct destination**. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy:** The system must **deliver the data accurately**. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness:** The system must **deliver data in a timely manner**. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
4. **Jitter:** Jitter refers to the **variation in the packet arrival time**. It is the uneven delay in the delivery of audio or video packets.

For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Components of a data communication system

- A data communications system has five components:

Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

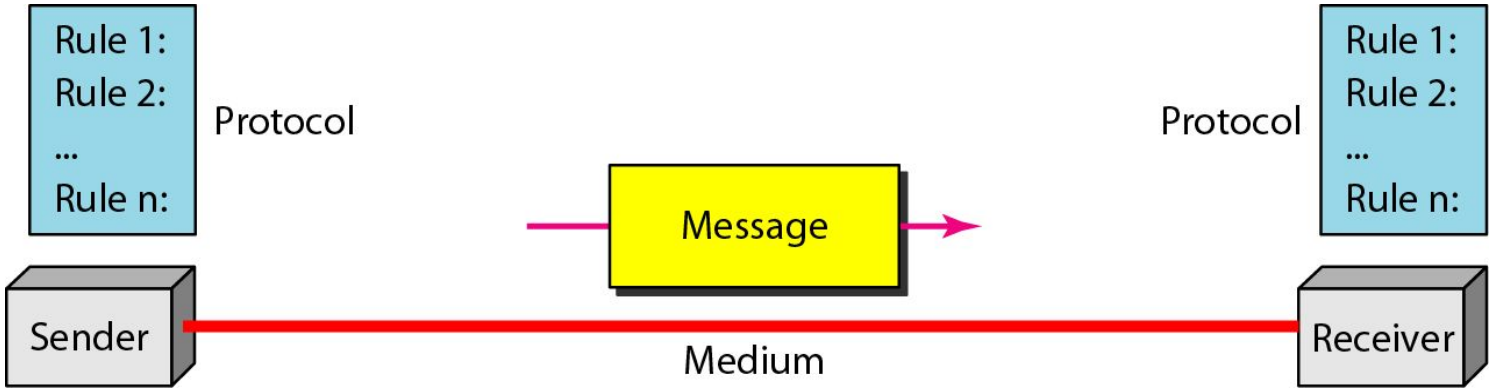
Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

Protocol: A **protocol** is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Components of a data communication system



Data Representation

- Information today comes in different forms such as text, numbers, images, audio, and video.

Text

- In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a **code**, and the process of representing symbols is called **coding**.
  - ASCII – developed by ANSI – code uses 7 bits for each symbol. This means 128 (2^7) different symbols can be defined by this code.

Numbers

- Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images

- Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot.
- The size of the pixel depends on the **resolution**.
- For example, an image can be divided into 1000 pixels or 10,000 pixels.
- In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image.
- After an image is divided into pixels, each pixel is assigned a **bit pattern**. The **size and the value of the pattern** depend on the image.

- If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns.
- A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.
- There are several methods to represent color images. One method is called **RGB,** so called because each color is made of a combination of three primary colors: *red,* green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it.
- Another method is called **YCM**, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

- Audio is a **representation of voice**. Audio refers to the **recording or broadcasting** of **sound** or **music**. Audio is by nature different from text, numbers, or images. It is **continuous**, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video

- Video refers to the **recording or broadcasting of a picture or movie**. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Direction of Data flow

- Communication between two devices can be **simplex, half-duplex, or full-duplex.**

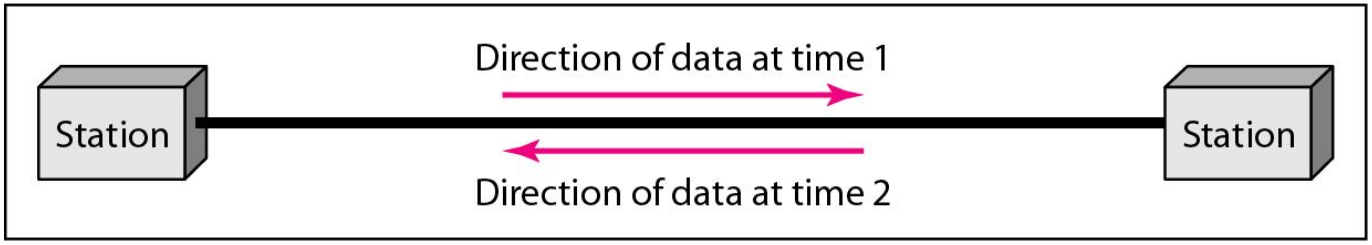
Simplex

- In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.

a. Simplex

Half-Duplex

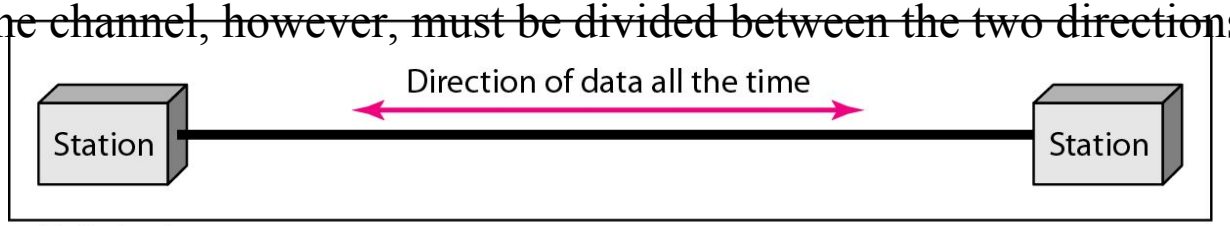
- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.
- The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.



b. Half-duplex

Full-Duplex

- In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.
- The full-duplex mode is like a 2-way street with traffic flowing in both directions at the same time.
- In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.
- One common exampleof full-duplex communication is the telephone network.
- When two people are communicating by a telephone line, both can talk and listen at the same time.
- The full-duplex mode is used when communication in both directions is required all the time.
- The capacity of the channel, however, must be divided between the two directions.



c. Full-duplex

1-2 NETWORKS

- A **network** is a set of devices (often referred to as **nodes**) connected by communication **links**.
- A **node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- A **link** can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

Distributed Processing

- Most networks use distributed processing, in which a task is divided among multiple computers.
- Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria

Performance

- Performance can be measured in many ways, including transit time and response time.
- **Transit time** is the amount of time required for a message to travel from one device to another.
- **Response time** is the elapsed time between an inquiry and a response.
- The **performance of a network depends** on a number of factors
  - the **type of transmission medium**
  - the **capabilities of the connected hardware**
  - the **efficiency of the software**.
- Measured in terms of **Delay and Throughput** - If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

- measured by the **frequency of failure**, the **time it takes a link to recover from a failure**, and the **network's robustness** in a catastrophe.

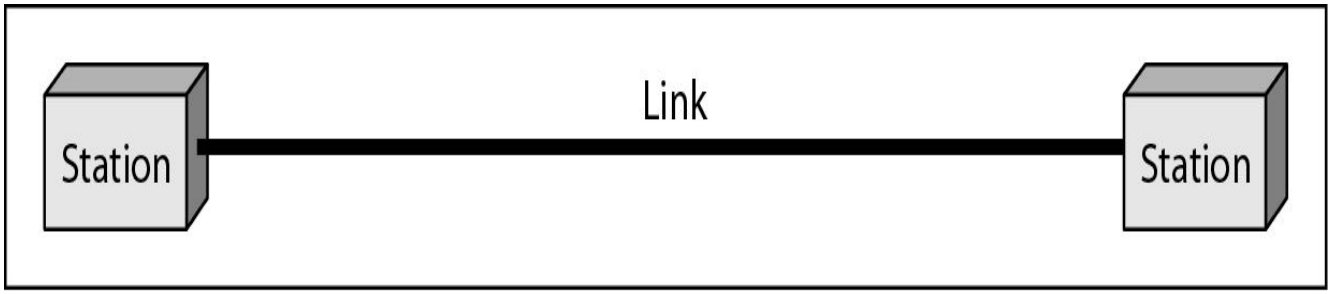
Security

- Network security issues include **protecting data** from **unauthorized access**, **protecting data from damage and development**, and **implementing policies and procedures** for recovery from breaches and data losses.

Physical Structures

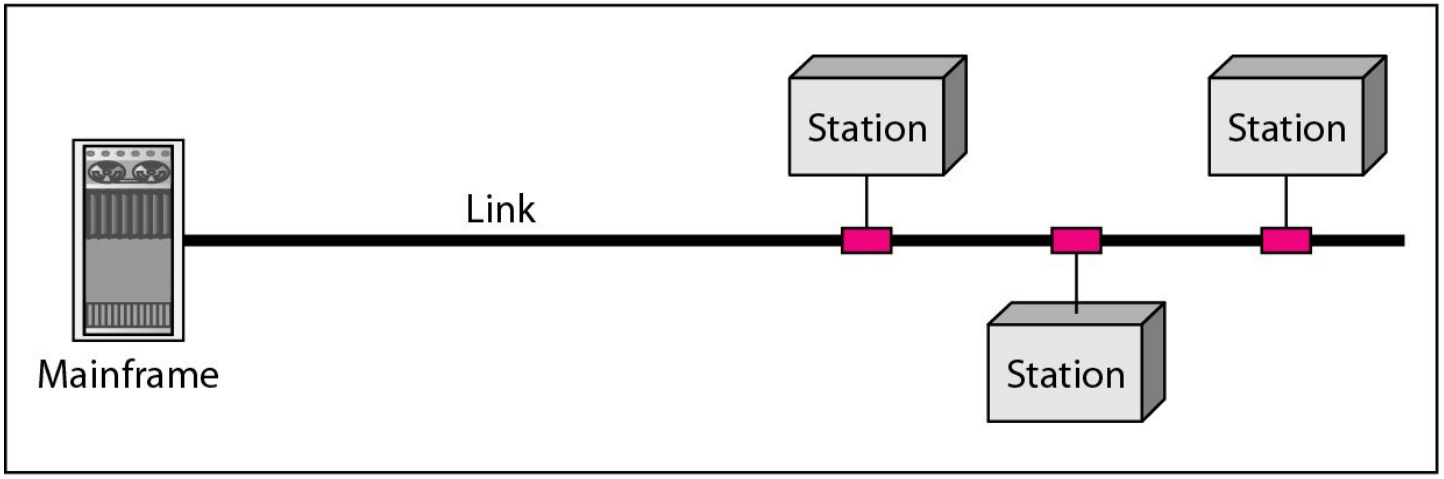
Types of Connection

- **Point to Point** – provides a dedicated link between 2 devices.
  - The entire capacity of the link is reserved for transmission between those two devices.
  - Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.
  - When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.
  - single transmitter and receiver



a. Point-to-point

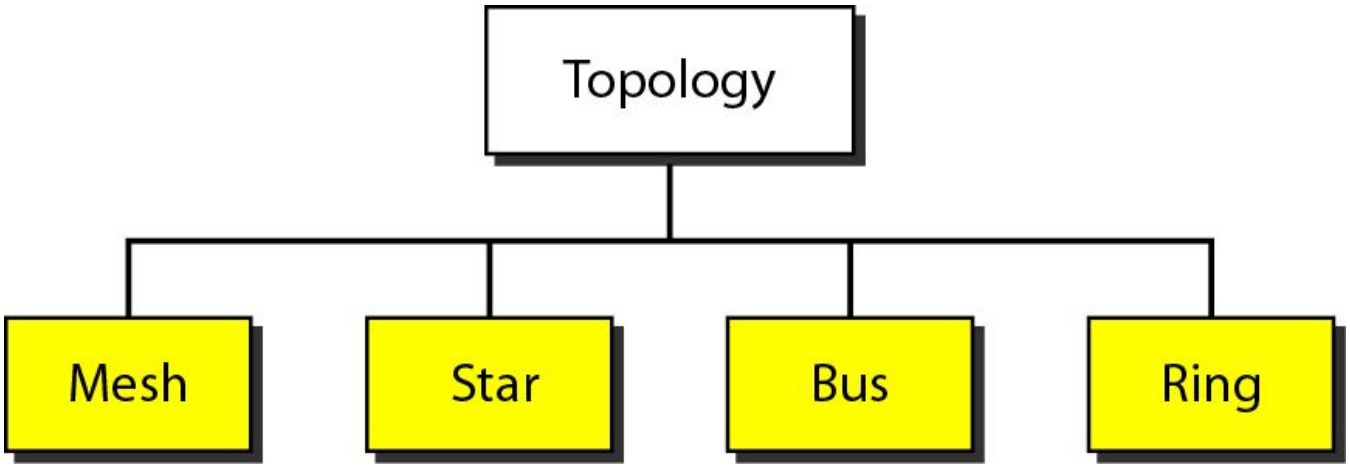
- **Multipoint**
  - multiple recipients of single transmission
  - A multipoint (also called **multidrop)** connection is one in which more than two specific devices share a single link.
  - In a multipoint environment, the capacity of the channel is shared, either **spatially** or **temporally**.
  - If several devices can use the link simultaneously, it is a ***spatially shared connection***.
  - If users must take turns, it is a ***timeshared* connection**.



b. Multipoint

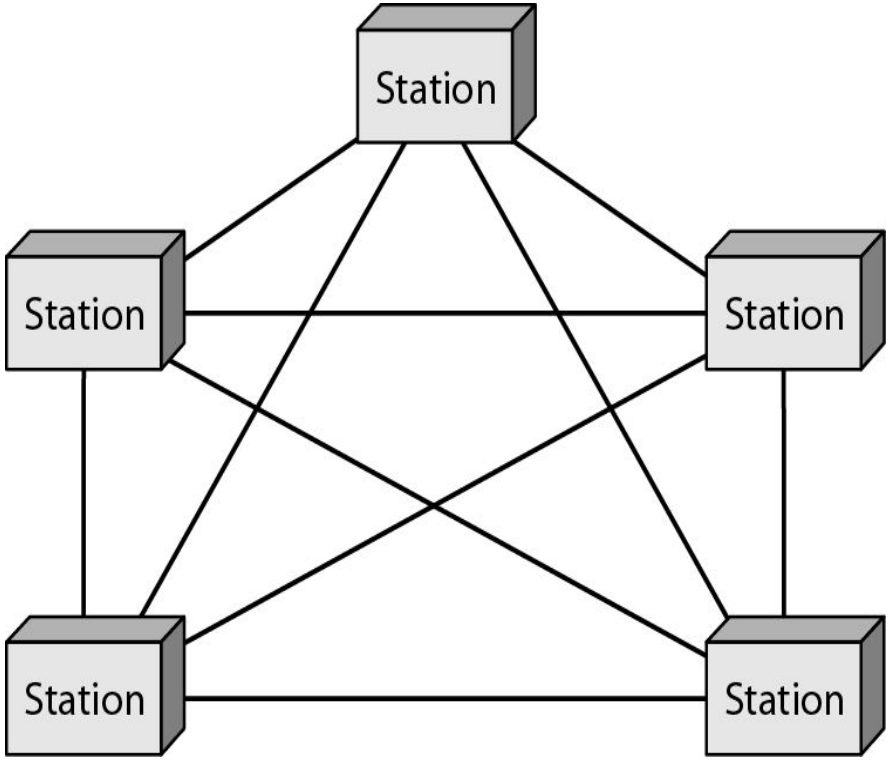
Physical Topology

- The term ***physical topology*** refers to the way in which a network is laid out physically.
- Two or more devices connect to a link; two or more links form a topology.
- The **topology of a network** is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are **four basic topologies:**



Mesh topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term *dedicated* means that the link carries traffic only between the two devices it connects.
- A fully connected mesh networks has $n(n-1)/2$ physical channels to link devices.
- Every device on the network must have $n-1$ input/output (I/O) ports



Advantages:

- The use of dedicated links guarantees that **each connection can carry its own data load**, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is **robust**. If one link becomes unusable, it does not incapacitate the entire system.
- There is the advantage of **privacy or security**. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
- Point-to-point links make **fault identification and fault isolation easy**. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

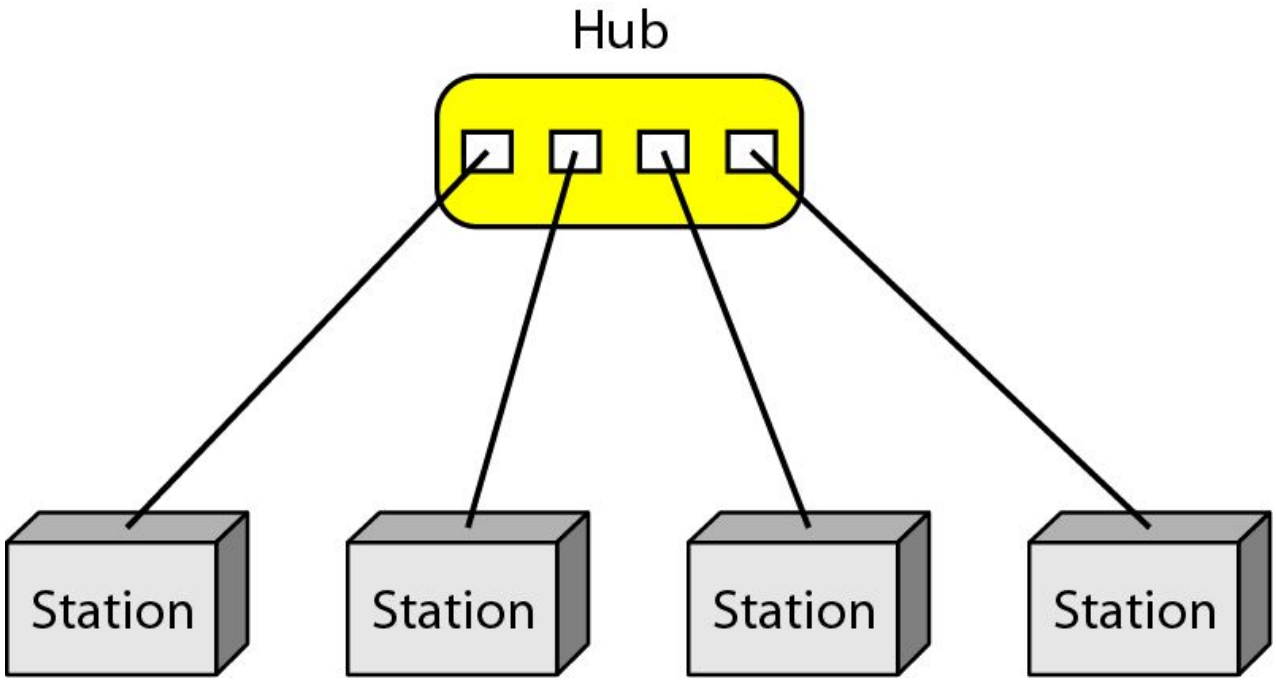
Disadvantages:

- Every device must be connected to every other device, **installation and reconnection are difficult.**
- The **sheer bulk of the wiring** can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- The hardware required to connect each link (I/O ports and cable) can be prohibitively **expensive.**

Practical example is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- A star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Advantages:

- A star topology is less expensive than a mesh topology.
- In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Robustness - If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

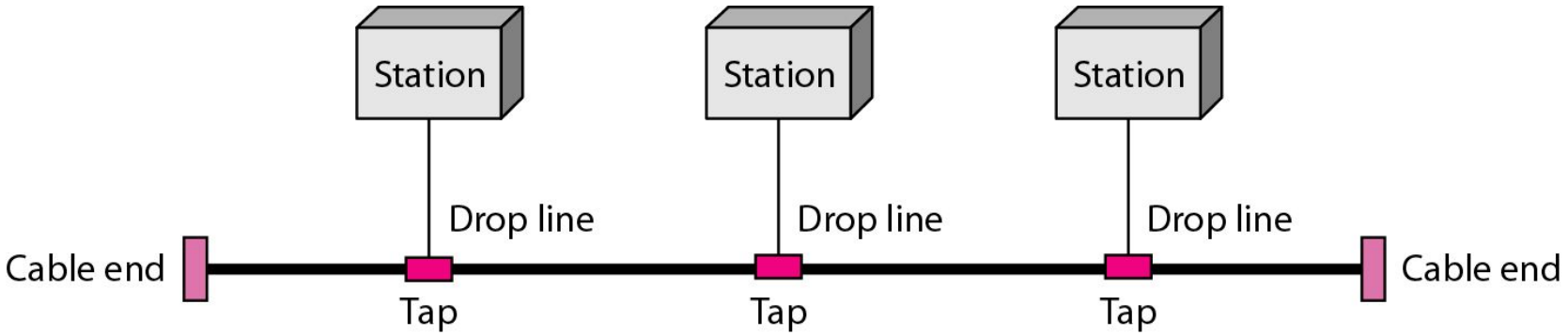
Disadvantages

- The **dependency of the whole topology on one single point**, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more **cabling is required in a star than in some other topologies** (such as ring or bus).

- The star topology is used in local-area networks (LANs).
- High-speed LANs often use a star topology with a central hub.

Bus topology

- One long cable acts as a **backbone** to link all the devices in a network.
- **Nodes** are connected to the **bus cable** by **drop lines** and **taps**.
- A **drop line** is a connection running between the device and the main cable.
- A **tap** is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed **into heat**. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



Advantages

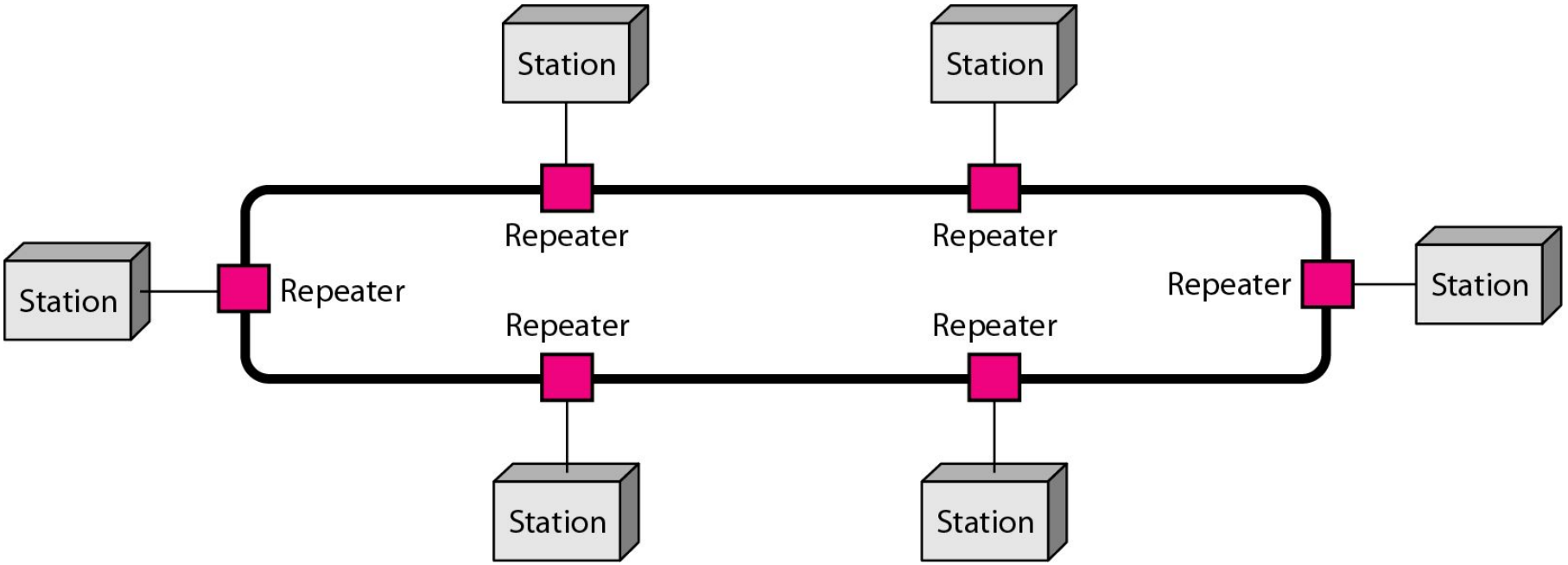
- Ease of installation.
  - Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a **bus uses less cabling than mesh or star topologies.**
  - In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub.
  - In a bus, this **redundancy is eliminated**. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages

- difficult reconnection and fault isolation.
- A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.
- A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages:

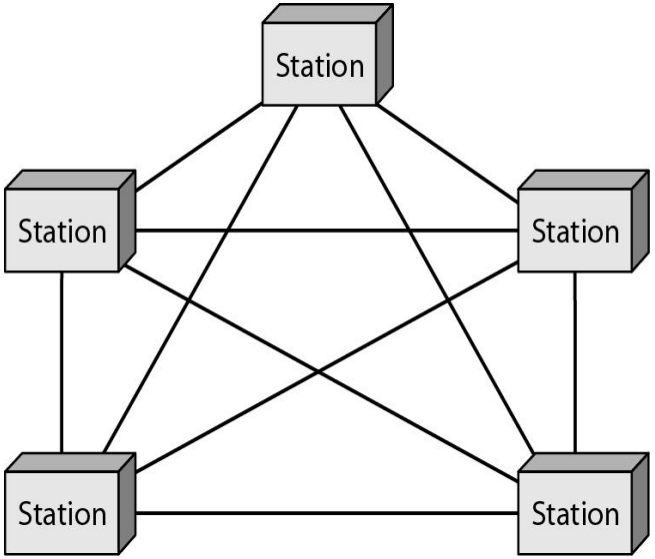
- A ring is relatively **easy to install and reconfigure**. Each device is linked to only its immediate neighbors (either physically or logically).
- To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).
- **Fault isolation** is simplified.
- Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

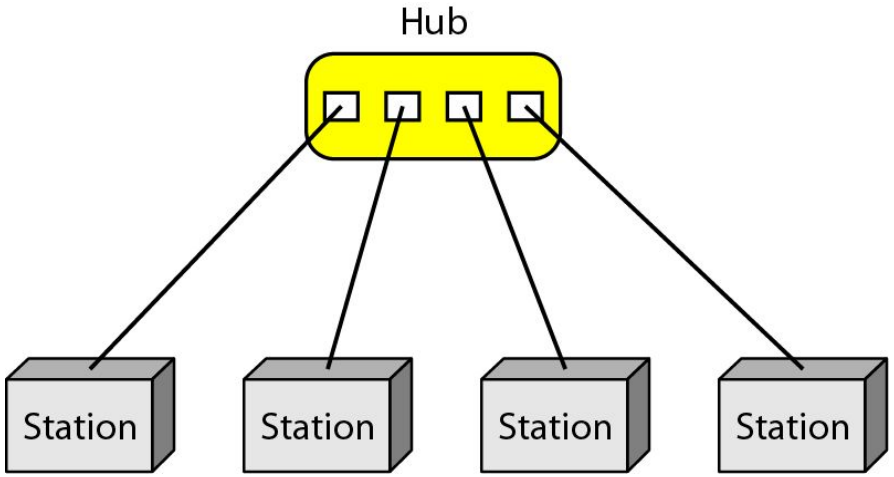
Disadvantages:

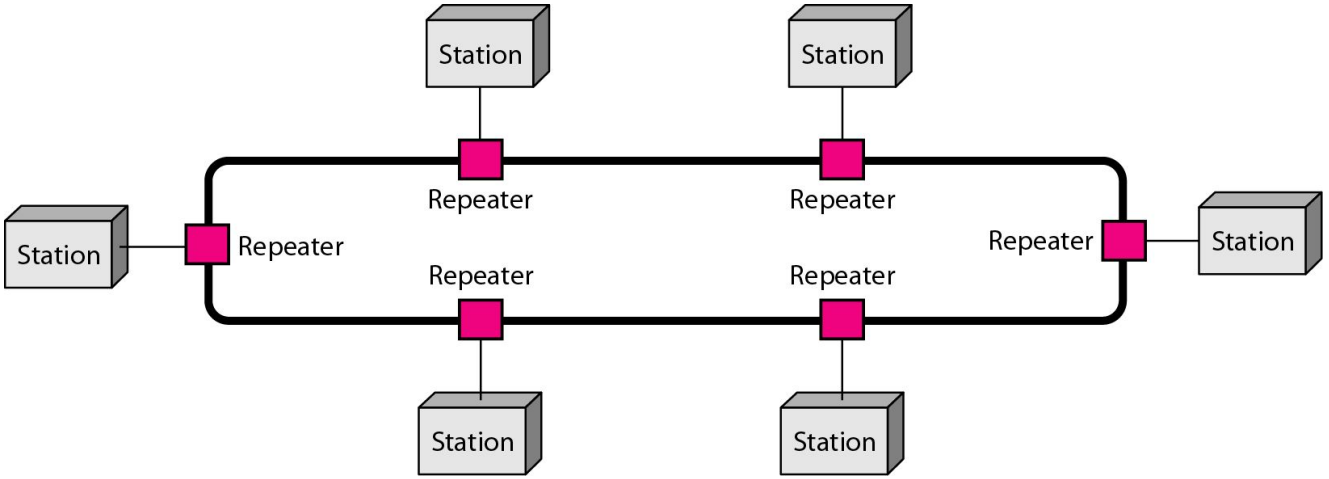
- Unidirectional traffic can be a disadvantage.

- In a simple ring, a break in the ring can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.
- Ring topology was prevalent when IBM introduced its local-area network Token Ring.

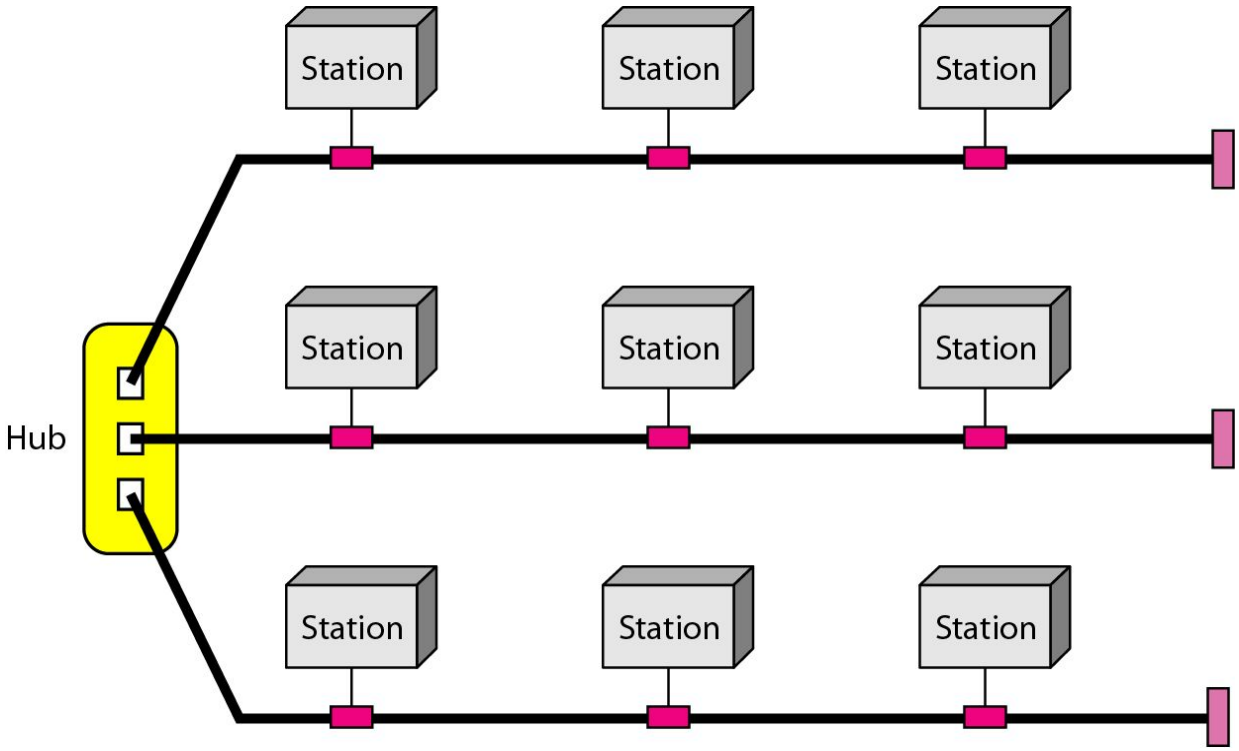
What type of connection does the following topology follow?







Hybrid topology



Categories of Networks

- **Local Area Networks (LANs)**
  - **Short distances**
  - **Designed to provide local interconnectivity**
- **Wide Area Networks (WANs)**
  - **Long distances**
  - **Provide connectivity over large areas**
- **Metropolitan Area Networks (MANs)**
  - **Provide connectivity over areas such as a city, a campus**

Figure 1.10 *An isolated LAN connecting 12 computers to a hub in a closet*

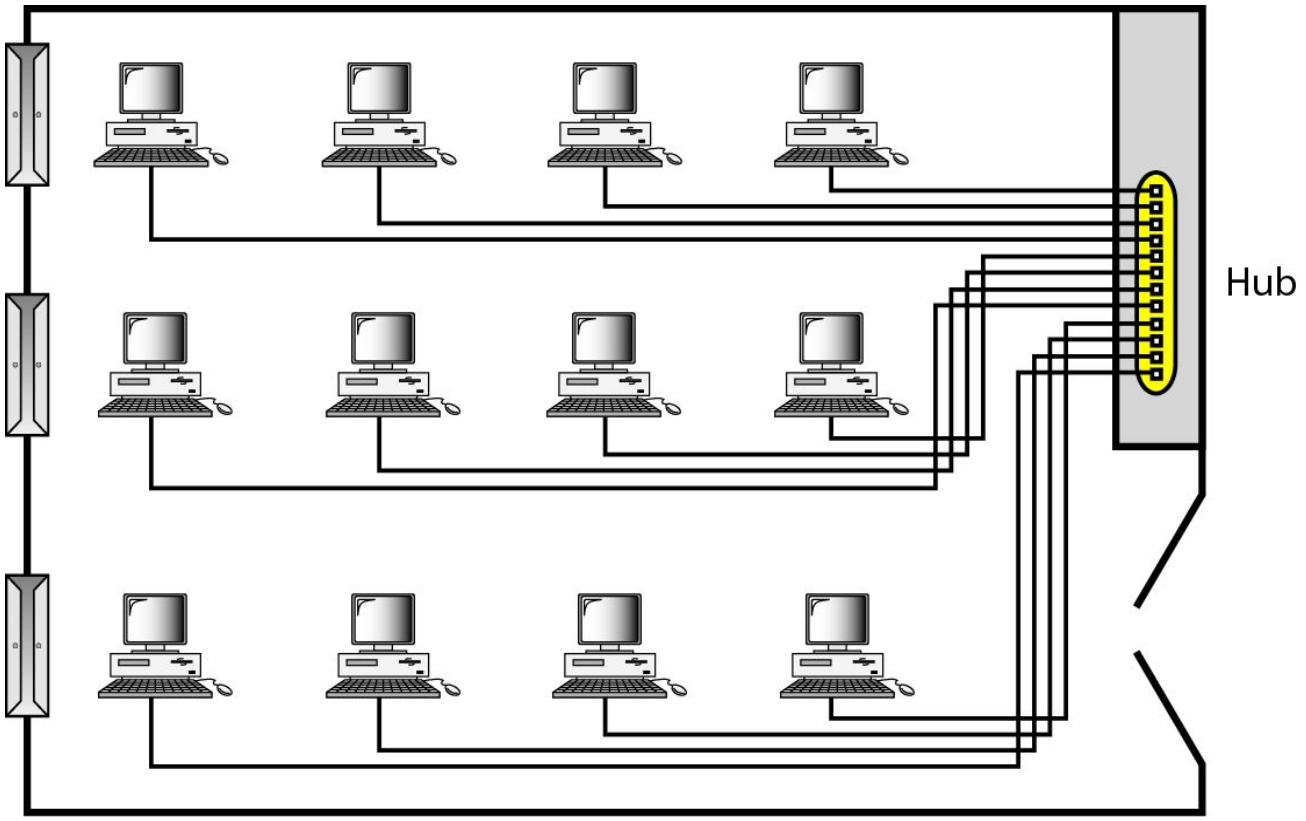
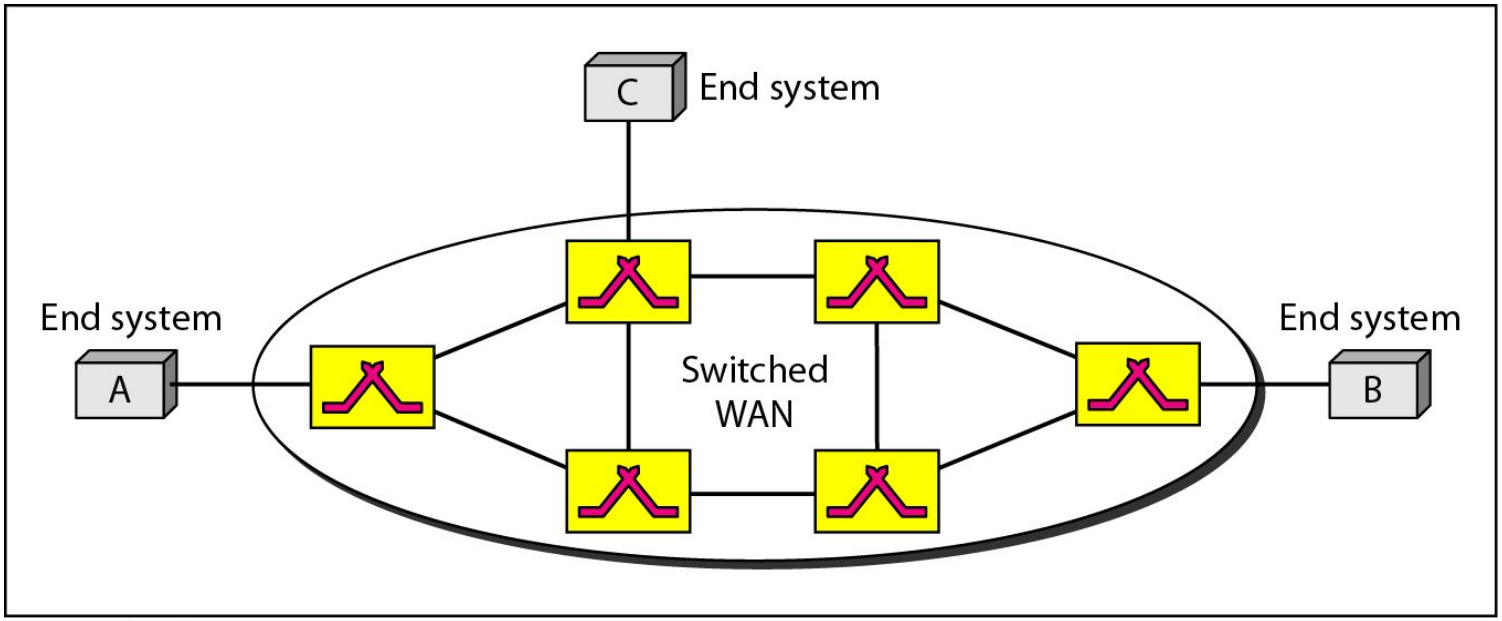
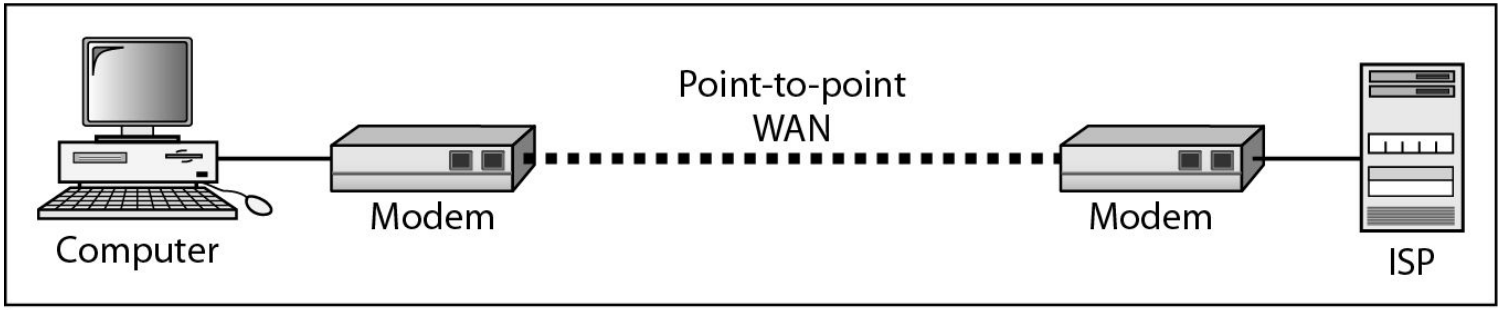


Figure 1.11 *WANs: a switched WAN and a point-to-point WAN*

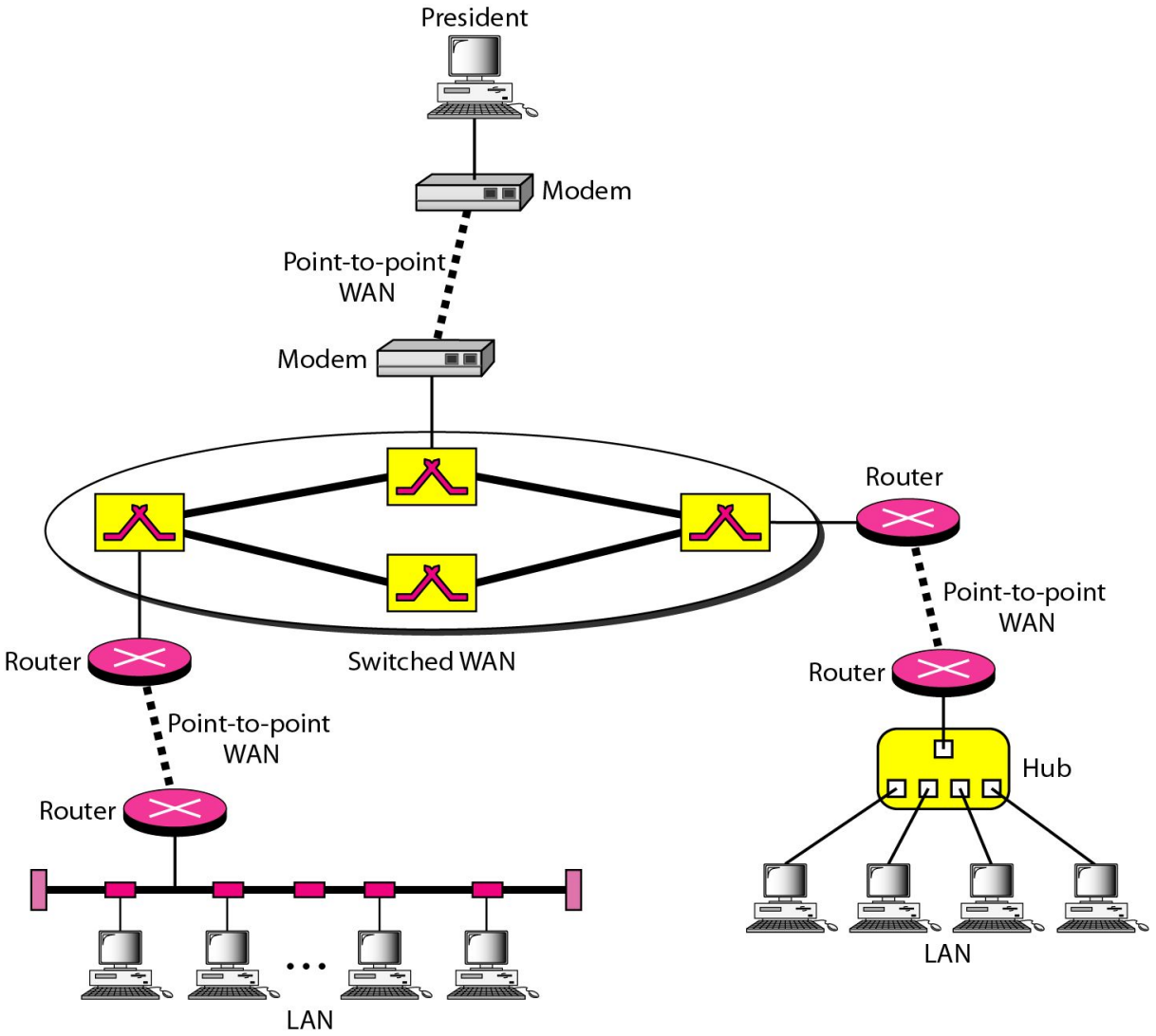


a. Switched WAN



b. Point-to-point WAN

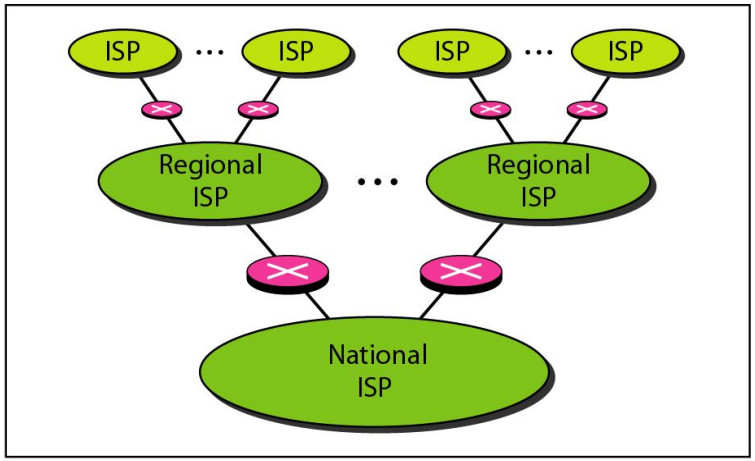
Figure 1.12 *A heterogeneous network made of four WANs and two LANs*



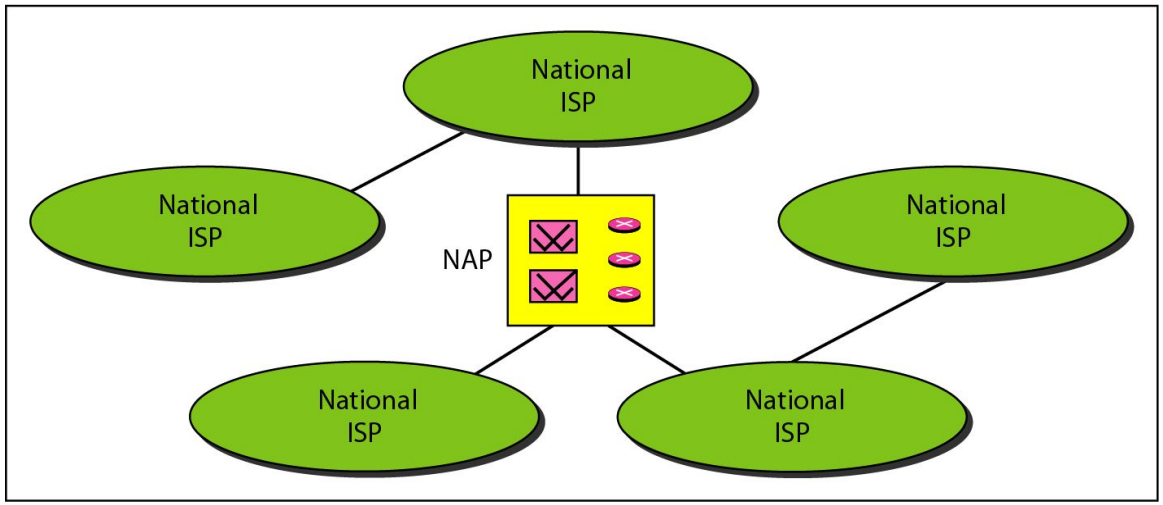
1-3 THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

1-4 PROTOCOLS

A protocol is timing synonymous with rule. It consists of a set of rules that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

Elements of a Protocol

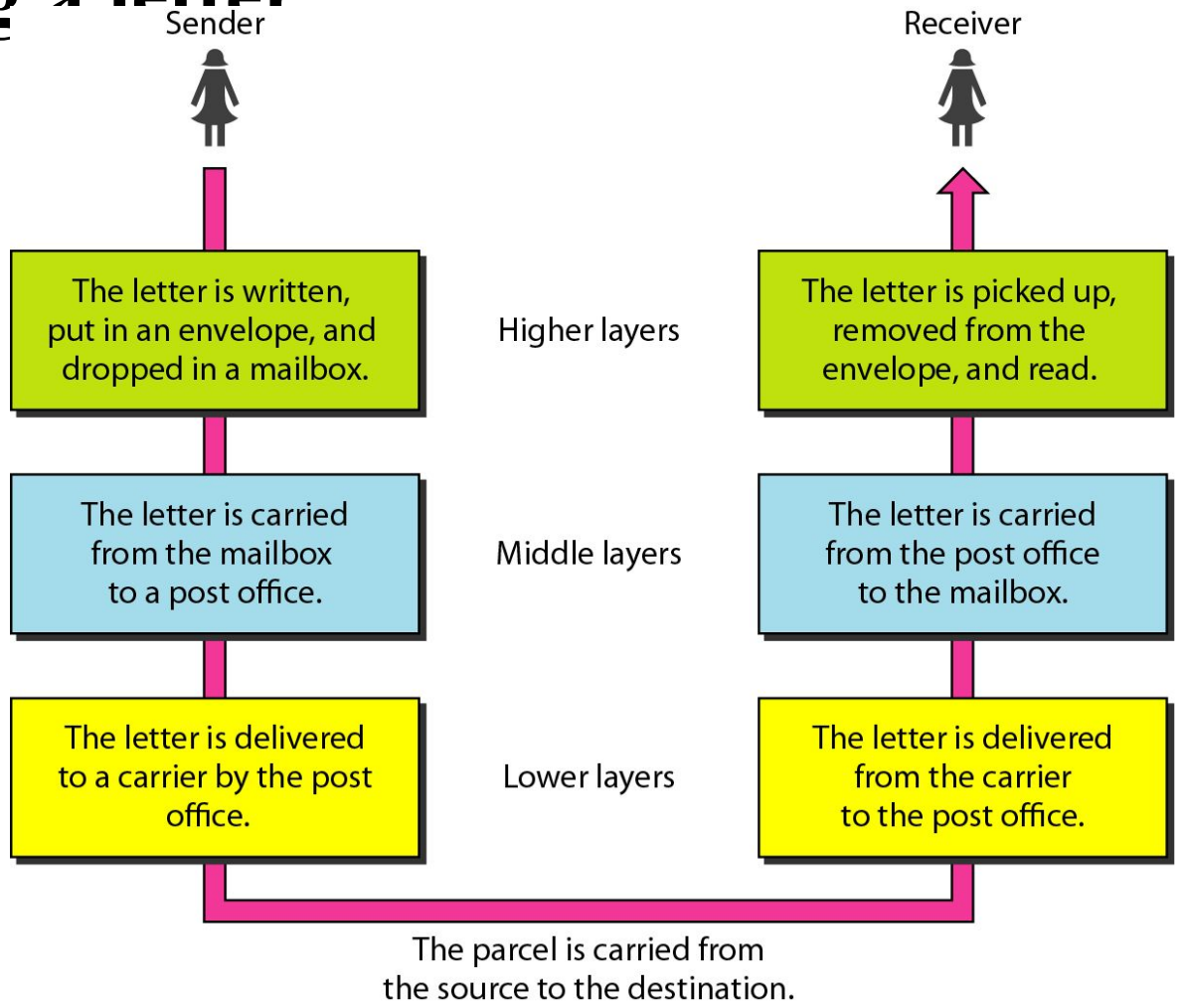
- Syntax
  - Structure or format of the data
  - Indicates how to read the bits - field delineation
- Semantics
  - Interprets the meaning of the bits
  - Knows which fields define what action
- Timing
  - When data should be sent and what
  - Speed at which data should be sent or speed at which it is being received.

Network Models

2-1 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.

Figure 2.1 Tasks involved in sending a letter



2-2 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.

Note

ISO is the organization.
OSI is the model.

Figure 2.2 *Seven layers of the OSI model*

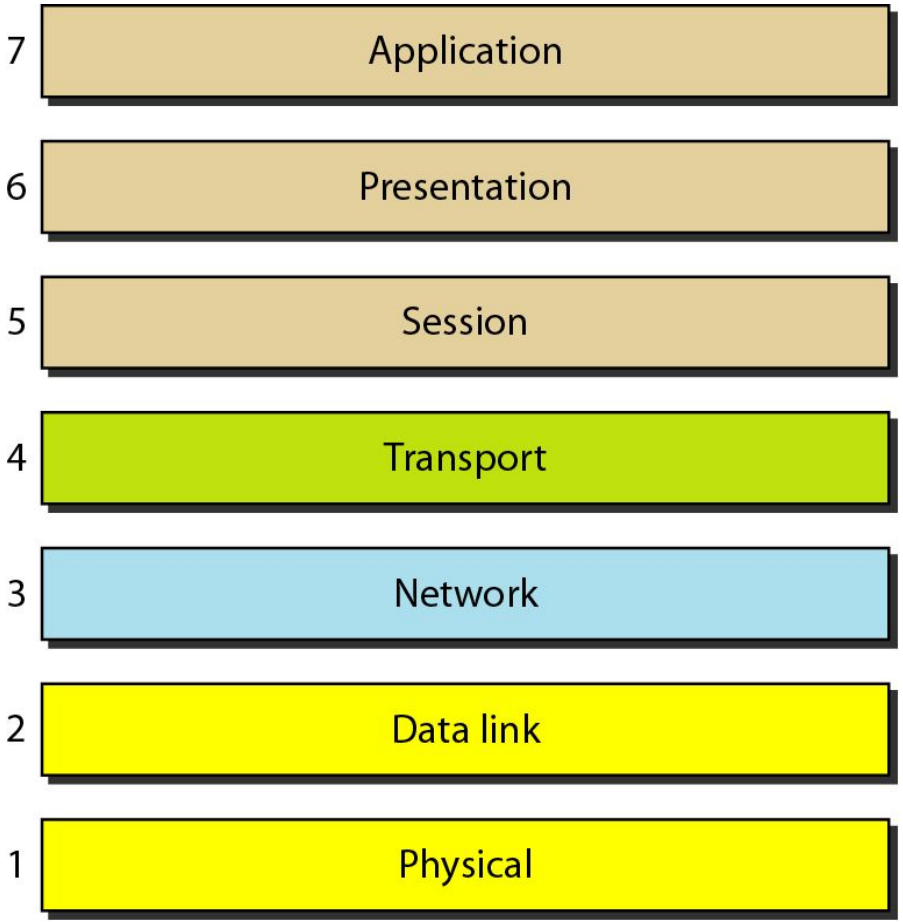
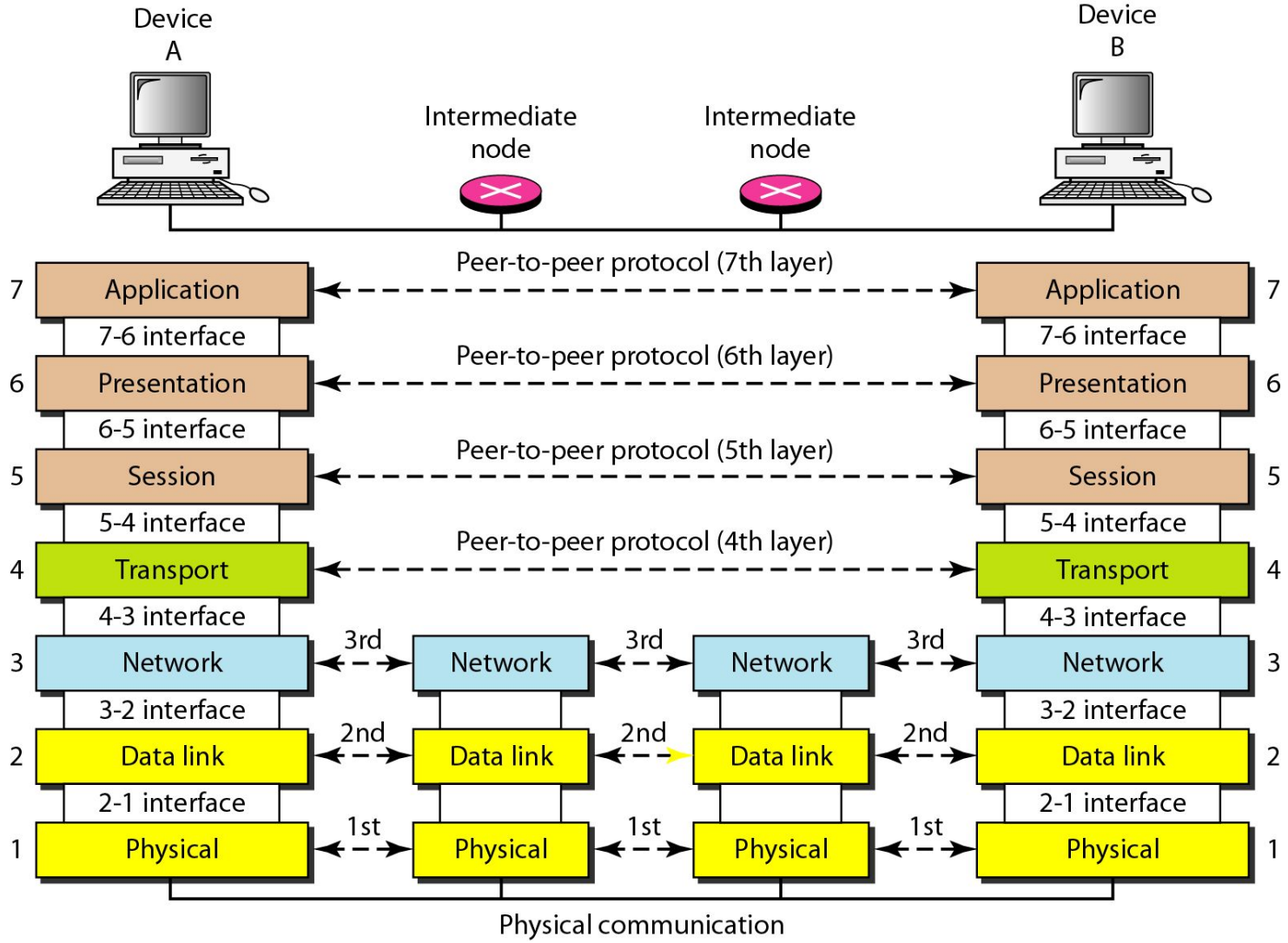


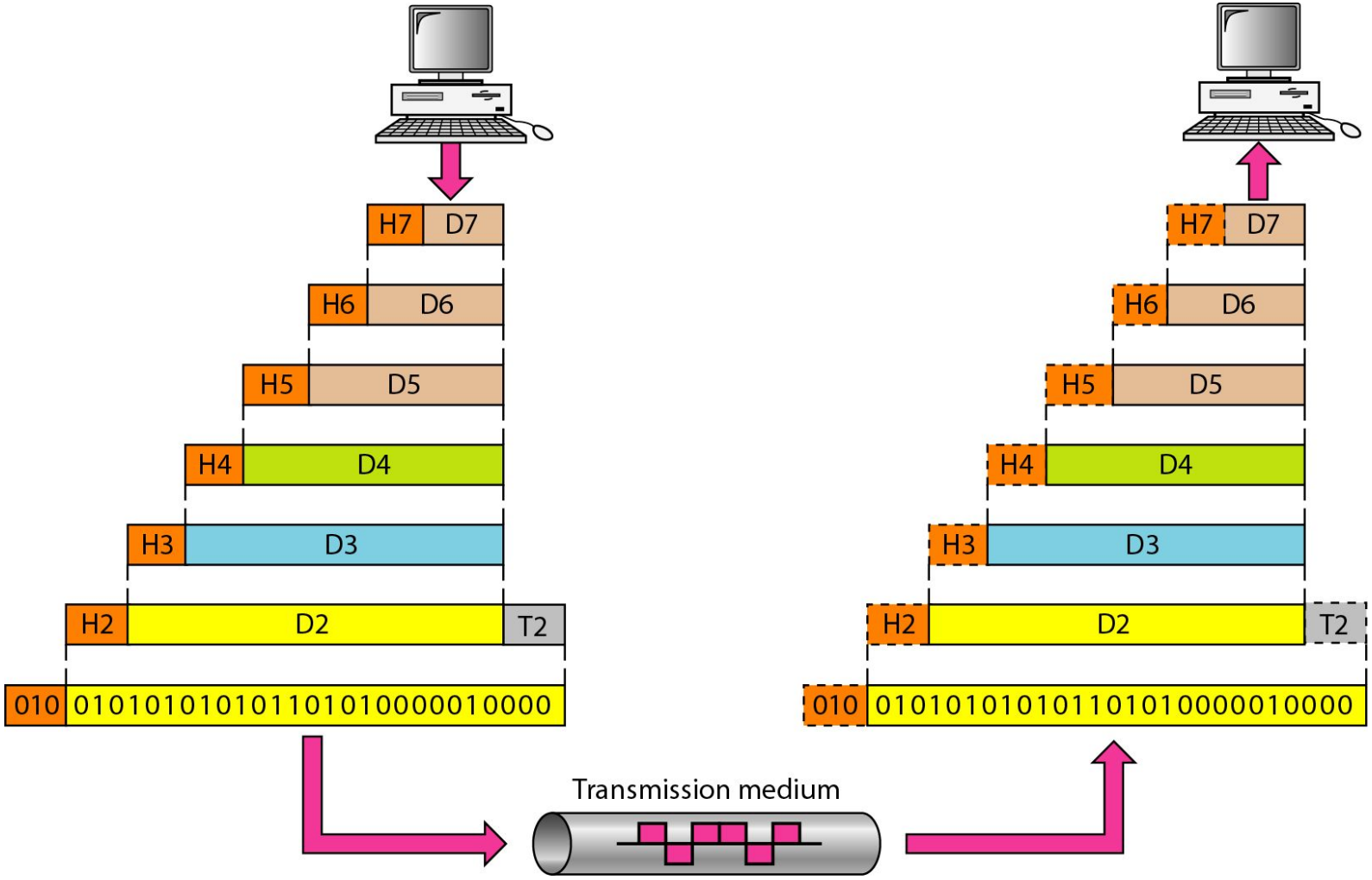
Figure 2.3 *The interaction between layers in the OSI model*



Interfaces Between Layers

- The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an **interface** between each pair of adjacent layers.
- Each interface defines the **information and services a layer** must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.

Figure 2.4 *An exchange using the OSI model*



2-3 LAYERS IN THE OSI MODEL

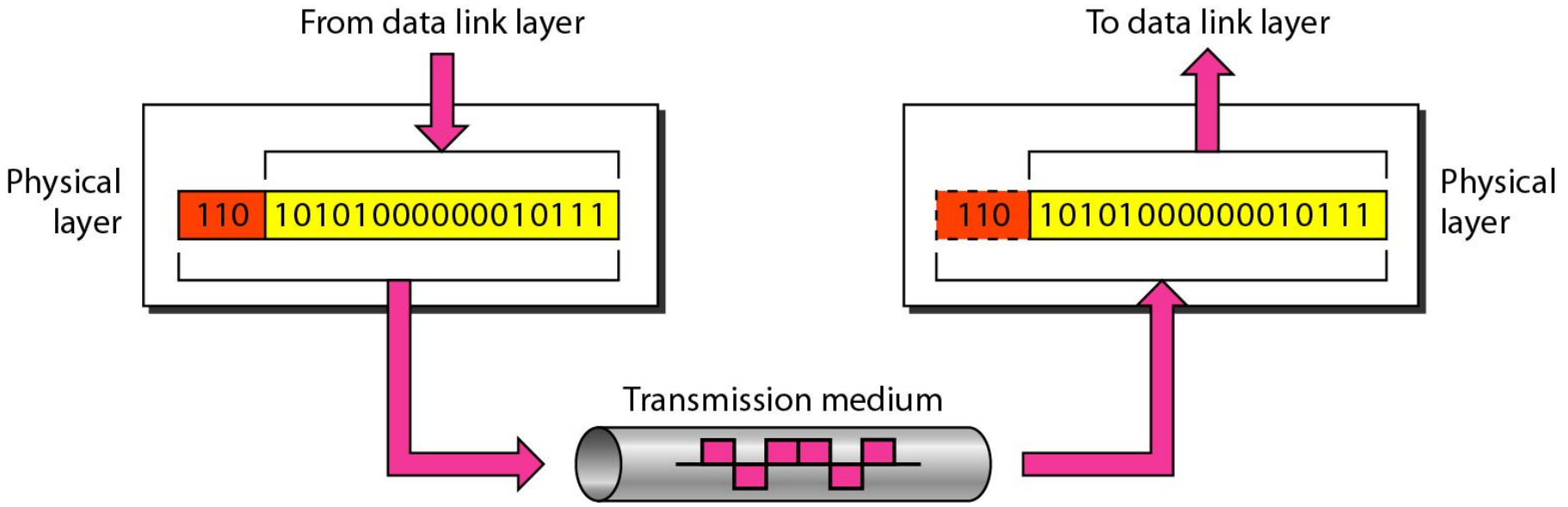
Physical Layer

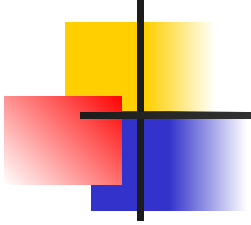
- The **physical layer** coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the **mechanical and electrical specifications** of the interface and transmission medium.
- It also defines the **procedures and functions** that physical devices and interfaces have to perform for transmission to occur.

The physical layer is also concerned with the following:

- Physical characteristics of interfaces and medium.
- Representation of bits.
- Data rate – transmission rate
- Synchronization of bits.
- Line configuration.
- Physical topology
- Transmission mode

Figure 2.5 *Physical layer*





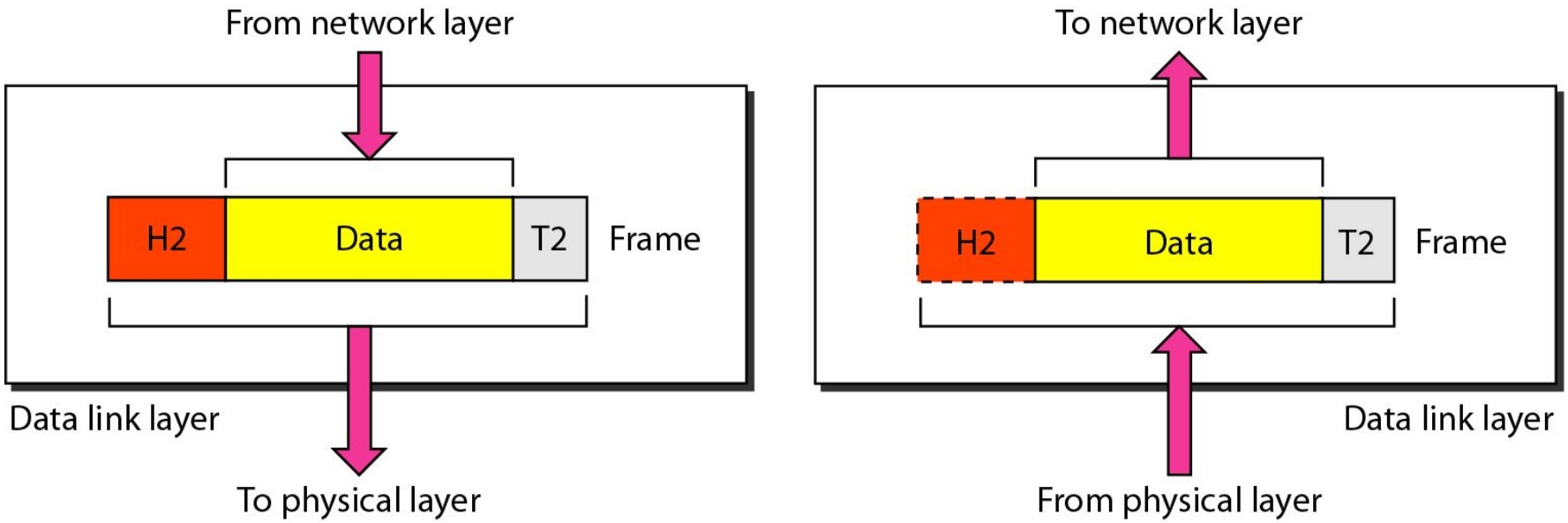
Note

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

Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- It makes the physical layer appear error-free to the upper layer (network layer).
- Other responsibilities of the data link layer include the following:
  - Framing.
  - Physical addressing.
  - Flow control.
  - Error control.
  - Access control.

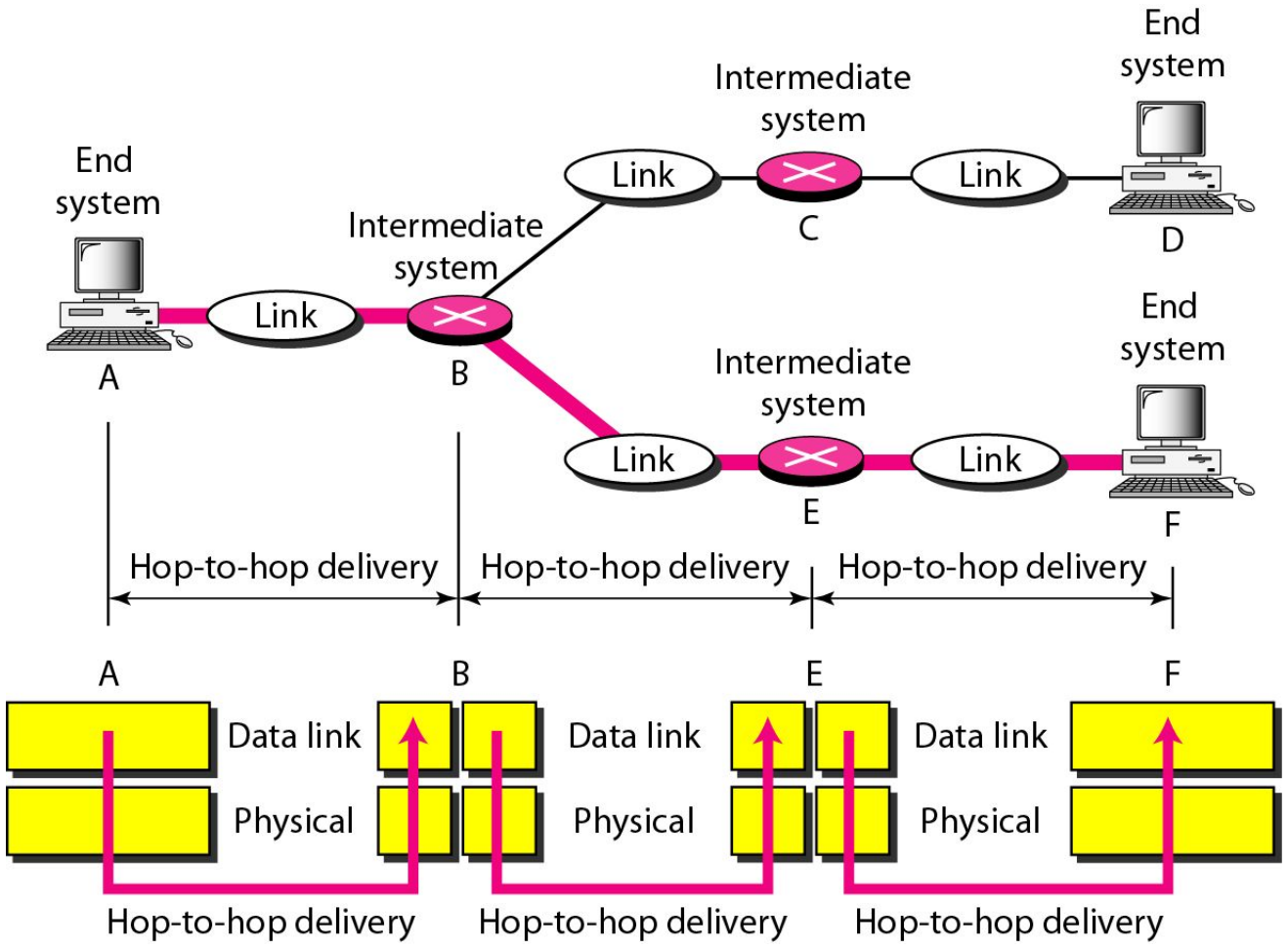
Figure 2.6 *Data link layer*



Note

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

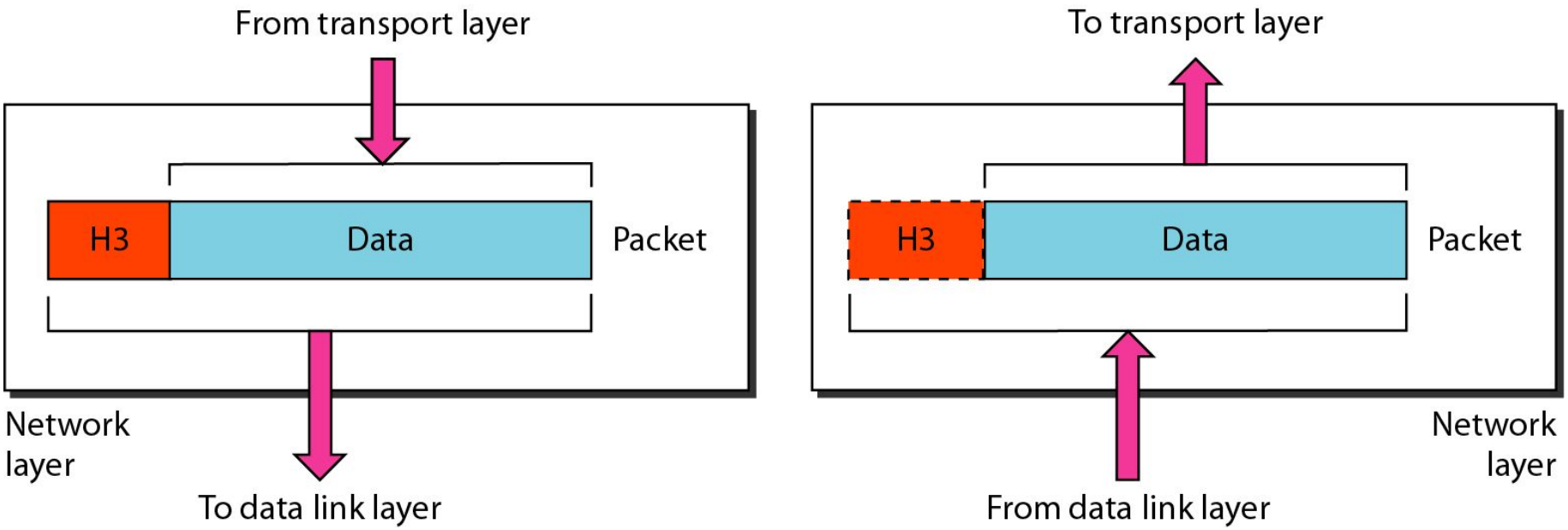
Figure 2.7 *Hop-to-hop delivery*



Network Layer

- The network layer is responsible for the **source-to-destination delivery of a packet**, possibly across multiple networks (links).
- Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.
- If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.
- Other responsibilities of the network layer include the following:
  - Logical addressing.
  - Routing.

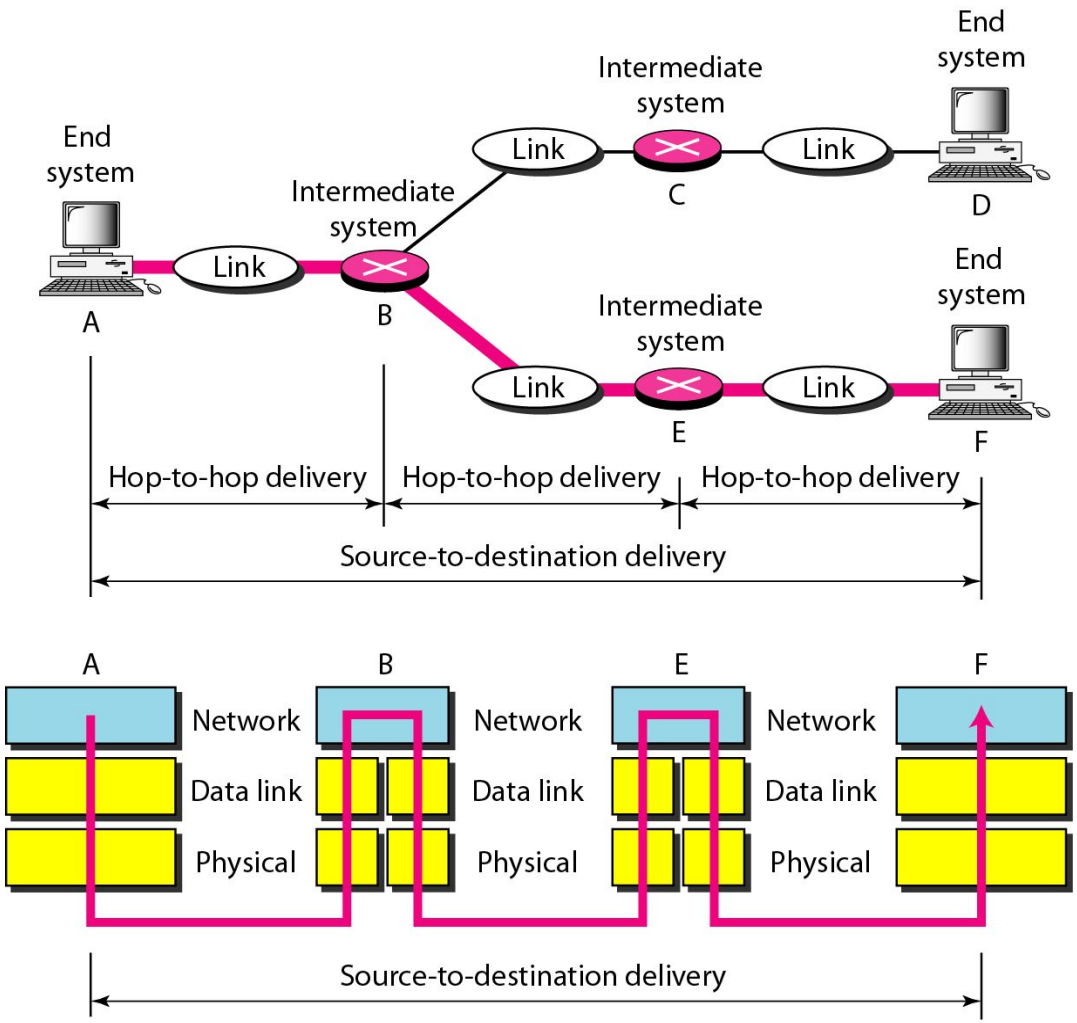
Figure 2.8 *Network layer*



Note

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

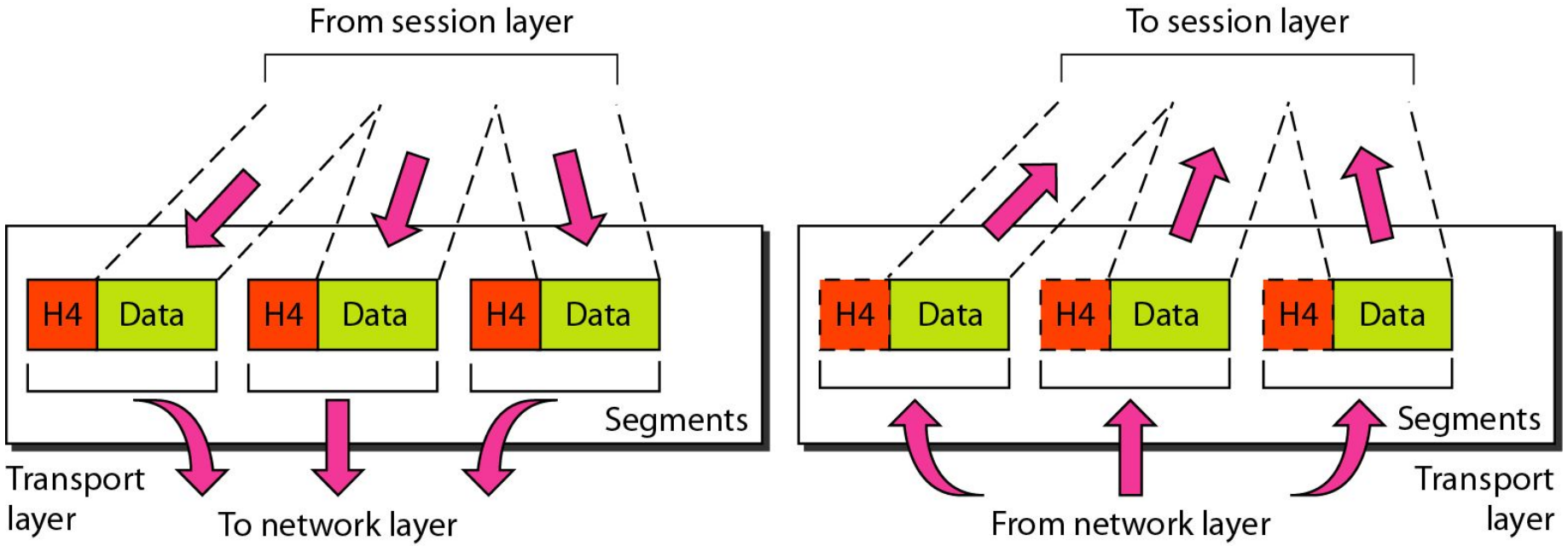
Figure 2.9 *Source-to-destination delivery*



Transport Layer

- The transport layer is responsible for **process-to-process delivery** of the entire message.
- A process is an application program running on a host.
- Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
- It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.
- Other responsibilities of the transport layer include the following:
  - Port addressing.
  - Segmentation and reassembly
  - Connection control
  - Flow control
  - Error control

Figure 2.10 *Transport layer*



Note

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

Figure 2.11 *Reliable process-to-process delivery of a message*

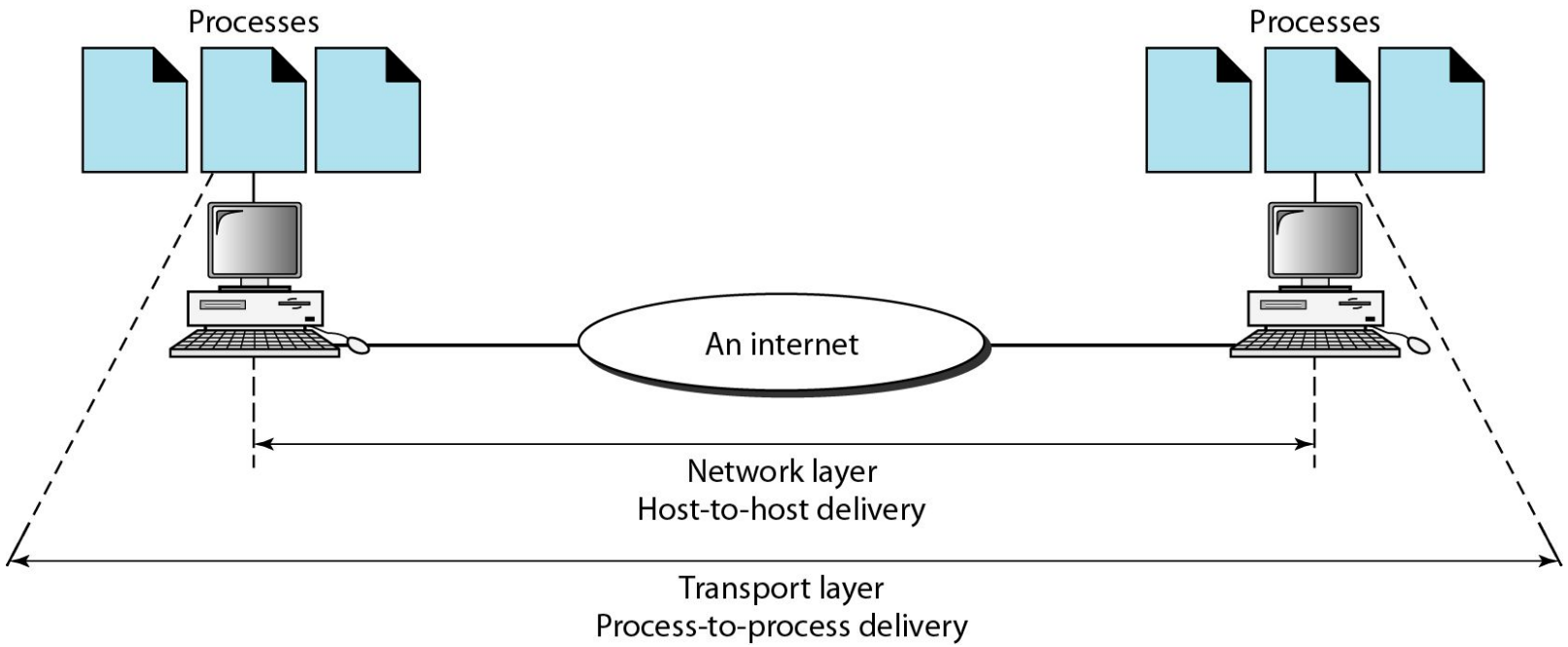
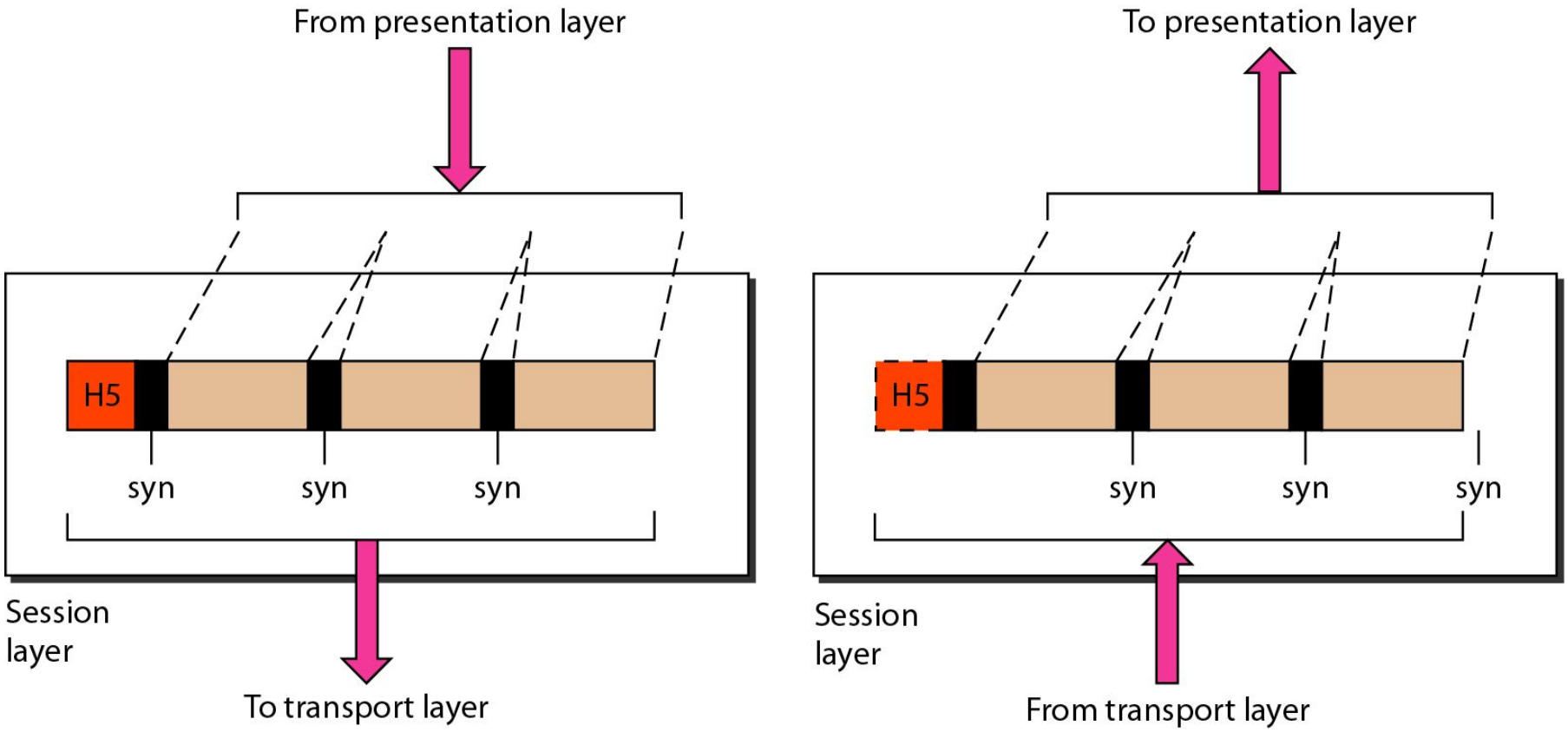


Figure 2.12 *Session layer*



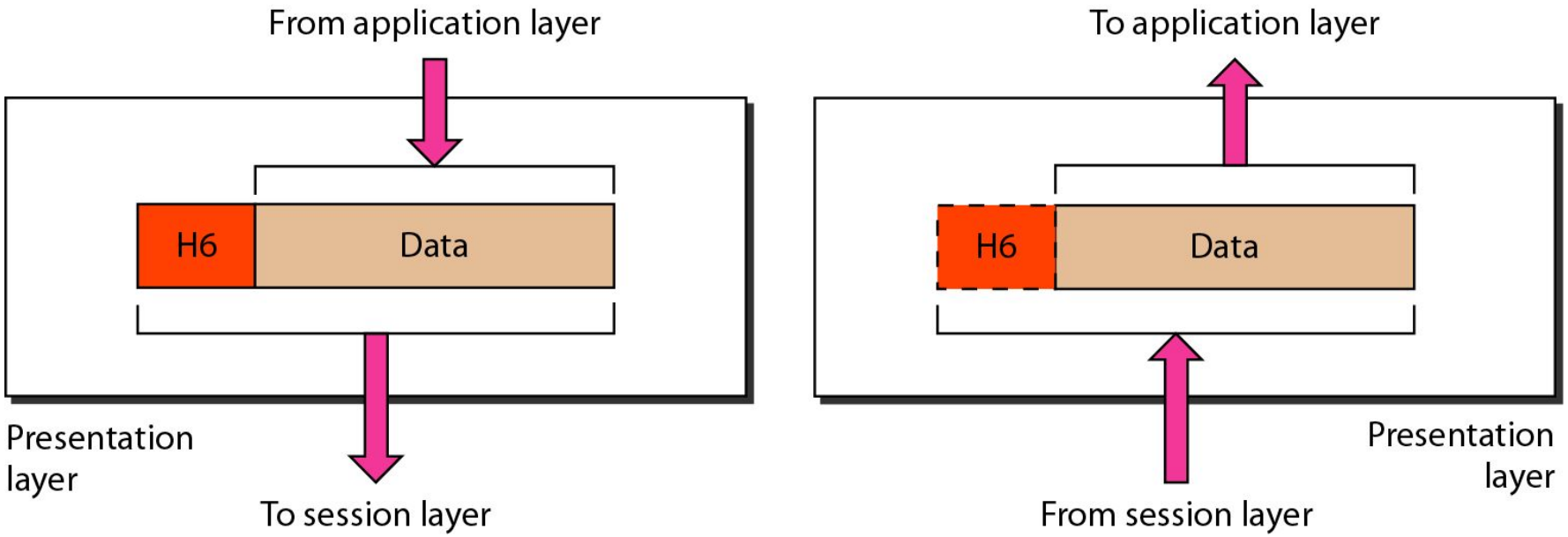
Note

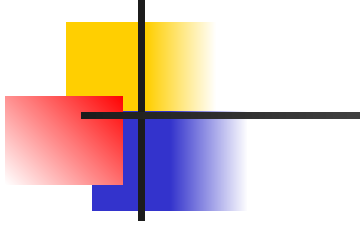
The session layer is responsible for dialog control and synchronization.

Session Layer

- The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.
- The session layer is the **network *dialog controller***.
- It **establishes**, **maintains**, and **synchronizes** the interaction among communicating systems.
- **Specific responsibilities of the session layer :**
  - **Dialog control**
  - **Synchronization**

Figure 2.13 *Presentation layer*





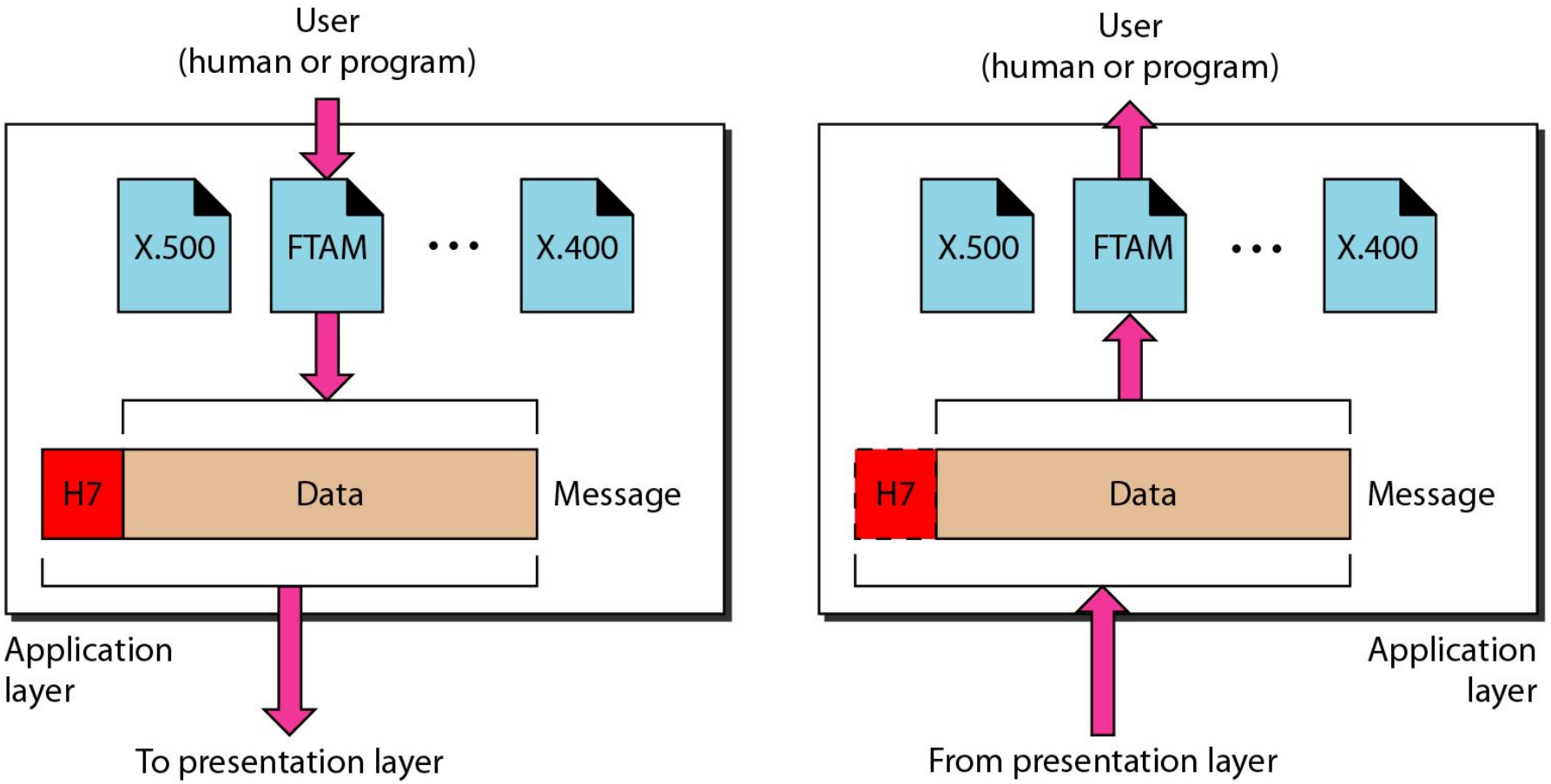
Note

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

Presentation Layer

- The presentation layer is concerned with the **syntax and semantics** of the information exchanged between two systems.
- **Specific responsibilities of the presentation layer :**
  - Translation
  - Encryption - Decryption
  - Compression.

Figure 2.14 *Application layer*



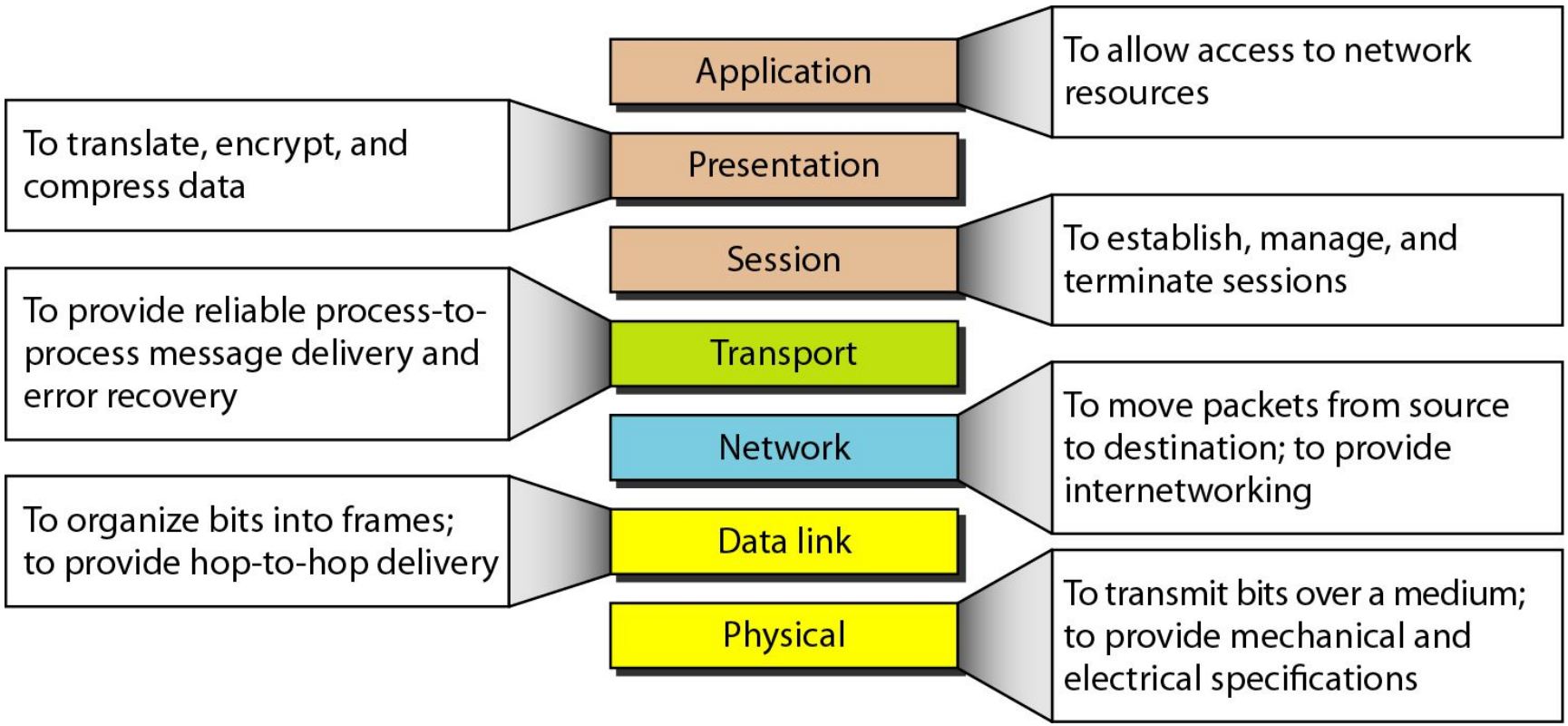
Note

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

Application Layer

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Specific services provided by the application layer include the following:
  - **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. To do so, the application creates a **software emulation** of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
  - **File transfer, access, and management:** This application allows a user to access files in a remote host (to make changes or read data), 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 the basis for e-mail forwarding and storage.
  - **Directory services:** This application provides distributed database sources and access for global information about various objects and services.

Figure 2.15 *Summary of layers*

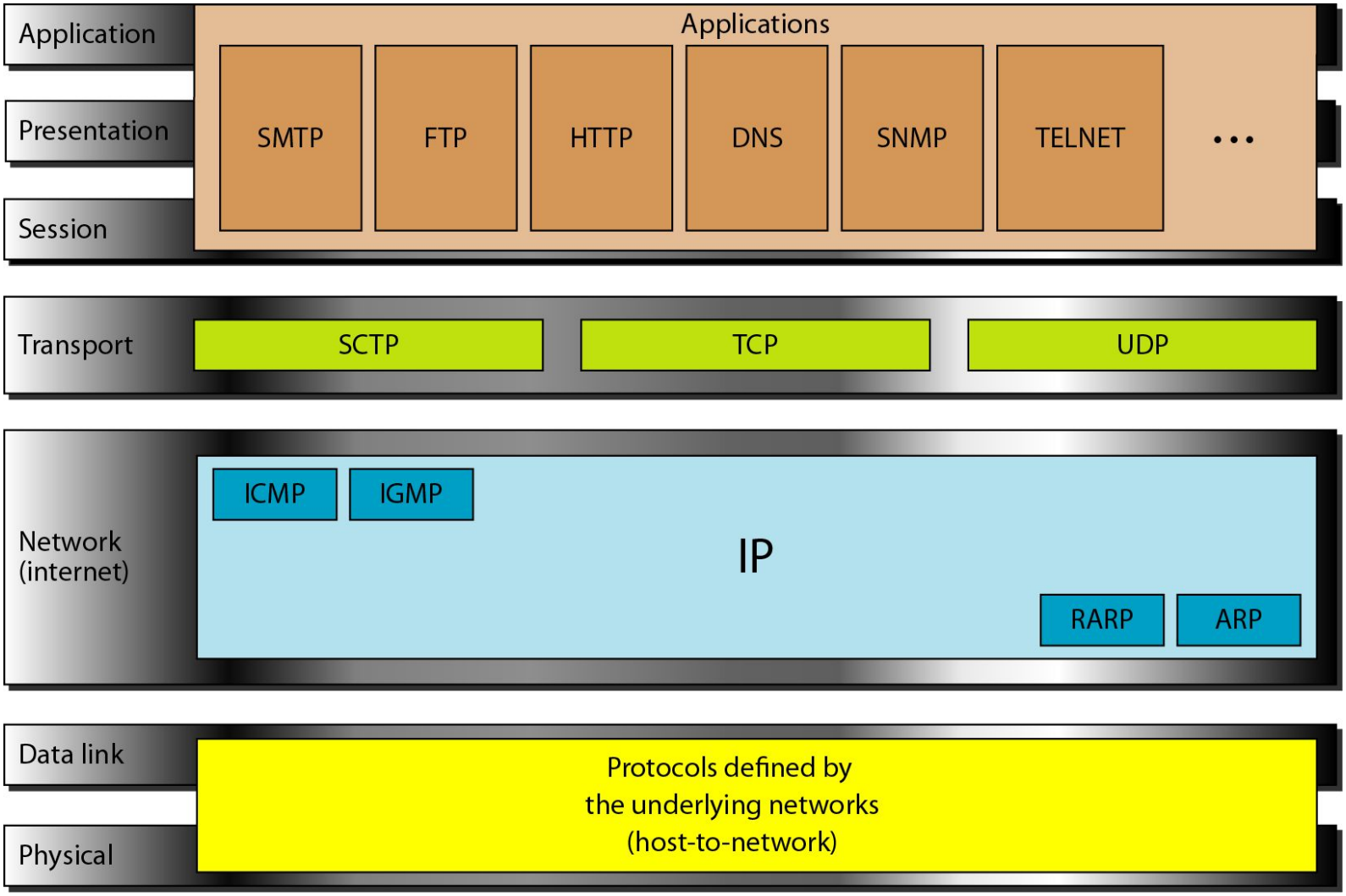


2-4 TCP/IP PROTOCOL SUITE

- The TCP/IP protocol suite was developed prior to the OSI model.
- **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.**

- The **host-to-network layer** is equivalent to the combination of the physical and data link layers.
- The **internet layer** is equivalent to the network layer.
- The **transport layer** in TCP/IP taking care of part of the duties of the transport layer.
- The **application layer** is roughly doing the job of the session, presentation, and application layers.
- *TCP/IP* is a **hierarchical protocol** made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- The term ***hierarchical*** means that each **upper-level protocol is supported by one or more lower-level protocols.**
- At the transport layer, *TCP/IP* defines three protocols: **Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).**
- At the network layer, the main protocol defined by TCP/IP is the **Internetworking Protocol (IP).**

Figure 2.16 *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**
  - At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol.
  - IP uses four supporting protocols: **ARP, RARP, ICMP, and IGMP.**
    - *Internetworking Protocol (IP)*
    - The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an **unreliable and connectionless protocol-a** best-effort delivery service. The term *best effort* means that IP provides no error checking or tracking.
    - IP transports data in packets called ***datagrams,*** each of which is transported separately.
    - Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
    - IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

- **Address Resolution Protocol**
  - The Address Resolution Protocol (ARP) is used to associate **a logical address with a physical address.**
  - On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC).
  - **ARP** is used to find the **physical address of the node when its Internet address is known.**
- **Reverse Address Resolution Protocol**
  - The Reverse Address Resolution Protocol (RARP) allows a **host** to **discover its Internet address** when it **knows only its physical address**.
  - It is used when a **computer is connected to a network for the first time** or when a diskless computer is booted.

- **Internet Control Message Protocol**
  - The Internet Control Message Protocol (ICMP) is a mechanism used by **hosts and gateways to send notification of datagram problems** back to the sender.
  - ICMP sends **query and error reporting messages**.
- **Internet Group Message Protocol**
  - The Internet Group Message Protocol (IGMP) is used to facilitate the **simultaneous transmission of a message to a group** of recipients.

- **Transport Layer**
  - Traditionally the transport layer was represented in *TCP/IP* by two protocols:
    - TCP and UDP.
  - **IP is a host-to-host protocol**, meaning that it can **deliver a packet from one physical device to another**.
  - **UDP and TCP** are transport level protocols responsible for delivery of a message from a **process (running program) to another process.**
  - A new transport layer protocol, **SCTP,** has been devised to meet the needs of some newer applications.

- **User Datagram Protocol**
  - The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols.
  - It is 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**
  - The Transmission Control Protocol (TCP) provides full **transport-layer services** to applications.
  - TCP is a reliable **stream transport protocol**.
  - The term *stream,* in this context, means **connection-oriented**: A connection must be established between both ends of a transmission before either can transmit data.
  - At the sending end of each transmission, TCP divides a stream of data into smaller units called ***segments***.
  - Each **segment** includes a **sequence number for reordering after receipt, together with an acknowledgment number for the segments received.**
  - Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream Control Transmission Protocol

- The **Stream Control Transmission Protocol (SCTP)** provides support for newer applications such as voice over the Internet.
- It is a transport layer protocol that **combines the best features of UDP and TCP.**

2-5 ADDRESSING

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

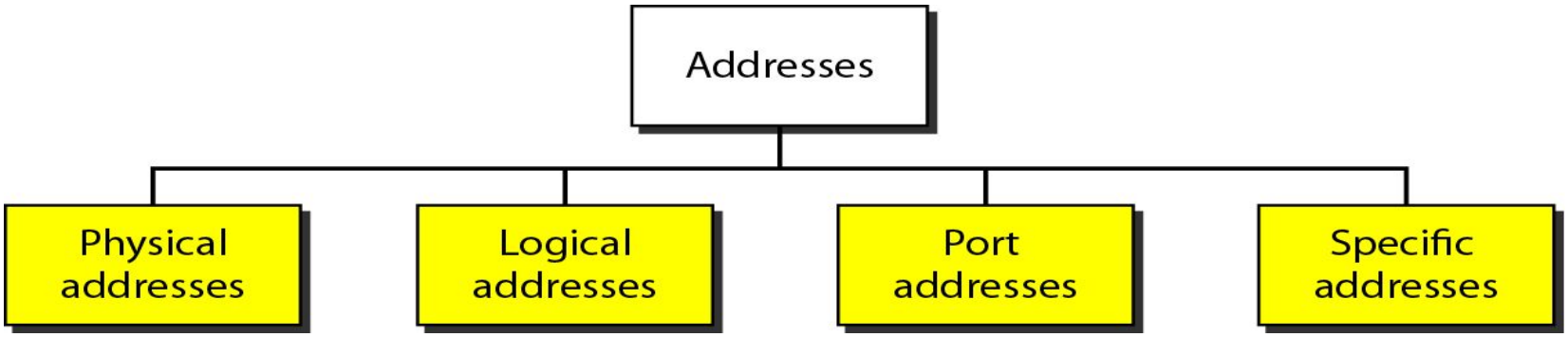
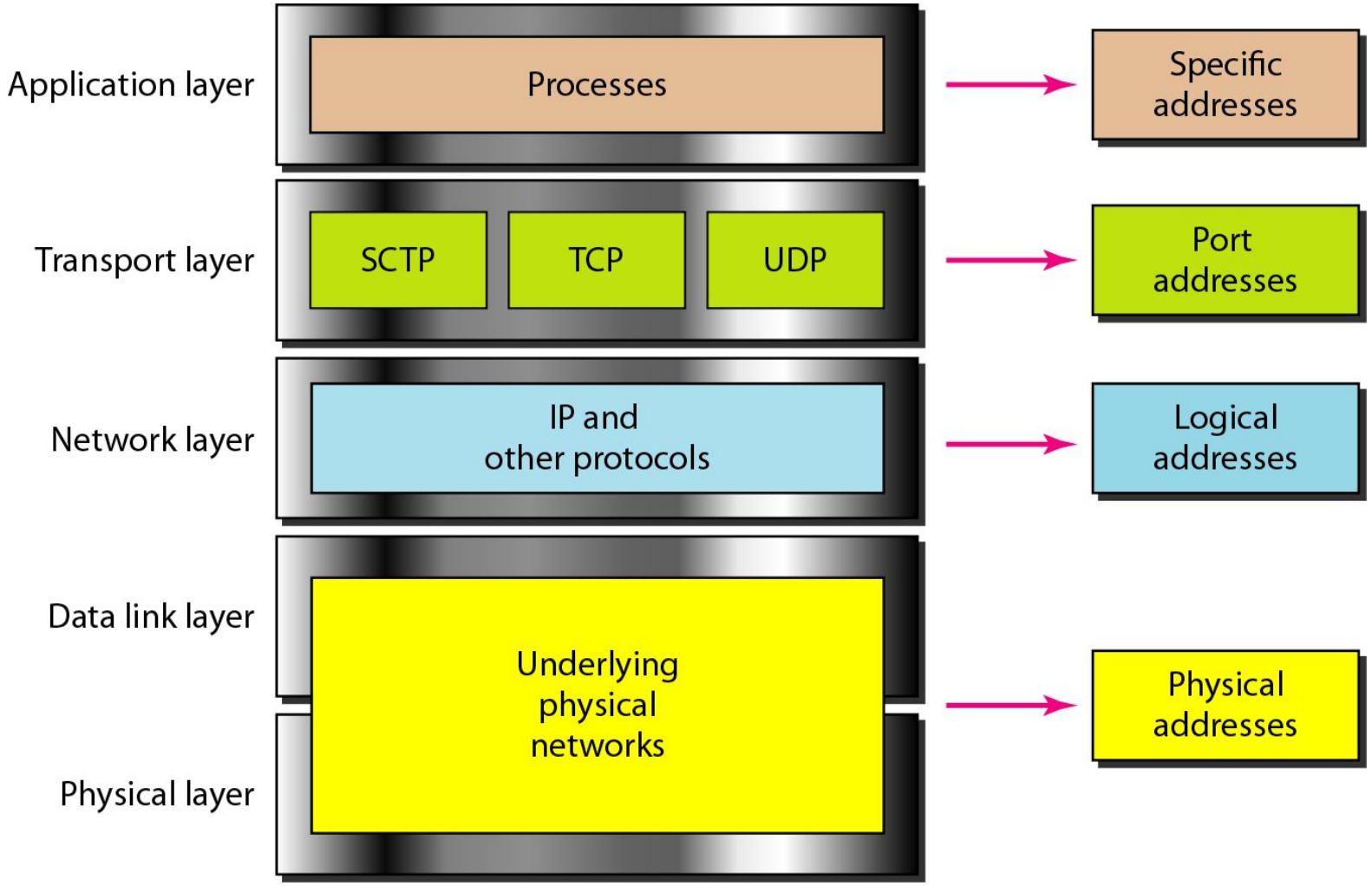


Figure 2.18 *Relationship of layers and addresses in TCP/IP*



Physical Addresses

- The physical address, also known as the **link address**, is the address of a node as defined by its LAN or WAN.
- It is included in the **frame used by the data link layer**. It is the **lowest-level address**.
- The physical addresses have **authority over the network** (LAN or WAN).
- The size and format of these addresses vary depending on the network.
- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). LocalTalk (Apple), however, has a I-byte dynamic address that changes each time the station comes up.

Logical Addresses

- **Logical addresses** are necessary for universal communications that are independent of underlying physical networks.
- **Physical addresses are not adequate** in an internetwork environment where different networks can have different address formats.
- A **universal addressing system is needed** in which each host can be identified uniquely, regardless of the underlying physical network.
- The **logical addresses are designed** for this purpose. A logical address in the Internet is currently a **32-bit address that can uniquely define a host connected to the Internet.**
- **No two** publicly addressed and visible **hosts on the Internet** can have the **same IP address**.

Port Addresses

- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host.
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- A system that sends nothing but data from one computer to another is not complete.
- Today, computers are devices that can run multiple processes at the same time.
- The end objective of Internet communication is a process communicating with another process.
- For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.
- In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A **port address** in TCP/IP is **16 bits in length**.

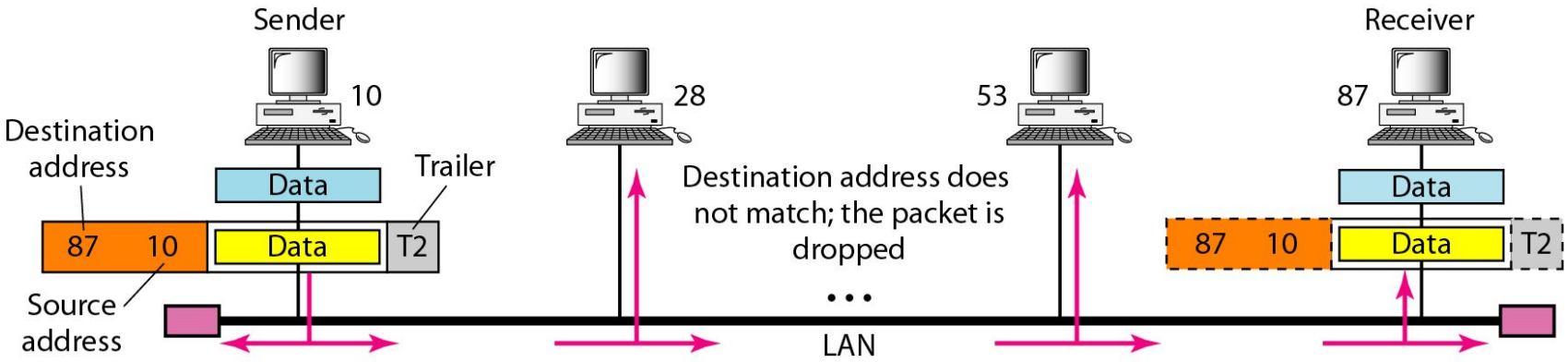
Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific address.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com).
- The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.
- These addresses, however, get changed to the corresponding port and logical addresses by the sending computer,

Example 2.1

In Figure 2.19 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.

Figure 2.19 *Physical addresses*

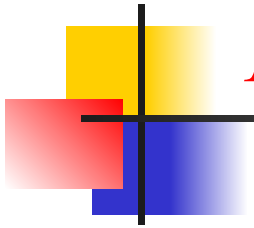


Example 2.2

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

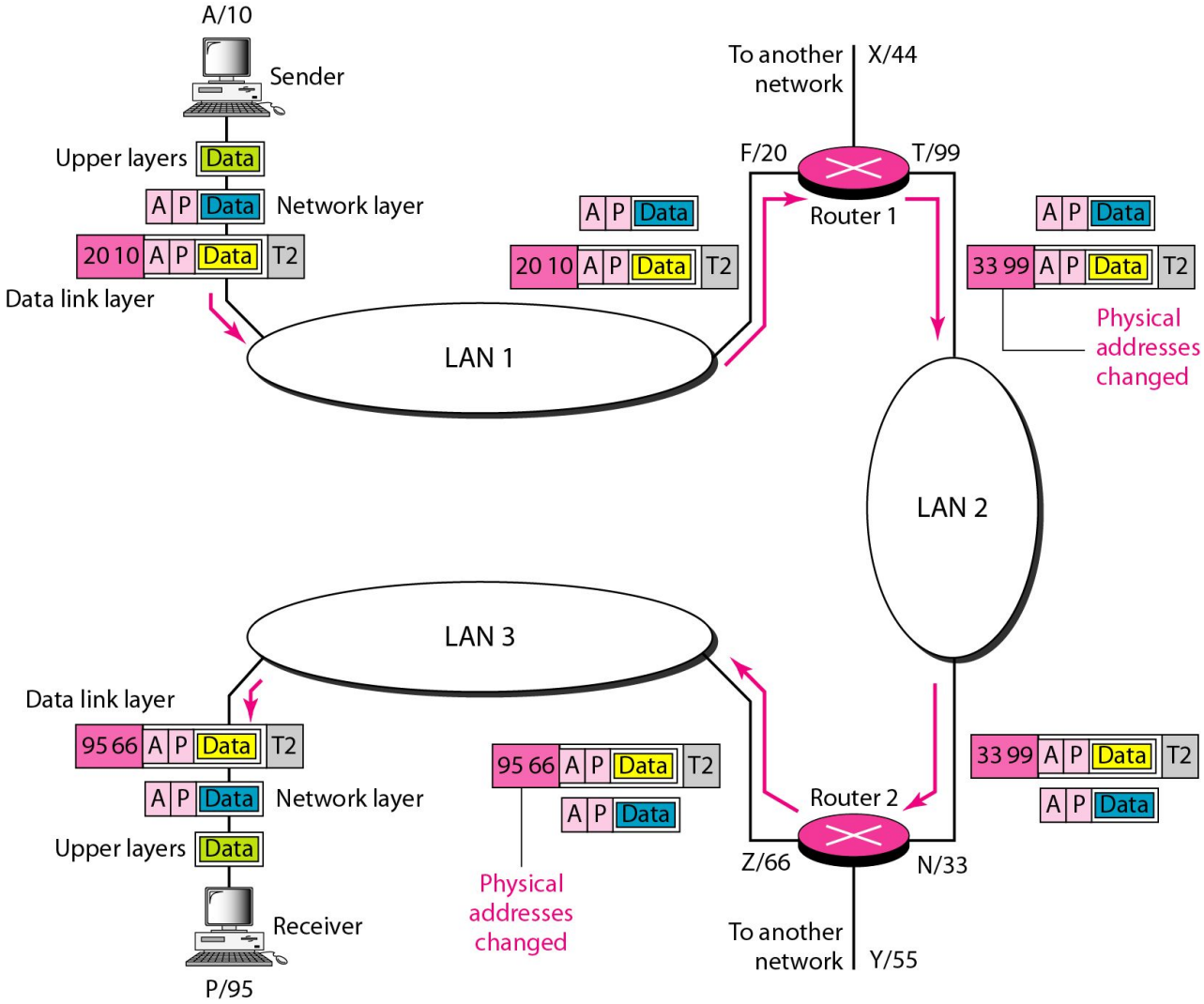
A 6-byte (12 hexadecimal digits) physical address.

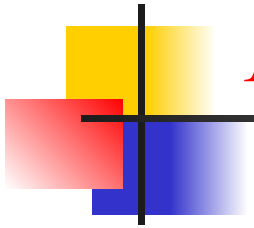


Example 2.3

Figure 2.20 shows a part of an internet with two routers connecting three LANs. 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.

Figure 2.20 *IP addresses*

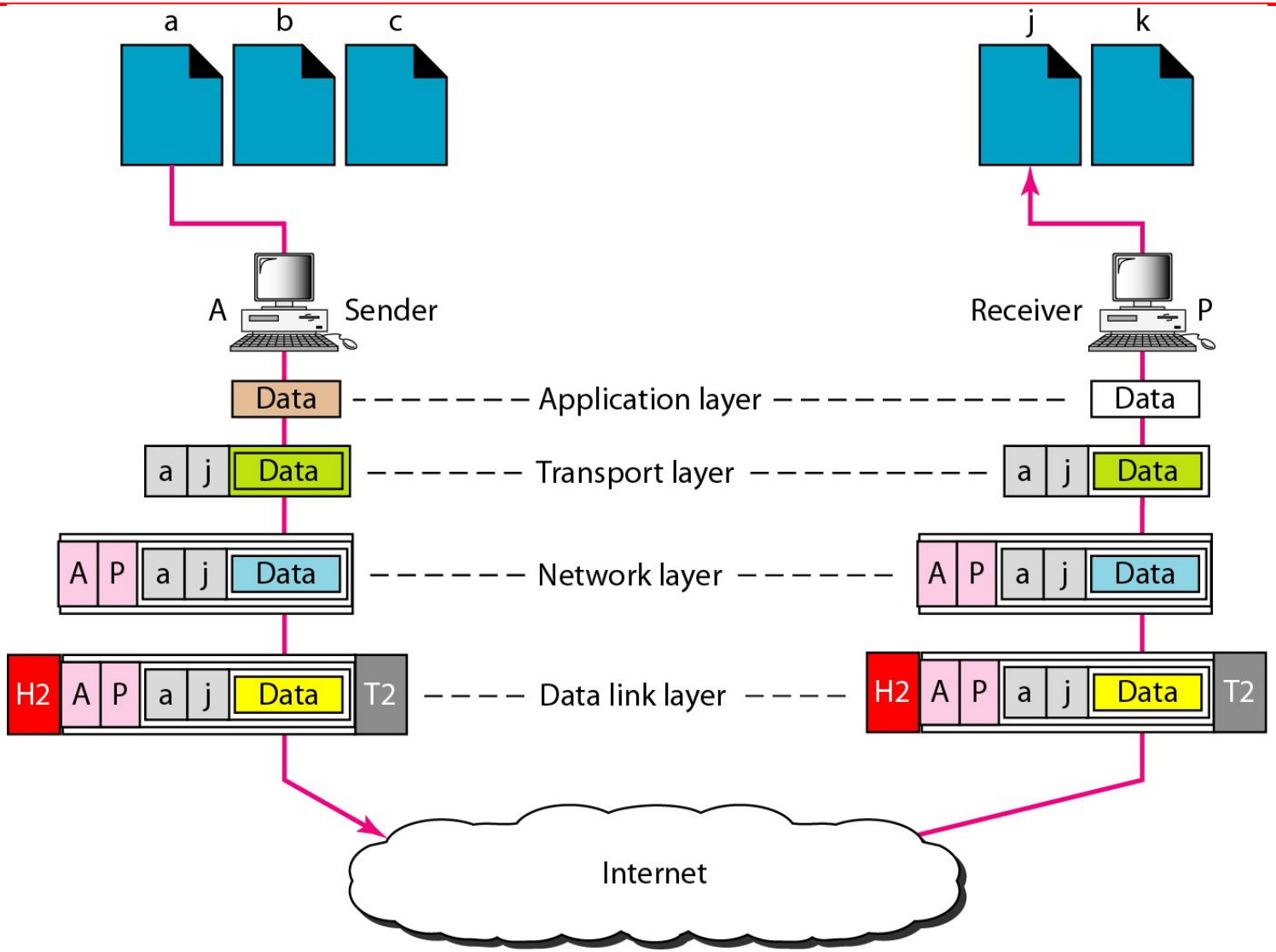




Example 2.4

Figure 2.21 shows two computers 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.

Figure 2.21 *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.