COMPUTER NETWORK ENGINEERING

- What is computer networks?

Ans) A group of computers interconnected for the purpose of sharing resources.

- Why do you need to study this subject?
- Which is the most important Resource in the world?

  Gold or Oil?

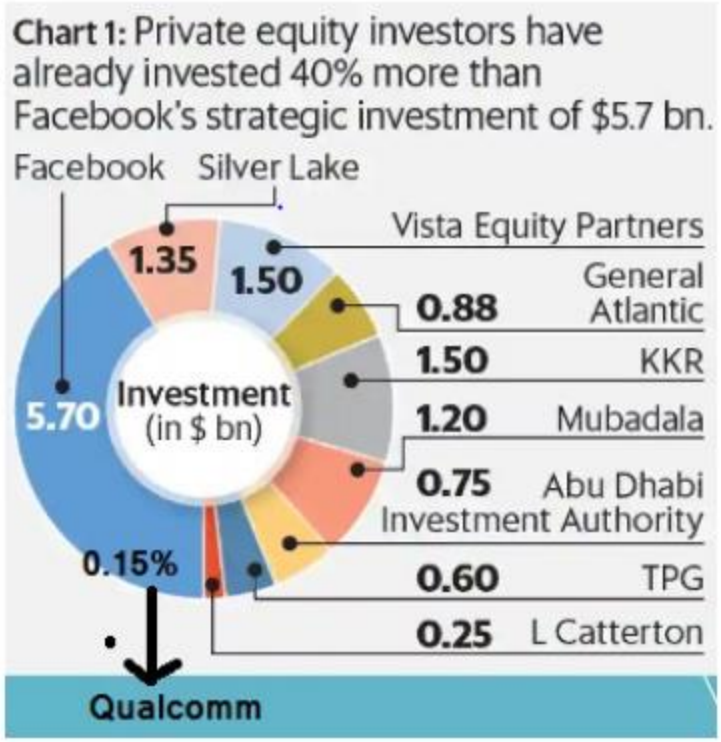
  Is oil the most valuable resource in 2020?

https://www.marketwatch.com/investing/future/crude%20oil%20-%20electronic

- Which is the most valuable resource then?

Ans) DATA

- Examples : Amazon,Facebook,Cambridge Analytica, Reliance.



- https://www.moneycontrol.com/india/stockpricequote/refineries/relianceindustries/RI
- Internet is the biggest example of a computer network.
- Importance of Internet?

Internet in our daily life:

https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#1.1.1.1

- The need to interact with others ranks just below our need to sustain life.
- Communication is almost as important to us as our reliance on air, water, food, and shelter.
- Connected like never before.
- Instant Communication.
- News events and discoveries are known worldwide in seconds.

Applications(Advantages) of computer networks(Internet) : A few

- E- Commerce: online shopping(Buy and Sell).
- Networks support the way we learn: Online Education
- Networks support the way we communicate: Email, Social Media.
- Networks support the way we work: Online Jobs
- Networks Support the Way We Play: Entertainment

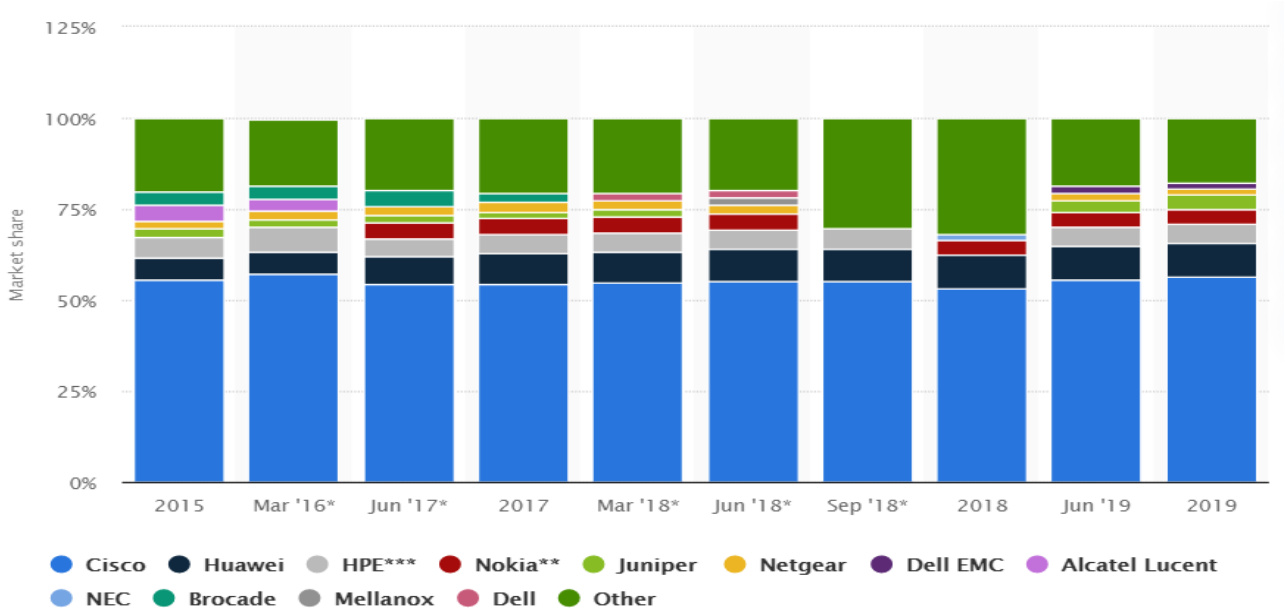
Technology then and now:

https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#1.1.1.2

- Does learning computer networks help in getting a job?
- Networking jobs can be pursued by completing certifications.

Examples: CCNA(Cisco Certified Network Associate).

- Cisco systems is a fortune 500 company and a pioneer in networking solutions.



- Cisco Networking Academy offers online certifications for students.
- S.R.K.R. is Cisco Networking Academy.

- **Learning Outcomes(what will you learn from this subject?):**

1. Explain basic computer network principles and layers of the OSI model and TCP/IP.
2. Explain the concepts of transmission media, switching and multiplexing techniques.
3. Explain and analyze the error control and flow control methods.
4. Explain different multiple access control protocols and IEEE Standards for LANS and MANS.
5. Identify the different types of connecting devices and explain the basic concepts of congestion control algorithms and internetworking.
6. Explain TCP and UDP header formats.

- **Broadly u can understand**

1. How Internet works.
2. The rules, procedures and technologies that help in transmitting data across Internet.

Syllabus

- UNIT-I : Uses of Computer Networks, Line Configuration, Topology, Transmission mode, Categories of Networks-LAN, MAN, WAN; Network Software- Protocol Hierarchies, Design issues of layers, Connection Oriented and Connectionless services; Reference Models- The OSI Reference Model, The TCP/IP Reference Model, The B-ISDN ATM Reference Model.
- UNIT-II: **PHYSICAL LAYER :**Theoretical basis for Data communication, Transmission media- Guided and Unguided Transmission media; The Telephone System-Structure of Telephone system, Trunks and Multiplexing, Frequency Division Multiplexing, Time Division Multiplexing, Switching- Circuit Switching, The Switch Hierarchy, Crossbar switches, Space Division Switches, Time Division Switches; Narrow band ISDN, Broadband ISDN and ATM- Virtual Circuits versus Circuit Switching.
- UNIT-III: **DATA LINK LAYER:** Design issues, Error Detection and Correction, Elementary Data link protocols, Sliding window protocols, HDLC, Medium access sub layer-The Channel allocation problem, Multiple Access Protocols-ALOHA, Carrier Sense Multiple Access protocols; IEEE standard for 802 LANs, Satellite Networks.
- UNIT-IV: **NETWORK LAYER:** Design considerations, Difference between Gateways, Ethernet switch, Router, Hub, Repeater, Congestion Control algorithms- General principles of Congestion Control, Congestion prevention policies. The Leaky bucket algorithm and Token bucket algorithm, The Network Layer in the Internet- The IP Protocol, IP Addresses.
- UNIT-V: **TRANSPORT LAYER:** The Transport layer Service, Elements of Transport protocols, The Internet Transport Protocols- UDP, TCP.
  APPLICATION LAYER: The Domain Name System, Electronic mail, The World Wide Web.

- **Learning Resources and Teaching Aids:**

1. Computer Networks, Tanenbaum.
2. Data Communications and Networking, Behrouz A. Forouzan.
3. Simulation Tools(Cisco Packet Tracer, Wireshark).
4. Regular Assessments(Quizzes and Assignments).

Basics of DATA communications

- The term ***telecommunication,*** which includes telephony, telegraphy, and television, means communication at a distance *(tele* is Greek for "far").

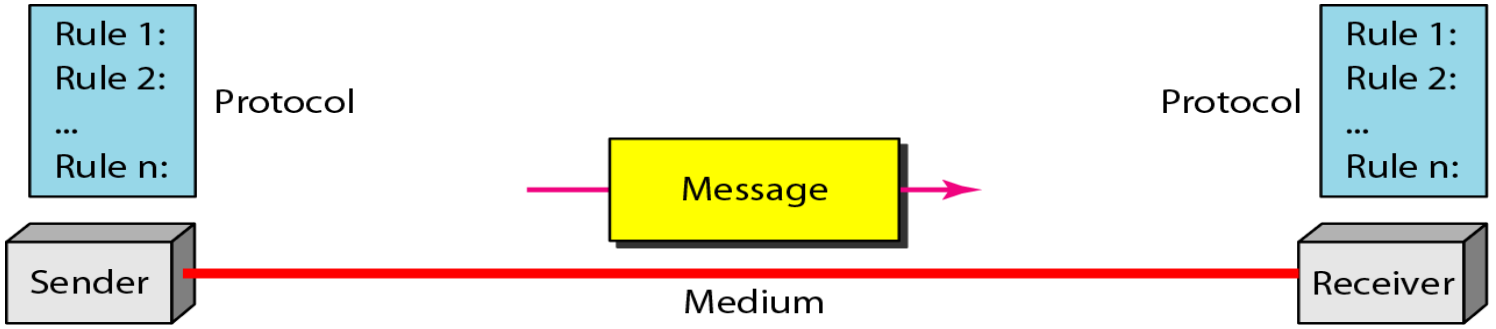
- The word ***data*** refers to information presented in whatever form is agreed upon by the parties creating and using the data.

- DATA can be of the form

1. *Text*
2. *Images*
3. *Audio*
4. *Video*

- Data communications is the exchange of data between two or more devices via some form of transmission medium such as a wire cable, which is the simplest form of a network.

- **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, mobile, telephone handset, video camera, and so on.
- *Receiver:* The receiver is the device that receives the message. It can be a computer, mobile, 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.

- The effectiveness of a data communications system depends on four fundamental characteristics:

Delivery. The system must deliver data to the correct destination.

Accuracy. The system must deliver the data accurately.

Timeliness. The system must deliver data in a timely manner.

Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

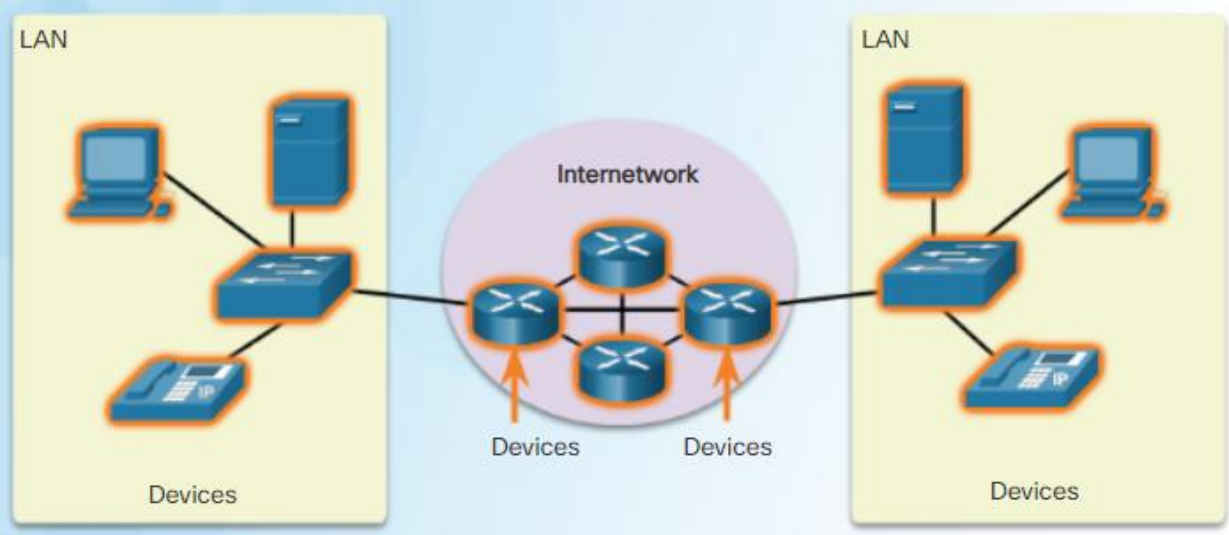
- The network infrastructure contains three categories of network components:

  Devices (Network Hardware)

  Media (Network Hardware)

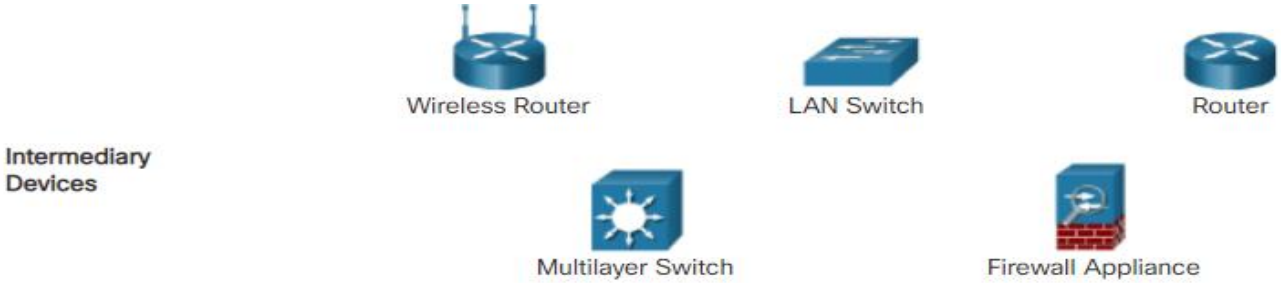
  Protocols, services (Network Software)

- Network Components – Devices



- Devices include both End devices and Intermediate devices.
- End Devices are the most familiar.
- An end device is either the source or destination of a message transmitted over the network.
- https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#1.2.1.2

- Intermediary Network Devices

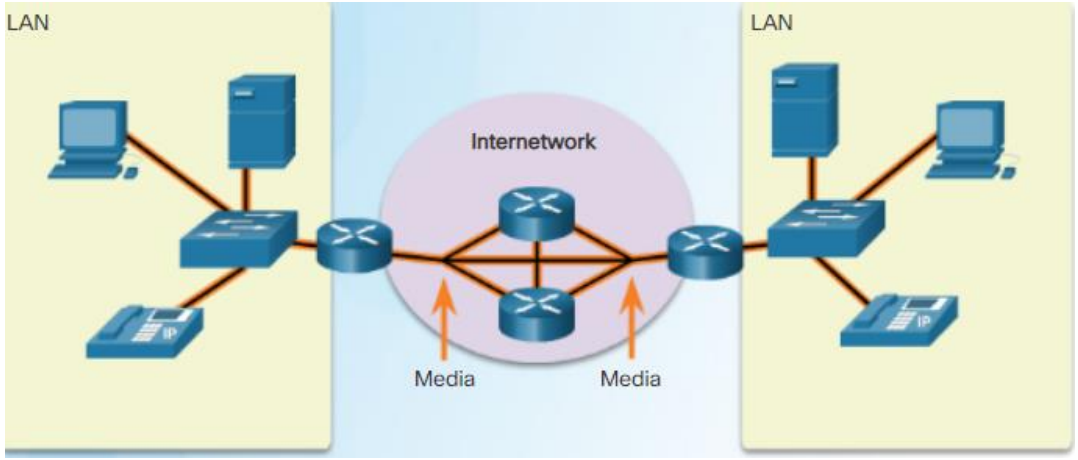


Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork.

Intermediary network devices perform some or all of these functions:

- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to priorities
- Permit or deny the flow of data, based on security settings

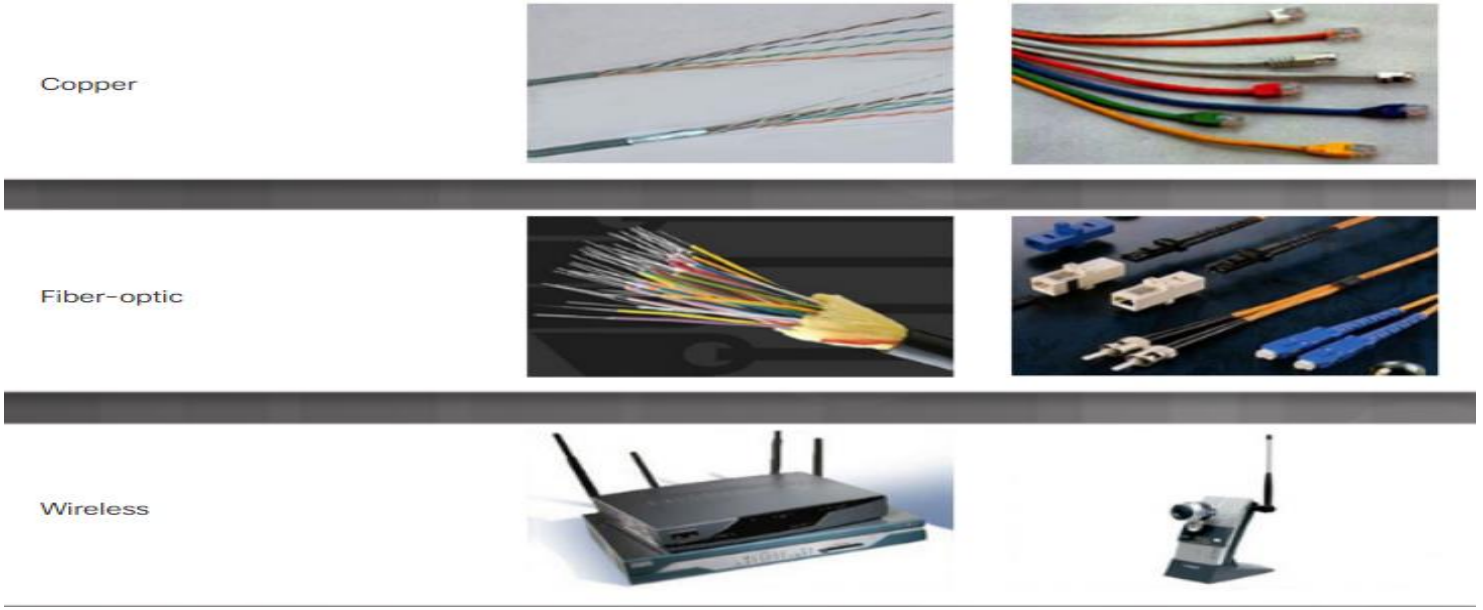
- Network Media



- The medium provides the channel over which the message travels from source to destination.
- The choice of Network Media is based on:

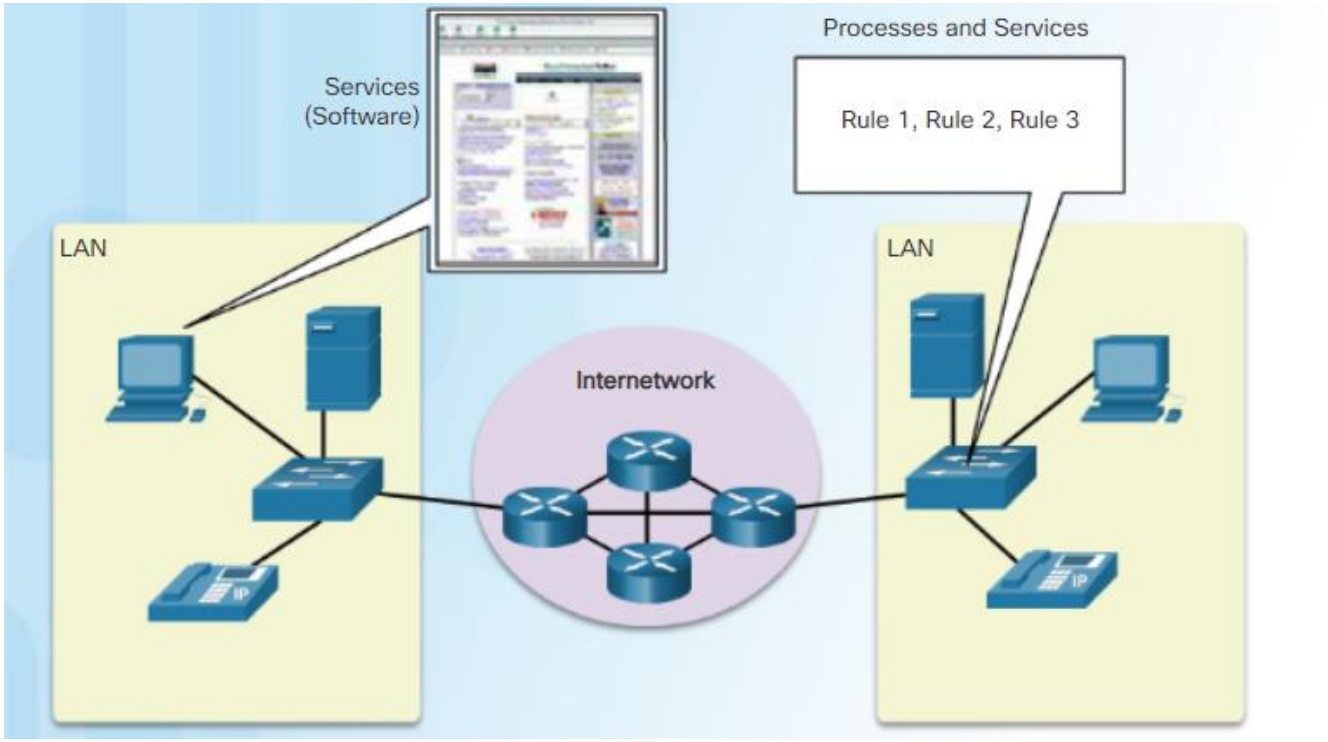
i) The distance that the media can successfully carry a signal.
ii) The environment the media will installed.
iii) Speed of data transmission.
iv) The cost of media and installation.

- **Types of Network Media**



- **Metallic wires within cables** - data is encoded into electrical impulses
- **Glass or plastic fibers (fiber optic cable)** - data is encoded as pulses of light
- **Wireless transmission** - data is encoded using wavelengths from the electromagnetic spectrum

- Network Software



- Includes services, protocols(processes).
- Services include many of the common network applications people use every day, like email hosting services and web hosting services.
- Protocols provide the functionality that directs and moves the messages through the network. Protocols are less obvious to us but are critical to the operation of networks.

Computer Network Terminologies(Hardware)

- Data Flow
- Line Configuration(Type of Connection)
- Topologies
- Types of Networks

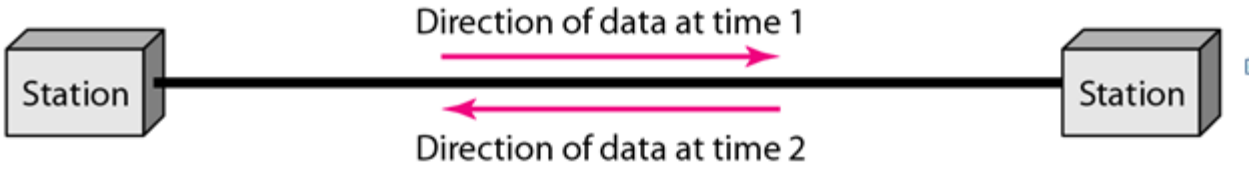
- *Data Flow:* Communication between two devices can be either simplex, half duplex or full duplex.

  Simplex mode: Communication is unidirectional.

Only one device on a link can transmit, the other can only receive.

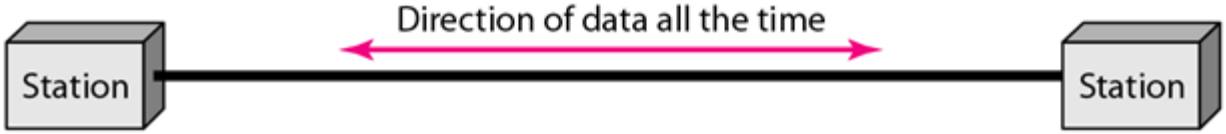
Ex: Keyboards, Monitors, Mouse, Printers, Scanners etc.

- Half Duplex Mode: Both the devices can transmit and receive but not at the same time.



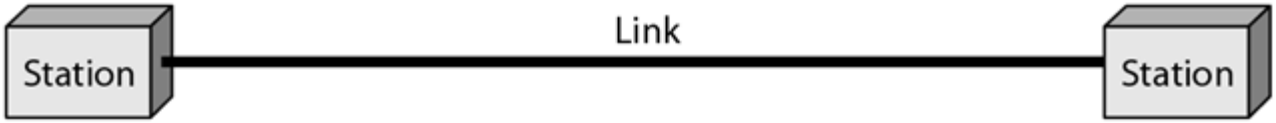
- https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#4.4.3.2
- When one device is sending, the other can only receive and vice versa.
- Ex: Walkie-Talkies, Citizen band radios.

- Full Duplex Mode: Both the devices can transmit and receive simultaneously.



- Ex: Mobile Communications, Internet Communication.

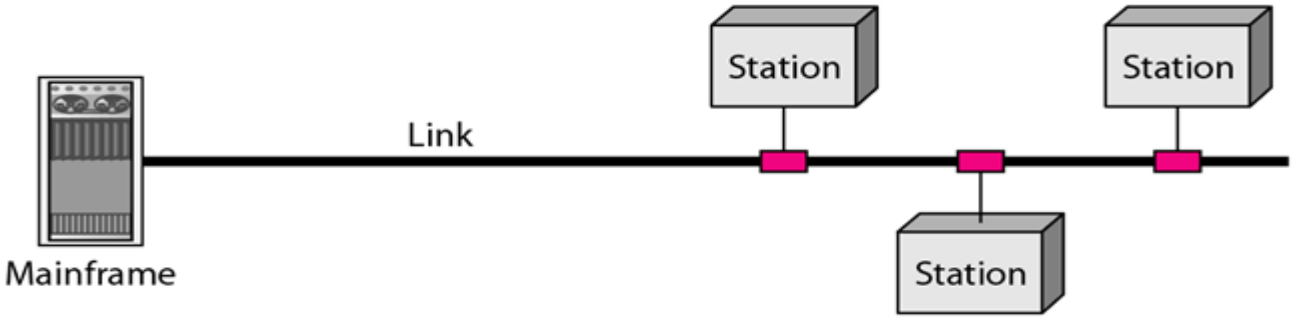
- ***Line configuration(Type of connection):*** It refers to the way two or more devices attached to a link.
- Point to point link:



Provides a dedicated link between only two devices.

The entire capacity of the link is reserved for transmission between these two devices.

- Multi Point link:



More than two devices share a single link.

The capacity of the link is shared, either spatially or temporarily.

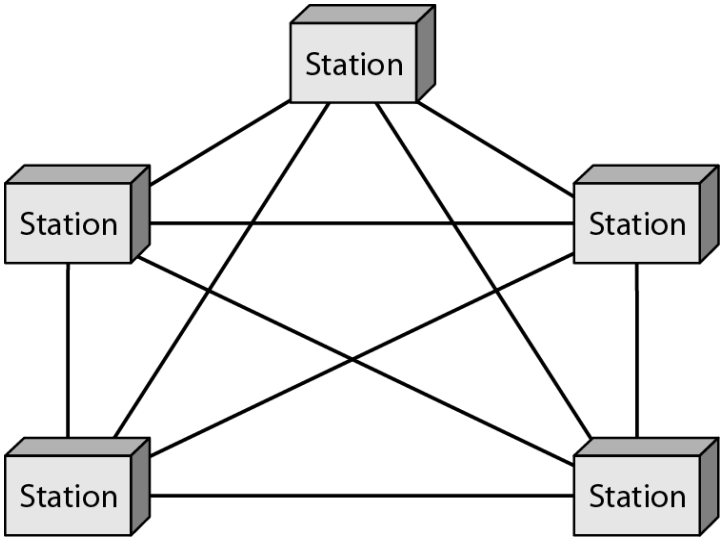
- Spatial sharing: several devices share the link simultaneously.
- Time sharing: Devices take turns in using the link.

- ***Topology:***
- It is a geometrical representation of the links and devices.
- Two or more devices connect to a link, two or more links form a topology.

- Four basic Topologies:

1) Mesh Topology
2) Star Topology
3) Bus Topology
4) Ring Topology
5) Hybrid Topology

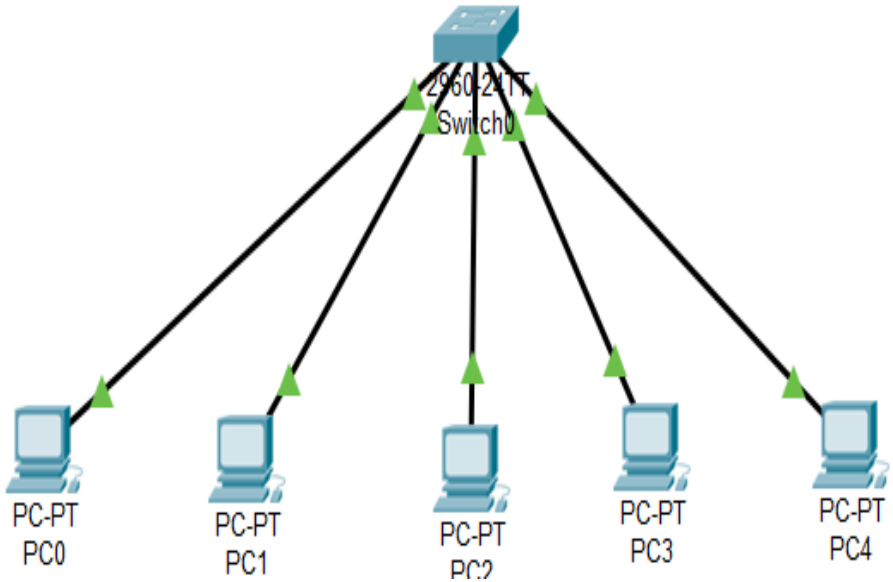
- **Mesh Topology:**



- Every device has a dedicated point to point link to every other device.
- For n devices n(n-1)/2 links are needed.
- For each device n-1 input/output ports are required.

- **Merits:**
- Eliminates Traffic problems.
- It is Robust.
- Privacy or security.
- Easy fault identification and isolation.
- **Demerits:**
- More amount of cabling and I/O ports required.
- Installation and reconnection are difficult.
- Usually implemented as a backbone network.

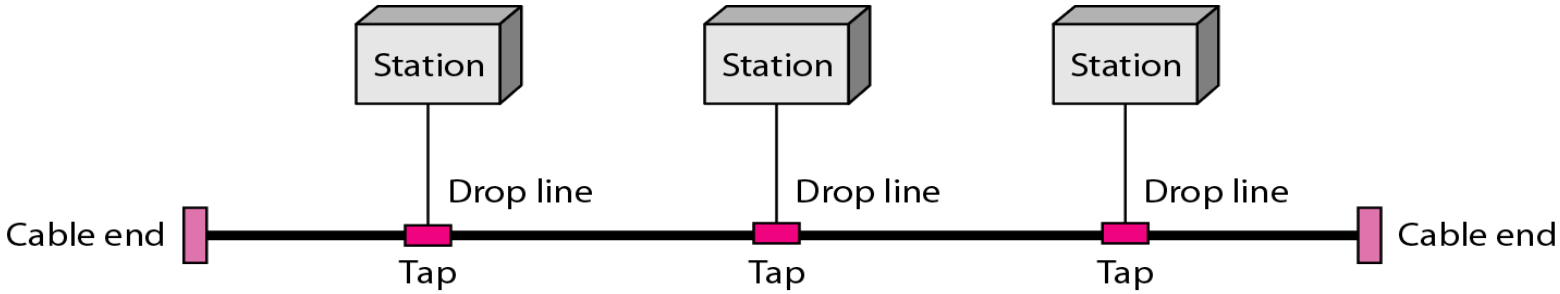
- **Star Topology:** Each device has a dedicated point to point link only to a central controller, usually a switch.
- No direct link or traffic between devices.
- The switch relays the data between devices.



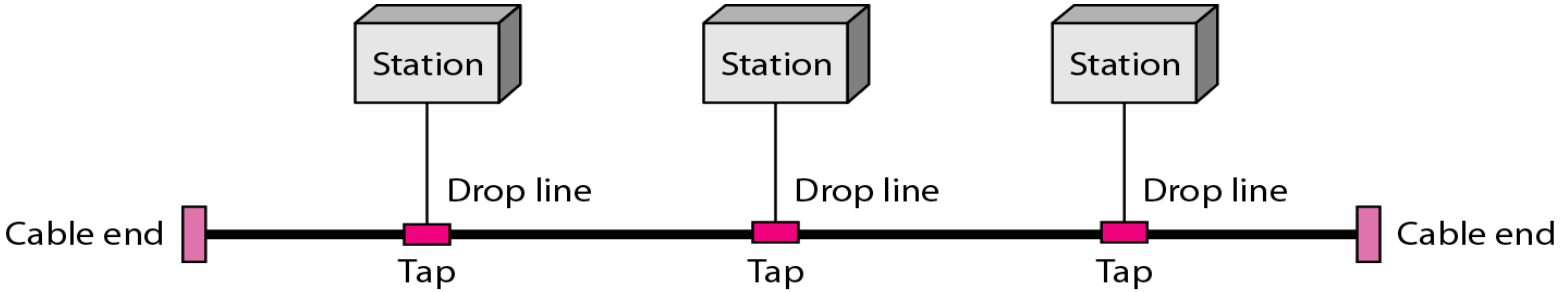
- **Merits:**
- Less expensive than a mesh topology.
- Less cabling than mesh topology.
- Each device needs only one link and one I/O port.
- Easy to install and reconfigure.
- If one link fails, only that link is affected.
- Easy fault identification and isolation.

- **Demerits:**
- Dependency of whole topology on one single device. If the switch goes down, the network goes down.
- Requires more cabling than some other topologies.
- Mainly used in LANs.

- **Bus Topology:**



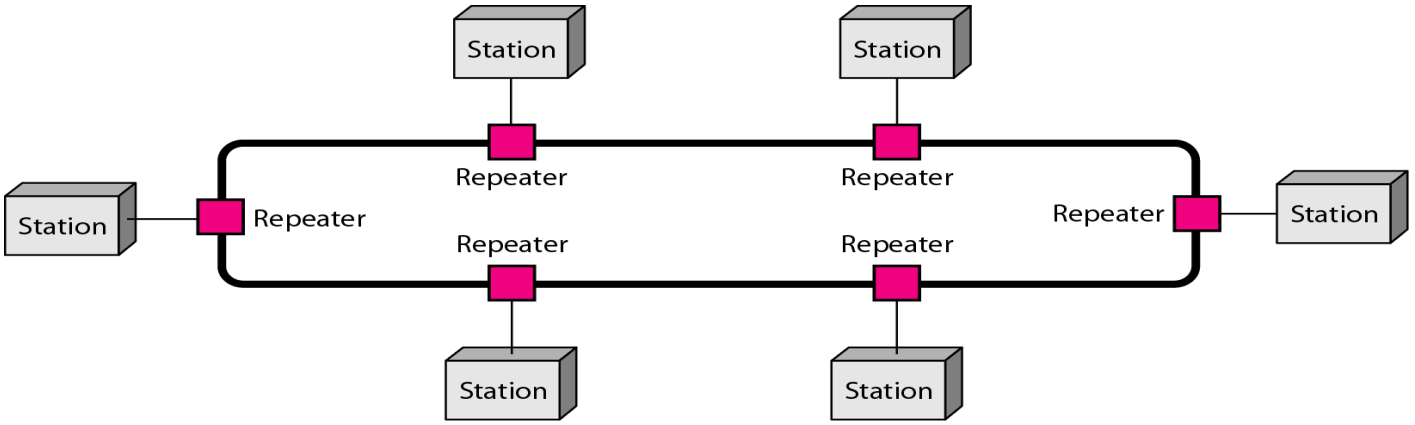
- It is a multipoint link. All devices are connected to a single link.
- Devices are connected to the bus cable by drop lines and taps.
- A drop line is a connection between the device and the main cable.
- A tap is a connector that slices into the main cable.



- **Merits:**
- Ease of installation
- Less cabling than mesh or star topologies

- **Demerits:**
- Difficult fault isolation and reconnection
- Fault or break in the bus cable stops multiple transmissions.
- Limit on number of taps
- Difficult to add new systems.
- Ethernet LANs use bus topology

- **Ring Topology:**

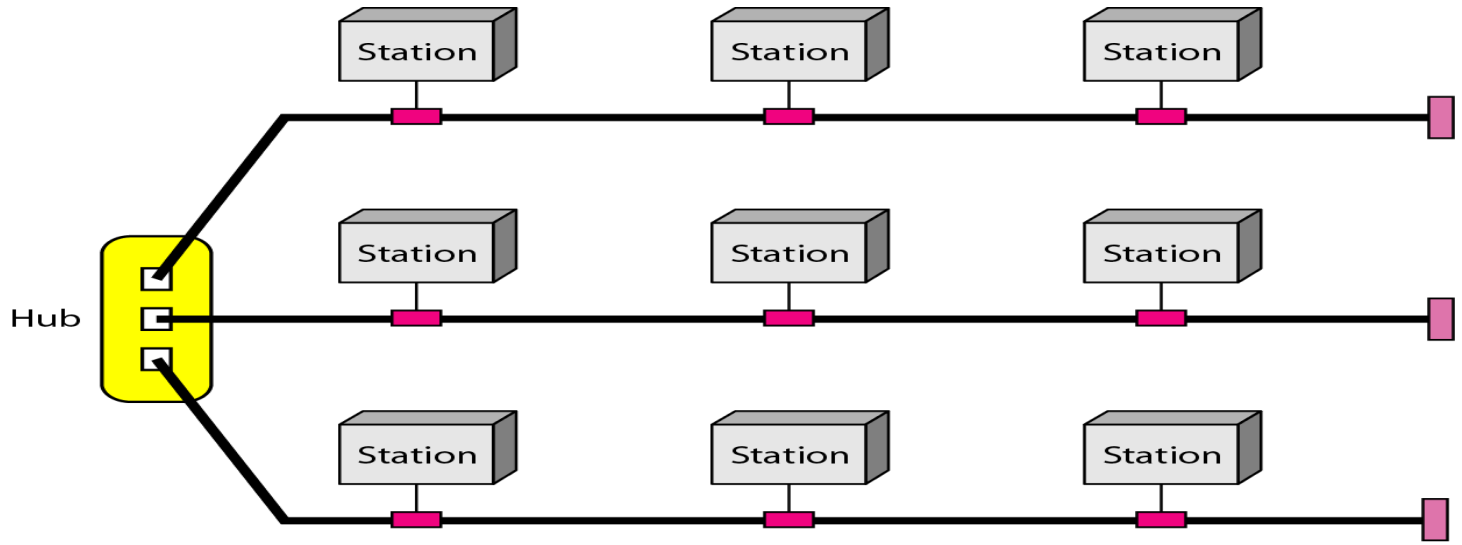


- Each device has a dedicated point to point link with only two devices on either side.
- A ring is relatively easy to install and reconfigure.
- Fault isolation is simplified.
- Maximum ring length and number of devices are constraints.
- Unidirectional traffic can be disadvantage.
- In a simple ring, a break in the ring can disable the entire network.

- **Message Delivery options:**
- Unicast: One to one delivery

- Broadcast: One to all delivery
- Multicast: One to many delivery
- https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#3.1.1.7

- **Hybrid Topology:** Consists a combination of two or more different topologies.



- **Types of Networks**

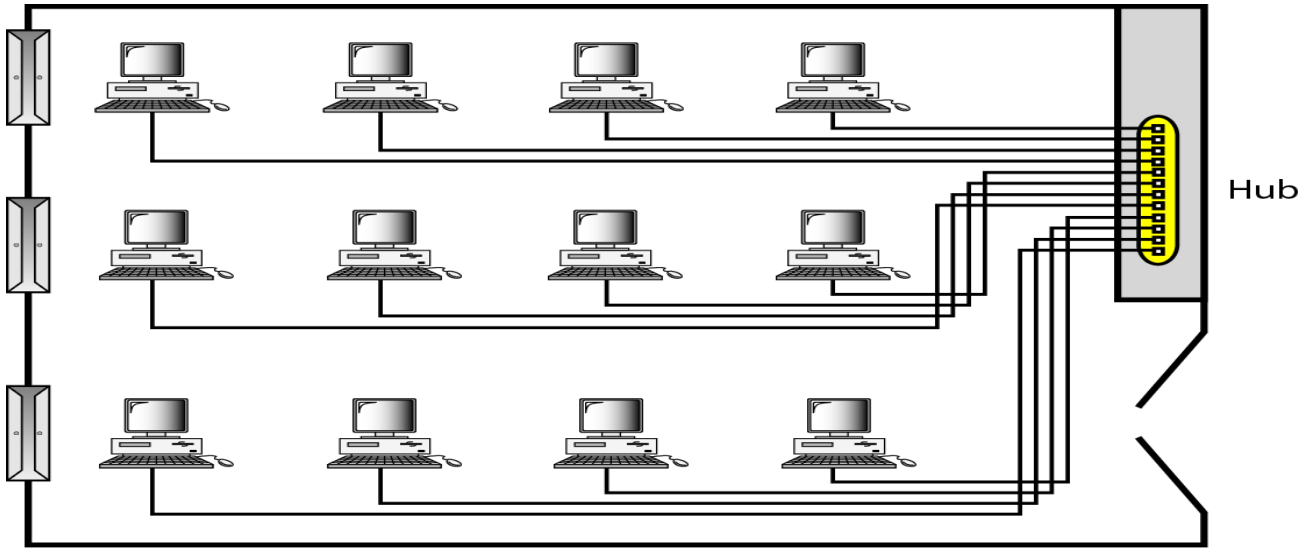
- Different categories of networks include

1. Local Area Networks(LAN)
2. Wide Area Networks(WAN)
3. Metropolitan Area Networks(MAN)

- Each type of network is classified based on

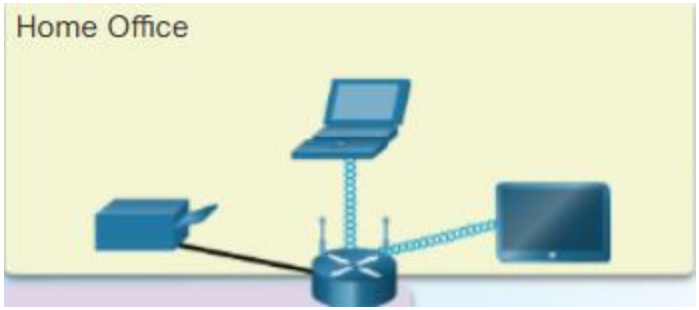
1. Size of the area covered.
2. Number of users connected.
3. Number and types of services or recourses shared.
4. Type and area of ownership.

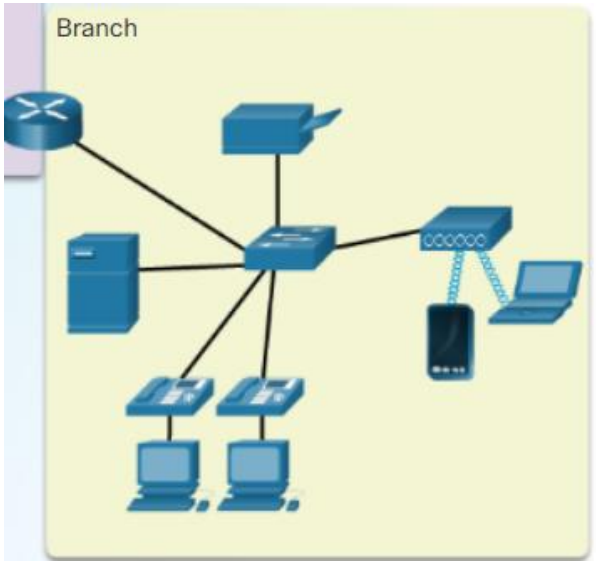
- **Local Area Network**

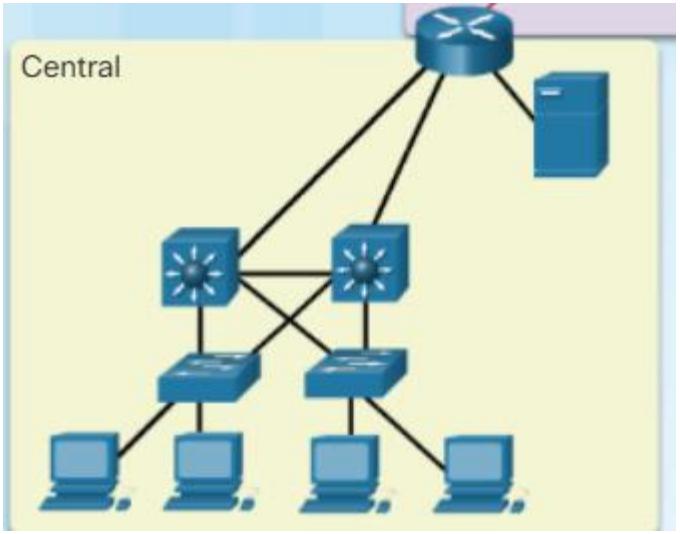


- LANs span a small geographical area, typically limited to few kilometres.
- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
- A LAN is usually privately owned and administered by a single organization or individual.
- Used to share resources between devices. Shared resources include hardware(printer, scanner), software(an application program).

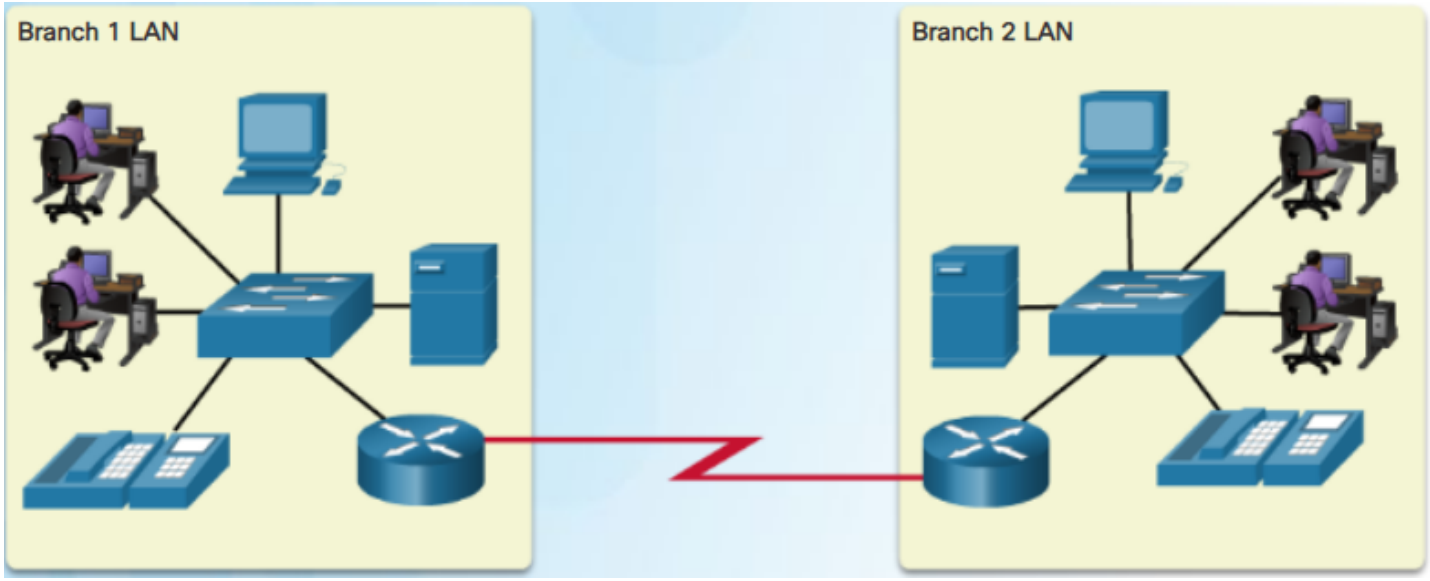
- Examples: A single system connected to a printer, devices connected throughout a campus.
- A LAN may also be distinguished by licensing restrictions, type of transmission media and topology.
- Common LAN topologies include star, bus and ring.





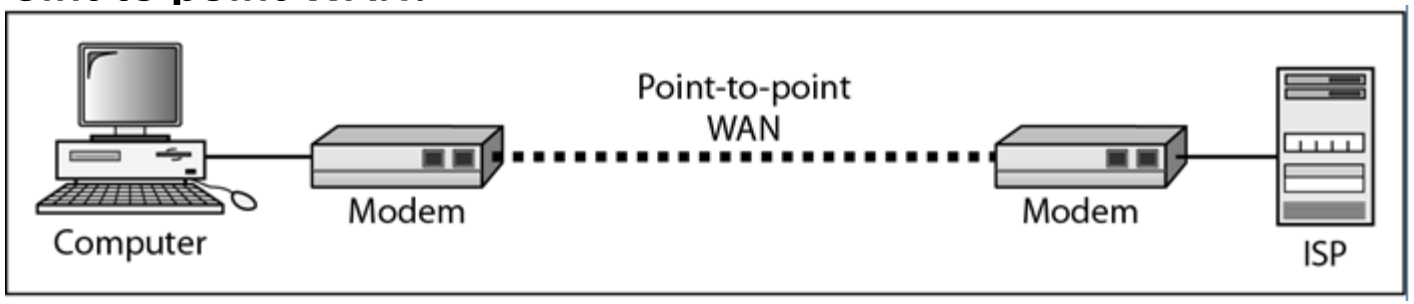


- **Wide Area Network**
- WANs are a network infrastructure that span a wide geographical area.

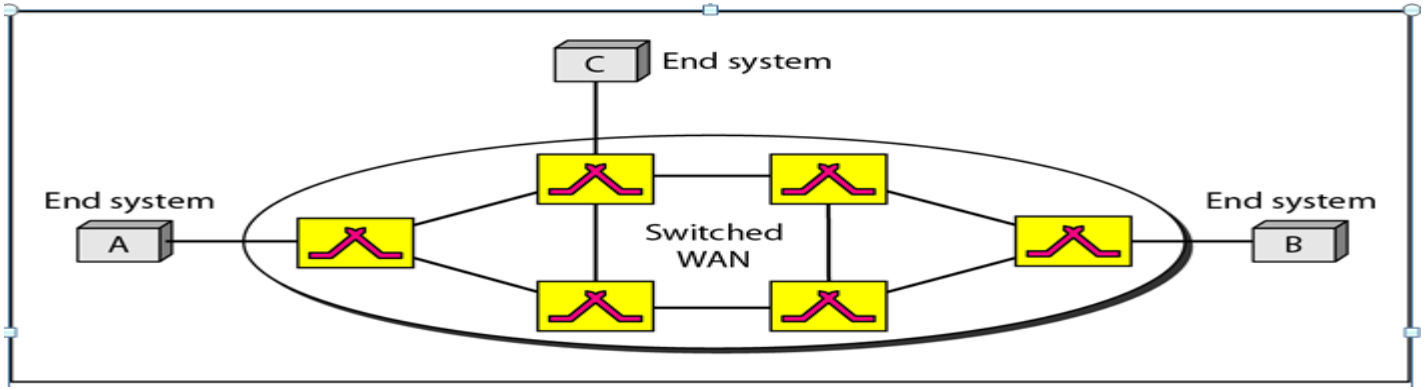


- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- A WAN connection is generally publicly owned by service providers.
- A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.

- **Point to point WAN:**



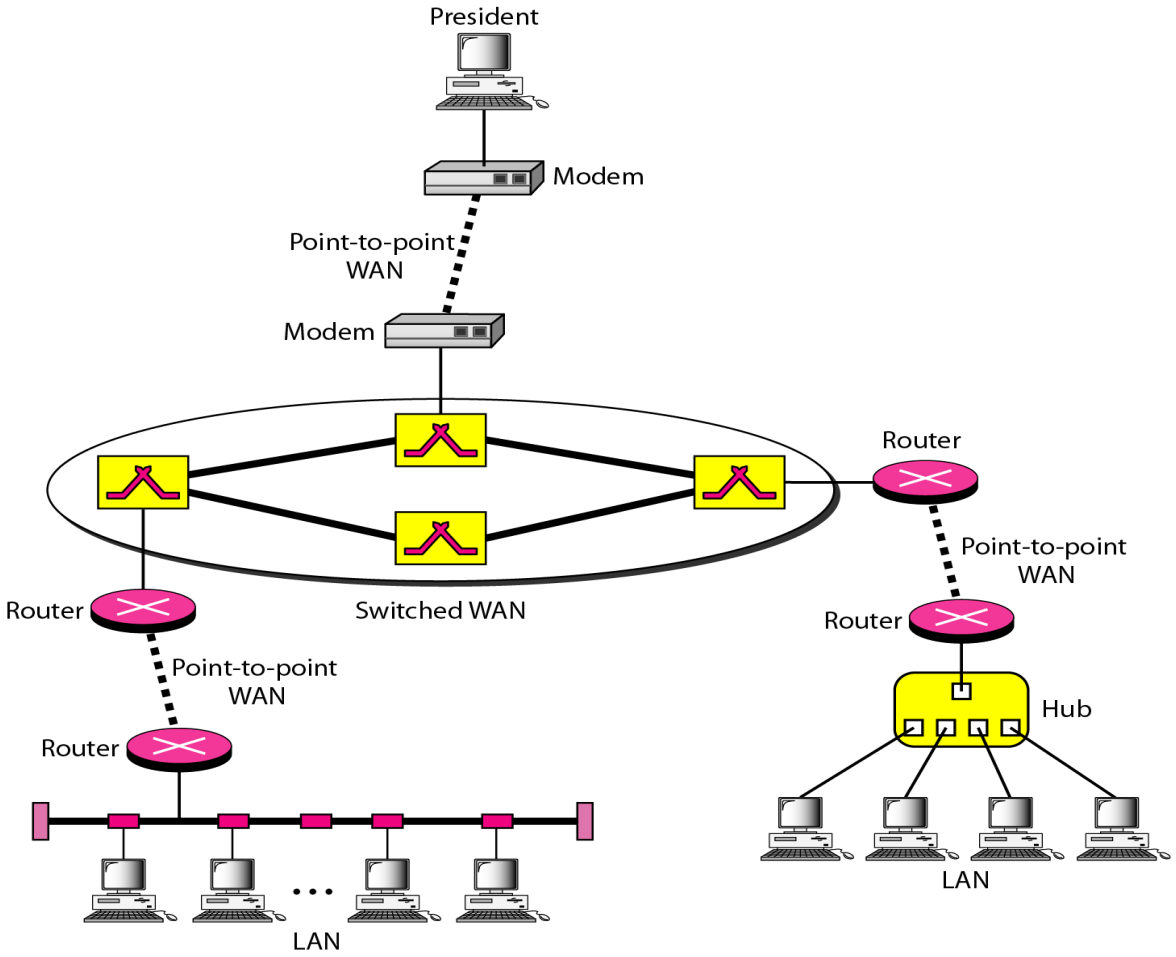
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP).
- This type of WAN is often used to provide Internet access.
- **Switched WAN:**
- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.



- A switched WAN is the backbone that connects the Internet.
- Ex: X.25, Frame relay, ATM(Asynchronous Transfer Mode).

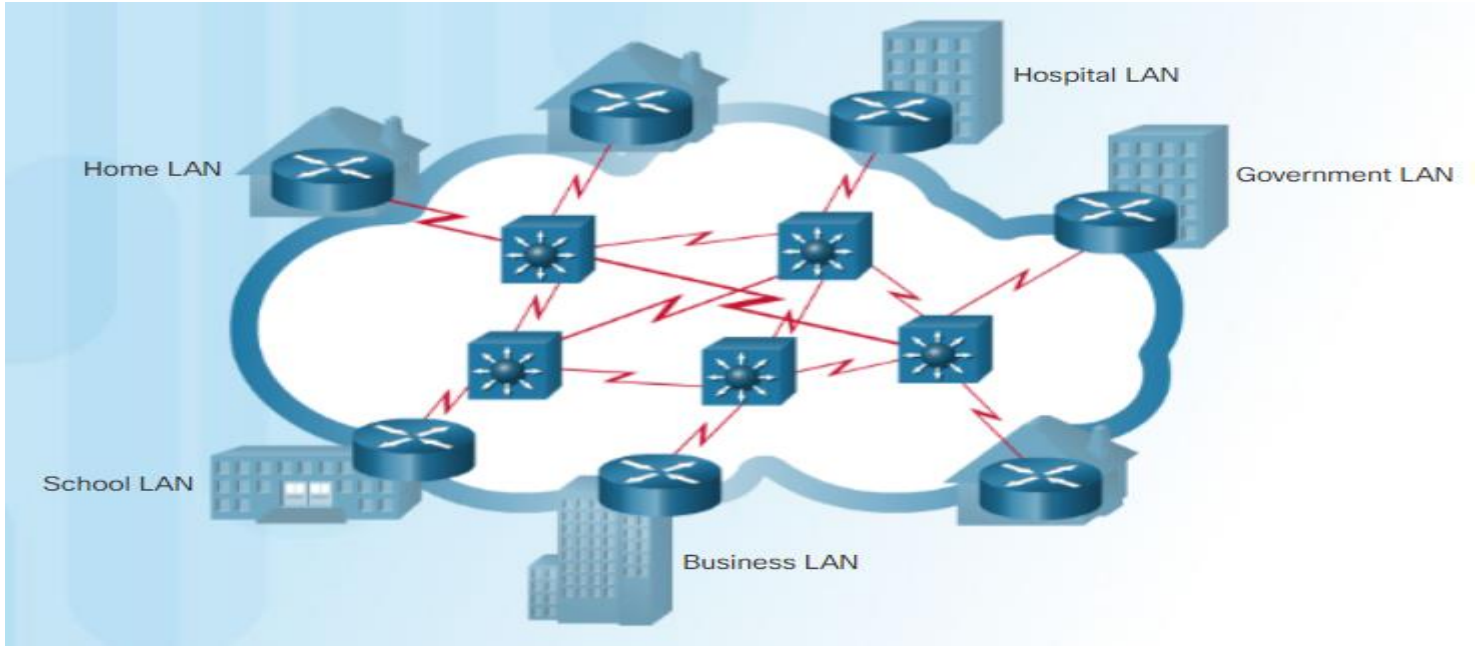
- **Metropolitan Area Network:**
- A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city).
- It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.
- One example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.
- MANs are typically operated by a single entity such as a large organization.

- **Internetwork:**
- When two or more networks are connected, they become an internetwork.



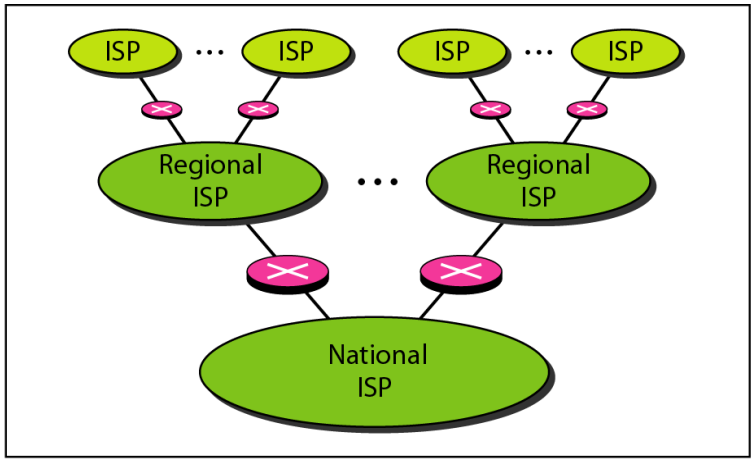
- A network is a group of devices connected together.
- An internetwork is two or more networks connected together.
- The most notable internetwork is the Internet we use daily, which is a collaboration of millions of interconnected networks.

- It is an interconnection of millions of LANs and WANs.

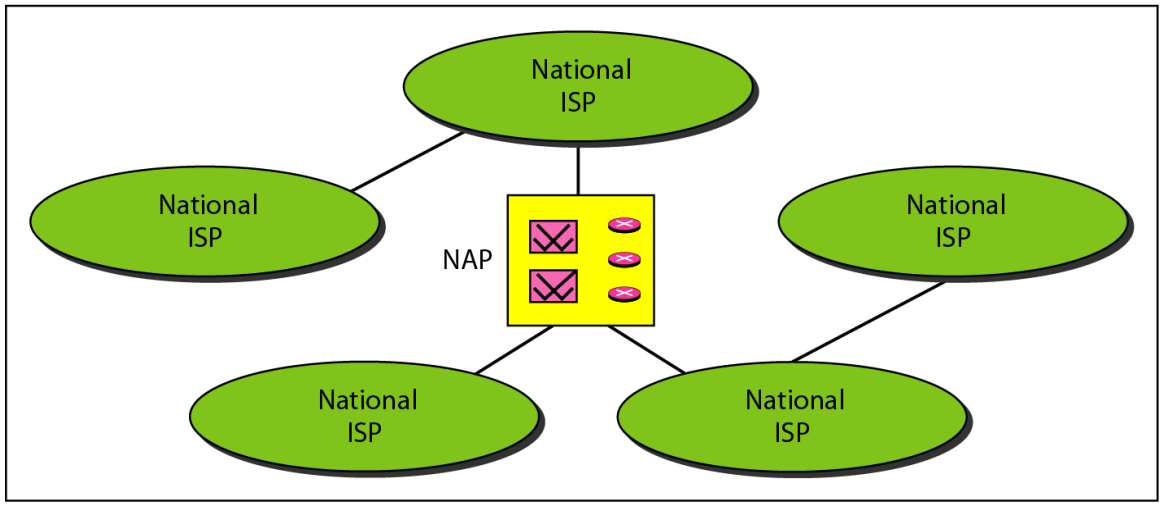


- The Internet is not owned by any individual or group.
- It involves services of Internet Service Providers at several levels.
- There are international service providers, national service providers, regional service providers, and local service providers.
- The Internet today is run by private companies, not the government.

- Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

- Networks can vary in size, shape, and function.
- A network can be as complex as devices connected across the Internet, or as simple as two computers directly connected to one another with a single cable, and anything in-between.
- However, simply having a wired or wireless physical connection between end devices is not enough to enable communication.
- For communication to occur, devices must know “how” to communicate.
- Devices need Network Software: Protocols and Standards.

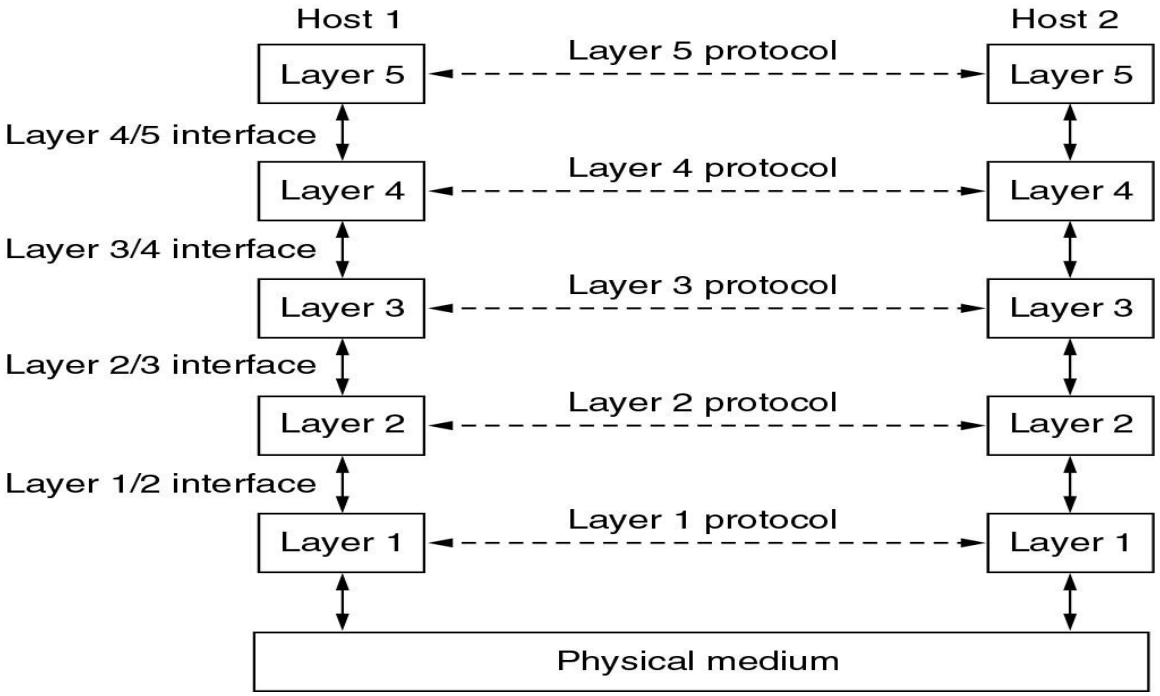
- **Protocols:**
- communication occurs between entities in different systems.
- An entity is anything capable of sending or receiving information.
- However, two entities cannot simply send bit streams to each other and expect to be understood.
- For communication to occur, the entities must agree on a protocol.
- A protocol is a set of rules that govern data communications.
- A protocol defines what is communicated, how it is communicated, and when it is communicated.

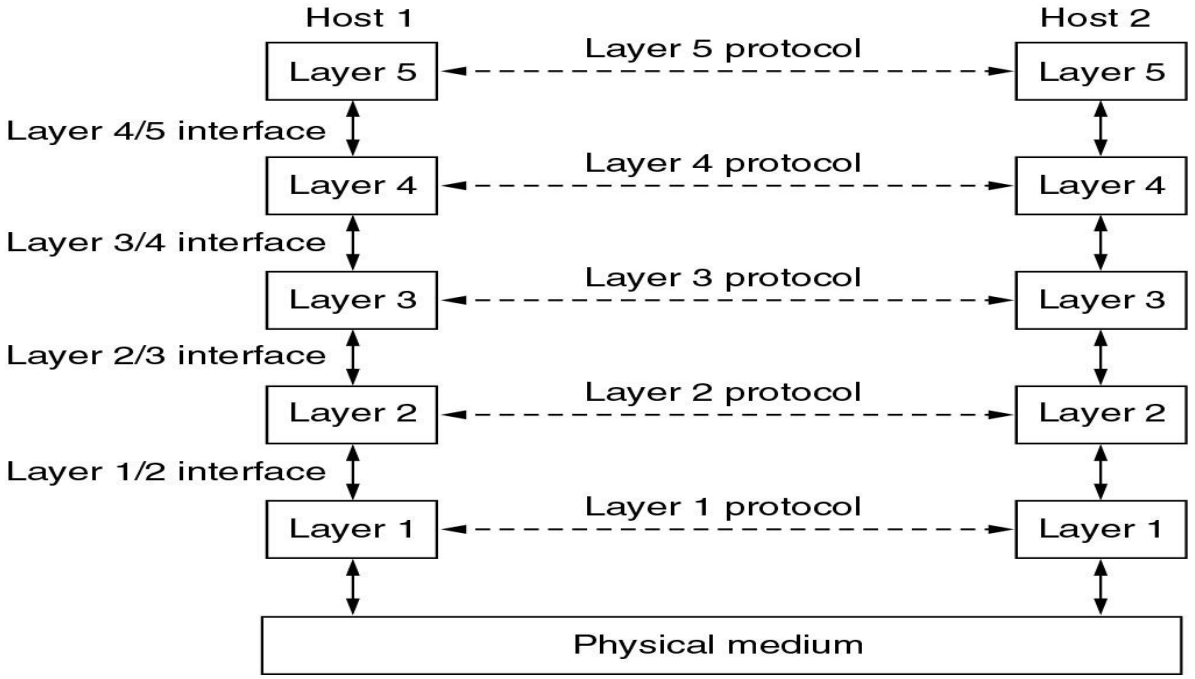
- The key elements of a protocol are syntax, semantics, and timing.
- Syntax. The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented.
- For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#3.1.1.4
- Semantics. The word *semantics* refers to the meaning of each section of bits.
- How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?
- Timing. The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

- **Standards**
- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.
- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

- Data communication standards fall into two categories:
- De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards.
- De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

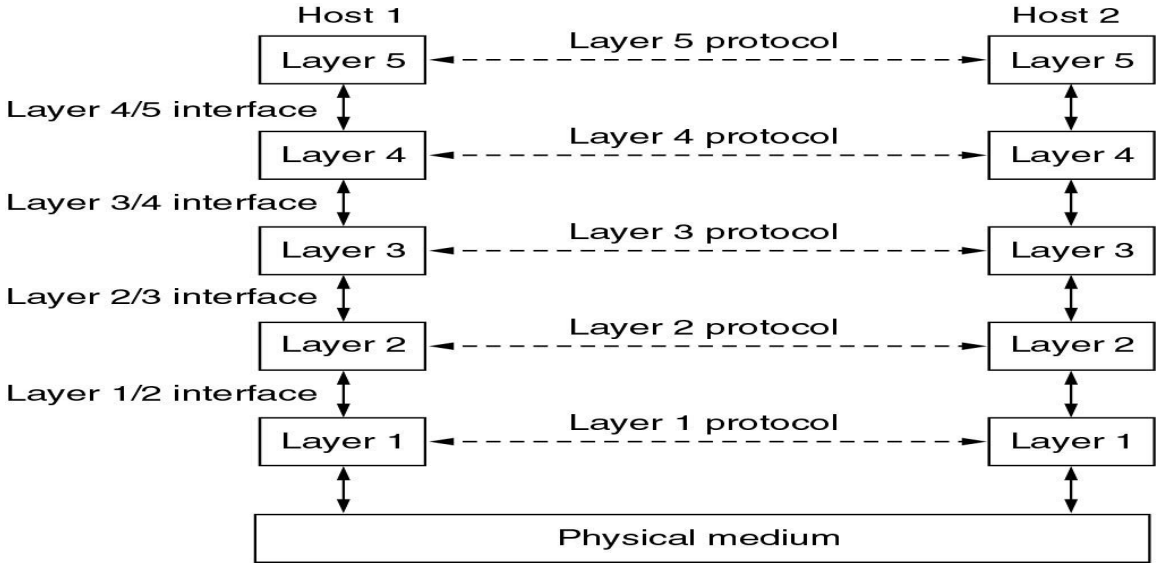
- Network software consists of number of protocols and is highly structured.
- **Protocol Hierarchies**
- To reduce their design complexity, most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it.





- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the layer above it while shielding those layers from the details of how the offered services are actually implemented.
- Layer *n* on one machine carries on a conversation with layer *n* on another machine.
- The rules and conventions used in this conversation are collectively known as the layer *n* protocol.

- The entities comprising the corresponding layers on different machines are called **peers**.
- It is the peers that communicate by using the protocol to talk to each other.



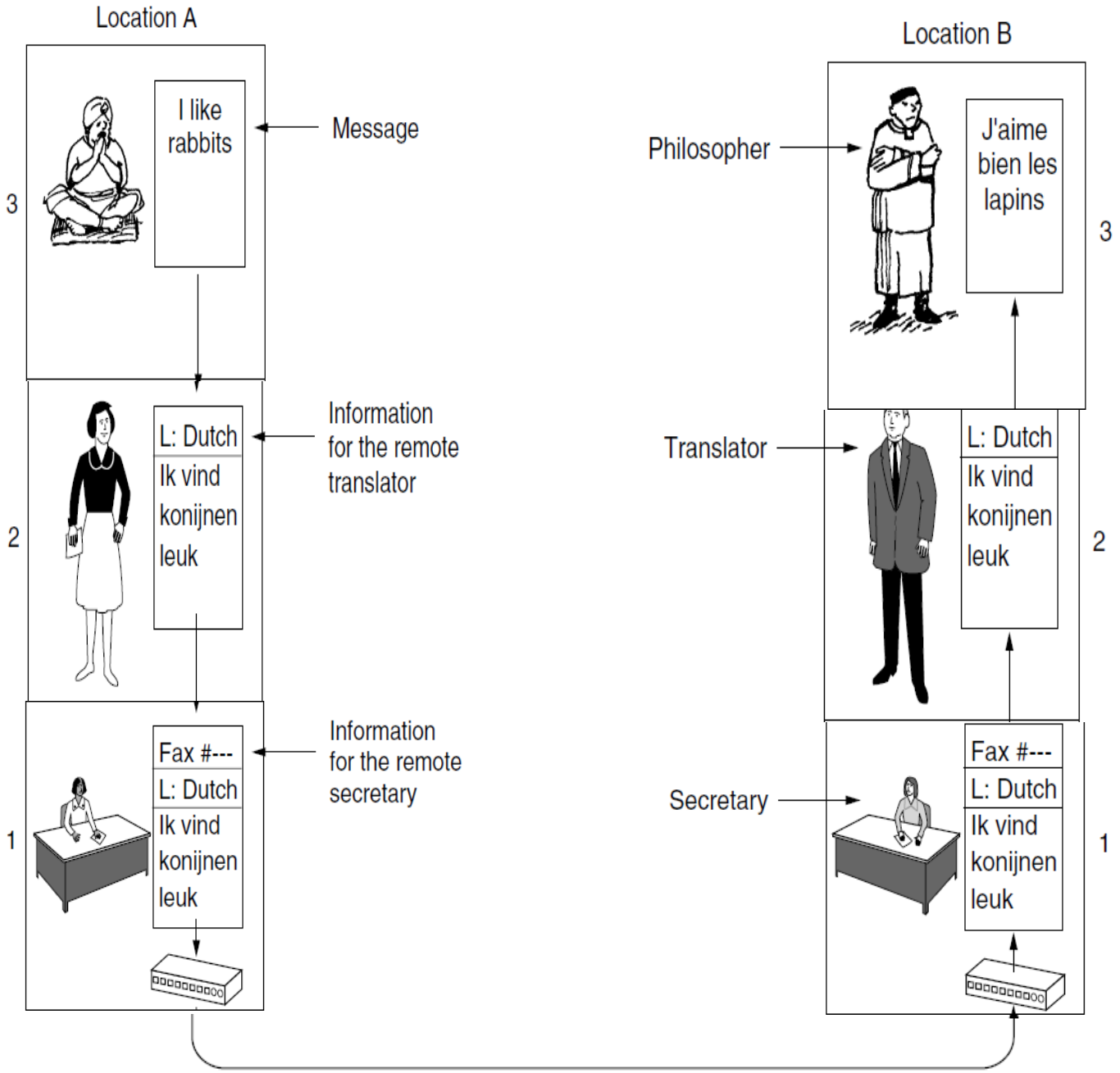
- In reality, no data are directly transferred from layer *n* on one machine to layer *n* on another machine.
- Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the **physical medium** through which actual communication occurs.
- Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one.

- A set of layers and protocols is called a **network architecture**.
- A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack**.
- An analogy may help explain the idea of multilayer communication.
- Imagine two philosophers one of whom speaks Hindi and English and the other of whom speaks Japanese and French.

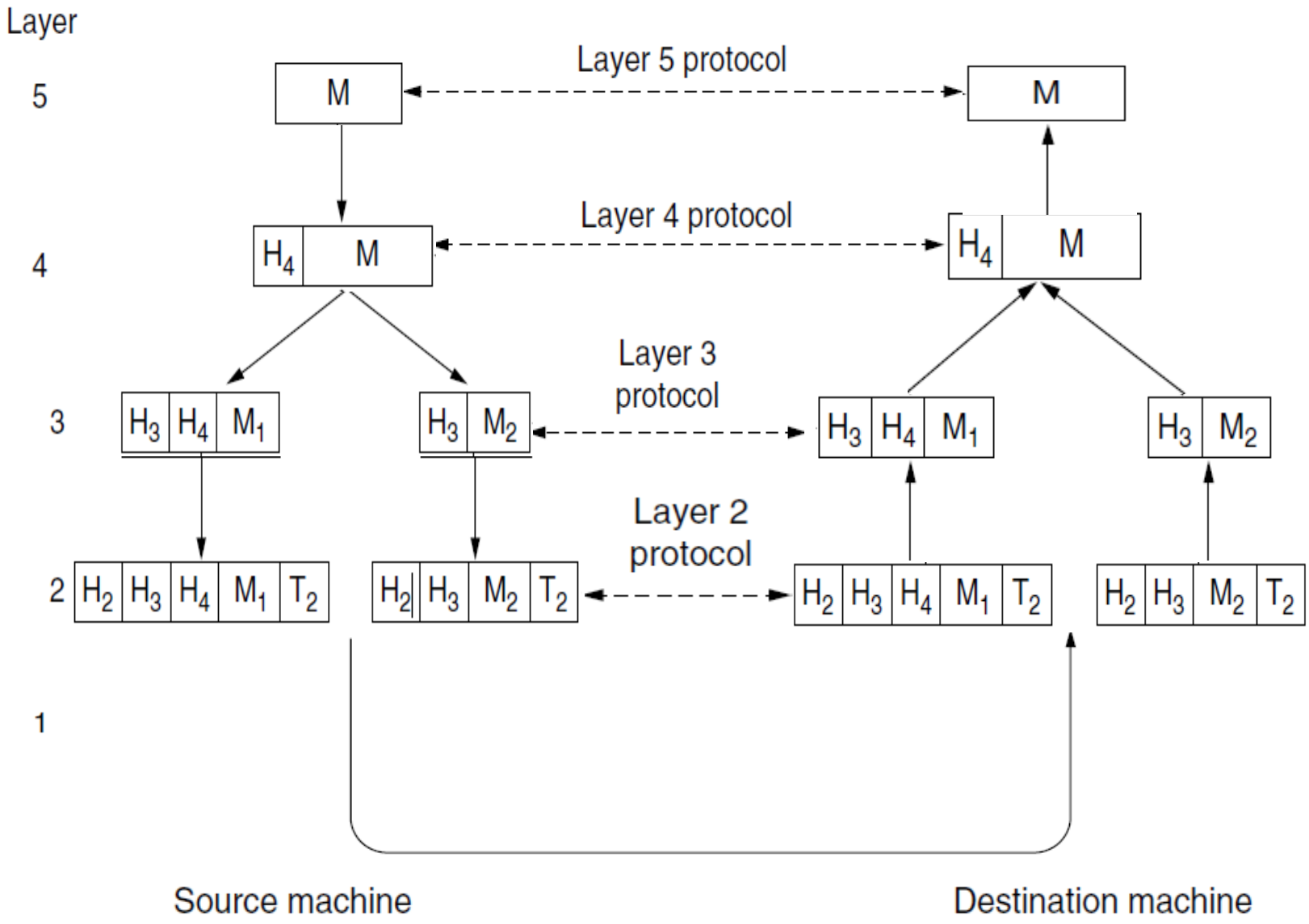
- Philosopher A

Philosopher B

- Assuming a three layer model. Philosophers reside at third layer.
- Since both of them does not have common medium of communication, they employ a translator at layer 2 and a secretary for transmitting the message at layer 1.


Location A
Location B
I like rabbits
Message
3
Philosopher
J'aime bien les lapins
3
L: Dutch
Ik vind konijnen leuk
Information for the remote translator
2
Translator
L: Dutch
Ik vind konijnen leuk
2
Fax #---
L: Dutch
Ik vind konijnen leuk
Information for the remote secretary
1
Secretary
Fax #---
L: Dutch
Ik vind konijnen leuk
1

- Entities:
- Philosophers(layer 3), Translators (layer2), Secrateries(layer1).
- services:
- Layer 2 offers translation, layer 1 offers transmission.
- Interfaces:
- Layer2/3 provides the choice of common language for translation.
- Layer1/2 provides the choice of electronic medium for communication.
- Protocols:
- At layer2: choice of the common language.
- At layer1: source and destination address.


Layer
5
4
3
2
1
Layer 5 protocol
Layer 4 protocol
Layer 3 protocol
Layer 2 protocol
M
M
H4 M
H4 M
H3 H4 M1
H3 M2
H3 H4 M1
H3 M2
H2 H3 H4 M1 T2
H2 H3 M2 T2
H2 H3 H4 M1 T2
H2 H3 M2 T2
Source machine
Destination machine

- **Design Issues for the Layers**
- The functions of different layers are determined from issues faced in transmitting data across networks.

- **Addressing.** Since there are many computers on the network, every layer needs a mechanism for identifying the senders and receivers that are involved in a particular message.

- **Error Control.** Transmission media are not perfect. Reliability is the design issue of making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable.

  Error control mechanisms involve either error detecting codes or error correcting codes.

  When error detecting codes are used information that is incorrectly received can then be retransmitted until it is received correctly.

  When error correcting codes are used correct message can be recovered from the possibly incorrect bits that were originally received.

  Both of these mechanisms work by adding redundant information.

- **Sequencing.** Messages are transmitted in the form of segments. Communication channels do not preserve the order in which the segments are sent.
  The receiver must reassemble the segments in a sequence.

https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#3.1.1.5

- **Flow control**. An allocation problem that occurs at every level is how to keep a fast sender from swamping a slow receiver with data. Feedback from the receiver to the sender is often used.

- **Routing.** Another reliability issue is finding a working path through a network. Often there are multiple paths between a source and destination, and in a large network, there may be some links or routers that are broken. The network should automatically choose the route.

- **internetworking**. Another problem is differences in the maximum size of a message that different networks can transmit. This leads to mechanisms for disassembling, transmitting, and then reassembling messages.

- **Multiplexing and De-multiplexing.** When it is inconvenient or expensive to setup a separate connection for each pair of communicating processes, the underlying layer may decide to use the same connection for multiple, unrelated conversations.

- **Rules of Data transfer.** The protocol must determine how many logical channels the connection corresponds to and what their priorities are. Many networks provide at least two logical channels per connection, one for normal data and one for urgent data.

- **congestion**. Sometimes the problem is that the network is oversubscribed because too many computers want to send too much traffic, and the network cannot deliver it all. This overloading of the network is called congestion. One strategy is for each computer to reduce its demand when it experiences congestion.

- Other key design issues include **Quality of service, confidentiality, authentication, integrity.**

- Layers can offer two different types of service to the layers above them:

- **Connection-Oriented Service and Connectionless Service.**
- **Connection-oriented** service is modeled after the telephone system.
- To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- The essential aspect of a connection is that it acts like a tube: the sender pushes bits in at one end, and the receiver takes them out at the other end.
- In most cases the order is preserved so that the bits arrive in the order they were sent.
- In some cases when a connection is established, the sender, receiver, and subnet conduct a **negotiation** about the parameters to be used, such as maximum message size, quality of service required, and other issues.
- A **circuit** is another name for a connection with associated resources, such as a fixed bandwidth.

- Connectionless service is modelled after the postal system.
- Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes in the subnet independent of all the subsequent messages.
- The messages might reach the destination out of order.

- Each of the above services can be characterized by the quality of service: **reliable service and unreliable service.**
- A reliable service never loses data.
- A reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.
- The acknowledgement process introduces overhead and delays, which are often worth it but are sometimes undesirable.
- An unreliable service does not seek acknowledgement.

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

- Example of **reliable connection oriented service** is File transfer. Loss of bits is not accepted in a file transfer.
- Reliable connection-oriented service has two minor variations: **message sequences and byte streams.**
- In Message sequences, the message boundaries are preserved.
- When two 1024-byte messages are sent, they arrive as two distinct 1024-byte messages, never as one 2048-byte message.

- In byte stream, the connection is simply a stream of bytes, with no message boundaries.
- When 2048 bytes arrive at the receiver, there is no way to tell if they were sent as one 2048-byte message, two 1024-byte messages, or 2048 1-byte messages.

- **Unreliable Connection oriented service:** For some applications, the transit delays introduced by acknowledgements are unacceptable.
- Eg: VOIP(digitized voice), Video transmissions.

- Not all applications require connections.
- **Unreliable Connection less service:** often called **datagram** service, in analogy with telegram service.
- Ex: Spam mails.

- **Reliable Connection less service:** Also called **acknowledged datagram** service. Provides acknowledgement but without connection.

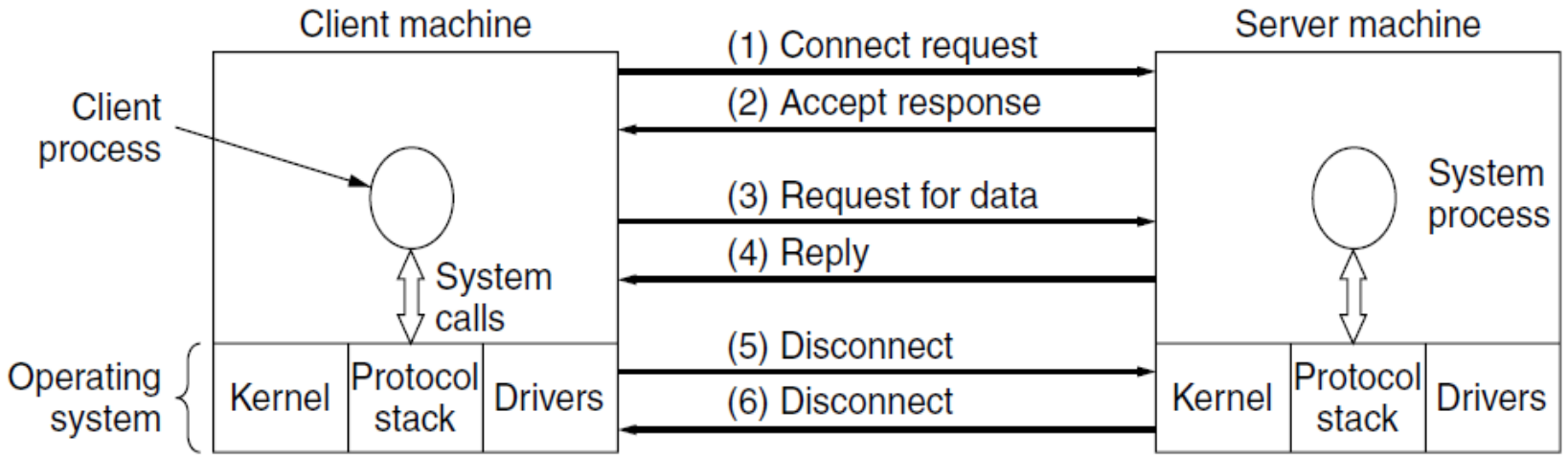
- In some situations, the convenience of not having to establish a connection to send one message is desired, but reliability is essential.
- Ex: Registered mail.
- **Request-Reply service:** In this service the sender transmits a single datagram containing a request; the reply contains the answer.
- Ex: Client-Server Model.

- **Service Primitives:**
- A service is formally specified by a set of **primitives** (operations) available to user processes to access the service.
- These primitives tell the service to perform some action or report on an action taken by a peer entity.
- The set of primitives available depends on the nature of the service being provided.
- The primitives for connection-oriented service are different from those of connectionless service.

- Examples of the service primitives for reliable byte stream.

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

- Ex: Client Server Model



REFERENCE MODELS: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.

It deals with connecting open systems.

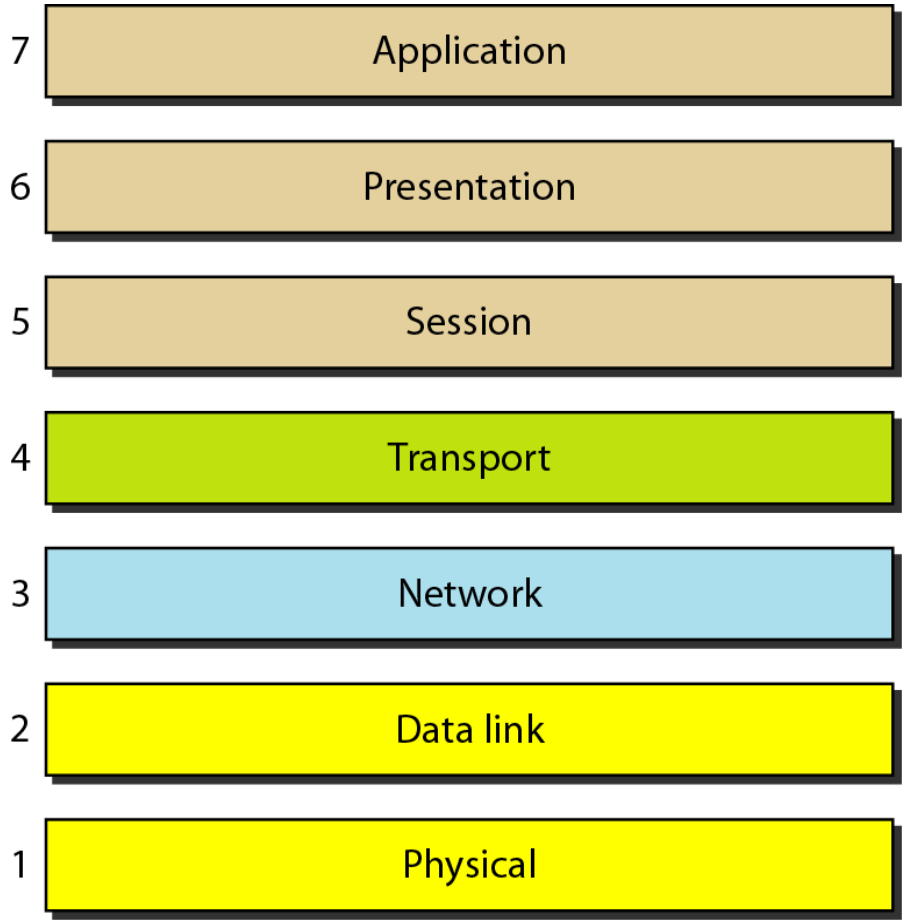
It is the first step toward International standardization of protocols used in various layers.

The OSI model has seven layers.

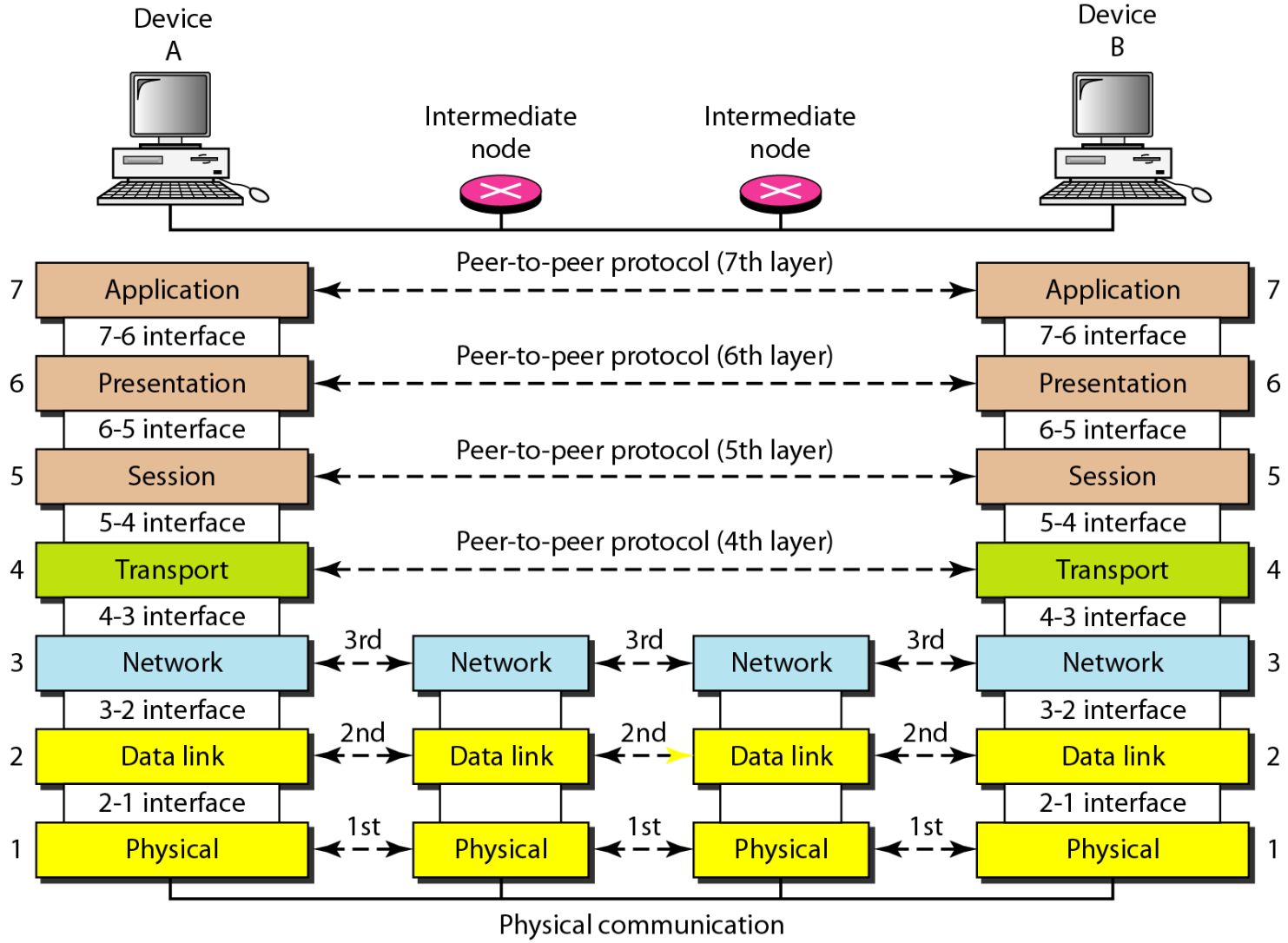
The number of layers are decided based on the following principles.

1) A layer should be created where a different abstraction is needed.
2) Each layer should perform a well defined function.
3) The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4) The layer boundaries should be chosen to minimize the information flow across the interfaces.
5) The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture doesn't become unwieldy.

Seven layers of the OSI model



The interaction between layers in the OSI model



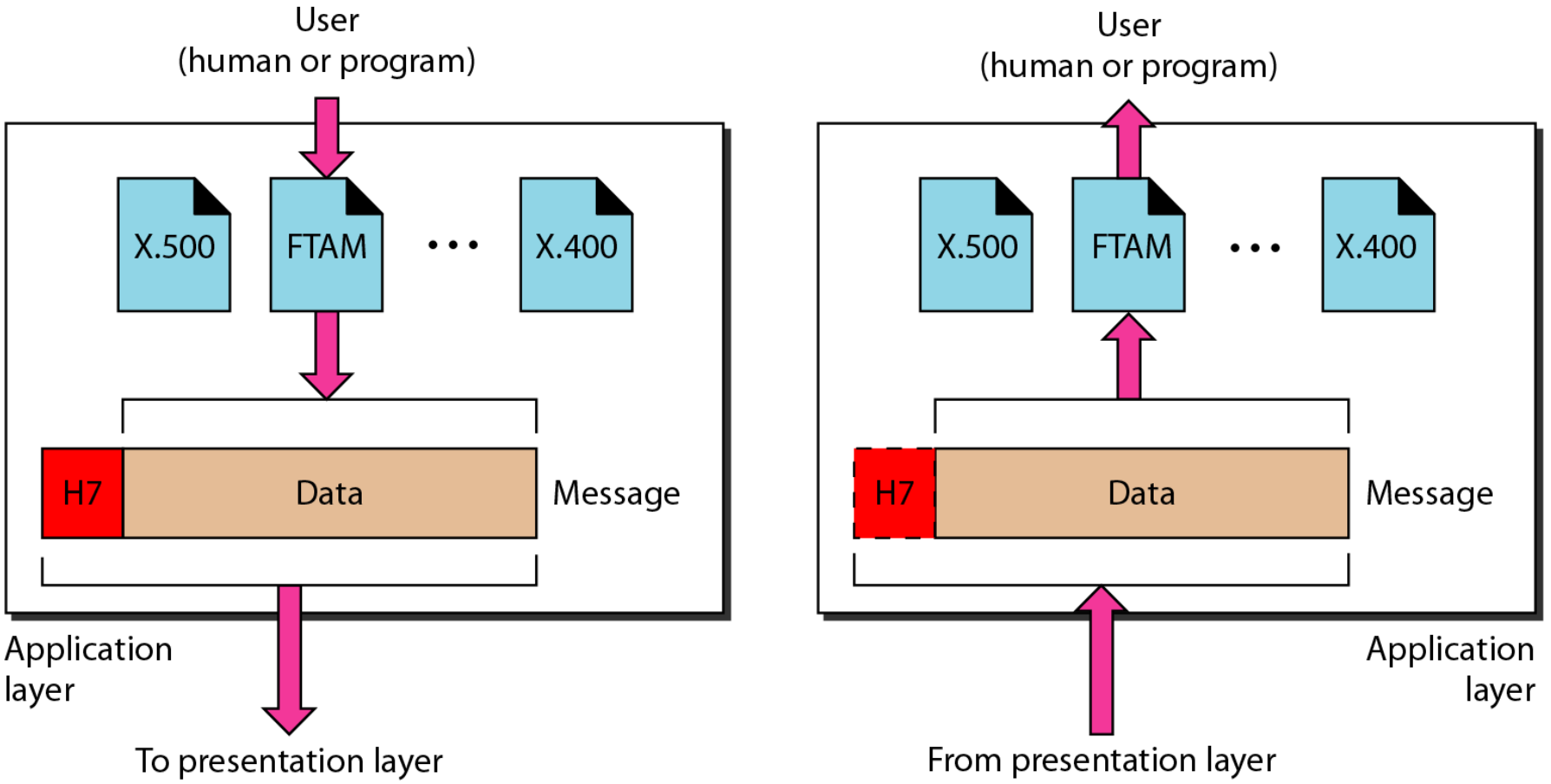
Application layer

- *The application layer is responsible for providing services to the user.*
- *It provides user interfaces and support for services such as email, file transfer and other distributed information services.*

Specific services provided by the application layer include

- ***Network virtual terminal:*** *Allows a user to log on to a remote host.*
- ***File transfer, access and management(FTAM):*** *Allows user to access files in a remote host, to retrieve files from a remote computer.*
- ***Mail services(X.400):*** *Provides basis for e-mail forwarding and storage.*
- ***Directory services(X.500):*** *Distributed database sources and access for global information*

Application layer



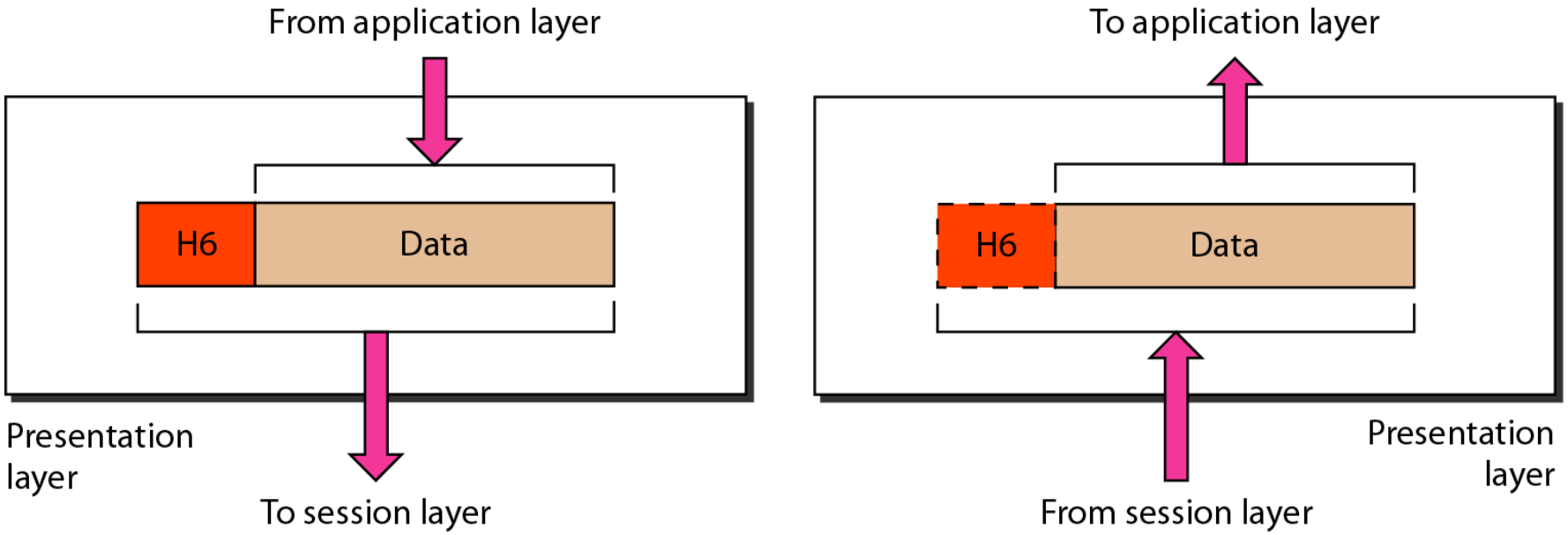
Presentation layer

The presentation layer is concerned with syntax and semantics.

Specific responsibilities include:

- ***Translation:*** *Presentation layer is responsible for interoperability between different encoding methods.*
- ***Encryption:*** *Sender encrypts the original information to another form and transmits over the network. The receiver decrypts the incoming message into original form.*
- ***Compression:*** *Compression involves reducing the number of bits in the original message.*

Presentation layer

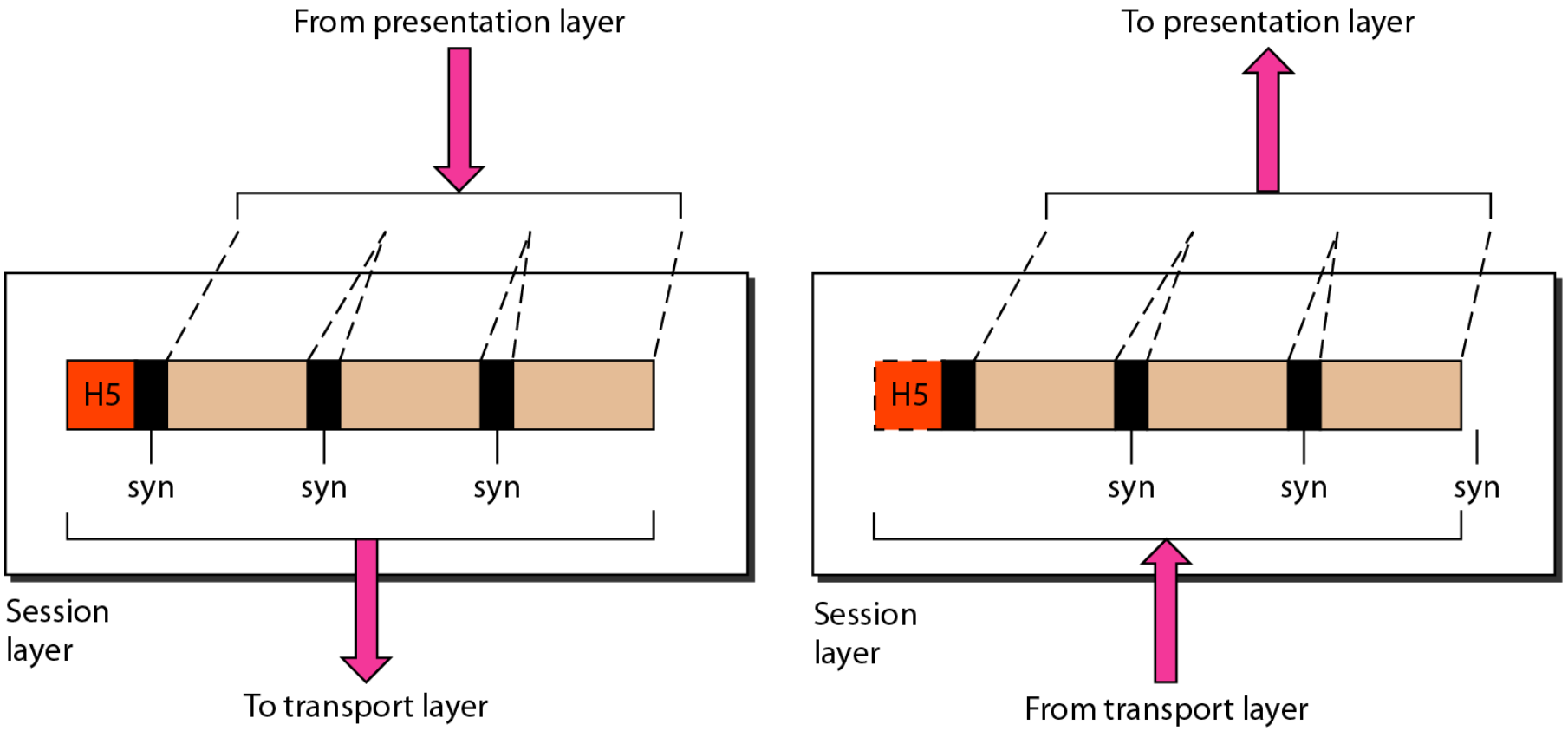


Session layer

The Session layer is responsible for dialog control and synchronization.

- ***Dialog control:*** *Allows communication between two processes to take place in either half duplex or full duplex mode.*
- ***Synchronization:*** *Allows process to add check points or synchronization points, to a stream of data.*

Session layer



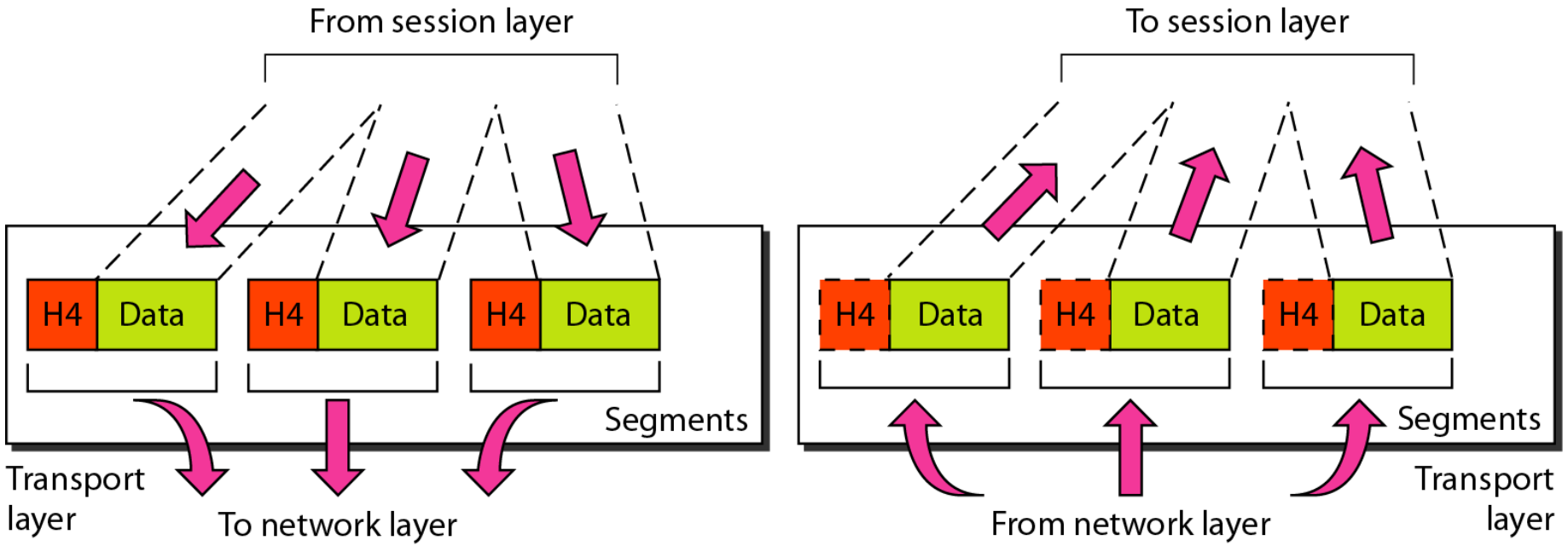
Transport layer

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

Specific services provided by the Transport layer include

- ***Service point addressing:*** *The transport layer header includes a type of address called service point address or port address to identify specific process on a computer.*
- ***Segmentation and reassembly:*** *At the sender the message is divided into segments with each segment containing a sequence number. At the receiver the segments are reassembled.*
- ***Connection control:*** *Offers either connection oriented or connectionless service.*
- ***Flow control:*** *Flow control is performed for end to end processes.*
- ***Error control:*** *Error control is performed process to process. Ensures entire message is received without error(damage, loss,duplication).*

Transport layer



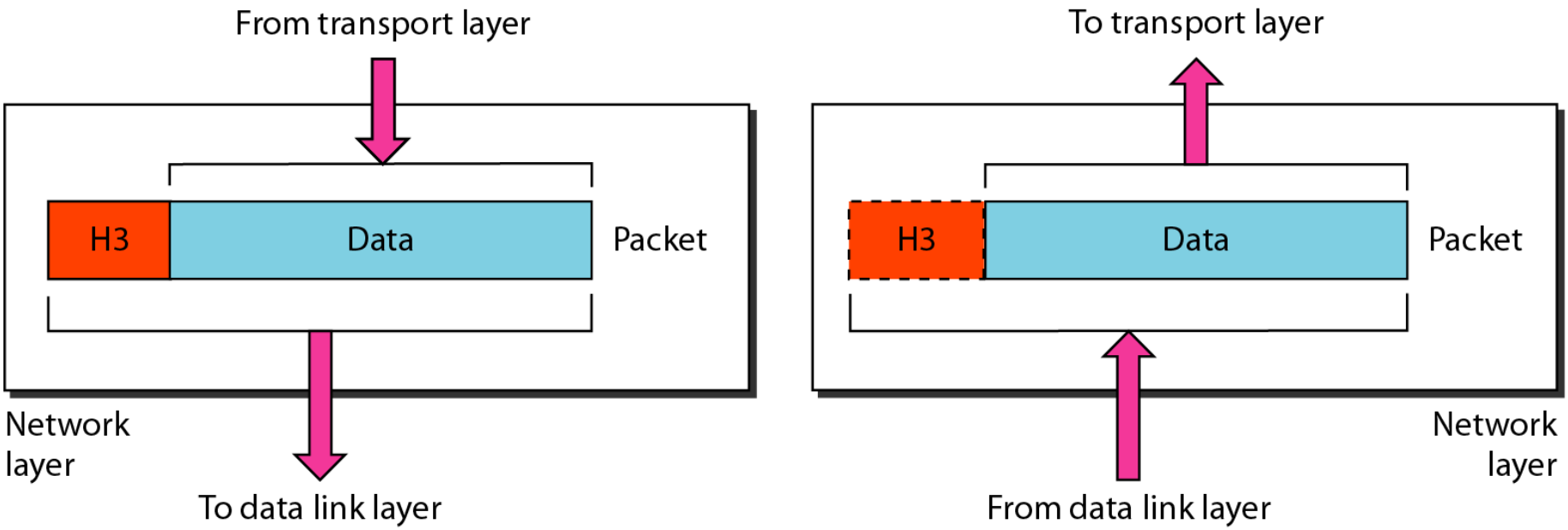
Network layer

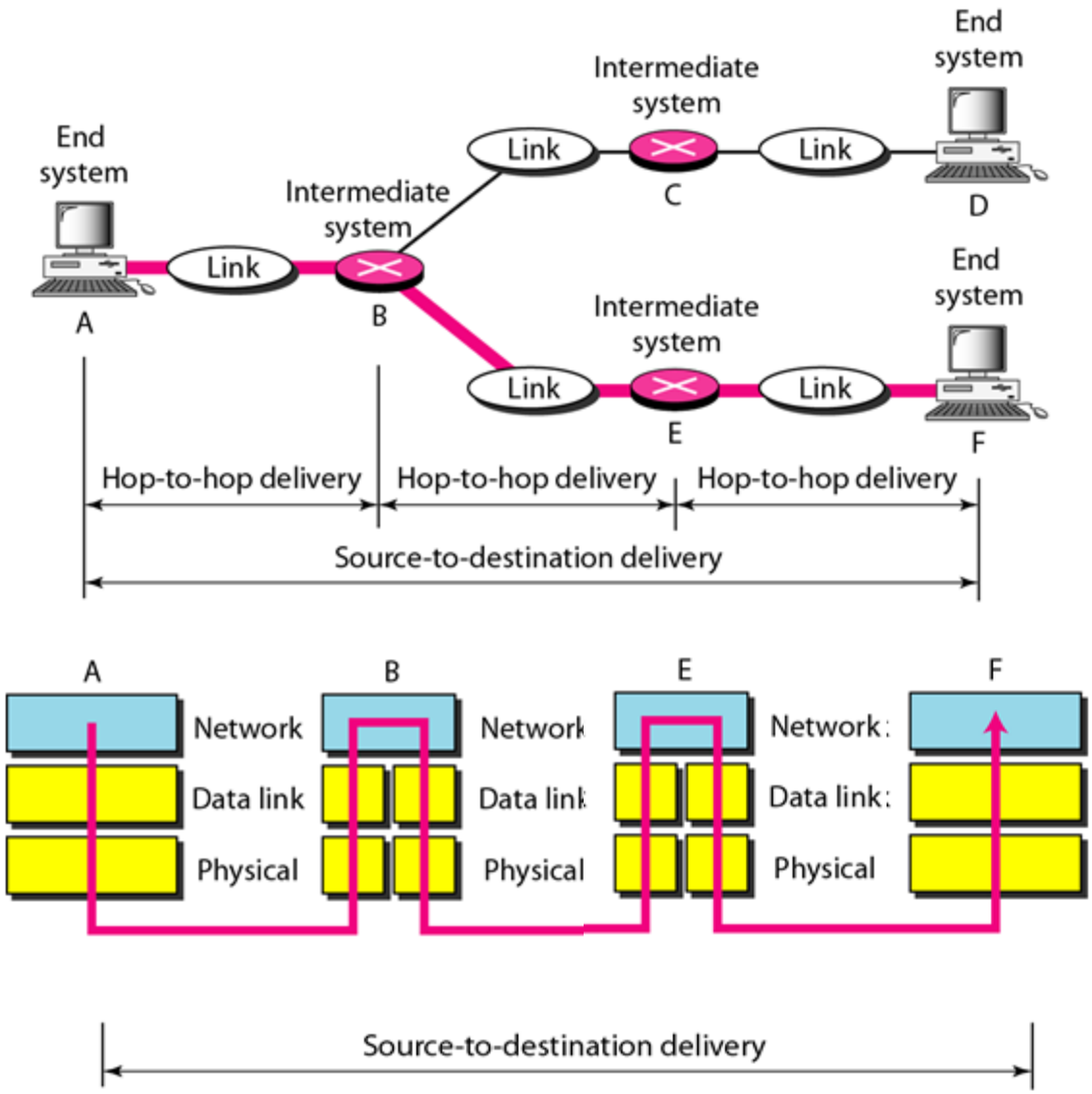
The network layer is responsible for the delivery of individual packets from the source host to destination host

Specific responsibilities provided by the network layer include

- ***Logical addressing:*** *Logical address helps packets to be delivered across networks. Network layer adds the logical address of the sender and receiver in the header of the outgoing packets.*
- ***Routing:*** *When the end systems are connected across networks, the connecting devices route the packets to their final destination.*

Network layer




End system
Intermediate system
End system
Link
Link
C
D
End system
Intermediate system
Link
A
B
Intermediate system
End system
Link
Link
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
Source-to-destination delivery
A
B
E
F
Network
Network
Network
Data link
Data link
Data link
Physical
Physical
Physical
Source-to-destination delivery

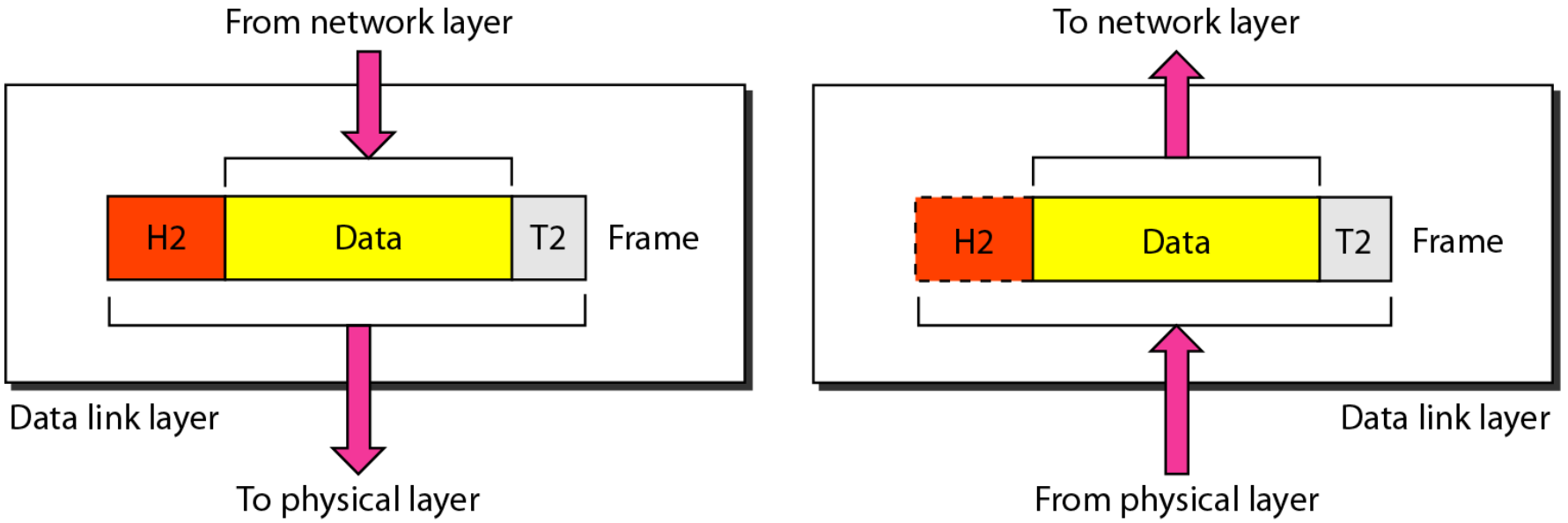
Data Link layer

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

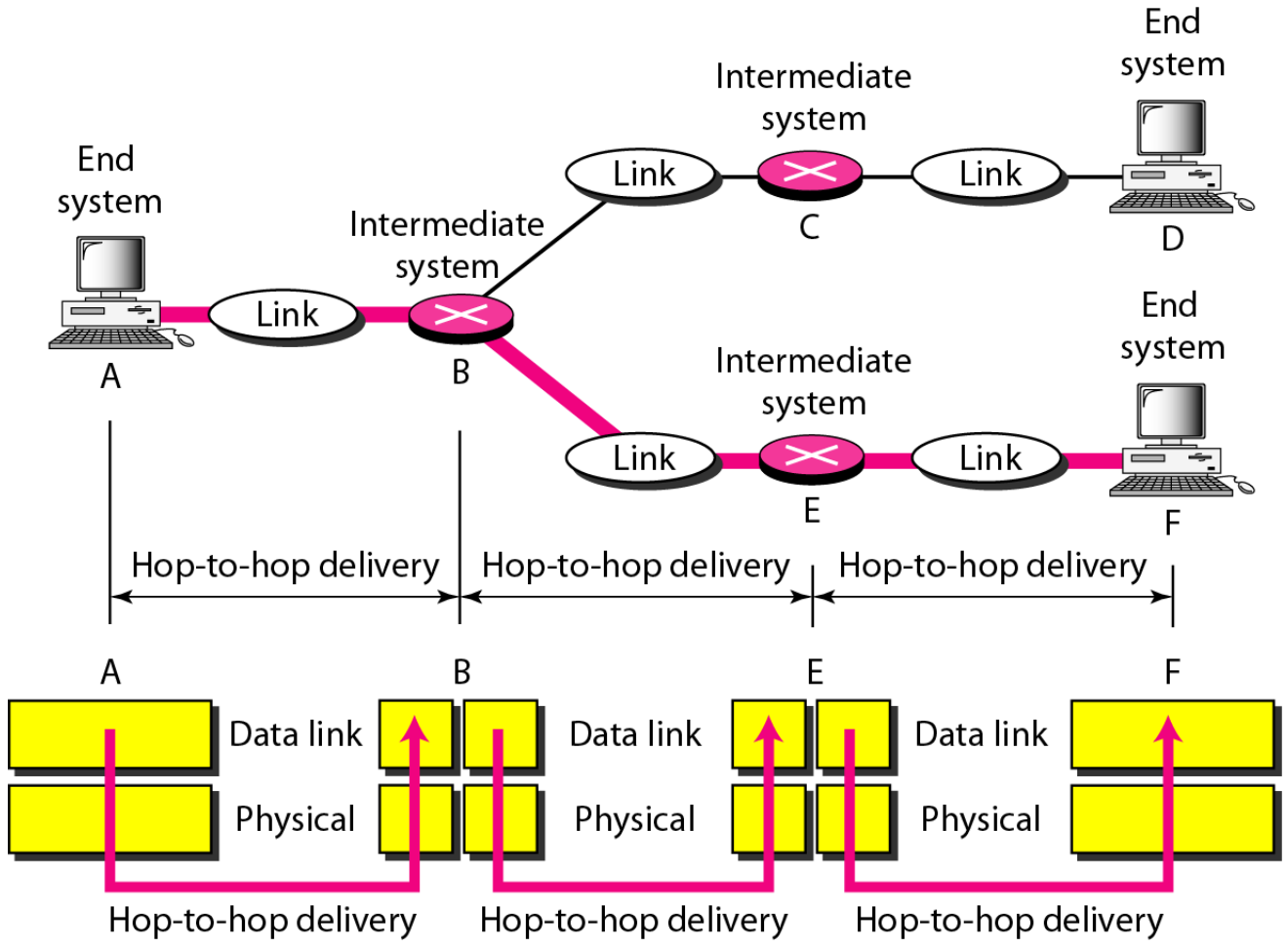
Other responsibilities of the data link layer include:

- ***Framing:*** *The data link layer divides the stream of bits received from the network layer into manageable units called frames.*
- ***Physical addressing:*** *The data link layer adds a header to the frame to identify the sender and receiver of the frame in the same network.*
- ***Flow control:*** *Data link layer imposes a flow control mechanism to avoid overwhelming the receiver. Flow control is implemented between systems that are directly connected.*
- ***Error control:*** *Adds mechanisms to detect and retransmit damaged or lost frames, identify duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.*
- ***Access control****: When two or more devices are connected to the link, data link layer determines which device has control over the link at any given time.*

Data link layer



Hop-to-hop delivery



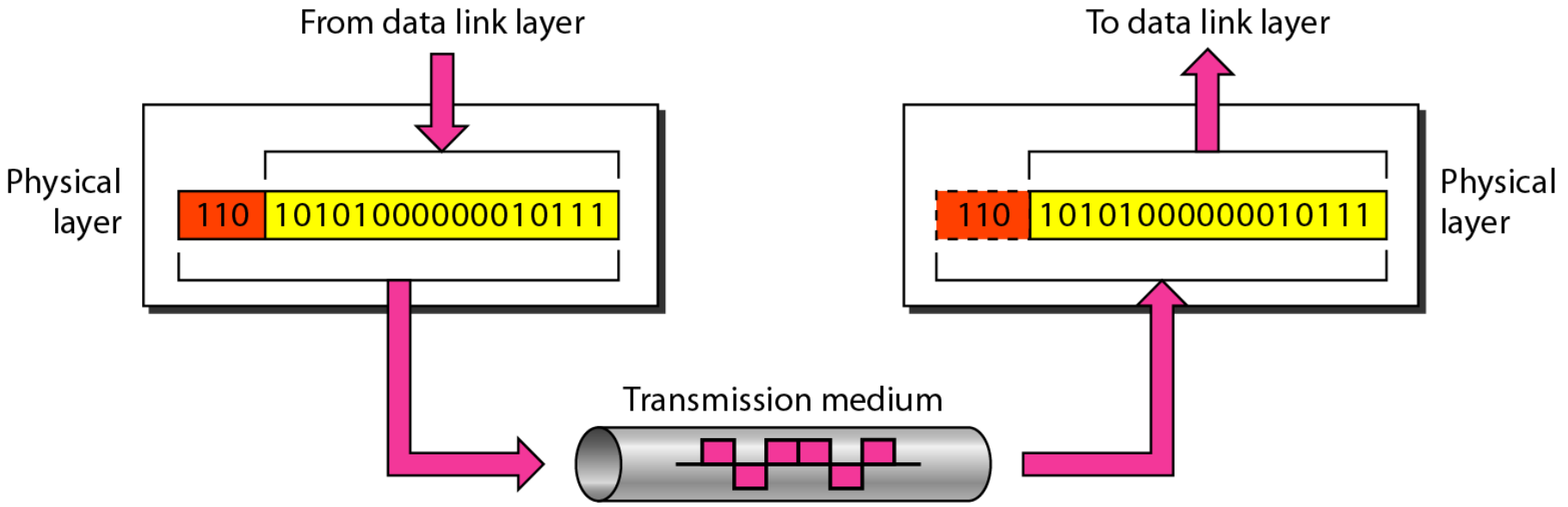
Physical layer

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

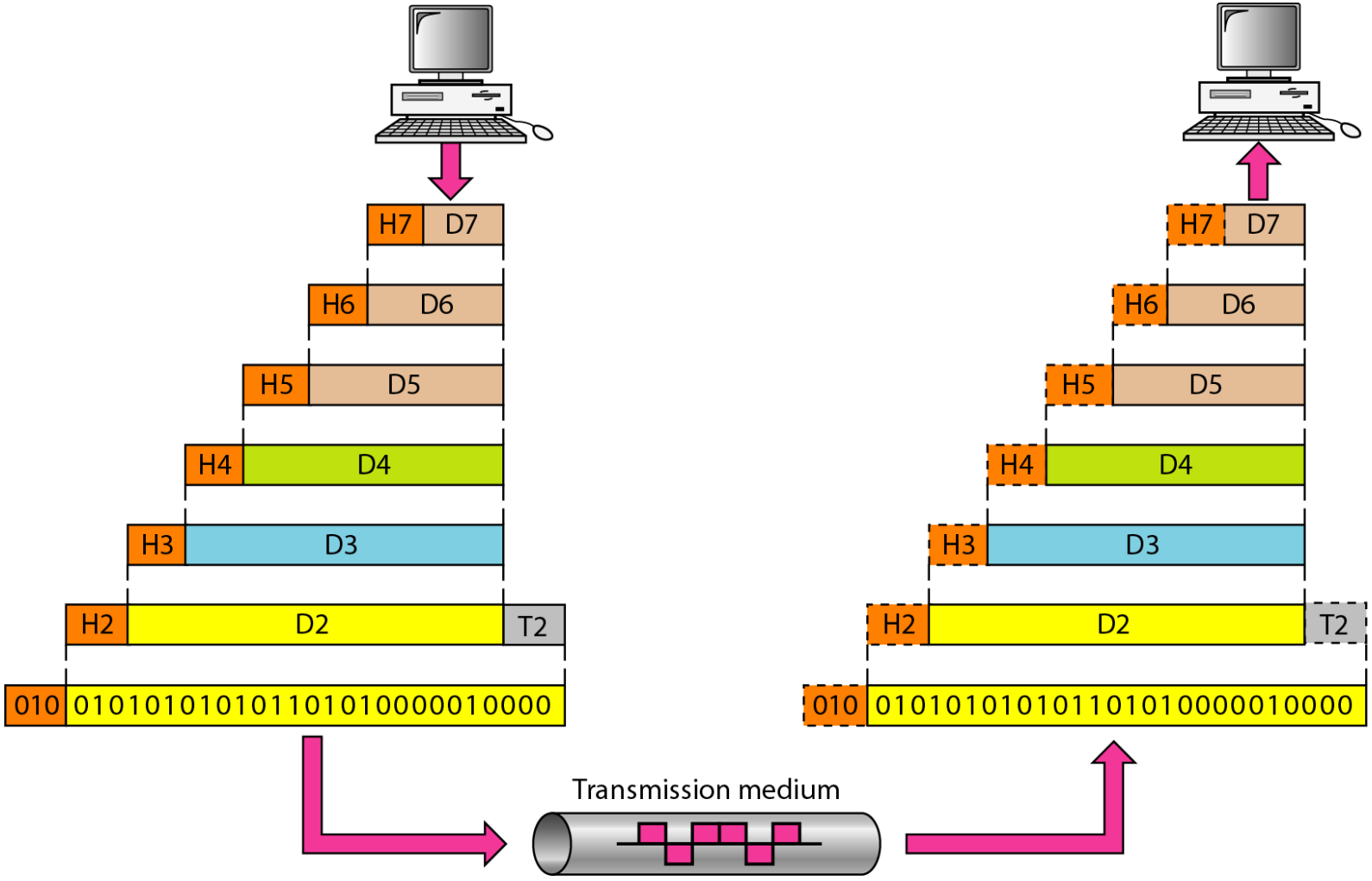
The physical layer is also concerned with the following:

- ***Physical characteristics of interfaces and medium:*** *Defines the characteristics of the interface between the devices and transmission medium. It also defines the type of transmission medium.*
- ***Representation of bits:*** *Defines the type of encoding (how 0s and 1s are changed to signals).*
- ***Data rate:*** *Defines the number of bits to be sent for each second.*
- ***Line configuration:*** *Concerned with the type of connection (point-to-point or multipoint configuration)*
- ***Physical topology****: Defines the type of topology.*
- ***Transmission mode:*** *Defines the direction of transmission.*

Physical layer

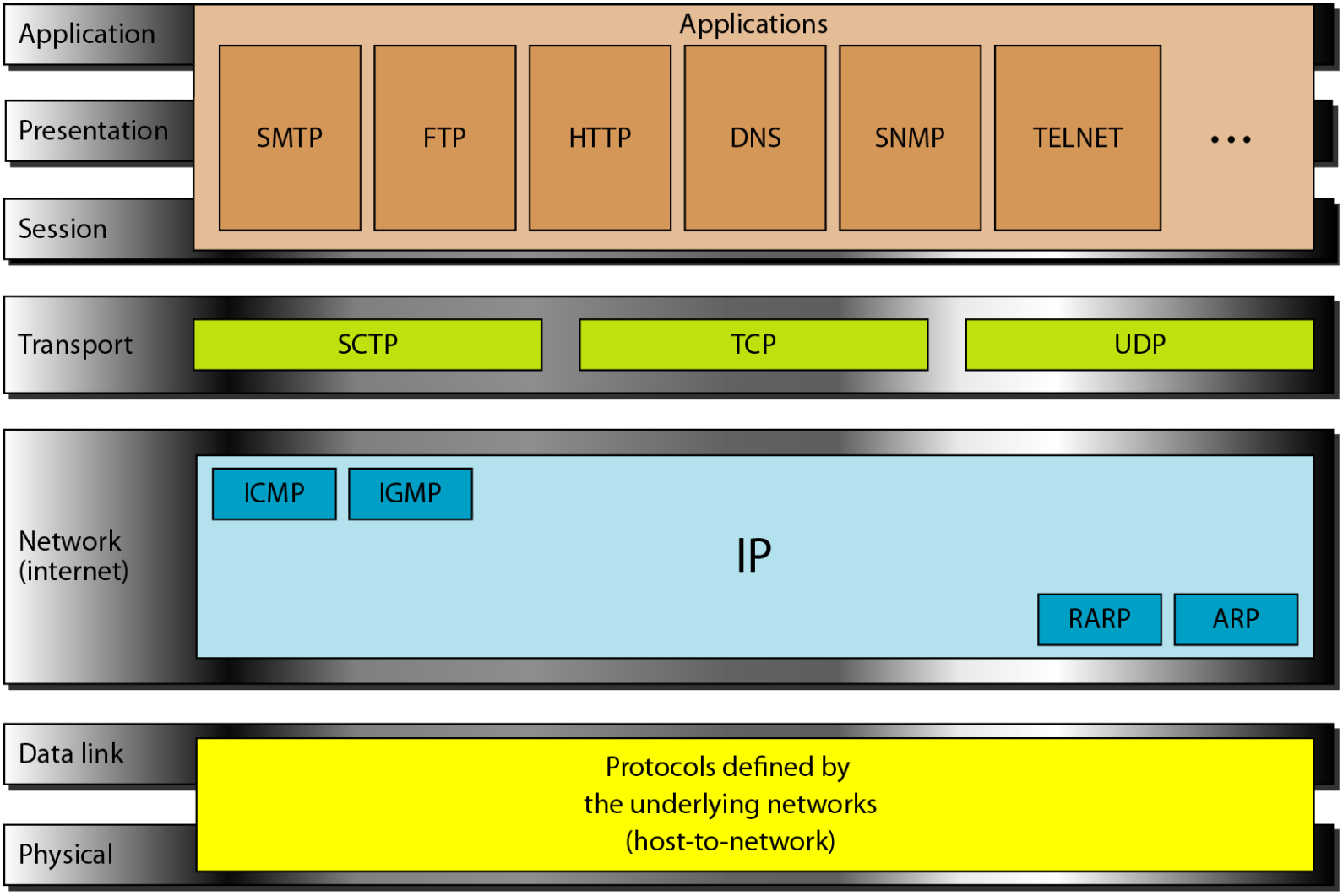


An exchange using the OSI model



TCP/IP Protocol Suite

- The TCP/IP protocol suite was developed prior to the OSI model.
- Therefore, 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 host-to-network layer is equivalent to the combination of the physical and data link 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.
- Whereas the OSI model specifies which functions belong to each of its layers, the layers of the *TCP/IP* protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.


Application
Presentation
Session
Applications
SMTP
FTP
HTTP
DNS
SNMP
TELNET
• • •
Transport
SCTP
TCP
UDP
Network
(internet)
ICMP
IGMP
IP
RARP
ARP
Data link
Physical
Protocols defined by
the underlying networks
(host-to-network)

- **Application Layer:** The Application layer in TCP/IP is equivalent to combined session, presentation and application layers in the OSI model.
- Many protocols are defined in this layer.
- **Hyper Text Transfer Protocol (HTTP).** HTTP is the underlying protocol used by WWW and this protocol defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.
- **Hyper Text Markup Language (HTML).** HTML ensures how web pages are formatted and displayed.
- **File Transfer Protocol (FTP).** Is used for exchanging files over the Internet. FTP promotes reliable and efficient data transfer.
- **Domain Name Service (DNS).** DNS translates domain names into IP address to help browsers communicate with remote servers.
- **Simple Mail Transfer Protocol (SMTP).** Protocol used for sending messages from one server to another.
- **TELNET.** Protocol used for remote login access.

- **Transport Layer:** Transport layer protocols are responsible for delivery of a message from one process to another process.
- **Transmission Control Protocol.** TCP is a reliable stream transport protocol. The term stream here refers to connection-oriented.
- At the sender , TCP divides the stream of data into smaller units called segments.
- Each segment includes a sequence number for reordering after receipt, together with an acknowledgement number for the segments received.
- At the receiving end , TCP collects each segment and re-orders them based on sequence numbers. It also sends an acknowledgement to the sender.
- It also ensures error control.
- **User Datagram Protocol.** UDP is a connectionless protocol.
- It is a process to process protocol that adds only port address, error control, and length information to the data from the upper layer.
- **Stream Control Transmission Protocol.** SCTP provides support for newer applications such as voice over the Internet.

- **Internet Layer.** Main protocol is Internetworking Protocol (IP). Supporting protocols include Address resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Internet Control Message Protocol (ICMP), Internet Group Message Protocol (IGMP).

- **IP.** IP is the transmission mechanism used by the TCP/IP protocols.
- It is an unreliable and connectionless protocol- a best effort delivery service.
- Best effort means that IP provides no error checking or tracking, to get a transmission through to its destination but with no guarantees.
- 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. Does not keep track of routes and has no facility for reordering datagrams.
- Provides for bare bones transmission functions and allows for maximum efficiency.

- **ARP.** ARP is used to associate a logical address with a physical address.
- In a LAN ARP is used to find the physical address of the device when its Internet address is known.

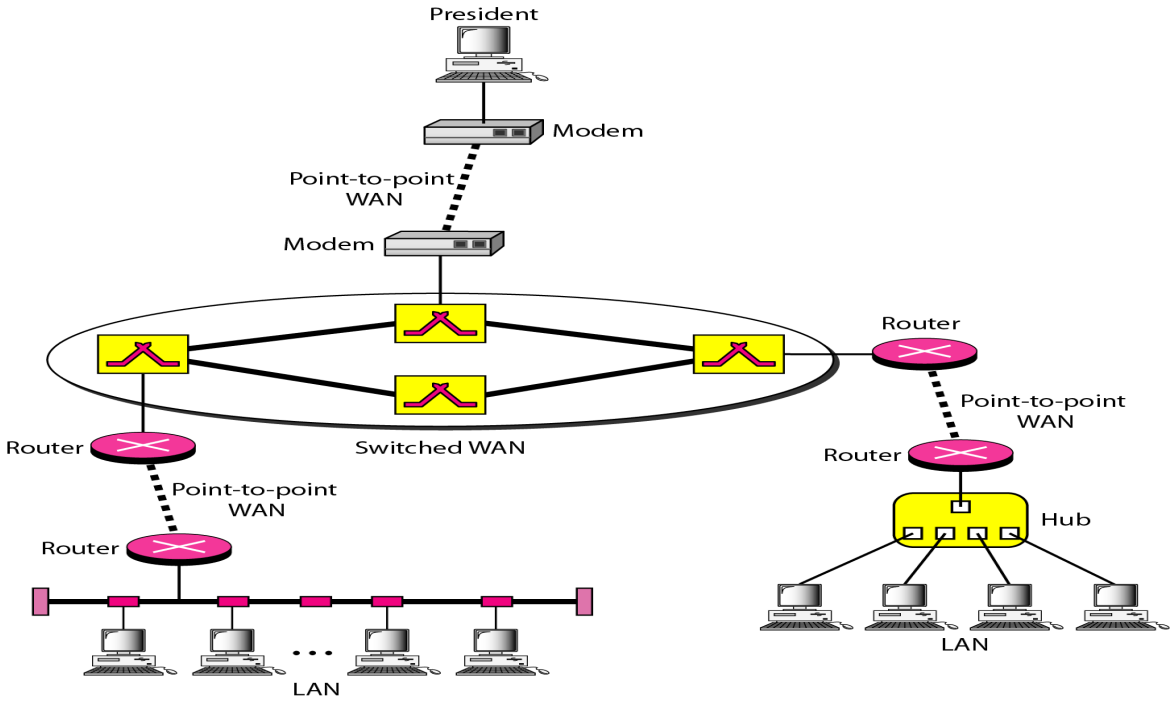
- **RARP.** RARP allows a host to discover its Internet address when it knows only its physical address.
- It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

- **ICMP.** It is used by hosts and network devices to send notifications of datagram problems such as host could not be reached or service not available.
- ICMP sends query and successful/error reporting messages.

- **IGMP.** It is used to facilitate simultaneous transmission of a message to a group of recipients.

- **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.

- **Connection Oriented Networks: X.25, Frame Relay and ATM**
- A subnet uses such connection oriented networks and models.



- Initially X.25 and frame relay were used.
- Asynchronous Transfer Mode (ATM) was designed to integrate different message types.
- ATM is an important connection oriented network.
- It is now mostly used by carriers for Internet transport.
- Connections are established by virtual circuits, where each connection has a unique connection identifier.
- Most ATM networks support permanent virtual circuits.
- ATM transmits fixed size packets called as cells.
- The cells are 53 bytes long, of which 5 bytes are header and 48 bytes are payload(data).

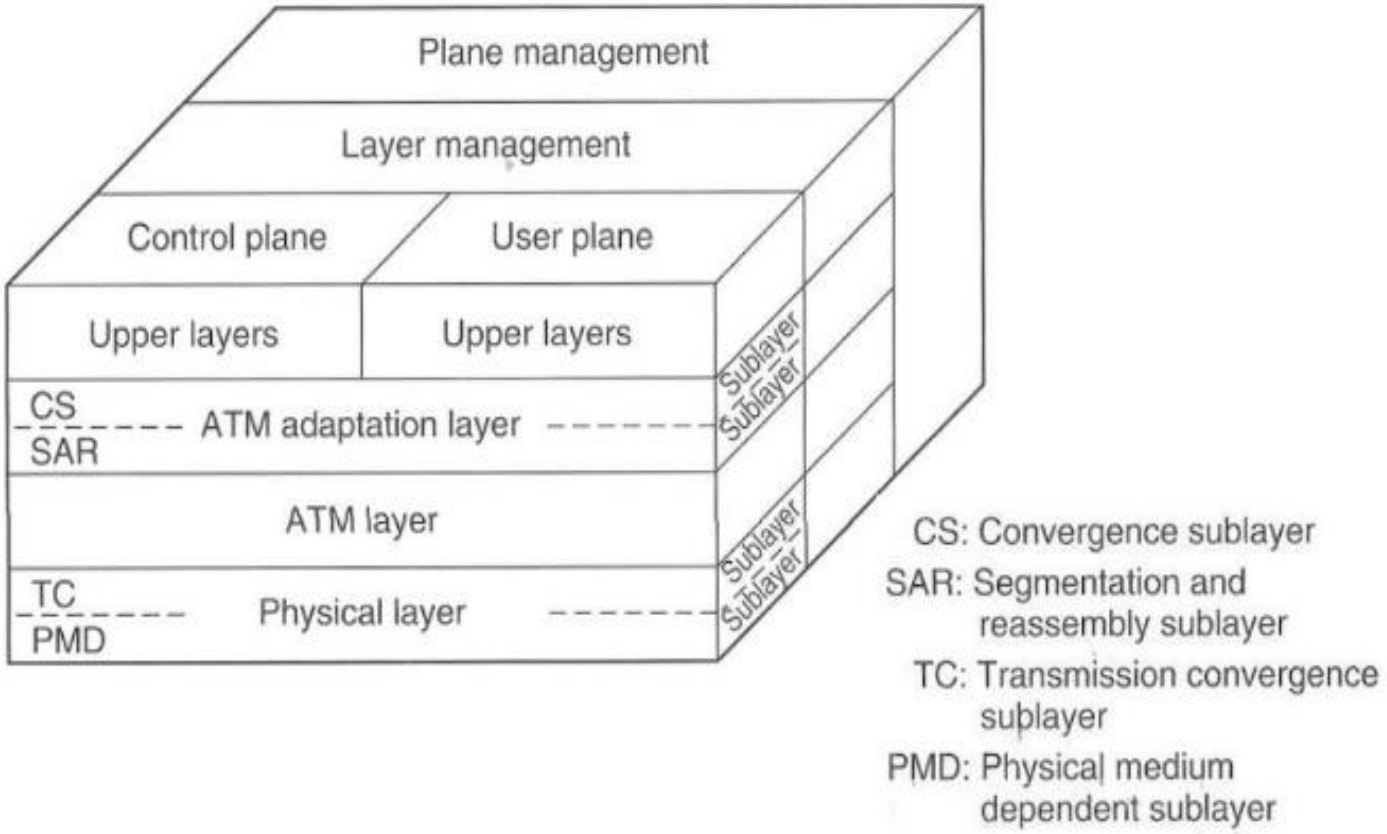
- Bytes

- Part of the header is the connection Identifier.
- Cell delivery is not guaranteed, but their order is.

- **Benefits of ATM:**
- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

- Common speeds for ATM networks are 155 Mbps and 622 Mbps.

- ATM Reference Model



OSI layer	ATM layer	ATM sublayer	Functionality
3/4	AAL	CS	Providing the standard interface (convergence)
		SAR	Segmentation and reassembly
2/3	ATM		Flow control Cell header generation/extraction Virtual circuit/path management Cell multiplexing/demultiplexing
2	Physical	TC	Cell rate decoupling Header checksum generation and verification Cell generation Packing/unpacking cells from the enclosing envelope Frame generation
1		PMD	Bit timing Physical network access

The ATM layers and sublayers and their functions.

- The user plane deals with data transport, flow control, error correction and other user functions.
- Control plane is concerned with connection management.
- The layer and plane management functions relate to resource management and interlayer co-ordination.