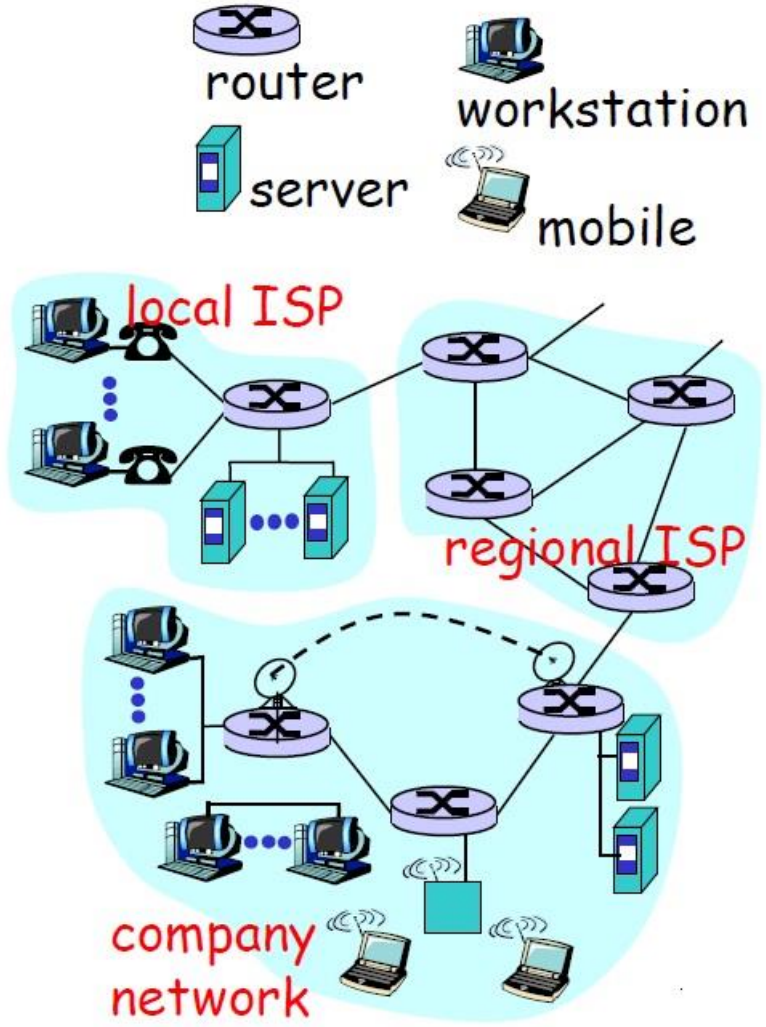
COMPUTER NETWORKS

CONTENTS

- **Introduction to Computer Networks**
- **Uses of Computer Networks**
- **Network Hardware**
- **Network Topology**
- **Network Software**

- A set of communication elements connected by communication links
  - **Communication elements**
    - Computers, printers, mobile phones, …
    - Routers, switches, …
  - **Communication links**
    - optic fiber
    - coaxial cable
    - twisted pair
    - wireless (radio, microwave, satellite)
  - **Topologies**
    - Ring, Star, Bus, Tree, Mesh



- A software/hardware infrastructure
  - **Share resources**
    - data, files, computing power, video,…
  - **Information highway**
    - communication between geographically dispersed users
  - **Electronic Society**
    - Cyberspace
    - Virtual global nation

Computer Network

- an interconnected collection of autonomous computers Internet: “network of networks”
  - loosely hierarchical
  - public Internet versus private intranet.
- WWW a distributed systems run on the top of Internet

Distributed System

- High degree of cohesiveness and transparency
- A software system built on top of a network

USES OF COMPUTER NETWORKS

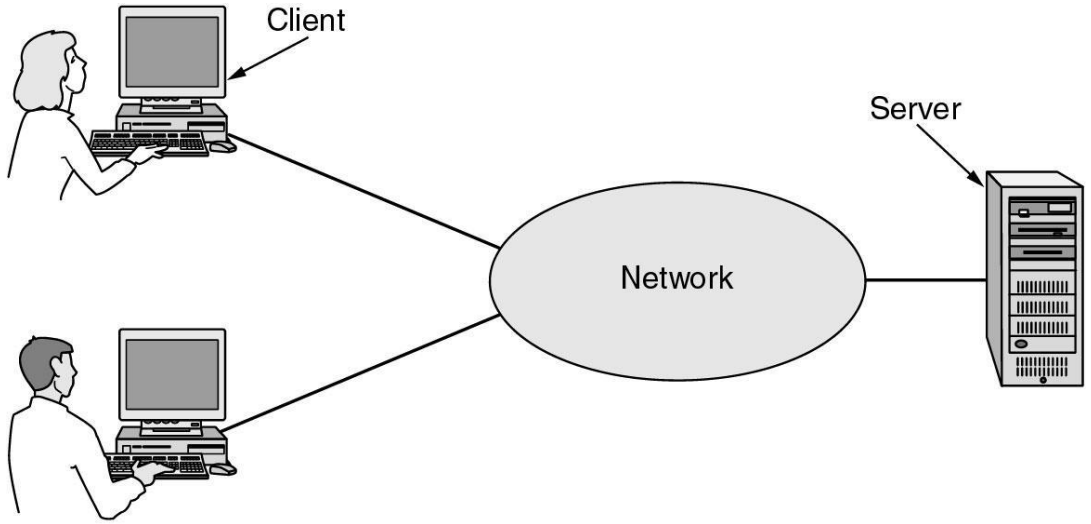
- **Business Applications**
- **Home Applications**
- **Mobile Users**
- **Social Issues**

Business Applications of Networks

a. Resource sharing (hardware, software, information, …)

b. Providing communication medium (e-mail, videoconferenceing)

c. Doing business electronically (B2B, B2C, e-commerce)



A network with two clients and one server.

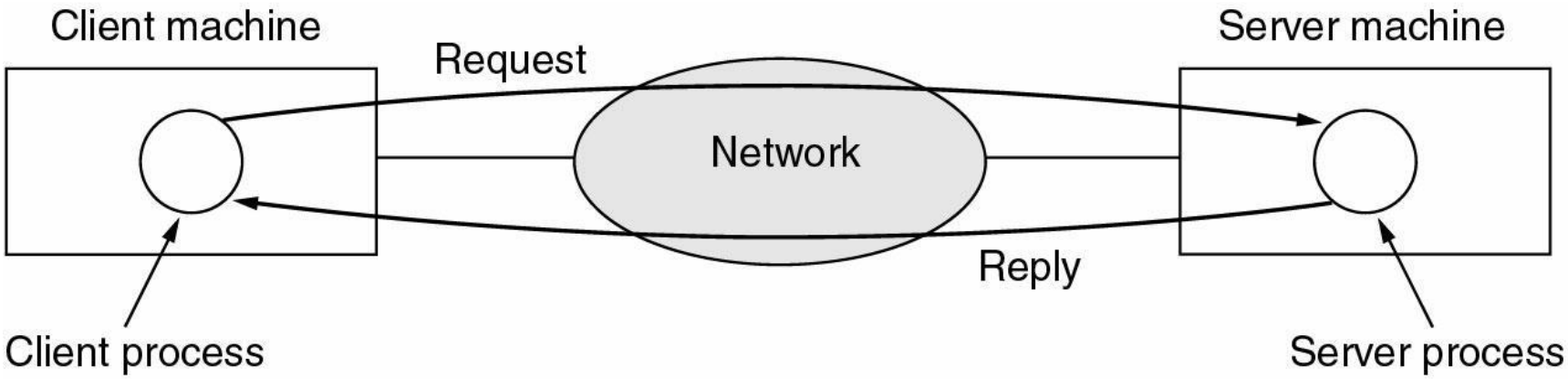
Goals of Networks for Companies

- **Resource sharing: equipment, programs, data**
- **high reliability**
  - replicated data
  - hardware
- **Saving money**
  - mainframe: 10 times faster, but 1000 times more expensive than PC
  - client-server model
- **Scalability**
  - mainframe: replace a larger one
  - client-server model: add more servers
- **Communication medium for separated employees**

Business Applications of Networks (2)

a. Two processes are involved

b. A communication network is needed



The client-server model involves requests and replies.

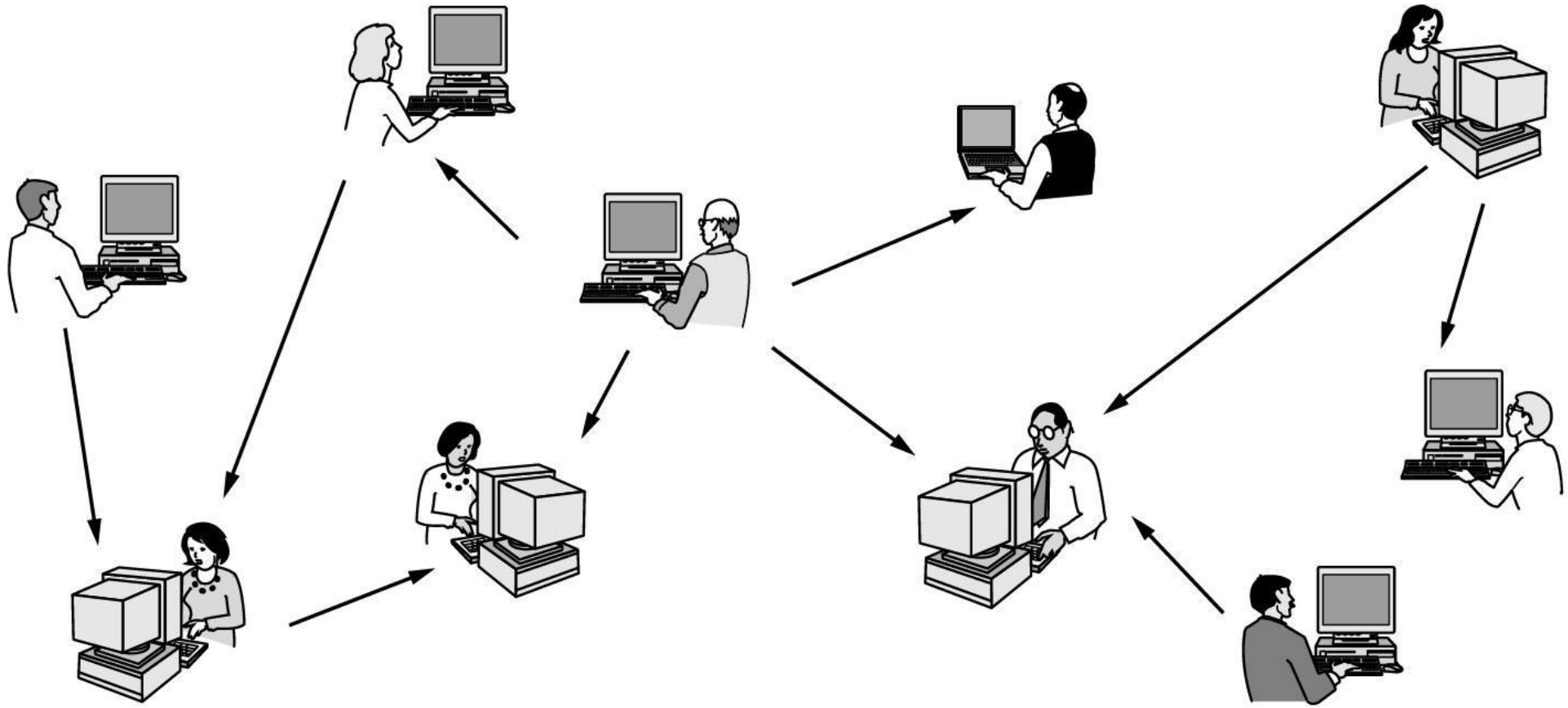
Home Network Applications

- Access to remote information
- Person-to-person communication
- Interactive entertainment
- Electronic commerce

Home Network Applications

- Networks for People
  - **Access to remote information**
    - ✓e.g.: financial, shopping, customized newspapers, on-line digital library, WWW
  - **Person-to-person communication**
    - ✓email, video conference, newsgroup
  - **Interactive entertainment**
    - ✓VOD, interactive movies or TVs, game playing

Home Network Applications



In peer-to-peer system there are no fixed clients and servers.

Home Network Applications

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

Some forms of e-commerce.

Mobile Network Users

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	NO	Networks in older, unwired buildings
Yes	Yes	Store inventory with a handheld computer

Combinations of wireless networks and mobile computing.

Social Issues

- **Network neutrality**
- **Digital Millennium Copyright Act**
- **Profiling users**
- **Phishing**

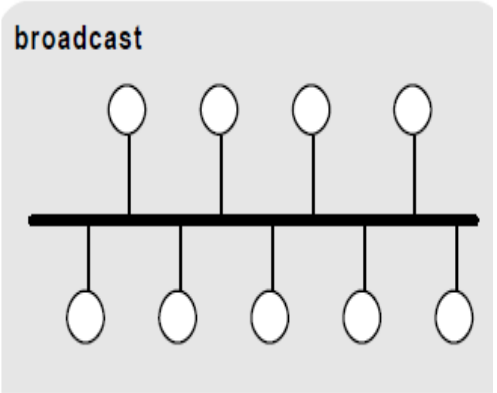
NETWORK HARDWARE

NETWORK HARDWARE

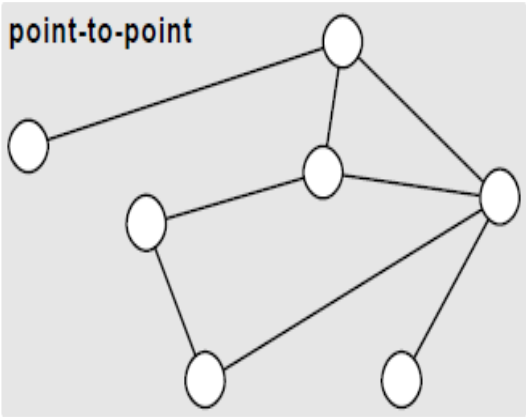
- The user machines in a network are called **hosts**.
- The hosts are connected by a **subnet** which carries messages between hosts.
- The subnet is made up of **transmission lines** (trunks, channels, circuits) and **switching elements** (computers).
- Computer Networks can be classified by two dimensions:
  - **Transmission Technology**
  - **Scale**

- There are two types of transmission technology (subnet design):
- **Point-to-Point subnets:** Point-to-point links connect individual pairs of machines. (ex. Postal Service, mobile).
  - **Unicasting –** one sender and exactly one receiver
- **Broadcast subnets:** In this system a message is broadcast over the network and all machines have the possibility of receiving the message (ex. LAN, WAN).
  - **Broadcasting –** received and processed by every machine on the network
  - **Multicasting –** received and processed by subset of machines

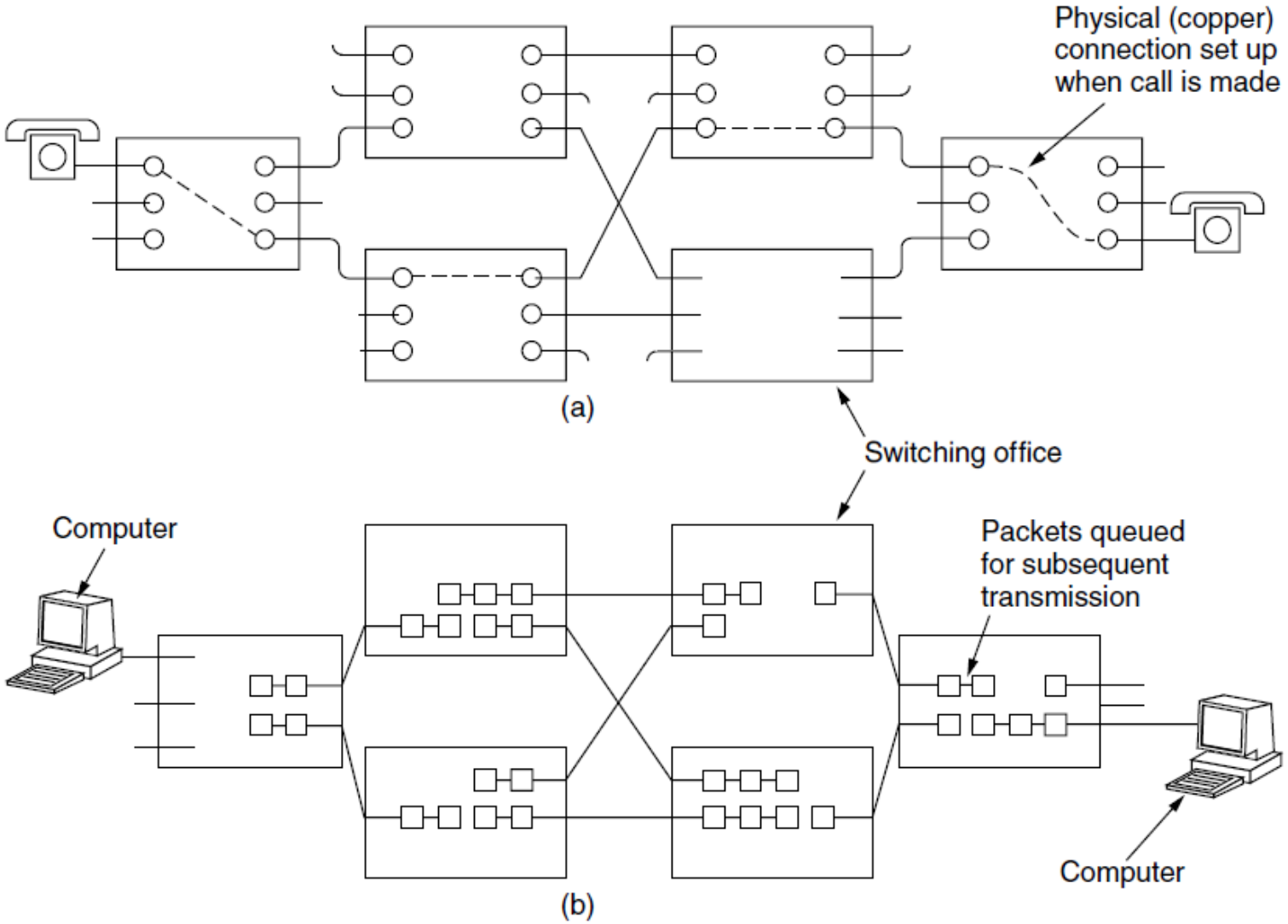
- **Broadcast Sub-networks:** These are typically configured as either a bus or a ring network. They can be further classified as Static or Dynamic.
- In static broadcast subnet the transmission is done turn by turn.
- **Advantage:** No collision of message and hence no corruption of message
- **Limitation:** In-sufficient use of network time
- In dynamic broadcast subnet the system allows any station to transmit at any time the network is free of traffic.



- **Point to Point Networks:** The second type of subnet, the point to point subnet, is mainly found in Wide Area Networks (WANs).
- If possible, the point to point subnet transmits directly to the relevant station. If no direct route is available, it will send the message to a "switch" which re-transmits the message to the destination.
- The best known example of this type of network is the telephone network (Public Switched Telephone Network or PSTN).



- In Point to point model, nodes either employ **circuit switching** or **packet switching.**
- In **circuit switching**,
  - a dedicated communication path is allocated between A and B, via a set of intermediate nodes.
  - the data is sent along the path as a continuous stream of bits.
- In **packet switching**,
  - data is divided into packets which are sent from A to B via intermediate nodes.
  - each intermediate node temporarily stores the packet and waits for the receiving node to become available to receive it.

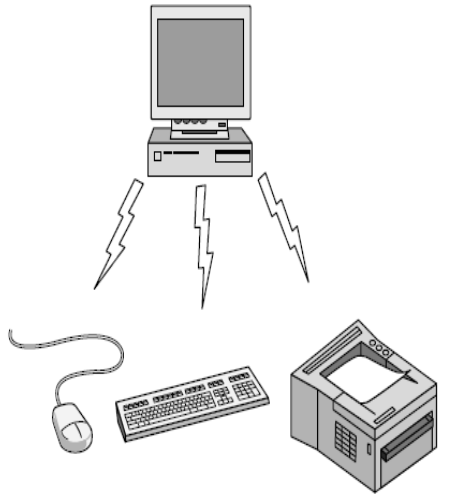

Physical (copper)
connection set up
when call is made
(a)
Switching office
Computer
Packets queued
for subsequent
transmission
Computer
(b)

- An alternative criterion for classifying networks is by **scale**. Distance is important as a classification metric because different technologies are used at different scales.
- **Personal Area Network (meant for one person)**
- **Longer range Network – LAN, MAN, WAN**
- **Internetwork**

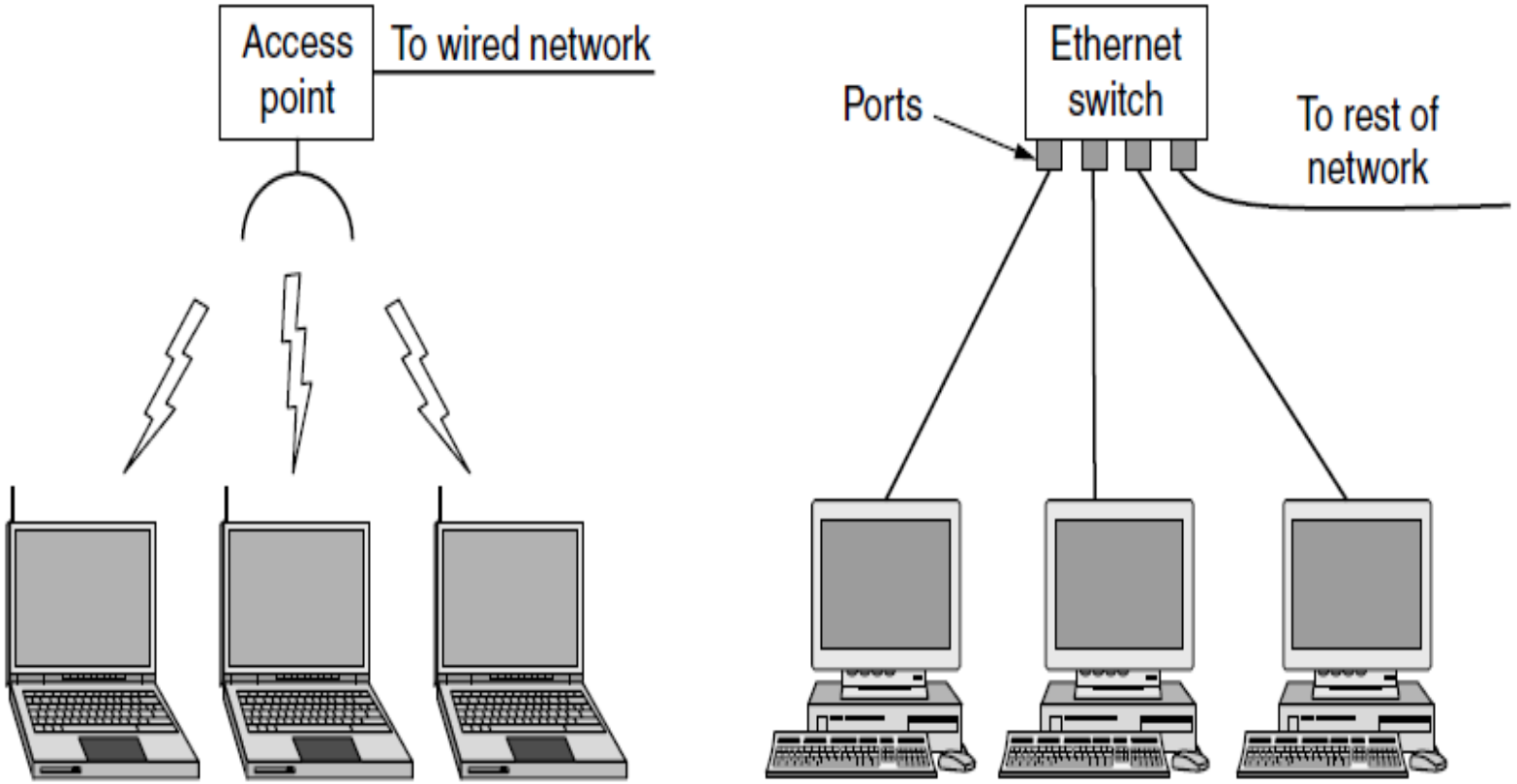
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Personal Area Networks (PAN)

- PANs let devices communicate over the range of a person (ex. Computer and its peripherals).
- PANs can also be built with other technologies that communicate over short ranges, such as RFID, Bluetooth, etc..
- These short range technologies use master-slave paradigm.



Local Area Networks (LAN)



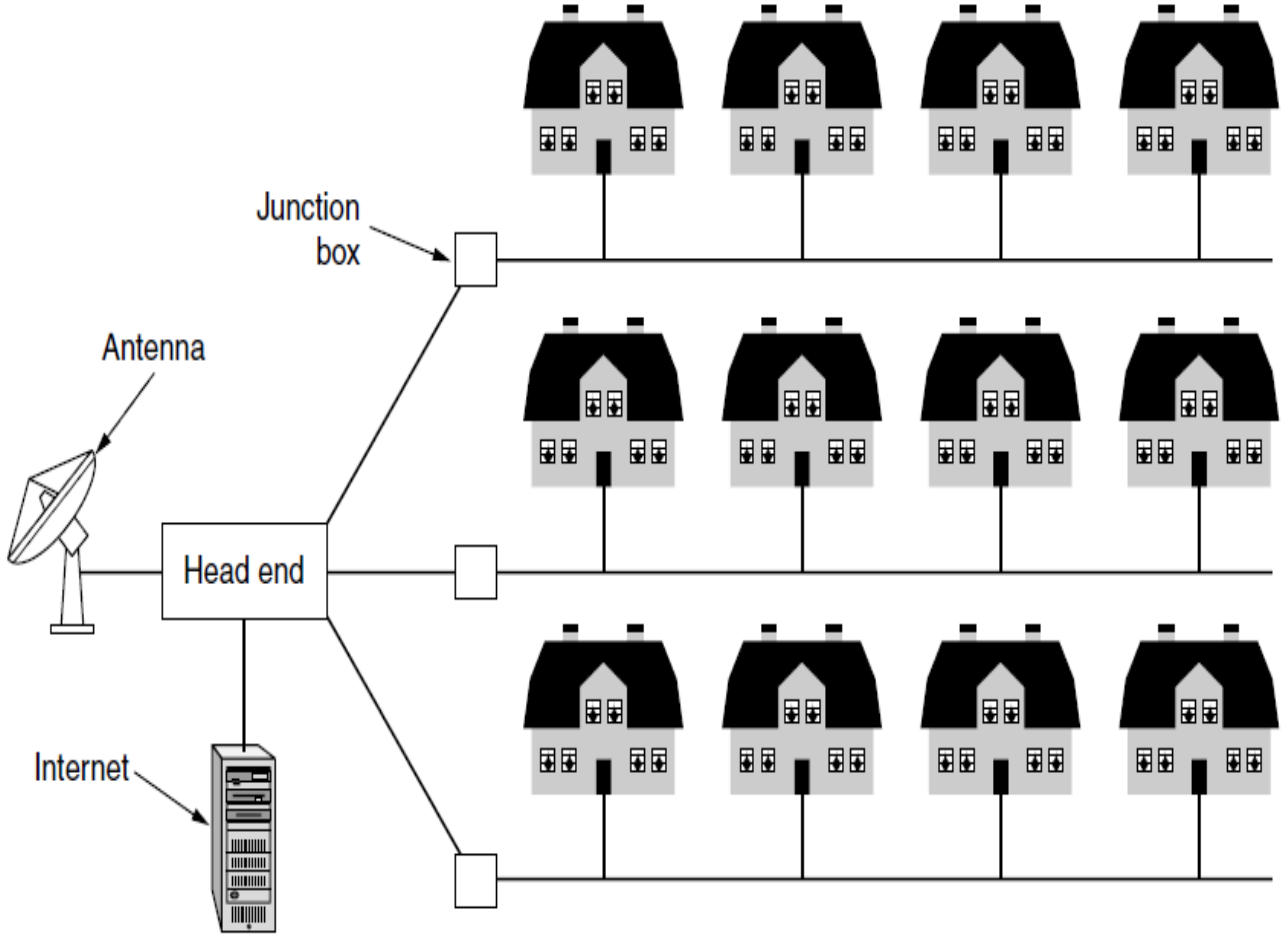
Local Area Networks (LAN)

- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are widely used to connect personal computers and consumer electronics to let them share resources (**ex. printers**) and exchange information.
- In another configuration it can be used as wireless LAN consisting of a radio modem and an antenna (**Access Point**).
- Typically, wired LANs run at speeds of 100 MBPS to 1 GBPS, have low delay (microseconds or nanoseconds), and make very few errors.
- Newer LANs can operate at up to 10 GBPS.
- Various topologies are possible for LAN (bus-based, ring-based N/W)
- Channel allocation can be Static or dynamic

Metropolitan Area Networks (MAN)

- A MAN is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or 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 (ex. Cable tv, high speed internet access WiMax).
- It may be private or public.
- It support data & voice.
- It has one or more cable and does not contain switching element.
- Channel allocation can be Static or dynamic

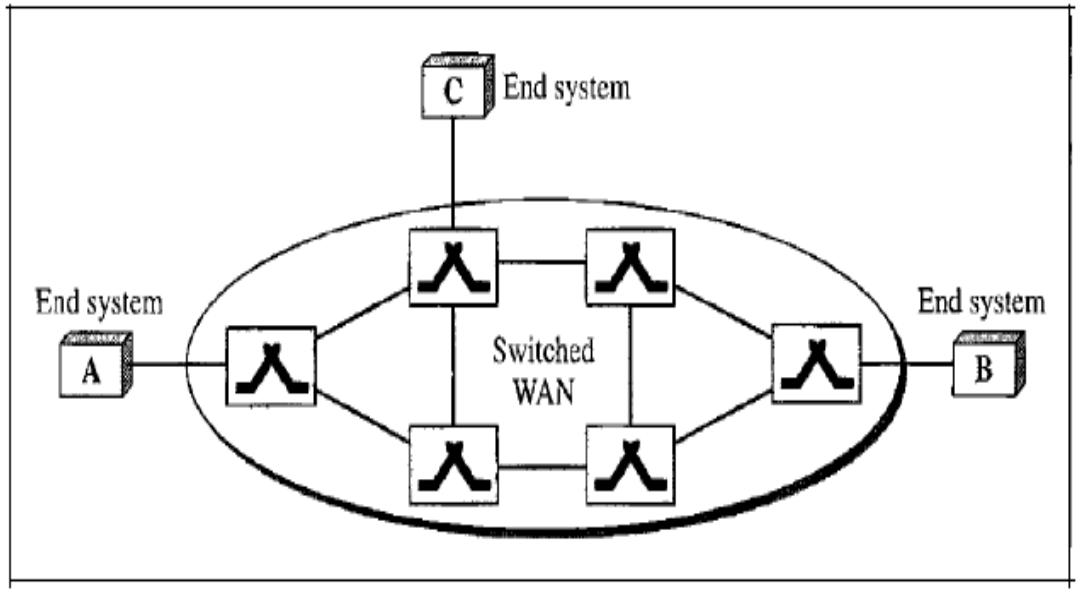
Metropolitan Area Networks (MAN)



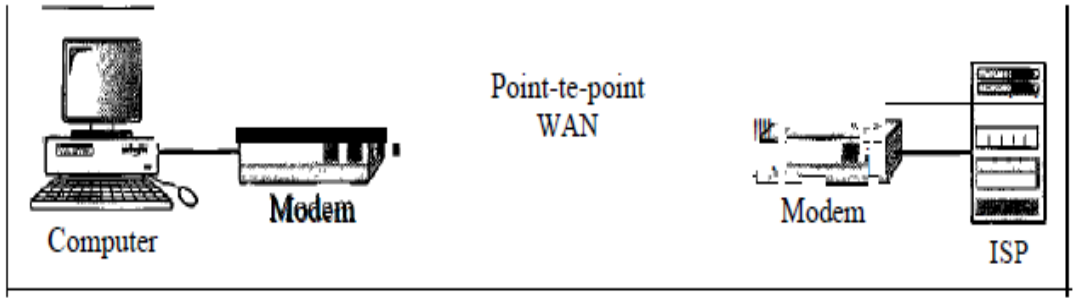
Wide Area Networks (WAN)

- A WAN spans a large geographical area, often a country or continent.
- It is available in two configurations namely switched WAN and poit-to-point WAN.
- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN (ex. ATM).
- 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 (lSP).

Wide Area Networks (WAN)



a. Switched WAN



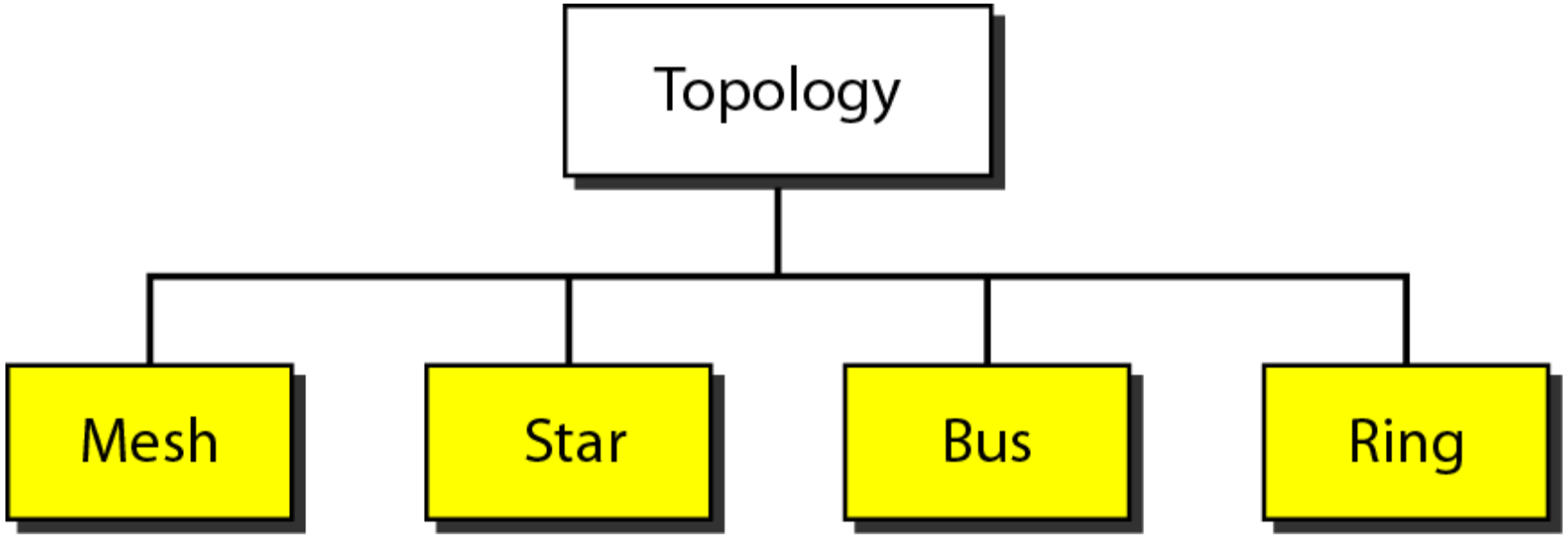
b. Point-to-point WAN

Internetworks

- A collection of interconnected networks is called an internetwork or internet.
- Connecting a LAN and a WAN or connecting two LANs is the usual way to form an internetwork.
- People on one n/w can communicate with people on different n/w.
- It is widely used to connect universities, government offices, companies and also private individuals.
- Applications: Email, News, Remote login, file transfer, etc…

NETWORK TOPOLOGY

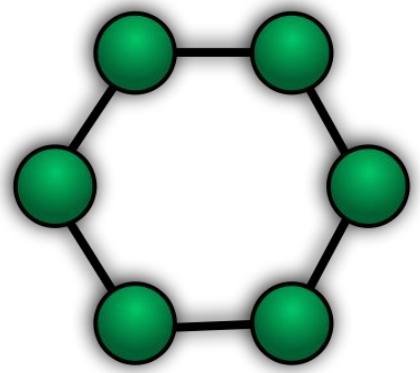
NETWORK TOPOLOGIES



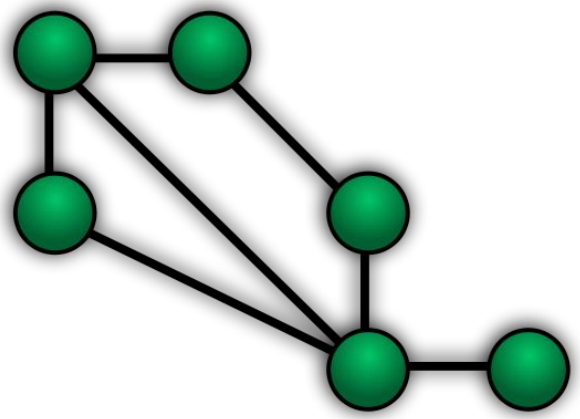
NETWORK TOPOLOGIES

- Computer networks can be configured in a number of ways.
- Messages are broken into smaller units called **packets** for transmission on a network.
- **Bus/Ring configuration:** Each packet of information is sent off around the ring on its own.
- **Complete network:** In this configuration each station is connected directly to every other station on the network.
- **Loop:** Each packet is transmitted along the line until it encounters a computer.
- **Tree**, Intersecting loop and Star configurations are same as above.

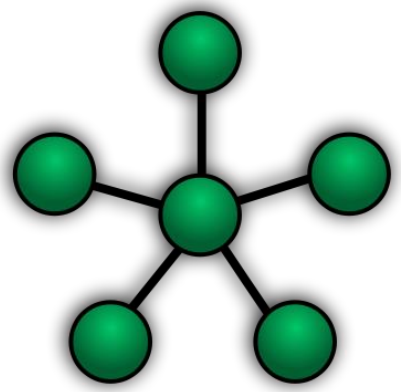
NETWORK TOPOLOGIES



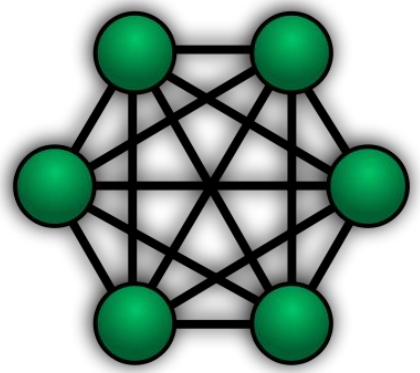
Ring



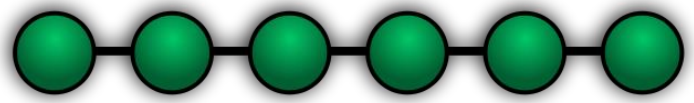
Mesh



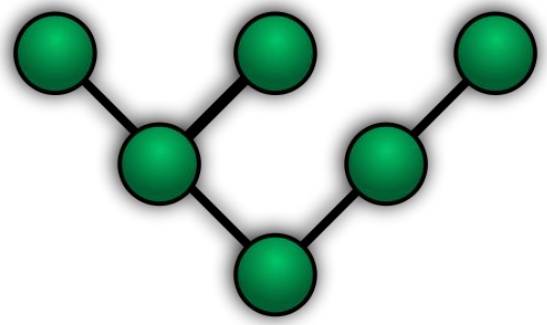
Star



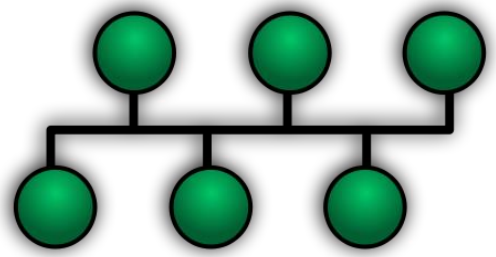
Fully Connected



Line



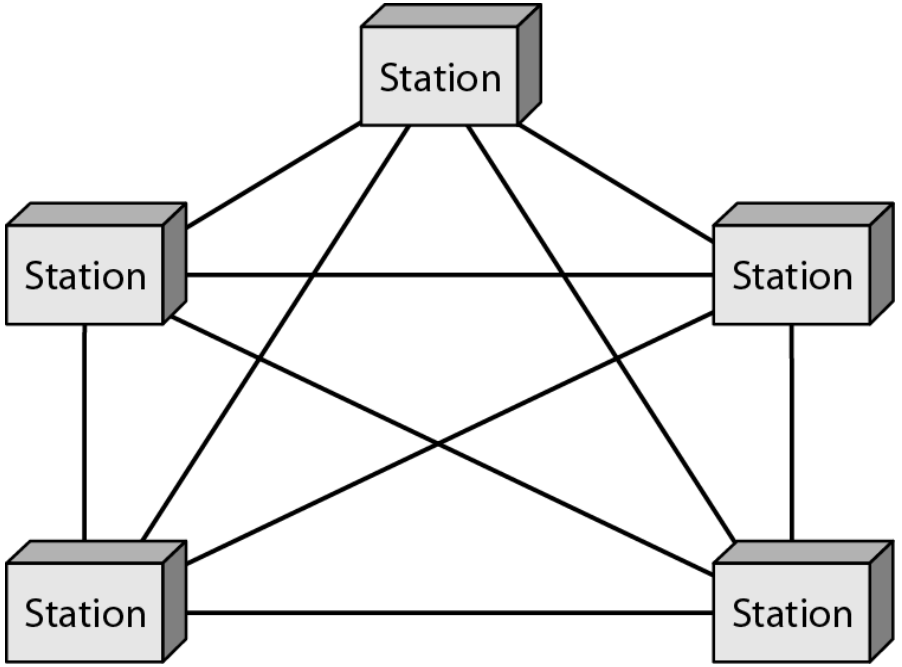
Tree



Bus

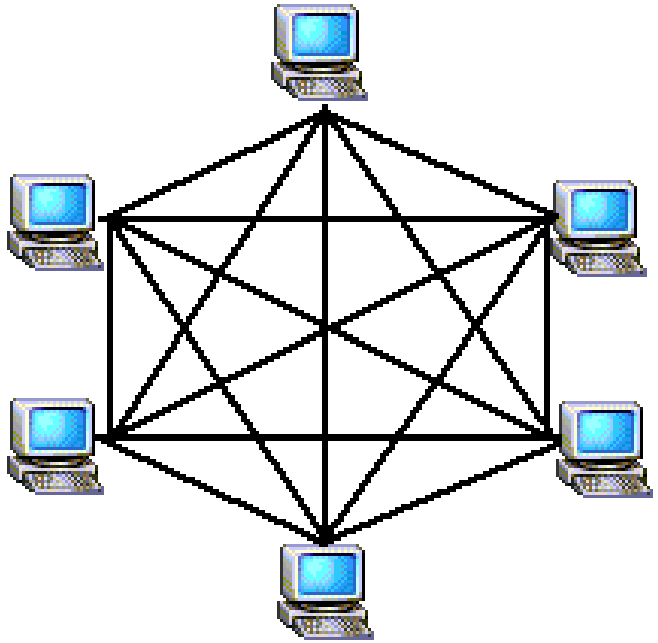
Mesh:

- Every link is dedicated point-to-point link
- The term dedicated means that the link carries traffic only between the two devices it connects



Mesh:

- To link **n** devices fully connected mesh has: **n (n - 1) / 2** physical channels (Full-Duplex)
- Every Device on the network must have **n - 1** ports



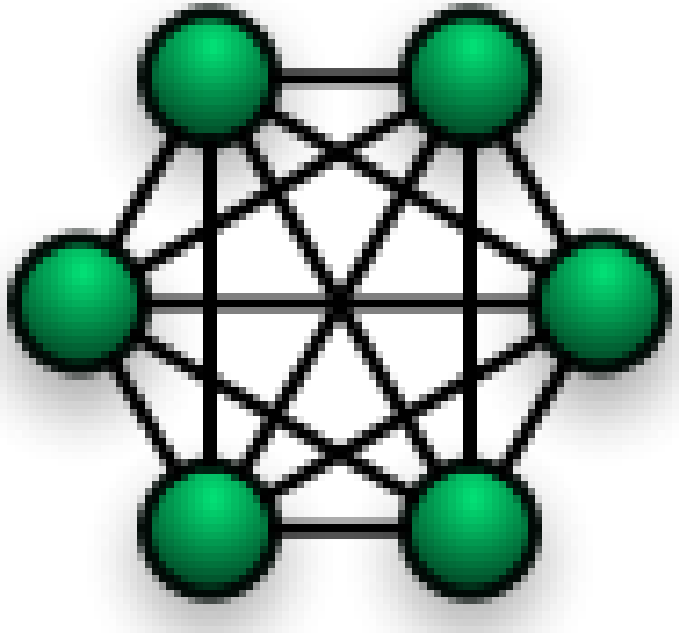
Mesh:

- Example:

  8 devices in mesh has links: n(n-1) / 2

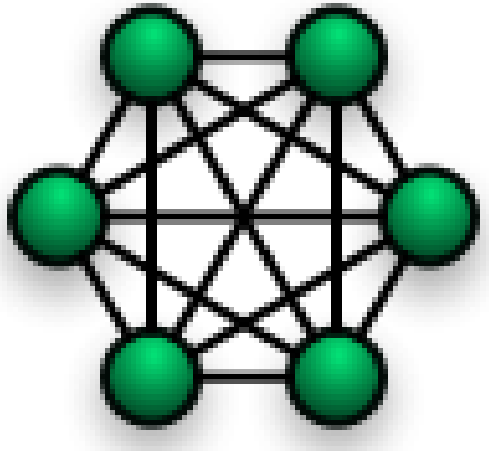
  number of links = 8 (8-1)/2 = **28**

  number of ports per device = n – 1 = 8 –1 = **7**

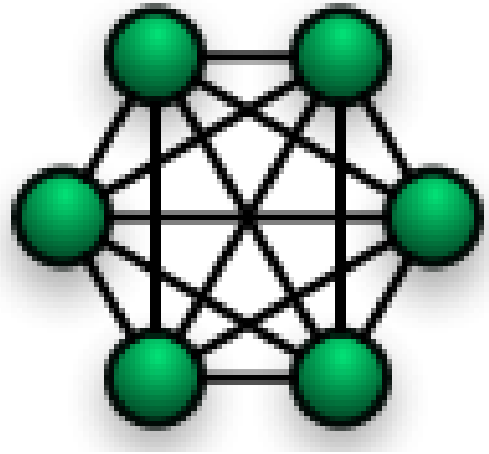


Mesh:

- **Advantages**
  - Each connection carry its own data load (no traffic problems)
  - A mesh topology is robust
  - Privacy or security
  - Fault identification and fault isolation
  -



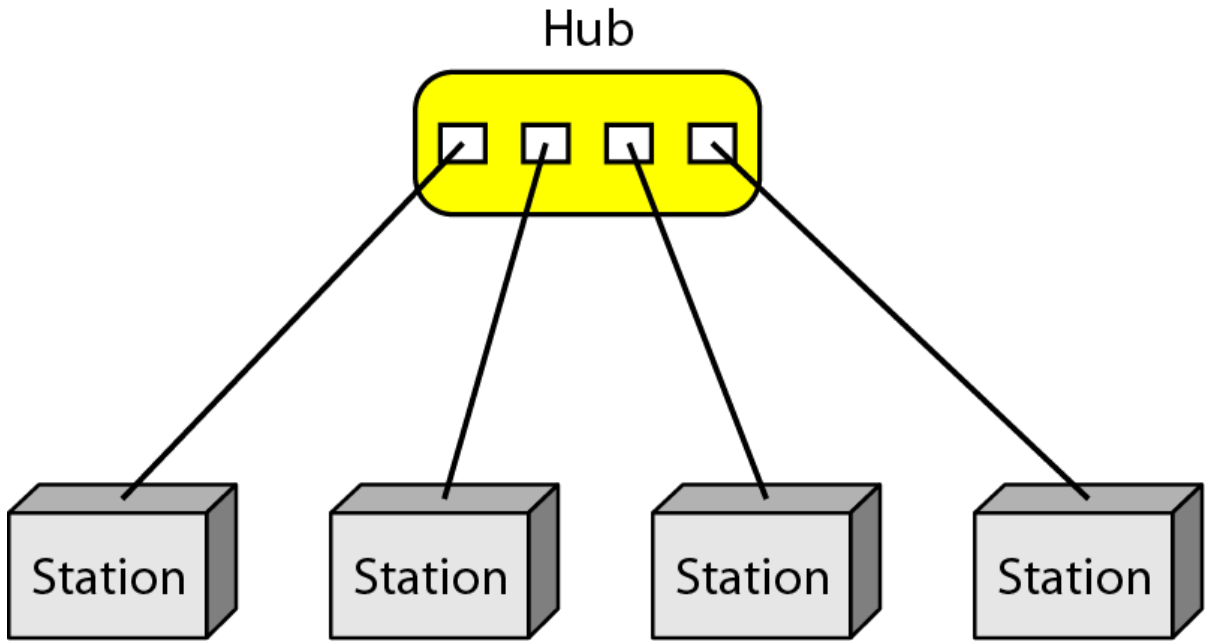
Mesh:



- **Disadvantages**
  - ✓ Big amount of cabling
  - ✓ Big number of I/O ports
  - ✓ Installation and reconnection are difficult
  - ✓ Sheer bulk of the wiring can be greater than the available space
  - ✓ Hardware connect to each I/O could be expensive
- Mesh topology is implemented in a limited fashion; e.g., as backbone of hybrid network

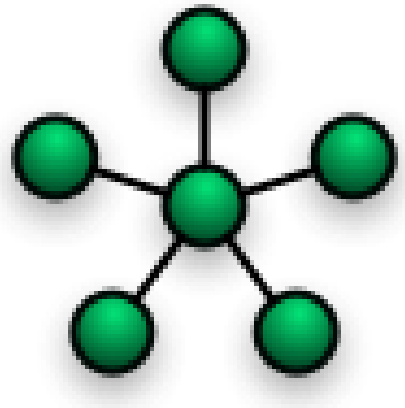
Star:

- Dedicated point-to-point to a central controller (Hub)
- No direct traffic between devices
- The control acts as an exchange



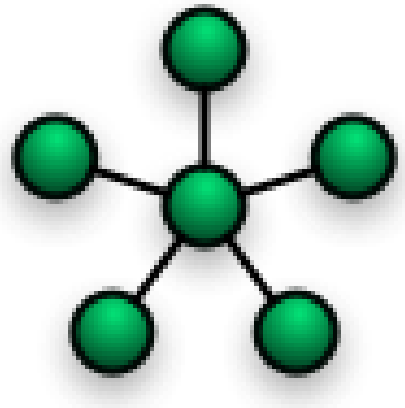
Star:

- **Advantages**
  - Less expensive than mesh (**1** Link + **1** port per device)
  - Easy to install and reconfigure
  - Less cabling
  - Additions, moves, and deletions required one connection
  - Robustness : one fail does not affect others
  - Easy fault identification and fault isolation



Star:

- **Disadvantages:**
  - Dependency of the whole topology on one single point (hub
  - More cabling than other topologies (ring or bus)
- Used in LAN

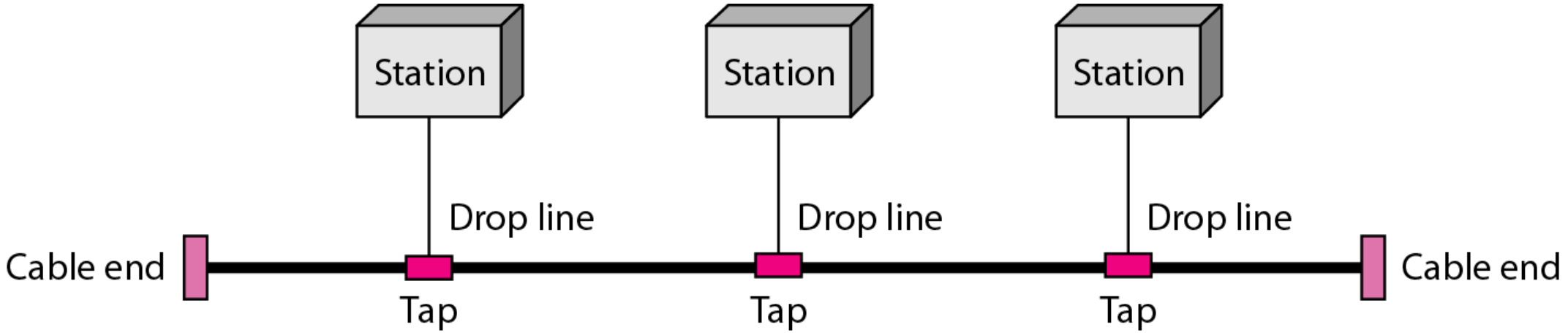


Bus:

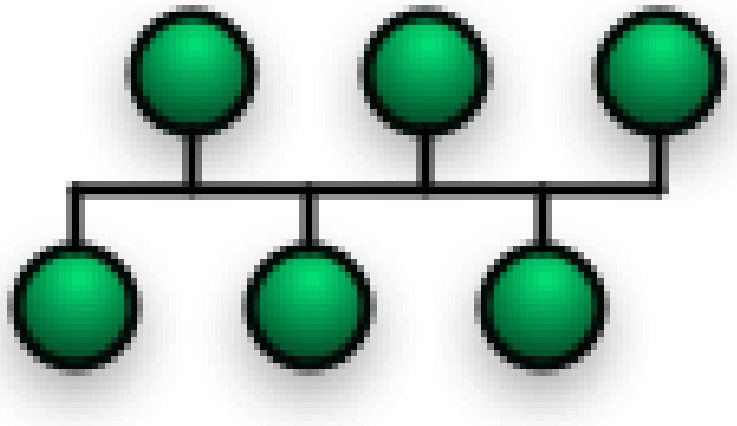
- It is multipoint
- One long cable acts as a backbone
- Used in the design of early LANS, and Ethernet LANs

Bus:

- Nodes connect to cable by drop lines and taps
- Signal travels along the backbone and some of its energy is transformed to heat
- Limit of number of taps and the distance between taps



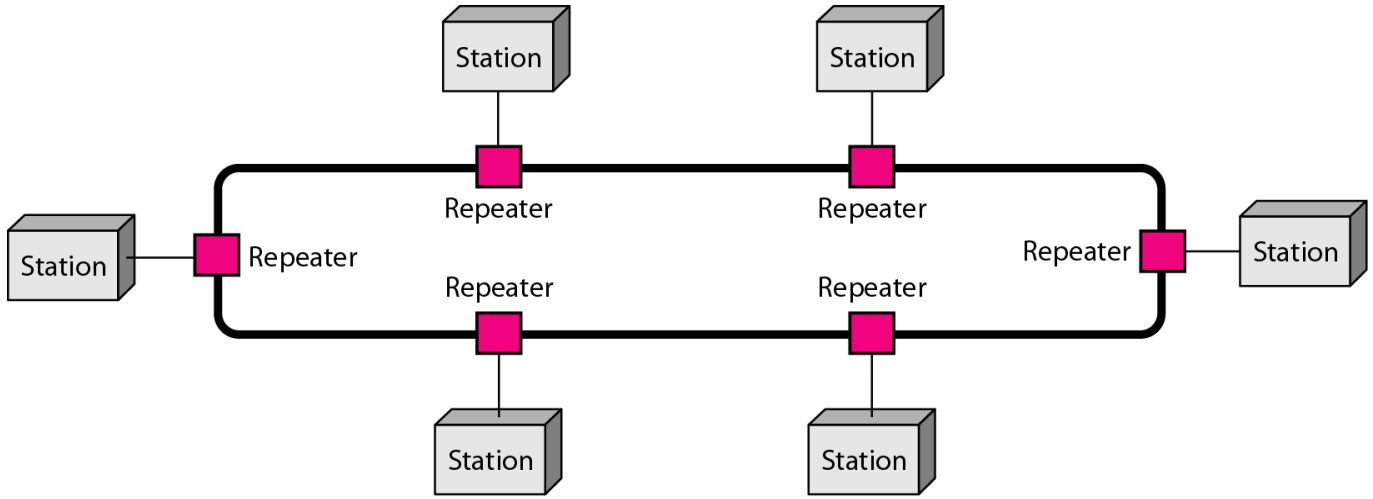
Bus:



- **Advantages**
  - Ease of installation
  - Less cables than mesh, star topologies
- **Disadvantages**
  - Difficult reconnection and fault isolation (limit of taps)
  - Adding new device requires modification of backbone
  - Fault or break stops all transmission
  - The damaged area reflects signals back in the direction of the origin, creating noise in both directions

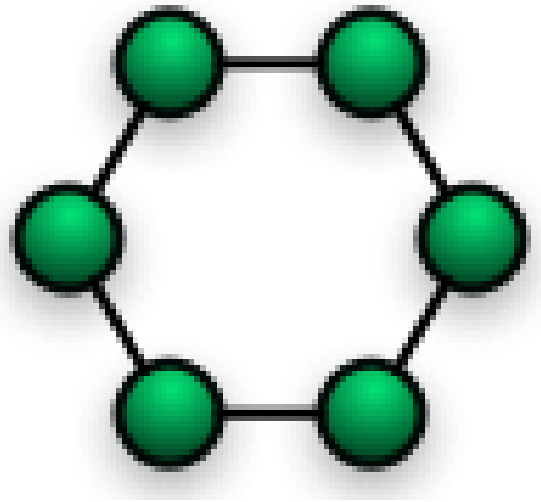
Ring:

- Each device has 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 devices incorporates a Repeater



Ring:

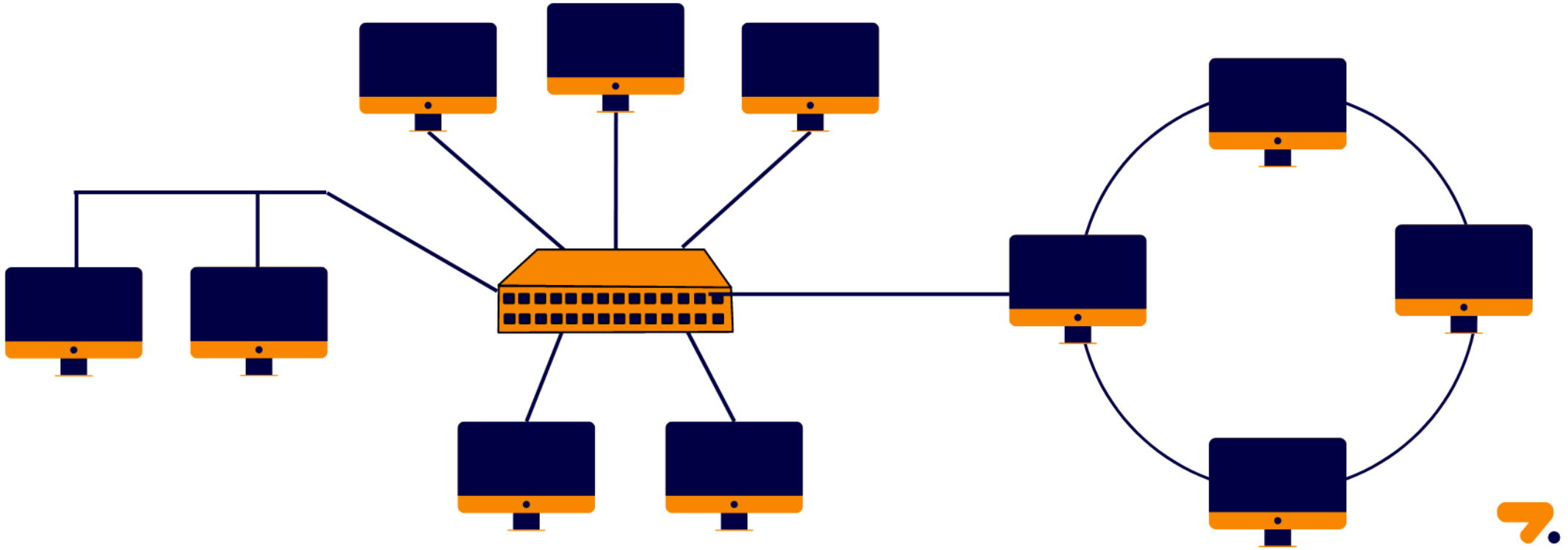
- **Advantages**
  - Easy of install and reconfigure
  - Connect to immediate neighbors
  - Move two connections for any moving (Add/Delete)
  - Easy of fault isolation



- **Disadvantages:**
  - Unidirectional
  - One broken device can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break

Hybrid Topology:

- **Example:** having a main star topology with each branch connecting several stations in a bus topology



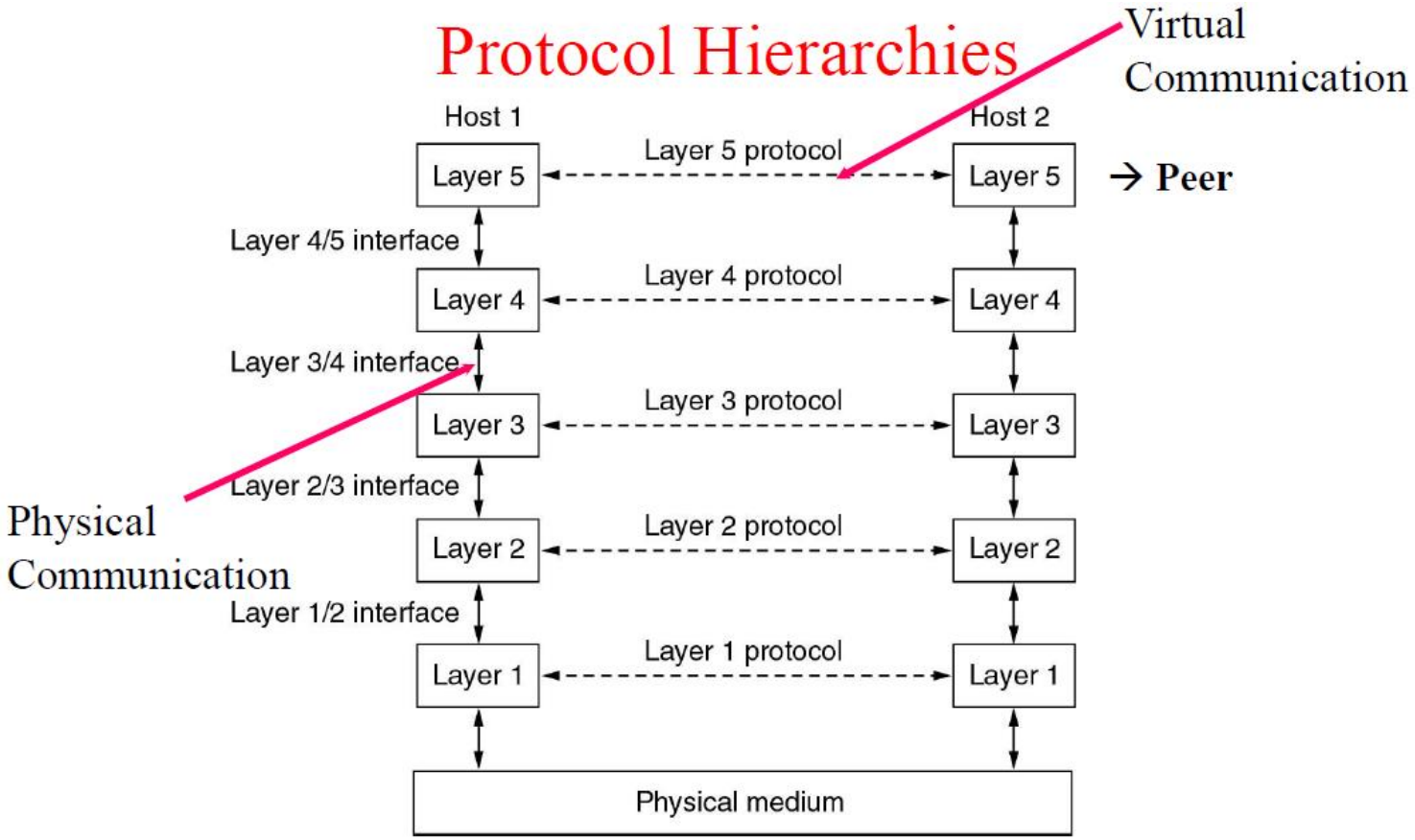
NETWORK SOFTWARE

NETWORK SOFTWARE

- The earlier computer networks were designed with the hardware as the main concern and the software as an afterthought.
- Now-a-days software are of prime importance and are highly structured.
  - Protocol Hierarchies (Layer structure)
  - Design Issues for the Layers
  - Connection-Oriented and Connectionless Services
  - Service Primitives
  - The Relationship of Services to Protocols

Protocol Hierarchies

- a series of layers (levels)
- lower layer provides service to higher layers
- **protocol:**
  - an agreement between the communication parties on how communication is to proceed
- **Peers:**
  - the corresponding layers on different machines.
- **Network architecture:** a set of layers and protocols
- **Protocol stack:**
  - a list of protocols used by a certain system, one protocol per layer



Layers, protocols, and interfaces.

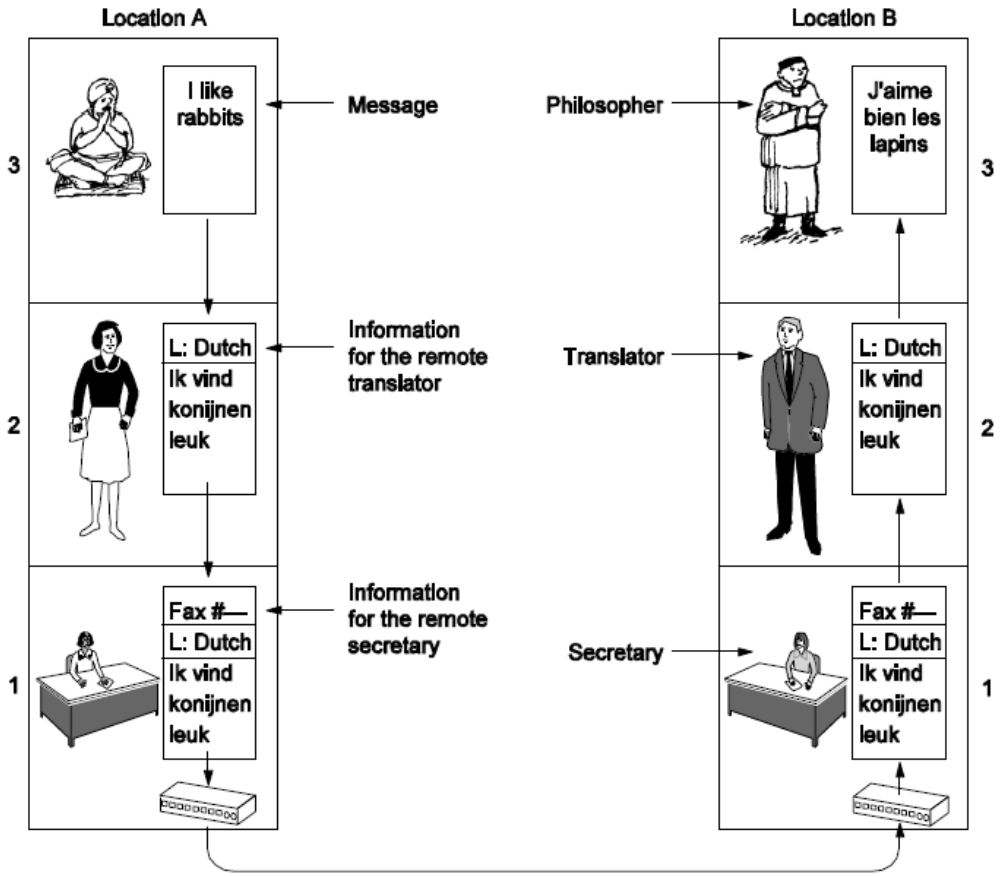
Network Architecture: A set of layers and protocols

Protocol Stack: A list of protocols used by a certain system, one protocol per layer.

Layering

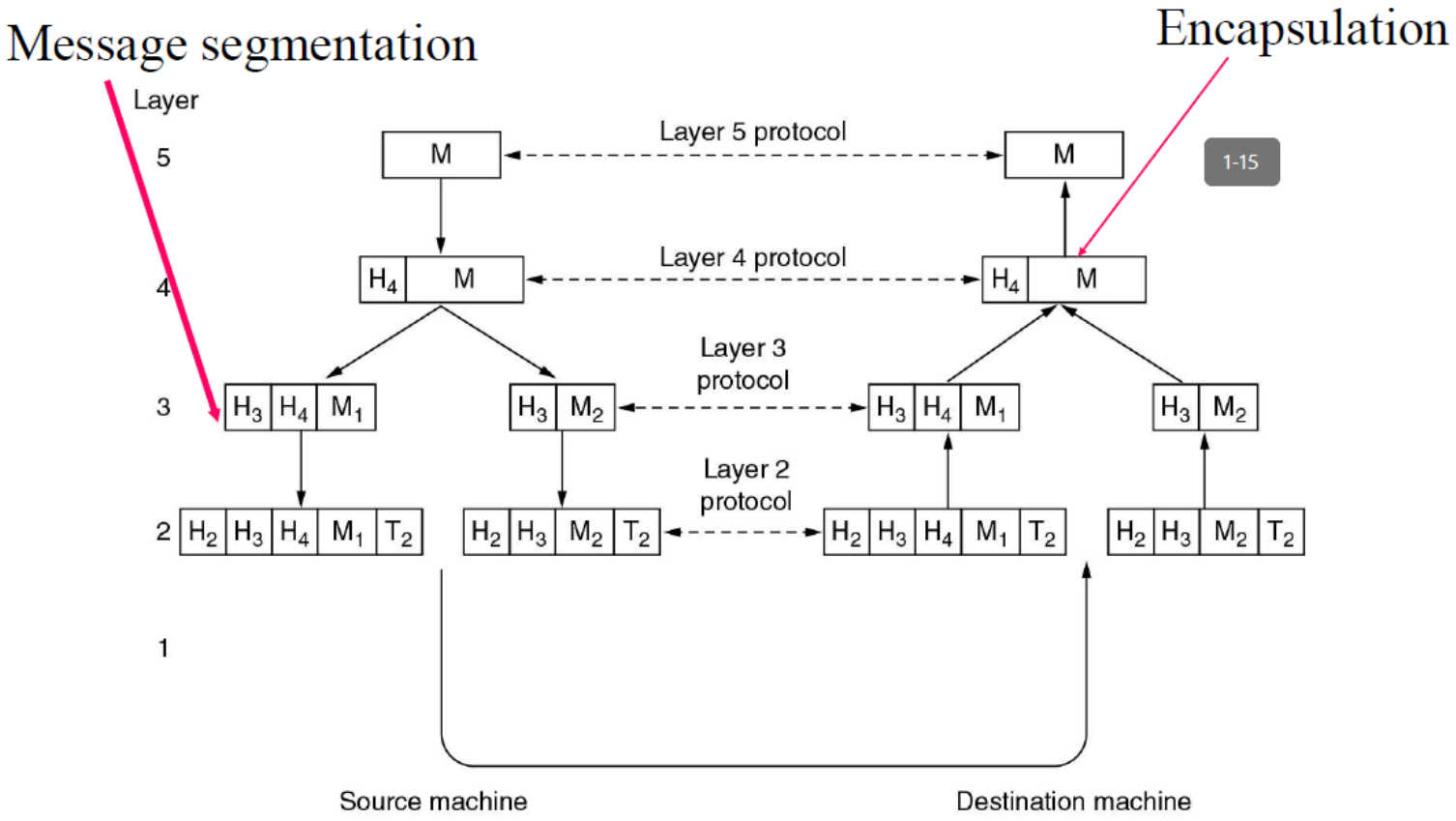
- To make things simple: modularization container
- Different layer has different functions
- Create layer boundary such that
  - description of services can be small
  - number of interactions across boundary are minimized
  - potential for interface standardized
- Different level of abstraction in the handling of data (e.g., syntax, semantics)
- Provide appropriate services to upper layer
- Use service primitives of lower layer

Protocol Hierarchies



The philosopher-translator-secretary architecture.

Protocol Hierarchies



Example information flow supporting virtual communication in layer 5.

37

Design Issues of Layers:

- There are some key design issues occur in computer networks are present in several layers
  - Addressing (telephone number, e-mail address, IP address,…)
  - Error Control (error correction codes, ARQ, HARQ,…)
  - Flow Control (feedback-based, rate-based)
  - Multiplexing (gathering several small messages with the same destination into a single large message or vice versa)
  - Demultiplexing
  - Routing (directing traffic to the destination)

Design Issues of Layers:

- **Identify senders and receivers**
  - multiple computers and processes: addressing
- **Data transfer**
  - simplex, half-duplex, full-duplex communication
  - # of logical channels per connections, priorities
- **Error control**
  - error detection
  - error correction
- **Sequencing of pieces**

Design Issues of Layers:

- **Flow control**
  - feedback from the receiver
  - agreed upon transmission rate
- **Length of messages**
  - long messages: disassemble, transmit, and reassemble messages
  - short messages: gather several small messages
- **Multiplexing and Demultiplexing**
  - when expensive to set up a separate connection
  - needed in physical layer
- **Routing: split over two or more layers**
  - High level: London -> France or Germany -> Rome
  - Low level: many available circuits

Connection Oriented and Connectionless Services:

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Six different types of service.

Interfaces and Services:

- The function of each layer is to provide services to the layer above it.
- The active elements in each layer are called entities.
- The entities in layer n implement a service used by layer n+1.
- The layer n is called service provider & layer n+1 is called the service user.

Service Primitives:

- A Primitive means operation
- A service in computer network consists of a set of primitives
- The primitives are to be used by a user to access the service
- The primitives asks the service to do some action or to report on an action
- The primitives are system calls
- The primitive varies for different services

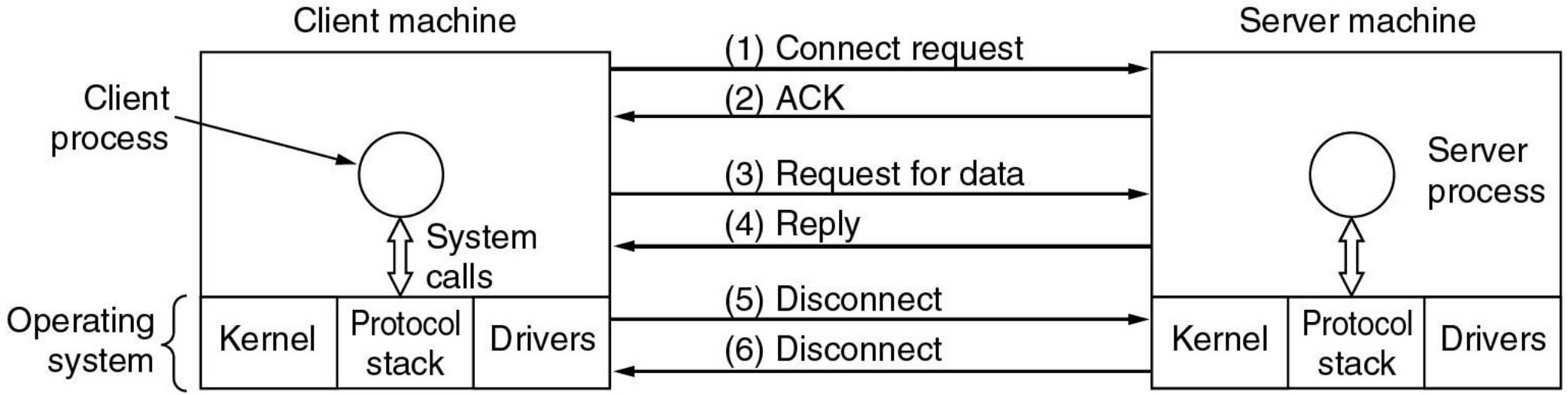
Service Primitives:

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

Six service primitives that provide a simple connection-oriented service

Service Primitives:

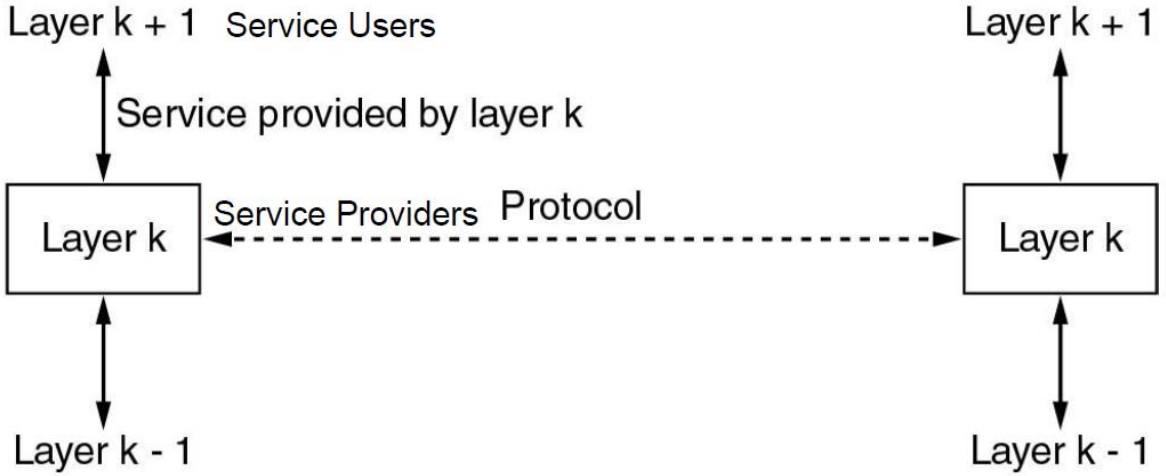
If the protocol stack is located in the operating system, the primitives are normally system calls.



Packets sent in a simple client-server interaction on a connection-oriented network.

Services to Protocols Relationship:

- The service defines what operations the layer is prepared to perform on behalf of its users
- A service is a set of primitives that a layer provides to the layer above it.
- A protocol is a set of rules governing the format and meaning of the packets which are exchanged by the peer entities in the same layer.
- Services related to the interfaces between layers;
- Protocols related to the packets sent between peer entities on different machine.



The relationship between a service and a protocol.

REFERENCE MODELS

REFERENCE MODELS

- OSI reference model
- TCP/IP reference model
- Comparison of OSI and TCP/IP
- Critique of OSI model and protocols
- Critique of the TCP/IP model

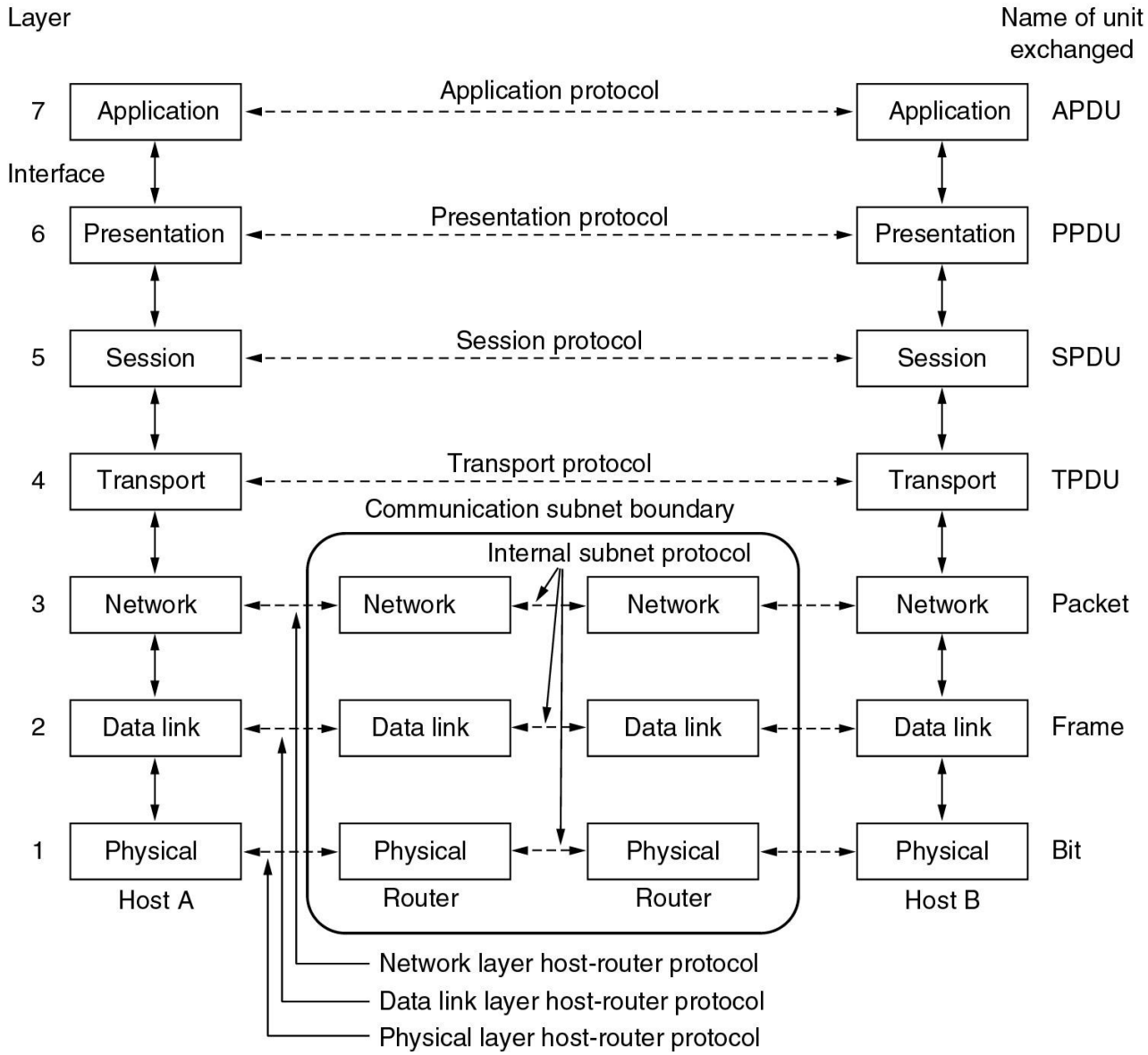
OSI REFERENCE MODEL

- This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (1983). o It was revised in 1995.
- The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems.
- The OSI model has 7 layers.
- OSI model itself is not a network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do.

The design principle of the OSI reference model:

- A layer should be created where a different abstraction is needed
- Each layer should perform a well defined function
- The function of each layer can be chosen as an international standard
- The layer boundaries should be chosen to minimize the information flow across the interfaces
- 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 does not become unwieldy.

OSI REFERENCE MODEL



Physical Layer:

- The Physical Layer is concerned with transmitting raw bits over a communication channel.
- It has to make sure that when one side sends a I bit, it is received by the other side as a '1' bit, not as a '0' bit.
- The typical questions here are:
  - How many volts should be used to represent a 1 and a 0;
  - How many nanoseconds a bit lasts;
  - Whether transmission may proceed simultaneously in both directions;
  - How the initial connection is established and how it is torn down when both sides are finished;
  - How many pins the network connector has and what each pin is used for;
- The design issues here largely deal with mechanical, electrical, and timing interfaces, and the physical transmission medium, which lies below the physical layer.

Functions of Physical Layer:

- Physical characteristics of interfaces and media defines the characteristics of interface between the devices and the transmission medium
- Representation of bits - conversion between representation of bits and corresponding signals
- Transmission rate - number of bits sent each second, the duration of a bit
- Synchronization of bits - the synchronization between sender and receiver clocks

Data Link Layer:

- The main task of The Data Link Layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer.
- The Data Link Layer executes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially.
- If the service is reliable, the receiver confirm correct receipt of each frame by sending back an acknowledgement frame.

Data Link Layer:

- Another issue that arises in Data Link Layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data.
- Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.
- **Medium access control sublayer:** which is the part of the data link layer in the broadcast networks, deals how to control access to the shared channel.

Functions of Data Link Layer:

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

Network Layer:

- The Network Layer controls the operation of the subnet.
- A key design issue is determining how packets are routed from source to destination.
- Routes can be based on static tables that are “wired info” the network and rarely changed.
- Tables can also be determined at the start of each conversation.
- Tables can be highly dynamic, being determined a new for each packet, to reflect the current network load.

Network Layer:

- The Network Layer controls the congestions when too many packets are present in the subnet at the same time;
- More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.
- Converting the addresses and packet sizes between networks is also a job of the network layer.
- In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

Network Layer:

- When a packet has to travel from one network to another to get to its destination, many problems can arise.
- The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on.
- It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

Functions of Network Layer:

- Logical addressing
- Routing

Transport Layer:

- The Transport Layer' s basic function is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- Furthermore, all this must be done efficiently and in a way that isolates the upper layer from the inevitable changes in the hardware technology.
- The Transport Layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network.

Transport Layer:

- An error-free point-to-point channel that delivers messages or bytes in the order in which they were sent is the most popular type of transport connection.
- The transport layer is a true end-to-end layer, all the way from the source to the destination.
- Due to the transport layer a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages.

Transport Layer:

- In the lower layers, the protocols are between each machine and its immediate neighbors, and not between the ultimate source and destination machines, which may be separated by many routers.
- The basic function of the transport layer is to accept data from session layer, split it up into smaller units and pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- The transport layer determines what type of service to provide to the session layer, and, ultimately, to the users of the network.
- The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.

Functions of Transport Layer:

- Port addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control

Session Layer:

- The Session Layer allows users on different machine to establish sessions between them.
- Sessions offer various services:
  - **Dialog control** (keeping track of whose turn it is to transmit);
  - **Token management** (preventing two parties from attempting the same critical operation at the same time);
  - **Synchronization** (check pointing long transmissions to allow them to continue from where they were after a crash).

Functions of Session Layer:

- It allows two applications running on different computers to establish, use and end a connection called a session.
- It performs name recognition and security.
- It provides synchronization by placing checkpoints in the data stream.
- It implements dialog control between communicating processes.

Presentation Layer:

- Unlike lower layers, which are mostly concerned with moving bits around, the Presentation Layer is concerned with the syntax and semantics of the information transmitted.
- In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used “on the wire”.
- The Presentation Layer manages these abstract data structures and allows higher-level data structures to be defined and exchanged.

Functions of Presentation Layer:

- **Data compression** — reduction in the size of data to achieve faster transmission over the network
- **Data encryption** — translation of data from a format used by application layer into a common format and vice-versa.
- **Protocol translation** — conversion of data from one protocol to another to transfer between different platforms or operating systems.

Application Layer:

- The Application Layer contains a variety of protocols that are commonly needed by users.
- One widely used application protocol is HTTP (Hyper Text Transfer Protocol) which is the basis for World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.
- Other application protocols are used for file transfer, electronic mail, and network news.

Functions of Application Layer:

- Mail services - basis for email forwarding and storage
- File transfer and access
- Remote login
- Accessing the world wide web

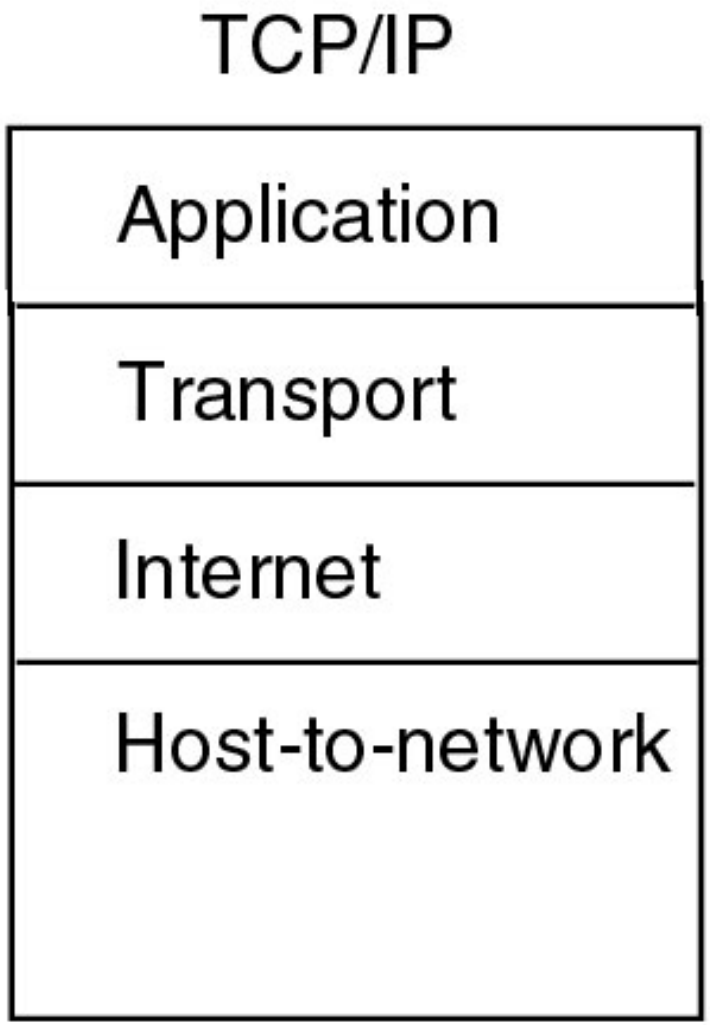
THE TCP / IP REFERENCE MODEL

- TCP/IP reference model originates from the grandparent of all computer networks, the ARPANET and now is used in its successor, the worldwide Internet.
- The ARPANET was a research network sponsored by the DOD (U.S. Department of Defense) that connected hundreds of universities and government installations, using leased telephone lines.
- When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so a new reference architecture was needed. This architecture later became known as the TCP/IP Reference Model, after its two primary protocols.

THE TCP / IP REFERENCE MODEL

- It was first defined in 1974. A later perspective is give in 1985.
- DOD wanted connections to remain intact as long as the source and destination machines were functioning, even if some of the machines or transmission lines in between were suddenly put out of operation.
- Furthermore, a flexible architecture was needed since applications with divergent requirements were envisioned, ranging from transferring files to real time speech transmission.
- The TCP/IP Reference Model includes 4 layers.

THE TCP / IP REFERENCE MODEL



Host – to – Network Layer:

- Host-to-Network Layer allow the host to connect to the network using some protocol so it can send IP packets to it.
- Protocols used here are not defined and vary from host to host and network to network.

Internet Layer:

- The Internet Layer provides a packet-switching network based on a connectionless internetwork layer;
- The Internet Layer permits hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network);
- They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.
- The Internet Layer defines an official packet format and protocol called IP (Internet Protocol).
- Packet routing is clearly the major issue in the Internet Layer, as is avoiding congestion.
- The job of the internet layer is to deliver IP packets where they are supposed to go.

Transport Layer:

- TCP/IP internet layer is similar in functionality to the OSI network layer
- This layer is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer.
- Two end-to-end transport protocols have been defined here.
  - TCP (Transmission Control Protocol)
  - UDP (User Datagram Protocol)

Transport Layer:

Transmission Control Protocol

- TCP is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
- It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer.
- At the destination, the receiving TCP process reassembles the received messages into the output stream.
- TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

Transport Layer:

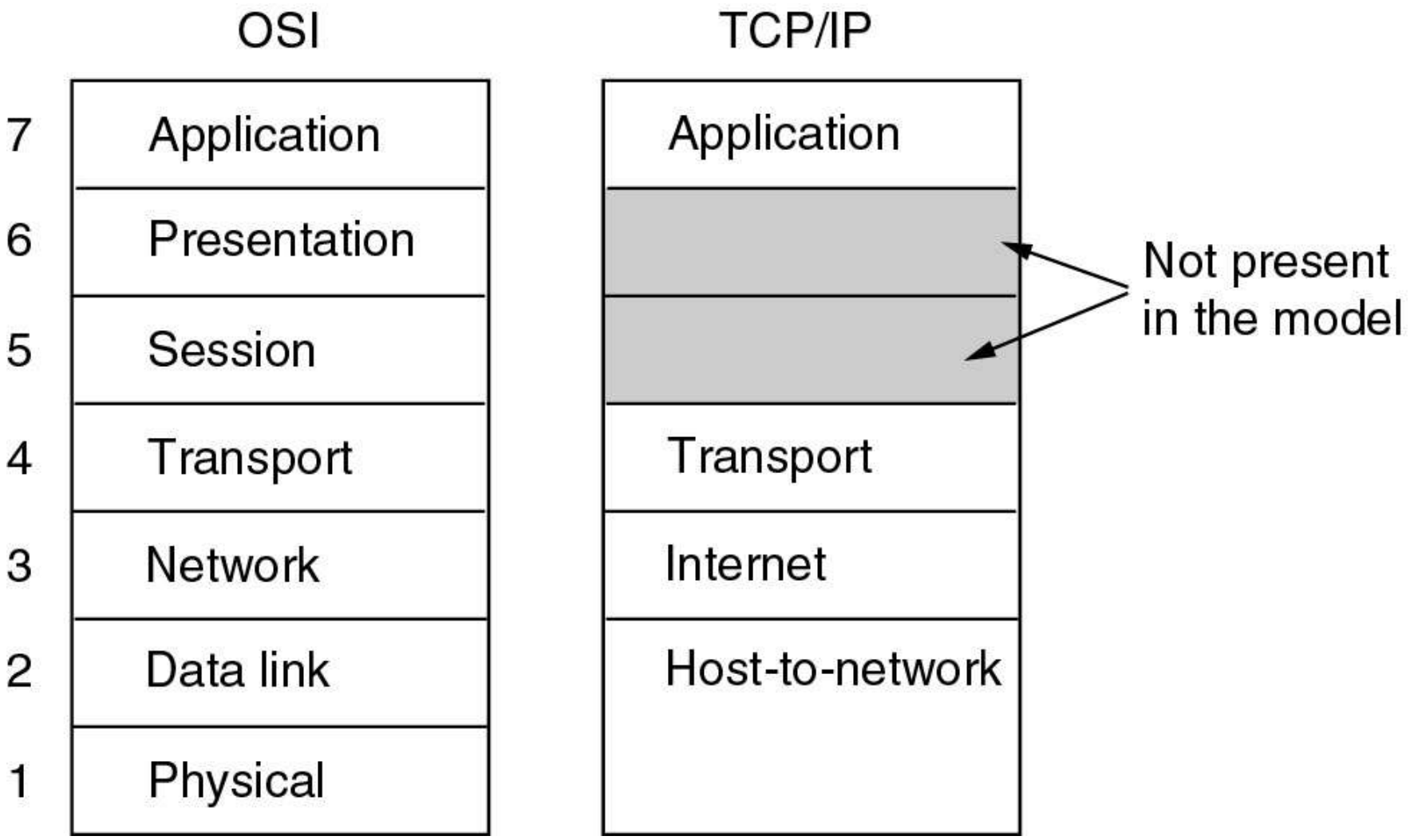
User Datagram Protocol

- UDP is an unreliable connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.
- It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

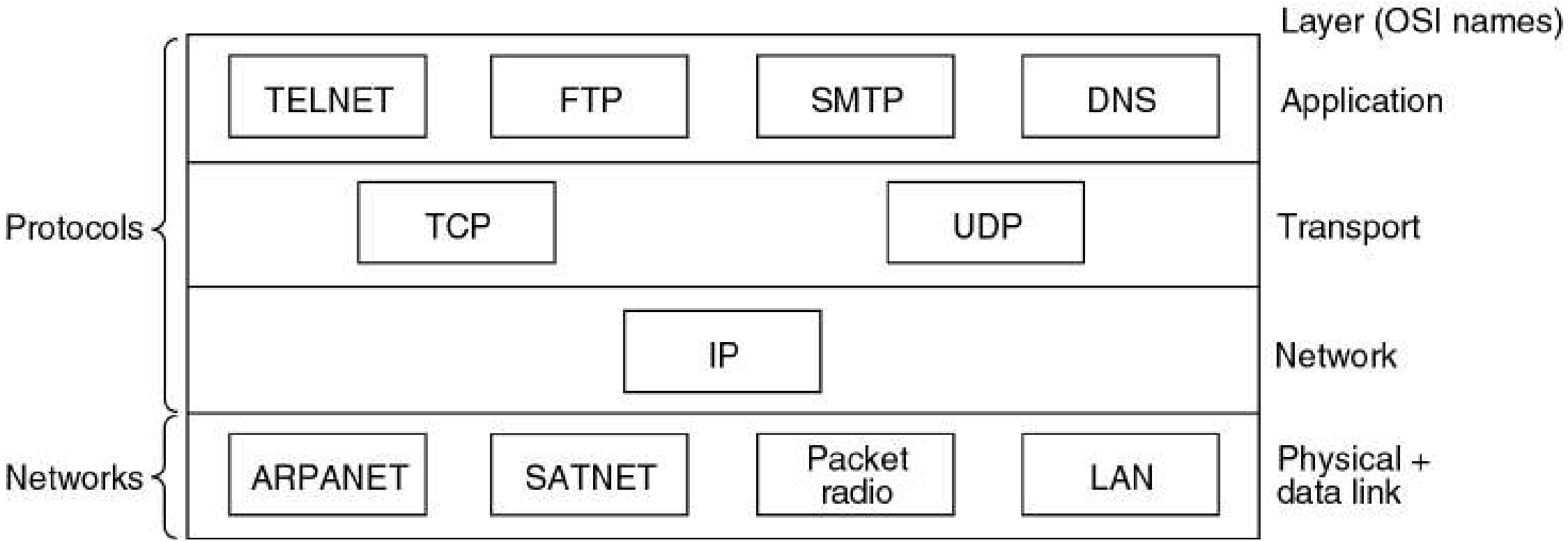
Application Layer:

- It contains all the higher-level protocols such as virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP), DNS, NNTP and HTTP.
- The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there.
- The file transfer protocol provides a way to move data efficiently from one machine to another.
- Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it.
- Domain Name System (DNS) for mapping host names onto their network addresses.
- NNTP, the protocol for moving USENET news articles around
- HTTP, the protocol for fetching pages on the World Wide Web, and many others.

THE TCP / IP REFERENCE MODEL



THE TCP / IP REFERENCE MODEL



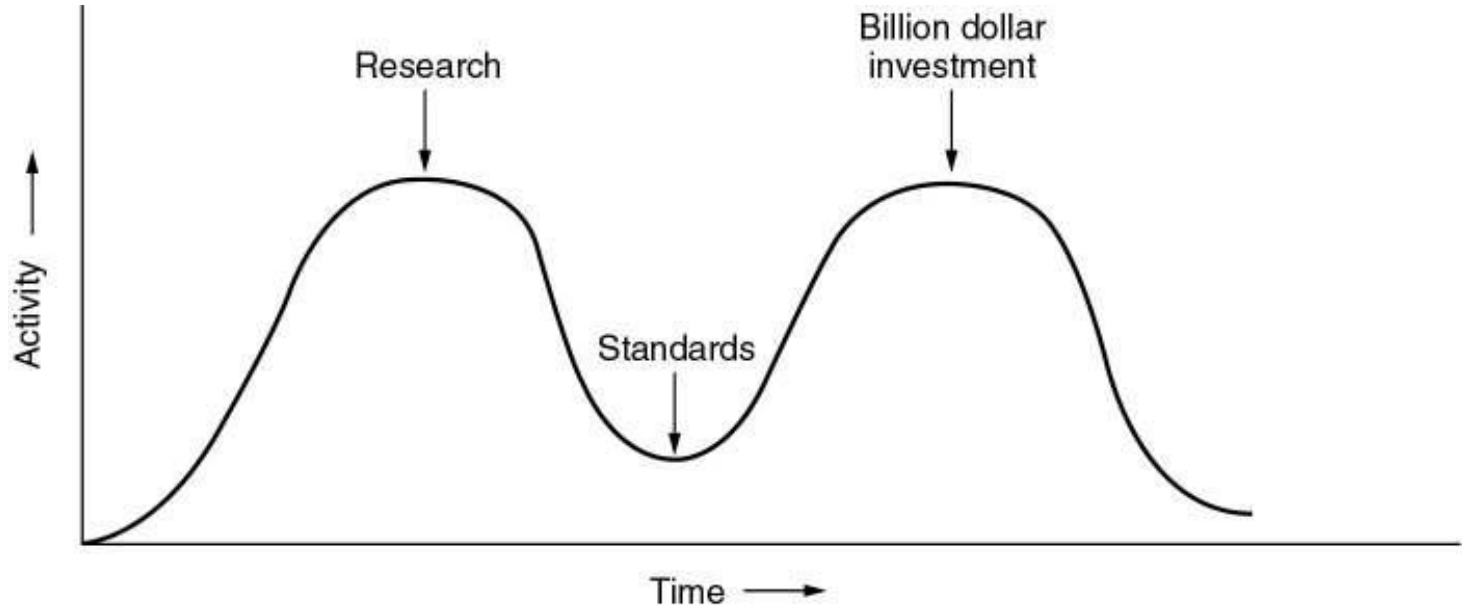
Protocols and networks in the TCP/IP model initially.

A critique of the OSI Model and Protocols

- Neither the OSI model and its protocols nor the TCP/IP model and its protocols are perfect.
- Initially it appeared to many experts in the field that the OSI model and its protocols were going to take over the world and push everything else out of their way.
- This did not happen. The model was criticized on the basis of following reasons:
    1. Bad timing
    2. Bad technology
    3. Bad implementations
    4. Bad politics

Bad timing

- The time at which a standard is established is absolutely critical to its success.
- David Clark of M.I.T. has a theory of standards that he calls the apocalypse of the two elephants is shown below:



The apocalypse of the two elephants.

Bad timing

- This figure shows the amount of activity surrounding a new subject.
- When the subject is first discovered, there is a burst of research activity in the form of discussions, papers, and meetings.
- After a while this activity subsides, corporations discover the subject, and the billion-dollar wave of investment hits.
- It is essential that the standards be written in the trough in between the two "elephants.“
- If the interval between the two elephants is very short (because everyone is in a hurry to get started), the people developing the standards may get crushed.

Bad Technology

- The second reason is that both the model and the protocols are flawed.
- The choice of 7 layers was more political than technical, and two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull.
- The OSI model, along with the associated service definitions and protocols, is extraordinarily complex.
- Some functions, such as addressing, flow control, and error control, reappear again and again in each layer. For example, error control must be done in the highest layer to be effective, repeating it over and over in each of the lower layers is unnecessary and inefficient.

Bad Implementations

- Due to enormous complexity of the model and the protocols, the initial implementations were huge, unwieldy, and slow.
- Everyone who tried them got burned.
- It did not take long for people to associate "OSI" with "poor quality."
- Although the products improved in the course of time, the image stuck.

Bad Politics

- On account of the initial implementation, many people, especially in academia, thought of TCP/IP as part of UNIX, and UNIX in the 1980s in academia was considered apple pie.
- OSI, on the other hand, was widely thought to be the creature of the European telecommunication ministries, the European Community, and later the U.S. Government.
- This belief was only partly true.

A critique of the OSI Model and Protocols

- The TCP/IP model and protocols have their problems too.
- First, the model does not clearly distinguish the concepts of service, interface, and protocol. Good software engineering practice requires differentiating between the specification and the implementation, something that OSI does very carefully, and TCP/IP does not.
- Consequently, the TCP/IP model is not much of a guide for designing new networks using new technologies.

A critique of the OSI Model and Protocols

- Second, the TCP/IP model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.
- Trying to use the TCP/IP model to describe Bluetooth, for example, is completely impossible.
- Third, the host-to-network layer is not really a layer at all in the normal sense of the term as used in the context of layered protocols.
- It is an interface (between the network and data link layers). The distinction between an interface and a layer is crucial, and one should not be sloppy about it.

A critique of the OSI Model and Protocols

- Fourth, the TCP/IP model does not distinguish (or even mention) the physical and data link layers. These are completely different.
- The physical layer has to do with the transmission characteristics of copper wire, fiber optics, and wireless communication.
- The data link layer's job is to delimit the start and end of frames and get them from one side to the other with the desired degree of reliability.
- A proper model should include both as separate layers. The TCP/IP model does not do this.

A critique of the OSI Model and Protocols

- Finally, although the IP and TCP protocols were carefully thought out and well implemented, many of the other protocols were ad hoc, generally produced by a couple of graduate students.
- The protocol implementations were then distributed free, which resulted in their becoming widely used, deeply entrenched, and thus hard to replace. Some of them are a bit of an embarrassment now.
- The virtual terminal protocol, TELNET, for example, was designed for a ten-character per second mechanical Teletype terminal. It knows nothing of graphical user interfaces and mice. Nevertheless, 25 years later, it is still in widespread use.

A critique of the OSI Model and Protocols

- In summary, despite its problems, the OSI model (minus the session and presentation layers) has proven to be exceptionally useful for discussing computer networks. In contrast, the OSI protocols have not become popular.
- The reverse is true of TCP/IP: the model is practically nonexistent, but the protocols are widely used.