Computer Networks

Andrew S Tanenbaum

4th Edition

Syllabus

Module I

Introduction – Uses – Network Hardware – LAN – MAN – WAN, Internetworks – Network Software – Protocol hierarchies – Design issues for the layers – Interface & Service – Service Primitives. Reference models – OSI – TCP/IP.

Data Link layer Design Issues – Flow Control and ARQ techniques. Data link Protocols – HDLC. DLL in Internet.

Introduction

- Computer Network:
  - Interconnected collection of autonomous computers
  - 2 computers are interconnected if they are able to exchange information
  - *Communication* is the process of *exchanging information* between two persons or devices
  - Connection can be made via *copper wire*, *fiber optics*, *microwaves or communication satellites* etc
  - If one computer cannot forcibly start, stop or control another computer then it is termed as autonomous

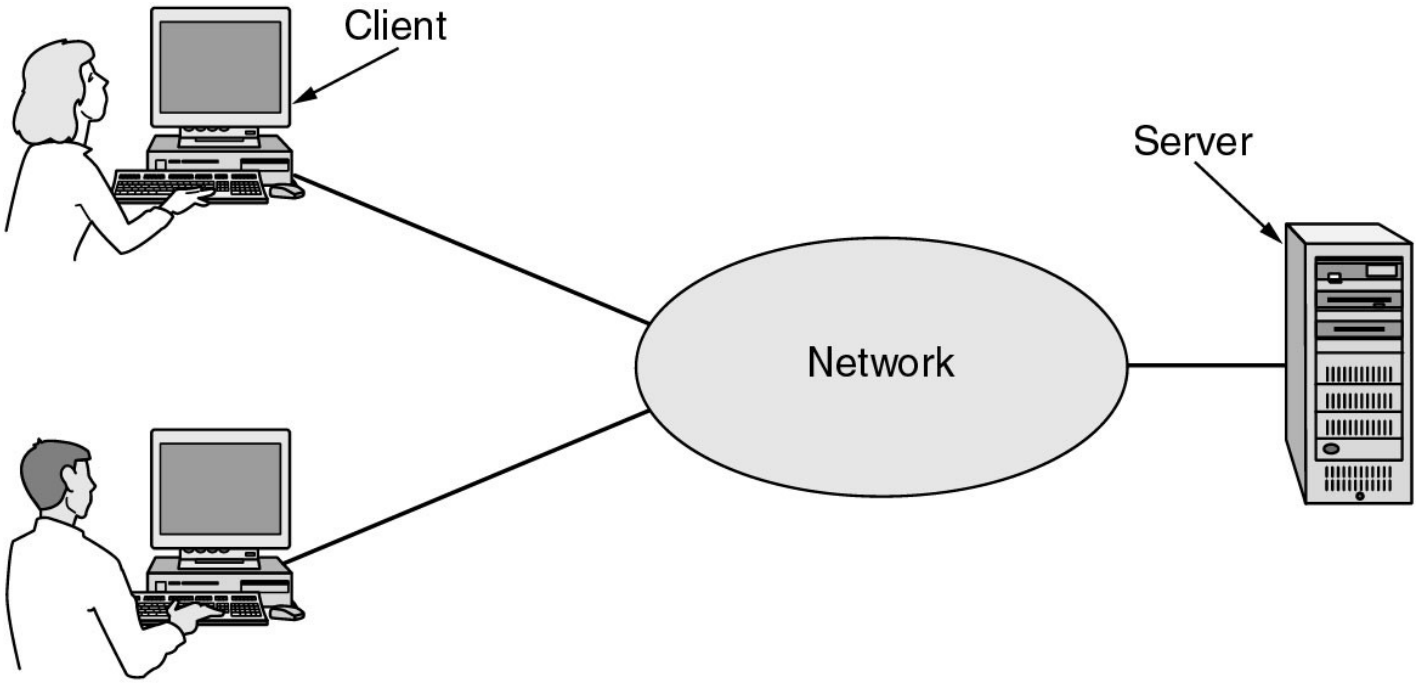
Uses of Computer Networks

- Business Applications or
  Networks for companies
- Home applications or
  Networks for People
- Mobile Network Users
- Social Issues

Uses of Computer Networks

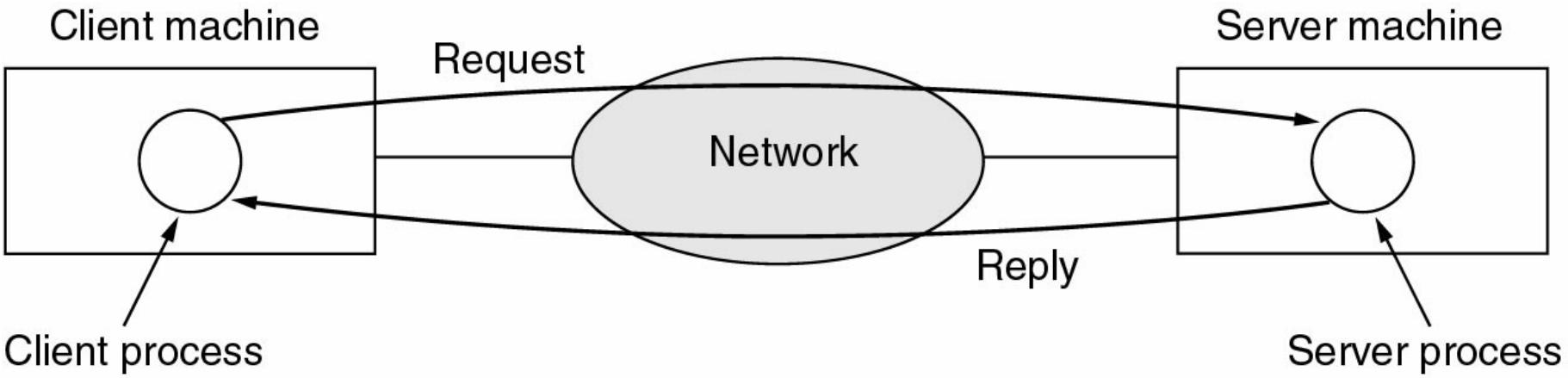
- Business Applications
  - Resource Sharing
    - programs, equipment, data etc
  - High reliability
    - alternative sources of supply
  - Saving money
    - by having client server model
  - Scalability
    - Ability to increase system performance
  - Powerful Communication medium
    - online documents, human to human communication

Business Applications of Networks



A network with two clients and one server.

Business Applications of Networks



The client-server model involves requests and replies.

Home Network Applications

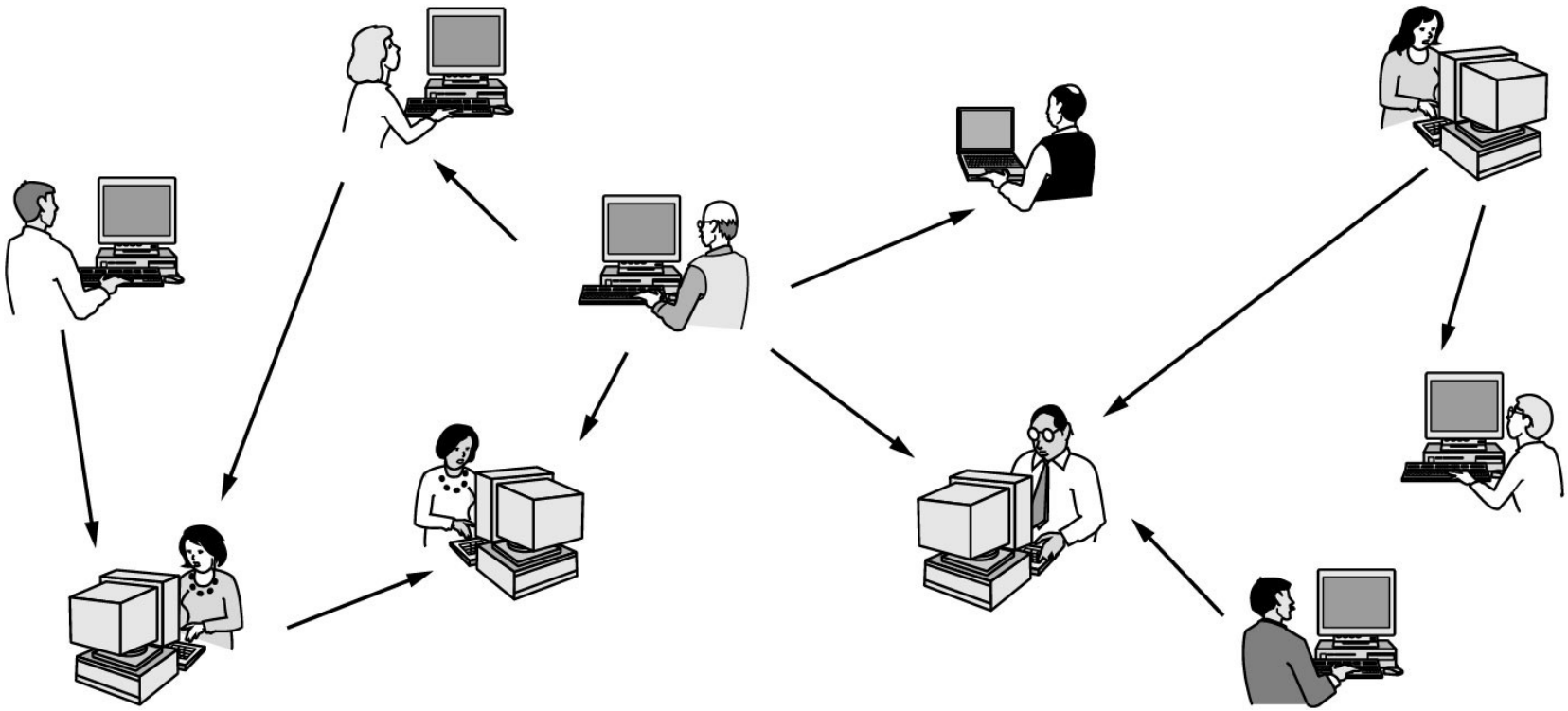
- Access to remote information
  - Home shopping
  - Online newspaper
  - Access to WWW
- Person-to-person communication
  - E-mails
  - Video conference
  - Worldwide newsgroup

Home Network Applications

- Interactive entertainment
  - Video on demand
  - Live Television
  - Game playing
- Electronic commerce (e-commerce)
  - convenience of shopping from home with online catalogs

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

Home Network Applications



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

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	Portable office; PDA for store inventory

- Mobile commerce (m-commerce)

Social Issues

- Exchange messages using newsgroup may lead to conflicts
- Employee rights vs employer rights
- Network offers the potential to send anonymous messages
- Electronic junk mails (Spam) may contain viruses
- Copyright violation due to transmission of music & videos

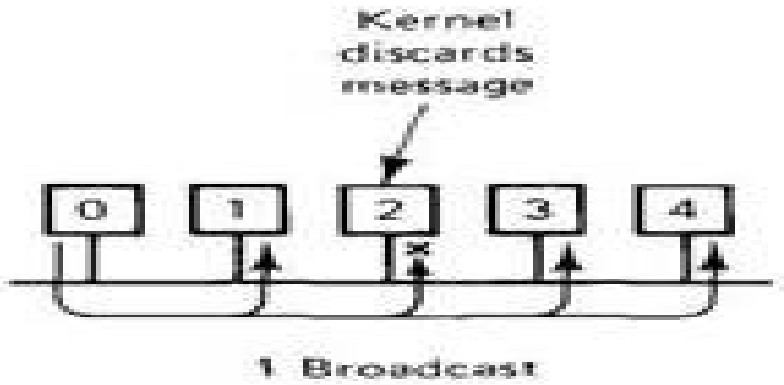
Network Hardware

- Based on types of transmission technology
  - Broadcast Networks
  - Point-to-point Networks
- Based on Scale

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

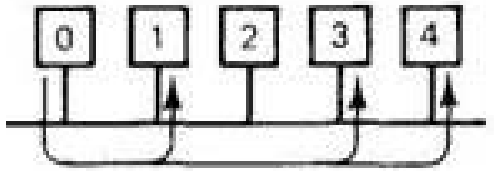
Network Hardware

- Broadcast Networks
  - A *single communication channel* is shared by all the machines on the network
  - Short messages called ***packets*** sent by any machine are received by all the others
  - Address field in a packet specifies the recipient
  - After receiving the packet, the address field is checked
  - If it is intended for itself, it processes the packet, otherwise it is ignored



1 Broadcast

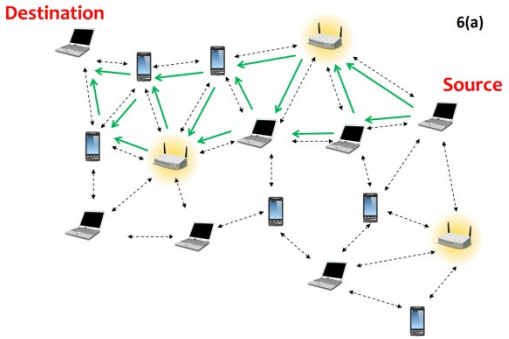
Network Hardware



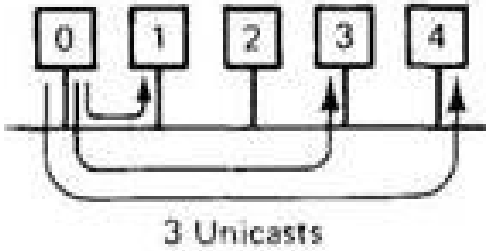
1 Multicast

- Broadcasting
  - Broadcast systems allow the possibility of addressing a packet to all destinations by using special code in the address field
  - Smaller localized network use broadcasting
- Multicasting
  - Broadcast systems also support transmission to a subset of the machines
  - By reserving a bit to indicate multicasting & the remaining n-1 address bits can hold the group number
  - Each machine can subscribe to any or one of the groups

Network Hardware



- Point-to-point Networks
  - Many connections between individual pair of machines
  - Transfer from source to destination may includes one or more intermediate machines
  - Multiple routes of different lengths leads to the role of routing algorithm for route selection
  - Larger networks use point-to-point
  - Point-to-point transmission with one sender and one receiver is sometimes called unicasting



Network Hardware

- Based on Scale
  - Personal Area Networks
  - Local Area Networks
  - Metropolitan Area Networks
  - Wide Area Networks
  - Internetworks or Internet

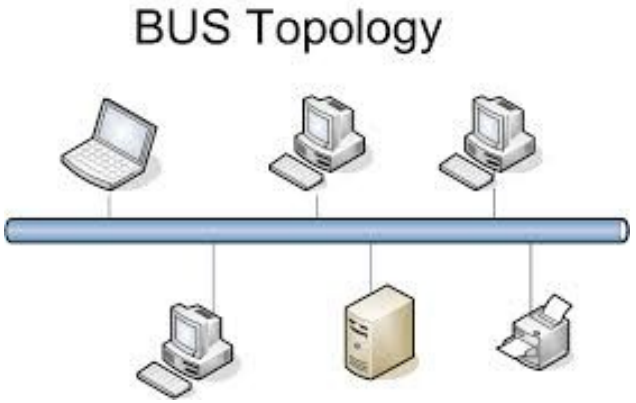
Network Hardware

- Personal Area Networks
  - Networks that are meant for one person
  - Eg: a wireless network connecting a computer with its mouse, keyboard, and printer
- Local Area Networks
  - Generally called as LANs
  - Privately owned networks
  - Inter-processor distance:10m to 1km
  - Networks placed in a single room or building or campus
  - LANs are distinguished by 3 characteristics –
    - Size
    - Transmission Technology
    - Topology

LAN

- **Size :-**
  - Worst-case transmission time is bounded and known in advance.
  - Knowing this bound makes it possible to use certain kinds of designs
  - Simplifies Network management.
- **Transmission Technology :-**
  - consist of a single cable to which all the machines are attached .
  - Traditional LAN runs at speed of 10 to 100 Mbps
  - Newer LANs operate at 10 Gbps
  - Low delay
  - Makes very few errors

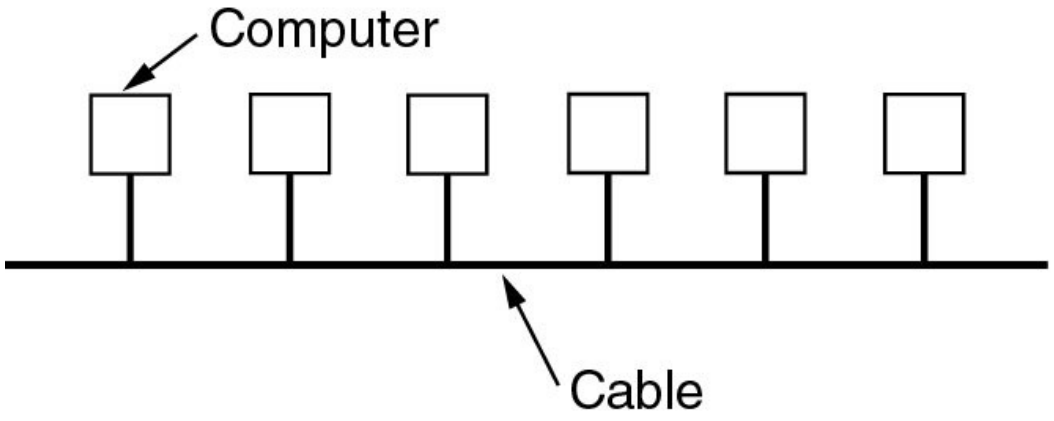
LAN



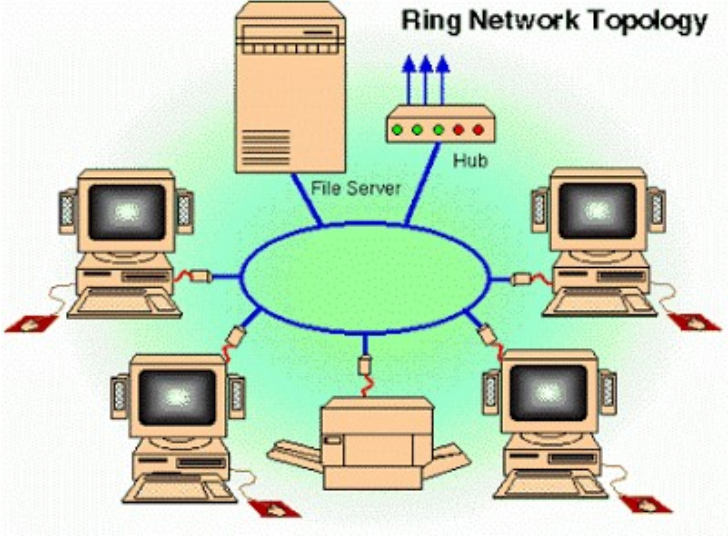
- **Topology** :-
- 2 broadcast network types:
  - Bus & Ring
- Bus (Linear cable) network
  - at any instant, at most one machine is the master and is allowed to transmit.
  - All other machines are required to refrain from sending
  - **Arbitration mechanism** :- to resolve conflicts when two or more machines want to transmit simultaneously.
  - It may be Centralized or distributed (decentralized)

LAN

- Eg:-IEEE 802.3 popularly called Ethernet is bus based broadcast network with decentralized control
  - operates at 10 Mbps to 10 Gbps
  - Computers on an Ethernet can transmit whenever they want to;
  - if two or more packets collide, each computer just waits a random time and tries again later

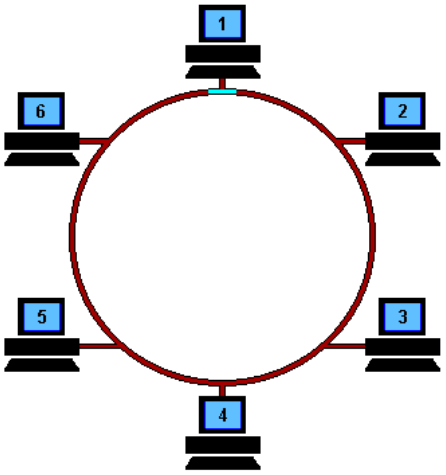


LAN



- Ring Network:
  - Devices acts as repeaters to boost the signal
  - The transmission of data takes place by token passing.
  - A token is a special series of bits that contains control information.
  - Possession of the token allows a network device to transmit data to the network.
  - Each network has only one token.

LAN



- Working of Ring Network:
  - The sending computer removes the token from the ring and sends the requested data around the ring.
  - Each computer passes the data until the packet finds the computer that matches the address on the data.
  - The receiving computer then returns a message to the sending computer indicating that the data has been received.
  - After verification, the sending computer creates a new token and releases it to the network.

LAN

- ✓ Ring Network:

Advantages:

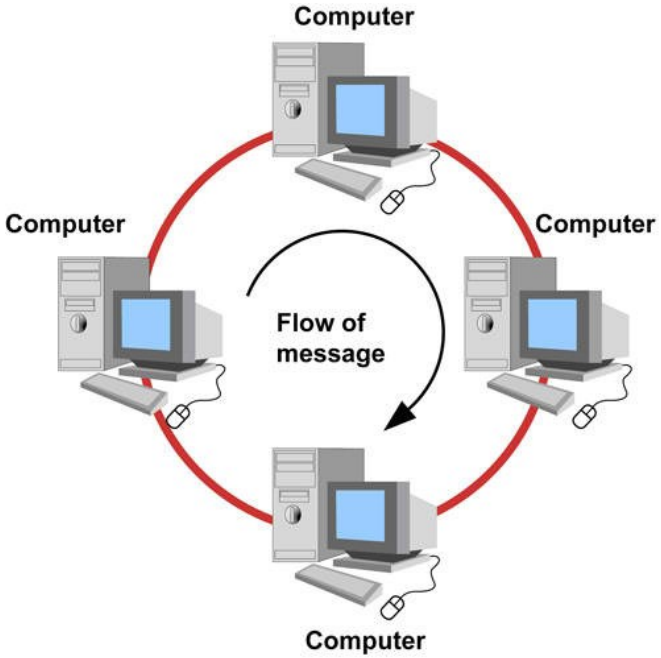
- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a bus topology under heavy network load
- Does not require network server to manage the connectivity between the computers

Disadvantages:

- One malfunctioning workstation or bad port can create problems for the entire network
- Devices moved, added and changed can affect the network
- Network adapter cards are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load

LAN

- Ring Network:
  - Egs:
    - IEEE 802.5 (the IBM token ring), is a ring-based LAN
      - operates at 4 and 16 Mbps.
    - FDDI (*Fiber Distributed Data Interface*) is another example of a ring network



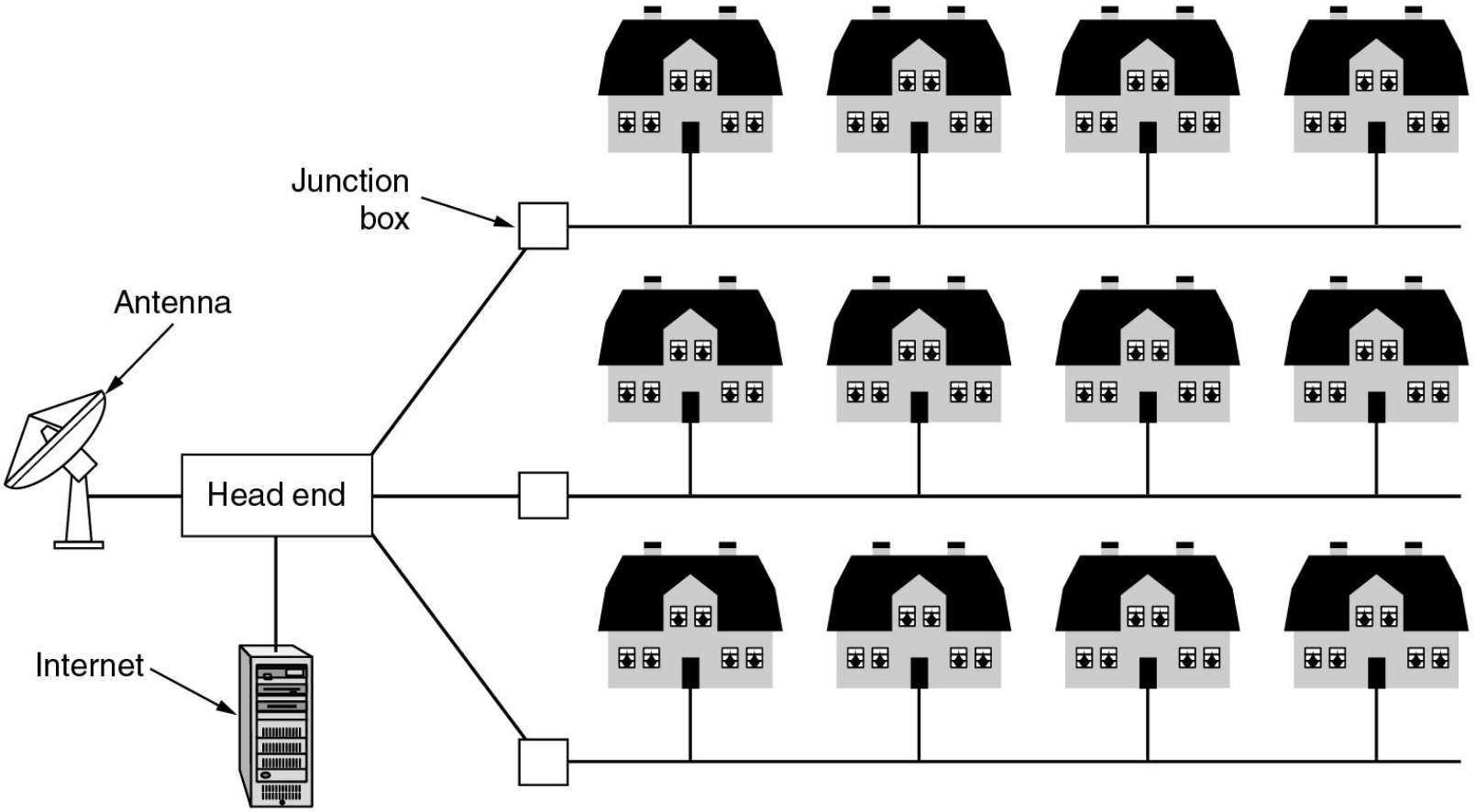
LAN

- Broadcast networks can be further divided into 2, depending on how the channel is allocated
  - Static and Dynamic
- A typical static allocation is
  - to divide time into discrete intervals and use a round-robin algorithm
  - allowing each machine to broadcast only when its time slot comes up
  - Drawback: wastes channel capacity when a machine has nothing to say during its allocated slot
  - So, most systems attempt to allocate the channel dynamically (i.e., on demand).

LAN

- Dynamic allocation methods are either centralized or decentralized.
- In the centralized channel allocation method,
  - there is a single entity,
  - for example, a bus arbitration unit,
  - which determines who goes next.
  - It might do this by accepting requests and making a decision according to some internal algorithm.
- In the decentralized channel allocation method,
  - there is no central entity;
  - each machine must decide for itself whether to transmit.

Metropolitan Area Networks (MAN)



A metropolitan area network based on cable TV in a city.

Another eg: IEEE 802.16 (Broadband wireless MANs) for high-speed wireless Internet access

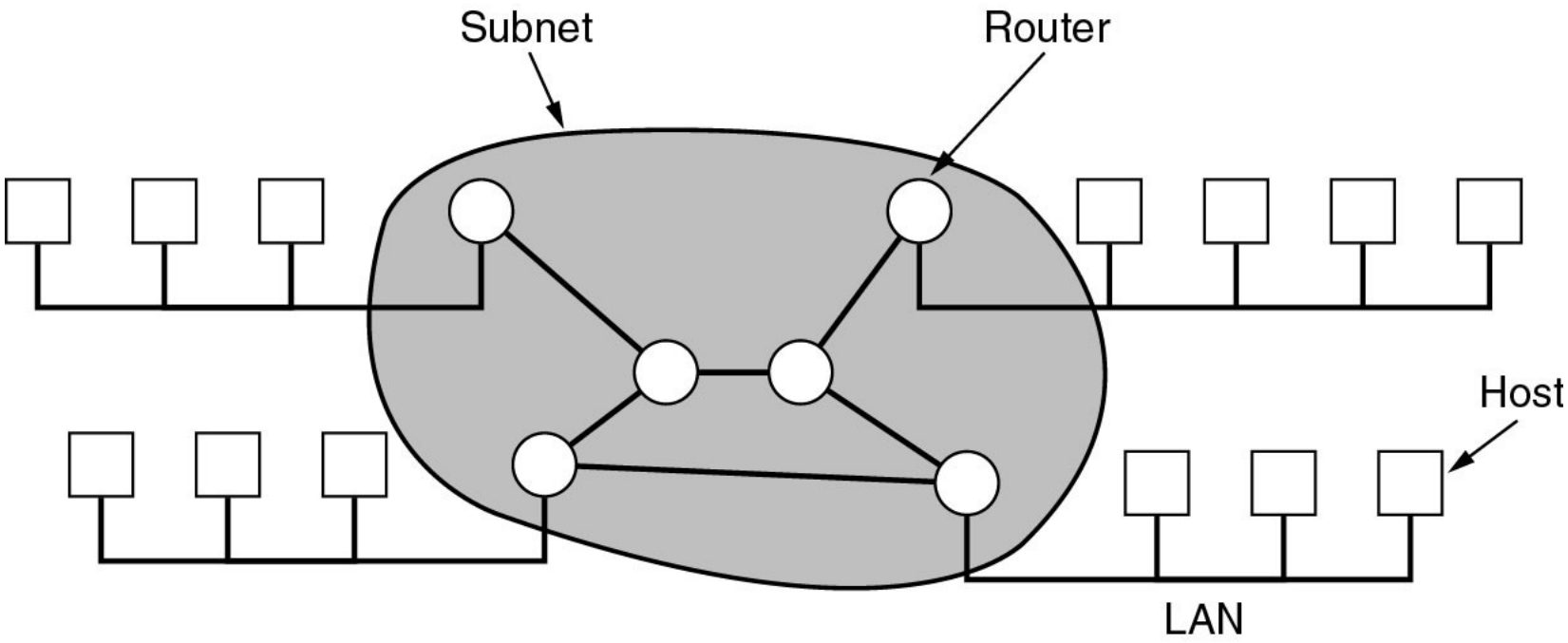
Wide Area Networks (WAN)

- WAN spans a large geographical area, often a country or continent
- It contains a collection of machines called hosts intended for running user (i.e., application) programs
- The hosts are owned by the customers
- The hosts are connected by a communication subnet, or just subnet
- The communication subnet is typically owned and operated by a telephone company or Internet service provider
- The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener

Wide Area Networks (WAN)

- Subnet consists of two distinct components:
  - transmission lines
  - switching elements
- Transmission lines
  - move bits between machines.
  - made of copper wire, optical fiber, or even radio links.
- Switching elements
  - Specialized computers that connect three or more transmission lines.
  - When data arrive on an incoming line, it must choose an outgoing line on which to forward them.
  - Switching elements are also called as routers

Wide Area Networks (WAN)



Relation between hosts on LANs and the subnet.

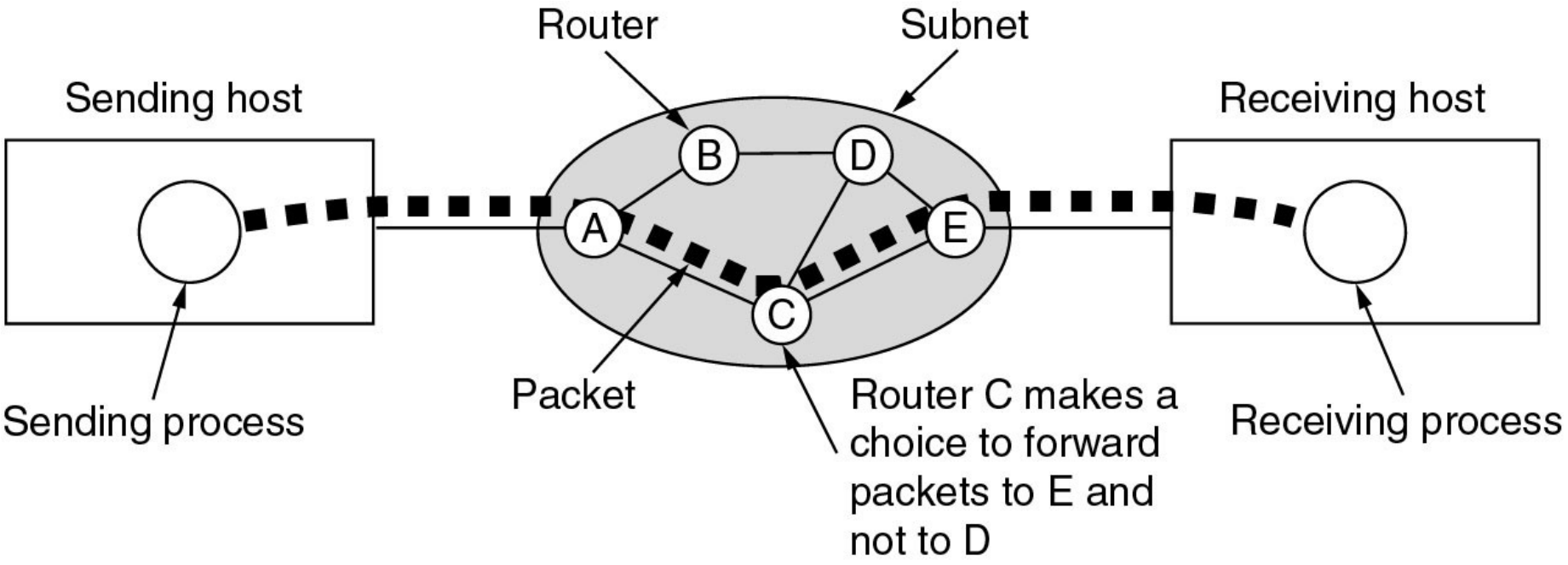
Wide Area Networks (WAN)

- Store-and-forward or packet-switched subnet
  - When a packet is sent from one router to another via one or more intermediate routers,
  - the packet is received at each intermediate router in its entirety,
  - stored there until the required output line is free, and then forwarded.
  - When the packets are small and all of the same size, they are often called cells

Wide Area Networks (WAN)

- Principle of a packet-switched WAN:
  - When a process on some host has a message to be sent to a process on some other host,
  - the sending host first cuts the message into packets,
  - each one bearing its number in the sequence.
  - These packets are then injected into the network one at a time in quick succession.
  - The packets are transported individually over the network and deposited at the receiving host,
  - where they are reassembled into the original message and delivered to the receiving process

Wide Area Networks



A stream of packets from sender to receiver.

- Routing decisions are made locally.
- When a packet arrives at router A, it is up to A to decide if this packet should be sent on the line to B or the line to C.
- How A makes that decision is called the routing algorithm.

Wide Area Networks (WAN)

- Not all WANs are packet switched.
- A second possibility for a WAN is a satellite system.
- Each router has an antenna through which it can send and receive.
- All routers can hear the output from the satellite
- In some cases, they can also hear the upward transmissions of their fellow routers to the satellite as well.
- Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna.
- Satellite networks are inherently broadcast and are most useful when the broadcast property is important

Internetworks

- A collection of interconnected networks is called an internetwork or internet
- A common form of internet is a collection of LANs connected by a WAN
- If the intermediate system contains only routers, it is a subnet
- if it contains both routers and hosts, it is a WAN
- An internetwork is formed when distinct networks are interconnected

Wireless Networks

- Digital wireless communication is not a new idea.
- As early as 1901, the Italian physicist Marconi demonstrated a ship-to-shore wireless telegraph, using Morse Code (dots and dashes as binary).
- Modern digital wireless systems have better performance, but the basic idea is the same.
- Categories of wireless networks:
  - System interconnection
  - Wireless LANs
  - Wireless WANs

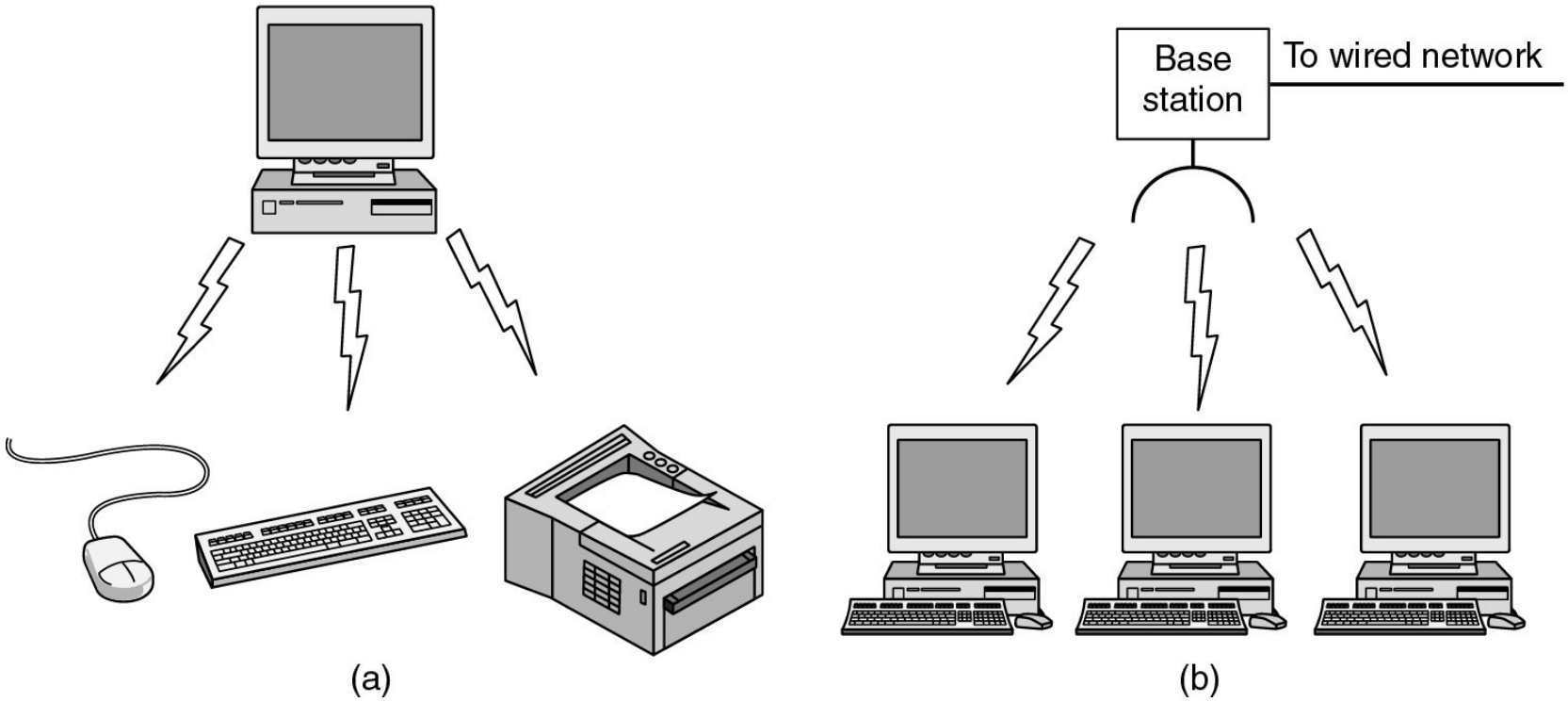
Wireless Networks

- System interconnection
  - interconnecting the components of a computer using short-range radio
  - every computer has a monitor, keyboard, mouse, and printer connected to the main unit by cables
  - some companies got together to design a short-range wireless network called Bluetooth to connect these components without wires
  - Bluetooth also allows digital cameras, headsets, scanners, and other devices to connect to a computer by merely being brought within range

Wireless Networks

- System interconnection
  - System interconnection networks use the master-slave paradigm
  - System unit is normally the master, talking to the mouse, keyboard, etc., as slaves.
  - The master tells the slaves
    - what addresses to use,
    - when they can broadcast,
    - how long they can transmit,
    - what frequencies they can use, and so on

Wireless Networks



(a) Bluetooth configuration

(b) Wireless LAN

Wireless Networks

- Wireless LANs
  - systems in which every computer has a radio modem and antenna with which it can communicate with other systems
  - if the systems are close enough, they can communicate directly with one another in a peer-to-peer configuration
  - Wireless LANs are becoming increasingly common in small offices and homes, where installing Ethernet is considered too much trouble
  - Standard for wireless LANs is called IEEE 802.11

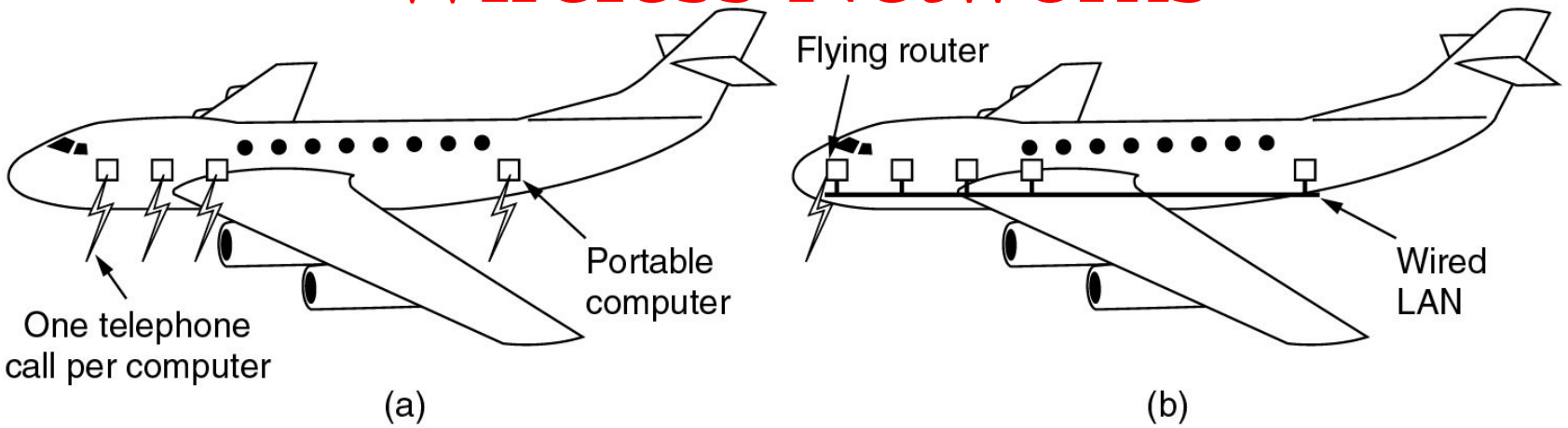
Wireless Networks

- Wireless WANs
  - radio network used for cellular telephones is an example of a low-bandwidth wireless system.
  - This system has already gone through three generations.
    1. The first generation was analog and for voice only.
    2. The second generation was digital and for voice only.
    3. The third generation is digital and is for both voice and data.

Wireless Networks

- Wireless WANs
  - In a certain sense, cellular wireless networks are like wireless LANs, except that the distances involved are much greater and the bit rates much lower.
    - Wireless LANs can operate at rates up to about 50 Mbps over distances of tens of meters.
    - Cellular systems operate below 1 Mbps, but the distance between the base station and the computer or telephone is measured in kilometers

Wireless Networks



(a) Individual independent mobile computers

- airplane with a number of people using modems and seat-back telephones to call the office independently.

(b) A flying LAN (more efficient)

- each seat comes equipped with an Ethernet connector into which passengers can plug their computers.
- A single router on the aircraft maintains a radio link with some router on the ground, changing routers as it flies along.
- This is just a traditional LAN, except that its connection to the outside world is a radio link instead of a hardwired line

Home Network Categories

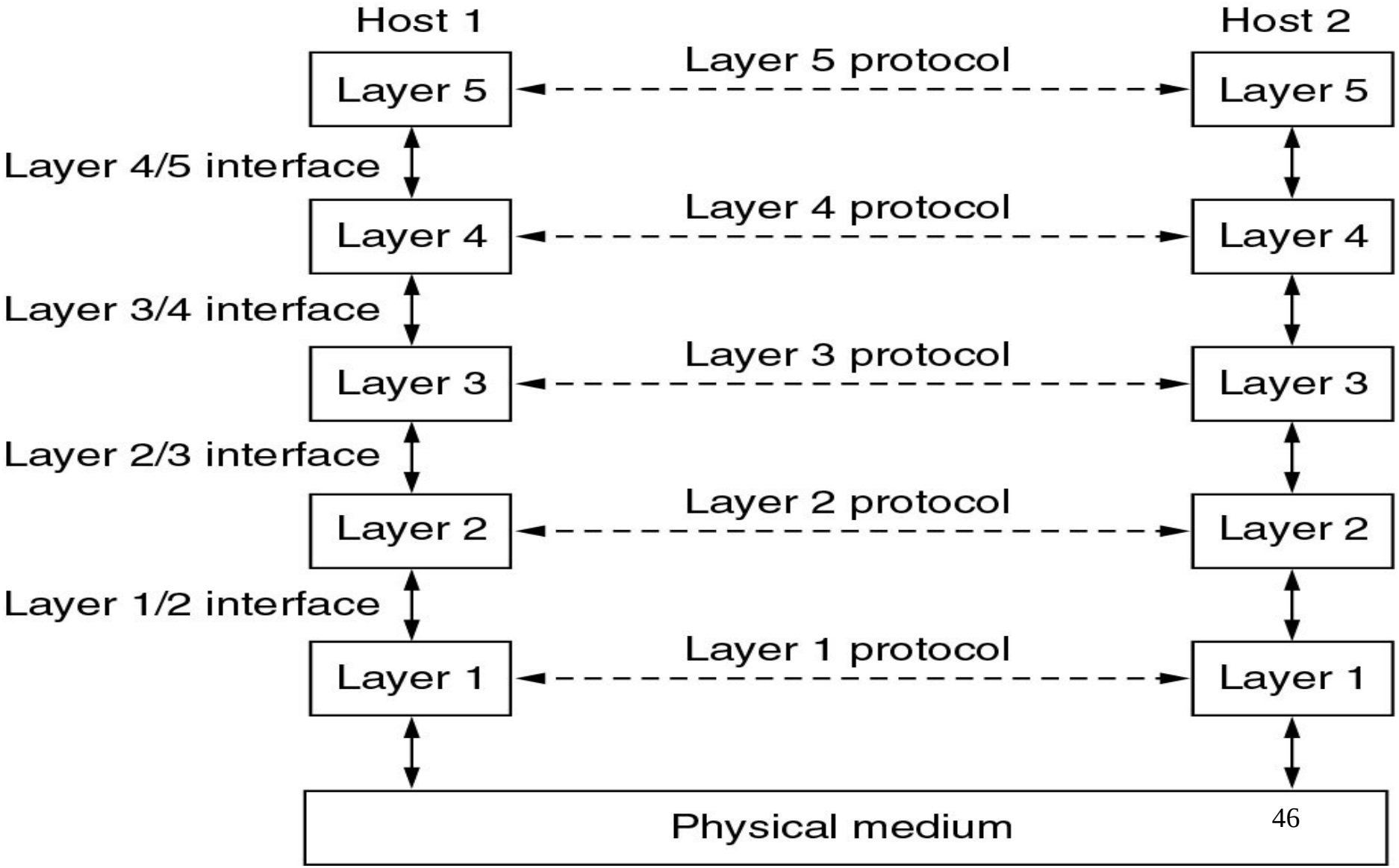
- Computers (desktop PC, PDA, shared peripherals)
- Entertainment (TV, DVD, VCR, camera, stereo, MP3)
- Telecomm (telephone, cell phone, intercom, fax)
- Appliances (microwave, fridge, lights)
- Telemetry (utility meter, burglar alarm, thermostat, babycam).

Network Software

- Protocol Hierarchies
- Design Issues for the Layers
- Connection-Oriented and Connectionless Services
- Service Primitives
- The Relationship of Services to Protocols

Network Software

Protocol Hierarchies



Protocol Hierarchies

- To reduce their design complexity, most networks are organized as a stack of layers or levels
- Number of layers, name of each layer, contents of each layer, and function of each layer differ from network to network
- Purpose of each layer
  - to offer certain services to the higher layers,
  - shielding those layers from the details of how the offered services are actually implemented
- The rules and conventions used in this conversation are collectively known as the layer n protocol
- Protocol is an agreement between the communicating parties on how communication is to proceed

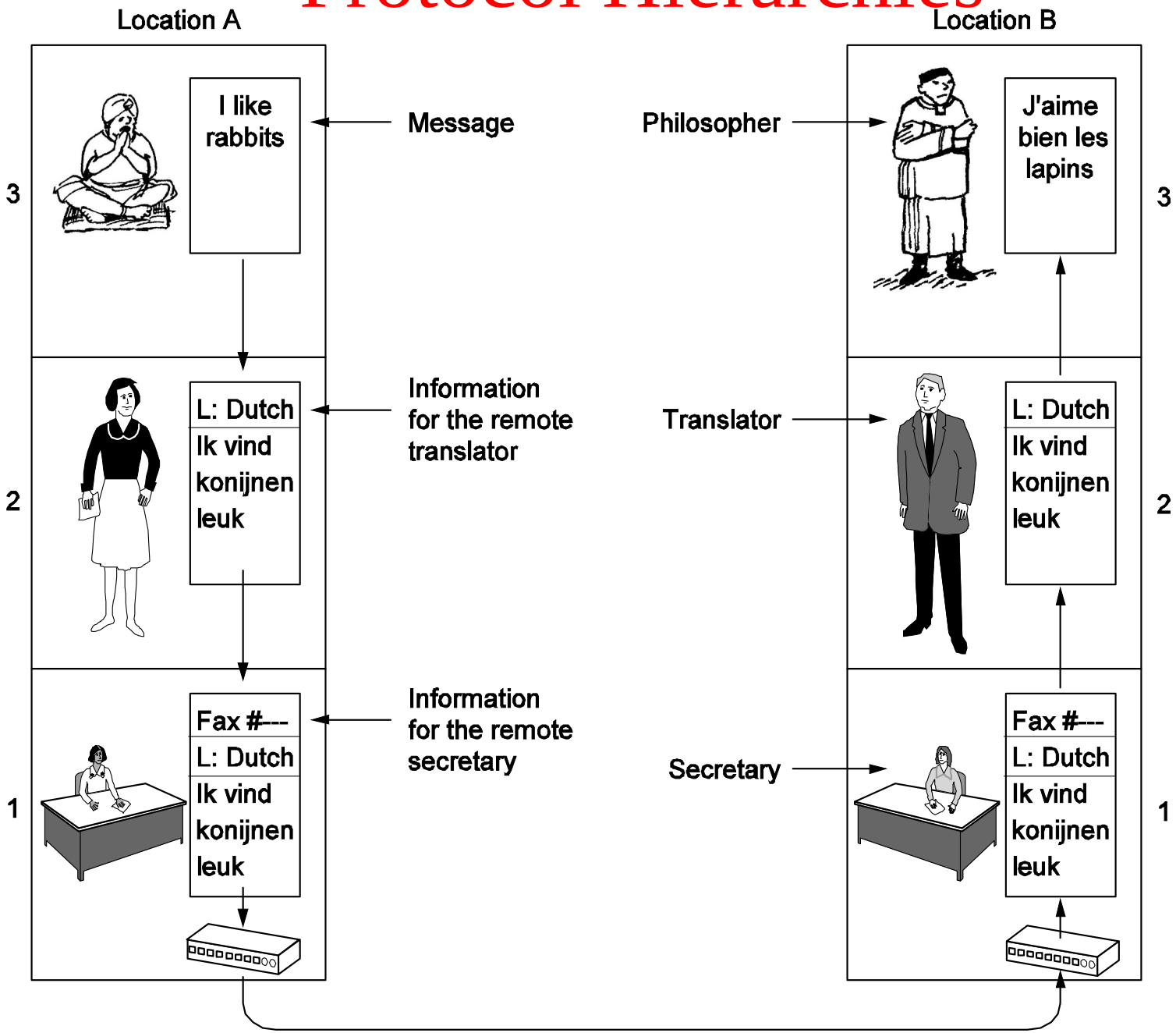
Protocol Hierarchies

- 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
- Interface defines which primitive operations and services the lower layer makes available to the upper one

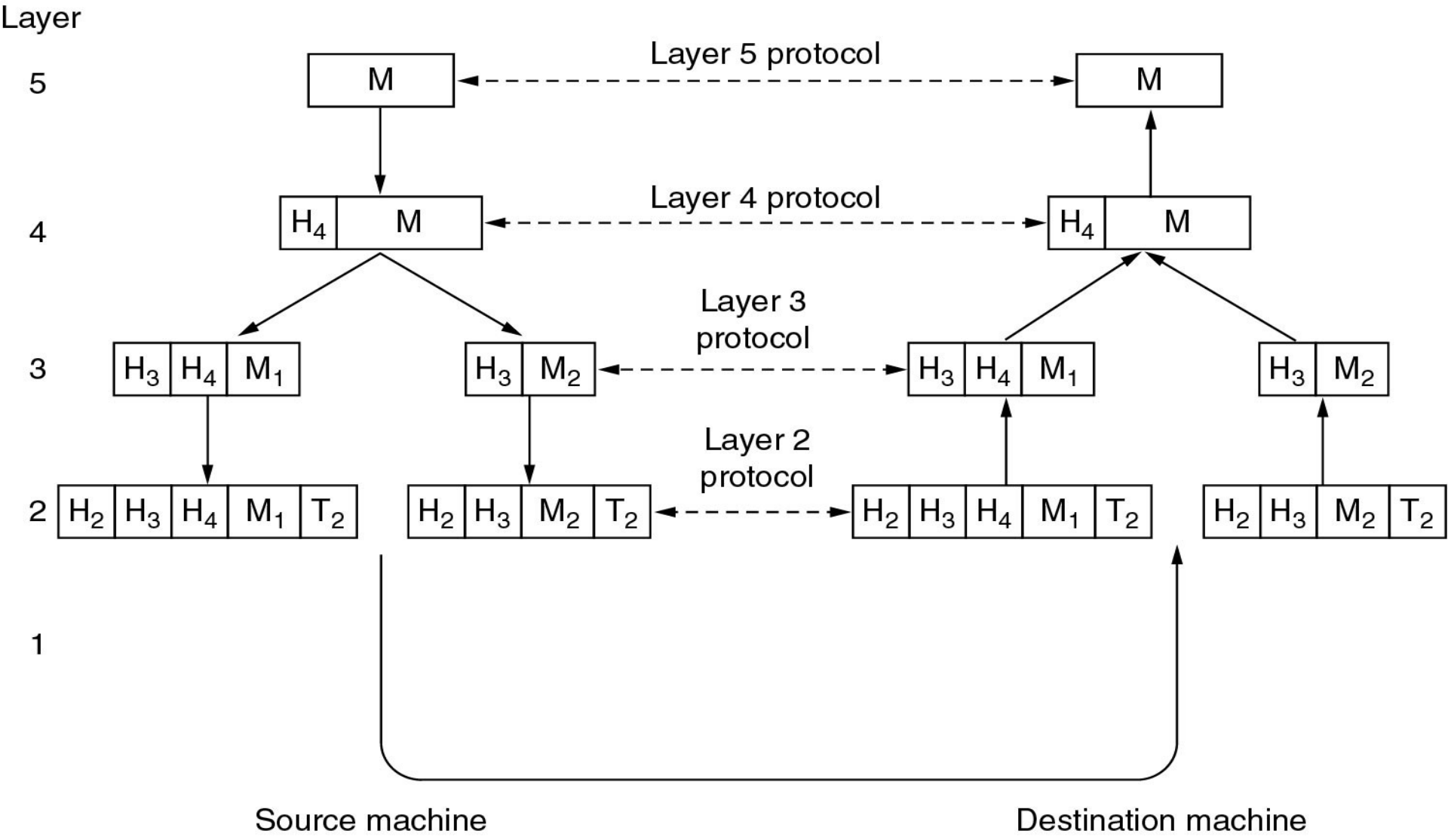
Protocol Hierarchies

- clear-cut interfaces makes it simpler to replace the implementation of one layer with a completely different implementation
- e.g., all the telephone lines are replaced by satellite channels
- A set of layers and protocols is called a network architecture
- A list of protocols used by a certain system, one protocol per layer, is called a protocol stack

Protocol Hierarchies



Protocol Hierarchies



header & trailer includes control information, such as sequence numbers, sizes, times, and other control fields

Design Issues for the Layers

- Addressing
- Rules for data transfer
- Error Control
- Flow Control
- Long messages
- Too short messages
- Multiplexing & demultiplexing
- Routing

Design Issues for the Layers

- Addressing
  - Every layer needs a mechanism for identifying senders and receivers
  - So, addressing is required

- Rules for data transfer
  - Unidirectional or bidirectional (Simplex / Half duplex / Full duplex)
  - 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.

Design Issues for the Layers

- Error Control
  - Problem: physical communication circuits are not perfect
  - error-detecting and error-correcting codes are available
  - both ends of the connection must agree on which one is being used
  - receiver must have some way of telling the sender which messages have been correctly received and which have not
  - To deal with a possible loss of sequencing, the protocol must make explicit provision for the receiver to allow the pieces to be reassembled properly

Design Issues for the Layers

- Flow Control
  - Problem: how to keep a fast sender from swamping (overloading) a slow receiver with data
  - Solution 1: some kind of feedback from the receiver to the sender, about the receiver's current situation
  - Solution 2: limit the sender to an agreed-on transmission rate (flow control)
- Long messages
  - Problem: inability of all processes to accept arbitrarily long messages
  - Solution: disassembling, transmitting, and then reassembling messages

Design Issues for the Layers

- Too short messages
  - Problem: transmitting data in units that are so small that sending each one separately is inefficient.
  - Solution: to gather several small messages heading toward a common destination into a single large message and dismember the large message at the other side.
- Multiplexing & demultiplexing
  - underlying layer may decide to use the same connection for multiple, unrelated conversations (Physical layer)
- Routing
  - When there are multiple paths between source and destination, a route must be chosen based on the current traffic load

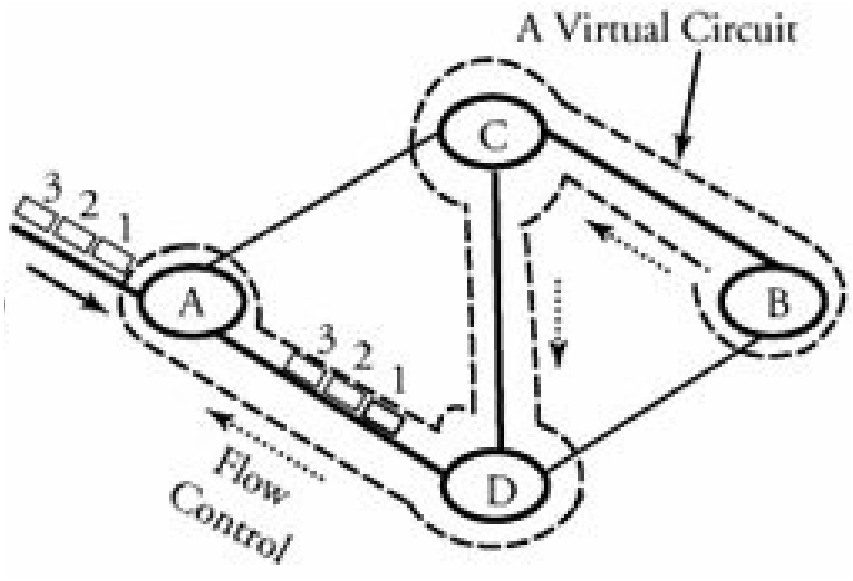
Connection-Oriented Services

- Similar to telephone service
- to use a connection-oriented network service, the service user
  - establishes a connection,
  - uses the connection, and
  - releases the connection

- acts like a tube
  - sender pushes objects (bits) in at one end, and the receiver takes them out at the other end
  - the order is preserved so that the bits arrive in the order they were sent

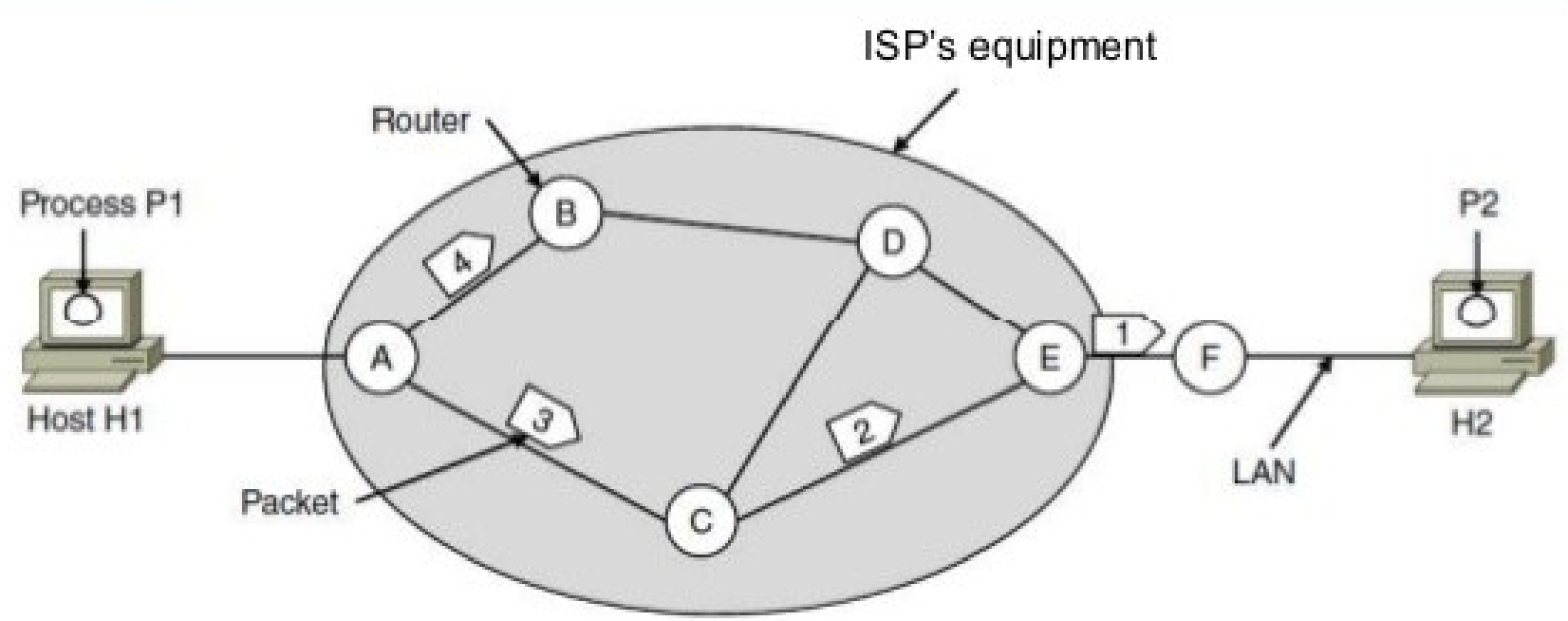
Connection-Oriented Services

- When a connection is established, the sender, receiver, and subnet conduct a negotiation
- about parameters to be used, such as
  - maximum message size,
  - quality of service
    - error rates,
    - bandwidth,
    - throughput,
    - transmission delay,
    - jitter,
    - Availability
  - other issues.
- Typically, one side makes a proposal and the other side can accept it, reject it, or make a counterproposal



Connectionless Services

- Similar to postal system
- Each message (letter) carries the full destination address
- Each one is routed through the system independent of all the others



Connection-Oriented Services

- Classifications: Reliable & Unreliable
- Each service can be characterized by a quality of service
- Some services are reliable that they never lose 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
- Eg for reliable connection-oriented service is file transfer
- Reliable connection-oriented service has two minor variations:
  - message sequences and
  - byte streams

Connection-Oriented Services

- Message sequences
  - 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
  - Eg: Sending the pages of book
- Byte streams
  - 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
  - Eg: user logging details to a remote server

Connection-Oriented Services

- For some applications, transit delays introduced by acknowledgements are unacceptable. (Unreliable is better)
- Application 1: digitized voice traffic.
  - It is preferable for telephone users to hear a bit of noise on the line from time to time than to experience a delay waiting for acknowledgements.
- Application 2: video conference
  - when transmitting a video conference, having a few pixels wrong is no problem, but having the image jerk along as the flow stops to correct errors is irritating

Connectionless Services

- Connectionless service is often called datagram service
- Unreliable (meaning not acknowledged) datagram service
  - does not return an acknowledgement to the sender
  - Eg: junk mails
- acknowledged datagram service
  - convenience of not having to establish a connection to send one short message is desired,
  - but reliability is essential.
  - Eg: sending a registered letter and requesting a return receipt
- request-reply service
  - the sender transmits a single datagram containing a request; the reply contains the answer
    - Egs: a query to the local library, Client server model

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

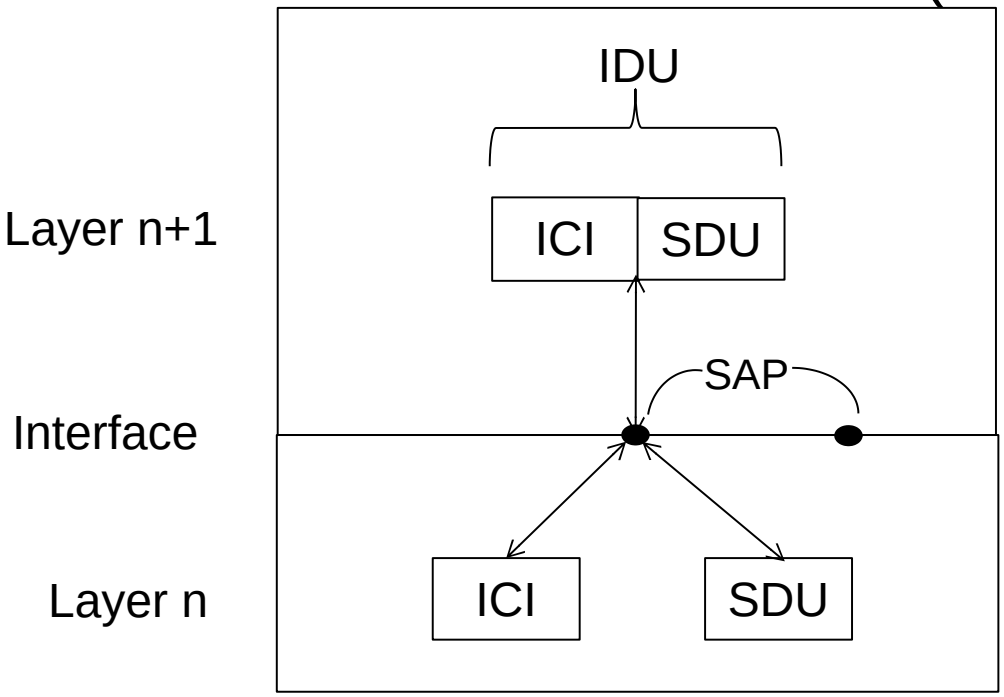
Six different types of service.

Interfaces & Services

- active elements in each layer are called entities
- An entity can be a
  - software entity (such as a process), or
  - hardware entity (such as an intelligent I/O chip)
- Entities in the same layer on different machines are called peer entities
- entities in layer n implement a service used by layer n+ 1
  - Layer n is the service provider
  - Layer n + 1 is the service user
- Classes of services
  - Fast & expensive communication
  - Slow & cheap communication

Interfaces & Services

- Services are available at SAPs (Service Access Points)



IDU – Interface Data Unit
ICI – Interface Control Information
SDU – Service Data Unit
SAP – Service Access Point

- Each SAP has an address that uniquely identifies it
  - Eg: SAPs are the sockets into which telephones are plugged
  - SAP addresses are telephone numbers of sockets

Service Primitives

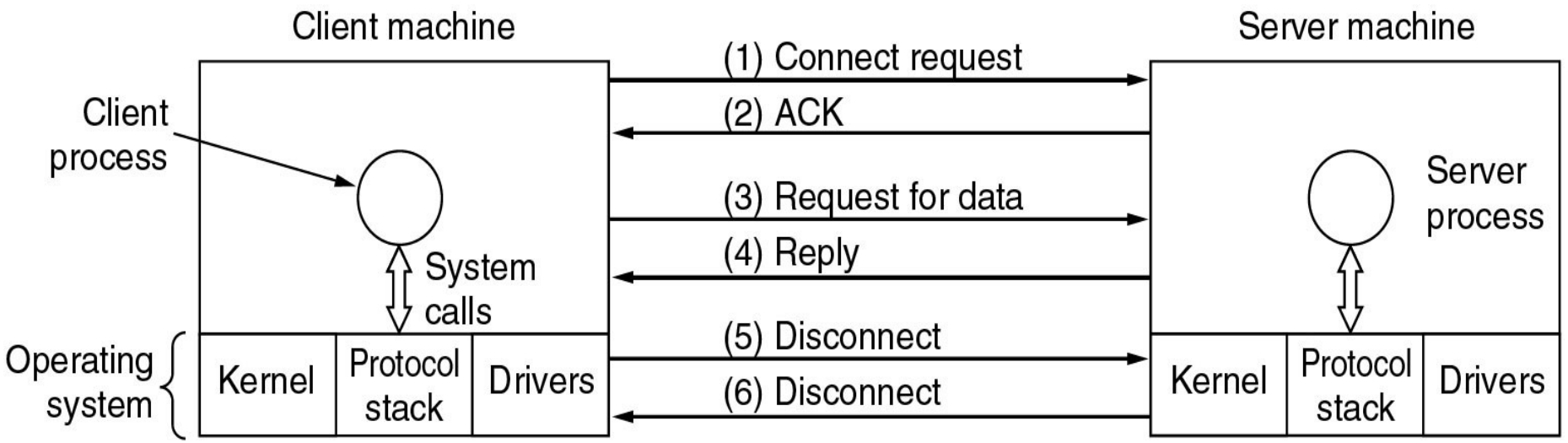
- A service is specified by a set of primitives (operations) available to a user process to access the service.
- These primitives tell the service to perform some action or report on an action taken by a peer entity.
- If the protocol stack is located in the operating system, the primitives are normally system calls.
- These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.

Service Primitives

Five service primitives for implementing a simple connection-oriented service.

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

Service Primitives



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

Service Primitives

- Eg Illustration:
- Server executes LISTEN to indicate that it is prepared to accept incoming connections.
- A common way to implement LISTEN is to make it a blocking system call.
- After executing the primitive, the server process is blocked until a request for connection appears
- Client process executes CONNECT to establish a connection with the server
- Operating system then typically sends a packet to the peer asking it to connect
- Client process is suspended until there is a response

Service Primitives

- When the packet arrives at the server, it is processed by its operating system
- When the system sees that the packet is requesting a connection, it checks to see if there is a listener.
- If so, it does two things:
  - unblocks the listener and
  - sends back an acknowledgement
- arrival of this acknowledgement then releases the Client
- At this point the Client and Server are both running and they have a connection established
- If a connection request arrives and there is no listener, the result is undefined

Service Primitives

- The next step is for the Server to execute RECEIVE to prepare to accept the first request.
  - Normally, the server does this immediately upon being released from the LISTEN, before the acknowledgement can get back to the client.
- The RECEIVE call blocks the Server
- Then the Client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply
- The arrival of the request packet at the server machine unblocks the Server process so it can process the request.
- After it has done the work, it uses SEND to return the answer to the Client.
- The arrival of this packet unblocks the Client, which can now inspect the answer.

Service Primitives

- If the Client has additional requests, it can make them now.
- If it is done, it can use DISCONNECT to terminate the connection.
- Usually, an initial DISCONNECT is a blocking call, suspending the client and sending a packet to the server saying that the connection is no longer needed.
- When the Server gets the packet, it also issues a DISCONNECT of its own, acknowledging the client and releasing the connection.
- When the Server's packet gets back to the Client machine, the Client process is released and the connection is broken.

Reference Models

- The OSI Reference Model
- The TCP/IP Reference Model

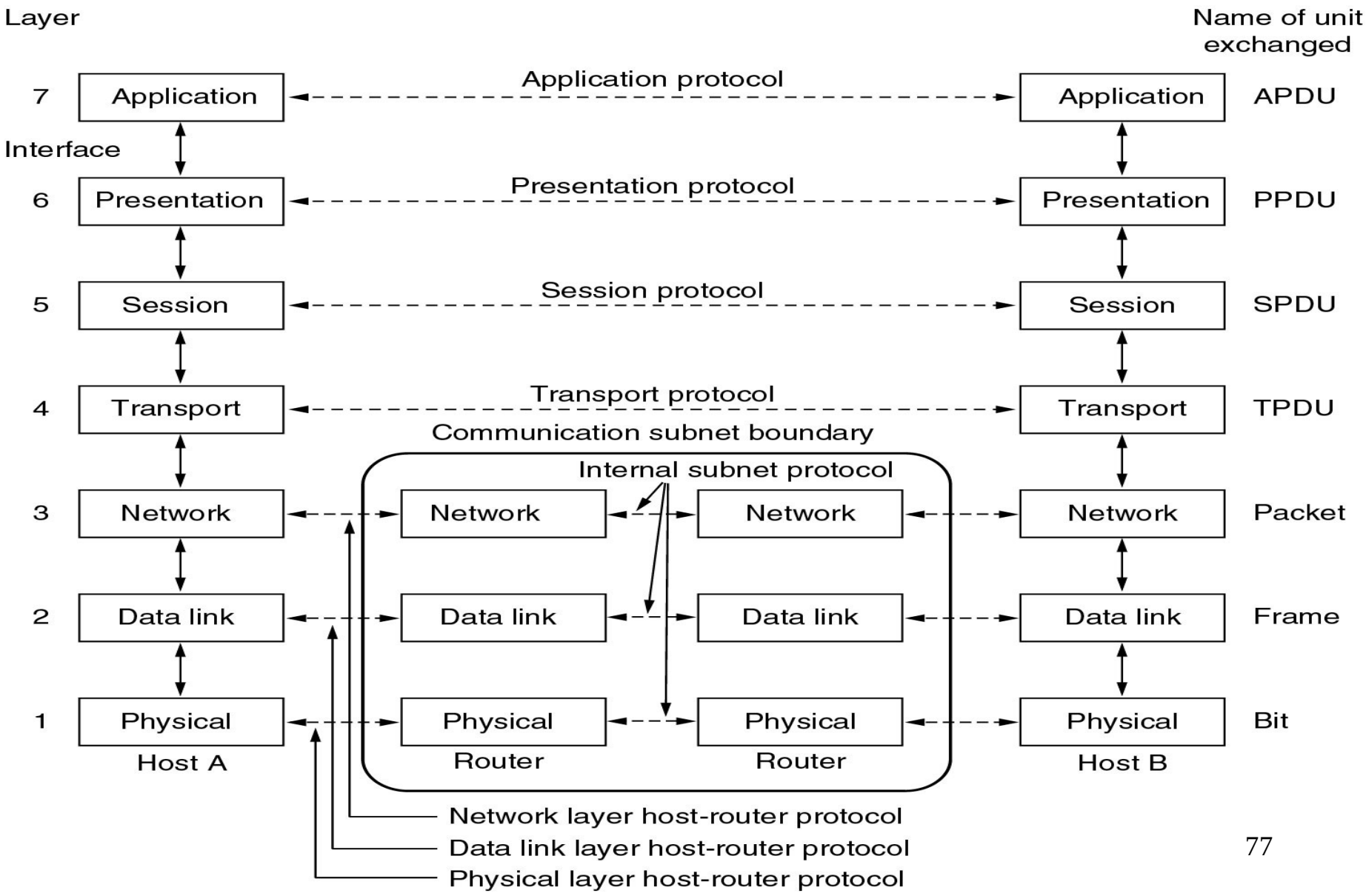
OSI Reference Model

- The model is called the ISO OSI (International Organization for Standardization Open Systems Interconnection) Reference Model.
- because it deals with connecting open systems
  - ie, systems that are open for communication with other systems
- OSI model has seven layers
  1. Physical layer
  2. Data link layer
  3. Network Layer
  4. Transport Layer
  5. Session Layer
  6. Presentation Layer
  7. Application Layer

OSI Reference Model

- Principles behind the seven layer design
  - A layer should be created where a different abstraction (concept) is needed.
  - Each layer should perform a well-defined function.
  - The function of each layer should be based on internationally Standardized Protocols
  - The layer boundaries should be chosen to minimize the information flow across the interfaces
  - number of layers should be
    - large enough that distinct functions need not be thrown together in the same layer out of necessity
    - small enough that the architecture does not become unmanageable

OSI Reference Models



OSI Reference Model

- *Physical Layer*
  - concerned with transmitting raw bits over a communication channel
  - Design issues are
    1. when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.
    2. how many volts should be used to represent a 1 and how many for a 0,
    3. how many nanoseconds a bit lasts,
    4. whether transmission may proceed simultaneously in both directions,
    5. how the initial connection is established and
    6. how it is torn down when both sides are finished,
    7. how many pins the network connector has
    8. what each pin is used for

OSI Reference Model

- *Physical Layer*
  - Design issues deal with
    - Mechanical, electrical, & timing interfaces, and
    - physical transmission medium, which lies below the physical layer
- *Data link Layer*
  - Main task: Error Control
    - to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer
    - 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 confirms correct receipt of each frame by sending back an acknowledgement frame

OSI Reference Model

- *Data link Layer*
  - Another Issue: Flow control
    - how to keep a fast transmitter from drowning a slow receiver in data
    - traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has
  - Additional issue in broadcast networks:
    - how to control access to the shared channel
  - Data link layer is subdivided into 2 for this purpose
    - Logical Link Control (LLC) sub layer
    - Medium Access Control (MAC) sub layer
      - MAC handles the broadcast networks

OSI Reference Model

- *Network Layer*
  - controls the operation of the subnet
  - design issues
    - determining how packets are routed from source to destination
    - Routes
      - can be based on static tables that are fixed into the network and are rarely changed
      - can be highly dynamic, being determined anew for each packet, to reflect the current network load
      - can also be determined at the start of each conversation (e.g., a login to a remote machine)

OSI Reference Model

- *Network Layer*
  - Congestion control
    - If too many packets are present in the subnet at the same time, they will get in one another's way creating congestion
  - Providing QOS
    - transit time, delay, jitter, error rate, bandwidth, availability, throughput, etc
  - to allow heterogeneous networks (different addressing, protocols, message size, etc) to be interconnected
  - In broadcast networks, the routing problem is simple
    - so the network layer is often thin or even nonexistent

OSI Reference Model

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

OSI Reference Model

- *Transport Layer*
  - most popular type of transport connection
    - error-free point-to-point channel that delivers messages or bytes in the order in which they were sent
  - other possible kinds of transport service
    - transporting of isolated messages, with no guarantee about the order of delivery, and
    - the broadcasting of messages to multiple destinations
  - Type of service is determined when the connection is established

OSI Reference Model

- *Transport Layer*
  - transport layer is a true end-to-end layer, all the way from the source to the destination
  - ie, 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.
  - In the lower layers, the protocols are between each machine and its immediate neighbors (routers), and not between the ultimate source and destination machines

OSI Reference Model

- *Session Layer*
  - allows users on different machines to establish sessions between them
  - Sessions offer various services, including
    - 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

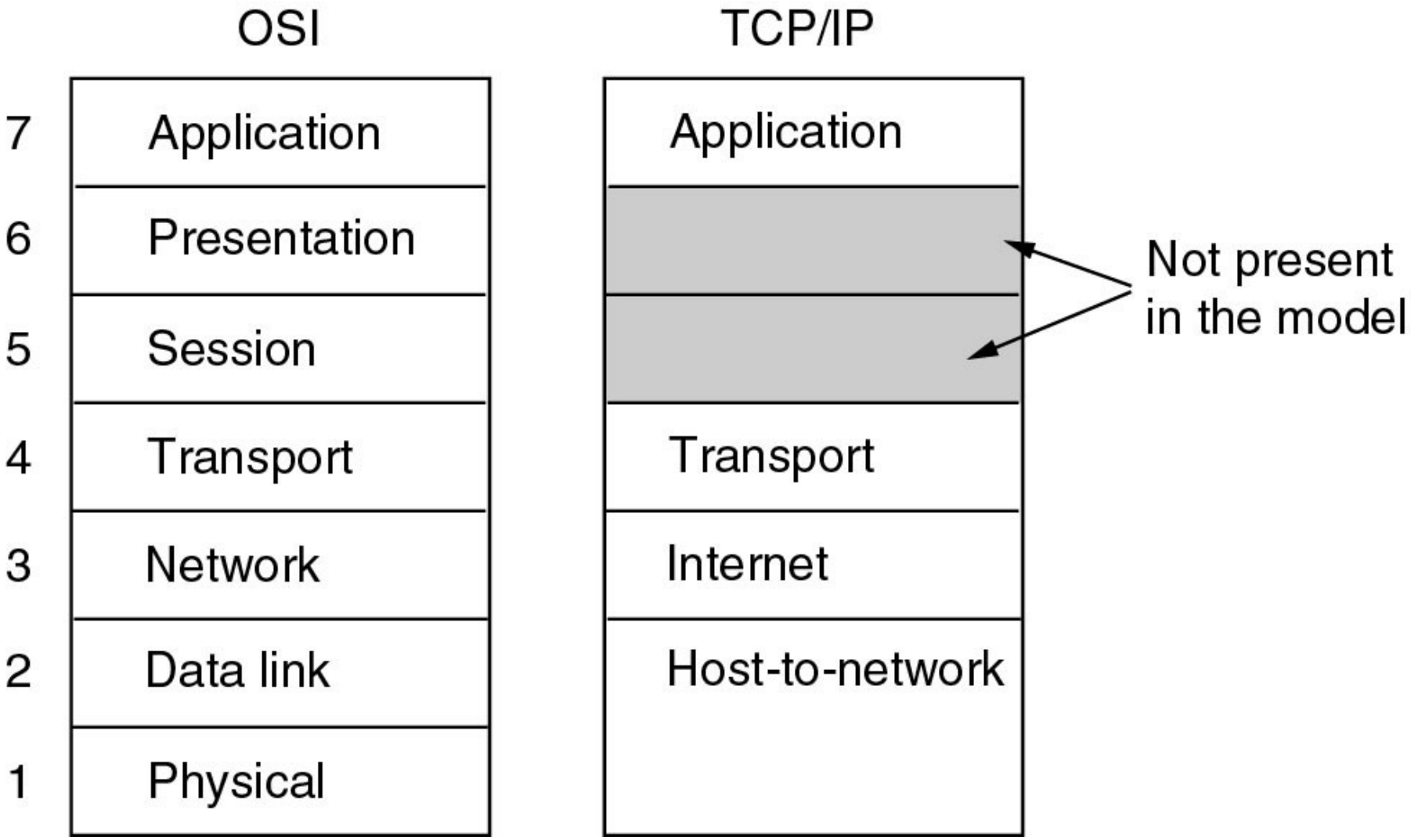
OSI Reference Model

- *Presentation Layer*
  - 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
  - manages these abstract data structures and allows higher-level data structures (e.g., banking records) to be defined and exchanged

OSI Reference Model

- *Application Layer*
  - Contains a variety of protocols that are commonly needed by users
  - Widely-used application protocol
    - HTTP (Hyper Text Transfer Protocol)
      - basis for the World Wide Web
      - When a browser wants a Web page, it sends the name of the page it wants to server using HTTP
      - server then sends the page back
  - Other application protocols
    - File transfer (FTP)
    - Electronic mail (SMTP)
    - Domain Name System (DNS)
    - Network News Transfer Protocol (NNTP)

TCP/IP Reference Models



TCP/IP Reference Model

- Reference model used in the ARPANET (grandparent of all WAN) and its successor, the worldwide Internet
- ***ARPANET (***Advanced Research Projects Agency Network***)***
  - Research network sponsored by the DoD (U.S. Department of Defense)
  - 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
  - Thus, the ability to connect multiple networks in a seamless way was one of the major design goals from the very beginning
  - This architecture later became known as the TCP/IP Reference Model, after its two primary protocols

TCP/IP Reference Model

- Another major goal
  - network must be able to survive loss of subnet hardware, with existing conversations not being broken off.
  - ie, 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.
  - Also, a flexible architecture was needed
    - since applications with divergent requirements were envisioned, ranging from transferring files to real-time speech transmission

TCP/IP Reference Model

- ***Host-to-Network Layer***
  - host has to connect to the network using some protocol so that it can send IP packets to it
  - protocol is not defined and varies from host to host and network to network
  - TCP/IP reference model does not really say much about what happens here
- ***Internet Layer***
  - All requirements of DoD led to the choice of a packet-switching network based on a connectionless internetwork layer
  - This layer is called the internet layer, because it is the key player that holds the whole architecture together

TCP/IP Reference Model

- ***Internet Layer***
  - Job is to permit hosts to inject packets into any network and
  - have them travel independently to the destination on a different network
  - They may even arrive in a different order than they were sent
  - it is the job of higher layers to rearrange them, if in-order delivery is desired
  - Note that "internet" is used here in a generic sense, even though this layer is present in the Internet

TCP/IP Reference Model

- ***Internet Layer***
  - Internet layer defines an official packet format and protocol called IP (Internet Protocol).
  - The job of the internet layer is to deliver IP packets where they are supposed to go.
  - Packet routing & avoiding congestion are the major issue here
  - For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer

TCP/IP Reference Model

- ***Transport Layer***
  - designed to allow peer entities on the source and destination hosts to carry on a conversation
  - Two end-to-end transport protocols
    - TCP (Transmission Control Protocol)
    - UDP (User Datagram Protocol)
  - ***TCP***
    - Reliable connection-oriented protocol
    - 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.

TCP/IP Reference Model

- ***Transport Layer***
  - ***TCP***
    - 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

TCP/IP Reference Model

- ***Transport Layer***
  - ***UDP***
    - Unreliable connectionless protocol
    - for applications that do not want TCP's sequencing or flow control and wish to provide their own
    - 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

TCP/IP Reference Model

- ***Application Layer***
  - TCP/IP model does not have session or presentation layers
  - Because they are of little use to most applications
  - contains all the higher-level protocols like
    - virtual terminal (TELNET)
    - file transfer (FTP)
    - electronic mail (SMTP)
    - Domain Name System (DNS)
    - Network News Transfer Protocol (NNTP)
    - Hyper Text Transfer Protocol (HTTP)

TCP/IP Reference Model

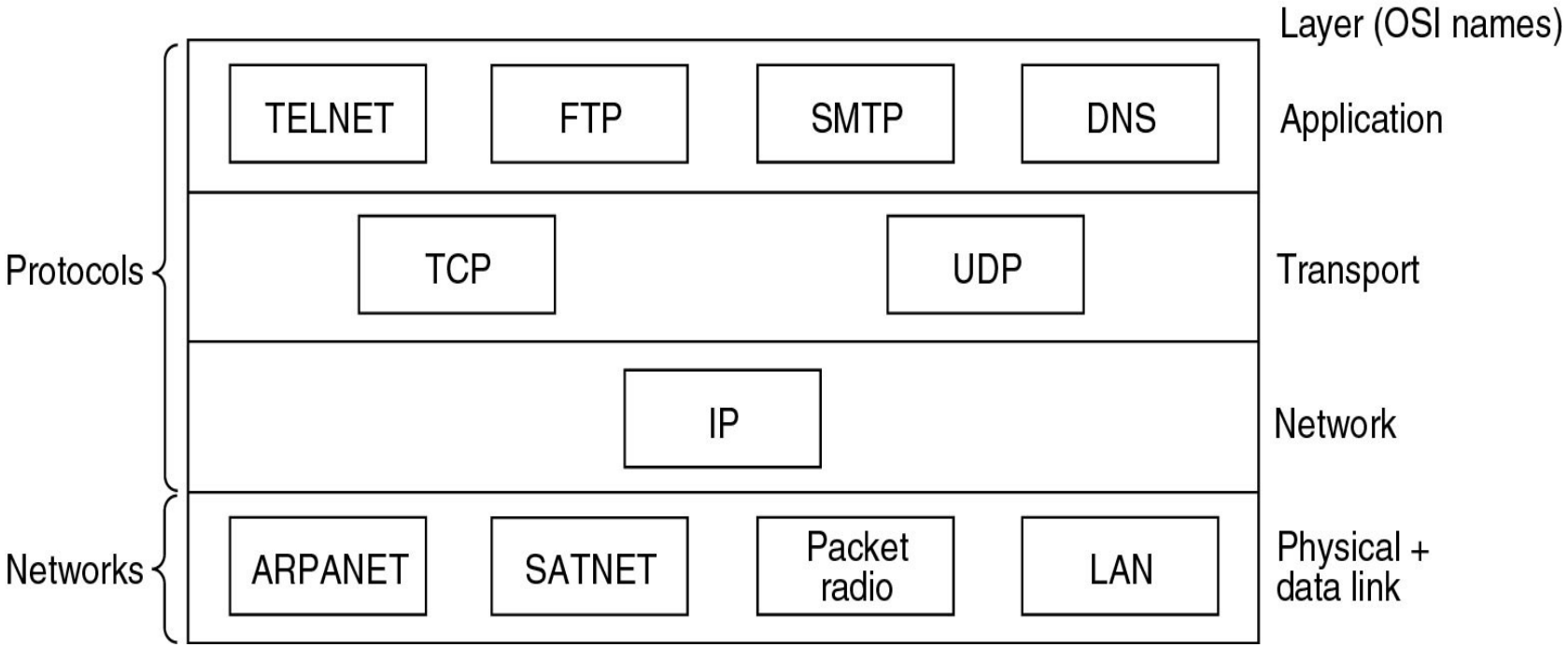
- ***Application Layer***
  - TELNET
    - virtual terminal protocol allows a user on one machine to log onto a distant machine and work there
  - FTP (File Transfer Protocol)
    - provides a way to move data efficiently from one machine to another
  - SMTP (Simple Mail Transfer Protocol)
    - Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it

TCP/IP Reference Model

- ***Application Layer***
  - DNS (Domain Name System)
    - for mapping host names onto their network addresses
  - NNTP (Network News Transfer Protocol)
    - protocol for moving USENET news articles around
    - USENET (worldwide distributed Internet discussion system)
  - HTTP (Hyper Text Transfer Protocol)
    - protocol for fetching pages on the World Wide Web (WWW)

Reference Models

Protocols and networks in the TCP/IP model initially.



ARPANET - Advanced Research Projects Agency Network
SATNET – Sustainable Agriculture Trainers Network

Assignment I

Comparison & critiques of OSI and TCP/IP Models