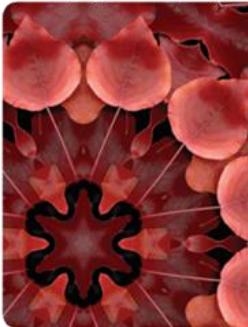




Computer Networks (CS2008)

Faculty Incharge
Dr. Vinod Kumar Jain



Course Info.

Course: “Computer Networks”

Course Code: CS2008

Time-Table (Tentative):

Batch-A	Tuesday 10:00-11:00	Wednesday 12:00-13:00	Wednesday 15:00-16:00	Friday 11:00-12:00
Batch-B	Tuesday 11:00-12:00	Tuesday 14:00-15:00	Wednesday 10:00-11:00	Friday 10:00-11:00

Location: Batch-A:L104, Bact-B:L105

Instructor: Dr. Vinod Kumar Jain

Email: vkjain@iiitdmj.ac.in

Course Page: <https://sites.google.com/view/dr-vinod-kumar-jain/home?authuser=0>



Course Structure

Topic	Discription
Introduction:	History and Development of Computer Networks, Data communication concepts and techniques, Networks Topologies, Network model components, layered network models (OSI reference model, TCP/IP networking architecture).
Physical Layer:	Theoretical Basis, Transmission Media, Wireless Transmission, Digital Transmission, Switching.
Data Link and MAC sublayer:	Error Control, Flow Control , Sliding Window Protocols, Aloha Protocols, CSMA Protocols, Collision Free Protocols, Local Area Networks -- Ethernet, Wireless LAN, Broadband Wireless.
Network Layer:	Routing Algorithms, Congestion Control Algorithms, Internetworking -- Bridges and Routers.
Transport Layer:	Connection Establishment, and release, TCP, UDP, Flow Control and Congestion Control, Quality of Services..
Application Layer:	Introduction to Application Layer protocols. Use of TCP/IP Protocol Suite as Running Example. Introduction to Network Security.

3

References

Text Book:
1. Computer Networks, Andrew S. Tanenbaum, David J. Wetherall , 5th Edition, Pearson/Prentice Hall Publictaion.
Reference Book:
1. Data and Computer Communication, William Stallings, 8th Edition, Pearson/Prentice Hall Publictaion.
2. Data Communications and Networking, Behrouz A Forouzan, 3/e, McGrawHill Publication.
3. Computer Networks: A Systems Approach, Bruce S. Davie and Larry L. Peterson, 4e, Morgan Kaufmann Publication.
4. The TCP/IP Guide, by Charles M. Kozierok, Free online Resource http://www.tcpipguide.com/free/ .

4

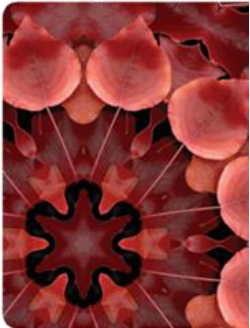
Assesments

Assesment	Weightage	Description
Class Participation	10%	
Quizzes	20%	Two Quizzes (Schedule will be announced in classes)
Midterm Exam	30%	Dates as per Academic Calendar
Major Exam	40%	Dates as per Academic Calendar



5

Introduction to Computer Networks



6

COMPUTER NETWORKS

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



7

COMPUTER NETWORKS

- ❑ A **Computer Network** is a collection of autonomous computers interconnected by a single technology.
- ❑ Two computers are said to be interconnected if they are able to exchange information.
- ❑ The connection need not be mandatorily via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.



8

DATA COMMUNICATIONS

The *Data Communication* consist two terms: *Data* and *Communication*.

- ❑ The term *telecommunication* means communication at a distance.
- ❑ The word *data* refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.



9

DATA COMMUNICATIONS

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

- ❑ *Delivery*: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- ❑ *Accuracy*: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- ❑ *Timeliness*: The system must deliver data in a timely manner. Data delivered late are useless.
 - In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
- ❑ *Jitter*: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.
 - For example, let us assume that video packets are sent every 30ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.



10

Components of a data communication system

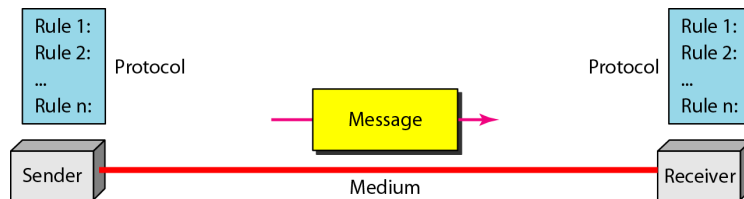


Figure 1 Components of a data communication system

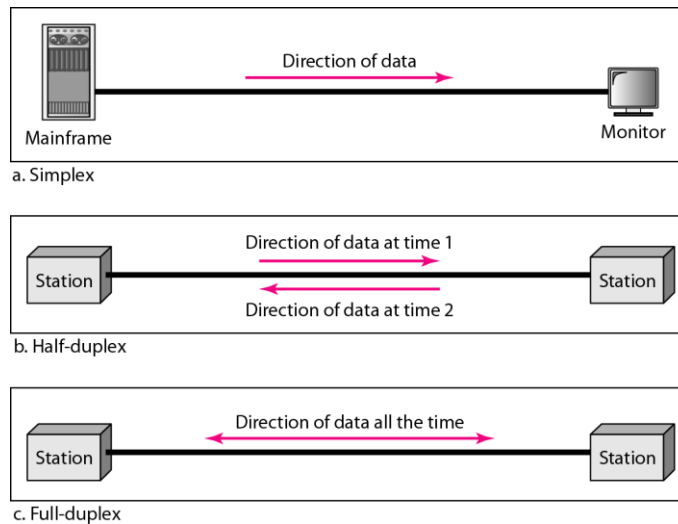
11

Components of a data communication system

- ❑ **Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- ❑ **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video-camera, and so on.
- ❑ **Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- ❑ **Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- ❑ **Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French can not be understood by a person who speaks only Japanese.

12

Figure 2 *Data flow (simplex, half-duplex, and full-duplex)*



13

Data flow (simplex, half-duplex, and full-duplex)

□ **Simplex:** In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 2a).

- Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.
- The simplex mode can use the entire capacity of the channel to send data in one direction.

14

Data flow (simplex, half-duplex, and full-duplex)

□ **Half Duplex** : In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice-versa (see Figure2b).

- The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- Walkie-talkies and CB(citizens band) radios are both half-duplex systems.
- The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.



15

Data flow (simplex, half-duplex, and full-duplex)

□ **Full-Duplex**: In full-duplex mode, (also called duplex), both stations can transmit and receive simultaneously (see Figure2c).

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



16

Network Criteria

□ Performance

- Depends on Network Elements
- Measured in terms of Delay and Throughput

□ Reliability

- Failure rate of network components
- Measured in terms of availability/robustness

□ Security

- Data protection against corruption/loss of data due to:
 - Errors
 - Malicious users



17

Physical Structures

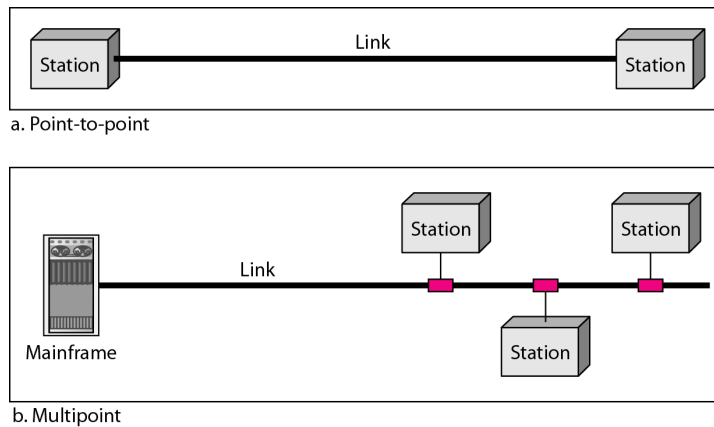
□ Type of Connection

- Point to Point - single transmitter and receiver
 - A point-to-point connection provides a dedicated link between two devices.
 - The entire capacity of the link is reserved for transmission between those two devices.
 - Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 3a).
- Multipoint - multiple recipients of single transmission
 - A multipoint (also called multi drop) connection is one in which more than two specific devices share a single link (see Figure 3b).
 - In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
 - If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



18

Figure 3 *Types of connections: point-to-point and multipoint*



19

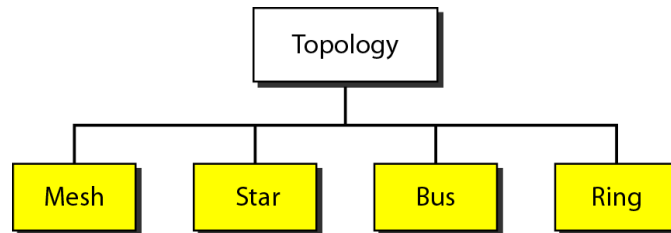
Physical Structures

□ Network Topology (Connection of devices)

- The term physical topology refers to the way in which a network is laid out physically.
- A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.
- Two or more devices connect to a link; two or more links form a topology.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are four basic topologies possible: mesh, star, bus, and ring.

20

Figure 4 *Categories of topology*



21

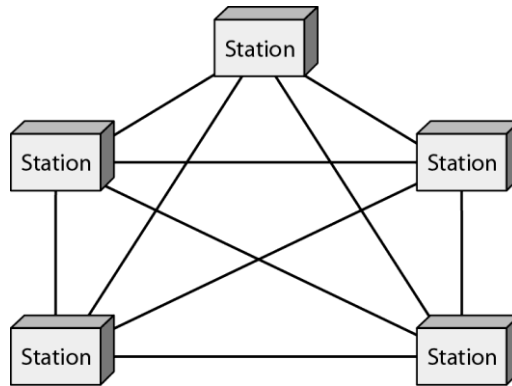
Mesh Topology

□ Mesh Topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
- In mesh topology we need $n(n-1)$ physical links to form the network. However, if each physical link allows communication in both directions (duplex mode), then, we need $n(n-1)/2$ duplex-mode links.
- To accommodate that many links, every device on the network must have $n - 1$ input/output (I/O) ports to be connected to the other $n - 1$ stations.

22

Figure 5 *A fully connected mesh topology (five devices)*



23

Mesh Topology

□ Advantages of Mesh Topology

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

24

Mesh Topology

❑ Disadvantages of Mesh Topology

- The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports; required.
 - First, because every device must be connected to every other device, installation and reconnection are difficult.
 - Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
 - Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
 - For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.
 - One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

25

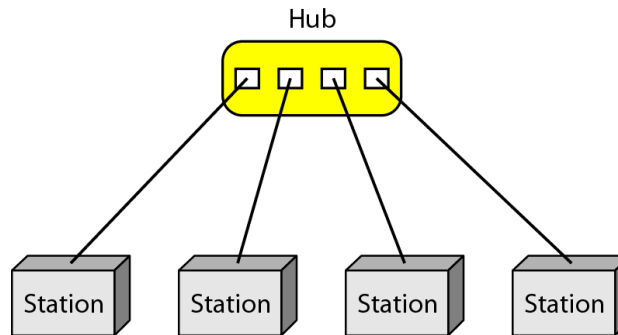
Star Topology

❑ Star Topology

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

26

Figure 6 *A star topology connecting four stations*



27

Star Topology

□ Advantages of Star Topology

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

28

Star Topology

❑ Disadvantages of Star Topology

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



29

Bus Topology

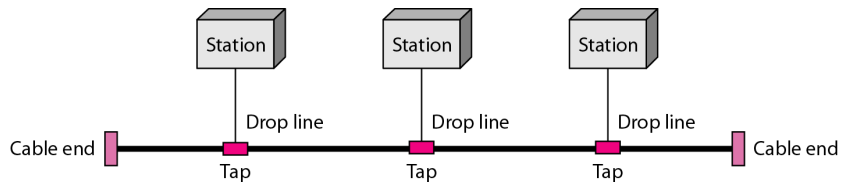
❑ Bus Topology

- The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network .
- Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
- In this way, a bus uses less cabling than mesh or star topologies.



30

Figure 7 *A bus topology connecting three stations*



31

Bus Topology

□ Bus Topology

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

32

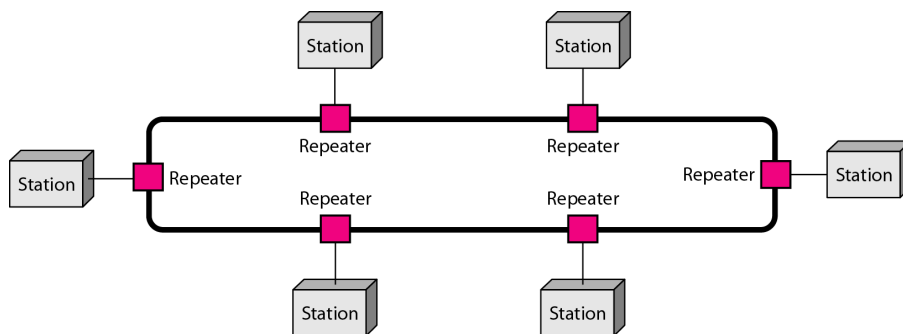
Ring Topology

□ Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.
- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbours (either physically or logically).
- To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).

33

Figure 8 *A ring topology connecting six stations*



34

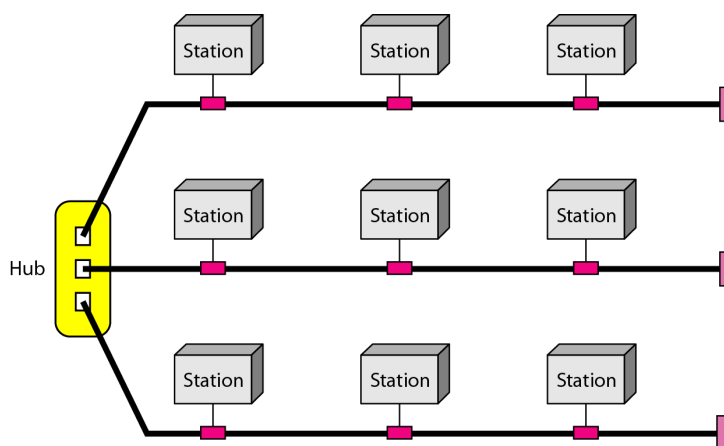
Ring Topology

□ Ring Topology

- In Ring, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.
- However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.
- This weakness can be solved by using a dual ring or a switch capable of closing off the break.
- Ring topology was prevalent when IBM introduced its local-area network Token Ring.
- Today, the need for higher-speed LANs has made this topology less popular.

35

Figure 9 *A hybrid topology: a star backbone with three bus networks*



36

Categories of Networks

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

37

Classification of interconnected processors by 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

Classification of interconnected processors by scale.

38

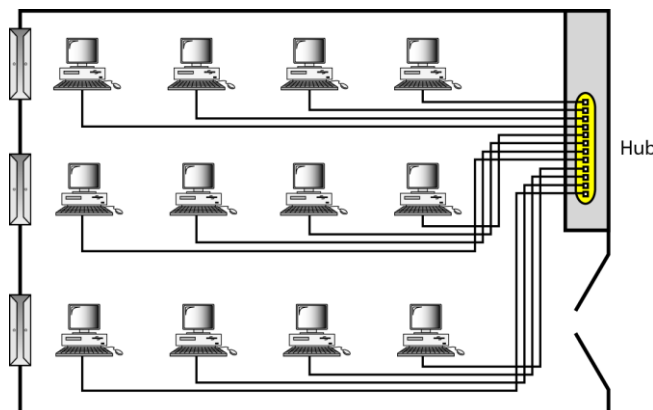
Local Area Networks (LANs)

□ Local Area Networks (LANs)

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals.
- Currently, LAN size is limited to a few kilometers.
- In addition to size, LANs are distinguished from other types of networks by their transmission media and topology.
- In general, a given LAN will use only one type of transmission medium.
- The most common LAN topologies are bus, ring, and star.
- Early LANs had data rates in the 4 to 16 mega bits per second(Mbps) range. Today, however, speeds are normally 100 or 1000Mbps.
- Wireless LANs are the newest evolution in LAN technology.

39

Figure 10 *An isolated LAN connecting 12 computers to a hub in a closet*



40

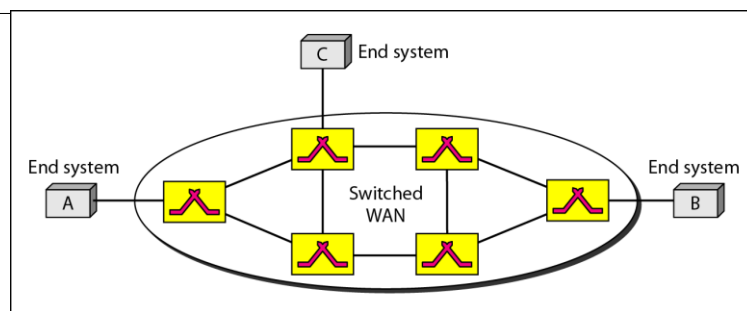
Wide Area Networks (WANs)

□ Wide Area Networks (WANs)

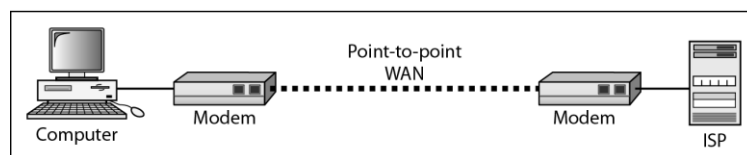
- A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.
- A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN.
- An early example of a switched WAN is X.25, a network designed to provide connectivity between end users.
- Another good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells.

41

Figure 11 WANs: a switched WAN and a point-to-point WAN



a. Switched WAN



b. Point-to-point WAN

42

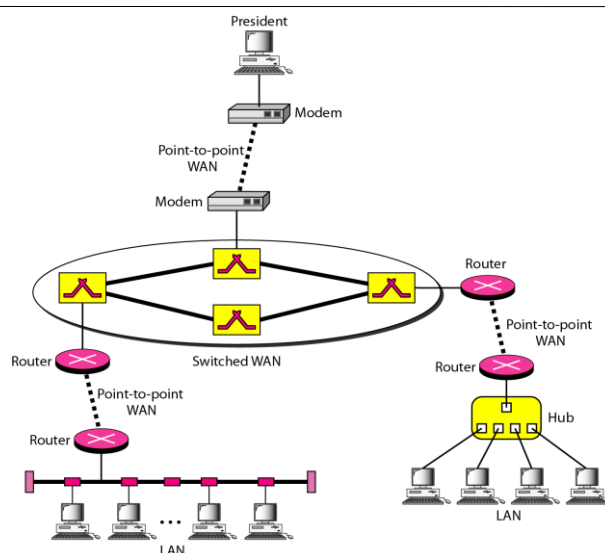
Metropolitan Area Networks (MANs)

□ Metropolitan Area Networks (MANs)

- A metropolitan area network (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.
- A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.
- Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

43

Figure 12 *A heterogeneous network made of four WANs and two LANs*



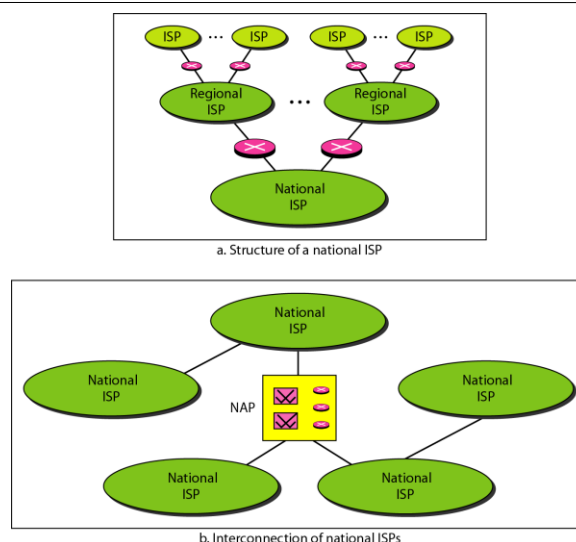
44

THE INTERNET

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

45

Figure 13 *Hierarchical organization of the Internet*



46

PROTOCOLS

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



47

Elements of a Protocol

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



48





Network Models



49



LAYERED TASKS

- ❑ A network is a combination of **hardware** and **software** that sends data from one location to another.
 - ❑ The hardware consists of the **physical equipment** that carries signals from one point of the network to another.
 - ❑ The software consists of **instruction sets** that make possible the services that we expect from a network.
 - ❑ The first computer networks were designed with the hardware as the main concern and the software as an afterthought.
 - ❑ This strategy no longer works. Network software is now highly structured.
- 
- 

50

LAYERED TASKS

- ❑ To reduce their design complexity, most networks are organized as a **stack of layers** or **levels**, each one built upon the one below it.
- ❑ The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- ❑ The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
- ❑ In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.



51

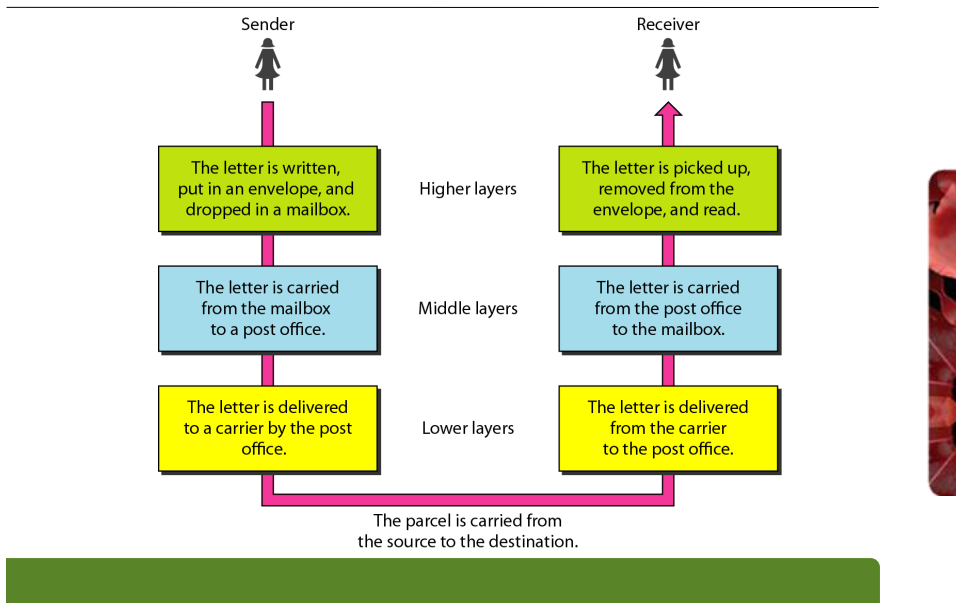
LAYERED TASKS

- ❑ We also use the concept of **layers** in our daily life.
- ❑ As an example, let us consider two friends who communicate through postal mail.
- ❑ The process of sending a letter to a friend would be complex if there were no services available from the post office.



52

Figure 14 Tasks involved in sending a letter



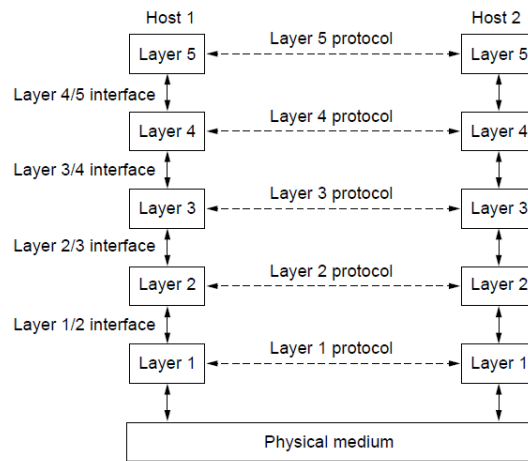
53

Layers, Protocols, and Interfaces

- ❑ When layer n on one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as the **layer n protocol**.
- ❑ Basically, a **protocol** is an agreement between the communicating parties on how communication is to proceed.
- ❑ Violating the protocol will make communication more difficult, if not completely impossible.
- ❑ The entities comprising the corresponding layers on different machines are called **peers**.
- ❑ The **peers** may be software processes, hardware devices, or even human beings.
- ❑ In other words, it is the peers that communicate by using the protocol to talk to each other.

54

Figure 15 Protocol Hierarchies



Layers, protocols, and interfaces.

55

Layers, Protocols, and Interfaces

- ❑ In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- ❑ Below layer 1 is the physical medium through which actual communication occurs. In Figure 15, virtual communication is shown by dotted lines and physical communication by solid lines.
- ❑ Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one.
- ❑ When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers.

56

Layers, Protocols, and Interfaces

- ❑ Doing so, in turn, requires that each layer perform a specific collection of well-understood functions.
- ❑ In addition to minimizing the amount of information that must be passed between layers, clear-cut interfaces also make it simpler to replace one layer with a completely different protocol or implementation (e.g., replacing all the telephone lines by satellite channels) because all that is required of the new protocol or implementation is that it offer exactly the same set of services to its upstairs neighbour as the old one did.
- ❑ It is common that different hosts use different implementations of the same protocol (often written by different companies).
- ❑ In fact, the protocol itself can change in some layer without the layers above and below it even noticing.



57

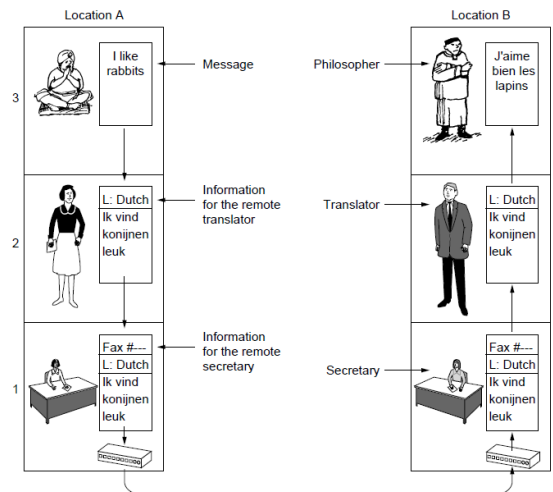
Layers, Protocols, and Interfaces

- ❑ A set of layers and protocols is called a [network architecture](#).
- ❑ The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.
- ❑ Neither the details of the implementation nor the specification of the interfaces is part of the architecture because these are hidden away inside the machines and not visible from the outside.
- ❑ A list of the protocols used by a certain system, one protocol per layer, is called a [protocol stack](#).
- ❑ Consider an analogy, which may help explain the idea of multilayer communication.



58

Figure 16 The philosopher-translator-secretary architecture



The philosopher-translator-secretary architecture

59

Layers, Protocols, and Interfaces

- ❑ Imagine two philosophers (peer processes in layer 3), one of whom speaks Urdu and English and one of whom speaks Chinese and French.
- ❑ Since they have no common language, they each engage a translator (peer processes at layer 2), each of whom in turn contacts a secretary (peer processes in layer 1).
- ❑ Philosopher 1 wishes to convey his affection to his peer. To do so, he passes a message (in English) across the 2/3 interface to his translator, saying "I like rabbits,".
- ❑ The translators have agreed on a neutral language known to both of them, Dutch, so the message is converted to "Ik vind konijnen leuk."
- ❑ The choice of the language is the layer 2 protocol and is up to the layer 2 peer processes.

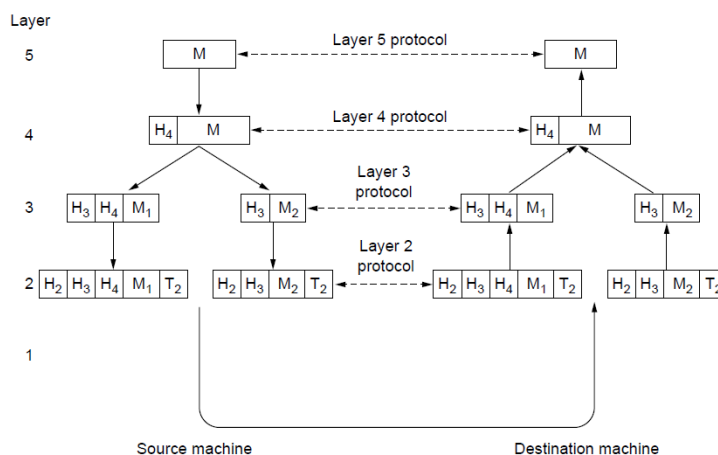
60

Layers, Protocols, and Interfaces

- ❑ The translator then gives the message to a secretary for transmission, for example, by email (the layer 1 protocol).
- ❑ When the message arrives at the other secretary, it is passed to the local translator, who translates it into French and passes it across the 2/3 interface to the second philosopher.
- ❑ Note that each protocol is completely independent of the other ones, as long as the interfaces are not changed.
- ❑ The translators can switch from Dutch to, say, Finnish, at will, provided that they both agree, and neither changes his interface with either layer 1 or layer 3.
- ❑ Similarly, the secretaries can switch from email to telephone without disturbing (or even informing) the other layers.
- ❑ Each process may add some information intended only for its peer. This information is not passed up to the layer above.

61

Figure 17 Information flow in 5 layer network architecture



Example information flow supporting virtual communication in layer 5.

62

Design Issues for the Layers

- ❑ Some of the key design issues that occur in computer networks will come up in layer after layer.
 - Reliability
 - How is it possible that we find and fix errors?
 - error detection
 - error correction
 - Routing
 - finding a working path through a network
 - Addressing or Naming
 - Every layer needs a mechanism for identifying the senders and receivers that are involved in a particular communication.



63

Design Issues for the Layers

- internetworking
 - different network technologies often have different limitations.
 - not all communication channels preserve the order of messages.
 - differences in the maximum size of a message that the networks can transmit.
 - disassembling, transmitting, and then reassembling messages.
- Scalability
- Resource allocation



64

Design Issues for the Layers

- Flow control
 - how to keep a fast sender from swamping a slow receiver with data.
- Congestion control
 - want to send too much traffic, and the network cannot deliver it all.
- Quality of service
 - Most networks must provide service to applications that want real-time delivery at the same time that they provide service to applications that want high throughput.
- Security
 - Confidentiality
 - Authentication
 - integrity

65

Types of Services

- Layers can offer two different types of service to the layers above them:
 - connection-oriented and,
 - connectionless.
- Connection-oriented service is modeled after the telephone system.
 - To talk to someone, you pick up the phone, dial the number, talk, and then hang up.
 - Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.

66

Types of Services

- The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end.
- In most cases the order is preserved so that the bits arrive in the order they were sent.
- In some cases when a connection is established, the sender, receiver, and subnet conduct a negotiation about the parameters to be used, such as maximum message size, quality of service required, and other issues.
- Typically, one side makes a proposal and the other side can accept it, reject it, or make a counterproposal.
- A circuit is another name for a connection with associated resources, such as a fixed bandwidth.



67

Types of Services

- In contrast to connection-oriented service, connectionless service is modeled after the postal system.
 - Each message (letter) carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.
 - There are different names for messages in different contexts; a packet is a message at the network layer.
 - When the intermediate nodes receive a message in full before sending it on to the next node, this is called store-and-forward switching.
 - The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called cut-through switching.



68

Types of Services

❑ Connection-Oriented Versus Connectionless Service

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

69

Service Primitives

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

70

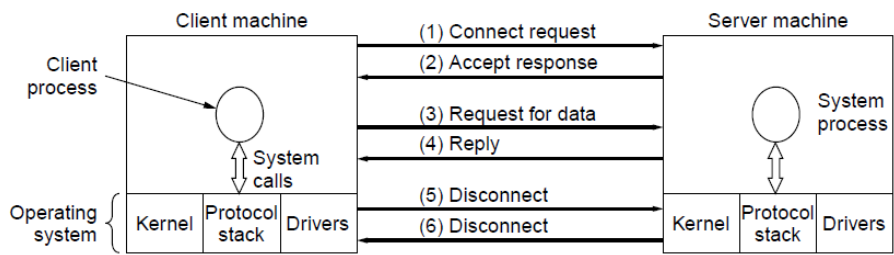
Service Primitives

Six service primitives that provide a simple connection-oriented service

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

71

Service Primitives



A simple client-server interaction using acknowledged datagrams.

72

The Relationship of Services to Protocols

- ❑ Services and protocols are distinct concepts. This distinction is so important that's why I emphasize it again here.
- ❑ A service is a set of primitives (operations) that a layer provides to the layer above it.
 - The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
 - A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.



73

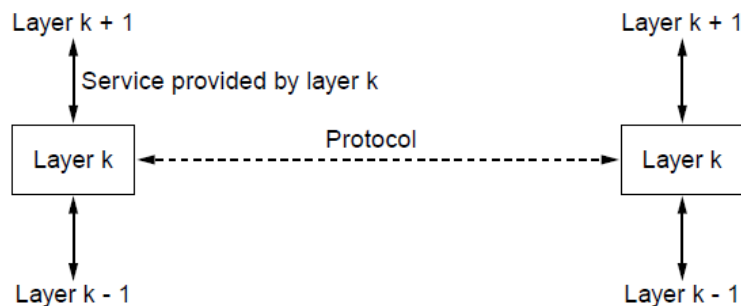
The Relationship of Services to Protocols

- ❑ A protocol, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer.
 - Entities use protocols to implement their service definitions.
 - They are free to change their protocols at will, provided they do not change the service visible to their users.
- ❑ To repeat this crucial point, services relate to the interfaces between layers, as illustrated in Fig. on next slide.
- ❑ In contrast, protocols relate to the packets sent between peer entities on different machines. It is very important not to confuse the two concepts.



74

The Relationship of Services to Protocols



The relationship between a service and a protocol.

75

The OSI Reference Model

- ❑ Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- ❑ An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s. It was revised in 1995.
- ❑ The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

76

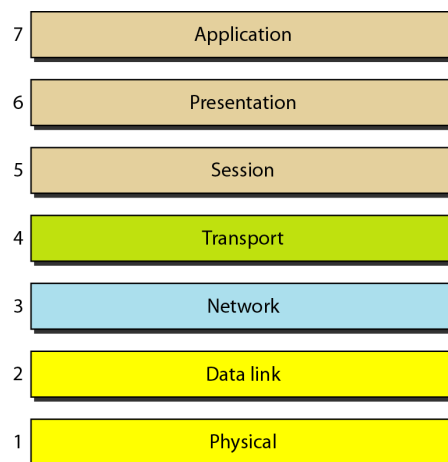


Note

ISO is the organization.
OSI is the model.

77

Figure 18 *Seven layers of the OSI model*



78

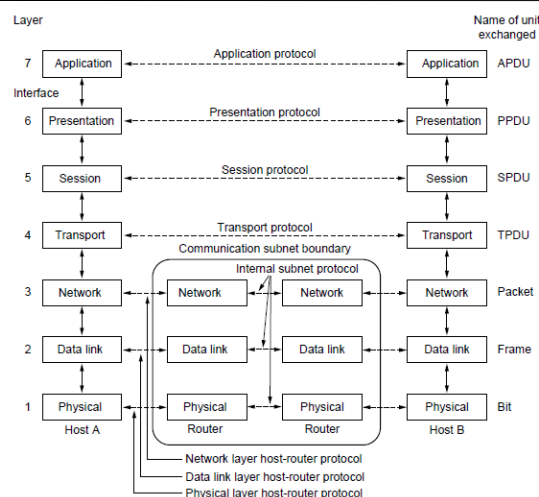
The OSI Reference Model

Principles for the seven layers

- ❑ A layer should be created where a different abstraction is needed.
- ❑ Each layer should perform a well-defined function.
- ❑ Function of layer chosen with definition of international standard protocols in mind.
- ❑ The layer boundaries should be chosen to minimize the information flow across the interfaces.
- ❑ Number of layers should be optimum
 - 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.

79

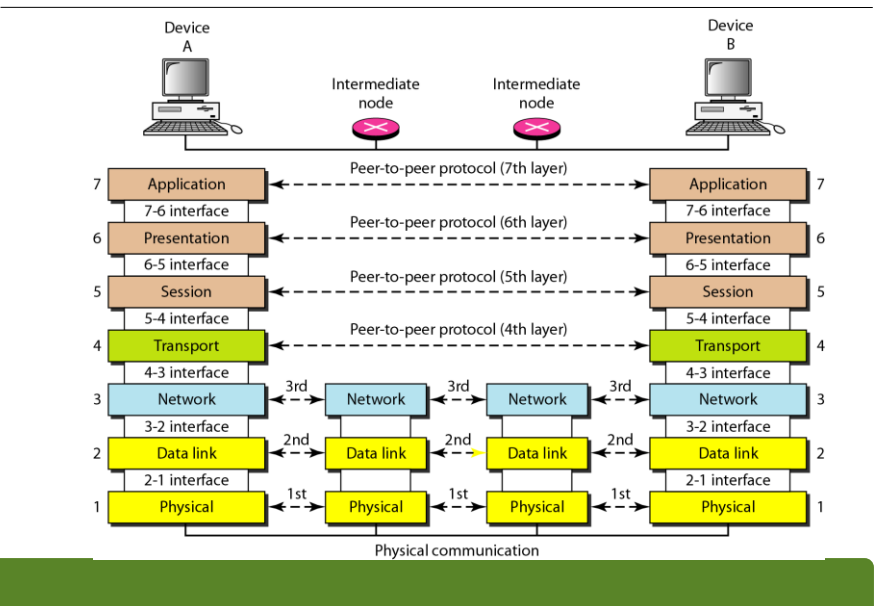
The OSI Reference Model



The OSI reference model

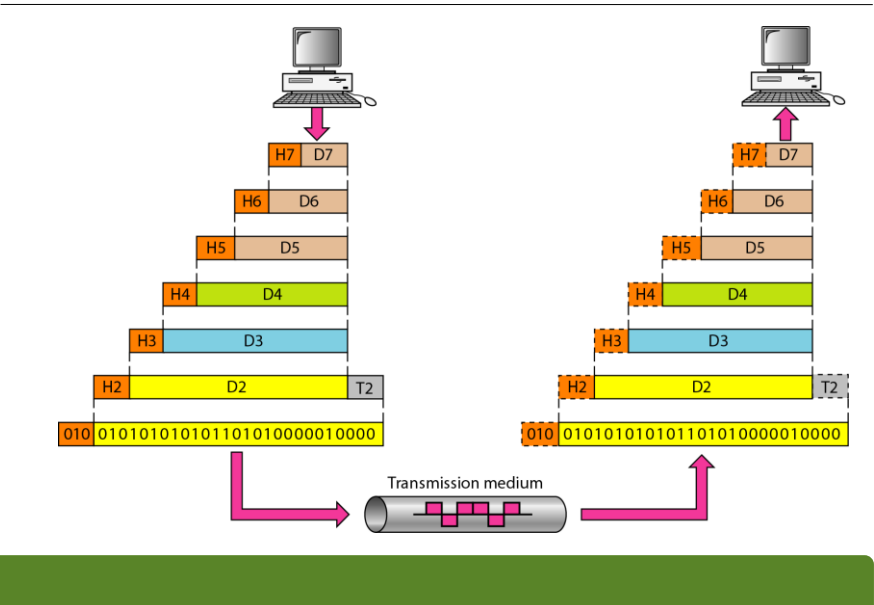
80

Figure 19 The interaction between layers in the OSI model



81

Figure 20 An exchange using the OSI model



82

LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



83

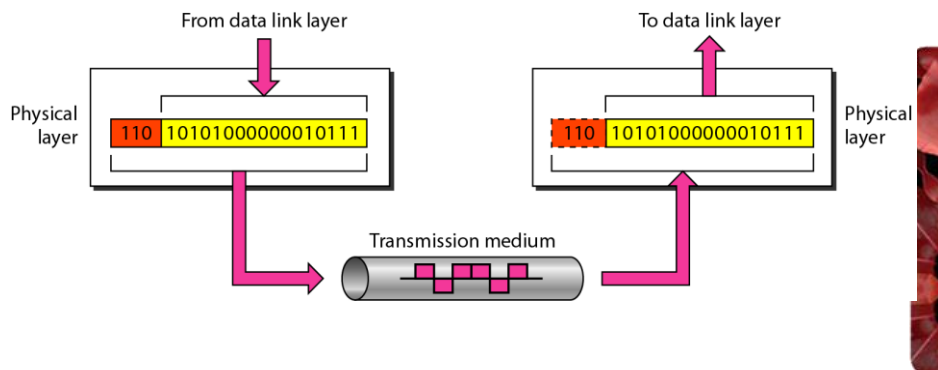
The Physical Layer

- ❑ The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- ❑ It deals with the mechanical and electrical specifications of the interface and transmission medium.
- ❑ It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- ❑ The physical layer is concerned with the following:
 - Physical characteristics of interfaces and medium.
 - Representation of bits.
 - Data rate.
 - Synchronization of bits.
 - Line configuration.
 - Physical topology.
 - Transmission mode.



84

Figure 21 *Physical layer*



85



Note

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

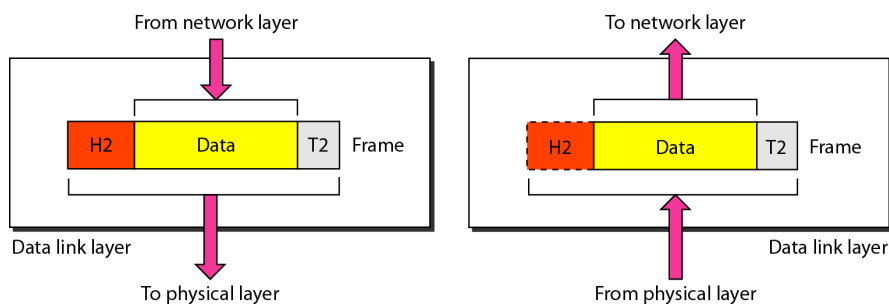
86

The Datalink Layer

- ❑ The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- ❑ It makes the physical layer appear error-free to the upper layer (network layer).
- ❑ Other responsibilities of the data link layer include the following:
 - Framing.
 - Physical addressing.
 - Flow control.
 - Error control.
 - Access control.
 - Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel.
 - A special sublayer of the data link layer, the medium access control sublayer, deals with this problem.

87

Figure 22 *Data link layer*



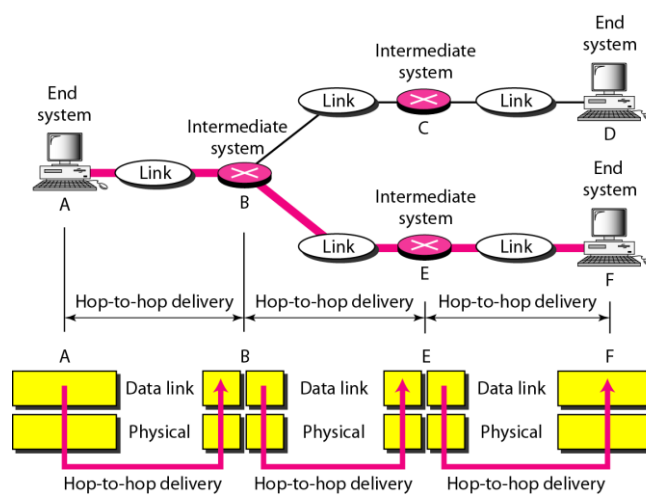
88

Note

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

89

Figure 23 Hop-to-hop delivery



90

The Network Layer

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

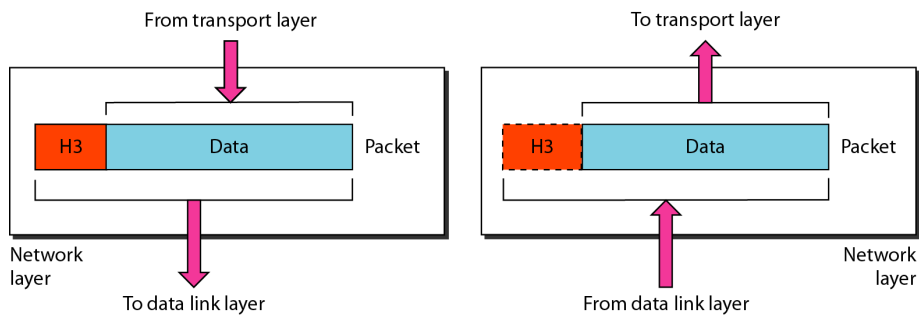
91

The Network Layer

- ❑ Other responsibilities of the network layer include the following:
 - Logical addressing.
 - The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems.
 - Routing.
 - When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.
 - Congestion control.
 - If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. Handling congestion is also a responsibility of the network layer, in conjunction with higher layers that adapt the load they place on the network.

92

Figure 24 *Network layer*



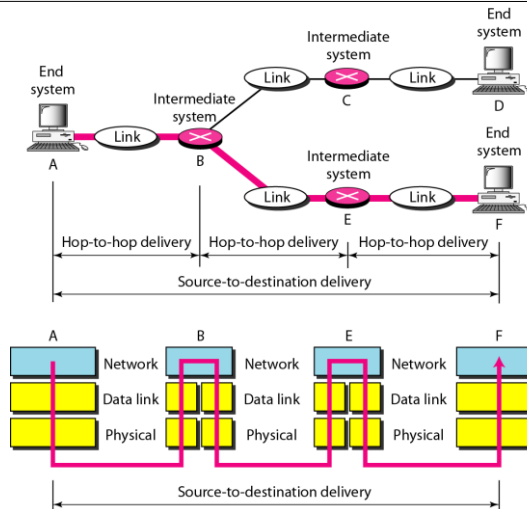
93

Note

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

94

Figure 25 *Source-to-destination delivery*



95

The Transport Layer

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

96

The Transport Layer

- ❑ The basic function of the transport layer is to accept data from above it, 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 layers from the inevitable changes in the hardware technology over the course of time.
- ❑ Other responsibilities of the transport layer include the following:
- ❑ Service-point (port) addressing.
 - Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.



97

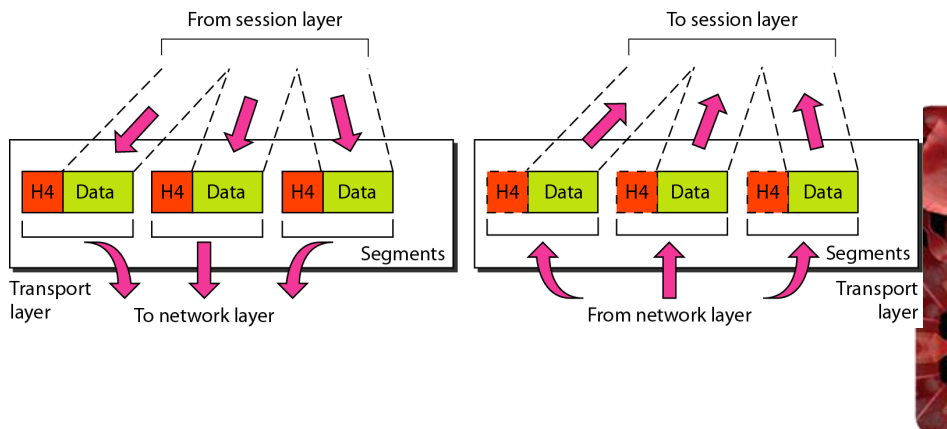
The Transport Layer

- ❑ Segmentation and reassembly.
- ❑ Connection control.
 - The transport layer can be either connectionless or connection oriented.
- ❑ Flow control.
- ❑ Error control.
 - However, error control at this layer is performed process-to process rather than across a single link.
 - The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).



98

Figure 26 *Transport layer*



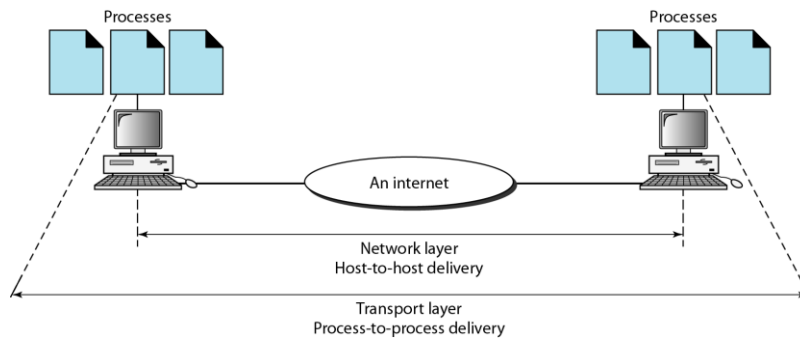
99

Note

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

100

Figure 27 *Reliable process-to-process delivery of a message*



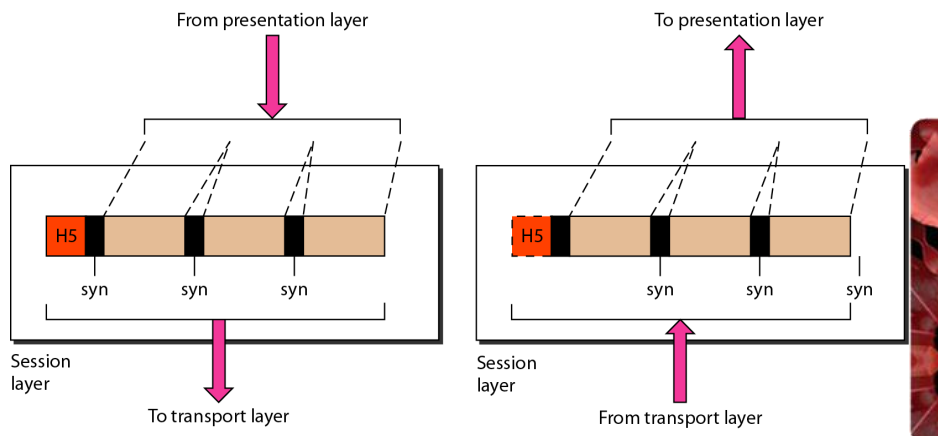
101

The Session Layer

- ❑ The 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 simultaneously),
 - synchronization (checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

102

Figure 28 *Session layer*



103

Note

The session layer is responsible for dialog control and synchronization.

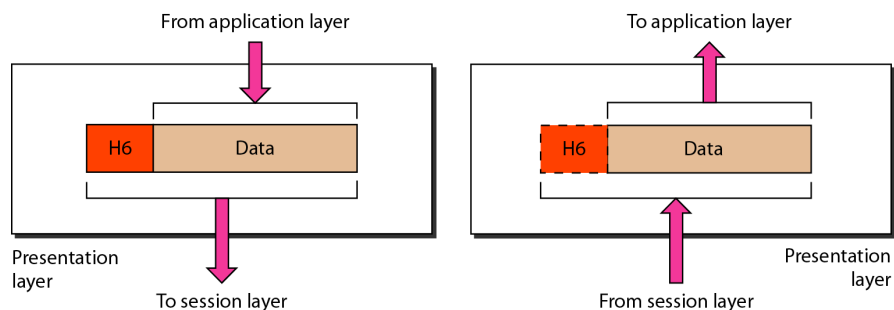
104

The Presentation Layer

- ❑ The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- ❑ Specific responsibilities of the presentation layer include the following:
 - **Translation:** The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
 - **Encryption:** To carry sensitive information, a system must be able to ensure privacy.
 - **Compression:** Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

105

Figure 29 *Presentation layer*



106



Note

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



107

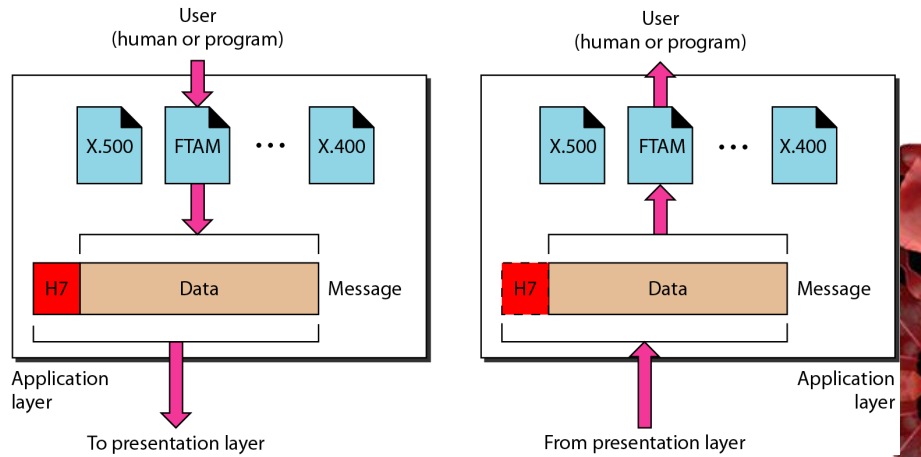
The Application Layer

- ❑ The application layer enables the user, whether human or software, to access the network.
- ❑ It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- ❑ Specific services provided by the application layer include the following:
 - **Network virtual terminal:** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
 - **File transfer, access, and management.**
 - **Mail services.**
 - **Directory services:**



108

Figure 30 *Application layer*



109

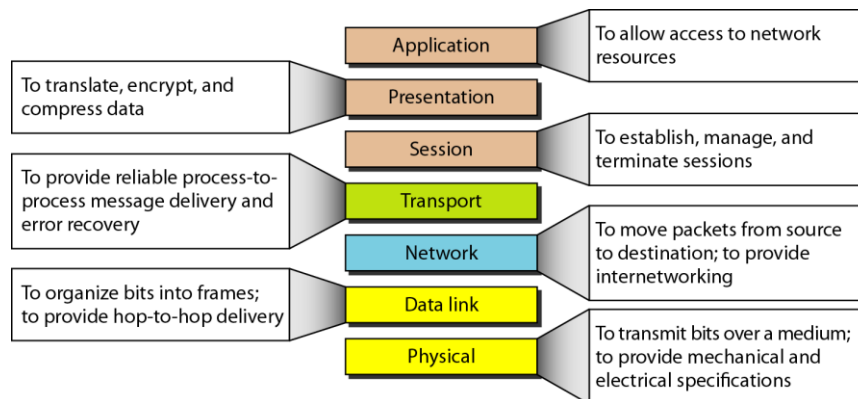


Note

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

110

Figure 31 Summary of layers



111

TCP/IP PROTOCOL SUITE

The layers in the [TCP/IP protocol suite](#) do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: [host-to-network](#), [internet](#), [transport](#), and [application](#). However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: [physical](#), [data link](#), [network](#), [transport](#), and [application](#).

[Physical and Data Link Layers](#)

[Network Layer](#)

[Transport Layer](#)

[Application Layer](#)

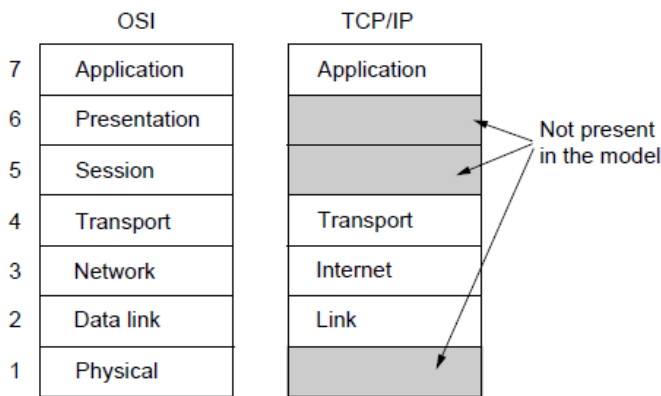
112

The TCP/IP Reference Model Layers

- ❑ Link layer
- ❑ Internet layer
- ❑ Transport layer
- ❑ Application layer

113

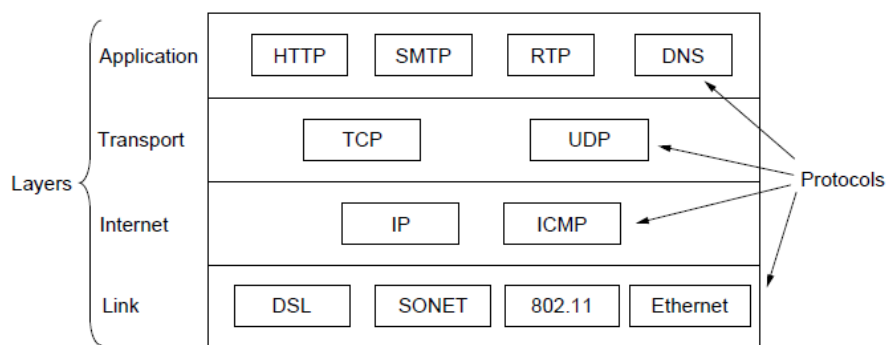
The TCP/IP Reference Model



The TCP/IP reference model

114

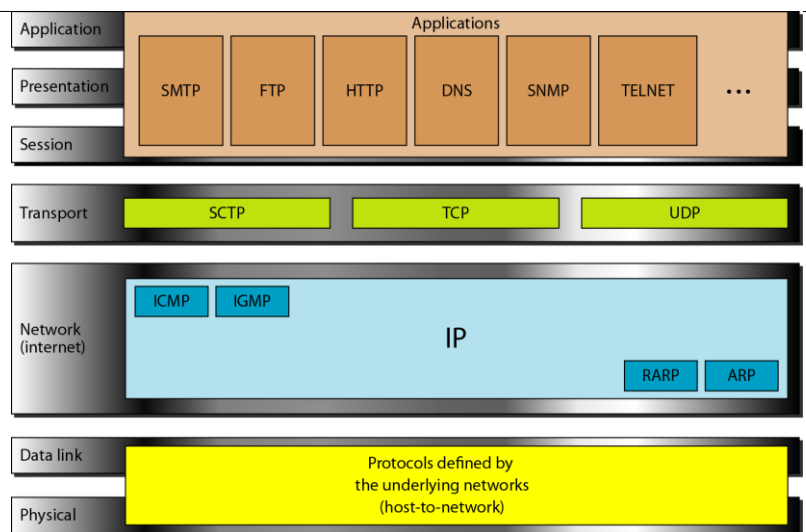
The TCP/IP Reference Model



The TCP/IP reference model with some protocols we will study

115

Figure 32 *TCP/IP and OSI model*



116

ADDRESSING

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

Physical Addresses

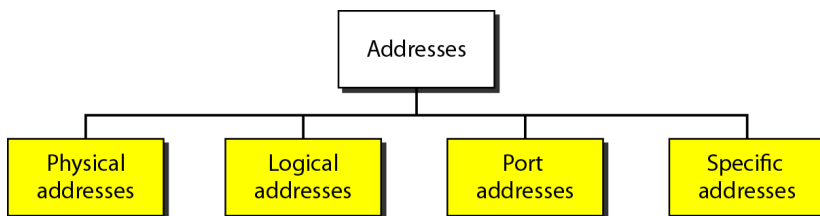
Logical Addresses

Port Addresses

Specific Addresses

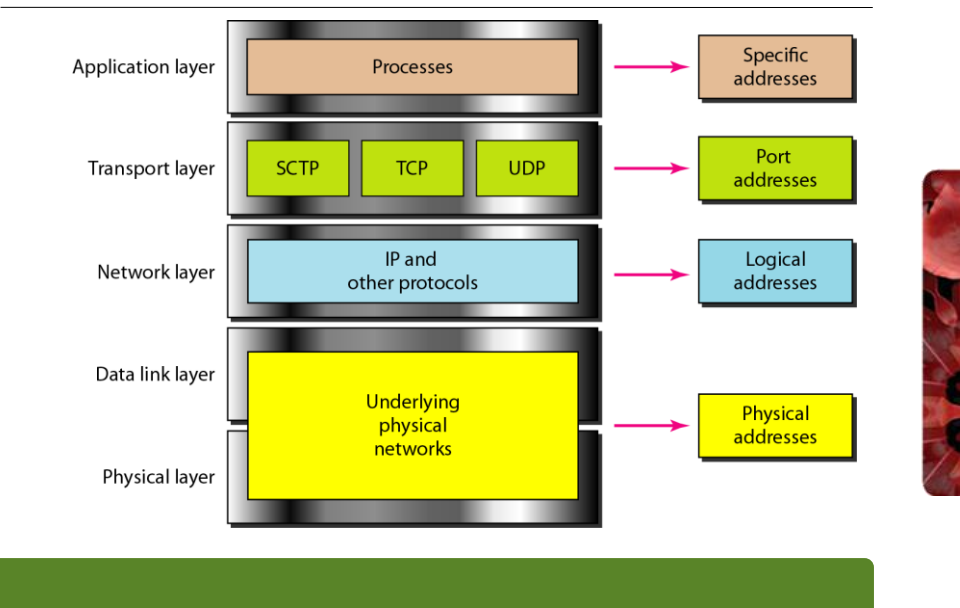
117

Figure 33 *Addresses in TCP/IP*



118

Figure 34 Relationship of layers and addresses in TCP/IP



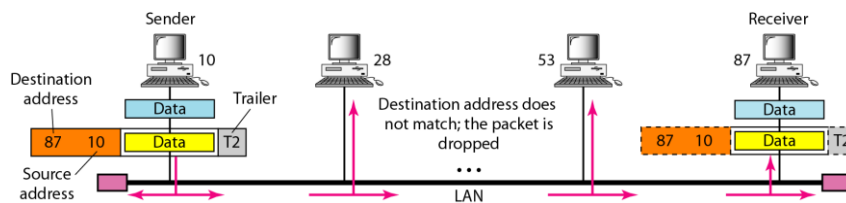
119

Example 1

In Figure 35 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

120

Figure 35 *Physical addresses*



121

Example 2

Most local-area networks use a **48-bit** (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

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

122

Example 3



Figure 36 *IP addresses*

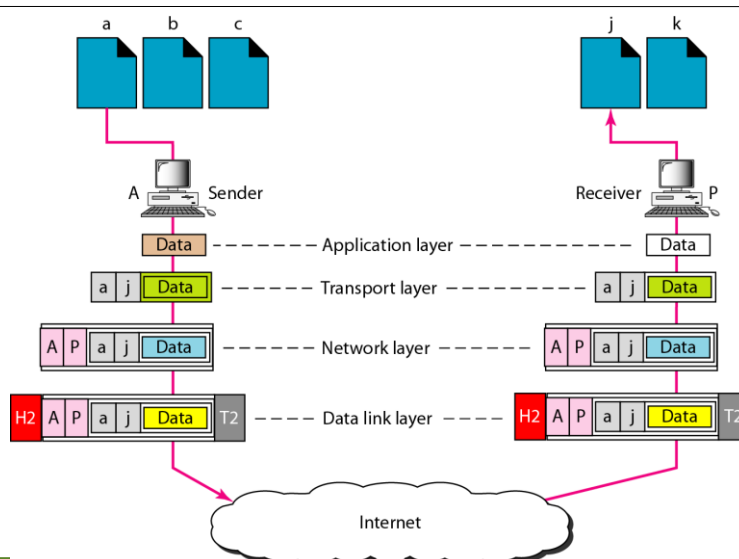


Example 4

Figure 37 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

125

Figure 37 *Port addresses*



126



Note

The physical addresses will change from hop to hop, but the logical addresses usually remain the same.



127



Example 5

A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented as one single number.



128

Comparison of the OSI and TCP/IP Reference Models

Concepts central to OSI model

- ❑ Services
- ❑ Interfaces
- ❑ Protocols



130

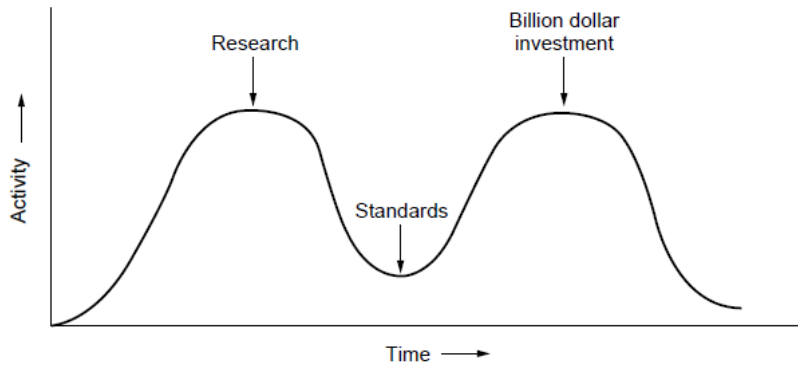
Critique of the OSI Model and Protocols

- ❑ Bad timing.
- ❑ Bad technology.
- ❑ Bad implementations.
- ❑ Bad politics.



131

OSI Model Bad Timing



The apocalypse of the two elephants.

132

