R.M.K
GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

20CS501
Computer Networks

Department

Computer Science and Engineering
Artificial Intelligence and Data Science

Batch/Year

2020-2024 / III Year

Created by

Ms.S.Srijayanthi (ADS)
Ms.K.Ramya Devi (CSE)
Mr.Kingsley (CSE)

Date

30.07.2022

Table of Contents

COURSE OBJECTIVES

- To study the fundamental concepts of computer networks and physical layer.
- To gain the knowledge of various protocols and techniques used in the data link layer.
- To learn the services of network layer and network layer protocols.
- To describe different protocols used in the transport layer.
- To understand the application layer protocols.

SYLLABUS

UNIT I INTRODUCTION AND PHYSICAL LAYER

Data Communications – Network Types – Protocol Layering – Network Models (OSI, TCP/IP) Networking Devices: Hubs, Bridges, Switches – Performance Metrics – Transmission media - Guided media -Unguided media- Switching-Circuit Switching - Packet Switching.

UNIT II DATA LINK LAYER

Introduction – Link-Layer Addressing- Error Detection and Correction - DLC Services – Data Link Layer Protocols – HDLC – PPP - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth

UNIT III NETWORK LAYER

Network Layer Services – Packet switching – Performance – IPV4 Addresses – Forwarding of IP Packets - Network Layer Protocols: IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

UNIT IV TRANSPORT LAYER

Introduction – Transport Layer Protocols – Services – Port Numbers – User Datagram Protocol –Transmission Control Protocol – SCTP.

UNIT V APPLICATION LAYER

Application layer-WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP

Course Outcomes

CO1: Understand the fundamental concepts of computer networks and physical layer.

CO2: Gain knowledge of various protocols and techniques used in the data link layer.

CO3: Learn the network layer services and network layer protocols.

CO4: Understand the various protocols used in the transport layer.

CO5: Analyze the various application layer protocols.

CO- PO/PSO Mapping

Overall Correlation Matrix of the Course as per Anna University Curriculum

Course Code	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C302	3	1	2									

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes Including Course Enrichment Activities

Course Outcomes (COs)		Programme Outcomes (POs), Programme Specific Outcomes (PSOs)														
		PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
		K3	K4	K5	K5	K3 /K5	A2	A3	A3	A3	A3	A3	A2	K3	K3	K3
C302.1	K2	2	1											2	2	2
C302.2	K4	3	3	2	2									3	3	3
C302.3	K4	3	3	2	2									3	3	3
C302.4	K4	3	2	2	2									3	3	3
C302.5	K3	3	2	1	1									3	3	3
C302.6	K2	2	1											2	2	2
C302.7	A2												3			
C302.8	A2								2	2	2		3			
C302.9	A3						3	3		3	3		3			
C302		3	3	2	2		1	1	1	3	3		3	3	3	3

LECTURE PLAN

UNIT – I

S No	Topics	No of periods	Proposed date	Actual Lecture Date	pertaining CO	Taxonomy level	Mode of delivery
1	Course objective, course outcome delivery Data Communications	1	10.08.2022		CO1	K1	Chalk & Talk
2	Network Types	1	11.08.2022		CO1	K1	ICT Tools
3	Protocol Layering	1	12.08.2022		CO1	K2	ICT Tools
4	Network Model– TCP/IP Protocol suite	1	13.08.2022		CO1	K2	ICT Tools
5	Network Model _ OSI	1	18.08.2022		CO1	K2	ICT Tools
6	Networking Device	1	20.08.2022		CO1	K3	Chalk & Talk
7	Performance Metric	1	24.08.2022		CO1	K2	Chalk & Talk
8	Transmission Media	1	25.08.2022		CO1	K2	Chalk & Talk
9	Switching	1	26.08.2022		CO1	K2	ICT Tools
	Content Beyond the Syllabus		27.08.2022		CO1 CO2	K2	Group Discussion

ACTIVITY BASED LEARNING

(MODEL BUILDING/PROTOTYPE)

S NO	TOPICS
1	OSI Model
2	Stop and Wait protocol
3	TCP/IP Protocol Suite
4	Types of Topology
5	Virtual Packet Switching

https://youtu.be/octsVZwf68E

https://youtu.be/N_kgTxJ29j8

https://youtu.be/kdoleTyUqwo

UNIT – I

1.1 Data Communications

Introduction

Communication is needed to share information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

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

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

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

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

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 30 ms. 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.

A data communications system has five components, as shown in Figure -1. **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 soon.

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

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

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

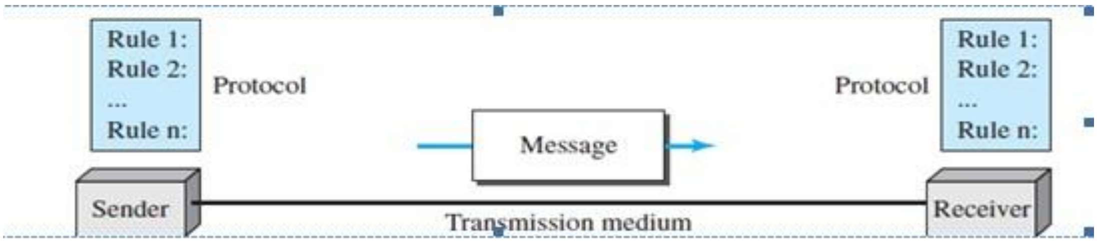


Figure -1.1 Five components of data communication

UNIT – I

- A **network** is the interconnection of a set of devices capable of communication. a device can be a host (or an end system as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system.

- A device in this definition can also be a connecting device such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on. These devices in a network are connected using wired or wireless transmission media such as cable or air.

Network Criteria

The most important criteria are performance, reliability, and security.

1. Performance

- Performance can be measured in terms of transit time and response time.
- Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.
- The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- Performance is often evaluated by two networking metrics: throughput and delay.
- If throughput is increased, we increase the delay because of traffic congestion in the network.

2. Reliability

Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness.

3. Security

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

Physical Structures

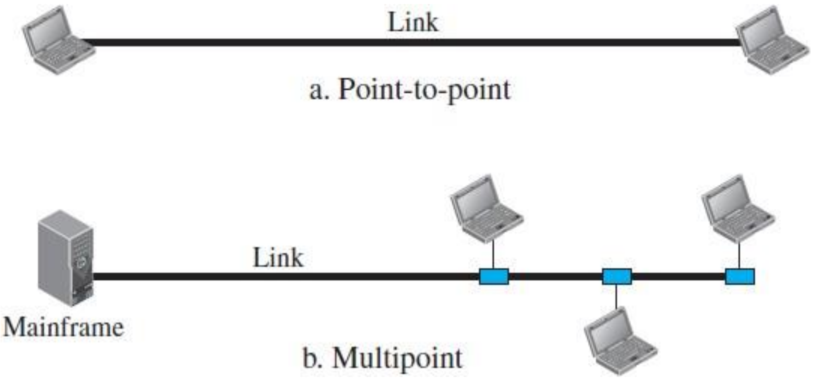
1. Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

Point-to-Point: 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.

Multipoint: A **multipoint** (also called **multidrop**) **connection** is one in which more than two specific devices share asingle link.

Figure – 1.2 – Types of communications: (a) Point to Point (b) Multipoint



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.

2. Physical Topology

The term physical topology refers to the way in which a network is laid out physically. 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.

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. The number of physical links in a fully connected mesh network with n nodes, we need n (n–1) physical links (simplex links). We need n (n – 1) / 2 duplex-mode links. Every device on the network must have n – 1 input/output (I/O) ports.

Advantages

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating traffic problems.
- A mesh topology is robust.
- There is an advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
- Point-to-point links make fault identification and fault isolation easy.

Disadvantages

- Amount of cabling and the number of I/O ports required.
- Because every device must be connected to every other device, installation and reconnection aredifficult.
- The hardware required to connect each link is expensive.

Example of a mesh topology is the connection of telephone regional offices in which each regional officeneeds to be connected to every other regional office.

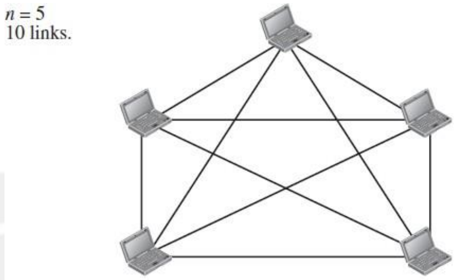


Figure 1.3 – A fully connected mesh topology (five devices)

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.

Advantages

- Less expensive.
- Each device needs only one link and one I/O port to connect it to any number of others.
- Easy to installand reconfigure.
- Less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Robustness. If one link fails,
  only that link is affected

Disadvantages

- Dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system isdead.

- The star topology is used in local-area networks

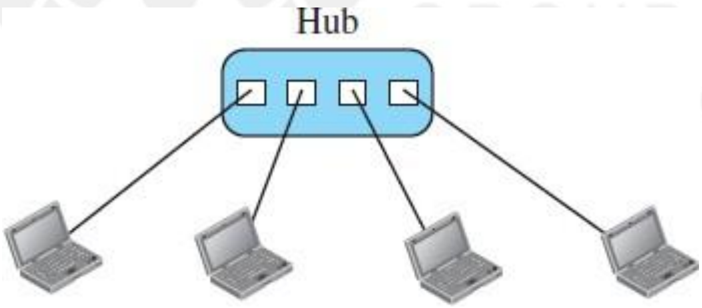


Figure 1.4 – A Star topology connecting four stations

UNIT – I

Bus Topology

A **bus topology** is multipoint. One long cable acts as a **backbone** to link all the devices in a network.

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

Advantages

Ease of installation. Backbone cable can be laid along the most efficient path. Each drop line has to reachonly as far as the nearest point on the backbone.

Disadvantages

- Difficult reconnection and fault isolation.
- Difficult to add new devices. Adding new devices may therefore require modification or replacement ofthe backbone.
- Signal reflection at the taps can cause degradation in quality.
- 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.

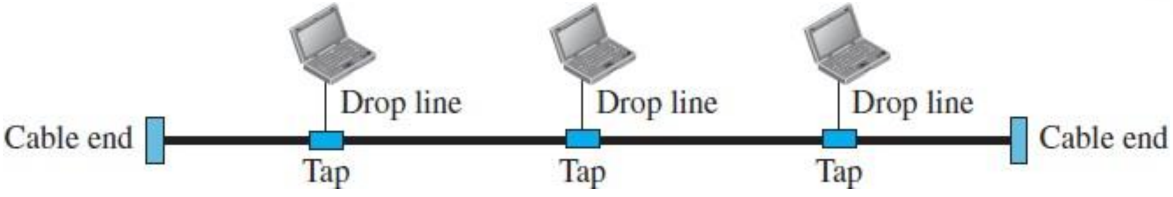


Figure 1.5 – A bus topology

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.

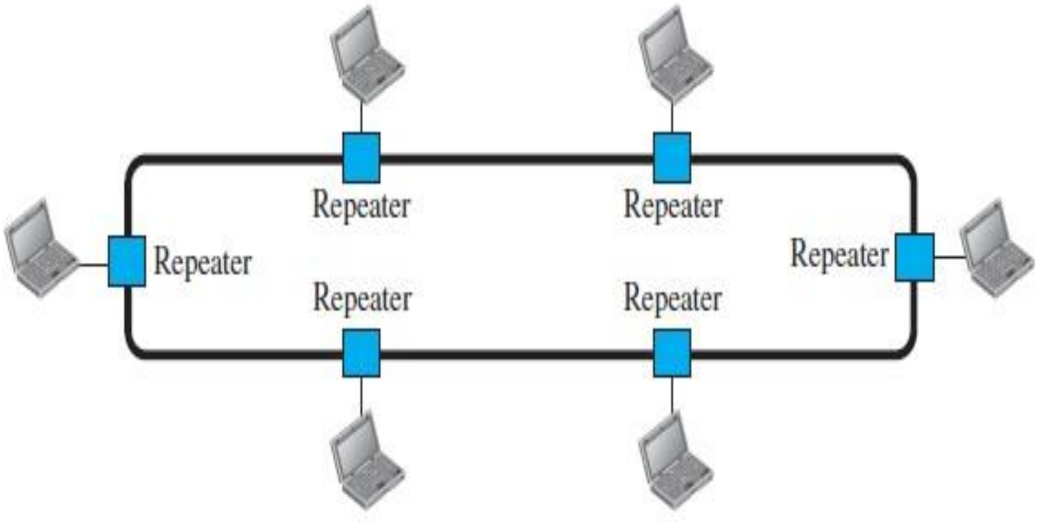


Figure – 1.6 – A ring topology

Advantages

- Easy to install and reconfigure.
- To add or delete a device requires changing only two connections.
- fault isolation is simplified

Disadvantages

A break in the ring can disable the entire network. This weakness can be solved by using a dual ring or aswitch capable of closing off the break.

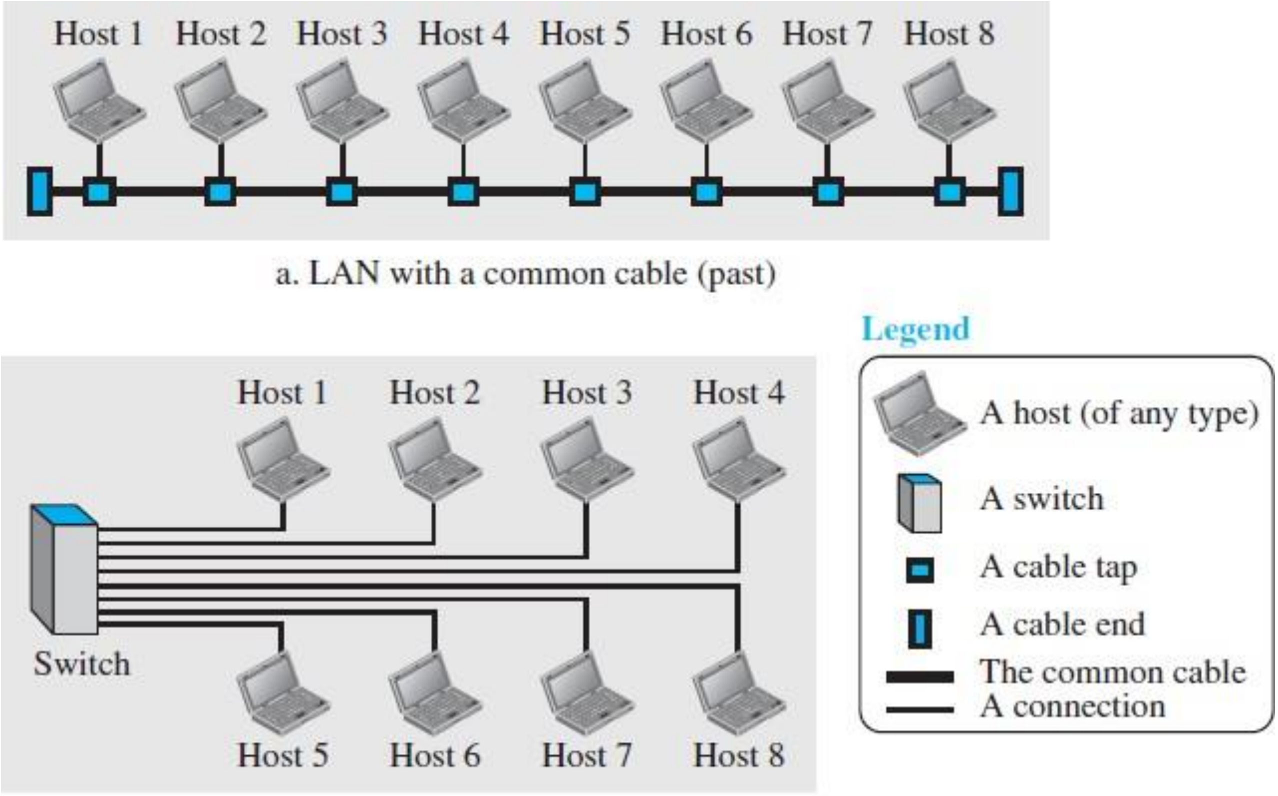
1.2 Network Types

Local Area Network

A **local area network** (**LAN**) is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, 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 devices.

- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.

- In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet.
- Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts. The data rate is more than 1 Mbps.



a. LAN with a common cable (past)

b. LAN with a switch (today)

Figure 1.7 – Isolated LAN in past and present

Wide Area Network

- A **wide area network (WAN)** is also an interconnection of devices capable of communication. WAN has a wider geographical span, spanning a town, a state, a country, or even the world. WAN interconnects connecting devices such as switches, routers, or modems.
- WAN is normally created and run by communication companies and leased by an organization that uses it.

Point-to-Point WAN

- A point-to-point WAN is a network that connects two communicating devices through a transmission Media

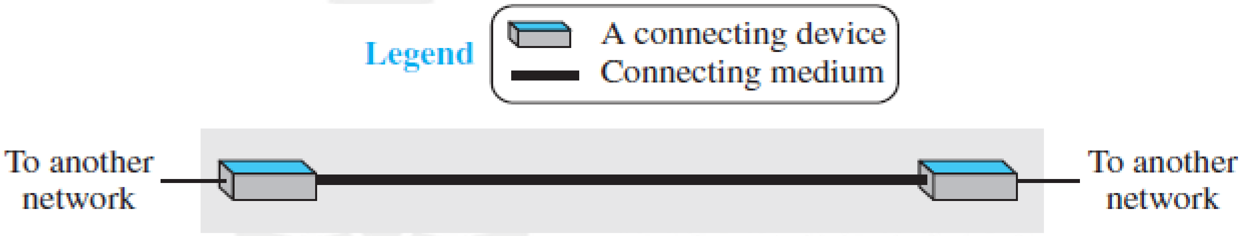


Figure 1.8 – Point to point WAN

Switched WAN

A switched WAN is a network with more than two ends. A switched WAN, as we will see shortly, is used in the backbone of global communication today. A switched WAN is a combination of several point-to-point WANs that are connected by switches.

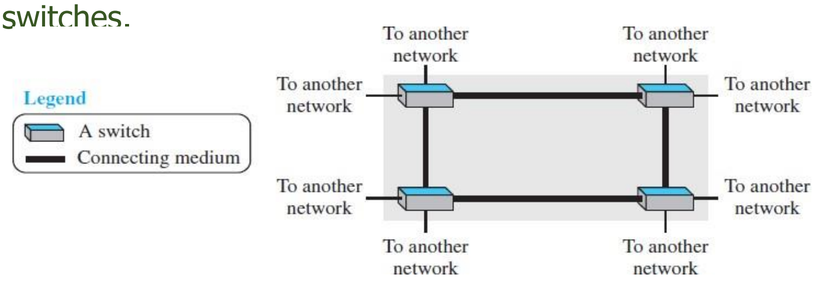


Figure 1.9 – Switched WAN

When two or more networks are connected, they make an **internetwork,** or **internet.** Each office has a LAN that allows all employees in the office to communicate with each other.

To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs. Now the company has an internetwork, or a private internet (with lowercase i). Communication between offices is now possible.

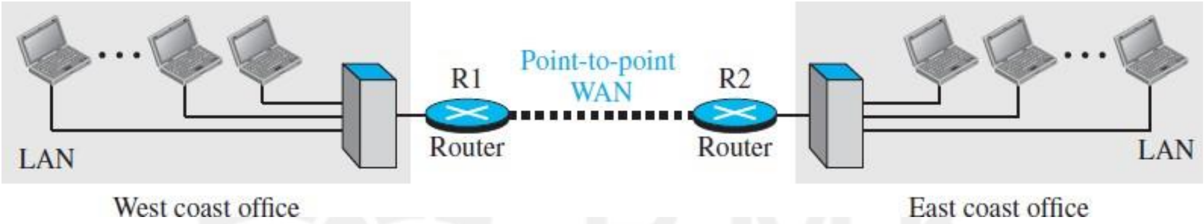


Figure 1.10 – Two LANs interconnected with point to point WAN

Metropolitan Area Network

It is larger than LAN and limited to a city or a group of nearby corporate offices. The data transfer rate is from 34 Mbps to 150 Mbps. It is designed with two unidirectional buses with independent traffic in each.

1.3 Protocol Layering

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**

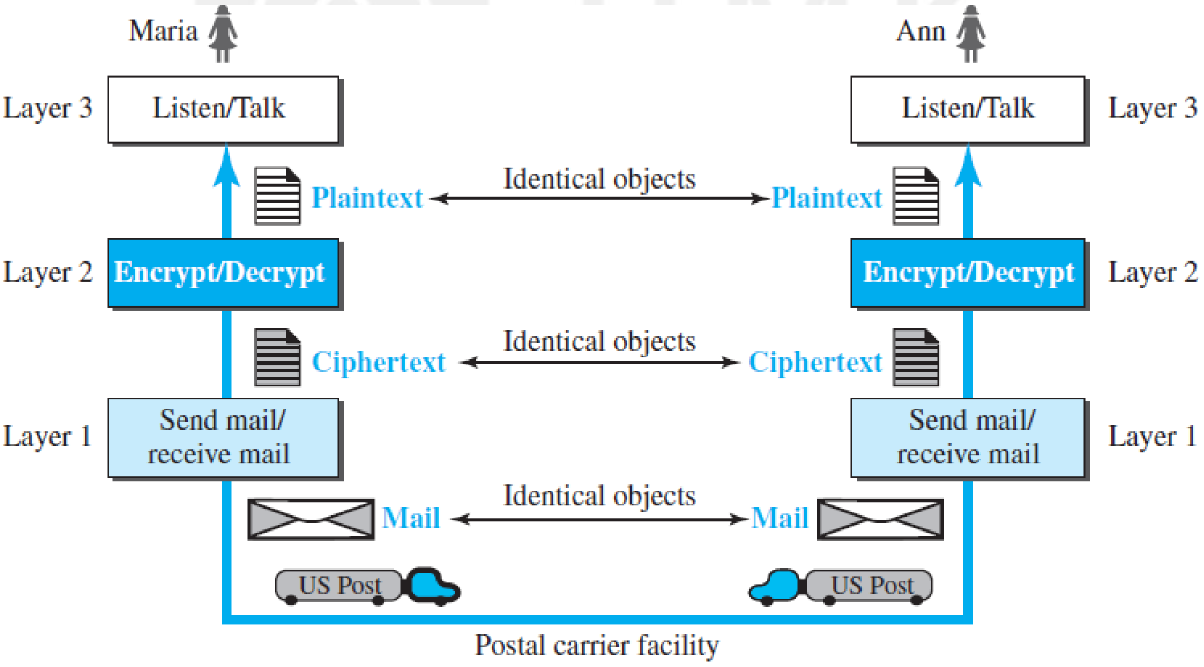
UNIT – I

Protocol layering enables us to divide a complex task into several smaller and simpler tasks. Modularity means independent layers. A layer (module) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs.

Advantages:

- Allows us to separate the Services from the implementation. A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer without knowing how the layer is implemented.
- Communication does not always use only two end systems; there are intermediate systems that need onlysome layers, but not all layers.

Principles of Protocol Layering



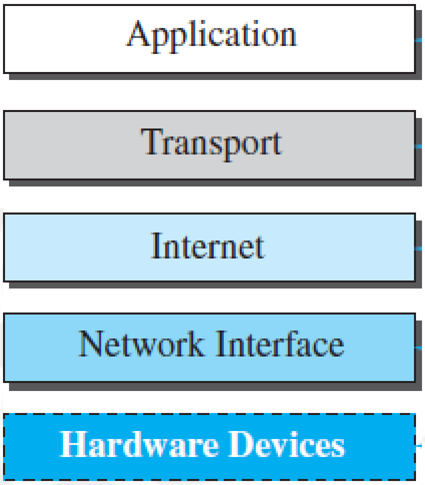
1.11 A Three Layered Protocol

UNIT – I

TCP /IP protocol Suite

- TCP/IP (Transmission Control Protocol/Internet Protocol) is a protocol suite used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or morelower level protocols. TCP/IP is of a five-layer model.

Layered Architecture



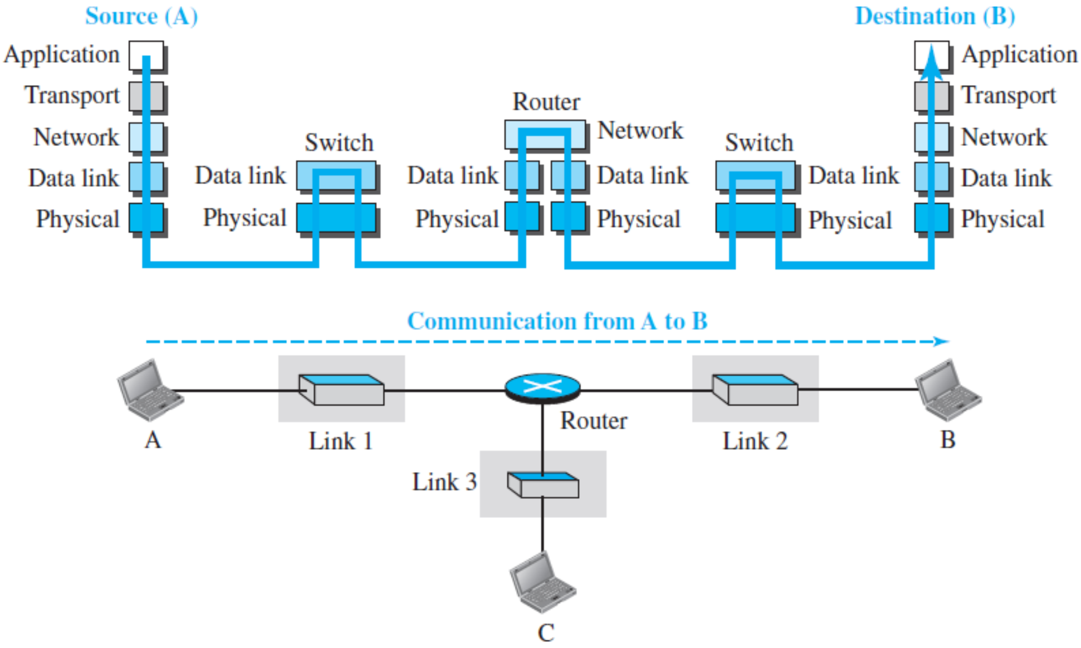
1.12 Layers in the TCP/IP protocol suite

Computer A communicates with computer B. There are five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B).

- Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.

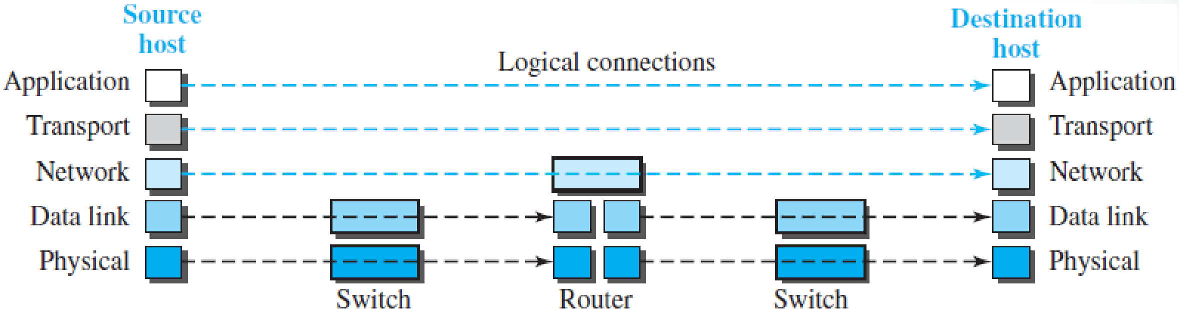
❁ The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer. The router is involved in only three layers; there is no transport or application layer in a router as long as the router is used only for routing. A link-layer switch in a link is involved only in two layers.

Layers in the TCP/IP Protocol Suite



1.13 Communication through an internet

- ➢ The duty of the application, transport, and network layers is end-to-end.
- ➢ However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router. In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.
- ➢ In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.



1.14 Logical connections between layers of the TCP/IP protocol suite

Physical Layer

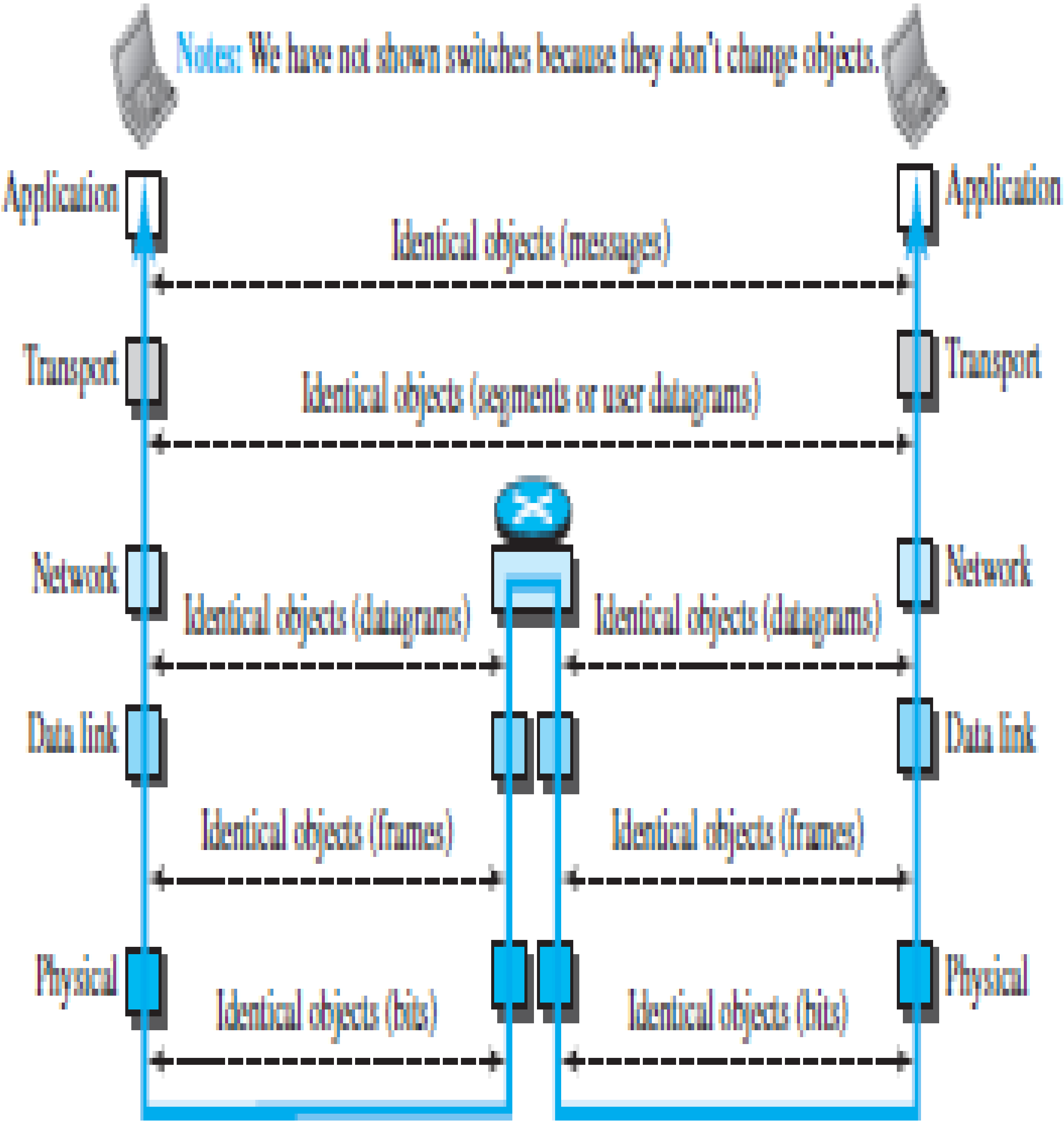
- The physical layer is responsible for carrying individual bits in a frame across the link. Physical layer is the lowest level in the TCP/IP protocol Suite.

- The communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.

- Two devices are connected by a transmission medium (cable or air). The transmission medium does not carry bits; it carries electrical or optical signals.

- The bits received in a frame from the data- link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit.

- There are several protocols that transform a bit to a signal.


Notes: We have not shown switches because they don't change objects.
Application
Application
Identical objects (messages)
Transport
Transport
Identical objects (segments or user datagrams)
Network
Network
Identical objects (datagrams)
Identical objects (datagrams)
Data link
Data link
Identical objects (frames)
Identical objects (frames)
Physical
Physical
Identical objects (bits)
Identical objects (bits)

Data-link Layer

- The data-link layer is responsible for taking the datagram and moving it across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
- The data-link layer takes a datagram and encapsulates it in a packet called a frame. Each link-layer protocol may provide a different service.
- Some link-layer protocols provide complete error detection and correction, some provide only error correction.

Network Layer

- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.
- Network layer is responsible for host-to-host communication and routing the packet through possible routes.
- Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer. IP also defines the format and the structure of addresses used in this layer. IP is also responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.

- The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols. A routing protocol does not take part in routing (it is the responsibility of IP),
- but it creates forwarding tables for routers to help them in the routing process.
- The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.

- The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet.
- The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking.
- The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host.
- The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

Transport Layer

- The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host.
- There are a few transport-layer protocols in the Internet, each designed for some specific task. Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data.

- It creates a logical pipe between two TCPs for transferring a stream of bytes.
- TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination), error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones), and congestion control to reduce the loss of segments due to congestion in the network.

- User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection.
- In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless).
- UDP is a simple protocol that does not provide flow, error, or congestion control.

- A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

Application Layer

- The two application layers exchange messages between each other. Communication at the application layer is between two processes. To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer.

- The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW).
- The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service. The File Transfer Protocol (FTP) is used for transferring files from one host to another.

- The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.

- The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internetat global and local levels.
- The Domain Name System (DNS) is used by other protocols to find the network-layer address of acomputer.
- The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

Encapsulation and Decapsulation

Encapsulation at the Source Host

At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer. The message is passed to the transport layer.

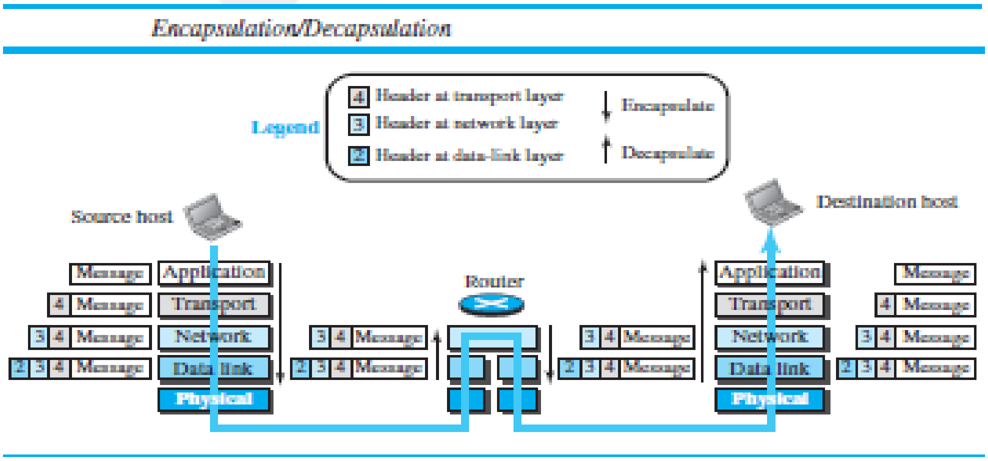


Figure 1.21 - Encapsulation/Decapsulation

1. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.

2. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on.

The result is the network-layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

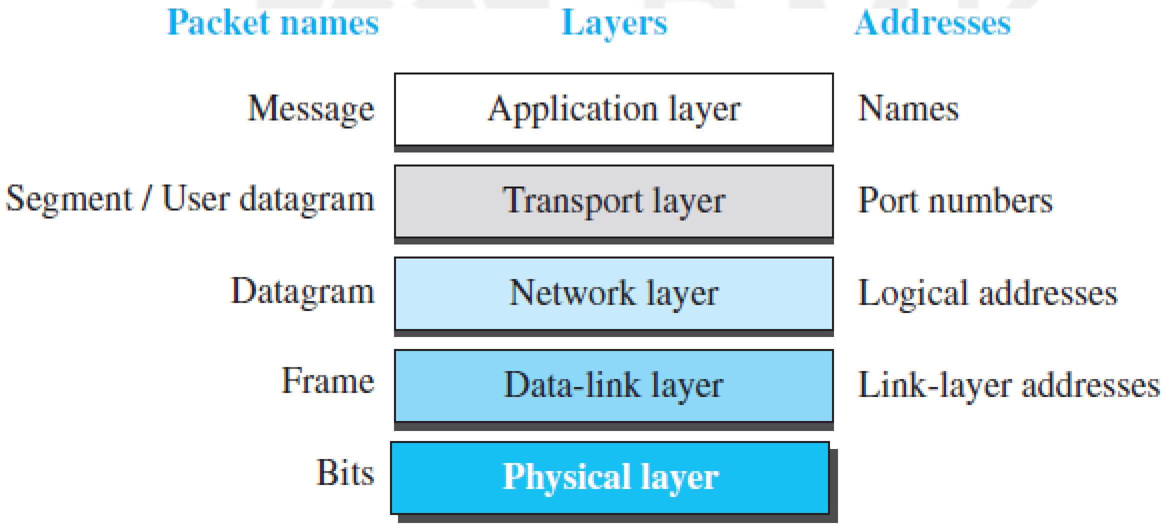
1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layerof the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layerfor transmission.

Decapsulation at the Destination Host

At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking.

Addressing

- Any communication that involves two parties needs two addresses: source address and destination address. At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguish between several programs running at the same time. At the network-layer, the addresses are global, with the whole Internet as the scope. A network-layer address uniquely defines the connection of a device to the Internet. The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).



Packet names	Layers	Addresses
Message	Application layer	Names
Segment / User datagram	Transport layer	Port numbers
Datagram	Network layer	Logical addresses
Frame	Data-link layer	Link-layer addresses
Bits	Physical layer	

Figure 1.22 – Addressing in the TCP/IP protocol suite

UNIT – I

Addressing in the TCP/IP protocol suite

Multiplexing and Demultiplexing

Multiplexing means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time). Demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time). To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong. At the transport layer, either UDP or TCP can accept a message from several application-layer protocols. At the network layer, IP can accept a segment from TCP or a user datagram from UDP. IP can also accept a packet from other protocols such as ICMP, IGMP, and so on. At the data-link layer, a frame may carry the payload coming from IP or other protocols such as ARP.

ISO - OSI reference Model

- **International Organization for Standardization (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.
- An open system is a set of protocols that allows any two different systems to communicate.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- There are 7 Layers in the OSI model. Each layer has a specific function.

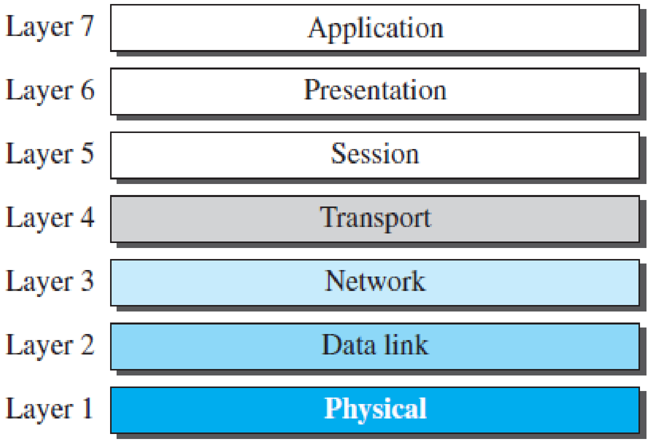


Figure - 1.24 -The OSI model

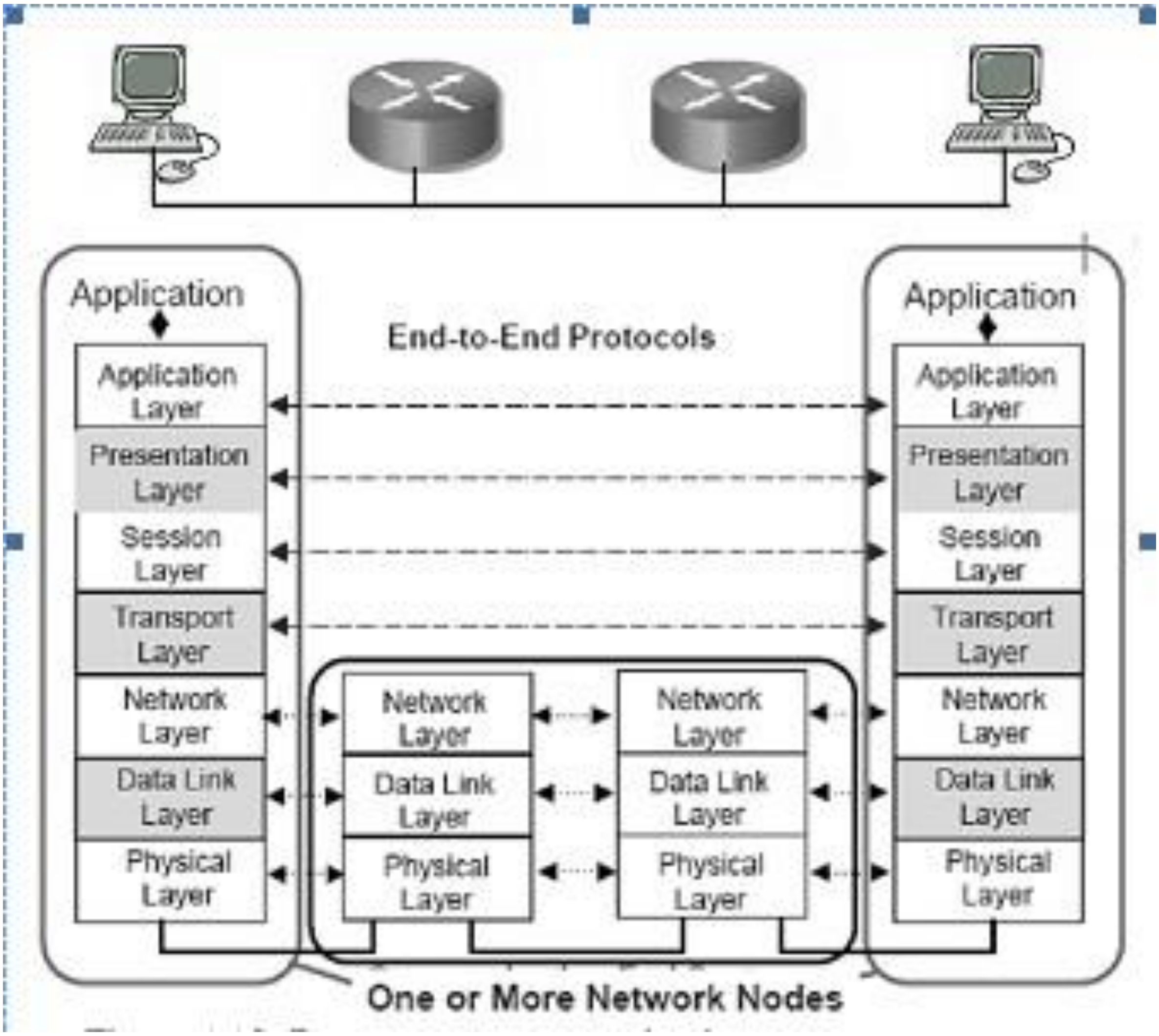
Physical Layer:

It coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical (cable, plugs, pins etc.) and electrical (modulation, signal strength, voltage levels, bit times) specifications of the interface and transmission media. It also defines the procedures and functions that physical devices and interfaces have to perform for transmissionto occur.

Major responsibilities of Physical layer are:

- **Physical characteristics of interfaces and media:** It defines the characteristics of the interface between the devices and the transmission media. Also defines the type of transmission medium.
- **Representation of bits:** To transmit the bits, it must be encoded into electrical or optical signals. Physical layer defines the type of representation i.e. how Os and 1's are changed to signals.
- **Data rate:** The number of bits sent each second is also defined by the physical layer. That is the physical layer defines the duration for which the bit lasts.
- **Synchronization of bits:** Sender and the receiver must be synchronized at the bit level. That is the physical layer ensures that the sender and the receiver clocks are synchronized.

UNIT – I



Peer-to-peer communication processes

UNIT – I

Data link layer:

The data link layer is responsible for hop-to-hop (node-to-node) delivery

The duties of the data link layer are:

- **Framing:** The data link layer divides the stream of bits received from the network layer intomanageable data units called frames.
- **Physical Addressing:** If the frames are to be distributed to different systems on the network the data link layer adds a header to the frame to define the receiver or sender of the frame.
- **Flow Control:** If the rate at which the data absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to overwhelming the receiver.
- **Error control:** Reliability is added to the physical layer by data link layer to detect and retransmit loss or damaged frames and also to prevent duplication of frames.
- **Access control:** When two or more devices are connected to the same link it determines whichdevice has control over the link at any given time.

Network Layer:

- The network layer is responsible for source-to-destination delivery of a packet across multiple networks. It ensures that each packet gets from its point of origin to its final destination.
- It does not recognize any relationship between those packets.
- It treats each one independently as though each belong to separate message.

UNIT – I

The functions of the network layer are:

- **Internetworking:** The logical gluing of heterogeneous physical networks together to look like asingle network to the upper layers.
- **Logical Addressing:** If a packet has to cross the network boundary then the header contains information of the logical addresses of the sender and the receiver.
- **Routing:** When independent networks or links are connected to create an internetwork or a large network the connective devices route the packet to the finaldestination.
- **Packetizing:** Encapsulating packets received from the upper layer protocol. Internet Protocol is usedfor packetizing in the network layer.
- **Fragmenting:** Router has to process the incoming frame and encapsulate it as per the protocol used bythe physical network to which the frame is going.

Transport Layer: The transport layer is responsible for process-to-process delivery of the entire message.

The responsibilities of Transport layer are:

- **Service-point (port) addressing:** Computers run several programs at the same time. Source-to- destination delivery means delivery from a specific process on one computer to a specific process on the other. The transport layer header therefore includes a type of address called port address.

Segmentation and reassembly:

- A message is divided into segments and each segment contains a sequence number.
- These numbers enable the Transport layer to reassemble the message correctly upon arriving at the destination.
- The packets lost in the transmission is identified and replaced.

Connection control: The transport layer can be either connectionless or connection- oriented.

- A connectionless transport layer treats segment as an independent packet and delivers it to the transport layer.

- A connection-oriented transport layer makes a connection with the transport layer at the destination machine and delivers the packets. After all the data are transferred the connection is terminated.

Flow control: Flow control at this layer is performed end

Error Control: Error control is performed end to end.

Session Layer:

Session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems.

- **Specific responsibilities of the layer are:**

  - **Dialog Control:** Session layer allows two systems to enter in to a dialog. Communication between two processes takes place either in half-duplex or full-duplex.
  - **Synchronization:** The session layer allows a process to add checkpoints into a stream of data. Example: If a system is sending a file of 2000 pages, check points may be inserted after every 100 pages to ensure that each 100 page unit is advised and acknowledged independently. So if a crash happens during the transmission of page 523, retransmission begins at page 501, pages 1 to 500 need not be retransmitted.

Presentation layer: It is concerned with the syntax and semantics of the information exchanged between two systems.

Responsibilities of the presentation layer are

Translation: The processes in two systems are usually exchanging information in the form ofcharacter strings, numbers, and so on.

Since different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. At the sender, the presentation layer changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver dependent format.

- **Encryption:** The sender transforms the original information from one form to another form and sends the resulting message over the entire network. Decryption reverses the original process to transform the message back to its original form.
- **Compression:** It reduces the number of bits to be transmitted. It is important in the transmission oftext, audio and video.

Application Layer: It enables the user (human/software) to access the network. It provides user interfacesand support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information services.

Services provided by the application layer are

- **Network Virtual terminal:** A network virtual terminal is a software version of a physical terminaland allows a user to log on to a remote host.
- **File transfer, access and management:** This application allows a user to access files in a remote computer, to retrieve files from a remote computer and to manage or control files in a remote computer.
- **Mail services:** This application provides the basis for e-mail forwarding and storage.

Directory services: It provides distributed database sources and access to global information about various objects and services.

Networking Devices

Hub

- A hub is basically a multiport repeater.
- A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- In other words, the collision domain of all hosts connected through Hub remains one.
- Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.
- Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of the hierarchy of stations.
- The stations connect to the hub with an RJ-45 connector having a maximum segment length is 100 meters.
- This type of interconnected set of stations is easy to maintain and diagnose. The figure shows how several hubs can be connected in a hierarchical manner to realize a single LAN of a bigger size with a large number of nodes.

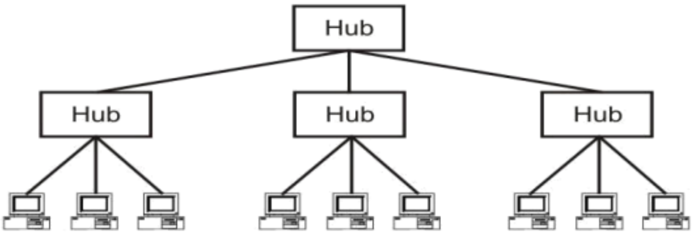


Figure Hub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes

Bridge

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.

It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

The device that can be used to interconnect two separate LANs is known as a bridge. It is commonly used to connect two similar or dissimilar LANs as shown in Figure. The bridge operates in layer 2, that is the data-link layer and that is why it is called level-2 relay with reference to the OSI model.

It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations.

The flow of information through a bridge is shown in Fig. 6.1.5. Use of bridges offer a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN.

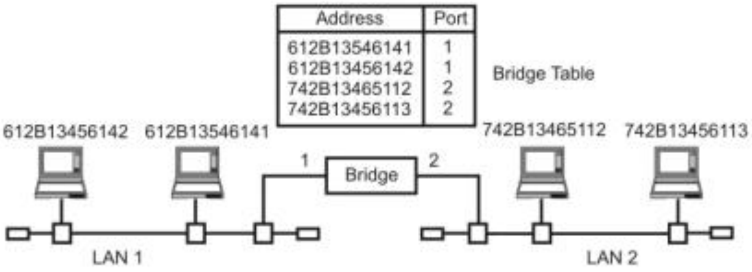
The parameters that define the QOS include availability, frame mishaps, transit delay, frame lifetime, undetected bit errors, frame size and priority. Key features of a bridge are mentioned below:

- A bridge operates both in physical and data-link layer
- A bridge uses a table for filtering/routing
- A bridge does not change the physical (MAC) addresses in a frame
- Types of bridges: Transparent Bridges and Source routing bridges

A bridge must contain addressing and routing capability. Two routing algorithms have been proposed for a bridged LAN environment.

The first, produced as an extension of IEEE 802.1 and applicable to all IEEE 802 LANs, is known as transparent bridge.

And the other, developed for the IEEE 802.5 token rings, is based on source routing approach. It applies to many types of LAN including token ring, token bus and CSMA/CD bus.



Address	Port
612B13546141	1
612B13456142	1
742B13465112	2
742B13456113	2

Figure A bridge connecting two separate LANs

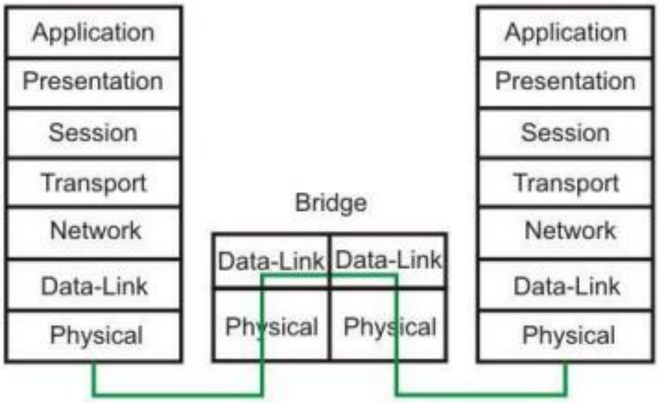


Figure Information flow through a bridge

Switch

A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance.

Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

In other words, switch divides collision domain of hosts, but broadcast domain remains same. A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames.

Some of important functionalities are:

- Ports are provided with buffer
- Switch maintains a directory: #address - port#
- Each frame is forwarded after examining the #address and forwarded to the proper port#

Three possible forwarding approaches: Cut-through, Collision-free and Fullybuffered as briefly explained below.

Cut-through: A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.

Collision-free: In this case, the switch forwards the frame after receiving 64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.

Fully buffered: In this case, the switch forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

1.6 Network Performance

It is measured in two ways:

- **Bandwidth (bandwidth in hertz and bandwidth in bits per second)**

Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz. The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

- **Throughput**

- The **throughput** is a measure of how fast we can actually send data through a network. A link may have a bandwidth of B bps, but we can only send T bps through this link with T always less than B. In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast wecan send data.

Example: A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution

We can calculate the throughput as

Throughput = **(12,000** X **10,000) / 60** = **2 Mbps**

The throughput is almost one-fifth of the bandwidth in this case.

- **Latency (Delay)**

The **latency** or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = **propagation time** + **transmission time** + **queuing time** + **processing delay**

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = Distance / (Propagation Speed)

Example

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagationspeed to be 2.4 × 10^8 m/s in cable.

Solution

We can calculate the propagation time as

Propagation time = **(12,000** X **1,000) / (2.4** X **10^8) = 50 ms**

The **transmission time** of a message depends on the size of the message and the bandwidth of the channel.

Transmission time = **(Message size) / Bandwidth**

Example: What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message (an email) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4 × 10^8 m/s.

Solution

We can calculate the propagation and transmission time as

Propagation time = **(12,000** X **1000) / (2.4 X 10^8)** = **50 ms**

Transmission time = **(2500** X **8) / 10^9** = **0.020 ms**

Example

What are the propagation time and the transmission time for a 5-MB (megabyte) message (an image) if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 12,000km and that light travels at 2.4 × 108 m/s.

Solution

We can calculate the propagation and transmission times as

Propagation time = **(12,000** X **1000) / (2.4** X **10^8) = 50 ms Transmission time** = **(5,000,000** X **8) /10^6** = **40 s**

The **queuing time is** the time needed for each intermediate or end device to hold the message before it can be processed. It is not a fixed factor. When there is heavy traffic on the network, the queuing time increases.

- **Jitter**

Jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example). If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

1.7 Transmission media

- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A **transmission medium** can be broadly defined as anything that can carry information from a source to a destination.

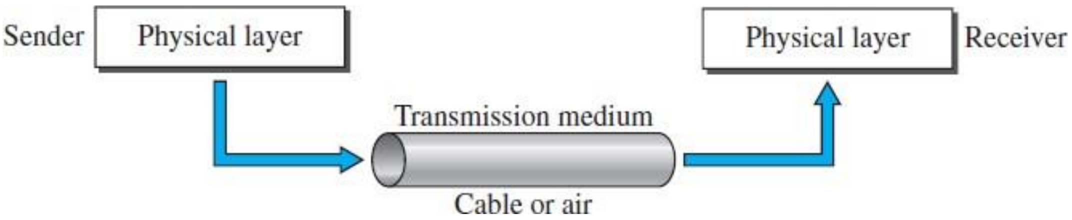


Figure 1.26 – Transmission media with physical layer

Transmission medium and physical layer

In telecommunications, transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

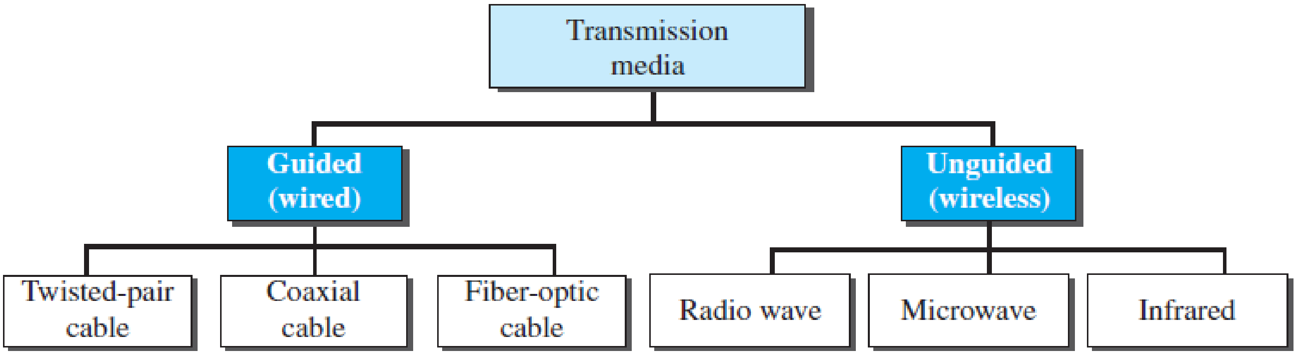


Figure 1.27 Transmission medium and physical layer

UNIT – I

Classes of transmission media

Guided Media

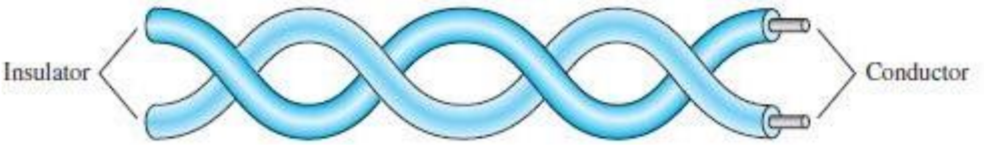
- **Guided media,** which are those that provide a conduit from one device to another, include **twisted-pair cable, coaxial cable,** and **fiber-optic cable.**

- A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.

- **Optical fiber** is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable

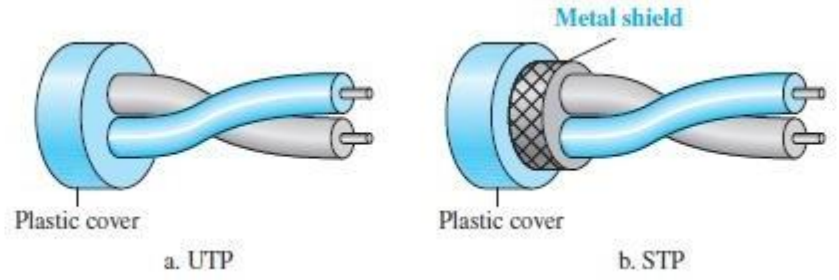
A twisted pair consists of two conductors, each with its own plastic insulation, twisted together.



Twisted-pair cable

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

Figure 1.29 UTP and STP cables



a. UTP

b. STP

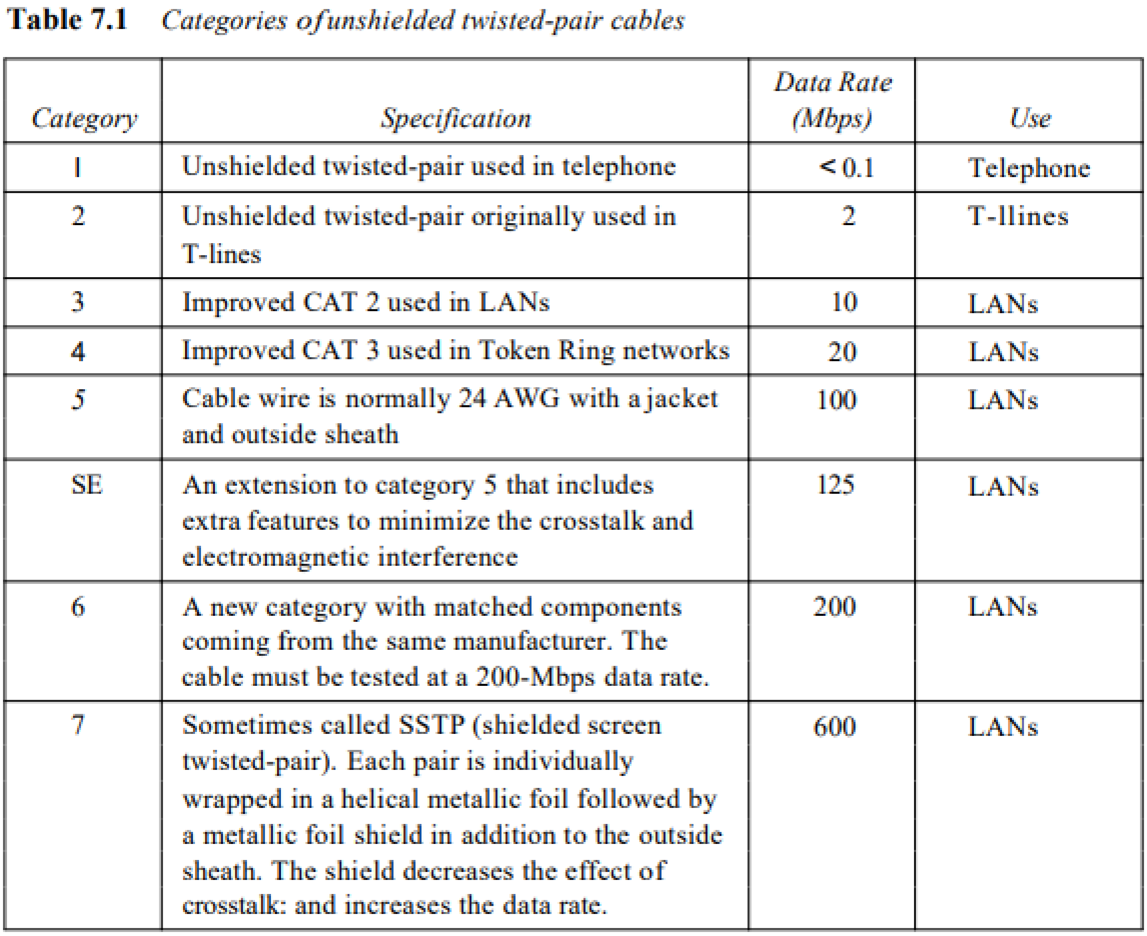
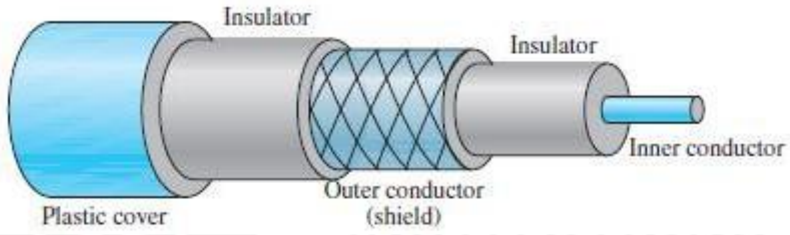


Table 7.1 *Categories ofunshielded twisted-pair cables*

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-llines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk: and increases the data rate.	600	LANs

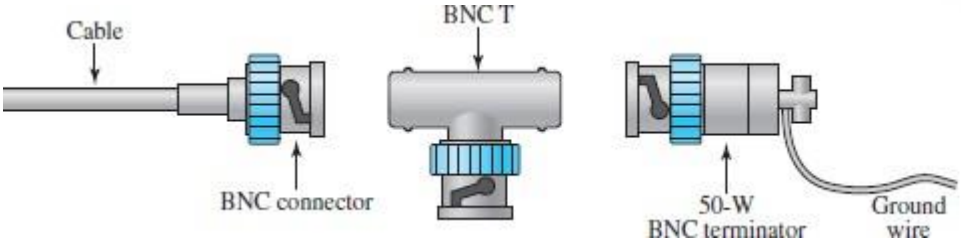
Coaxial Cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted-pair cable, in part because the two media are constructed quite differently.
- Coax has a central core conductor of solid or stranded wire enclosed in an insulating sheath, which in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Coaxial cable

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the **Bayonet Neill-Concelman (BNC)** connector. The three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

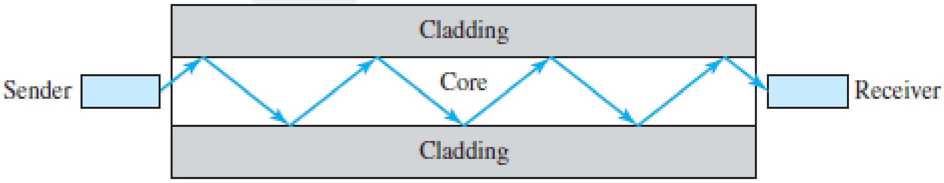


BNC connectors

- Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
- Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps.
- Cable TV networks also use coaxial cables. Another common application of coaxial cable is in traditional Ethernet LANs.

Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Optical fibers use reflection to guide light through a channel.



Optical fiber

Current technology supports two modes, **multimode and single mode** for propagating light along optical channels, each requiring fiber with different physical characteristics.

Multimode can be implemented in two forms: **step-index or graded-index**

- **Multimode** is so named because multiple beams from a light source move through the core in different paths.
- In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density. The term step-index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber. A second type of fiber, called multimode graded-index fiber, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction.
- **Single-mode** uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density.
- There are three types of connectors for fiber-optic cables. The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.
- Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer repeaters when we use fiber-optic cable.
- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network.

UNIT – I

Advantages and Disadvantages of Optical Fiber

- **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

- **Less signal attenuation.** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

- **Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables. **Resistance to corrosive materials.** Glass is more resistant to corrosive materials than copper. **Light weight.** Fiber-optic cables are much lighter than copper cables.
- **Greater immunity to tapping.** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

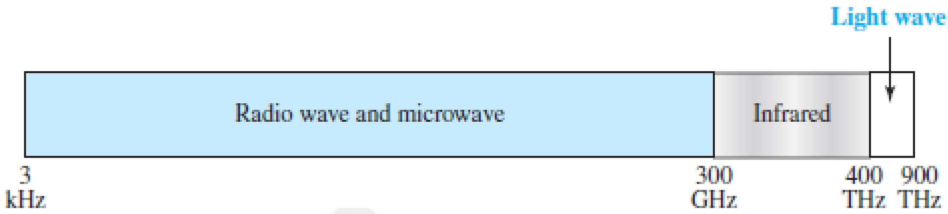
- **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

- **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

- **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

Unguided Media: Wireless

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as **wireless communication.** Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. Unguided signals can travel from the source to the destination in several ways: ground propagation, sky propagation, and line-of- sight propagation.



Electromagnetic spectrum for wireless communication

Propagation Modes

- In **ground propagation,** radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna. The greater the power, the greater the distance.
- In **sky propagation,** higher-frequency radio waves radiate upward into the where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.
- In **line-of-sight propagation,** very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth.
- We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves.

UNIT – I

Radio Waves

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; Radio waves are omnidirectional.
- When an antenna transmits radio waves, they are propagated in all directions. A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.
- The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into subbands, the subbands are also narrow, leading to a low data rate for digital communications.
- Omnidirectional Antenna: Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Figure 7.20 shows an omnidirectional antenna.
- The omnidirectional property has a disadvantage. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Applications

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

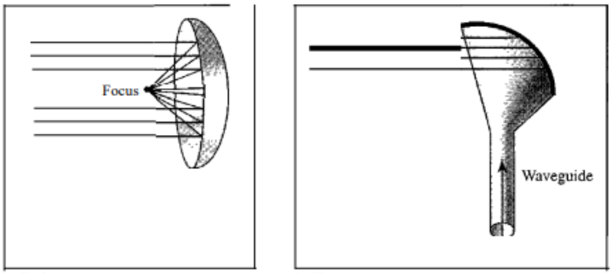
Microwaves

- Electromagnetic waves ranging in frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

- ➢ Microwave propagation is line-of-sight. Repeaters are often needed for long distance communication.
- ➢ Very high-frequency microwaves cannot penetrate walls.
- ➢ The microwave band is relatively wide, almost 299 GHz. A high data rate is possible.
- ➢ Use of certain portions of the band requires permission from authorities.
- ➢ Microwaves need unidirectional antennas that send out signals in one direction.
- ➢ Two types of antennas are used for microwave communications: the **parabolic dish** and the **horn**. A parabolic dish antenna is based on the geometry of a parabola. The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point.

- A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem. Received transmissions are collected by the scooped shape of the horn

- Microwaves wireless LANs.



a. Dish antenna

b. Horn antenna

Applications

- Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver.

- Microwaves are used in cellular phones, satellite networks, and wireless LANs.

Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz can be used for short-range communication. There is no interference. Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

- Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

- When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

- The Infrared Data Association (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers. For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. The standard originally defined a data rate of 75 kbps for a distance up to 8 m.

1.8 Switching

Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. media and equipment. A better solution is **switching.** A switched network consists of a series of interlinked nodes, called **switches.** Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems. Others are used only for routing.

Circuit-Switched Networks

- A **circuit-switched network** consists of a set of switches connected by physical links in which each link is divided into n channels.
- A connection between two stations is a dedicated path made of one or more links.
- However, each connection uses only one dedicated channel on each link.
- A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

Figure 8.3 shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

- The end systems, such as computers or telephones, are directly connected to a switch.
- When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path.
- After the dedicated path made of connected circuits (channels) is established, data transfer can take place. After all data have been transferred, the circuits are torn down.

❁ We need to emphasize several points here:

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.
- Data transferred between the two stations are not packetized. The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.

- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to end addressing used during the setup phase

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties can communicate, a dedicated circuit needs to be established.

The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Note that end-to-end addressing is required for creating a connection between the two end systems.

Data-Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

- When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency

- Circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections.

Delay

Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

Packet Switching

- If the message is going to pass through a **packet-switched network**, it needs to be divided into packets of fixed or variable size.
- The size of the packet is determined by the network and the governing protocol.
- In packet switching, there is no resource allocation for a packet.
- This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand.
- The allocation is done on a first come, first-served basis.
- When a switch receives a packet, no matter what the source or destination is, the packet must wait if there are other packets being processed.

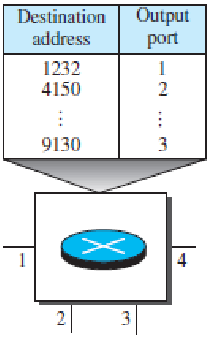
There are two types of packet-switched networks: **datagram networks and virtual circuit networks.**

Datagram Networks

- In a datagram network, each packet is treated independently of all others. Packets in this approach are referred to as datagrams.
- Datagram switching is normally done at the network layer. Different packets from same message may travel through different paths to the destination.
- Packets may arrive at the destination out of order. Packets may also be lost or dropped because of a lack of resources. The datagram networks are sometimes referred to as connectionless networks.
- The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases.

Routing Table

- Each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables.



Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

- Every packet in a datagram network carries a header that contains, among other information, the destination addresses of the packet.
- When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

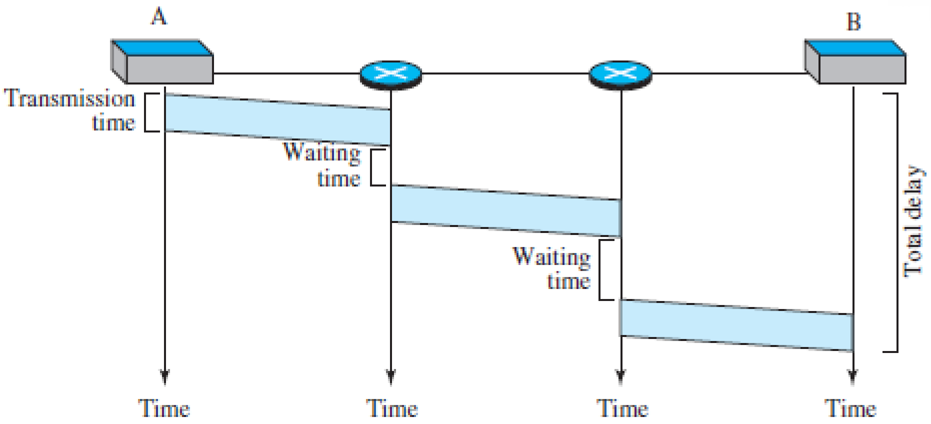
Efficiency

- The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.
- If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Delay

- There may be greater delay in a datagram network. Since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.
- The packet travels through two switches. There are three transmission times (3T), three propagation delays (slopes 3τ of the lines), and two waiting times (w1 + w2). We ignore the processing time in each switch. The total delay is

Total delay = **3T + 3**τ + **w1 + w2**



Delay in a datagram network

Virtual-Circuit Networks

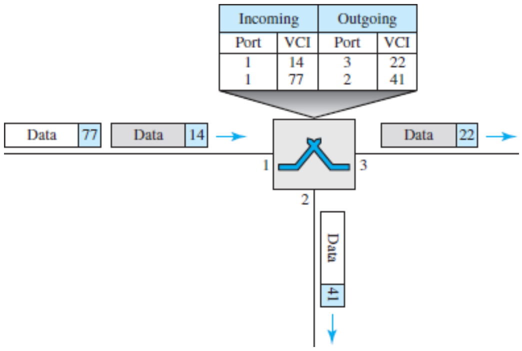
A **virtual-circuit network** is a cross between a circuit-switched network and a datagram network. It hassome characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transferphase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in adatagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data-link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

In a virtual-circuit network, two types of addressing are involved: global and local.

Global Addressing

- A source or a destination needs to have a global address—an address that can be unique in the scope of the network or internationally if the network is part of an international network.
- **Virtual-Circuit Identifier**
- The identifier that is actually used for data transfer is called the **virtual-circuit identifier (VCI)** or the **label.** A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.
- There are three phases in a virtual-circuit network: setup, data transfer, and teardown.
- In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection. In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
- Data-Transfer Phase: To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The switch holds four pieces of information for each virtual circuit that is already set up.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41

Switch and tables in a virtual-circuit network

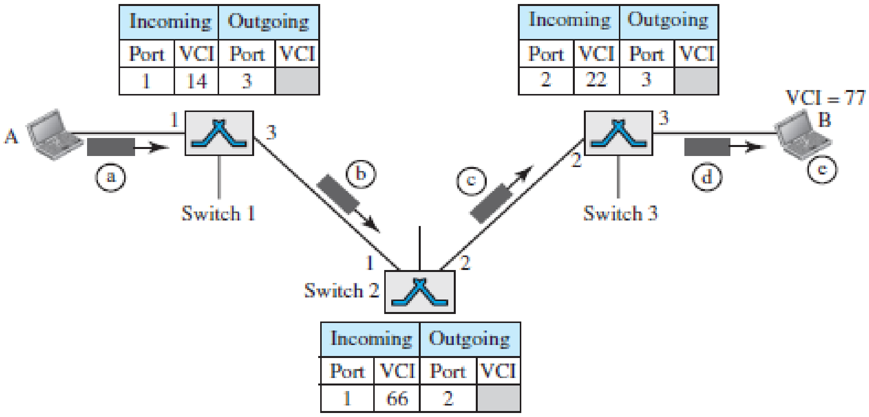
- A frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3. The data-transfer phase is active until the source sends all its frames to the destination.

Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B. Two steps are required: the setup request and the acknowledgment.

Setup Request

A setup request frame is sent from the source to the destination.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	

a. Source A sends a setup frame to switch 1.

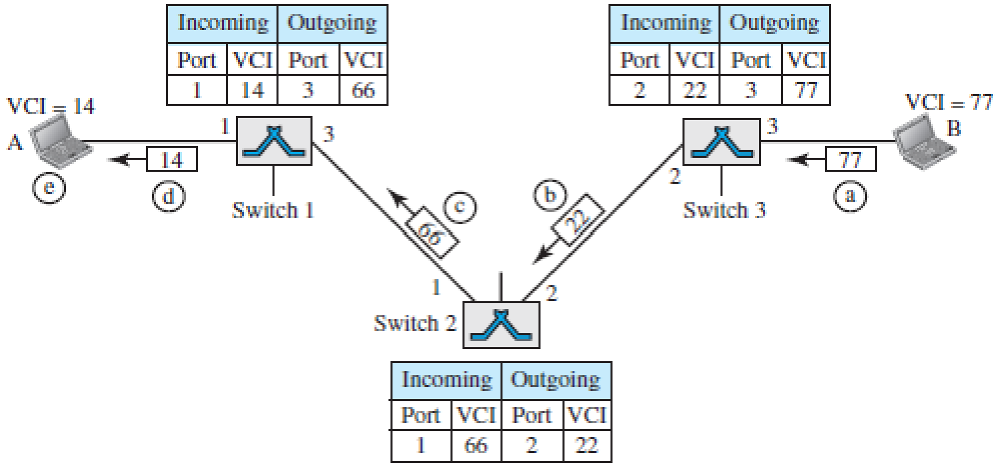
b. Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port

- 3. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.

a. Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (1), incoming VCI (66), and outgoing port (2).

b. Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).

c. Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

Acknowledgment

- A special frame, called the acknowledgment frame, completes the entries in the switching tables.

a. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but theoutgoing VCI for switch 3.

b. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

c. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.

d. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosenin the previous step.

e. The source uses this as the outgoing VCI for the data frames to be sent to destination B.

Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency

Resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data-transfer phase. The delay for each packet is the same or different. In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays. There is one big advantage in a virtual-circuit network even if resource allocation is on demand. The source can check the availability of the resources, without actually reserving it.

Delay

- In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets.
- The packet is traveling through two switches (routers). There are three transmission times (3T), three propagation times (3τ), data transfer depicted by the sloping lines, a setup delay (which includes ransmission and propagation in two directions), and a teardown delay. The total delay time is

Total delay = **3T** + **3τ** + **setup delay + teardown delay**

ASSIGNMENT

1. Assume six devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?

2. For each of the following four networks, discuss the consequences if a connection fails.

a. Five devices arranged in a mesh topology

b. Five devices arranged in a star topology (not counting the hub)

c. Five devices arranged in a bus topology d. Five devices arranged in a ring topology

3. Match the following to one or more layers of the OSI model:

a. Format and code conversion services

b. Establishes, manages, and terminates sessions

c. Ensures reliable transmission of data

d. Log-in and log-out procedures e. Provides independence from differences in data representation

5. Suppose a computer sends a frame to another computer on a bus topology LAN. The physical destination address of the frame is corrupted during the transmission. What happens to the frame? How can the sender be informed about the situation?

MINI PROJECT

1. The design of overall topology need reflects on the network performance. Use any of the tools to build topology by varying the density of the network.

- Network Simulator 3
- Opnet
- Qualnet
- OMNeT++
-

Unit – I Question Bank
Part – A

1.Define networks.(Nov 12) (K1,CO1)

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

2.Compare LAN and WAN. (K4,CO1)

LAN	WAN
Scope of Local Area Network is restricted to a small/ single building	Scope of Wide Area Network spans over large geographical area country/ Continent
LAN is owned by some organization.	A part of n/w asserts are owned or not owned.
Data rate of LAN 10-.10-100mbps.	Data rate of WAN is Gigabyte.

3.What are the four fundamental characteristics that the data communication system depends on? (K1,CO1)

The four fundamental characteristics are: Delivery, Accuracy, Timeliness and Jitter.

4.What are the five components of data communications system? (K1,CO1)

The five components are Message, Sender, Receiver, Transmission Medium and Protocol.

5.Define link and state the types of connection. (K1,CO1)

A link is the communication pathway that transfers data from one device to another. The two possible types of connections are point to point and multipoint

6.What are the two types of line configuration? (Nov/Dec 2010) (K1,CO1)

The two types of line configuration are Point to point line configuration and multipoint line configuration.

Point to point line configuration It provides a dedicated link between 2 devices. Entire capacity of the link is reserved for transmission between 3 devices only Eg: connection between remote control and TV's control system

Multipoint line configuration

- Also called as multi drop connection
- Here the channel capacity is shared and
- If many devices share the link simultaneously it is called spatially shared connection

7. Define point to point and Multipoint. (K1,CO1)

- Point to point – A point to point connection provides a dedicated link between two devices
- Multipoint – A multipoint connection is one in which more than two specific devices share a single link.

8. What is Network topology? List its types. (K1,CO1)

Network topology is the interconnected pattern of network elements. A network topology may be physical, mapping hardware configuration, or logical, mapping the path that the data must take in order to travel around the network. The types are Bus topology, Star topology, Mesh topology and Ring Topology.

9. List the key ingredients of technology that determines nature of a LAN. List the common topologies available for LAN. (K1,CO1)

Topology, Transmission medium and Medium access control technique are the technology that determines nature of a LAN. Star Topology, Ring Topology, Bus Topology and Tree Topology are the topologies available for LAN.

10. What is a protocol? What are the key elements of a protocol? (Nov 15) (K1,CO1)

Protocol is used for communications between entities in a system and must speak the same language. Protocol is the set of rules governing the exchange of data between two entities. It defines what is communicated, how it is communicated, when it is communicated. The Key elements of a Protocol are as follows,

Syntax –It refers to the structure or format of data meaning the order in which they are presented.

- Semantics –It refers to the meaning of each section of bit. How to do interpretation.

- Timing –When data should be sent and how fast they can be sent.

11. What is OSI? (K1,CO1)

OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. It is partitioned into seven layers. It was developed by the International Organization for Standardization (ISO).

12. What are the uses of transport layer? (K1,CO1)

- Reliable data exchange
- Independent of network being used
- Independent of application

13. What is Protocol Data Unit (PDU)? (K1,CO1)

At each layer, protocols are used to communicate and Control information is added to user data at each layer. Transport layer may fragment user data. Each fragment has a transport header added and header consists of destination SAP, sequence number and error detection code.

14. What are the uses of internet layer in TCP/IP? (K1,CO1)

- Systems may be attached to different networks
- Routing functions across multiple networks
- Implemented in end systems and routers

15.What is a layered Network Architecture? (May/June 2015, Nov/Dec 2013) (K1,CO1)

- A layer is created when a different level of abstraction occurs at protocol. Each layer should perform a well defined function.
- Function of each layer should be chosen using internationality standardized protocols. Boundaries between should be chosen to minimize information flow across the interfaces.
- A set of layers and protocol is called network architecture. A list of protocols used by a system is called protocol stack.

16.Compare OSI and TCP. (K4,CO1)

Open System Interconnection	**Transmission Control Protocol**
distinguishes between Service, Interface, Protocol	It does not distinguish between Service,Interface,Protocol
Protocols are well hidden	Protocols are not just hidden
Dejure standard Fit Model	Defacto standard Fit Model
In transport layer only connection oriented services are available	In Transport layer choice is for connection oriented and connectionless
Contains 7 layers	Contains 5 layers

17.How do layers of the internet model correlate to the layers of the OSI model? (K1,CO1)

OSI	**TCP/IP**
Physical Layer	Physical Layer
Data Link Layer	Network Access Layer
Network Layer	IP Layer
Transport Layer	TCP Layer
Session Layer	Application Layer
Presentation Layer	
Application layer	

18. What is the use of data link layer in OSI? (Nov 15) (K1,CO1)

- **Frame synchronization**: Data is divided by data link layer as frames, a manageableunit.
- **Flow Control**: Sending station does not overwhelm receiving station.
- **Error Control**: Any error in bits must be detected and corrected using somemechanism.
- **Addressing**: Two stations in a multi point that involved in transmission must bespecified using physical address
- **Access Control**: When two or more devices are connected to the same link, Accesscontrol mechanism is needed to determine which device has control over the link at any given time.

19.What are the functions of physical layer and presentation layer? (K1,CO1)

- **Functions of Physical Layer-**
- Encoding/ decoding of signals
- Preamble generation/removal (for synchronization)
- Bit transmission/ reception
- **Functions of Presentation Layer-**
- Translation, Encryption / Decryption, Authentication and Compression

20.What are the functions of Application Layer? (May/June 2011) (K1,CO1)

- It enables the user (human/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. Services provided by the application layer are Network Virtual terminal, File transfer, access and management. Mail services, Directory services.

21. Give the purpose of layering. (May/June 2013) (K2,CO1)

- To reduce the complexity of getting all the functions maintained by one a new technique called layering technology was introduced.
- In this, the architecture contains several layers and each layer is responsible for certain functions.
- The general idea is that the services offered by underlying hardware, and then add a sequence of layers, each providing a higher level of service.

22. What are the major duties of Network Layer? (May/June 2012) (K1,CO1)

- It is used to send the data from source to destination with help of logical address.

23. What are the features provided by layering? (K1,CO1)

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.
- Uses abstraction to hide complexity of network from application.

24. Write the parameters used to measure network performance. (May 2016/2018) (K1,CO2)

- The parameters used to measure network performance are Latency, Throughput, Delay, Bandwidth, Jitter, Load, Path cost, Maximum Transmission Unit (MTU), Reliability and Communications Cost.

25. Define Bandwidth (K1,CO2)

- Bandwidth refers to the number of bits per second that a channel, a link, or even a network can transmit.

26. What is Throughput? (K1,CO2)

- It is a measure of how data can actually sent through network.

27. Differentiate between delay and jitter. (Nov/Dec 2013) (K4,CO2)

- **Delay**: Is the amount of time data (signal) takes to reach the destination. Now a higher delay generally means congestion of some sort of breaking of the communication link.

- **Jitter**: Is the variation of delay time. This happens when a system is not in deterministic state eg. Video Streaming suffers from jitter a lot because the size of data transferred is quite large and hence no way of saying how long it might take to transfer.

28. What are the kinds of Cable in Guided Media? (K1,CO2)

- Twisted Pair Cable
- Coaxial Cable
- Optical Fiber Cable

29. What are the types of Transmission Media? (K1,CO2)

- Guided Transmission Media (Wired)
- Unguided Transmission Media (Wireless)

29. What are the types of Unguided Media? (K1,CO2)

- Radio waves
- Microwaves
- Infrared

30. Which cable is suitable long distance communication? (K1,CO2)

- Optical Fiber Cables are suitable for long distance communication.

31. Define Full Duplex and simplex transmission system. (K1,CO2)

- With Full duplex transmission, two stations can simultaneously send and receive data from each other. This mode is known as two-way simultaneous. The signals are transmitted in only one direction. One is the sender and another is the receiver called simplex.

33.What are the three criteria necessary for an effective and efficient network? (K1,CO2)

- The most important criteria are performance, reliability and security.
  - Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w.
  - Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the networks robustness in a catastrophe.
  - Security issues include protecting data from unauthorized access and viruses.

34. Brief the terms unicast, multicast and broadcast. (K5,CO1)

- The different types of addressing are unicast (one-to-one communication), multicasting (communicating to all members of a group) and broadcast (sending to all nodes on the network).

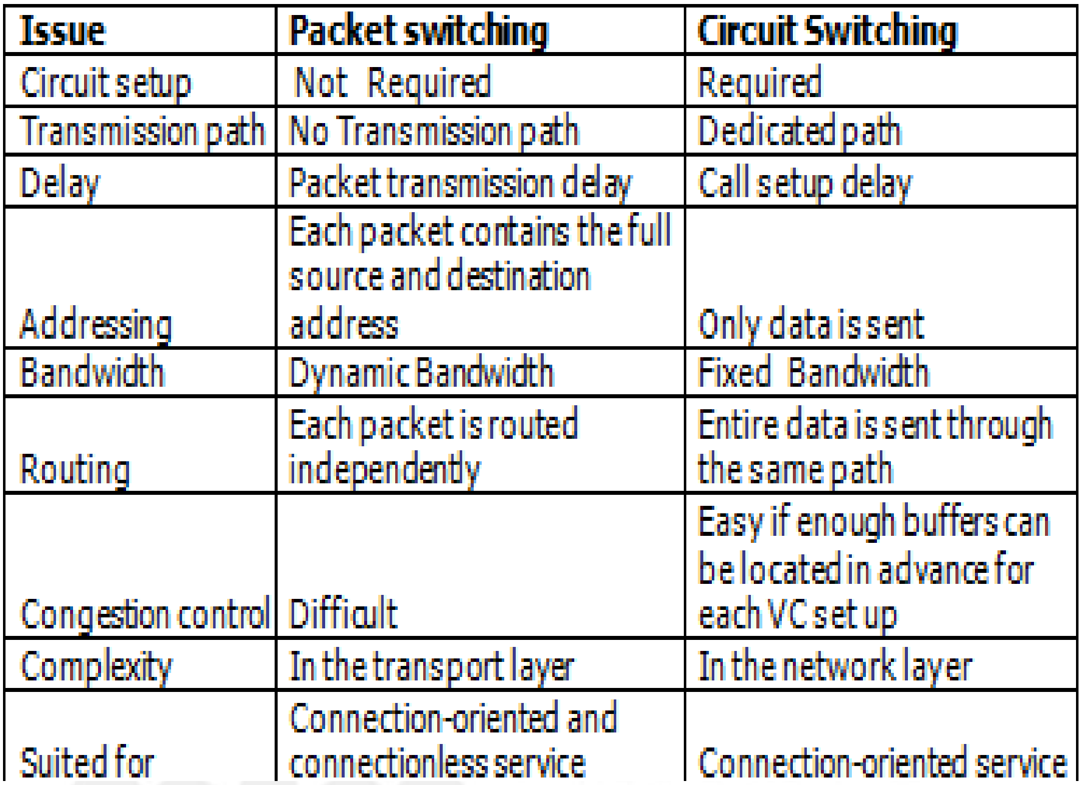
35. What is the role of VCI? (May/June 2011) (K1,CO2)

- A Virtual Circuit Identifier that uniquely identifies the connection at this switch, and which will be carried inside the header of the packets that belongs to this connection.

36. What is meant by switching? (May 2018) (K1,CO2)

- The mechanism for exchange of information between different computer networks and network segments is called switching in Networking. On the other words we can say that any type signal or data element directing or Switching toward a particular hardware address or hardware pieces.

37.List the difference between Packet Switching and Circuit Switching. (May 2017, Nov/Dec 2014, May/June 2014) (K1,CO2)



Issue	Packet switching	Circuit Switching
Circuit setup	Not Required	Required
Transmission path	No Transmission path	Dedicated path
Delay	Packet transmission delay	Call setup delay
Addressing	Each packet contains the full source and destination address	Only data is sent
Bandwidth	Dynamic Bandwidth	Fixed Bandwidth
Routing	Each packet is routed independently	Entire data is sent through the same path
Congestion control	Difficult	Easy if enough buffers can be located in advance for each VC set up
Complexity	In the transport layer	In the network layer
Suited for	Connection-oriented and connectionless service	Connection-oriented service

QUESTION BANK

PART – B and PART – C

1.Explain different types of Network in detail with neat diagram. (K5,CO1)

2.Explain the various network topologies in detail. (K5,CO1)

3.Discuss in detail about Internet Architecture (TCP/IP Protocol Suite). (May 2017, May/June 2015, May/June 2011) (K2,CO1)

(i) Explain the general concept of encapsulation and decapsulation. (K5,CO1)

(ii) Write short notes on multiplexing and demultiplexing. (K1,CO1)

4. Discuss in detail about the layers in OSI model. (Nov 10,11,12,15,16)(May 2018) (K2,CO1)

5.Explain the various performance metrics in detail. (Nov/Dec 2016) (K5,CO1)

6.Explain Transmission media and its types in detail. (K5,CO1)

7.Explain Datagram Networks or packet switched networks in detail (K5,CO1)

8.Explain Circuit Switching in detail. (K5,CO1)

9. How packet switching works in computer networks? Compare circuit switch and packet switching. (K5,CO1)

10. Consider all links in the network use TDM with 24 slots and have a data rate of 1.536 Mbps. Assume that host A takes 500 ms to establish an end to end circuit with host B before begin to transmit the file. If the file is 512 kilobytes, then how much time will it take to send the file from host A to host B? (K5,CO1)

11.Consider the network having bandwidth of 1 MBps and message of size 1000 bytes has to be sent. Each packet contains a header of 100 bytes if packet switching technique is used. Out of the following, in how many packets the message must be divided so that total time taken is minimum- 1 packet 5 packets 10 packets 20 packets (K5,CO1)

SUPPORTIVE ONLINE COURSES

S No	Course provider	Course title	Link
1	Udemy	Introduction to Networking for Complete Beginners	https://www.udemy.com/course/introduction-to-networking-for-complete-beginners/
2	Coursera	Fundamentals of Network Communication	https://www.coursera.org/learn/fundamentals-network-communications/
3	Coursera	Peer-to-Peer Protocols and Local Area Networks	https://www.coursera.org/learn/peer-to-peer-protocols-local-area-networks/
4	Coursera	Packet Switching Networks and Algorithms	https://www.coursera.org/learn/packet-switching-networks-algorithms
5	Coursera	TCP/IP and Advanced Topics	https://www.coursera.org/learn/tcp-ip-advanced
6	edX	Computer Networks and the Internet	https://www.edx.org/course/computer-networks-and-the-internet

REAL TIME APPLICATIONS IN DAY TO DAY LIFE AND TO INDUSTRY

1.Examine the different networking technologies and applications that you are using during this covid lockdown? In what ways it supports you. (K4, CO1)

2.Explore the networking resources available at your home and at your college? (K3,CO2)

3.Summarize the role of system administrator for both the cases. (K2,CO2)

COVID-19 - How Tech is Helping

https://www.youtube.com/watch?v=KEG_sQrXtzE

Ethics and digital technologies in times of COVID-19 pandemic

https://www.youtube.com/watch?v=LhzF-Y8xXBc

Contents beyond the Syllabus

Evolution of the Telephone

Reference Video – Content Beyond Syllabus

https://www.youtube.com/watch?v=BiYRaxKPnFY&feature=youtu.be

Assessment Schedule

- **Tentative schedule for the Assessment During 2022-2023 odd semester**

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	IAT 1	16.09.2022	22.09.2022	UNIT 1 & 2
2	IAT 2	02.11.2022	08.11.2022	UNIT 3 & 4
3	REVISION	26.11.2022	29.11.2022	UNIT 5 , 1 & 2
4	MODEL	01.12.2022	10.12.2022	ALL 5 UNITS

Prescribed Text Books & Reference Books

TEXT BOOK

Data Communications and Networking, Behrouz A. Forouzan, McGraw Hill Education, 5th Ed., 2017.

REFERENCES

1. Computer Networking- A Top Down Approach, James F. Kurose, University of Massachusetts and Amherst Keith Ross, 8th Edition, 2021.
2. Computer Networks, Andrew S. Tanenbaum, Sixth Edition, Pearson, 2021.
3. Data Communications and Computer Networks, P.C. Gupta, Prentice-Hall of India, 2006.
4. Computer Networks: A Systems Approach , L. L. Peterson and B. S. Davie, Morgan Kaufmann, 3rd ed., 2003.

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.