



CHAPTER-1

COMPUTER NETWORKS

1.1 Introduction to Computer Networks

Ex.Q.1 Define a computer network. Explain its importance and uses in daily life.

Computer Network

A computer network is a **group of computers** and other digital devices connected together. It allows them to communicate and share data, files, and other resources. Networks can be connected through cables or wireless technologies such as Wi-Fi.

Today, computer networks are an important part of daily life and are widely used in homes, schools, offices, banks, hospitals, and businesses.

A computer network can connect computers, mobile phones, printers, and many other digital devices. These devices communicate through cables or wireless technologies such as Wi-Fi. Networks allow files, data, and other resources to be shared between connected devices. Networks can be small, such as a home network, or very large, such as the Internet.

Example

In a school computer lab, all computers are connected through a network. Students can access the Internet, share files, and use a shared printer from any computer.

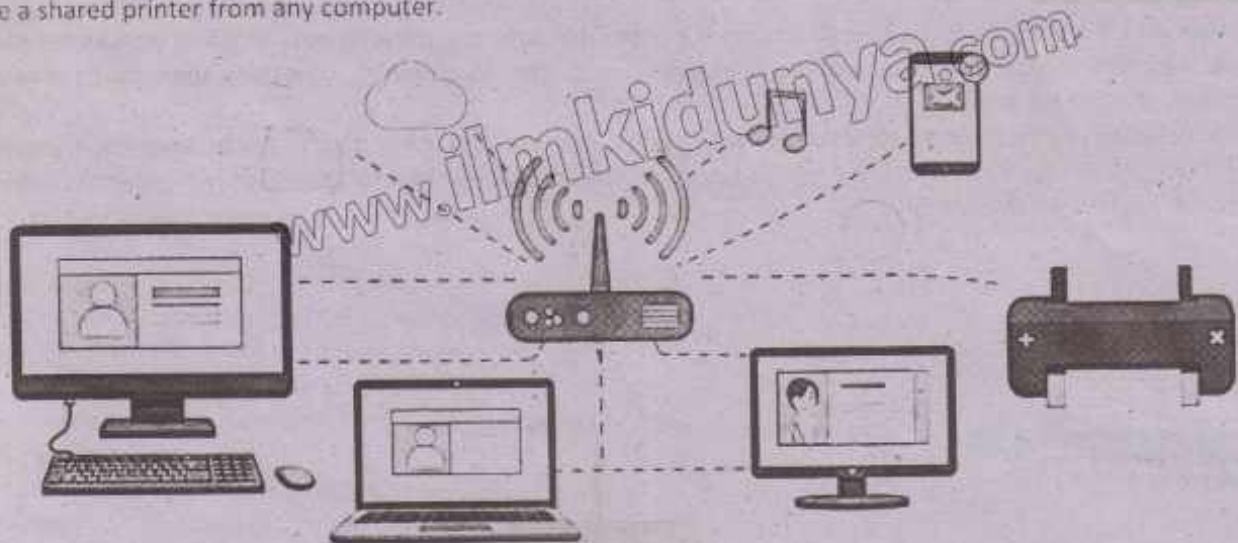


Figure 1.1: A computer network connects multiple devices to share data and resources.

Importance of Computer Networks

- Computer networks allow different devices to connect and communicate with each other.
- They help users to share information, data, and resources quickly and easily.
- Communication through a network saves both time and effort.
- They also make easy to access the Internet and use online services.

Short Question

Why computer networks are important?

Uses of Computer Network

i. Internet Browsing and Information Search

Computer networks allow users to browse the Internet, search for information, and watch online videos.

ii. Mobile Communication

Mobile phones use computer networks to make calls, send messages, and use different mobile applications.

iii. Education

Schools use computer networks for online classes and Learning Management Systems (LMS).

iv. Banking Services

Banks use computer networks for online banking, money transfers, and ATM services.

v. Social Media

Social media platforms work through computer networks, allowing people to communicate and share information.

vi. Smart Homes

Computer networks help control smart home devices such as lights, fans, cameras, and security systems.



TIDBIT

➤ Networks support online learning and remote work. Businesses rely on networks for daily operations.

1.2 Network Architecture and Basic Concepts

Ex.O.2 Explain network architecture and describe the main components of a computer network.

Network Architecture

Network architecture is the overall design of a computer network. It shows how different devices are connected and how they communicate with each other. It includes the hardware, software, communication media, and network protocols used in the network.

Network architecture also explains how computers, servers, printers, and other devices are arranged to share data and resources. A good network architecture provides fast communication, better performance, easy management, and allows the network to grow when needed.

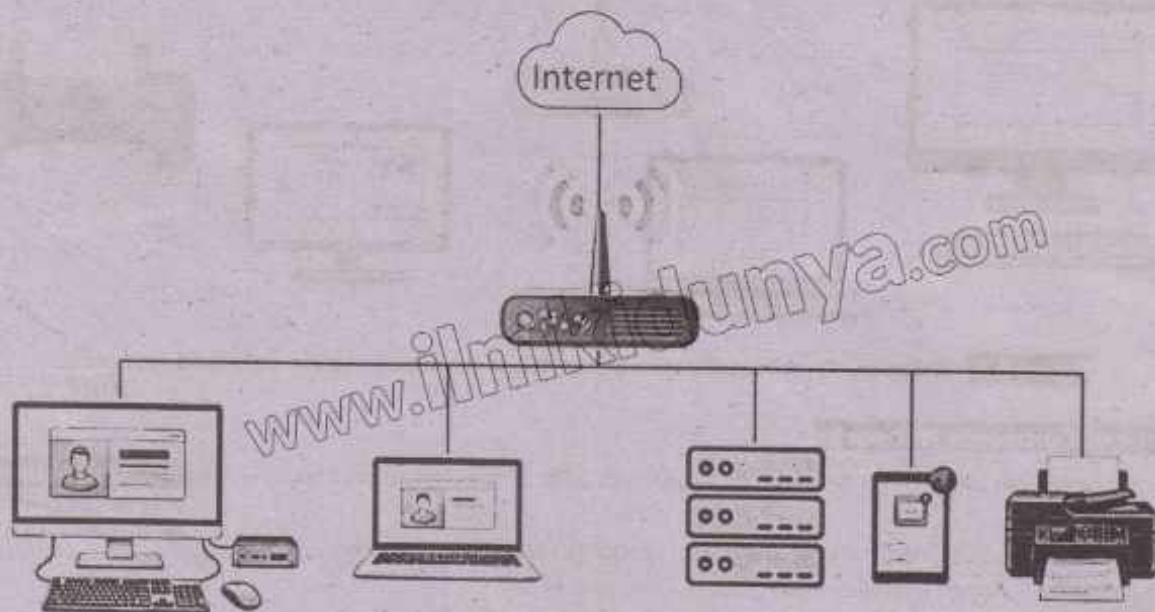


Figure 1.2: Network architecture shows how devices and components are organized in a network

Main Components of a Computer Network

The main components of a computer network are:

1. Devices (Nodes)

Devices are the main parts of a network that send and receive data. These devices are also called nodes. Examples include computers, laptops, mobile phones, printers, and servers. Each device uses the network to communicate with other connected devices and share information and resources.

2. Transmission Media

Transmission media is the **communication path** through which data travels from one device to another. It connects different devices in a network. Transmission media can be **wired** or **wireless**. Wired media includes twisted pair cable, coaxial cable, and fiber optic cable. Wireless media includes Wi-Fi and Bluetooth.

3. Networking Devices

Networking devices are used to **connect different devices** and control the movement of data in a network. They help in sending data to the correct destination. Common networking devices include switches, routers, hubs, modems, wireless access points, and Network Interface Cards (NIC).

4. Network Protocols

Network protocols are a **set of rules** that allow devices to communicate with each other. They define how data is prepared, transmitted, received, and managed over a network. Protocols ensure that different devices can communicate successfully.

Examples: TCP/IP, HTTP, FTP, and SMTP.

Ex.Q.5 Explain the types of computer networks. Describe LAN, WAN, and the Internet.

1.3 Types of Computer Networks

Computer networks are divided into different types based on their size and coverage area. Different types of computer networks are used for different purposes. Each type connects devices in a specific way. The most common types are Local Area Network (LAN), Wide Area Network (WAN), and the Internet (Public WAN). Understanding these network types helps in selecting the right network for different needs.

1. Local Area Network (LAN)

A Local Area Network (LAN) is a network that connects devices within a **small area**. A LAN connects devices in places such as a home, school, office, or computer lab. It provides high data transfer speed. It is usually owned and managed by one organization. Ethernet and Wi-Fi are the most common technologies used in LANs. A LAN is cost-effective and easy to maintain.

Examples:

- In a **school**, all computers in Computer Lab can be connected to a LAN for sharing files and printers.
- In an **office**, a LAN allows employees to share resources like printers and project files.

2. Wide Area Network (WAN)

A Wide Area Network (WAN) is a network that connects devices over a **large geographic area**.

A WAN connects networks located in different cities, countries, or even continents. It uses leased lines, satellites, or the Internet to transfer data. The data transfer speed is usually slower than a LAN. A WAN is more expensive to install and manage because it covers large distances. The Internet is the largest example of a WAN.

Examples

- A bank connects all of its branches in different cities through a WAN.
- A company with offices in different countries

3. The Internet (Public WAN)

The Internet is a global network that connects millions of devices **around the world**. The Internet allows people to share information worldwide. It provides services such as email, websites, and cloud storage. It uses standard communication protocols to connect devices. The Internet supports education, business, communication, entertainment, and many other daily activities. Today, it plays an important role in everyday life.

Short Question

What is a Wide Area Network (WAN)?

Short Question

What is a public WAN (Internet)?

Example:

- Internet
- A home broadband connection provided by PTCL or Nayatel

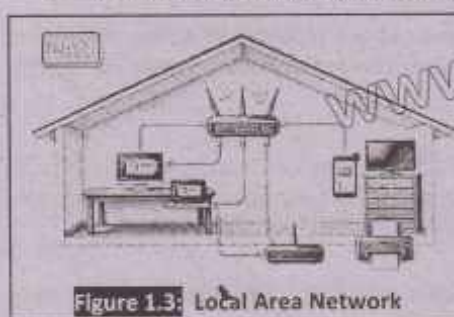


Figure 1.3: Local Area Network



Figure 1.4: Wide Area Network

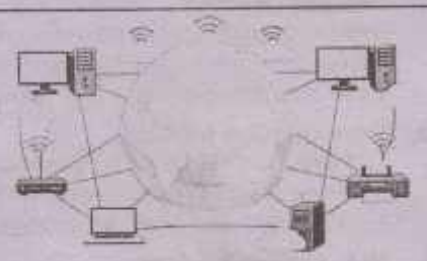


Figure 1.5: Internet

4. Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) connects computers across a **city** or **large campus**. It is larger than a LAN but smaller than a WAN. It uses fiber optic cables or microwave transmission.

Example:

- Network of cable TV in a city
- Campuses of a college in a city

5. Personal Area Network (PAN)

A Personal Area Network (PAN) connects devices over a very short distance around one person. It is the **smallest type of network**. It commonly uses **Bluetooth, USB, or Wi-Fi** to connect personal devices.

Example:

- Mobile phone connected to wireless earbuds using Bluetooth
- Mobile phone connected to a laptop using a Wi-Fi hotspot



CLASS ACTIVITY

Students list services that use the Internet. Discuss its importance.

Sol:

Services That Use the Internet	Importance of the Internet
<ul style="list-style-type: none"> ➤ Email ➤ Web browsing ➤ Social media (Facebook, Instagram, X) ➤ Video calling (Zoom, Google Meet) ➤ Online learning ➤ Online banking ➤ Online shopping ➤ Cloud storage (Google Drive, OneDrive) ➤ Video streaming (YouTube, Netflix) ➤ Online gaming 	<ul style="list-style-type: none"> ➤ It helps people communicate quickly. ➤ It provides easy access to information. ➤ It supports online education and learning. ➤ It allows online shopping and banking. ➤ It helps businesses connect with customers. ➤ It provides entertainment through videos, music, and games.

It enables people to work from home and share files easily.



TIDBIT

- **DSL (Digital Subscriber Line):** Internet through telephone lines; allows calling and browsing at the same time.
- **ISP (Internet Service Provider):** Company that provides Internet access to users.



Additional Multiple Choice Questions

- A group of connected computers and digital devices is called:
(a) database (b) computer network (c) operating system (d) software
- Which technology is commonly used in a wireless network?
(a) Bluetooth (b) Ethernet (c) Fiber optic (d) Coaxial cable
- Which of the following is the main purpose of a computer network?
(a) Edit videos (b) Create software (c) Share resources (d) Design graphics
- The overall design of a computer network is called:
(a) Network protocol (b) Network software (c) Network architecture (d) Transmission media
- Devices that send and receive data in a network are called:
(a) Routers (b) Nodes (c) Protocols (d) Modems
- Which component provides the communication path for data transmission?
(a) Network software (b) Networking device (c) Network protocol (d) Transmission media
- Which protocol is mainly used to transfer web pages on the Internet?
(a) HTTP (b) FTP (c) SMTP (d) TCP/IP
- A network that connects devices within a small area is called:
(a) WAN (b) Internet (c) LAN (d) MAN
- Which type of network connects different cities and countries?
(a) LAN (b) PAN (c) CAN (d) WAN
- The largest example of a Wide Area Network (WAN) is:
(a) School LAN (b) Home network (c) Internet (d) Bluetooth

Answers:

1 B 2 A 3 C 4 C 5 B 6 D 7 A 8 C 9 D 10 C

1.4 Networking Devices

Ex.0.6 Describe the main networking devices used in a computer network and explain their functions.

Networking Devices

Networking devices are hardware devices that connect computers and other devices in a network. They control the flow of data. Each networking device performs a specific function. Networking devices help computers and other digital devices to communicate with each other. These devices make communication faster, more reliable, and more efficient.

1. Network Interface Card (NIC)

A Network Interface Card (NIC) is a device that allows a device to connect to a network.

It can be wired or wireless. Every NIC has a unique address called a **MAC address**. It sends data to the network and receives data from the network. A device cannot communicate on a network without a NIC. Most modern computers and laptops have a built-in NIC.

Short Question

Describe purpose of network interface card (NIC)?

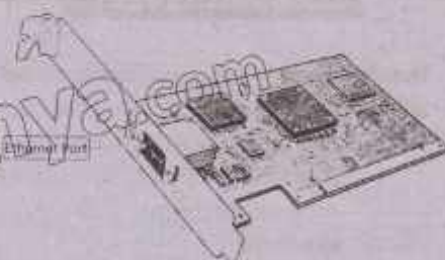


Figure 1.6: Network Interface Card

2. Switch

A switch is a networking device that connects multiple devices. It sends data only to the correct destination device. This improves network speed and efficiency. A switch connects computers, printers, and other devices in the same network. Switches are commonly used in schools, offices, and businesses networks.

Short Question

What is the purpose of a switch?

3. Router

A router is a networking device that **connects different networks**. It directs data packets to their correct destination. A router connects a local network to the Internet. It uses IP addresses to send data to the correct destination. It improves network security and helps manage network traffic. They are widely used in homes, schools, and offices networks.

4. Modem

A modem is a networking device that **connects a local network** to an Internet Service Provider (ISP). It converts digital data into signals that can travel through communication lines. It also converts incoming signals back into digital data. Modems are used with cable, DSL, or fiber Internet connections. Internet access depends on a modem. In many networks, the modem works together with a router.

Short Question

What is the purpose of a modem?



Modem

Router

Switch

5. Wireless Access Point

A Wireless Access Point is a networking device that provides Wi-Fi connectivity. It allows wireless devices to connect to a network. It extends the coverage of a wireless network. A Wireless Access Point allows laptops, smartphones, and tablets to connect to a network without cables.

Access points are commonly used in schools, universities, hospitals, offices, and large buildings. They improve Wi-Fi signal strength and provide stable wireless connectivity.

Short Question

What is the purpose of a wireless access point device?

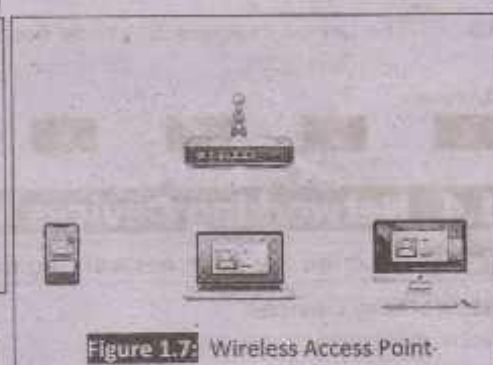


Figure 1.7: Wireless Access Point.



CLASS ACTIVITY

Teacher explains modem using signal conversion example. Students summarize.

Sol: A modem is a device that connects a computer or home network to the Internet. It converts digital signals from a computer into analog signals for transmission through communication lines. When data comes back from the Internet, the modem converts the analog signals back into digital signals so the computer can understand them.

Example:

A student opens a website on a laptop. The laptop sends digital data to the modem. The modem converts it into analog signals and sends it through the Internet connection.

When the website data returns, the modem changes the analog signals back into digital data, and the webpage appears on the laptop screen.

1.5 Network Topologies

Ex.Q.4 Define network topology. Explain bus, star, ring, mesh and tree topologies with advantages and disadvantages.

Network Topology

Network topology is the layout of a computer network. It shows how devices and cables are arranged in a network.

Network topology explains how computers and other devices are connected to each other. It can be physical or logical. The choice of topology affects the performance, reliability, and maintenance of the network.

Short Question

What is network topology?

i. Physical Topology

Physical topology shows the actual connections between devices and cables. It helps in network installation and maintenance.

ii. Logical Topology

Logical topology shows how data moves through the network. It does not show the actual cable connections. It helps us to understand how the network works.

Bus Topology

Bus topology is a network topology in which all devices are connected to a single main cable called **bus**. Data travels through the main cable to reach different devices. It is simple to install and has a low cost. If the main cable fails, the entire network stops working. It is suitable for small networks. It is not good for large networks.

A **terminator** is a small device used at both ends of the bus cable. It absorbs signals so they do not reflect back and interfere with data transmission.

Example

A small office connects all its computers using one main cable.

Short Question

What is bus topology?

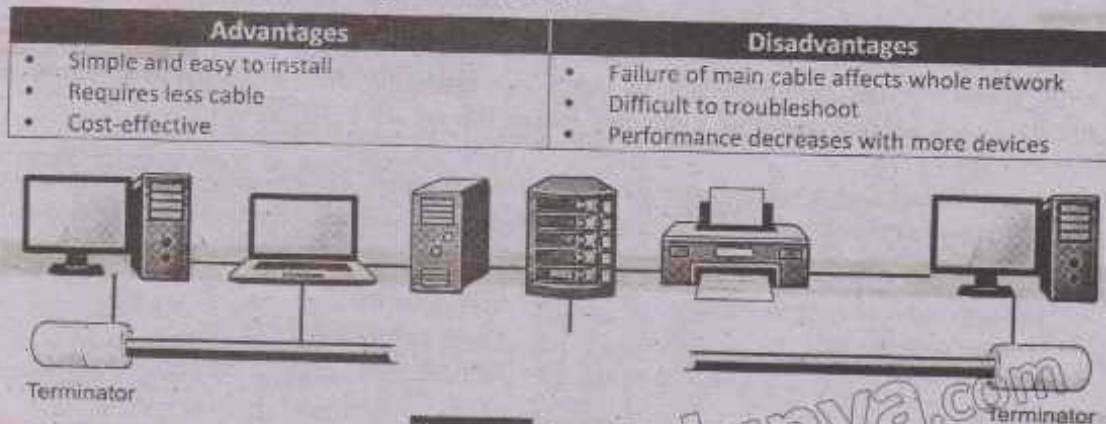


Figure 1.8: Bus Topology

Star Topology

Star topology is a network topology in which all devices are connected to a central hub or switch.

Data passes through the central hub or switch. It is easy to install, manage, and expand. If one device fails, the other devices continue to work normally. If the central hub or switch fails, the whole network stops working. It is widely used in modern networks.

Example: A school computer lab connects all computers to a central switch.

Short Question

What is star topology?

Advantages	Disadvantages
<ul style="list-style-type: none">• Easy to install and manage• Failure of one device does not affect others• Easy to detect faults	<ul style="list-style-type: none">• Central device failure stops entire network• Requires more cable• Higher cost

Ring Topology

Ring topology is a network topology in which devices are connected in a circular path. Data moves in one direction around the ring. Each device receives the data and passes it to the next device. If one device fails, the entire network may be affected. It is more complex than bus topology. It is rarely used today.

Example:

A metro railway communication system uses a ring topology so data can travel between stations in a circular path.

Short Question
What is ring topology?

Advantages	Disadvantages
<ul style="list-style-type: none">• Data flows in an organized manner• No data collision• Equal access for all devices	<ul style="list-style-type: none">• Failure of one device affects whole network• Difficult to add/remove devices• Rarely used today

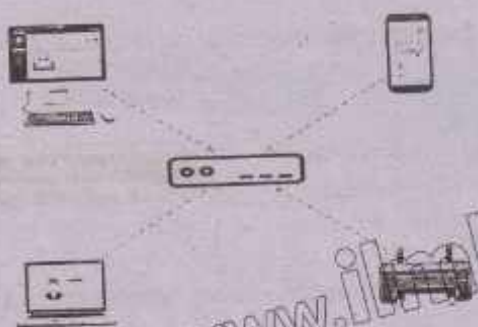


Figure 1.9: Star Topology

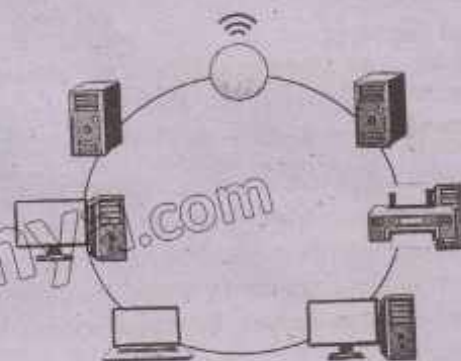


Figure 1.10: Ring Topology

Mesh Topology

Mesh-topology is a network topology in which each device is connected to many other devices. Data can travel through multiple paths to reach its destination. If one connection fails, data uses another available path. This makes the network highly reliable and fault tolerant.

It is expensive and complex because it requires many connections. It is mainly used in large and critical networks.

Example: Banks and military networks use mesh topology to ensure communication continues even if one connection fails.

Short Question
What is mesh topology?

Advantages	Disadvantages
<ul style="list-style-type: none">• Highly reliable and fault-tolerant• Multiple paths for data• High security	<ul style="list-style-type: none">• Very expensive• Complex installation• Requires large number of cables

Tree Topology

Tree topology is a network topology in which devices are arranged in a hierarchical structure like a tree.

It combines the features of both bus and star topologies. Multiple star networks are connected to a central backbone. Data flows from the root (main node) to branches and sub-branches. It is easy to expand and manage large networks. If backbone fails, the entire network may be affected. It is commonly used in large organizations.

Example

A university network connects different departments through a central backbone network.

Short Question
What is tree topology?

Advantages	Disadvantages
<ul style="list-style-type: none">• Easy to expand• Suitable for large networks• Hierarchical management	<ul style="list-style-type: none">• Backbone failure affects whole network• Complex setup• More cabling required

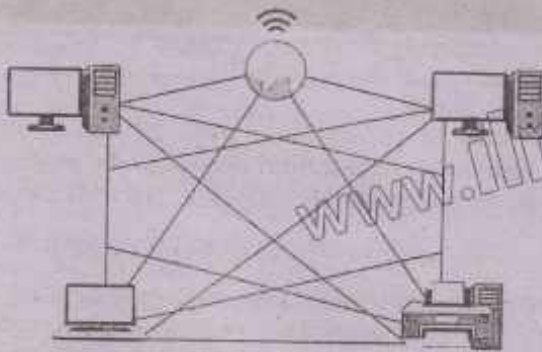


Figure 1.11: Mesh Topology

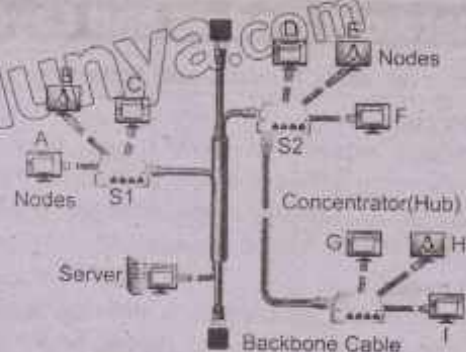


Figure 1.12: Tree Topology



Additional Multiple Choice Questions

- A hardware device that allows a computer to connect to a network is called:
(a) Router (b) Modem (c) Network Interface Card (d) Switch
- Every Network Interface Card (NIC) has a unique:
(a) IP address (b) MAC address (c) URL address (d) Email address
- Which networking device sends data only to the correct destination device?
(a) Modem (b) Router (c) Access Point (d) Switch
- A networking device that connects different networks is called:
(a) Hub (b) Switch (c) Router (d) NIC
- Which networking device connects a local network to an Internet Service Provider (ISP)?
(a) Switch (b) Modem (c) Router (d) NIC
- A device that provides Wi-Fi connectivity is called:
(a) Modem (b) Switch (c) Wireless Access Point (d) Router
- Physical layout of network is known as:
(A) Topology (B) Session (C) Link (D) Style
- In which topology are all devices connected to a single main cable?
(a) Ring topology (b) Star topology (c) Mesh topology (d) Bus topology
- Which topology connects all devices to a central hub or switch?
(a) Bus topology (b) Tree topology (c) Star topology (d) Ring topology
- A network topology in which devices are arranged in a hierarchical structure is called:
(a) Ring topology (b) Mesh topology (c) Bus topology (d) Tree topology
- The topology used for a small number of computers is called:
(A) Star (B) Bus (C) Mesh (D) Ring
- Terminators are used in topology.
(A) Bus (B) Star (C) Ring (D) Mesh
- Which is most complicated topology:
(A) Ring (B) Star (C) Tree (D) Mesh
- Every device has exactly two neighbors in:
(A) Bus (B) Tree (C) Star (D) Ring
- Which type of topology is known for its high redundancy and reliability?
(a) Bus Topology (b) Star Topology (c) Mesh Topology (d) Ring Topology
- What is the main disadvantage of Ring Topology?
(a) Limited bandwidth (b) High cost (c) Complex installation (d) Prone to failure

Answers:

1	C	2	B	3	D	4	C	5	B	6	C	7	A	8	D	9	C	10	D
11	B	12	A	13	D	14	D	15	C	16	D								

1.6 Network Models and Layers

Q. What are network models and network layers?

Network Models

Network models explain how data travels from one device to another in an organized way. They divide network communication into different layers. Each layer performs a specific task during data transmission. Layered models make networks easier to understand and manage. It also helps in finding and fixing network problems. Network models are used as standards in computer networking.

Network Layers

Network layers divide the communication process into smaller parts. Each layer has its own responsibility. Data passes through these layers one by one before reaching the destination. This structure makes network design simple and organized. A change in one layer does not affect the other layers. Layered communication improves reliability and better control.

Ex.O.3 What is the OSI model? Explain its layers and their functions.

OSI Model (Open Systems Interconnection)

The OSI Model stands for **Open Systems Interconnection**. It is a standard model used to understand network communication. The OSI Model has **seven layers**. Each layer performs a different function. The OSI Model is widely used for learning, designing, and troubleshooting computer networks. It helps different computer systems to communicate with each other properly.

Functions of OSI Model Layers

Each OSI layer has a specific role in data communication. The lower layers handle the physical transfer of data. The middle layers manage routing and reliable delivery. The upper layers provide services to users and applications. All layers work independently, but together they ensure successful communication.

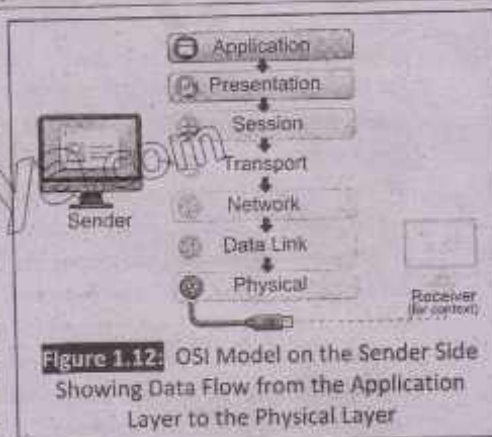


Figure 1.12: OSI Model on the Sender Side Showing Data Flow from the Application Layer to the Physical Layer

1. Physical Layer

The Physical Layer **sends raw data** as electrical, optical, or radio signals through the transmission medium. It defines hardware components such as cables, connectors, voltage levels, and data transmission speed.

Example: Cables, hubs, and repeaters work at this layer to carry the data across a network.

2. Data Link Layer

The Data Link Layer provides **error-free communication** between directly connected devices. It creates data frames, detects errors, and controls access to the shared communication medium.

Example: A switch works at this layer to send data to the correct device on a local network.

3. Network Layer

The Network Layer is responsible for **routing data** from the source device to the destination device across different networks. It uses **IP addresses** and selects the best path for data transmission.

Example: A router works at this layer to send data from one network to another, such as when you browse the internet.

4. Transport Layer

The Transport Layer ensures **reliable and correct delivery** of data. It divides data into smaller parts. It controls the flow of data. It recovers lost or damaged data when needed.

Example: When you download a file, this layer ensures that all parts of the file arrive in the correct order.

5. Session Layer

The Session Layer **establishes, manages, and ends communication sessions** between applications. It also supports recovery if communication is interrupted.

Example: During a video call, the Session Layer keeps the connection open and ensures both devices stay synchronized.

Short Question

Describe function of physical layer of OSI model?

Short Question

Describe function of network layer of OSI model?

6. Presentation Layer

The Presentation Layer converts data into a format that applications can understand. It also performs **encryption, compression, and data format conversion**.

Example: If you send an image, this layer ensures that the receiving computer can display it correctly.

Short Question

Describe function of presentation layer of OSI model?

7. Application Layer

The Application Layer provides **network services** directly to users and application software. It supports communication protocols such as HTTP, FTP, and email services.

Example: When you send an email, the Application Layer helps to create and send the message.

Short Question

Describe function of application layer of OSI model?

1.7 Network Protocols and Services

Ex.Q.7. What are network protocols? Explain TCP/IP, HTTP, FTP, and DNS.

Network Protocols

A network protocol is a set of rules that controls communication between devices in a network. It defines how data is formatted, transmitted, and received. All devices must follow the same protocol for successful communication. It also controls error handling and data delivery. All devices in a network must follow the same protocol. This ensures smooth and correct data exchange. Common examples of network protocols are TCP/IP and HTTP.

1. Transmission Control Protocol and Internet Protocol (TCP/IP)

TCP/IP stands for Transmission Control Protocol and Internet Protocol. It is the main protocol used on the Internet. TCP ensures that data is delivered correctly and reliably. IP is responsible for addressing and routing data from the source to the destination. Together, TCP/IP allows communication between devices. It is used in almost all computer networks.

Short Question

What is TCP/IP protocol?

2. Hypertext Transfer Protocol (HTTP)

HTTP stands for Hypertext Transfer Protocol. It is used to **transfer web pages** between a web browser and a web server. It allows users to open and view websites. HTTP does not encrypt data.

HTTPS is the secure version of HTTP. It uses encryption to protect data sent between a web browser and a web server. This protection is provided by **SSL/TLS** protocols. It keeps passwords, personal information, and payment details safe from attackers.

Short Question

Describe purpose of HTTP protocol?

3. File Transfer Protocol (FTP)

FTP stands for File Transfer Protocol. It is used to **upload and download files** between computers. It allows easy file sharing over a network. FTP is commonly used by web developers to manage website files. It can transfer large files. Secure versions of FTP are also available.

4. Domain Name System (DNS)

DNS stands for Domain Name System. It converts **website names into IP addresses**. This makes websites easy to access because users do not need to remember numbers. DNS servers perform this conversion. DNS is an important part of Internet communication.

Example

When you type **www.google.com** in a web browser, **DNS** converts the website name into an IP address. The browser uses **HTTP** or **HTTPS** to request the webpage. The data is delivered through **TCP/IP**, and if you upload website files to a server, **FTP** is used.

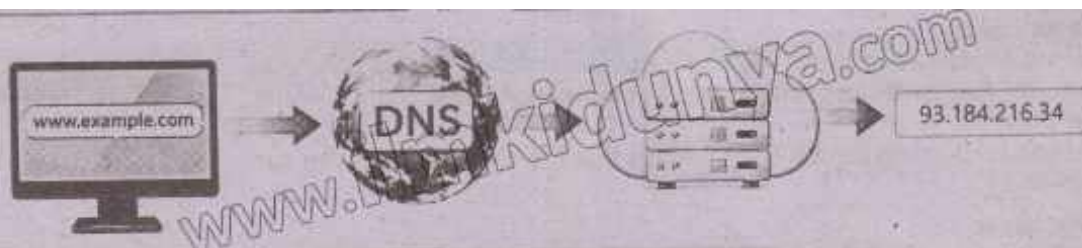


Figure 1.14: DNS Name Resolution Process

1.8 IP Addressing and Subnetting

Ex.Q8: Explain IP addressing. Describe IPv4, IPv6, the default gateway, and subnetting.

IP Addressing

An IP address is a unique number assigned to a device on a network. IP stands for Internet Protocol. It helps identify each device. Data uses IP addresses to find the correct destination. Every network device must have an IP address. Communication between devices is not possible without it. IPv4 and IPv6 are two versions of Internet Protocol addressing.

Short Question

What is IP address?

IPv4

IPv4 is the older version. IPv4 uses **32-bit numeric addresses**. It contains four numbers separated by dots. Each number is between 0 and 255. Each number is equal to 1 byte or 8 bits. The total size of an IPv4 address is 32 bits.

Short Question

What is IPv4 address? Give example

Example: 192.168.1.10

In an IPv4 address, the first part identifies the network, and the last part identifies the device on that network.

Network part: 192.168.1 – Identifies the network.

Host part: 10 – Identifies the specific device on the network.

IPv4 supports about **4.29 billion** unique addresses.

Breakdown of IPv4

Part	Value	What it means
Network part	192.168.1	Identifies your local network, like "Gulshan Block Street 3"
Host part	10	Identifies your specific device on that network, like "House #10"

IPv6

IPv6 is the newer version. IPv6 uses **128-bit addresses**. It contains eight groups of four hexadecimal digits separated by colons. Each group contains 16 bits. The total size of an IPv6 address is 128 bits. IPv6 provides a very large number of addresses for modern Internet use. IPv6 provides about 3.4×10^{38} unique addresses. This address space is so large that it is not expected to run out.

Short Question

What is IPv6 address?

Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

An IPv6 address has three main parts.

Global routing prefix: 2001:0db8:85a3 – Identifies the ISP or region.

Subnet ID: 0000 – Identifies the local network.

Interface ID: 0000:8a2e:0370:7334 – Identifies the specific device.

Breakdown of IPv6

Part	Value	What it means
Global routing prefix	2001:0db8:85a3	ISP/region, like "Pakistan, Sindh, Karachi"
Subnet ID	0000	Your local network inside the ISP, like "Gulshan area"
Interface ID	0000:8a2e:0370:7334	Your specific device, like "Your laptop"

Subnetting

Subnetting is the process of dividing a large network into smaller networks. Each part is called a subnet. It reduces network traffic and improves network performance. It also increases security and makes large networks easier to manage.

Network Address Translation (NAT)

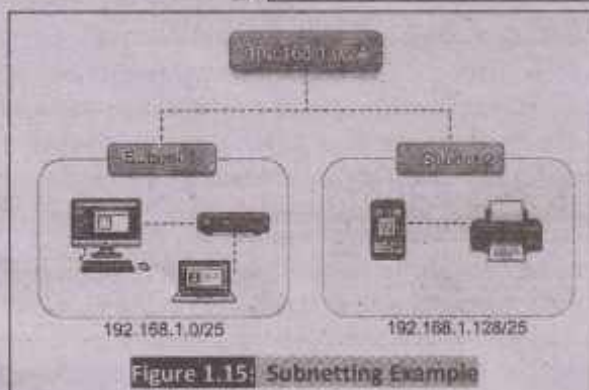
NAT stands for Network Address Translation. It allows many devices to share one public IP address. NAT is performed by routers. It hides private IP addresses from the Internet. This improves network security. NAT is commonly used in homes, schools, and offices.

Example

In a home network, all computers and mobile phones have their own private IP addresses. The router uses NAT to allow all of them to access the Internet through one public IP address.

Short Question

What is subnetting in computer networks?



Default Gateway

A default gateway connects a local network to other networks. It is usually a router. Data that is sent outside the local network passes through the default gateway. The gateway forwards the data to the correct destination. Internet access depends on the correct gateway settings.

Short Question

What is default gateway?



Additional Multiple Choice Questions

- A standard model used to understand network communication is called:
(a) OSI Model (b) FTP (c) DNS (d) IPv4
- Which OSI layer sends raw data as electrical, optical, or radio signals?
(a) Session Layer (b) Physical Layer (c) Network Layer (d) Application Layer
- A switch mainly works at which OSI layer?
(a) Physical Layer (b) Network Layer (c) Data Link Layer (d) Transport Layer
- Which OSI layer is responsible for routing data between networks?
(a) Network Layer (b) Session Layer (c) Presentation Layer (d) Data Link Layer
- The OSI layer that ensures reliable delivery of data is called:
(a) Application Layer (b) Physical Layer (c) Session Layer (d) Transport Layer
- A set of rules that controls communication between devices is called:
(a) IP address (b) Network protocol (c) Subnetting (d) Gateway
- Which protocol is mainly used to transfer web pages?
(a) FTP (b) DNS (c) HTTP (d) TCP/IP
- Which protocol converts website names into IP addresses?
(a) HTTP (b) FTP (c) TCP/IP (d) DNS
- An IP address is a unique number assigned to a:
(a) Website (b) Device (c) Browser (d) Protocol
- The process of dividing a large network into smaller networks is called:
(a) Routing (b) NAT (c) Subnetting (d) Encryption

Answers:

1	A	2	B	3	C	4	A	5	D	6	B	7	C	8	D	9	B	10	C
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	---

1.9 Home Network Setup and Configuration

Q. Explain Home Network Setup and Configuration. Also describe its components, wired network connections, and wireless network connections.

Home Network Setup and Configuration

A home network is a network that connects different devices in a house. It helps computers, laptops, mobile phones, printers, and other devices to communicate with each other. All devices can share the same internet connection. A router is the main device in a home network. Proper network setup makes data sharing easy and fast. Good network configuration also improves network speed and security.

Components of a Home Network

A home network has several important components.

- A router connects all the devices in the network.
- A modem connects the home network to the Internet Service Provider (ISP).
- Computers, laptops, mobile phones, and printers are the devices connected to the network.
- Network cables are used for wired connections. Wi-Fi is used for wireless connections.

Short Question

Describe components of home network?

Wired Network Connections

A wired network uses cables to connect devices. Ethernet cables are commonly used for this purpose. Devices are connected directly to a router or a switch. Wired networks provide high speed and stable performance. They are more secure than wireless networks. However, devices cannot move freely because they are connected with cables.

Wireless Network Connections

A wireless network connects devices without using cables. It uses radio signals to send and receive data. Wi-Fi is the most common wireless technology used in homes. It allows devices to move freely within the network range. Wireless networks are easy to install and use. However, they may be slower than wired networks in some situations.

1.10 Wi-Fi Security and Router Configuration

Q. Explain Wi-Fi Security and Router Configuration. Also describe Router Web Interface, Wi-Fi Encryption, Default Gateway, and Guest Networks.

Wi-Fi Security

Wi-Fi security protects the network from unauthorized users. Secure Wi-Fi keeps data safe and private. Without security, anyone can connect to the network and use the internet. Hackers can steal personal information from an unsecured network. It also prevents slow internet speed caused by unwanted users. Strong security improves the overall performance of the network.

Short Question

What is Wi-Fi security?

Router Web Interface

Router Configuration:

The router web interface is used to manage router settings. It is opened through a web browser. The user enters the router's IP address to access it. A username and password are required to log in. The interface allows users to change the Wi-Fi name and password. It also provides options to manage network security settings.

Wi-Fi Encryption:

Wi-Fi encryption protects data sent over a wireless network. It converts data into a secure form so that others cannot read it. WPA2 and WPA3 are the most common security protocols. Older protocols such as WEP are not secure. Users should always choose the latest encryption method to protect their network.

Default Gateway:

A default gateway connects a local network to other networks. It is usually a router. Data that is sent outside the local network passes through the default gateway. The gateway forwards the data to the correct destination. Internet access depends on the correct gateway settings.

Guest Networks

A guest network allows visitors to use the internet without accessing the main home network. It is separate from the main network. Guest users cannot access personal devices or files. This improves network security and privacy. Guest networks also help control internet usage. They are useful in homes and offices.

Short Question

Describe purpose of guest networks?

CLASS ACTIVITY

Create sample strong password with length of eight alpha-numeric.

Sol: A strong 8-character alpha-numeric password contains both letters and numbers.

Examples of strong passwords:

1. Ab7kP92x
2. M4n8Tq21
3. Zx5R9b6L
4. P7w3N8a2

A strong password should:

- Have at least 8 characters.
- Include uppercase and lowercase letters.
- Include numbers.
- Include special characters
- Avoid using easy words like name or date of birth.

1.11 Network Diagnostic Tools and Commands

Q. Explain Network Diagnostic Tools and Commands. Also describe Ping, Ipconfig, Ifconfig, Telnet, PuTTY, and SSH.

Network Diagnostic Tools and Commands

Network diagnostic tools are used to find network problems. They check internet and network connections. These tools show whether devices can communicate with each other. Commands are entered in the Command Prompt or Terminal. They help identify slow or broken network connections.

Network Troubleshooting

Network troubleshooting is the process of finding and fixing network problems. It helps to detect connection and speed issues. It checks network cables, devices, and settings. Troubleshooting reduces network errors and downtime. It helps keep communication smooth and improves network performance.

Ping Command

The ping command is used to test network connectivity. It checks whether another device is reachable on the network. Ping sends small data packets to the destination device. It measures the response time. This command helps to detect network delays and is commonly used to check an internet connection.

Short Question

What is Network troubleshooting?

Short Question

When Ping command is used?

PING COMMAND

```
C:\> ping google.com
```

Sample Output:

```
Pinging google.com [142.250.190.14] with 32 bytes of data:
Reply from 142.250.190.14: bytes=32 time=25ms TTL=118
Reply from 142.250.190.14: bytes=32 time=24ms TTL=118
Reply from 142.250.190.14: bytes=32 time=26ms TTL=118
Reply from 142.250.190.14: bytes=32 time=25ms TTL=118
```

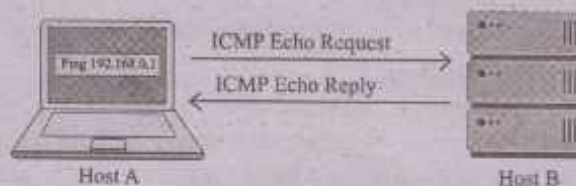


Figure 1.16: Ping Command

Ipconfig and Ifconfig Commands

- **Ipconfig** is used in the Windows operating system.
- **Ifconfig** is used in Linux and macOS.

These commands display network settings. They show the IP address, subnet mask, default gateway, and network status. They are useful for network troubleshooting.

Telnet, PuTTY, and Secure Shell (SSH)

- ❖ **Telnet** is used to access a remote device over a network. It sends data without encryption, so it is not secure.
- ❖ **PuTTY** is a popular program used for remote login to network devices.
- ❖ **SSH (Secure Shell)** is a secure method for remote access. It encrypts data during communication. This keeps the connection safe. These tools are commonly used to manage network devices.

Example

If the Internet is not working, you can use the **ping** command to check the connection. You can use **ipconfig** to view your computer's IP address. A network administrator can use **PuTTY** with **SSH** to securely access and manage a remote server.



CLASS ACTIVITY

Map packet paths between two locations.

Sol: To map packet paths between two locations, we can use the **tracert** (Trace Route) command. It shows the path that data packets follow from the source computer to the destination.

Example:

Command:

`tracert www.google.com`

Output:

Computer → Router → ISP Network → Google Server

The command displays each router (hop) that a packet passes through before reaching the final destination. It helps to identify the route and find network connection problems.

1.12 Network Performance

Q. What is Network Performance? Also describe Network Bandwidth, Network Latency, and the causes of Network Delay.

Network Performance

Network performance shows how well a network works. It measures the speed and quality of data transfer. Good network performance provides fast and smooth communication. Poor network performance causes slow Internet and delays. Network performance depends on different factors, such as bandwidth and latency.

Network Bandwidth

Network bandwidth is the amount of data that can be sent through a network in a given time. It shows the data carrying capacity of a network. Bandwidth is usually measured in Mbps (Megabits per second). Higher bandwidth allows faster data transfer. When many devices use the network at the same time, more bandwidth is needed. Low bandwidth can make the internet slow.

Short Question

What is Network bandwidth?

Network Latency

Network latency is the time taken by data to travel from one device to another. It is the delay between sending and receiving data. Latency is measured in milliseconds (ms). Low latency gives a faster response. High latency causes lag and delay. Online games and video calls require low latency for better performance.

Short Question

What is Network latency?

Causes of Network Delay

Network delay can happen for many reasons.

- Too many users on the network can reduce speed.
- Poor-quality cables can slow data transmission.
- A long distance between devices can increase delay.
- Network congestion can also reduce data speed.
- Hardware problems may also cause network delay.



CLASS ACTIVITY

Identify possible causes of Network delay in a given scenario.

A student is attending an online class, but the video keeps buffering and the audio is delayed.

Sol: Possible causes of network delay are:

- **Low bandwidth:** Too many users are sharing the same network, reducing available speed.
- **High network traffic:** A large amount of data is being transferred, causing delays.
- **Weak Wi-Fi signal:** The distance between the device and router can slow communication.
- **Hardware problems:** Faulty cables, routers, or network devices can increase delay.
- **Server delay:** The destination server may be slow or overloaded.

1.13 Network Load Balancing

Q. What is Network Load Balancing? Also describe its benefits and basic load balancing methods.

Network Load Balancing

Network load balancing is used to manage network traffic. It distributes work among multiple servers or network links. This prevents one server or device from becoming overloaded. Load balancing improves network speed and reliability. It is commonly used in large networks and data centers. It also helps networks handle a large number of users smoothly.

Benefits of Network Load Balancing

- Load balancing improves network speed and response time.
- It reduces the risk of server failure. If one server stops working, other servers continue providing services. This gives users a better experience.
- Load balancing also helps to manage heavy network traffic.
- It increases the reliability and availability of the network.

Short Question

Write down benefits of Network Load Balancing?

Basic Load Balancing Methods

There are different methods used for load balancing.

❖ Round Robin Method

Round Robin Method sends requests to servers one by one in order. This gives each server an equal share of the work.

❖ Least Connection Method

Least Connection Method sends new requests to the server that has the fewest active connections. This helps reduce the load on busy servers.

❖ IP Hash Method

IP Hash Method uses the IP address of the user to decide which server will handle the request. This helps distribute traffic among different servers.

These methods help to balance network traffic. They are simple and effective for improving network performance.



Additional Multiple Choice Questions

- A network that connects devices inside a house is called:
(a) Home network (b) WAN (c) MAN (d) PAN
- Which device is the main device in a home network?
(a) Modem (b) Switch (c) Router (d) NIC
- Which type of network uses Ethernet cables to connect devices?
(a) Wireless network (b) Wired network (c) Mesh network (d) Guest network
- The process of protecting a Wi-Fi network from unauthorized users is called:
(a) Network latency (b) Load balancing (c) Network troubleshooting (d) Wi-Fi security
- Which Wi-Fi encryption protocol is the most secure?
(a) WEP (b) WPA2 (c) WPA3 (d) FTP
- Which command is used to test network connectivity?
(a) SSH (b) Ping (c) Telnet (d) Ifconfig
- Which command is used in Windows to display network settings?
(a) Ping (b) SSH (c) PuTTY (d) Ipconfig
- The amount of data that can be sent through a network in a given time is called:
(a) Latency (b) Encryption (c) Bandwidth (d) Gateway
- The method that sends requests to servers one by one is called:
(a) IP Hash (b) Least Connection (c) Round Robin (d) Network Routing
- A separate network that allows visitors to use the Internet without accessing personal devices is called:
(a) Home network (b) Guest network (c) Local network (d) Private server

Answers:

1. a 2. c 3. b 4. d 5. c 6. b 7. d 8. c 9. c 10. b

1.14 Network Security

Q. What is Network Security? Also describe Firewalls, Encryption, Access Control, and common Network Security Threats.

Network Security

Network security is the protection of computer networks from unauthorized access. It keeps data safe from loss and damage. Many users connect to networks every day, so security is very important. Without proper security, networks become unsafe. Network security uses different tools and rules to protect data and devices. It is important for both homes and organizations. It protects personal and important information from hackers. It also protects devices from malware. Secure networks work smoothly without interruptions. Every network needs basic security measures.

1. Firewalls

A firewall is a security device or software. It controls incoming and outgoing network traffic. It blocks harmful or unwanted data from entering the network. A firewall acts as a barrier between trusted and untrusted networks. It protects computers from cyber-attacks. Firewalls are commonly used in homes and offices.

Short Question

Describe purpose of firewalls in networks?



Figure 1.17: Firewall Protection

2. Encryption

Encryption changes data into a secret form. Only authorized users can read the encrypted data. It protects data while it is being transferred over a network. Encryption is commonly used in emails and online banking. Strong encryption improves data security and helps prevent data theft.

3. Access Control

Access control decides who is allowed to use the network. It allows only authorized users to access network resources. Usernames and passwords are common methods of access control. Permissions decide what each user can do on the network. Access control protects important resources and helps manage network usage.

Common Network Security Threats

Network security faces many threats.

1. Malware

Malware is any harmful software designed to damage a computer, steal data, or disrupt normal operation.

2. Viruses

A virus is a harmful program that spreads from one file or computer to another. It can damage files and slow down the computer. A virus is one type of malware.

3. Hackers

Hackers try to access computers or networks without permission to steal or misuse information.

4. Phishing Attacks

Phishing attacks trick users into sharing sensitive information, such as passwords or bank details, through fake emails or websites.

5. Denial of Service (DoS) Attacks

A Denial of Service (DoS) attack makes a network or website unavailable by sending too many requests at the same time.

6. Security Tools

Security tools help protect computers and networks from threats.

Examples: Antivirus software, firewalls, and anti-malware programs.



CLASS ACTIVITY

Discuss how security protects sensitive data like CT scans of patients in a hospital.

Sol: Security protects patient CT scans by preventing unauthorized access and keeping medical information safe.

Ways security protects data:

- **Encryption:** It converts CT scan data into a secure format so unauthorized people cannot read it.
- **Access Control:** Only authorized doctors and staff can access patient records using passwords or authentication.
- **Backup:** Regular backups protect data from loss due to system failure or cyber-attacks.
- **Network Security:** Firewalls and security systems protect hospital networks from hackers and malware.
- **Privacy Protection:** Security ensures that patient information remains confidential and is only shared with authorized persons.

1.15 Data Backup and Recovery

Q. What is Data Backup and Recovery? Also describe the types of data backup and data recovery methods.

Data Backup and Data Recovery

Data backup is the process of making a copy of important data. It protects data from loss caused by viruses, hardware failure, or other problems. Backup makes it easy to restore lost data. It is the process of getting lost or damaged data back. Backup and recovery are important for keeping data safe. Every user should create backups regularly.

Types of Data Backup

There are different types of data backup.

- **Full Backup** saves all the data in one backup.
 - **Incremental Backup** saves only the data that has changed since the last backup.
 - **Differential Backup** saves all the changes made since the last full backup.
- Backups can be stored on hard drives or in cloud storage.

Short Question

List types of data backups?

Data Recovery Methods

Data recovery is used to restore lost or damaged data. Backup files can be used to recover data. Recovery software helps restore deleted files. System Restore can recover system data. Professionals can recover data from damaged storage devices. These methods help reduce data loss.

Example

A student saves important assignments in cloud storage and on an external hard drive. If the laptop stops working, the files can be restored from the backup.

1.16 Usability and Security Tradeoffs

Usability is the ease of using a system, while security protects the system and data from unauthorized access. A tradeoff means finding the right balance between these two.

Usability

Usability means how easy a system is to use. A usable system is simple and clear. Users can learn it quickly. They can complete tasks without confusion. Good usability saves time and effort. It also improves user satisfaction.

Short Question

What is usability?

Security

Security means protecting systems and data from unauthorized access. It protects against viruses, hackers, and other threats. Security keeps information private and safe. Strong security reduces risks and damage. Every system needs basic security measures.

Tradeoffs Between Usability and Security

Increasing security can make a system more difficult to use. For example, strong passwords are harder to remember, and extra login steps take more time. On the other hand, a system with very little security is easier to use but is less safe. Therefore, a balance between usability and security is necessary to keep a system both safe and easy to use.

Example

Online banking requires a password and a verification code before allowing access. These extra security steps take more time, but they protect the user's account and personal information.



Additional Multiple Choice Questions

1. The protection of computer networks from unauthorized access is called:
(a) Data backup (b) Network security (c) Load balancing (d) Network topology
2. A security device that controls incoming and outgoing network traffic is called:
(a) Antivirus (b) Firewall (c) Router (d) Switch
3. The process of changing data into a secret form is called:
(a) Encryption (b) Backup (c) Recovery (d) Compression
4. A method that allows only authorized users to use network resources is called:
(a) Malware (b) Firewall (c) Access control (d) Subnetting
5. Harmful software designed to damage a computer is called:
(a) Browser (b) Malware (c) Protocol (d) Gateway
6. Fake emails or websites used to steal personal information are called:
(a) Viruses (b) Phishing attacks (c) Firewalls (d) DoS attacks

7. The process of making a copy of important data is called:
 (a) Encryption (b) Data recovery (c) Data backup (d) Access control
8. Which type of backup saves only the data changed since the last backup?
 (a) Full backup (b) Differential backup (c) Cloud backup (d) Incremental backup
9. The ease of using a system is called:
 (a) Security (b) Reliability (c) Usability (d) Encryption
10. Finding the right balance between usability and security is called:
 (a) Data recovery (b) Tradeoff (c) Firewall (d) Authentication

Answers:

1	B	2	B	3	A	4	C	5	B	6	B	7	C	8	D	9	C	10	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	---

TEXTBOOK EXERCISE (SOLVED)



MULTIPLE CHOICE QUESTIONS

1. A computer network is:
 (a) A single computer system (b) A group of connected computers and devices
 (c) A software program (d) A storage device
2. The device used to connect a computer to a network is:
 (a) Monitor (b) Keyboard (c) Network Interface Card (NIC) (d) Printer
3. A network that covers a small geographical area, such as a school or office, is:
 (a) WAN (b) MAN (c) LAN (d) Internet
4. The topology that uses a central hub or switch is:
 (a) Bus Topology (b) Ring Topology (c) Star Topology (d) Mesh Topology
5. The OSI model contains:
 (a) Five layers (b) Six layers (c) Seven layers (d) Eight layers
6. The protocol mainly used to view web pages is:
 (a) FTP (b) DNS (c) TCP (d) HTTP
7. The main function of a router is to:
 (a) Store data (b) Connect devices within a network
 (c) Connect different networks (d) Display web pages
8. DNS is used to:
 (a) Transfer files (b) Protect data
 (c) Convert domain names into IP addresses (d) Connect hardware devices
9. The device that converts digital signals for Internet transmission is:
 (a) Switch (b) Hub (c) Modem (d) NIC
10. The topology that provides the highest reliability is:
 (a) Bus Topology (b) Ring Topology (c) Star Topology (d) Mesh Topology

Answers:

1	B	2	C	3	C	4	C	5	C	6	D	7	C	8	C	9	C	10	D
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	---



SHORT QUESTIONS

1. **What is a computer network?**

Ans: A computer network is a group of computers and other digital devices connected together. It allows them to communicate and share data, files, and other resources. Networks can be connected through cables or wireless technologies such as Wi-Fi.

2. **Write two uses of computer networks.**

Ans: **Internet Browsing and Information Search**

Computer networks allow users to browse the Internet, search for information, and watch online videos.

Mobile Communication

Mobile phones use computer networks to make calls, send messages, and use different mobile applications

3. **What is network architecture?**

Ans: Network architecture is the overall design of a computer network. It shows how different devices are connected and how they communicate with each other. It includes the hardware, software, communication media, and network protocols used in the network.

4. **Name any two components of a computer network.**

Ans: Components of a computer network are:

- i. **Networking Devices:** Networking devices connect different devices and manage the flow of data in the network.
- ii. **Network Protocols:** Network protocols are a set of rules that control communication between devices.

5. **What is the OSI model?**

Ans: The OSI Model stands for **Open Systems Interconnection**. It is a standard model used to understand network communication. The OSI Model has **seven layers**. Each layer performs a different function. It helps different computer systems to communicate with each other correctly.

6. **Write the name of any two network topologies.**

Ans: **Any two network topologies are:**

- i. Star Topology
- ii. Bus Topology

7. **What is a Local Area Network (LAN)?**

Ans: A Local Area Network (LAN) is a network that connects devices within a small area such as a home, school, office, or computer lab. It provides high-speed data transfer and is easy to maintain.

8. **What is the function of a router?**

Ans: A router is a networking device that connects different networks. It directs data packets to the correct destination using IP addresses. It also connects a local network to the Internet.

9. **What is a network protocol?**

Ans: A network protocol is a set of rules that controls communication between devices in a network. It defines how data is formatted, transmitted, and received. All devices must follow the same protocol for successful communication.

10. **What is the purpose of DNS?**

Ans: DNS stands for Domain Name System. It converts website names into IP addresses. This makes websites easy to access because users do not need to remember IP address numbers. DNS servers perform this conversion. DNS is an important part of Internet communication.



LONG QUESTIONS

All Questions are Solved in Chapter

1. Define a computer network. Explain its importance and uses in daily life.
2. Explain network architecture and describe the main components of a computer network.
3. What is the OSI model? Explain its layers and their functions.
4. Define network topology. Explain bus, star, ring, and mesh topologies with advantages and disadvantages.
5. Explain the types of computer networks: Describe LAN, WAN, and the Internet.
6. Describe the main networking devices used in a computer network and explain their functions.
7. What are network protocols? Explain TCP/IP, HTTP, FTP, and DNS.
8. Explain IP addressing. Describe IPv4, IPv6, the default gateway, and subnetting.

ADDITIONAL SHORT QUESTIONS

Introduction to Computer Networks, Network Architecture and Basic Concepts

1. What are the uses of a computer network?

Ans:

- Computer networks are used for Internet browsing and online learning.
- They help in mobile communication and banking services.
- They are also used for social media and smart homes.
- Networks support many daily activities.

2. Name the main components of a computer network.

Ans: The main components of a computer network are devices (nodes), transmission media, networking devices and network protocols. These components work together to provide communication. They help devices share data and resources. They make the network work properly.

3. What are nodes in a computer network?

Ans: Nodes are the devices connected to a computer network. They send and receive data. Examples of nodes are computers, laptops, printers, mobile phones, and servers. They communicate with other connected devices.

4. Name any four networking devices.

Ans: Four networking devices are switch, router, modem, and wireless access point. These devices connect computers and other network devices. They help control data communication. They make the network work efficiently.

5. What is transmission media?

Ans: Transmission media is the path through which data travels. It connects different devices in a network. It can be wired or wireless. Wi-Fi and cables are common examples of transmission media.

Types of Computer Networks

6. List types of computer networks?

Ans: The main types are Local Area Network (LAN), Wide Area Network (WAN), and the Internet.

7. Why is a WAN more expensive than a LAN?

Ans: A WAN covers a large geographical area. It connects networks over long distances. It requires more equipment and communication links. Therefore, it is more expensive to install and manage.

8. Differentiate between LAN and WAN

Ans:

Local Area Network (LAN)	Wide Area Network (WAN)
A LAN connects devices within a small area.	A WAN connects devices over a large geographical area.
A LAN provides high data transfer speed.	A WAN usually provides slower data transfer speed than a LAN.
A LAN is less expensive to install and manage.	A WAN is more expensive to install and manage.

Networking Devices

9. **Why is a Network Interface Card (NIC) necessary in a computer network?**

Ans: A Network Interface Card (NIC) allows a device to connect to a network. It sends and receives data. Every NIC has a unique MAC address. Without a NIC, a device cannot communicate on the network.

10. **Why is a router used in a computer network?**

Ans: A router connects different networks together. It directs data to the correct destination using IP addresses. It also connects a local network to the Internet. It helps manage network traffic.

11. **How does a Wireless Access Point help users?**

Ans: A Wireless Access Point provides Wi-Fi connectivity. It allows wireless devices to connect without cables. It also extends the wireless network coverage. It provides a stable Wi-Fi connection.

Network Topologies

12. **Differentiate between physical Topology and logical Topology**

Ans:

Physical Topology	Logical Topology
Physical topology shows the actual arrangement of devices and cables in a network.	Logical topology shows how data moves between devices in a network.
It focuses on hardware connections.	It focuses on the flow of data.
It helps in network installation and maintenance.	It helps in understanding how the network works.

13. **What is the main disadvantage of Bus topology?**

Ans: The main disadvantage of Bus topology is that failure of the backbone cable can stop the whole network. It is difficult to find faults. Network performance decreases when many devices are connected. It is not suitable for large networks.

14. **What is the use of a terminator in a bus topology?**

Ans: A terminator is a small device used at both ends of the bus cable. It absorbs signals so they do not reflect back and interfere with data transmission.

15. **What is the main advantage of Star topology?**

Ans: Star topology is easy to install and maintain. Failure of one cable does not affect other devices. It is easy to find network faults. It provides better network performance.

16. **Why is star topology widely used in modern networks? / Which topology is most commonly used in modern networks?**

Ans: Star topology is the most commonly used network topology. It is easy to install and manage. If one device fails, the other devices continue working. It is also easy to find faults. These features make it popular.

17. **Why is mesh topology considered highly reliable? / Which topology provides the highest reliability?**

Ans: Mesh topology has multiple paths for data transmission. If one connection fails, data can use another path. This keeps the network working. It provides the highest reliability. It is used in large and critical networks.

18. **Why is tree topology suitable for large organizations?**

Ans: Tree topology connects devices in a hierarchical structure. It is easy to expand when the network grows. It helps manage large networks efficiently. It is commonly used in universities and large organizations.

19. **How does a bus topology work?**

Ans: In a bus topology, all devices are connected to a single cable called the **bus**. When a device sends data, it travels along the cable. All devices receive the data, but only the destination device accepts it.

20. **How does a star topology work?**

Ans: In a star topology, all devices are connected to a **hub or switch**. When a device sends data, it first goes to the hub or switch. The hub or switch then forwards the data to the destination device.

21. **How does a ring topology work?**

Ans: In a ring topology, each device is connected to two other devices, forming a **ring**. Data travels from one device to the next around the ring until it reaches the destination device.

OSI Reference Model

22. List/Name the seven layers of the OSI Reference Model.

Ans: The seven layers are Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, and Application Layer.

23. What is the function of the Data Link Layer?

Ans: The Data Link Layer provides error-free communication between directly connected devices. It creates data frames, detects errors, and controls access to the shared communication medium.

24. What is the function of the Transport Layer?

Ans: The Transport Layer ensures reliable and correct delivery of data. It divides data into smaller parts. It controls the flow of data. It recovers lost or damaged data when needed.

TCP/IP Protocol Suite

25. Why are network protocols necessary?

Ans: Network protocols are rules for communication. They control how data is sent and received. They allow different devices to communicate successfully. They also ensure correct data exchange.

26. Why is TCP/IP important on the Internet?

Ans: TCP/IP is the main protocol used on the Internet. TCP ensures reliable delivery of data. IP sends data to the correct destination. Together, they allow communication between devices.

27. How does DNS (Domain Name System) function like a phonebook for the Internet?

Ans: DNS works like a phonebook because it converts website names (domain names) into IP addresses. It helps users access websites using easy names instead of remembering complex numerical IP addresses.

IP Addressing

28. What is the purpose of an IP address? / Why is an IP address important?

Ans: An IP address identifies each device on a network. It helps data reach the correct destination. It allows devices to communicate with each other. Without an IP address, network communication is not possible.

29. Name the two versions of IP addresses.

Ans: The two versions of IP addresses are IPv4 and IPv6. Both are used to identify devices on a network. IPv4 is the older version. IPv6 is the newer version with a larger address space.

30. Why does every network device need an IP address?

Ans: An IP address is a unique number assigned to a device. It helps identify each device on the network. Data uses IP addresses to reach the correct destination. Communication is not possible without an IP address.

31. Why was IPv6 introduced?

Ans: IPv6 was introduced because the Internet was running out of IPv4 addresses. IPv6 is the newer version of Internet Protocol. It provides a very large number of IP addresses. Its address space is not expected to run out.

32. What is the difference between IPv4 and IPv6?

Ans:

IPv4	IPv6
IPv4 uses 32-bit addresses.	IPv6 uses 128-bit addresses.
IPv4 provides a smaller address space.	IPv6 provides a much larger address space.
IPv4 addresses are written in dotted decimal form.	IPv6 addresses are written in hexadecimal form.
IPv4 is the older version.	IPv6 is the newer version with a larger address space.

33. Why is NAT commonly used in homes and offices?

Ans: NAT allows many devices to share one public IP address. It hides private IP addresses from the Internet. This improves network security. It is commonly used in homes, schools, and offices.

34. Does every device need a MAC address?

Ans: Every Network Interface Card (NIC) has a unique MAC address. It helps identify a device on the network. It supports communication between connected devices. Every device connected to a network has its own MAC address.

Home Network Setup and Configuration

35. What is a home network?

Ans: A home network is a network that connects different devices in a house. It helps computers, laptops, mobile phones, printers, and other devices to communicate with each other. All devices can share the same internet connection. A router is the main device in a home network.

Wi-Fi Security and Router Configuration

36. Why is Wi-Fi security important?

Ans: Wi-Fi security protects the network from unauthorized users. It keeps personal and important information safe. It reduces the risk of cyber-attacks. It also ensures secure communication over the network.

37. What is router configuration?

Ans: Router configuration is the process of changing router settings. It helps make the network secure and efficient. Users can change the network name and password. They can also manage other network settings.

38. Describe the steps to secure a Wi-Fi network.

Ans: First, change the default router password. Then use a strong Wi-Fi password. Enable WPA2 or WPA3 security. Finally, keep the router firmware updated.

Network Diagnostic Tools and Commands

39. What are network diagnostic tools?

Ans: Network diagnostic tools are used to check and solve network problems. They help test network connections. They also identify communication errors. These tools help keep the network working properly.

40. List the common network diagnostic commands.

Ans: The common network diagnostic commands are **ping**, **ipconfig**, **tracert** and **nslookup**.

41. Describe purpose of network commands?

Ans:

- **ipconfig** command displays the IP configuration of a computer. It shows the IP address, subnet mask, and default gateway.
- **tracert** command shows the path taken by data packets to reach the destination. It displays each network device along the path.
- **nslookup** command is used to find information about domain names. It converts domain names into IP addresses.

Network Performance

42. What is network performance?

Ans: Network performance is the efficiency of a computer network. It shows how well the network transfers data. It depends on speed, reliability, and response time. Good network performance provides smooth communication.

43. List the factors that affect network performance.

Ans: The factors that affect network performance are bandwidth, latency, packet loss, and network congestion. Each factor influences data communication. They affect the speed and quality of the network. They should be managed properly for better performance.

44. What is network congestion?

Ans: Network congestion occurs when too much data travels through the network at the same time. It slows down communication. It increases delays. It reduces network performance.

Load Balancing

45. What is load balancing?

Ans: Load balancing is the process of distributing network traffic among multiple servers or devices. It prevents one server from becoming overloaded. It improves network performance. It also increases system reliability.

46. Why is load balancing important?

Ans: Load balancing distributes the workload evenly among servers. It prevents network congestion. It improves system performance. It also provides better availability of services.

Network Security

47. What is network security?

Ans: Network security is the protection of a computer network from unauthorized access and attacks. It keeps data and devices safe. It helps maintain privacy and security. It ensures that the network works safely.

48. Why is network security important?

Ans: Network security protects data from unauthorized access. It prevents cyber attacks and data theft. It keeps network services available. It also protects users' privacy.

49. Describe the common network security threats.

Ans:

- Malware is harmful software that damages computers and networks. It can destroy files or steal information.
- Phishing attack is an attempt to trick users into sharing personal or sensitive information.
- Denial-of-Service (DoS) attack makes a network service unavailable. It sends a large number of requests to the server.

50. List the methods used to improve network security.

Ans: The methods used to improve network security are strong passwords, firewalls, antivirus software, encryption, and regular software updates. These methods protect data and devices. They reduce cyber threats. They improve overall network security.

Data Backup and Recovery

51. What is data backup and data recovery?

Ans: Data backup is the process of making a copy of important data. It protects data from loss or damage. The backup copy can be used when the original data is lost. It helps keep important information safe. Data recovery is the process of restoring lost or damaged data. It uses backup copies to recover information.

52. Why is data backup important?

Ans: Data backup protects important files from being lost. It helps recover data after a system failure. It also protects data from accidental deletion and cyber attacks. It ensures that important information is not permanently lost.

53. Describe backup storage methods.

Ans: Backup storage methods are ways to store backup copies of important data. Common backup storage methods include:

- External hard drives
- USB flash drives
- Cloud storage

Usability and Security Trade-offs

54. What is a usability and security trade-off?

Ans: A usability and security trade-off is the balance between making a system easy to use and keeping it secure. Better security may reduce ease of use. Better usability may reduce security. A proper balance is important for an effective system.

CONCEPTUAL SHORT QUESTIONS

1. A bank has branches in different cities connected through a network to share data and services. Which type of network is suitable for this situation?
Ans: A WAN (Wide Area Network) is suitable because it connects networks over a large geographical area, such as different cities or countries.
2. A network architecture experiences a single cable break, and the entire network goes down. Which topology is being used, and why did this failure happen?
Ans: The network is using a **bus topology**. In this topology, all devices are connected through a single main cable (backbone cable). If this cable breaks, communication between all devices stops, causing the entire network to go down.
3. In an office, one computer's cable is damaged, but all other computers continue working normally. Which topology is most likely being used?
Ans: The office is using **Star Topology**. In a star topology, each device has its own cable connected to a hub or switch. If one cable fails, only that device is affected. The rest of the network continues to work normally.
4. A student types `www.google.com` instead of an IP address to open a website. Which service converts the website name into an IP address?
Ans: The **Domain Name System (DNS)** performs this task. DNS converts website names into IP addresses. This allows users to access websites without remembering numerical IP addresses. It makes Internet browsing easier.
5. A user logs in to an online banking website. Why is HTTPS used instead of HTTP?
Ans: **HTTPS** is used because it provides secure communication. It encrypts the data sent between the user and the website. This protects passwords and banking information from hackers. Therefore, HTTPS is safer than HTTP.
6. A computer cannot access websites because its default gateway is entered incorrectly. Why does this happen?
Ans: A **default gateway** connects a local network to other networks. It forwards data to destinations outside the local network. If the gateway is incorrect, data cannot reach the Internet. As a result, websites cannot be opened.
7. A family has four mobile phones and two laptops connected to the Internet through one router using a single public IP address. Which technology makes this possible?
Ans: This is possible because of **Network Address Translation (NAT)**. NAT allows many devices to share one public IP address. It hides private IP addresses from the Internet. It also improves network security.
8. A network administrator wants to check whether a server is reachable before troubleshooting other problems. Which command should be used first?
Ans: The **ping** command should be used first. It checks whether another device is reachable on the network. It also measures the response time. This helps identify connection problems.
9. A Windows user wants to check the computer's IP address, subnet mask, and default gateway. Which command should be used?
Ans: The **ipconfig** command should be used. It displays the computer's network settings. It shows the IP address, subnet mask, and default gateway. It is commonly used for network troubleshooting.
10. During an online game, the Internet speed is good, but players experience delays in their actions. Which network factor is causing this problem?
Ans: The problem is caused by **high network latency**. Latency is the time taken for data to travel between devices. High latency causes delays even when bandwidth is sufficient. Online games require low latency for smooth performance.

TEST YOUR SKILLS

Total Marks: 40

Time: 1:30 Hour

8 x 1 = 8

Q.1 MULTIPLE CHOICE QUESTIONS

1. A hardware device that allows a computer to connect to a network is called:
(a) Router (b) Modem (c) Network Interface Card (d) Switch
2. A network that covers a small geographical area, such as a school or office, is:
(a) WAN (b) MAN (c) LAN (d) Internet
3. The protocol mainly used to view web pages is:
(a) FTP (b) DNS (c) TCP (d) HTTP
4. The topology that provides the highest reliability is:
(a) Bus Topology (b) Ring Topology (c) Star Topology (d) Mesh Topology
5. Which OSI layer is responsible for routing data between networks?
(a) Network Layer (b) Session Layer (c) Presentation Layer (d) Data Link Layer
6. Which protocol converts website names into IP addresses?
(a) HTTP (b) FTP (c) TCP/IP (d) DNS
7. Which command is used in Windows to display network settings?
(a) Ping (b) SSH (c) PuTTY (d) ipconfig
8. A method that allows only authorized users to use network resources is called:
(a) Malware (b) Firewall (c) Access control (d) Subnetting

Q.2 SHORT QUESTIONS:

Note: Attempt any 8 short questions

8 x 2 = 16

- i. Write two uses of computer networks.
- ii. What is the function of a router?
- iii. What is the purpose of DNS?
- iv. Differentiate between LAN and WAN
- v. Differentiate between physical Topology and logical Topology
- vi. Write down advantages of ring topology?
- vii. Describe function of application layer of OSI model?
- viii. What is the difference between IPv4 and IPv6?
- ix. What is default gateway?
- x. Windows user wants to check the computer's IP address, subnet mask, and default gateway. Which command should be used?

LONG QUESTIONS:

Note: Attempt any 2 long questions

2 x 8 = 16

3. What is the OSI model? Explain its layers and their functions.
4. Define network topology. Explain bus, star, ring, and mesh topologies with advantages and disadvantages.
5. What are network protocols? Explain TCP/IP, HTTP, FTP, and DNS.