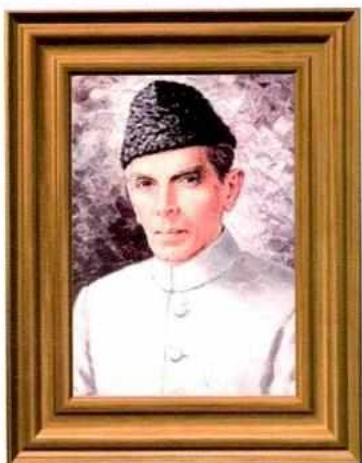


Computer Science and Entrepreneurship

12



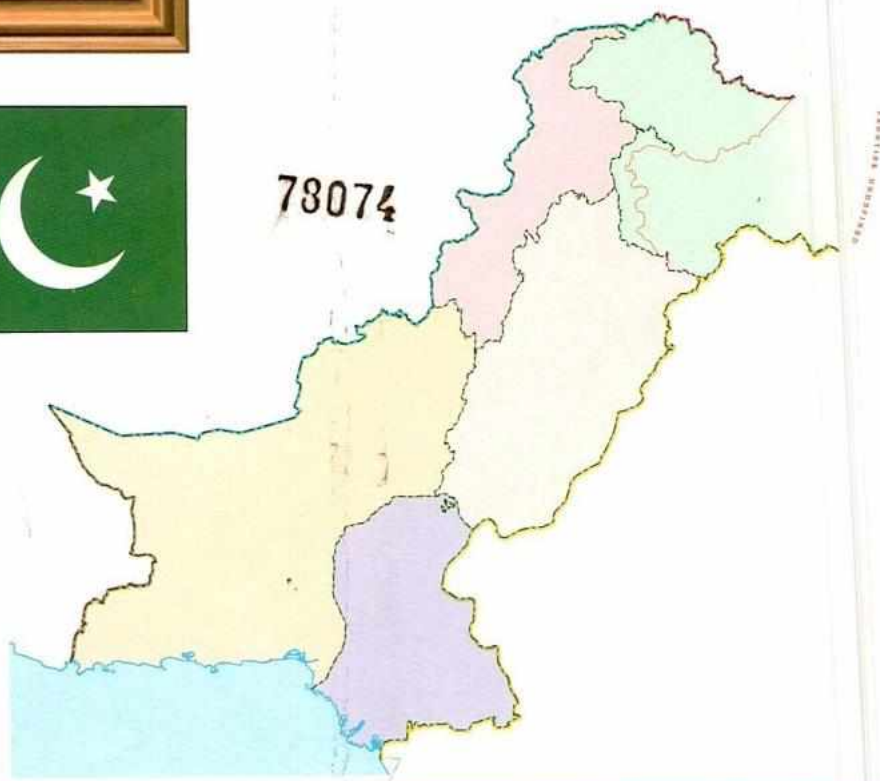
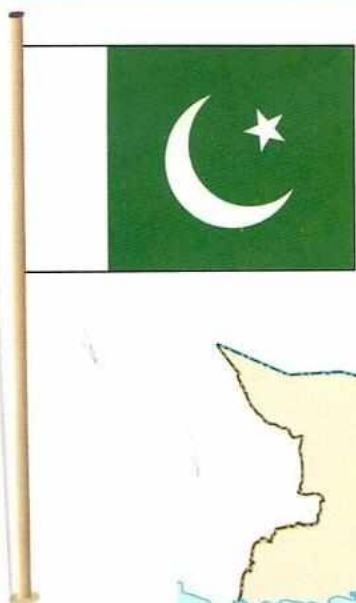
**PUNJAB EDUCATION, CURRICULUM, TRAINING
AND ASSESSMENT AUTHORITY**



"Education is a matter of life and death for Pakistan. The world is progressing so rapidly that without requisite advance in education, not only shall we be left behind others but may be wiped out altogether."

(September 26, 1947, Karachi)

Quaid-e-Azam
Muhammad Ali Jinnah محمد علی جناح
Founder of Pakistan



Instructions for Security Sticker

All textbooks of the Punjab Education, Curriculum, Training and Assessment Authority, carry a rectangular shaped security sticker on the title cover. The sticker exhibits a unique colour shift (orange to green) due to change of angle in the specific circle on it. Moreover, if you scratch protective coating on the specific given space of the sticker with a coin, it will reveal the registered trade name "PECTAA". For further verification, scan the given QR Code with any QR App from your cellphone, then a weblink will be opened to show the original sticker. Look for the security sticker while purchasing the textbooks. If there is no sticker on the title cover or it has been tampered with, do not buy such a textbook and feel free to inform on the given address of PECTAA.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

(In the Name of Allah, the Most Merciful, the Most Compassionate.)

COMPUTER SCIENCE AND ENTREPRENEURSHIP

12



**PUNJAB EDUCATION, CURRICULUM,
TRAINING AND ASSESSMENT AUTHORITY**

Authors

- ✱ **Dr. Abdul Sattar,**
Assistant Professor (CS),
Lahore Garrison University, Lahore.

- ✱ **Mr. Zulfiqar Ali Kullachi,**
Headmaster, Govt. High School,
Kot Haibat, D.G.Khan

Editor

- ✱ **Prof. Saqib Ubaid,**
Institute of CS. Khwaja Fareed University of Engineering and IT, Rahim Yar Khan.

External Review Committee

- ✱ **Muhammad Faheem,** Associate Prof. , Govt. Graduate College Gulberg Lahore.
- ✱ **M. Zeeshan Shabbir,** Associate Prof. , Govt. Graduate College of Science.
Wahdat Road, Lahore.
- ✱ **Mahvish Ponum,** Lecturer (CS), Govt. Associate College (W), Gawalmandi, Lahore.
- ✱ **Kashif Shahzad Ch,** SST(CS/IT), Govt. Muslim High School No.2, Civil Lines, Lahore.
- ✱ **Muhammad Asif Majeed Khan,** SST(IT), Govt. Model High School, Jampur.
- ✱ **Mehmood Ahmad,** Computer Teacher, Cresnet Model School Lahore.

Supervision

- ✱ **Jahanzaib Khan,** Assistant Director (Compliance Sciences), PECTAA

Director

(Curriculum & Compliance)

- ✱ **Aamir Riaz**

Deputy Director

(Compliance Sciences)

- ✱ **Syed Saghir-ul-Hassnain Tirmizi**

Incharge

(Art Cell)

- ✱ **Mst. Aisha Saidq**

Layout & Designing

- ✱ **Minal Tariq**

Illustrations

EXPERIMENTAL
EDITION

- ✱ **Aiyatullah**

Published By: Tips Academy.

Printed By: Ishaq Al-Fateh Printers, Lahore.

Date of Printing	Edition	Impression	Copies	Price
July 2026	1st	1st	3500	134.00

**< This textbook is based on Revised National Curriculum
of Pakistan 2023 >**

All rights are reserved with Punjab Education, Curriculum, Training and Assessment Authority.
No part of this textbook can be copied, translated, reproduced or used for preparation of
test papers, guidebooks, keynotes and helping books.

TABLE OF CONTENTS

Sr No.	Chapters	Page No.
1	Computer Networks	1
2	Computational Thinking & Algorithms	20
3	Object Oriented Programming Using Python	33
4	Development of Graphical User Interface (GUI)	45
5	Code Testing and Debugging	60
6	Data and Analysis	72
7	Hypothesis Testing	89
8	Applications of Computer Science	103
9	Cybersecurity and Safe Digital Collaboration	118
•	Pairing Scheme	137
•	Model Paper	139

Chapter 1

Computer Networks

Student Learning Outcomes:

By the end of this chapter, students will be able to :

- Understand and explain network architecture, its fundamental concepts and become proficient in network diagnostic tools and commands.
- Set up and configure home networks effectively and develop network troubleshooting skills and differentiate between network connection types.
- Understand and measure network bandwidth and latency, and appreciate the importance of network load balancing, network security, data backup and recovery.

Introduction

This chapter introduces the fundamental concepts of computer networks and explains how devices communicate with each other. Students learn about network architecture, key components, and the basic working of networks. It covers network models and layers, particularly the OSI model, along with different network topologies and types. The chapter also explains common networking devices such as NICs, switches, routers, modems, and wireless access points.

Students are introduced to essential protocols and services like TCP/IP, HTTP, FTP, and DNS, as well as concepts of IP addressing, IPv4/IPv6, subnetting, and NAT. They learn how to set up and configure home networks, including wired and wireless connections, and understand Wi-Fi security and encryption. The use of network diagnostic tools such as ping and ipconfig is also discussed. Finally, the chapter highlights network performance, security measures, and real-world practices to ensure safe and efficient communication.

1.1 Introduction to Computer Networks

A computer network allows different devices to connect and communicate with each other. It helps in sharing information quickly and easily. Communication through networks saves time and effort. Computer networks are used in homes, schools, offices, and businesses. Modern life depends heavily on computer networks for daily tasks.

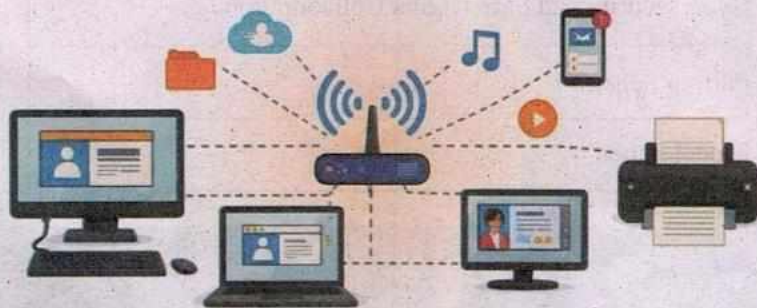


Figure 1.1: A computer network connects multiple devices to share data and resources

Networks can connect computers, mobile phones, printers, and other digital devices (as shown in Figure 1.1). These devices communicate using cables or wireless signals. A network allows data, files, and resources to move from one device to another. Networks can be small or large depending on the need.



TIDBIT

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

Uses of Computer Network

Internet browsing is a common example of network use. Mobile phones use networks for calls, messages, and apps. Schools use networks for online classes and learning systems. Banks use networks for online transactions and ATMs. Social media platforms work through computer networks. Smart homes also use networks to control devices.

1.2 Network Architecture and Basic Concepts

Network architecture is the overall design of a computer network. It shows how computers, servers, and other devices are arranged (as shown in Figure 1.2). It also defines how data is transmitted across the network. Network architecture includes hardware, software, and communication rules. A good architecture helps the network work efficiently. It also supports future expansion of the network.

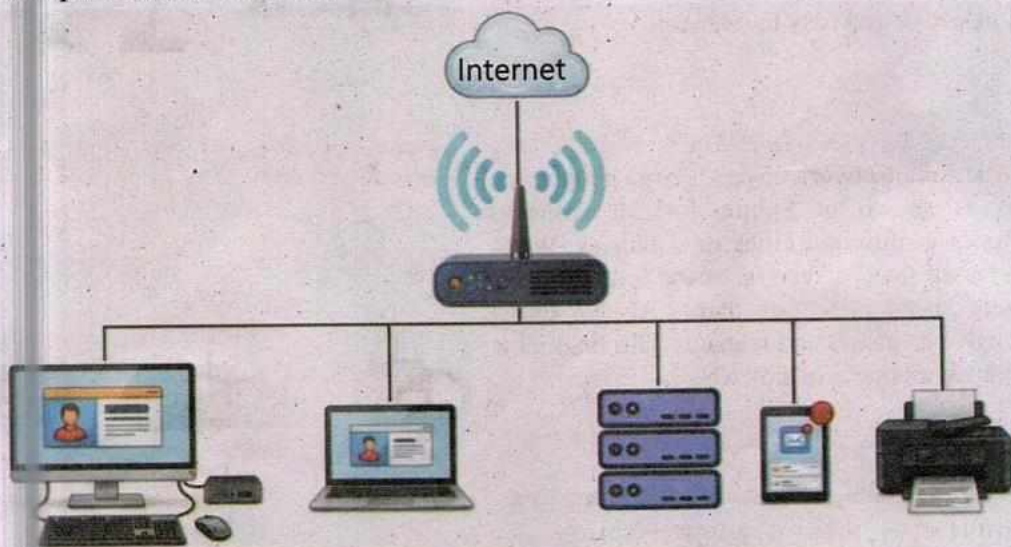


Figure 1.2: Network architecture shows how devices and components are organized in a network



CLASS ACTIVITY

Provide pictures or names of devices. Students match device names with functions. Discuss answers

A network works by sending data from one device to another. Data is broken into small packets before transmission. These packets travel through cables or wireless signals. Networking

devices guide packets to the correct destination. The receiving device reassembles the packets into the original data. This process allows smooth and fast communication.

1.3 Types of Computer Networks

Computer networks are classified based on size and coverage area. Different types of networks are used for different purposes. Each type connects devices in a specific way. The most common types are LAN, WAN, and the Internet (Public WAN). These networks help in communication and data sharing. Understanding network types helps in proper network selection.

DO YOU KNOW?

Computer networks are classified based on distance and coverage area.

Local Area Network (LAN)

A Local Area Network connects devices within a small area (as shown in Figure 1.3). This area can be a home, school, or office. LAN provides high data transfer speed. It is usually owned and managed by a single organization. Ethernet and Wi-Fi are commonly used in LANs. LAN is cost-effective and easy to maintain.



Figure 1.3: Local Area Network

Wide Area Network (WAN)

A Wide Area Network covers a large geographic area (as shown in Figure 1.4). It connects networks in different cities or countries. WAN uses leased lines, satellites, or the Internet. Data transfer speed is slower than LAN. WAN is expensive to install and manage. The Internet is the largest example of a WAN.

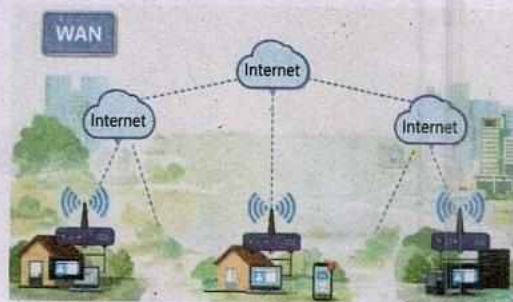


Figure 1.4: Wide Area Network

The Internet (Public WAN)

The Internet is a global network connecting millions of devices. It allows sharing of information worldwide. Services like email, websites and cloud storage use the Internet (as shown in Figure 1.5). It uses standard protocols for communication. The Internet supports education, business, and entertainment. It plays an important role in daily life.



Figure 1.5: Internet



CLASS ACTIVITY

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



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.

1.4 Networking Devices

Networking devices are used to connect computers and other devices in a network. These devices control the flow of data. Each device has a specific role in communication.

Network Interface Card (NIC)

A Network Interface Card allows a device to connect to a network (as shown in Figure 1.6). It can be wired or wireless. Each NIC has a unique address called MAC address. The NIC sends and receives data from the network. Without a NIC, a device cannot communicate on a network. NICs are built into most modern devices.

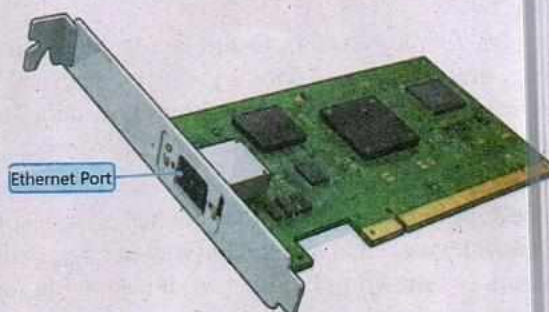


Figure 1.6: Network Interface Card

Switch

A switch connects devices and sends data to the correct device. Switches improve network speed and efficiency. Switches are common in modern networks.

Router

A router connects different networks together. It directs data packets to their correct destination. Routers connect local networks to the Internet. They use IP addresses to send data. Routers improve network security and control. Home and office networks use routers widely.

Modem

A modem connects a local network to an Internet Service Provider (ISP). It converts digital data into signals suitable for transmission. It also converts incoming signals back into digital form. Modems are used with cable, DSL, or fiber connections. Internet access depends on a modem. Modems often work with routers.



CLASS ACTIVITY

Teacher explains modem using signal conversion example. Students summarize.

Wireless access point

A wireless access point provides Wi-Fi connectivity. It allows wireless devices to connect to a network (as shown in Figure 1.7). It extends wireless network coverage. Access points are used in large buildings and campuses. They improve signal strength and stability. Wireless access points support mobile connectivity.



Figure 1.7: Wireless Access Point

1.5 Network Topologies

Network topology refers to the layout of a computer network. It explains how devices and cables are arranged. Topology can be physical or logical. Physical topology shows actual connections. Logical topology shows how data flows in the network. Topology affects network performance and maintenance.

Bus Topology

In bus topology, all devices are connected to a single main cable. Data travels along this cable to reach devices. It is simple and low in cost. Failure of the main cable can stop the entire network (as shown in Figure 1.8). It is suitable for small networks. Bus topology is not good for large networks.

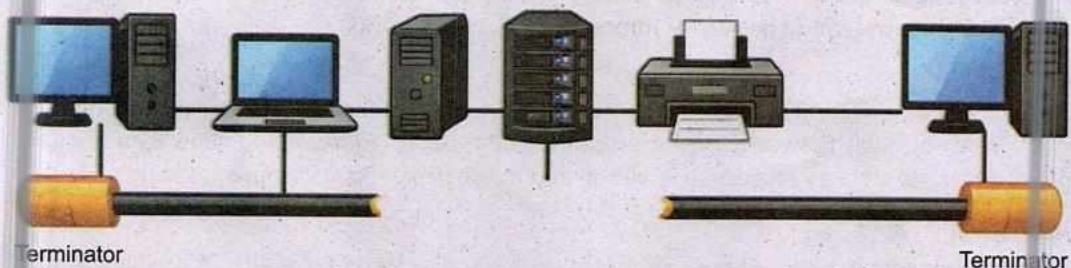


Figure 1.8: Bus Topology

Star Topology

In star topology, all devices connect to a central hub or switch (as shown in Figure 1.9). Data passes through the central device. It is easy to manage and expand. Failure of one device does not affect others. Failure of the central hub stops the network. Star topology is widely used in modern networks.

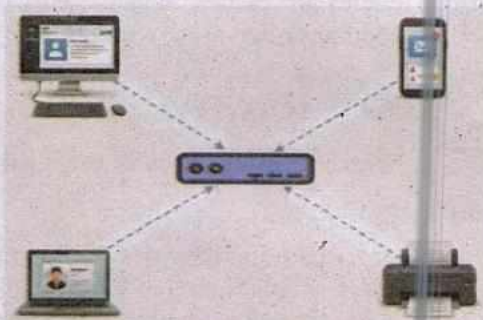


Figure 1.9: Star Topology

Ring Topology

In ring topology, devices are connected in a circular path (as shown in Figure 1.10). Data moves in one direction around the ring. Each device receives data and passes it along. Failure of one device can affect the whole network. It is more complex than bus topology. Ring topology is rarely used today.

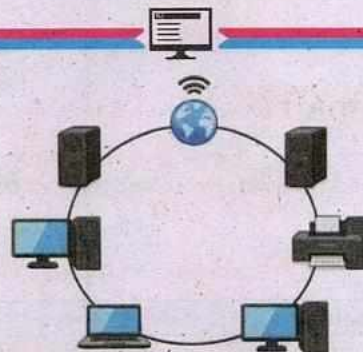


Figure 1.10: Ring Topology

CLASS ACTIVITY

Students stand in a circle and pass a message.
Discuss what happens if one student stops.

Mesh Topology

In mesh topology, devices are connected to many other devices. Multiple paths exist for data transmission. This increases reliability and fault tolerance. Failure of one link does not stop communication. Mesh topology is expensive and complex. It is used in large and critical networks.

Figure 1.11 shows a mesh topology network. In this topology, each device is connected to many other devices. Data can travel through multiple paths to reach its destination. If one connection fails, data can use another path. This figure explains why mesh topology is very reliable but complex.

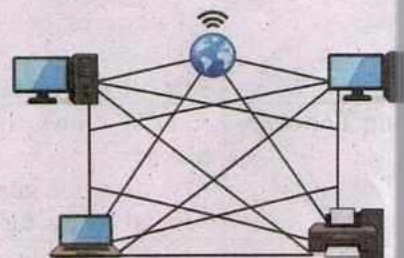


Figure 1.11: Mesh Topology

Tree Topology

In tree topology, devices are arranged in a hierarchical structure like a tree (as shown in Figure 1.12). It combines features of both bus and star topologies, where 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. However, failure of the backbone can affect the entire network. Tree topology is commonly used in large organizations.

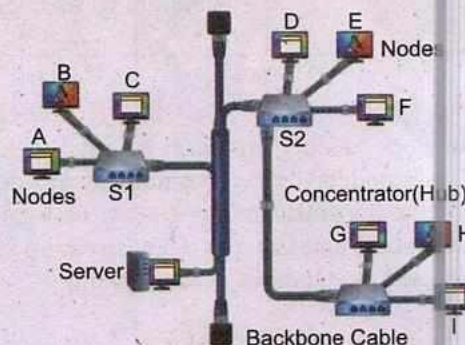


Figure 1.12: Tree Topology

Advantages and Disadvantages of Network Topologies

Different topologies offer different benefits. Some are easy to install and low-cost (as shown in Table 1.1). Others provide high reliability and performance. Certain topologies are easy to expand. Some are difficult to manage and expensive. Choosing the right topology depends on network needs.



TIDBIT

Some topologies are simple and cheap. Others are reliable but costly. Some are easy to expand. Others are difficult to manage. Choice depends on needs.

Table 1.1: Advantages & Disadvantages of Network Topologies

Topology	Advantages	Disadvantages
Bus Topology	• Simple and easy to install • Requires less cable • Cost-effective	• Failure of main cable affects whole network • Difficult to troubleshoot • Performance decreases with more devices
Star Topology	• Easy to install and manage • Failure of one device does not affect others • Easy to detect faults	• Central device failure stops entire network • Requires more cable • Higher cost
Ring Topology	• Data flows in an organized manner • No data collision • Equal access for all devices	• Failure of one device affects whole network • Difficult to add/remove devices • Rarely used today
Mesh Topology	• Highly reliable and fault-tolerant • Multiple paths for data • High security	• Very expensive • Complex installation • Requires large number of cables
Tree Topology	• Easy to expand • Suitable for large networks • Hierarchical management	• Backbone failure affects whole network • Complex setup • More cabling required

1.6 Network Models and Layers

Network models explain how data moves from one device to another in an organized way. These models divide communication into different layers. Each layer performs a specific task in data transmission (as shown in Figure 1.13). Layered models make networks easier to understand and manage. They also help in troubleshooting network problems. Network models are used as standards in networking.

? DO YOU KNOW?

Network models are used to understand complex network communication in simple steps.

Network Layers

Network layers divide the communication process into smaller parts. Each layer has a specific responsibility. Data passes through these layers step by step. This structure makes network

design simple and organized. Changes in one layer do not affect other layers. Layered communication improves reliability and control.

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. This model is used for learning and designing networks. It helps different systems communicate properly.

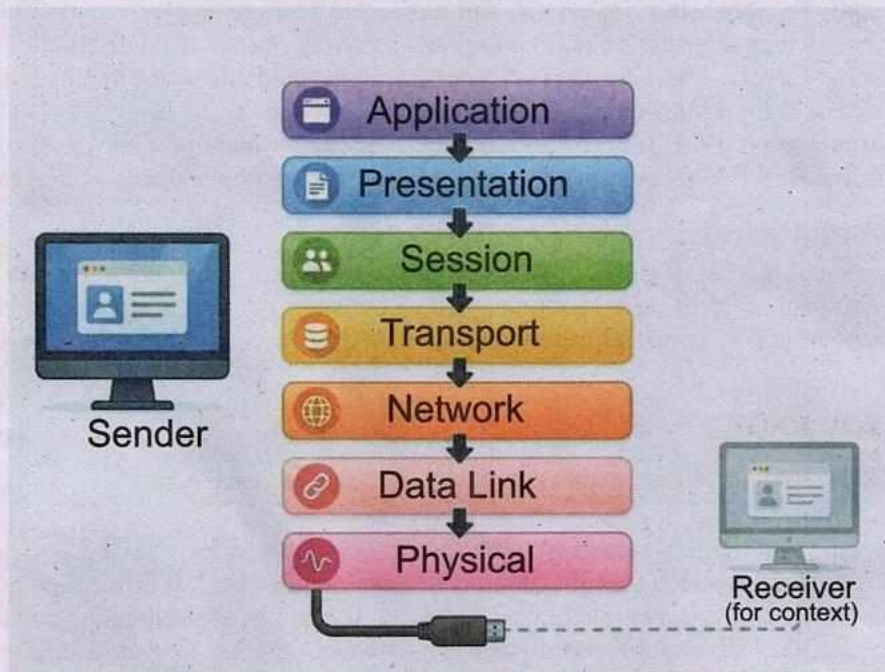


Figure 1.13: OSI Model on the Sender Side Showing Data Flow from the Application Layer to the Physical Layer

Functions of OSI Model Layers

Each OSI layer has a specific role in data communication. The physical layer sends raw data signals. The data link layer controls error-free transfer. The network layer handles routing of data. The transport layer ensures reliable delivery. The session, presentation, and application layers support user interaction and data formatting.

TIDBIT

Lower layers handle physical data transfer. Middle layers manage routing and delivery. Upper layers support user applications. Each layer works independently. Together, they ensure proper communication.

Each OSI layer has a specific role in data communication:

1. **Physical Layer:** Sends raw data as electrical, optical, or radio signals over the medium. It defines hardware aspects such as cables, connectors, voltage levels, and data transmission rates.



2. **Data Link Layer:** Ensures error-free data transfer between directly connected nodes. It handles framing, error detection/correction, and controls access to the shared transmission medium.
3. **Network Layer:** Responsible for routing data from source to destination across different networks. It manages logical addressing (IP addresses) and determines the best path for data delivery.
4. **Transport Layer:** Provides reliable and ordered delivery of data between devices. It performs error recovery, flow control, and segmentation of data into smaller units.
5. **Session Layer:** Establishes, maintains, and terminates communication sessions between applications. It manages session checkpoints and recovery in case of interruptions.
6. **Presentation Layer:** Translates data into a format understandable by the application layer. It handles data encryption, compression, and format conversion.
7. **Application Layer:** Provides services directly to end users and applications. It supports protocols like HTTP, FTP, and email services for communication and data exchange.

1.7 Network Protocols and Services

A network protocol is a set of rules for communication. It defines how data is formatted and transmitted. Protocols control error handling and data delivery. All devices in a network must follow the same protocol. Protocols ensure smooth data exchange. Examples include TCP/IP and HTTP.

DO YOU KNOW?

Protocols are like languages that computers use to talk to each other.

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 reliable data delivery. IP handles the addressing and routing of data. Together, TCP/IP enables communication between devices. It is used in almost all networks.

Hypertext Transfer Protocol (HTTP)

HTTP stands for Hypertext Transfer Protocol. It is used to transfer web pages. HTTP works between a web browser and a web server. It allows users to view websites. HTTP does not encrypt data; secure websites use HTTPS instead. HTTPS is the secure version of HTTP. It uses encryption to protect data transmitted between a web browser and a web server. This encryption is provided using SSL/TLS protocols, which ensure that sensitive information such as passwords, personal details, and payment data cannot be easily intercepted by attackers.

File Transfer Protocol (FTP)

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

Domain Name System (DNS)

DNS stands for Domain Name System. It converts website names into IP addresses. DNS makes websites easy to access (as shown in Figure 1.14). Users do not need to remember numbers. DNS servers perform this translation process. It plays a key role in Internet use.

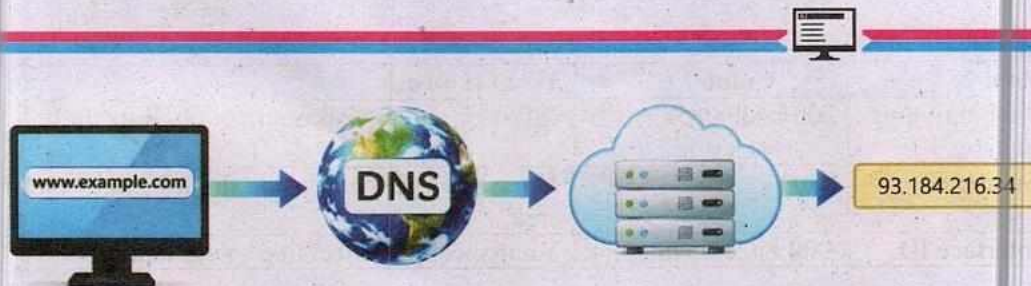


Figure 1.14: DNS Name Resolution Process



DO YOU KNOW?

DNS works behind the scenes every time a website is opened.

1.8 IP Addressing and Subnetting

An IP address is a unique number assigned to a device. IP stands for Internet Protocol. It helps identify devices on a network. Data uses IP addresses to find its destination. Every network device must have an IP address. Communication is not possible without it.

IPv4 and IPv6

IPv4 is an older version of IP addressing. It uses 32-bit numeric addresses. IPv4 has a limited number of addresses. IPv6 is the newer version with 128-bit addresses. IPv6 provides more address space. It supports modern Internet needs.

IPv4

Example: 192.168.1.10

IPv4 has 4 numbers, each 0–255, separated by dots.

Each number = 1 Byte = 8 bits

Total = 32 bits

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”



DO YOU KNOW?

Total IPv4 addresses possible: 4.29 billion

IPv6

Example:

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

IPv6 has 8 groups of 4 hexadecimal digits, separated by colons.

Each group = 16 bits

Total = 128 bits

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”

DO YOU KNOW?

- IPv6 addresses comprise: $2^{128} \approx 3.4 \times 10^{38}$ total addresses.
- IPv6 will never run out; it is an astronomically massive number.

Subnetting

Subnetting divides a network into smaller parts. Each part is called a subnet (as shown in Figure 1.15). It reduces network traffic. Subnetting improves performance. It increases security. Large networks use subnetting for management.

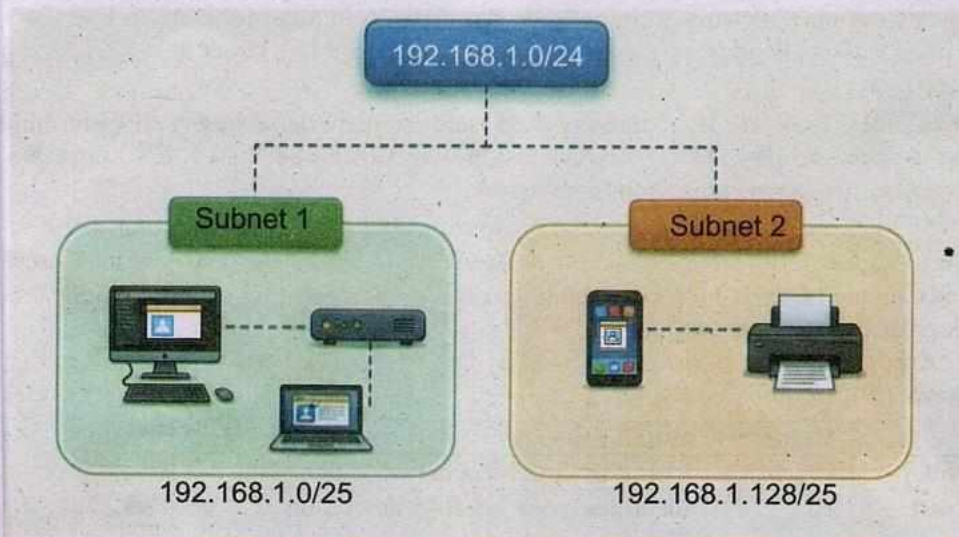


Figure 1.15: Subnetting Example

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. This improves network security. NAT is commonly used in networks.

1.9 Home Network Setup and Configuration

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



Components of a Home Network

A home network has different important components. A router connects all devices in the network. A modem connects the home network to the internet service provider. Computers, laptops, and mobile phones are network devices. Network cables are used for wired connections. Wireless devices use Wi-Fi signals to connect.

Wired Network Connections

A wired network uses cables to connect devices. Ethernet cables are commonly used in wired networks. Devices are connected directly to a router or switch. Wired connections provide high speed and stable performance. These networks are more secure than wireless networks. However, devices cannot move freely because of 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. Devices can move freely within the network range. Wireless networks are easy to install and use. They may be slower than wired networks in some cases.

1.10 Wi-Fi Security and Router Configuration

Wi-Fi security protects the network from unauthorized access. Without security, anyone can use the internet. Hackers can steal personal information from unsecured networks. Secure Wi-Fi keeps data safe and private. It also prevents slow internet speed. Strong security improves overall network performance.

Router Web Interface

1. Router Configuration: The router web interface is used to manage router settings. It is opened using 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 changes in Wi-Fi name and password. It also helps control security settings.

2. Wi-Fi Encryption: Protects data sent over the network. It converts data into a secure form. WPA2 and WPA3 are common security protocols. Older protocols like WEP are not secure. Strong encryption prevents data theft. Users should always select the latest encryption method.

3. Default Gateway: A default gateway connects a local network to other networks. It is usually a router. Data meant for outside networks goes through the gateway. The gateway forwards data to the correct network. Internet access depends on it. Proper gateway setting is necessary.



CLASS ACTIVITY

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

Guest Networks

A guest network allows visitors to use the internet. It is separate from the main home network. Guest users cannot access personal devices. This increases network safety and privacy. Guest networks help control internet usage. They are useful in homes and offices.

1.11 Network Diagnostic Tools and Commands

Network diagnostic tools are used to find network problems. They help check internet and network connections. These tools show whether devices can communicate properly.



Commands are entered using the command prompt or terminal. It helps identify slow or broken connections.

Network troubleshooting is done to find and fix network issues. It helps detect connection and speed problems. Troubleshooting checks cables, devices, and settings. It reduces network downtime and errors. It helps maintain smooth communication. Proper troubleshooting improves network performance.

Ping Command

The ping command is used to test network connectivity. It checks if a device is reachable on the network. Ping sends small data packets to another device (as shown in Figure 1.16). It measures response time from the destination. This command helps detect network delays. It is commonly used to check internet connection.

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
```

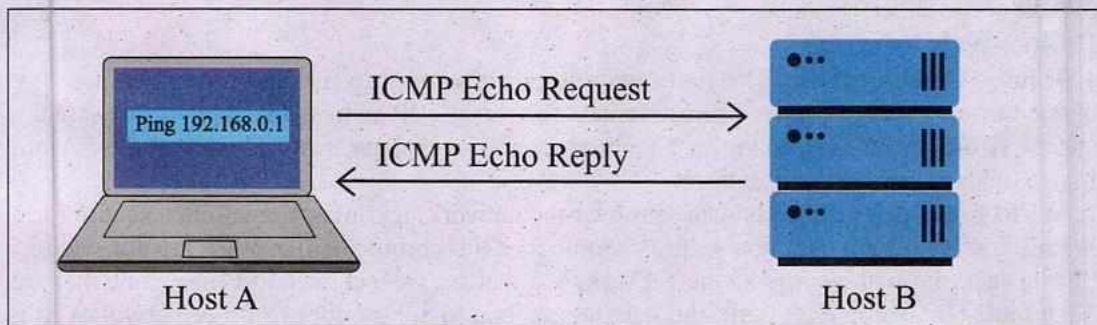


Figure 1.16: Ping Command



CLASS ACTIVITY

Map packet paths between two locations.

Ipconfig and ifconfig Commands

Ipconfig is used in Windows operating system. Ifconfig is used in Linux and macOS systems. These commands display network settings. They show IP address and subnet mask. They also show gateway and network status. These commands help in network troubleshooting.

Telnet, PuTTY, and Secure Shell (SSH)

Telnet is used for remote device access. It sends data without encryption. PuTTY is a popular tool for remote login. SSH is a secure method for remote access. SSH encrypts data for safety. These tools help manage network devices.



1.12 Network Performance

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

Network Bandwidth

Network bandwidth is the amount of data sent in a given time. It shows how much data a network can carry. Bandwidth is usually measured in Mbps. Higher bandwidth means faster data transfer. More devices use more bandwidth. Low bandwidth can cause slow internet speed.

Network Latency

Network latency is the time taken by data to travel. It is the delay between sending and receiving data. Latency is measured in milliseconds. Low latency means faster response. High latency causes lag and delay. Online games and video calls need low latency.

Causes of Network Delay

Network delay happens due to many reasons. Too many users can slow the network. Poor-quality cables can cause delay. Long distance between devices increases delay. Network congestion affects data speed. Hardware problems also cause network delay.



CLASS ACTIVITY

Identify possible causes of delay in a given scenario.

1.13 Network Load Balancing

Network load balancing is used to manage network traffic. It distributes work among multiple servers or links. This helps prevent overloading of one device. Load balancing improves network speed and reliability. It is used in large networks and data centers. Proper load balancing ensures smooth performance. It helps networks handle more users.

Benefits of Load Balancing

Load balancing improves network speed and response time. It reduces the risk of server failure. If one server fails, others continue working. It provides better user experience. Load balancing helps handle high traffic easily. It increases network reliability and availability.

Basic Load Balancing Methods

There are different methods of load balancing. Round Robin method sends requests one by one. Least Connection method sends traffic to less busy servers. IP Hash method uses IP address to decide traffic. These methods balance the network load. Simple methods are easy to implement.

1.14 Network Security

Network security is used to protect computer networks. It keeps data safe from unauthorized access. Security helps prevent data loss and damage. Many users connect to networks daily. Without security, networks become unsafe. Network security uses different tools and rules. It



CLASS ACTIVITY

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

is important for homes and organizations. Network security protects personal and important information. It stops hackers from entering the network. Security keeps data private and safe. It also protects devices from malware. Secure networks work smoothly without interruptions. Every network needs basic security measures.

Firewalls

A firewall is a security device or software. It controls incoming and outgoing network traffic. Firewalls block harmful or unwanted data (as shown in Figure 1.17). They act as a barrier between safe and unsafe networks. Firewalls protect computers from attacks. They are used in homes and offices.

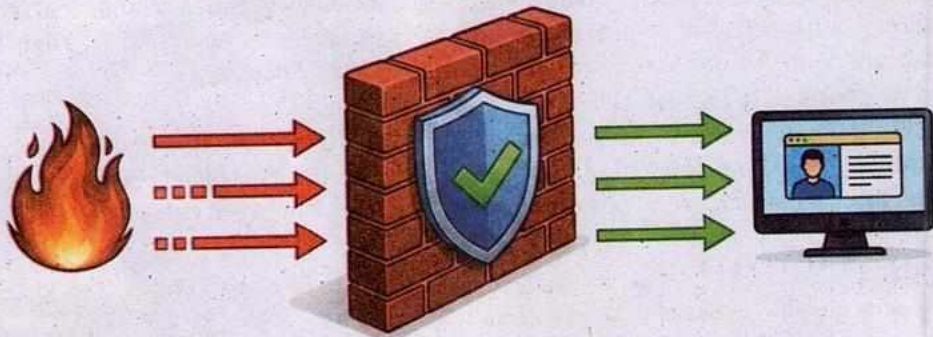


Figure 1.17: Firewall Protection

Encryption

Encryption changes data into a secret form. Only authorized users can read encrypted data. It protects data during transfer. Encryption is used in emails and online banking. Strong encryption improves data security. It prevents data theft.

Access Control

Access control decides who can use the network. It allows only authorized users to enter. Usernames and passwords are common access controls. Permissions limit what users can do. Access control protects important resources. It helps manage network usage.

Common Network Security Threats

There are many threats to network security. Viruses and malware damage systems. Hackers try to steal data. Phishing tricks users to share information. Denial of Service attacks stop network services. Security tools help reduce these threats.

1.15 Data Backup and Recovery

Data backup means making a copy of important data. It helps protect data from loss or damage. Data can be lost due to viruses or hardware failure. Backup allows data to be restored easily. Recovery is the process of getting data back. Backup and recovery are very important for safety. Every user should back up data regularly.



Types of Data Backup

There are different types of data backup. Full backup saves all data at once. Incremental backup saves only changed data. Differential backup saves changes since last full backup. Backups can be stored on hard drives. Cloud storage is also used for backup.

Data Recovery Methods

Data recovery is used to restore lost data. Backup files are used for recovery. Recovery software helps get deleted files. System restore can recover system data. Professionals can recover data from damaged devices. Recovery methods help reduce data loss.

1.16 Usability and Security Tradeoffs

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

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

Tradeoffs Between Usability and Security

Increasing security can make systems harder to use. Strong passwords are difficult to remember. Extra login steps slow down users. Simple systems are easier but less secure. Removing security increases risk. A balance is required for safe and easy use.



Summary

Computer Network

A computer network is a group of connected computers and devices that share data, resources, and services.

Network Architecture

Network architecture is the design and organisation of a network, including how devices are connected and how communication takes place.

Network Topology

Network topology is the arrangement of devices and connections in a network, such as star, bus, ring, mesh, or tree.

LAN

A Local Area Network (LAN) connects devices within a small area, such as a home, school, office, or computer lab.

WAN

A Wide Area Network (WAN) connects networks over large geographical areas, such as cities, countries, or continents.

Internet

The Internet is the largest public network that connects millions of devices and networks worldwide.

Networking Devices

Networking devices are hardware components, such as switches, routers, modems, NICs, and access points, used to connect devices and manage communication.

OSI Model

The OSI model is a seven-layer model that explains how data travels from one device to another in a network.

Network Protocol

A network protocol is a set of rules that controls how data is sent, received, and understood between devices.

IP Address

An IP address is a unique address assigned to a device so it can be identified on a network.

Subnetting

Subnetting is the process of dividing a large network into smaller networks for better management and security.

Network Security

Network security refers to the methods used to protect networks, devices, and data from unauthorized access, misuse, or attacks.



EXERCISE

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



Short Questions

1. What is a computer network?
2. Write two uses of computer networks.
3. What is network architecture?
4. Name any two components of a computer network.
5. What is the OSI model?
6. Write the name of any two network topologies.
7. What is a Local Area Network (LAN)?
8. What is the function of a router?
9. What is a network protocol?
10. What is the purpose of DNS?



Long Questions

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.



Answer Key

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