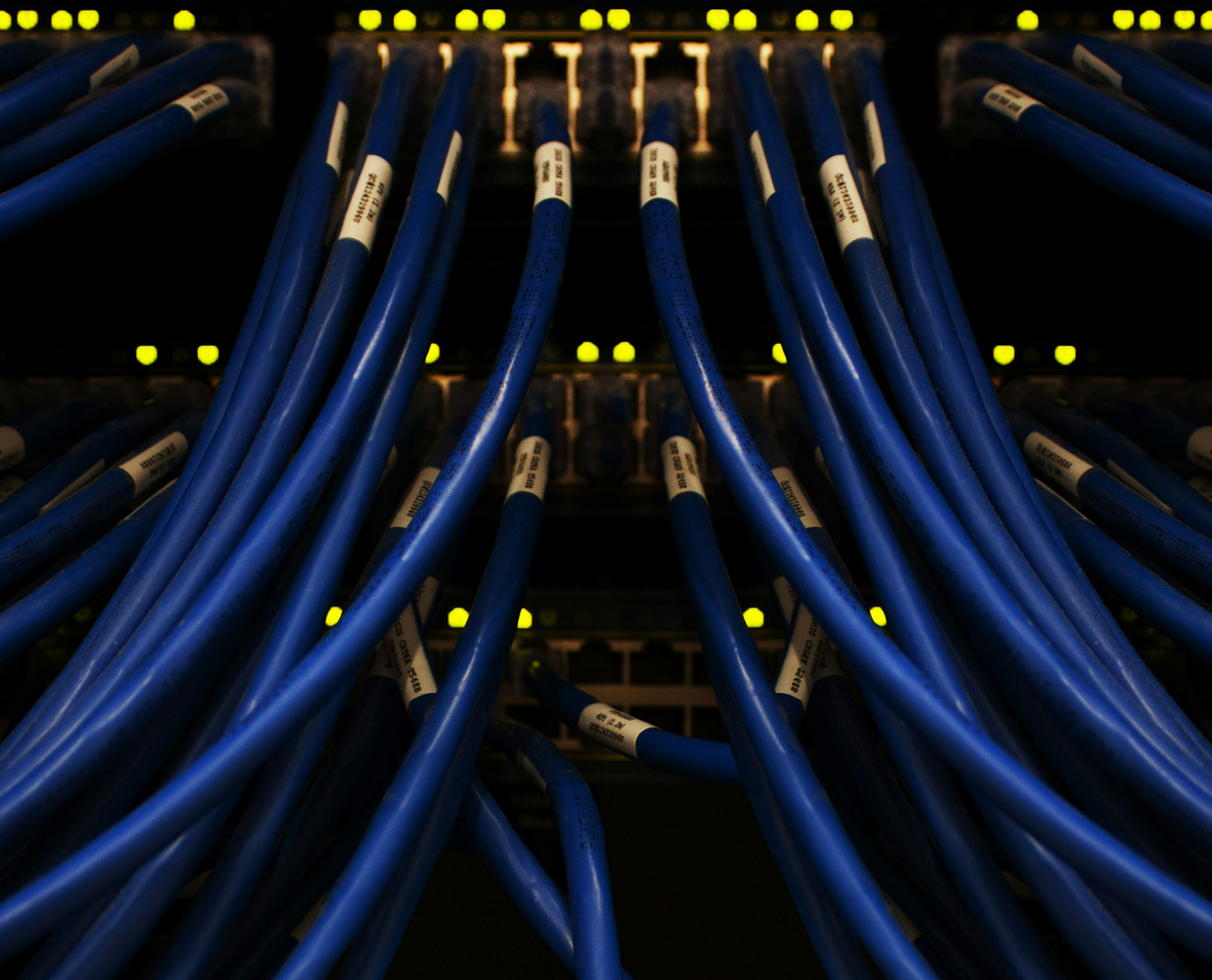


SECTION

3

COMPUTER
NETWORKING



Computer Architecture and Organisation

Data communication and Network systems

INTRODUCTION

The need to share information and resources among different computers has led to computer systems being linked together, called networks, in which computers are connected so that data can be transferred from machine to machine. The primary purposes of computer networks are to facilitate communication and share resources among connected devices. Using networks, computer users can exchange messages and share resources, such as printing capabilities, software packages, and data storage facilities.

Examples include an office network (connecting computers, printers, and a server in the lab), your school Wi-Fi (allowing you to research, and learn on the extended reading questions to the internet), and an ATM network (connecting ATMs to a bank's network to allow customers to access their accounts from various locations).

At the end of this section, you will be able to:

1. Demonstrate understanding of computer networks and how they work.
2. Identify at least 3 Types of Network Systems.
3. Differentiate among three types of Network Systems.

Key Ideas

1. A **computer network** is a connection of two or more computers or computing devices.
2. Some components of a computer network are; hub, nodes, and network interface cards (NIC).
3. A **stand-alone computer** is a computer that operates independently and is not connected to a network.
4. A **computer area network** refers to a type of network designed to connect computers within a limited area such as a building, campus, or small geographical area.
5. A **network topology** describes both the physical and logical arrangement of different components (links, nodes, etc) in a computer network.
6. A **network architecture**: The design and structure of a computer network.
7. A **client-Server model**: Clients request services from centralised servers, ensuring easier management, security, and scalability.
8. A **Peer-to-Peer model**: Is an architecture where devices or nodes share resources and services directly without centralised control.

9. A **network topology**: The physical and logical arrangement of network elements (routers, switches, hub, cables etc.).
10. **The cloud networks**: It involves a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
11. **The OSI model**: It is a set of rules that explains the process of transmitting data between network devices.
12. A **wireless network** or **wireless data connection** refers to the transfer of data between devices without the use of physical cables.
13. A **wired network** or **wired data connection** refers to the transfer of data between devices with the help of physical cables.

ADVANTAGES OF A COMPUTER NETWORK OVER STAND-ALONE

Computer networking offers numerous benefits, which have significantly transformed how we communicate, access information, and conduct business. Some of the key advantages of computer networking include:

1. Resource Sharing

One of the primary benefits of networking is the ability to share hardware resources (e.g., printers, scanners, storage devices) and software applications among multiple users. This reduces costs and increases efficiency as each device does not need to have dedicated resources.

2. Data Sharing and Collaboration

Networking enables seamless sharing of data and files between users, facilitating collaboration on projects and tasks. This is particularly useful in business settings where teams need to work together on documents and presentations.

3. Shared Internet Access

Networking allows multiple devices to share a single internet connection, making it a cost-effective and convenient way for businesses and households to provide internet access to all connected devices.

4. Centralised Management

In a business networked environment, system administrators can manage and monitor multiple devices and users from a central location. This centralised management simplifies tasks like software updates, security configurations, and user permissions.

5. Communication

Networking enables efficient communication through various means, such as email, instant messaging and VoIP (Voice over Internet Protocol). These communication tools help individuals and businesses stay connected regardless of geographic locations.

6. Improved Efficiency

Computer networking streamlines various processes, reducing the need for manual tasks. For example, automated backups and data synchronisation across devices improve data reliability and reduce data loss risks.

7. Remote Access

With network connectivity, users can access resources and data remotely. This is especially valuable for employees working from home or on the go, as they can access some office resources securely from any location, when using the correct tools such as VPN.

8. Scalability

Networks can be designed to easily scale to accommodate additional devices and users as an organisation grows, without significant changes to the existing infrastructure.

9. Cost Savings

By sharing resources, businesses can cut down on hardware and software expenses. Additionally, networked environments can reduce paper usage through digital file sharing and electronic communication.

10. Enhanced Security

While security is a concern in networking, a properly configured network can implement security measures like firewalls, encryption and access controls, which improve data protection and can prevent unauthorised access.

11. Real-Time Data Exchange

In industries like finance and manufacturing, real-time data exchange is crucial for decision-making. Networking allows the rapid transmission of information between systems and applications.

12. Global Connectivity

The internet and other wide area networks (WANs) enable global connectivity, linking people, businesses and information worldwide. This has revolutionised the way we access information and conduct international business.

COMPONENTS OF A COMPUTER NETWORK

Computer networks are composed of several key components that work together to enable communication and data exchange between devices. These components include:

1. Hub

This device serves as a central connection point for multiple devices in a network. It relays any signal it receives with some amplification back out to all the devices connected to it. Hubs are less common today due to their inefficiency and lack of intelligence in data transmission.

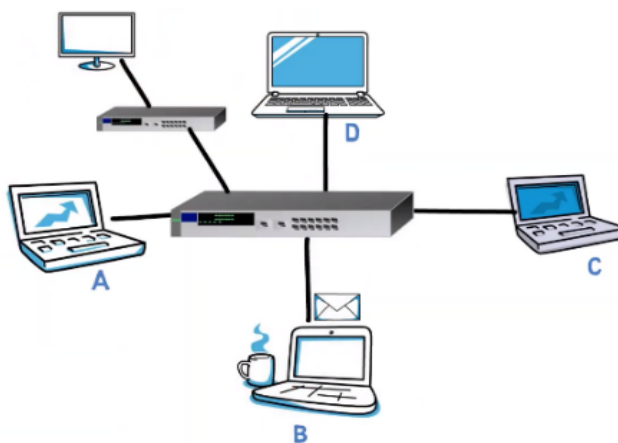


Figure 3.1: A hub connected to devices

2. Nodes

These are the devices connected to the network that can send, receive, and process data. Examples of nodes include computers, laptops, servers, routers, switches, smartphones, printers, and other smart devices.

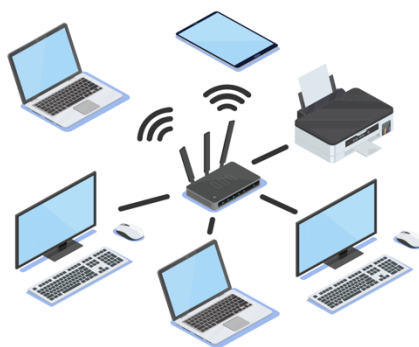


Figure 3.2: Network with 6 connected nodes

3. Network Interface Card (NIC)

This is a hardware component that allows a device to connect to the network. It is responsible for converting data from the device into a format suitable for transmission over the network, and vice versa. A WNIC (wireless NIC) enables wireless connectivity to a network.

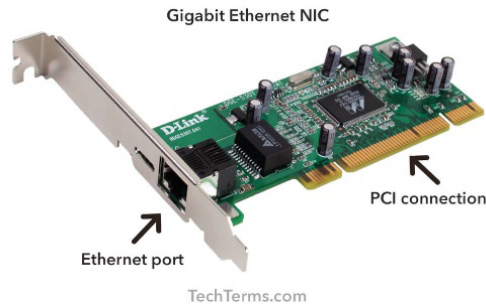


Figure 3.3: NIC

4. Communication Channels

These are the physical or logical pathways through which data is transmitted between nodes. They can be wired (e.g. Ethernet cables, fibre optics) or wireless (e.g. Wi-Fi, Bluetooth).

5. Switches

These are devices that facilitate the connection and communication between multiple devices within a local area network (LAN). They use MAC addresses (media access control addresses) to forward data to the intended recipient. A MAC address is a 48-bit number assigned to each device connected to the network. This intelligence is illustrated in Figure 9.4



Figure 3.4: A hub and switch

6. Routers

These are digital devices that connect different networks and determine the best path for data to travel from the source to the destination across the internet or other networks.

7. Modems

These devices are used to modulate and demodulate digital signals to enable communication over analogue communication channels, such as telephone lines. Modem router combo devices combine the functionalities of routers and modems.

8. Protocols

These are a set of rules and conventions that govern how data is transmitted, received, and processed over the network. Examples include TCP/IP (Transmission Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), and DNS (Domain Name System).

9. Network Operating System (NOS)

This is the software that manages and controls the network, providing services such as file sharing, network security, and network administration.

10. Firewalls

These are computer network security systems (hardware or software) that monitor and control incoming and outgoing network traffic, protecting the network from unauthorised access and potential threats. It will filter data by checking to see if it or its behaviour fits the profile of malicious code.

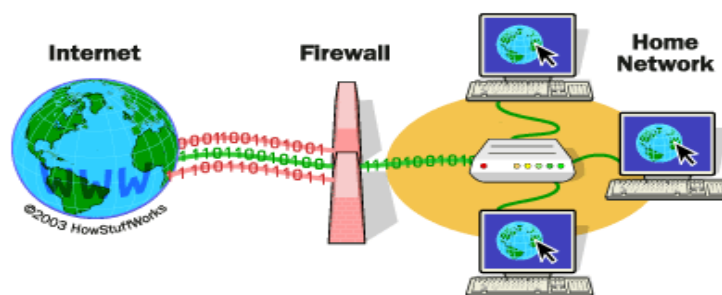


Figure 3.5: A firewall is an example of a network security solution

The main difference between a hardware firewall and a software firewall is that the hardware firewall runs on its own physical device, while a software firewall is a program installed on a computer. A common example of a software firewall is the firewall built into most operating systems like Windows and macOS (Macintosh Operating System).

11. Network Cables and Connectors

These physical cables (e.g., Ethernet cables) and connectors are used to establish wired connections between devices in a network.

12. Wireless Access Points (WAPs)

These provide wireless connectivity to devices within a local area network, allowing them to connect to the network without the need for physical cables. Some WAPs can be wall mounted – see Figure 9.6



Figure 3.6 WAP

13. Network Topology

This refers to the physical or logical arrangement of nodes and communication channels in a network. Common topologies include star, bus, ring, and mesh. (Topologies will be studied in Week 11)

14. Workstation

A term sometimes used to describe a computer (usually desktop) connected to a LAN.

Each of these components plays a specific role in a network, contributing to the efficiency and effectiveness of its operation. They work together to enable data sharing, resource sharing, and communication between network devices and users.

Activity 3.1

In your groups, do the following;

Each group will be assigned a specific type of network hardware to research (e.g., Group A: routers, Group B: modems, Group C: switches, etc.) discuss the importance of your assigned network hardware.

1. Each group has a fictional budget of Gh¢1000 to source two examples of your assigned hardware type.
2. Each device must cost no more than Gh¢1000
3. Use the internet to find two suitable examples of your assigned hardware type within the budget. Note: Look for reliable sources such as tech websites, online stores, and product reviews.
4. Collect information on specifications, features, prices, and customer reviews for each device.
5. Compare the two devices your group found, considering factors such as:
 - a. What features does each device offer?
 - b. Are there any common issues mentioned in reviews?

- c. How do the prices compare to the features offered?
6. Discuss within your group to decide which device is the better option based on your comparison.
7. Create a report or presentation summarising your findings to the whole class.

Activity 3.2

In your groups, observe the images of the network components below and correctly name the devices labelled A – F.

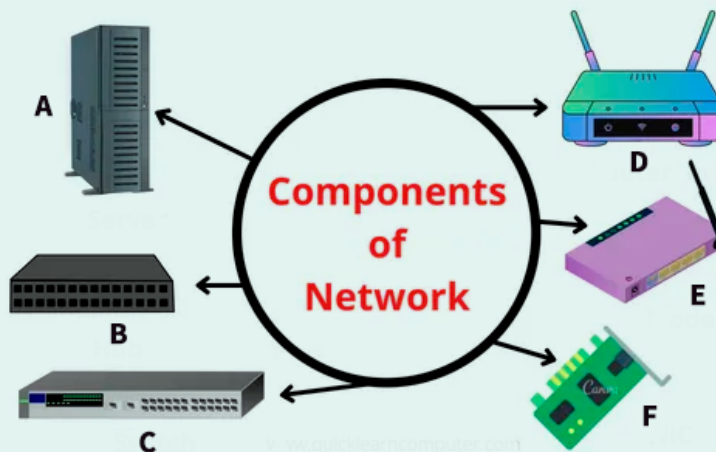


Figure 3.7: Network components

Activity 3.3

In your groups, and with the help of the teacher, connect a network device to a computer in your lab

Materials needed: Ethernet cable (network cable), a computer, switch/router/modem/hub

STEPS

1. Locate the Ethernet port at the back of the desktop computer. On a laptop, it can be found on the side or back of the device.
2. Take one end of the Ethernet cable and firmly plug it into the Ethernet port on your computer. You should hear a click when the cable is properly inserted.
3. Take the other end of the Ethernet cable and plug it into an available Ethernet port on your router, switch, or modem. Again, you should hear a click when it is properly inserted.

NOTE: On most devices, there are small LED lights next to the Ethernet ports. When the cable is connected properly, these lights should blink or turn solid to indicate a successful connection.

Conclusion: In a small home network setup like this, a switch is not required because the Wi-Fi router acts as the central point where devices connect and communicate. The router handles the switching functions internally, allowing devices to share resources and access the internet without the need for additional networking hardware like a switch.

TYPES OF COMPUTER AREA NETWORKS

Area networks include a personal area network (PAN), a local area network (LAN), a metropolitan area network (MAN), or a wide area network (WAN).

1. PAN (Personal Area Network)

It is normally used for short-range communications—typically less than a few metres, such as between a wireless mouse and a PC.



Figure 3.8: Personal area network

2. LAN (Local Area Network)

It normally consists of a collection of computers in a single building or building complex. For example, the computers in a school or those in a manufacturing plant might be connected by a LAN. LANs provide high data transfer rates and low latency (delay in network communication), making them ideal for resource sharing and collaborative work.



Figure 3.9 Local area network

3. MAN (Metropolitan Area Network)

It is a network of intermediate sizes, such as one spanning a campus, a region or even a city.

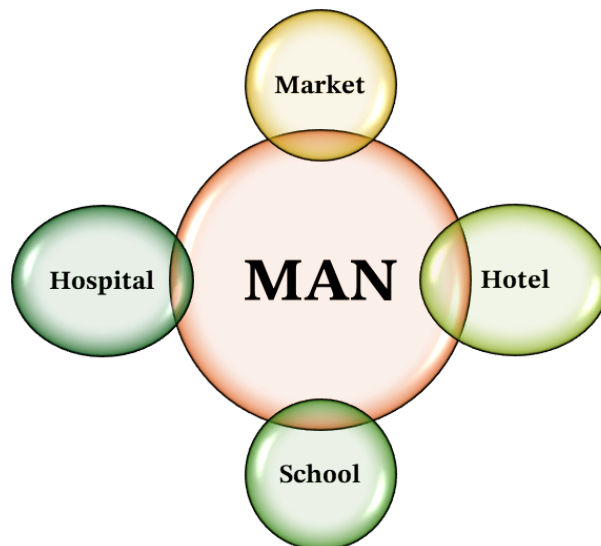


Figure 3.10: Metropolitan area network

4. WAN (Wide Area Network)

It links computers and devices over a greater distance—perhaps in neighbouring cities or on opposite sides of the world. WANs can also connect other small and medium networks like LANs and MANs – see Figures 3.11 and 3.12. The internet is essentially a huge international WAN.

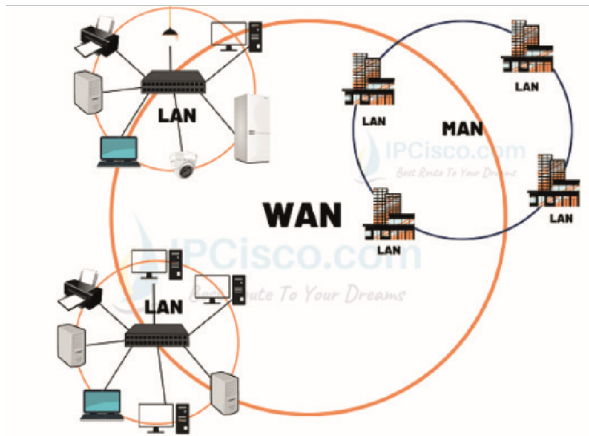


Figure 3.11 A WAN

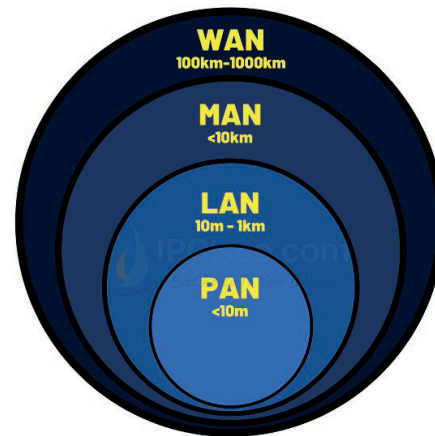


Figure 3.12: Range of area networks



Figure 3.13: A WAN

TYPES OF NETWORK TOPOLOGIES

Network topology refers to the physical or logical arrangement of devices and connections in a computer network. There are several types of network topologies, each with its advantages and disadvantages. Here are the main types:

1. Bus Topology

All devices are connected to a single central cable called the 'bus'. Each device on the network can communicate directly with the others. However, if the central bus cable fails, the entire network will go down.

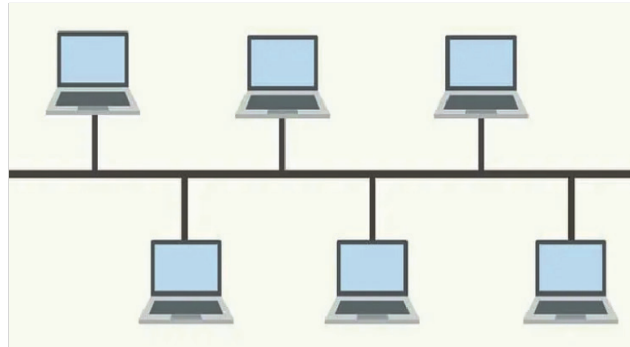


Figure 3.14: Bus Topology

2. Star Topology

All devices are connected to a central hub or switch. Each device has its dedicated connection to the central hub, making it easier to manage and troubleshoot individual connections. If one device fails, it does not affect the rest of the network. However, the central hub becomes a single point of failure.

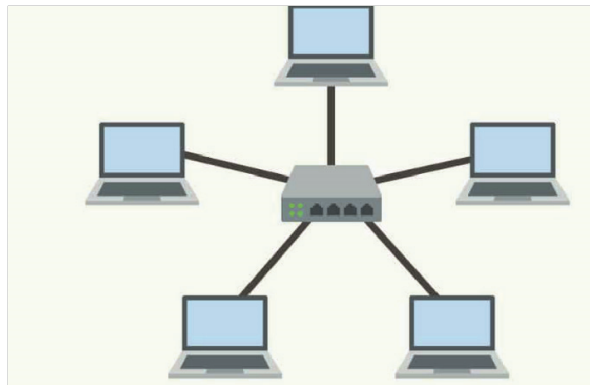


Figure 3.15: Star Topology

3. Ring Topology

The devices are connected in a closed loop. Each device is connected to two other devices, creating a continuous circle. Data travels around the ring from one device to the next until it reaches its destination. Ring topologies are less common due to the risk of a single connection failure disrupting the entire network.

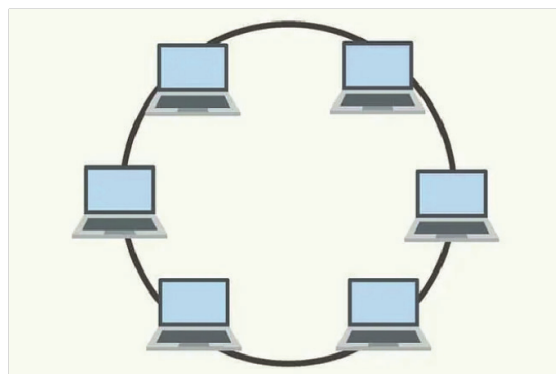


Figure 3.16: Ring Topology

4. Mesh Topology

Every device is connected to every other device in a fully-connected mesh network. This redundancy ensures multiple paths for data to travel, providing high reliability and fault tolerance. Fault tolerance refers to the ability of a network to continue operating without interruption when one or more of its components fail. Mesh topologies are highly resilient but can be costly to implement due to the large number of connections required.

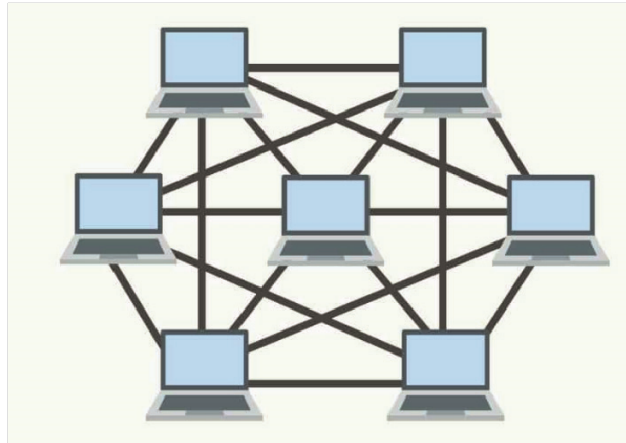


Figure 3.17: Mesh Topology

A partial mesh topology provides alternate routes from each node to some of the other nodes on the network.

5. Tree (Hierarchical) Topology

It is a combination of bus and star topologies. It has a central hub (root) connected to multiple devices in a star configuration. Each of these devices can then have additional devices connected to them, forming a hierarchical structure. Tree topologies are useful for large networks that require subnetworks and hierarchical organisation.

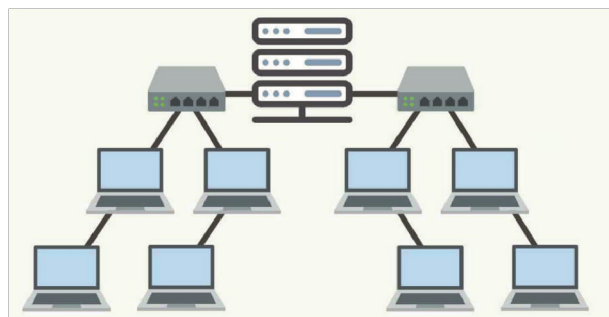


Figure 3.18: Tree Topology

6. Hybrid Topology

It combines two or more different types of topologies. For example, an example of a hybrid topology is a ring star, where a star network is connected through a hub

to a ring network. Hybrid topologies offer flexibility and can suit complex network requirements.

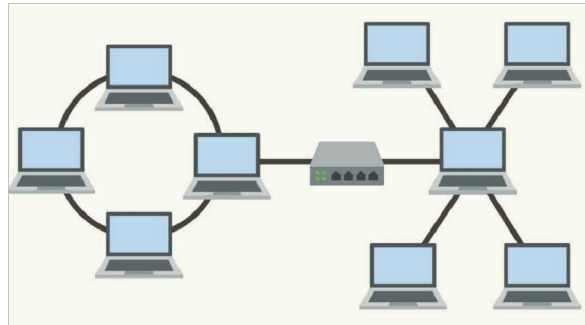


Figure 3.19: Hybrid Topology

Each network topology has its strengths and weaknesses, and the choice of topology depends on factors like the size of the network, the desired level of redundancy, cost considerations, and the specific needs of the organisation or application.

Note that network redundancy refers to the process of adding additional or alternate instances of network devices, equipment, and communication channels within a network infrastructure. This is done to ensure network availability in case of a network device or path failure.

Activity 3.4

In your group, do the following:

1. Observe the types of network systems in the diagram below.

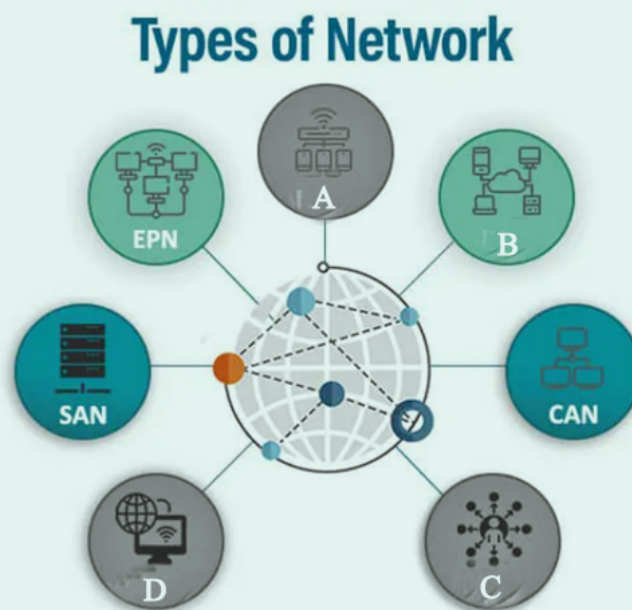


Figure 3.20: Types of networks

2. Select your group leader and secretary.
3. The secretary should write report on the activity.
4. Identify and match the types of networks labelled A, B, C, D to MAN, LAN, PAN, and WAN in the diagram.
5. Select any of the labels identified and matched in (d) above.
6. Explain the selected network area type in your own words.
7. Explain the main features of these area networks you selected.
8. Use the computer, create PowerPoint Slide of the report.
9. Group leader should present the report to the class.

Activity 3.5

Let us look at the diagrams below.

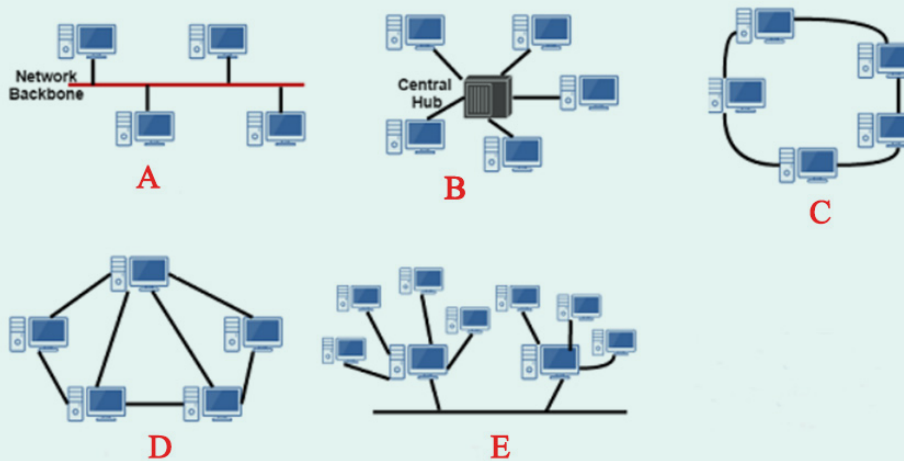


Figure 3.21

Individually, perform the activities that follow:

1. What name best suits the whole diagram above?
2. Identify the diagrams labelled A, B, C, D and E.
3. Describe each of the identified labels.
4. State and explain the advantages and disadvantages of each of the labels.

DIFFERENCES BETWEEN DIFFERENT TYPES OF NETWORKS

These notes will only look at the differences between the three types of area networks, LANs, MANs, and WANs. Other criteria other than those given in the Table 3.1 can be added when comparing these networks as we will see in later weeks. See Figure 3.19 for the range of these networks.

Table 3.1: Table showing the difference between the types of networks

Criterion	LAN	MAN	WAN
Area	A network that connects devices in a small geographic range.	A network that connects large areas than LANs such as small towns or cities.	The network covers a large area such as a country or several countries.
Example	School network	University network	Internet, ATM network
Ownership	Private	Public or private	Public or private
Topology	Star, Bus, or Ring	Ring, Mesh, hybrid	Point-to-point, Mesh
Transmission speed	High	Moderate	Low
Fault tolerance	More fault tolerance	Less fault tolerance	Less fault tolerance
Maintenance	Easy to maintain as has a less complex structure	More complex structure than LAN and is also more difficult to maintain.	Maintenance and the design structure is more complex compared to LAN and MAN.
Congestion	Less	More	More

Point-to-point networks are used to connect two locations together via a private, dedicated line.

Activity 3.6

In your group, do the following:

1. Select your group leader and secretary.
2. The secretary should write a report on the activity.

3. Each member should pick one of the following topologies: Bus, Star, Mesh, Ring, Tree, and Hybrid.
4. Explain in your own words the type of topology you picked.
5. Explain the main features of each type of topology.
6. Use the computer to create a PowerPoint slide of the report.
7. The group leader should present the report to the class.

Activity 3.7

Do the following:

1. Individually, think of possible criteria to compare different types of area networks such as geographical area and ownership.
2. Get into your groups,
3. Share your individual views with your members.
4. Settle on the five (5) most appropriate ones.
5. Fill in Table 3.2 with the five (5) criteria under criterion with aid of computer and PowerPoint application.
6. Complete the table with the differences between these four area networks under the criterion identified.
7. Present your results to the class with PowerPoint presentation.

Table 3.2: Comparing different types of area networks

Criterion	PANs	LANs	MANs	WAN

NETWORK ARCHITECTURE

Take a look at the classroom, just like how a classroom is organised with desks, chairs, students, and a teacher, computer networks are also arranged in a specific way to make sure everything runs smoothly. We will learn about the world of Computer Architecture and Organisation, focusing on data communication and network systems. We will find out how networks are designed and managed, reveal the secrets behind client-server and peer-to-peer models.

Picture the network as a well-organised classroom: the teacher is like the server, providing information and resources to the students (the clients). In another setup, students might share and exchange information directly with each other, much like a peer-to-peer network. As we journey through this topic, you will gain a practical understanding of how data travels across networks, ensuring seamless communication in our digital world.

Let us take a look at the network architecture and the two most common models, client-server and peer-to-peer models.

What is Network Architecture?

This refers to the way network devices and services are structured to serve the connectivity needs of the user devices. This includes the hardware, software, protocols, and configurations used to create and manage the network. There are several types of network architecture, each serving different purposes and catering to specific needs. Two of the most common models are client-server and peer-to-peer.

1. Client-Server Architecture

In this architecture, devices on the network are divided into two categories: clients and servers. Clients (e.g., computers, smartphones) request services or resources from servers (e.g., access to webpages from a web server, access to files from a file server). Servers respond to client requests, and this model allows for centralised management and resource sharing. Servers tend to be quite powerful machines. They need the processing power because many other computers connect to them. Clients may not store data, and they have no control over the network as a whole.

Because this model is centralised, it is more secure and easier to back up data. It is suitable for both small and large networks and for situations where many computers need access to the same information. Many schools use this model. Client-server networks are generally more stable than P2P networks but can cost more due to the infrastructure and maintenance required.

2. Peer-to-Peer (P2P) Architecture

In this architecture, all devices on the network are considered equal peers, capable of both requesting and providing resources (i.e., acting as both a client and a server). There is no central server. Each device can directly communicate, request and provide services to other devices on the network, which makes it a decentralised network.

P2P typically is used for smaller networks, often with fewer than 10 computers, or where fewer computers need access to the same data. It is less expensive and easy to set up compared to client-server networks. However, they can be less stable as the number of peers increases and may have security challenges since each node has equal authority.

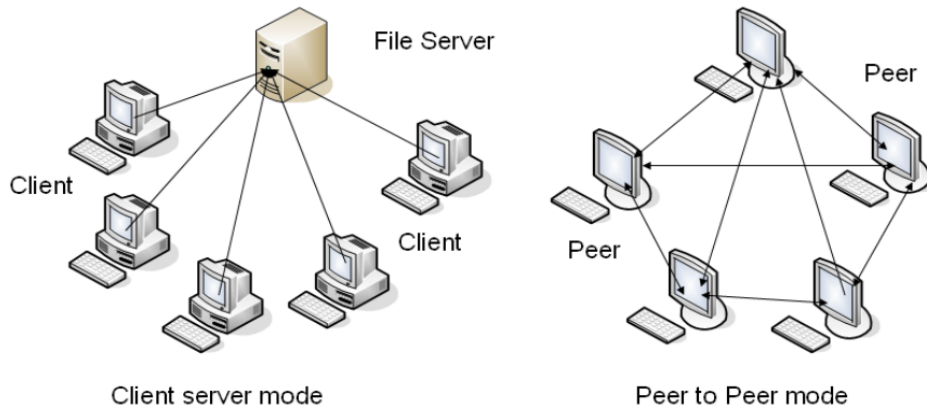


Figure 3:22 Two types of computer architecture

Note the link between network topology and network architecture. Network topology is the practical implementation of network architecture. *A network topology is the arrangement of different elements within the network, including devices like routers, switches, and computers, whereas network architecture refers to the design and physical structure of a computer network.*

CLOUD NETWORKS

The **CLOUD** refers to servers that are accessed over the internet, and the software and databases that run on those servers. Cloud servers are located in data centres all over the world. In a cloud network, the network is on-premises, but some or all resources used to manage it are in the cloud and these resources are rented from a third-party cloud provider/ cloud vendor. Cloud networking is the infrastructure that supports cloud computing, which is the delivery of various services through the Internet. It involves a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

A cloud network can employ a client-server architecture. In this model, the cloud acts as the server that provides resources and services, and the clients (which can be end-user devices like computers, smartphones, etc.) request and consume these services. The cloud-based delivery of services ensures that clients can access resources on-demand via the Internet.

The client-server architecture in a cloud environment is designed to be easily scalable and efficient, allowing for a robust network that can handle varying workloads and provide services to a large number of clients simultaneously.

With cloud networking, an organisation can shift its network management, control, and data connectivity from on-premises to a cloud infrastructure. Cloud networking allows organisations to create complex networks using only the internet.

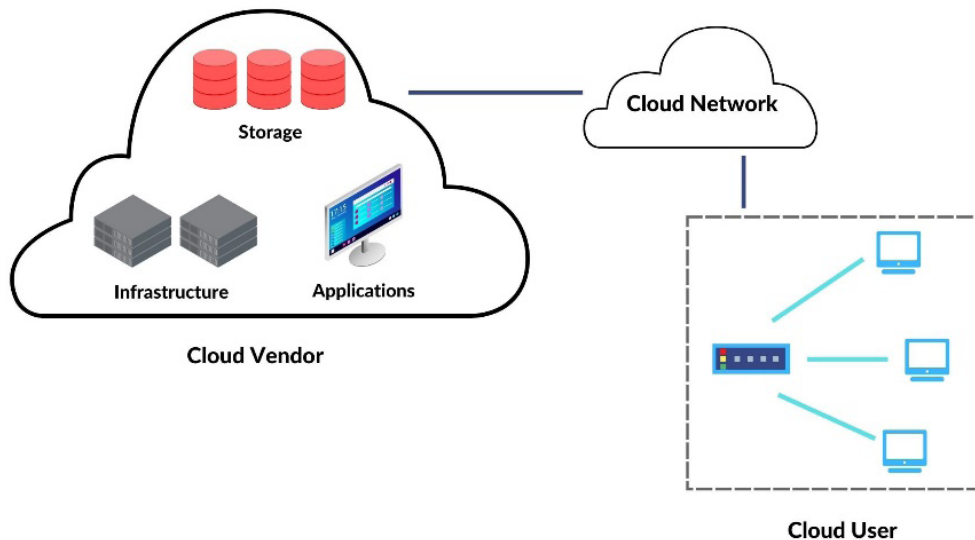


Figure 3.23: Cloud networking

OSI MODEL - What is it?

Networking is a vast and often complex topic. The OSI model helps us better understand it. The **OSI model** describes how a network functions and gives a reference framework (a set of rules) that explains the process of transmitting data between network devices. It is essentially a blueprint for a network architecture that standardises the way the nodes send data to each other.

This model makes use of what is called in networking, a layered architecture. In the OSI model, the process of communication between two devices on a network can be divided into seven distinct groups of related functions, or layers, with each layer having a specific job.

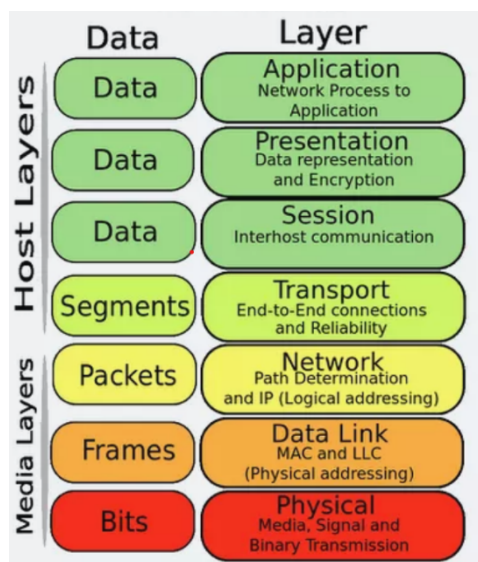


Figure 3.24: OSI Model Layers

From highest level to lowest level the seven levels of the OSI model are:

Layer 7: The Application Layer

Layer 6: The Presentation Layer

Layer 5: The Session Layer

Layer 4: The Transport Layer

Layer 3: The Network Layer

Layer 2: The Data Link Layer

Layer 1: The Physical Layer

The **Physical Layer (Layer 1)** is responsible for the transmission and reception of raw data bits over a physical medium, such as wires, optical fibres, or wireless signals.

The **Data Link Layer (Layer 2)** manages node-to-node data transfer and handles error detection and correction during the transmission between two physically connected devices.

The **Network Layer (Layer 3)** is responsible for routing data packets between different networks, this layer determines the best physical path for data to travel from source to destination.

The **Transport Layer (Layer 4)** ensures complete data transfer by providing end-to-end communication, error recovery, and flow control between devices, often using protocols like TCP or UDP.

The **Session Layer (Layer 5)** manages and controls the connections between devices, establishing, maintaining, and terminating communication sessions.

The **Presentation Layer (Layer 6)** converts data between the application layer and the lower layers, ensuring that data is in a usable format, and handling encryption and compression.

The **Application Layer (Layer 7)** provides network services directly to the user or application software, such as email, file transfer, and web browsing, facilitating end-user interaction with the network.

A possible mnemonic for remembering the names of the layers (highest to lowest) is: *A Penguin Said That Nobody Drinks Pepsi*

Why the OSI model is used?

Before the OSI model, each company had its own packet structure or data structure, which meant that peripherals of different companies were not compatible. For example, if you have a computer made by company A, then you need to buy peripherals such as a printer from company A. So, the International Organisation for Standardisation (ISO) decided that data had to go in a particular manner from one place to another place to overcome this issue. This is where the reference model (OSI model) came into being. ISO decided that when data goes from one place to another place it has to go through the layers of the OSI model so that others can also understand it.

Activity 3.8

1. In small groups perform the following activities in class
 - a. Research using the internet the differences between client/server and P2P networks in a school environment using agreed-upon criteria discussed in class.

Hint: Use the table below as a guide for (i).

Table 3.3: The differences between client/server and P2P networks

Criterion	CLIENT/SERVER	P2P NETWORKS
Typical uses		
Security		
Data Management		
Scalability		
Reliability		
Maintenance		
Cost		

- b. State the network model which would be more suitable for managing student and teacher data securely
 - c. Give the reason for your response in (ii) above.
2. In groups, Create an engaging presentation of each focal area:
 - a. Network architecture models
 - b. client-server
 - c. P2P
 - d. Cloud networks
 - e. The OSI Model
3. As a group, you will role-play the seven layers of the OSI model to demonstrate how data is sent from one computer to another.
 - a. Form a group of seven.
 - b. Assign each of the seven students one layer of the OSI model.
 - c. Each group should prepare a brief explanation of their layer's functions, including how it interacts with the layer above and below.
 - d. Consider using diagrams, or cards to help illustrate the data flow and transformation at each level.

WIRELESS DATA CONNECTIONS

Instead of connecting computers to peripheral devices or to another computers through ports and connectors, wireless communications technologies are used. Wireless media offer mobility and flexibility but they can be affected by environmental factors and have limited range and security concerns. This type of connection uses radio waves or other wireless technologies to communicate between devices.

There are many types of wireless technologies. They differ in various ways including frequency and modulation.

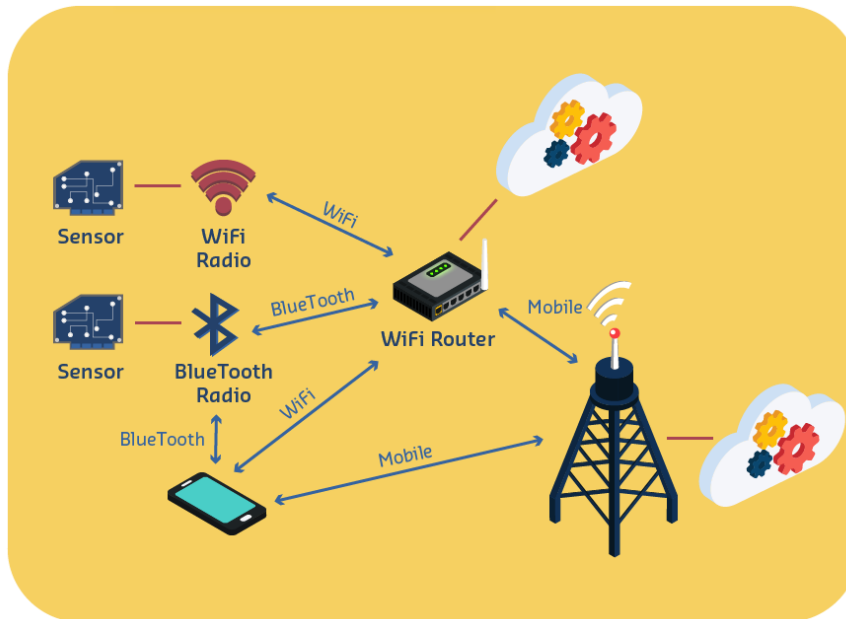


Figure 3.25: Wireless Technologies

Let us look at some of these technologies.

1. Bluetooth

Bluetooth technology uses short-range radio signals to transmit data between two Bluetooth-enabled computers or devices. In addition to computers, mobile devices and many peripherals' devices, such as a mouse, keyboard, printer, or headset, and many vehicles and consumer digital devices are Bluetooth enabled. The range of a Bluetooth connection is approximately 10 meters (30 feet). However, maximum communication range will vary depending on obstacles (such as person, metal, storm, or wall) or the electromagnetic environment. The range may be able to be extended with additional equipment. If you have a computer that is not Bluetooth enabled, you can purchase a Bluetooth adapter that will give a computer the ability to connect to Bluetooth devices either via an internal card (for a desktop computer), or a USB adapter.



Figure 3.26: Bluetooth Pairing Device

2. Near Field Communication (NFC)

NFC uses close-range radio signals to transmit data between two NFC-enabled devices. Examples of NFC-enabled devices include many smartwatches, most smartphones, and some digital cameras, computers, point of sales devices, ATMs, and smart televisions. Other objects, such as contactless debit and credit cards, and contactless travel cards, also use NFC technology. For successful communications, the devices either touch or are within a distance of 4 centimetres (1.6 inches) of each other.



Figure 3.27: Payment via credit card using NFC

3. Infrared (IR)

Infrared connectivity is a wireless technology that uses a beam of infrared light to transmit information. It is used for short-range or medium-range communications between two devices. IR communication is among the simplest wireless communication methods and serves as a cost-effective way of transmitting a few bits of data wirelessly. It requires direct line of sight and operates only at close

range. This is not particularly common nowadays for data transfer due to the very slow speeds, and the requirement for short distance line of sight.



Figure 3.28: Infrared devices

NOTE: Wireless Technologies used by Wireless Personal Area Networks (wPANs) include Bluetooth, NFC, IR

4. Wireless Fidelity (Wi-Fi)

Wi-Fi uses radio signals that conform to certain standards. Computers and devices that have the appropriate Wi-Fi capability can communicate via radio waves with other Wi-Fi computers or devices. Most computers and mobile devices are Wi-Fi enabled, or can have this added, along with routers and other communications devices. The reach of your signal will be impacted by the manufacturer of the equipment that you are using, the location where your router is installed, and the obstructions that might block the signal in your home or business.

Routers set to a 2.4Ghz frequency that are correctly placed should offer you coverage for about 45 metres (150 feet) indoors and about 91 metres (300 feet) outdoors. Routers set to a 5GHz frequency that are correctly placed should offer you coverage for about 15–30 metres (50–100 feet) indoors and about 45 metres (150 feet) outdoors, while routers on a 6GHz frequency typically offer similar or slightly reduced coverage indoors, with about 9–15 metres (30–50 feet) outdoors.



Figure 3.29: WiFi enabled devices

5. Cellular Communication

A cellular wireless network, often referred to as a mobile network, is a communication system that enables wireless communication via radio and microwave signals over a wide geographic area using cell towers. They enable smartphones, tablets and other digital devices to connect to the internet through the nearest cell tower. This setup (referred to as cellular or mobile data) allows for mobility and convenience, as users can get online without being bound to a physical location (for Wi-Fi you need to be located near a router to get an internet connection). You just need to be within the coverage area of the cellular network to connect to the internet. It is particularly useful for those who travel or work remotely. The first commercial cellular network, the 1G generation, was launched in Japan in 1979. 5G or the fifth-generation technology standard for cellular networks, began deployment worldwide in 2019. 5G has several advantages over 4G, including wider bandwidth resulting in faster speeds and greater capacity .



Figure 3.30: Cellular Communication

6. Satellite Communication

Satellite communication involves transmitting data signals to and from satellites in space. It is commonly used for long-distance communication in remote areas and for global connectivity. This is now becoming more and more common as mobile phones adapt the technology for emergency use when phone signal is not available. In recent years satellite-based internet has become mainstream under the name Starlink, providing fast internet to areas that previously would not have had access to it.

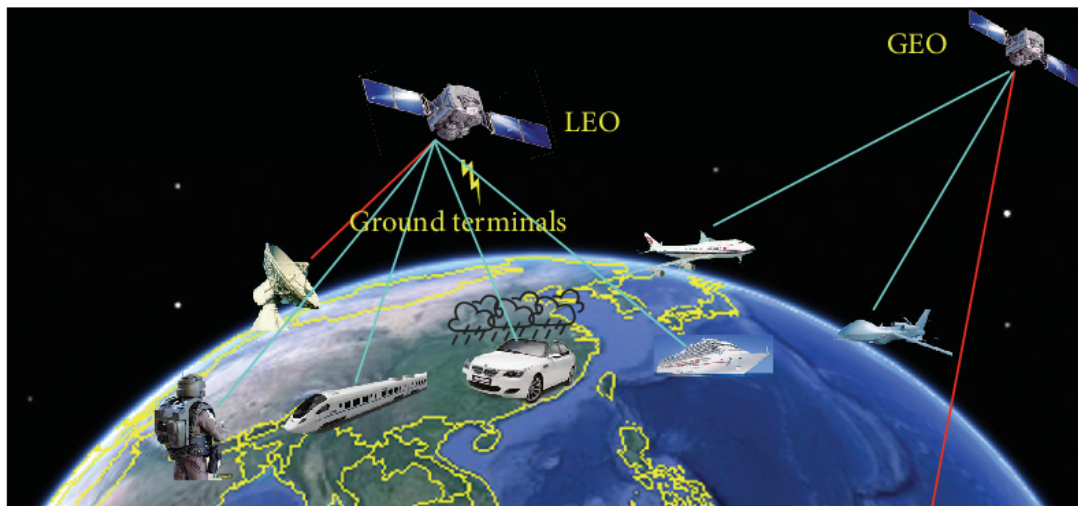


Figure 3.31: Satellite Communication

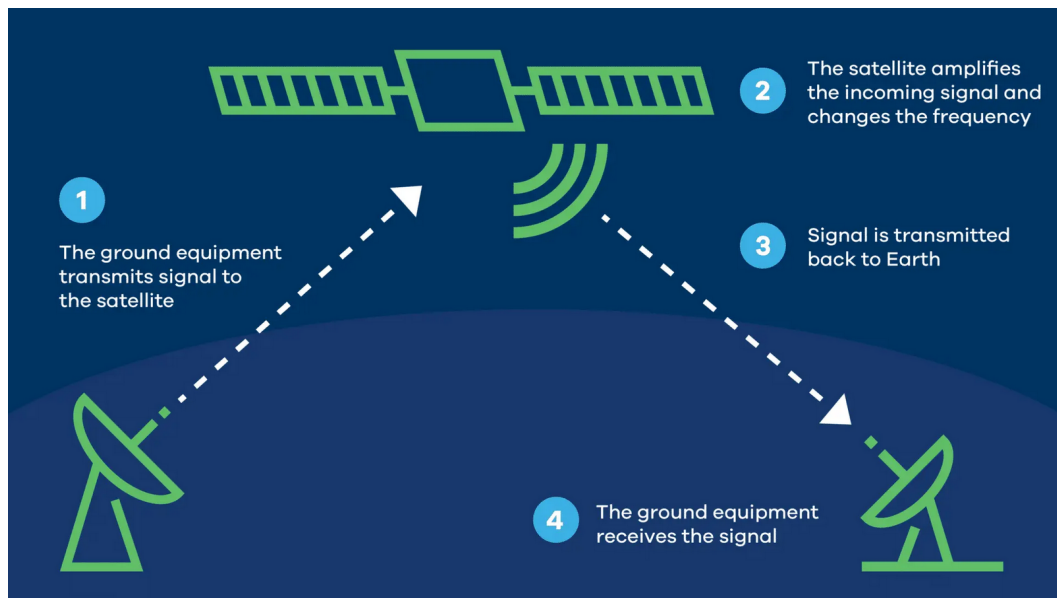


Figure 3.32: Picture showing how satellite communication is established

Wireless Metropolitan Area Networks (wMANs) use various wireless technologies, the most common being WiMAX and LTE.

Wireless Wide Area Networks (wMANs) use various wireless technologies, including cellular network and satellite.

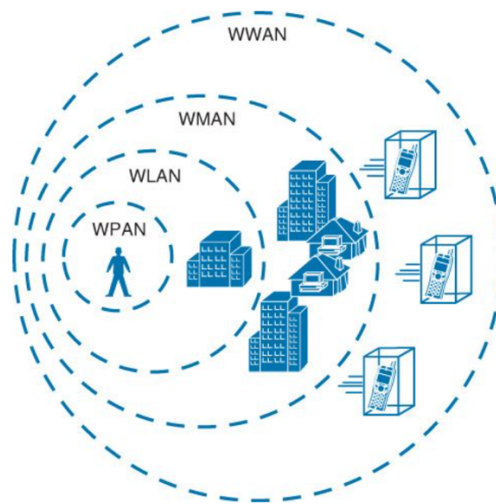


Figure 3.33: Picture showing how wireless network ranges

Activity 3.9

1. Perform the following task in group
 - a. Each group is assigned one of the following wireless transmission medium: Bluetooth, NFC, Infrared, WiFi, Cellular Communication and Satellite Communication.
 - b. Use the internet to get information to show how the assigned wireless transmission medium works, using videos, models or diagrams.
 - c. Your report should show their characteristics, advantages, disadvantages, and common use cases.
 - d. Make a power point presentation on the report to the class
2. Your mum has come to you to teach her how to send an audio from her phone to your auntie's phone.
 - a. Which wireless transmission media will you use and why?
 - b. Describe the steps which you will take to share the audio

WIRED DATA CONNECTIONS

Let's talk about wired connections. Wired connections use physical cables to transfer data between devices. This type of connection is known for being fast, reliable, and secure. These connections are often used in places where stable and high-speed internet is crucial, like offices and homes. Now, let's take a closer look at the different types of wired connections, their applications, each with its advantages and limitations.

There are also a number of different wired computing technologies, one of the most common being Ethernet. Ethernet can be considered a network protocol that controls how data is transmitted over cables. An Ethernet cable (layer 1 Physical layer of the

OSI model) plugs into a network interface card (NIC) which handles the Layer 2 Data Link functionality. Effectively, Layer 2 is responsible for putting 1's and 0's on the cable and pulling 1's and 0's from the cable.

Ethernet cables are commonly used in LANs, MANs and WANs. The original 10 base 5 Ethernet used a thick coaxial cable. More modern Ethernet variants use twisted pair, but more recently fibre optic has become more common for high speed over longer distances.

1. Twisted Pair Cable

A twisted pair cable is a widely used cable for transmitting data and information over certain distances. A twisted pair cable consists of two separate insulated copper wires that are twisted together within a wrapping shield and run parallel with each other. This helps to reduce the crosstalk or electromagnetic induction between the pair of wires. They come in categories like Cat5e, Cat6, Cat7 and Cat8. Cat6 cables are commonly used for high-speed Ethernet data transmissions in modern networks with a data rate of 10Gbps. Cat7 cables with a data rate of up to 100Gbps are more suited to data centres than residential applications.

There are two types twisted pair cables

a. Unshielded twisted pair (UTP)

Commonly used in LANs, UTP cables have twisted pairs of copper wires and come in categories like Cat5e and Cat6. UTP cables are small in diameter but unprotected against electrical interference.

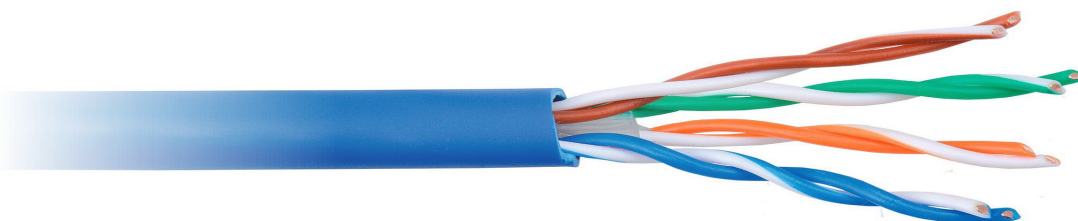


Figure 3.34: Unshielded twisted pair cable

b. Shielded twisted pair (STP)

This is a type of twisted pair cable that contains an extra wrapping foil or copper braid jacket to protect the cable from defects like cuts, losing bandwidth, noise, and signal to the interference. It is a cable that is usually used underground and is more costly than UTP. It supports higher data transmission rates across a long distance.

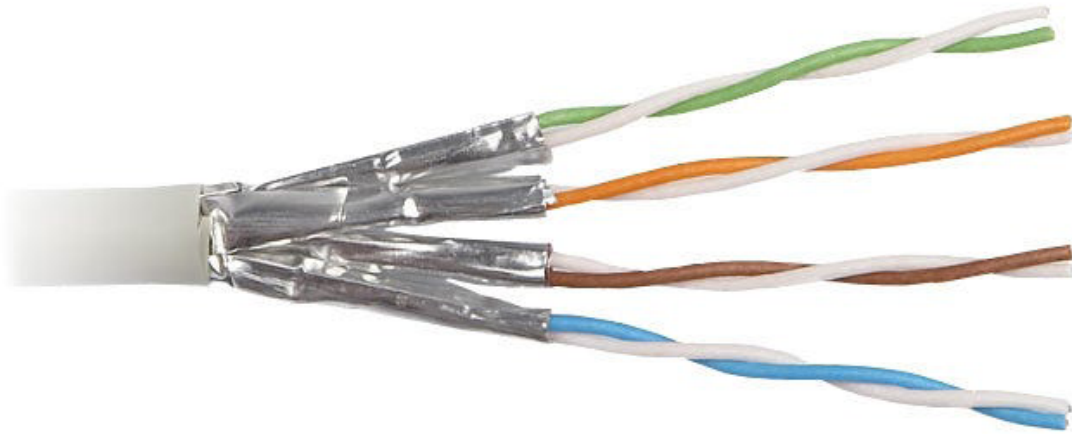


Figure 3.35: Shielded Twisted Pair Cable

2. Coaxial Cable

This is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It consists of a copper conductor surrounded by insulation, a braided metallic shield, and an outer jacket. These cables were commonly used for older Ethernet networks (e.g. 10Base2 and 10Base5). Coaxial cables have good bandwidth and resistance to interference but are bulky and less flexible compared to twisted pair cables.



Figure 3.36: Coaxial Cable

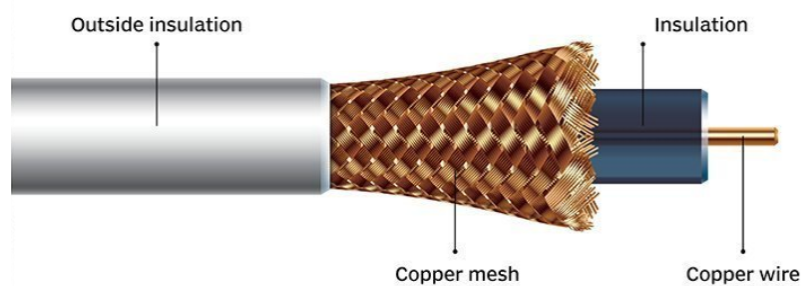


Figure 3.37: Coaxial cable with labels

A common use of coaxial cable in networking today is for connecting a cable modem to an Internet Service Provider (ISP), and for cable broadband internet. They are also used in automobiles, aircraft, military and medical equipment, as well as connecting satellite dishes, radio and television antennas to their respective receivers.

3. Fibre Optic Cable

Fibre optic cables use strands of glass or plastic to transmit data as pulses of light. They offer high bandwidth, long-distance transmission capabilities, and immunity to electromagnetic interference. Fibre optic cables are commonly used in high-speed networks, telecommunications, and data centres.

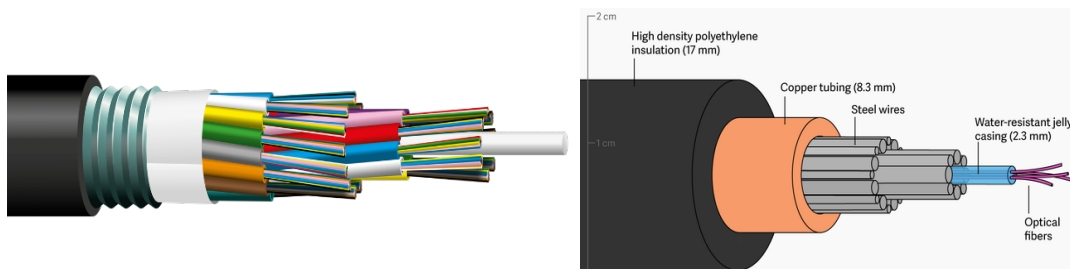


Figure 3.38: Fibre Optic Cable

4. Power Line Communication (PLC)

Power Line Communication uses a building's existing electrical system as the transmission medium and regular wall outlets as connecting points. It is commonly used to extend a wired Ethernet network into another room. You can form a Powerline network wherever there are power outlets, eliminating the need for expensive and complicated Ethernet cables. They depend entirely on the quality of the wiring within a building and are not guaranteed to work.

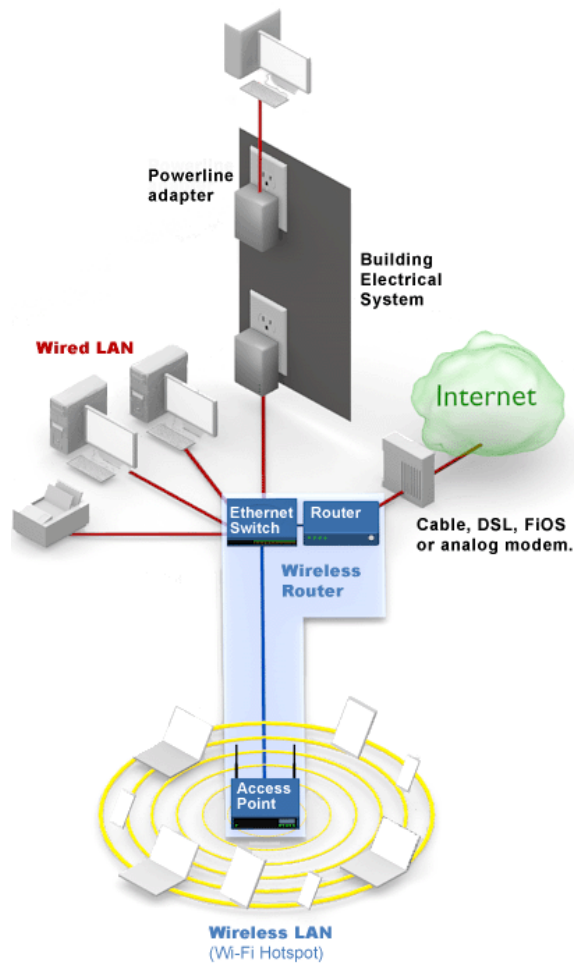


Figure 3.39: Power Line Communication

Advantages of PLC

1. Easy to set up: no cabling required, just plug and go
2. Large Reach: PLC can enable communication with hard-to-reach nodes by cable or where Wi-Fi signals might be weak or compromised

Disadvantages of PLC

1. Lower speed – the maximum speed is generally lower than Ethernet.
2. Can be impacted by electrical interference, for example such as from tumble dryers or microwaves
3. Powerline adaptors must be plugged into a wall and, usually do not work when plugged into extension cords. This means that users will have fewer electrical outlets available for other uses.

Activity 3.10

1. Perform the following task in the group
 - a. Each group is assigned one of the following wired transmission medium: twisted pair cables coaxial cable, fibre optic cable, power line communication
 - b. Using videos, models or diagrams, use the internet to get information to show how the assigned wired transmission medium works.
 - c. Your report should show their characteristics, advantages, disadvantages, and common use cases.
 - d. Make a PowerPoint presentation on the report to the class
2. In your group,
 - a. use the internet and find out two network transmission media from STP, UDP, Fibre optic, and coaxial.
 - b. create a comparison table between the two media in your exercise book or the Word processing application.
 - c. Show the answer to your teacher.

Comparing Different Network Cabling

Table 3.4: Comparing Different Network Cabling

Characteristics	Twisted pair cable	Co-axial cable	Optical fibre cable
Signal transmission	Takes place in the electrical form over the metallic conducting wires.	Takes place in the electrical form over the inner conductor of the cable.	Takes place in an optical form over glass fibre
Installation and Implementation	Simple and easy	Relatively difficult	Difficult
Cost	Very low	Moderate	Expensive
Diameter	Larger than optical fibre cable.	Larger than optical fibre cable.	Small diameter
Bandwidth	Low bandwidth.	Moderately high bandwidth.	A very high bandwidth.
Electromagnetic interference (EMI)	UTP susceptible to external interference	EMI is reduced due to shielding.	EMI is not present.
Attenuation ¹	Very high	Low	Very low
Noise immunity ²	Low noise immunity.	Higher noise immunity.	The highest noise immunity.

Characteristics	Twisted pair cable	Co-axial cable	Optical fibre cable
Repeater ³ Spacing	Repeater spacing is 2-10 km.	Repeater spacing is 1-10 km.	Repeater spacing is 10-100 km.

¹Attenuation is the reduction in the strength of a signal.

²Noise immunity is the ability to perform its functions when interference (noise) is present.

³A repeater on a network is a node that amplifies incoming signals and rebroadcasts them.

Conclusion

Each type of cable has its own unique features and is used for different purposes. Twisted-pair cable is the most common and cheapest option, Co-axial cable has a higher bandwidth and is used for high-speed connections, and optical fibre cable is immune to electromagnetic interference and has a very high bandwidth over long distances. The choice of cable depends on factors such as data transfer speed requirements, distance, cost, environment, and the type of network being deployed.

Wired Networks versus Wireless Networks


Table 3.5: Wired Networks versus Wireless Networks

	Wired networks	Wireless networks
Cost	Installation costs can be expensive	Cheaper to set up, devices can connect if in the range of a wireless access point
Installation	Installation requires technical knowledge and space to install cables	Installation is quick and simple as most wireless devices will connect automatically A solution for outdoor locations that are impossible for cabling.
Maximum transmission speed	Up to 10 Gbps for Ethernet (Cat6)	Up to 50 megabits per second
Maximum distance for reliable communication	Up to 100 metres for Ethernet. 40 to 100 kilometres for fibre optic (single mode)	Up to 50 metres
Security of connection	More secure as a physical connection is required to intercept data	Less secure as wireless signal cannot be contained within a building and no physical connection is needed to intercept data

Activity 3.11

1. In your groups Complete the Table 3.6 below

Table 3.6: Terms and their descriptions

TERM	DESCRIPTION	EXAMPLES
Bluetooth	A short-range wireless technology standard for exchanging data between fixed and mobile devices over short distances.	
NFC		
INFRARED		
Wi-Fi		
Bluetooth		
Unshielded twisted pair cable		
Shielded twisted pair cable		
Fibre optic cable		
Coxial cable		
Cellular communication		
Satellite communication		
Power line communication		

2. Complete the concept map on the content of this section with the title ‘Computer networks.

Instructions:

- Name the first node as the header or starting point of the map titled “Computer Networks”
- Name the nodes in orange respectively “Wireless Data Connection” and “Wired Data Connection”
- From each node created above in (b), add the name of the data connections respectively in grey colour as children’s nodes from (b)

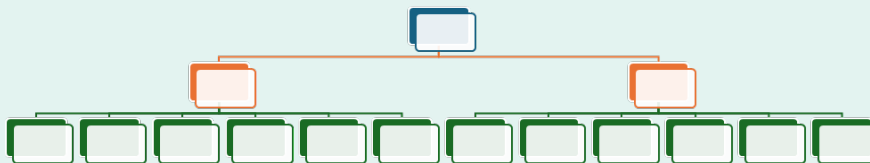


Figure 3.40

EXTENDED READING 3.1

1. Will ChatGPT replace network engineers? Discuss.
2. Investigate the impact of implementing AI in computer networks.

EXTENDED READING 3.2

1. Another type of area network is a Storage Area Network (SAN). Go online and find out this type of network and complete a report summarising your findings.
2. Use the link attached, find out and write a short analysis on how the internet of things (IoT) is impacting networking.
3. Read more on types of Network Topology from InterviewBit through the link <https://www.interviewbit.com/blog/types-of-network-topology/>
4. Assess the impact on network activity when adding or removing a node in a ring topology.

EXTENDED READING 3.3

1. Click on the link <https://www.youtube.com/watch?v=aDf7mteQu3Q&pp=ygUac2tpbGxzIGJ1aWxkIHRoZSBPU0kgTW9kZWw%3D> for **Video-Assisted Learning (VAL)** to know more about the OSI model.
2. Go online, learn about file server, print server, email server, web server, database server, proxy server, DNS server, cloud server, and application server and create a short summary of the function of each server. Present the summary to your fellow students and teacher in class.
3. Design a secure network for the school's computer lab. Choose between client-server and peer-to-peer architectures.
4. Do some research on three main types of cloud computing services: Infrastructure-as-a-Service (IaaS), Platforms-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Create a short report summarising your research findings.
5. Microsoft Azure and Amazon Web Services (AWS) are the two main cloud service providers. Investigate these two vendors and summarise the services that they provide and what they charge.

EXTENDED READING 3.4

1. Evaluate the relative advantages and disadvantages of a given data transmission medium in terms of its suitability for specific network architectures, such as LANs, WANs, and MANs.
2. Investigate edge computing and how it reduces latency and bandwidth usage in data communications.
3. Watch the video below and state where they can be used and its advantages.

- a. <https://www.youtube.com/watch?v=Gh2KRiSbGGE>
4. Scan this QRcode for more information on connecting a phone to a Wi-Fi Network



Review Questions 3.1

1. Which of the following best describes a node?
 - a. An Ethernet cable
 - b. Any device connected to a network
 - c. A type of network switch
 - d. The internet
2. HTTP is an example of which of the following?
 - a. Hardware
 - b. Software
 - c. A protocol
 - d. Multimedia
3. Describe one similarity and one difference between a switch and a router.
4. Krachi Senior High School located at Krachi needs five computers for its five departments to perform their day-to-day work which includes the processing and printing of letters and share students' records, scores and reports.
 - a. Give a reason why a network rather than five stand-alone computers would save the school money.
 - b. Describe how using a network can save the school's time.
5. Create a slideshow with descriptions of the main functions of each of the following items of network hardware: NIC, modem, router, switch, hub, and WAP. Include images and video links in your slideshow.
6. The library of your school needs five computers to perform its day-to-day work which includes the processing and printing of documents, emailing memos, and book keeping records.
 - a. Give three reasons to recommend networking these computers.
 - b. List the additional items of hardware that are required to set up a network in the library.
7. A travel agency business called STC located at Kumasi in the Ashanti Region, has several branches in the same city.
 - a. Design a strategy for their network that would mitigate against data loss through malicious or accidental activity.
 - b. Describe a network scenario where a switch would not be required.

Review Questions 3.2

1. Look at the diagram below and answer the questions:

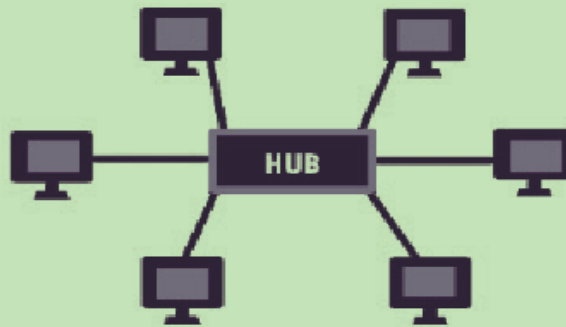


Figure 3.41

- a. Name the topology type used in this diagram.
 - b. What happens to the network if any of the computers fail?
 - c. What happens to the network if the central device (hub) fails?
2. Daniel Ishmael and Ama Golo were arguing about the differences between MAN and WAN but were not convinced of each other's answers. As a computing student who learnt types of computer network systems, settle the differences between them by describing two differences between a MAN and a WAN to them.
 3. Create a table in Word to show the difference between a PAN and a LAN in terms of coverage area and purpose.
 4. Dr. Yaw Afriyie is a Senior Lecturer and expert in Computer Networks at Simon Diedong Dombo - University of Business and Integrated Development Studies (SDD-UBIDS), Wa. As a student of computing, explain in your own words the differences between bus and star topologies to him. Use diagrams to support your explanation.
 5. Is GCB (Ghana Commercial Bank), including its 185 branch offices and ATMs an example of a MAN or a WAN? Justify your choice of area network.
 6. A network engineering firm called DM Technologies is setting up a local area network in their office block at Kete-Krachi, in the Oti Region of Ghana. It is required that 50 workstations across three floors need to connect to the network. There should also be the capacity to extend the number of workstations later. As a computing student,
 - a. Write an evaluation of the star, bus, and ring topology as possible topologies to use.
 - b. Recommend one of these topologies to DM Technologies with reasons for your choice.

Review Questions 3.3

1.
 - a. What are the possible benefits and risks involved in migrating your school's network to a cloud environment?
 - b. How would you address issues such as cost, security, and performance
2. Define a client-server architecture and explain the roles of clients and servers in this model.
3. Describe two advantages of a cloud network over a traditional network.
4. Evaluate the security implications of various network architecture designs, identifying potential vulnerabilities and recommending mitigation strategies.
5. Evaluate the cost efficiencies for an organisation switching to cloud networking.

Review Questions 3.4

1. Describe two advantages and one disadvantage of coaxial cabling over twisted wire cabling.
2. Why is coaxial cabling good for usage in situations where signals must be sent over great distances, such as cable TV networks?
3. Identify the similarities and differences of the physical properties, transmission characteristics, and applications of different types of data transmission media.
4. Analyse at least three factors that influence the choice of transmission medium when setting up a network.
5. Identify the type of Ethernet cable shown in Figure 3.43. Justify your answer.

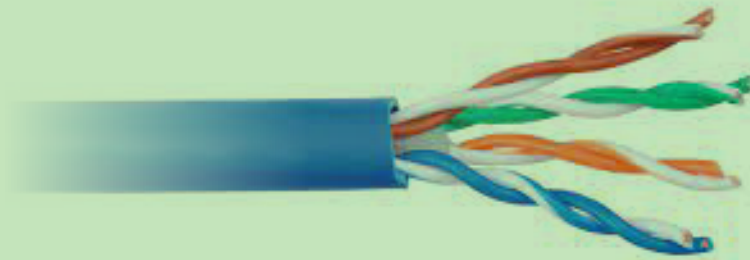


Figure 3.43

6. What activity and wireless technology are indicated in the image shown in Figure 3.44.



Figure 3.44

7. Study Figure 3.45

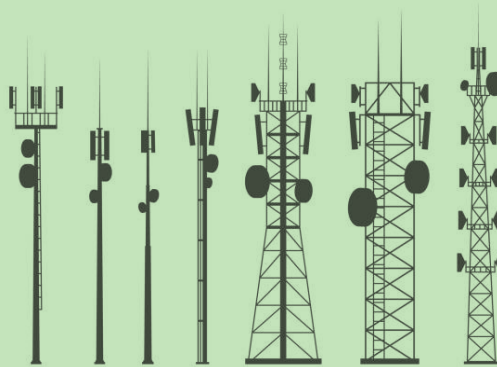


Figure 3.45

A cellular network uses these to enable mobile communication and provide internet access on digital devices such as smart phones. What are they?

Answers to Review Questions 3.1

1. b. Any device connected to a network
2. c. A protocol
3. **Similarity:** Both switches and routers are devices used in computer networks to manage and direct traffic. They are essential for ensuring data packets are efficiently transmitted from one device to another within a network.

Difference:

Switch: Typically used to connect multiple devices within the same LAN, such as computers, printers, and servers.

Router: Used to connect multiple networks together, allowing devices from different LANs or WANs to communicate with each other.

With a network setup, resources such as printers, scanners, and internet connections can be shared among all computers. This eliminates the need to purchase separate devices for each computer, thereby reducing hardware costs and this would help save money for the school.

4. Reason for saving money: A network allows the school to share resources like printers, software, and internet, reducing the need to purchase separate equipment for each computer.

Saving time: A network enables easy sharing of files and data between departments, reducing the time spent manually transferring information between computers.

5. **NIC:** Connects a computer to a network.

Modem: Converts digital data for transmission over telephone or cable lines.

Router: Directs data packets between different networks.

Switch: Connects devices within a LAN and forwards data based on MAC addresses.

Hub: Connects multiple devices within a LAN but does not manage traffic.

WAP: Provides wireless connectivity to devices within its range.

6. Three Reasons to Recommend Networking:

Resource Sharing: Networking allows the sharing of resources such as printers, scanners, and internet connections among all computers. This reduces the need for each computer to have its own separate devices, thereby saving costs on hardware and maintenance.

Improved Collaboration and Efficiency: Networking facilitates easier collaboration among employees. They can share documents and files seamlessly, which enhances productivity and reduces the time spent on transferring files manually or via external storage devices. Emailing customers becomes more efficient with a shared internet connection.

Centralised Data Management and Security: A network enables centralised data storage on a file server. This simplifies data backup procedures and ensures that important documents are securely stored and easily accessible to authorised personnel. Additionally, centralised security measures such as firewalls and antivirus software can be implemented to protect sensitive information from cyber threats.

Additional Items of Hardware Required to Set Up the Network:

- Network Switch
- Router
- Ethernet Cables
- Wireless Access Point (WAP) (Optional)
- Server (Optional)

7.

a. To mitigate data loss, STC should implement regular automated backups, both locally and in the cloud, along with strict access controls to limit data modification. They should also use antivirus software, firewalls, and encryption for secure data transmission. Employee training and network monitoring will help prevent and detect malicious or accidental data loss.

b. Why a Switch may not be required:

In a scenario where there are only two computers and a printer, and they can all connect directly to the Wi-Fi router, a separate switch is unnecessary. The Wi-Fi router already has built-in switching capabilities to manage the communication between the devices connected to it (computers and printer). Devices communicate with each other through the router, which routes data packets between the devices within the local network and manages the internet connection.

Answers to Review Questions 3.2

1.

- a. Star topology
- b. One computer failure does not affect the whole network, only that computer is affected and loose communication until it is repaired or replaced.
- c. If the central device (Hub) fails, then the whole network will be breakdown hence fail.

2. The differences between MAN and WAN include:

MAN	WAN
A network that connects large areas than LANs such as small towns or cities.	The network covers a large area such as a country or several countries.
Examples include university network	Examples include Internet, ATM network
Topology that can be used are ring, Mesh, hybrid	Topology that can be used are Point-to-point, Mesh
Transmission speed is moderate	Transmission speed is low

3. The differences between PAN and LAN in terms of coverage and purpose include:

Feature	PAN (Personal Area Network)	LAN (Local Area Network)
Coverage area	It is within a range of a few meters (around 10 meters)	It covers a larger area, from a single building to a group of buildings (up to several kilometres).
Purpose	Facilitates communication and data sharing among personal devices	Enables communication, resource sharing, and collaboration among multiple devices

4. Differences between bus topology and star topology

Feature	Bus Topology	Star Topology
Structure	Single central cable (bus)	Central hub or switch
Installation	Easier and less expensive	More complex and expensive

Feature	Bus Topology	Star Topology
Cable Requirement	Requires less cable	Requires more cable
Performance	Degrades with more devices; prone to collisions	Better performance with dedicated connections
Fault Tolerance	Difficult to isolate faults; entire network affected if bus fails	Easier to isolate faults; central hub failure affects entire network
Expansion	Difficult to expand	Easy to add new devices

Image of bus topology and star topology

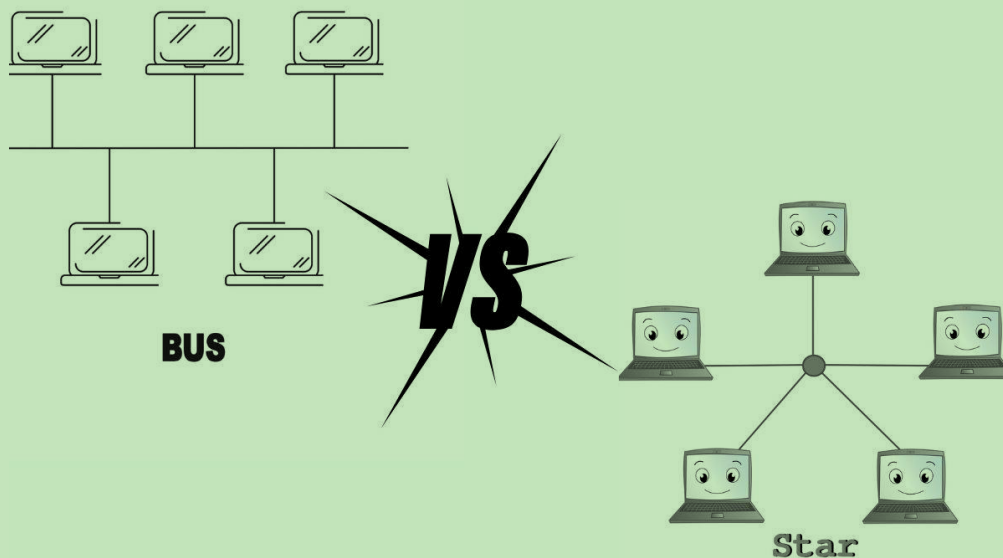


Figure 3.42

5. GCB (Ghana Commercial Bank), with its 185 branch offices and ATMs spread across the country, is an example of a Wide Area Network (WAN).

Justification:

a) Geographic Distribution:

Wide Area Network (WAN): WANs cover a large geographic area, often across cities, regions, or even countries. GCB's network spans the entire nation of Ghana, connecting branches and ATMs located in different cities and towns. This extensive geographic spread is characteristic of a WAN.

Metropolitan Area Network (MAN): MANs typically cover a smaller area, such as a city or metropolitan region. While GCB might have a MAN within a single city where multiple branches are interconnected, the overall network encompassing all branches across Ghana exceeds the scope of a MAN.

b) Interconnectivity:

WAN: WANs are designed to interconnect multiple local area networks (LANs) and MANs over long distances. GCB's branches and ATMs are interconnected through a network that links diverse geographic locations, fitting the description of a WAN.

MAN: A MAN might be used within a single city to connect branches within that urban area, but it would not encompass the entire national network.

c) Infrastructure:

WAN: WANs typically utilise leased telecommunication lines, satellite links, and other long-distance communication technologies to maintain connectivity over vast distances. GCB likely relies on such infrastructure to link its widespread branches and ATMs.

MAN: MANs often use high-speed fibre optics and other infrastructure suitable for city-wide connections, but these wouldn't be sufficient for a country-wide network.

Given the national reach of GCB's network, connecting branch offices and ATMs across Ghana, it is accurately categorised as a WAN. The network's need to cover extensive distances and interconnect diverse regional locations clearly fits the definition of a Wide Area Network.

6. Evaluation of the star, bus, and ring topologies, followed by a recommendation.

a. Star Topology

Advantages

- i.** Centralised Management: Easier to manage and troubleshoot due to the centralised hub or switch.
- ii.** Fault Isolation: A failure in one cable or workstation does not affect the rest of the network. Only the affected device is isolated.
- iii.** Scalability: Easy to add more workstations by connecting additional cables to the central hub or switch.
- iv.** Performance: Each device has a dedicated connection to the hub, reducing the chances of collisions and improving overall network performance.

Disadvantages

- i.** Cost: Requires more cabling and networking hardware (hubs or switches), which can be more expensive.
- ii.** Single Point of Failure: If the central hub or switch fails, the entire network goes down.

b. Bus Topology

Advantages

- i.** Cost-Effective: Requires less cabling compared to star topology, making it cheaper to implement.
- ii.** Simple Design: Easy to implement and extend with a single backbone cable.

Disadvantages

- i.** Performance Issues: As more workstations are added, the network can become slower and more prone to collisions.
- ii.** Fault Detection: Difficult to troubleshoot and isolate faults since a problem in the backbone cable can bring down the entire network.
- iii.** Limited Scalability: Adding too many devices can degrade performance and reliability.

c. Ring Topology

Advantages

- i.** Equal Access: Each device has equal access to the network, which can reduce the chances of collisions.
- ii.** Predictable Performance: Can perform better than bus topology under heavy load as data travels in one direction, reducing the chances of collisions.

Disadvantages:

- i.** Complexity: More difficult to install and configure compared to star and bus topologies.
- ii.** Fault Tolerance: A failure in any single cable or device can disrupt the entire network. However, some modern implementations use dual rings for redundancy.
- iii.** Scalability: Adding or removing devices can be more disruptive compared to star topology.

Recommended Topology: Star Topology

Reasons:

- 1. Scalability:** The star topology allows for easy expansion by simply adding more cables to the central hub or switch. This is particularly important for a network that needs to grow and accommodate more workstations in the future.
- 2. Fault Isolation:** In a star topology, a failure in one workstation or cable does not affect the entire network. This makes it easier to isolate and troubleshoot problems without bringing down the entire network.
- 3. Performance:** Each device in a star topology has a dedicated connection to the hub or switch, which helps maintain good performance even as more workstations are added. This reduces the likelihood of network collisions and congestion.
- 4. Management:** Centralised management via the hub or switch simplifies network administration, making it easier to monitor and manage network traffic.
- 5. Flexibility:** Star topology provides the flexibility to implement different network speeds and technologies for different floors or areas, which can be crucial in a multi-floor setup.

While star topology might have higher initial costs due to more cabling and the need for a central hub or switch, its benefits in terms of scalability, performance, and ease

of management make it the most suitable choice for connecting workstations across three floors with the capacity to extend the network in the future.

Answers to Review Questions 3.3

1.

a. Migrating the School's Network to a Cloud Environment

Benefits

- Scalability: Easily scale resources up or down based on demand.
- Cost Efficiency: Pay-as-you-go model reduces upfront costs and optimises spending.
- Accessibility: Access resources from anywhere with an internet connection.
- Disaster Recovery: Enhanced data backup and recovery solutions.
- Collaboration: Improved collaboration tools for students and teachers.

Risks

- Security Concerns: Potential vulnerabilities in cloud infrastructure.
- Data Privacy: Compliance with data protection regulations.
- Downtime: Dependence on internet connectivity and cloud provider uptime.
- Vendor Lock-in: Difficulty in switching providers or migrating data out of the cloud.

b. Addressing Issues

Cost

- Perform a cost-benefit analysis to compare on-premises vs. cloud costs.
- Use budgeting tools and cost management features provided by cloud services.

Security

- Choose a reputable cloud provider with strong security measures (e.g., Google Cloud, AWS, Microsoft Azure).
- Implement end-to-end encryption and strict access controls.
- Regularly audit cloud security policies and practices.

Performance

- Ensure adequate bandwidth and internet speed for cloud access.
- Use Content Delivery Networks (CDNs) to reduce latency.
- Monitor performance metrics and adjust resources as needed.

2. Client-server architecture is a network model where multiple clients (user devices) request and receive services from a centralised server.

Clients: Devices like computers or smartphones that initiate requests for resources or services, such as files, applications, or database access.

Servers: Centralised machines or systems that store, process, and manage resources, responding to client requests and delivering the required services.

3. Advantages of a Cloud Network Over a Traditional Network

Scalability:

Cloud Network: Cloud networks offer on-demand scalability, allowing businesses to easily adjust resources like storage, computing power, and bandwidth to meet changing needs. This is particularly beneficial for handling variable workloads and growth without significant upfront investments.

Traditional Network: In traditional networks, scaling up often requires significant investment in physical infrastructure, including hardware and software, which can be time-consuming and costly. This makes it less flexible and harder to adapt to changing business demands.

Cost Efficiency:

Cloud Network: Cloud services typically operate on a pay-as-you-go or subscription model, meaning businesses only pay for the resources they actually use. This reduces the need for large capital expenditures and ongoing maintenance costs associated with physical hardware.

Traditional Network: Traditional networks require significant upfront investment in physical infrastructure, including servers, storage devices, and networking equipment. Additionally, ongoing maintenance, upgrades, and energy costs can be substantial, making it less cost-efficient compared to cloud solutions.

These advantages make cloud networks a preferred choice for many modern businesses, offering flexibility, efficiency, and cost savings that traditional networks often struggle to match.

4. Security Implications of Various Network Architecture Designs

a. Client-Server Architecture

- **Potential Vulnerabilities:**

- **Single Point of Failure:** If the server is compromised or fails, the entire network can be affected.
- **DDoS Attacks:** Servers are susceptible to Distributed Denial of Service (DDoS) attacks, which can overwhelm the system.
- **Data Breaches:** If the server is hacked, sensitive data stored on it can be exposed.

- **Mitigation Strategies:**

- **Redundancy:** Implement failover servers and load balancers to distribute the load and ensure availability.
- **DDoS Protection:** Use DDoS protection services and rate limiting to mitigate attack impacts.
- **Strong Authentication:** Implement strong authentication and encryption methods to protect data.

b. Peer-to-Peer (P2P) Architecture

- **Potential Vulnerabilities:**

- **Security Risks:** Each peer can become a point of vulnerability, making the network harder to secure.
- **Data Integrity:** Ensuring data integrity can be challenging since data is distributed across multiple peers.
- **Malware Spread:** Malware can spread quickly across peers if one node is compromised.

- **Mitigation Strategies:**

- **Secure Protocols:** Use secure communication protocols and encryption to protect data transmission.
- **Regular Updates:** Ensure all peers have up-to-date security patches and antivirus software.
- **Monitoring:** Implement monitoring tools to detect and respond to suspicious activities.

c. Cloud Network Architecture

- **Potential Vulnerabilities:**

- **Data Breaches:** Sensitive data stored in the cloud can be targeted by hackers.
- **Account Hijacking:** User accounts can be compromised if proper security measures are not in place.
- **Insider Threats:** Employees with access to cloud resources can pose internal security risks.

- **Mitigation Strategies:**

- **Encryption:** Use encryption for data at rest and in transit to protect sensitive information.
- **Access Controls:** Implement strict access controls and multi-factor authentication (MFA) to secure user accounts.
- **Regular Audits:** Conduct regular security audits and monitoring to detect and respond to potential threats.

d. Hybrid Network Architecture

- **Potential Vulnerabilities:**

- **Complexity:** The integration of on-premises and cloud resources can create complex security challenges.
- **Data Sync Issues:** Synchronising data between different environments can lead to security gaps.
- **Inconsistent Policies:** Inconsistent security policies across environments can create vulnerabilities.

- **Mitigation Strategies:**
 - **Unified Security Policies:** Implement consistent security policies across both on-premises and cloud environments.
 - **Data Encryption:** Ensure data is encrypted during synchronisation and storage.
 - **Integrated Security Tools:** Use integrated security tools and platforms to manage and monitor the hybrid environment.

By understanding these potential vulnerabilities and implementing appropriate mitigation strategies, organisations can enhance the security of their network architectures and protect against various cyber threats.

5. Evaluating Cost Efficiencies of Switching to Cloud Networking

Switching to cloud networking offers several cost efficiencies for organisations. Below are the primary areas where organisations can realise savings:

i. Reduced Capital Expenditure

- **Traditional Network:**
 - Significant upfront costs for purchasing hardware (servers, storage devices, networking equipment).
 - Expenses related to setting up data centres, including space, power, and cooling.
- **Cloud Network:**
 - No need for large capital expenditures on physical infrastructure.
 - Costs are shifted to an operational expenditure model, paying only for the resources used.

ii. Operational Savings

- **Traditional Network:**
 - Ongoing maintenance and upgrades of hardware and software.
 - Hiring and retaining IT staff for managing and maintaining the infrastructure.
 - Energy costs associated with running and cooling data centres.
- **Cloud Network:**
 - Maintenance, upgrades, and infrastructure management are handled by the cloud service provider.
 - Potential reduction in IT staff costs or redeployment of IT staff to more strategic roles.
 - Lower energy costs as there is no need to run and cool local data centres.

iii. Scalability and Flexibility

- **Traditional Network:**

- Scaling up requires significant investment in additional hardware and software.
- Over-provisioning or under-utilisation of resources can lead to inefficiencies and wasted costs.

- **Cloud Network:**

- On-demand scalability allows organisations to quickly adjust resources based on demand, ensuring efficient use of resources.
- Pay-as-you-go pricing models ensure that organisations only pay for what they use, avoiding over-provisioning costs.

iv. Disaster Recovery and Business Continuity

- **Traditional Network:**

- High costs associated with setting up and maintaining redundant systems and disaster recovery sites.
- Complex and expensive to implement effective business continuity plans.

- **Cloud Network:**

- Built-in disaster recovery and business continuity solutions provided by cloud service providers.
- Reduced costs for backup and recovery infrastructure, with data often automatically replicated across multiple locations.

v. Software Licensing and Updates

- **Traditional Network:**

- Upfront costs for purchasing software licenses.
- Ongoing costs for software updates, patches, and renewals.

- **Cloud Network:**

- Many cloud services include software licenses in their subscription fees.
- Automatic updates and patches are typically included, reducing the need for manual updates and associated costs.

vi. Productivity and Collaboration

- **Traditional Network:**

- Additional investments in collaboration tools and infrastructure to support remote work and collaboration.

- **Cloud Network:**

- Many cloud services offer built-in collaboration tools, enhancing productivity without additional costs.
- Facilitates remote work with easy access to resources from anywhere, reducing the need for physical office space.

Answers to Review Questions 3.4

1. Advantages and Disadvantage of Coaxial Cabling over Twisted Wire Cabling

i. Advantages

- **Higher Bandwidth:** Coaxial cables can carry a higher bandwidth of data compared to twisted pair cables. This makes them suitable for applications requiring high-speed data transfer.
- **Better Shielding:** Coaxial cables have a central conductor surrounded by an insulating layer and a shield, providing better protection against electromagnetic interference (EMI) and radio frequency interference (RFI). This results in a more stable and reliable signal over longer distances.

ii. Disadvantages

- **Cost and Complexity:** Coaxial cables are generally more expensive and bulkier than twisted pair cables. The installation and maintenance can be more complex and costly, especially for large-scale deployments.

2. Coaxial cabling is effective for long-distance signal transmission due to its robust shielding, which minimises signal loss and interference. The cable's construction, with a central conductor surrounded by an insulating layer and metallic shield, ensures that signals maintain their integrity over extended distances. This makes it ideal for applications like cable TV networks, where signals need to be transmitted over vast areas without significant degradation.

3.

Aspect	Twisted Pair Cables	Coaxial Cables	Fibre Optic Cables	Wireless Communication
Physical Properties	- Two insulated copper wires twisted together.	- Central copper conductor.	- Core of glass or plastic fibres.	- Uses electromagnetic waves.
	- Shielded (STP) or Unshielded (UTP) options.	- Metallic shield and outer insulation.	- Cladding, buffer coating, and outer jacket.	- No physical cables.
	- Flexible and easy to install.	- Insulating layer.	- Thin, lightweight, and fragile.	- Requires antennas or transmitters and receivers.
		- Rigid and thicker than twisted pair.		

Aspect	Twisted Pair Cables	Coaxial Cables	Fibre Optic Cables	Wireless Communication
Transmission Characteristics	<ul style="list-style-type: none"> - Moderate data rates. - Susceptible to electromagnetic interference (EMI). - Maximum distance of 100 meters without signal booster. 	<ul style="list-style-type: none"> - Higher data rates than twisted pair. - Good resistance to EMI due to shielding. - Can transmit over longer distances than twisted pair. 	<ul style="list-style-type: none"> - Extremely high data rates. - Immune to EMI. - Can transmit data over very long distances without significant loss. 	<ul style="list-style-type: none"> - Variable data rates depending on technology (e.g., Wi-Fi, cellular). - Susceptible to interference from obstacles and other signals - Range depends on power and frequency.
Applications	<ul style="list-style-type: none"> - Local Area Networks (LANs) - Telephone lines - Short-distance communication. 	<ul style="list-style-type: none"> - Cable television (CATV). - Internet connections (broadband). - Long-distance video and data transmission. 	<ul style="list-style-type: none"> - Backbone networks. - Long-distance telecommunication. - High-speed internet and data connections. 	<ul style="list-style-type: none"> - Mobile networks (3G, 4G, 5G). - Wi-Fi and wireless LANs. - Satellite communication.

Summary of Key Differences

- **Twisted Pair Cables** are easy to install and cost-effective but have limited bandwidth and are susceptible to interference. They are ideal for short-distance, lower-speed applications like LANs and telephone lines.
 - **Coaxial Cables** offer higher bandwidth and better shielding against interference, making them suitable for applications such as cable TV and broadband internet that require longer distances and higher speeds.
 - **Fibre Optic Cables** provide the highest data rates and are immune to electromagnetic interference. They are the best choice for long-distance and high-speed data transmission, such as in backbone networks and high-speed internet connections.
 - **Wireless Communication** eliminates the need for physical cables and allows for mobile and flexible networking solutions. However, it can be affected by environmental factors and interference, making it ideal for applications where mobility and convenience are prioritised, like mobile networks and Wi-Fi.
4. When choosing a transmission medium for a networking scenario, several factors need to be analysed to ensure optimal performance, cost-effectiveness, and suitability for the specific requirements of the network. Here are three critical factors:
- Distance and Coverage Area**
The distance over which data needs to be transmitted significantly influences the choice of transmission medium:

- **Twisted Pair Cables:** Suitable for short distances (up to 100 meters) without signal boosters. Commonly used in Local Area Networks (LANs) within buildings.
- **Coaxial Cables:** Can transmit data over longer distances than twisted pair cables. Often used in Cable TV networks and broadband internet connections.
- **Fibre Optic Cables:** Ideal for long-distance transmission, capable of spanning several kilometres without significant signal loss. Used in backbone networks, long-distance telecommunications, and high-speed internet connections.
- **Wireless Communication:** Coverage area depends on the technology used (e.g., Wi-Fi, cellular networks). Suitable for both short-range (Wi-Fi) and wide-area (cellular networks) applications.

ii. Bandwidth and Data Transmission Rates

The required data transmission rate and bandwidth determine the appropriate medium to handle the expected network load:

- **Twisted Pair Cables:** Moderate data rates, suitable for typical LAN environments and office networks.
- **Coaxial Cables:** Higher bandwidth capabilities compared to twisted pair cables. Used for applications requiring higher data rates, such as video streaming and broadband internet.
- **Fibre Optic Cables:** Provides extremely high data rates and bandwidth. Ideal for applications demanding high-speed data transfer, such as data centres and high-performance computing networks.
- **Wireless Communication:** Data rates vary based on technology (e.g., Wi-Fi 6, 4G, 5G). Suitable for environments where mobility and flexibility are important, such as wireless LANs and mobile networks.

iii. Environmental Factors and Interference

The environment in which the network operates can impact the choice of transmission medium due to potential sources of interference and physical obstacles:

- **Twisted Pair Cables:** Susceptible to electromagnetic interference (EMI), especially in unshielded variants (UTP). Best used in environments with minimal EMI or where shielded cables (STP) can be employed.
- **Coaxial Cables:** Better protection against EMI due to shielding. Suitable for environments with moderate levels of interference.
- **Fibre Optic Cables:** Immune to EMI and radio frequency interference (RFI). Preferred in environments with high levels of electromagnetic noise, such as industrial areas or where high electrical interference is present.

- **Wireless Communication:** Susceptible to interference from physical obstacles (walls, buildings) and other electronic devices. Best suited for open environments or where the flexibility of wireless access outweighs potential interference issues.

iv. Additional Considerations

- **Cost:** The budget for the network infrastructure influences the choice, with twisted pair cables being the most cost-effective, followed by coaxial cables, and fibre optic cables being the most expensive. Wireless solutions can vary in cost depending on the technology and scale of deployment.
 - **Scalability and Future-Proofing:** Consideration for future network expansion and technological advancements. Fibre optic cables offer the highest scalability and future-proofing potential due to their high bandwidth capacity.
 - **Installation and Maintenance:** The ease of installation and ongoing maintenance requirements. Twisted pair cables are easier to install and maintain, while fibre optic cables require specialised skills and equipment.
5. Unshielded Twisted Pair (UTP) cable is commonly chosen as a wired data connection for several reasons, which make it a popular choice in many networking environments, especially for Local Area Networks (LANs). Here are the key reasons:

i. Cost-Effectiveness

- **Lower Cost:** UTP cables are generally less expensive than other types of cables like shielded twisted pair (STP) and coaxial cables. This makes them a cost-effective choice for large-scale network installations.
- **Widely Available:** The widespread use of UTP cables has driven down costs further due to economies of scale.

ii. Ease of Installation

- **Flexibility:** UTP cables are lightweight and flexible, making them easy to install and route through tight spaces, conduits, and around corners.
- **Standard Connectors:** They use standard connectors (RJ-45), which are easy to work with and widely supported by networking equipment.
- **Simple Termination:** Terminating UTP cables is straightforward and requires minimal specialised tools, unlike fibre optic cables that need precise splicing.

iii. Sufficient Performance for Many Applications

- **Adequate Bandwidth:** UTP cables provide sufficient bandwidth for most LAN applications. For instance, Category 5e (Cat 5e) and Category 6 (Cat 6) cables support speeds up to 1 Gbps and 10 Gbps, respectively, which is adequate for typical office and home networks.
- **Standardisation:** UTP cables conform to industry standards (such as TIA/EIA-568), ensuring compatibility and reliable performance.

iv. Minimisation of Electromagnetic Interference (EMI)

- **Twisted Pair Design:** The twisting of the pairs in UTP cables helps to cancel out electromagnetic interference (EMI) from external sources and crosstalk between adjacent pairs, improving signal quality and reliability.
- **Suitable for Low-Interference Environments:** While UTP cables lack the additional shielding found in STP cables, they perform adequately in environments with minimal EMI.

v. Versatility and Compatibility

- **Widely Supported:** UTP cables are compatible with a wide range of networking devices, including switches, routers, and network interface cards.
- **Multiple Categories:** UTP cables come in various categories (Cat 5e, Cat 6, Cat 6a, etc.) that offer different performance levels, allowing network designers to choose the appropriate type based on their specific needs.

vi. Maintenance and Troubleshooting

- **Ease of Maintenance:** UTP cables are relatively easy to maintain and troubleshoot. They can be quickly replaced if damaged, and issues can often be diagnosed with basic network testing tools.
- **Less Susceptible to Physical Damage:** While they lack shielding, UTP cables are still robust enough for most indoor environments, and their flexibility reduces the risk of damage from bending or handling.

6. Credit and debit cards use NFC (Near Field Communication) technology for transactions at point of sale (POS) terminals due to several benefits that enhance convenience, security, and efficiency. Here are some key reasons:

- **Convenience:** NFC technology allows for quick and easy transactions. Users can simply tap or wave their card near the POS terminal without needing to swipe or insert the card, speeding up the checkout process.
- **Security:** NFC transactions are typically more secure than traditional magnetic stripe transactions. NFC uses encryption to protect the data exchanged between the card and the terminal, reducing the risk of fraud. Many NFC transactions also use tokenisation, where a unique token (instead of the actual card number) is transmitted, adding an extra layer of security.
- **Contactless Transactions:** With the rise of contactless payments, especially during the COVID-19 pandemic, NFC technology has become more popular. It reduces physical contact between the card and the terminal, promoting hygiene and reducing the spread of germs.
- **Compatibility with Mobile Payments:** NFC technology is compatible with mobile payment solutions like Apple Pay, Google Pay, and Samsung Pay. This allows users to make payments using their smartphones or smartwatches, providing flexibility and convenience.

- **Improved Customer Experience:** Faster and more efficient transactions lead to shorter wait times and a better overall shopping experience for customers. This can increase customer satisfaction and loyalty.
 - **Reduced Wear and Tear:** NFC cards do not require physical contact with the terminal, reducing wear and tear on the card. This can extend the life of the card compared to traditional magnetic stripe or chip-and-PIN cards.
7. In a cellular network, **cell towers (or cell sites or base stations)** are used to enable mobile communication and provide internet access on digital devices such as smartphones. These cell towers contain antennas and other equipment necessary to transmit and receive signals between mobile devices and the network's core infrastructure. Here's how they work:

Key Components and Functions of Cell Towers:

- **Antennas:** Transmit and receive radio frequency (RF) signals to and from mobile devices. Multiple antennas may be used to cover different frequency bands and improve signal quality.
- **Base Transceiver Station (BTS):** The equipment that facilitates wireless communication between the network and mobile devices. It handles the radio communications with the mobile device.
- **Base Station Controller (BSC):** Manages multiple BTS units. Coordinates handoffs of mobile devices as they move between cell towers and handles traffic load balancing.
- **Backhaul Connection:** Connects the cell tower to the core network. Can be implemented using various technologies such as fibre optics, microwave links, or satellite connections.

How Cell Towers Enable Mobile Communication:

- **Coverage:** Cell towers are strategically placed to provide coverage over a geographic area. The area covered by each tower is known as a "cell." As a user moves, their mobile device connects to the nearest cell tower, allowing seamless communication.
- **Handoffs:** When a user moves from the coverage area of one cell tower to another, the network performs a handoff to maintain the connection without interruption.
- **Frequency Reuse:** To efficiently use the available spectrum, frequencies are reused in different cells. Proper planning ensures minimal interference between cells using the same frequencies.

Services Provided:

- **Voice Calls:** Allows users to make and receive voice calls.
- **Text Messaging:** Supports SMS (Short Message Service) for sending and receiving text messages.
- **Internet Access:** Provides mobile internet access through technologies like 4G LTE and 5G.
- **Data Services:** Enables data-intensive applications such as video streaming, online gaming, and mobile applications.

REFERENCES

1. [Anshuman Singh](https://www.shiksha.com/online-courses/articles/difference-between-bus-and-star-topology-blogId-158377) (2024). Difference Between Bus and Star Topology retrieved from <https://www.shiksha.com/online-courses/articles/difference-between-bus-and-star-topology-blogId-158377> on 25th June, 2024.
2. Computing – Teacher Manual (2023) for SHS, SHTS, STEM curriculum – pages 88 – 94
3. Computing – Teacher Manual (2023) for SHS, SHTS, STEM curriculum – pages 95 – 97
4. Computing – Teacher Manual (2023) for SHS, SHTS, STEM curriculum – pages 101 – 107
5. images of the components of a network: retrieved from: <https://medium.com/@hasonsnik/key-components-of-computer-network-7e3baaaeb749>
6. Keary, T. (2024, January 10). Network security and administration expert. Comparitech. <https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/>
7. NaCCA (2023) Computing Curriculum for Secondary Education (SHS 1 - 3), pg. 41
8. NaCCA (2023) Computing Curriculum for Secondary Education (SHS 1 - 3), pg. 41.
9. NaCCA (2023) Computing Curriculum for Secondary Education (SHS 1 - 3), pg. 40.
10. Types of Network Topology retrieved from InterviewBit <https://www.interviewbit.com/blog/types-of-network-topology/> on 25th June, 2024.
11. Types of networks and topologies https://docs.google.com/document/d/1E5naR7y40yahbFw9TY0DJPmvjKbUrP4M/edit?usp=drive_link&oid=102519533476148787893&rtpof=true&sd=true

ACKNOWLEDGEMENTS



Ghana Education
Service (GES)



List of Contributors

Name	Institution
Mark Kwadwo Ntoso	Krachi SHS
Mahama Seidu	Daboya Community SHS
Miheso Daniel	Wa SHTS, Wa
Francis Bennet Kouadio Kouame	Odorgonno SHS, Awoshie