

INTERNATIONAL ADVANCED LEVEL

INFORMATION TECHNOLOGY

UNIT 1

Topic 2: Networks



Academic Year: 2024-2025



Institution Name: European Institute of Innovation

Entrepreneurship and Technology

✍ Prepared by: Irikefe Hope Oniovosa

Table of Contents

1.0	<i>Networks</i>	3
2.0	<i>Types of Networks</i>	3
2.1.	LAN (Local Area Network)	3
2.2	WAN (Wide Area Network)	3
2.3.	MAN (Metropolitan Area Network)	4
2.4.	PAN (Personal Area Network)	4
3.0.	<i>Network Topologies</i>	5
3.1.	Star Topology	5
3.2	Bus Topology	6
3.3.	Ring Topology	6
3.4.	Mesh Topology	7
4.0	<i>Network Components</i>	8
5.0	<i>Networking Protocols</i>	9
5.1	Demonstration: How Data Travels Through a Network	9
6.0.	<i>Network Security</i>	10
a.	Security Threats	10
b.	Security Measures	10
7.0.	<i>Troubleshooting Network Issues</i>	11
a.	Common Network Issues & Fixes	11
b.	Troubleshooting Techniques	11
8.0.	<i>Case Study: Real-World Cyberattack</i>	11

1.0 Networks

A **network** is a collection of interconnected devices—such as computers, servers, smartphones, routers, and switches—that are linked together to communicate and share resources. These resources can include data, internet access, files, printers, and more. The connections between these devices can be established through wired technologies (like Ethernet cables) or wireless technologies (like Wi-Fi or cellular networks).

In addition to the physical hardware, networks also rely on communication protocols (rules and standards) that enable devices to understand each other and coordinate the exchange of information. Examples include TCP/IP for internet communications and various other protocols for different types of networks.

2.0 Types of Networks

2.1. LAN (Local Area Network)

- **Definition:** A LAN is a network that connects devices within a small area, such as a single building or campus.
- **Examples:**
 - **Home:** Your Wi-Fi network that connects your computer, smartphone, smart TV, and printer.
 - **School/Office:** Computers in a classroom or office connected to share files and access printers.

2.2 WAN (Wide Area Network)

- **Definition:** A WAN covers a large geographic area, such as cities, countries, or even the entire globe.
- **Examples:**
 - **The Internet:** It connects millions of smaller networks (including LANs) across the world.
 - **Corporate Networks:** A multinational company linking its offices in different cities or countries.

2.3. MAN (Metropolitan Area Network)

- **Definition:** A MAN is a network that spans a metropolitan area (a city or a large town) and connects multiple LANs.
- **Examples:**
 - **City Networks:** A network connecting government offices, public libraries, or businesses across a city.
 - **Campus Networks:** Sometimes, a group of nearby schools or universities within a city may be connected via a MAN.

2.4. PAN (Personal Area Network)

- **Definition:** A PAN is a short-range network designed for personal devices.
- **Examples:**
 - **Bluetooth Connections:** Connecting your smartphone to wireless earbuds or a smartwatch.
 - **Wired PAN:** A USB connection between your computer and a peripheral device like a printer.

Group Discussion: Divide into small groups and list real-life examples for each network type.

- **For LAN:** Consider your home Wi-Fi, your school computer lab, or an office network.
- **For WAN:** Think about how the Internet connects you to websites around the world or how international companies connect their offices.
- **For MAN:** Consider networks that might be used by your city for public services or how a local government might interconnect its offices.
- **For PAN:** Look at the Bluetooth connection between your phone and your headphones, or how your smartwatch connects to your phone.

3.0. Network Topologies

Network topology describes the way in which devices (nodes) are arranged and connected in a network. Different topologies have their own advantages and disadvantages in terms of cost, performance, and reliability.

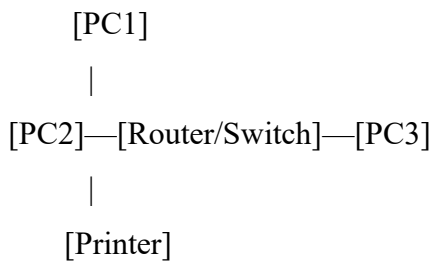
3.1. Star Topology

- **Description:**

In a **star topology**, every device is connected to a central device, such as a hub or switch.

- **Key Points:**

- **Central Control:** The hub/switch manages traffic between devices.
- **Ease of Management:** If one connection fails, only that device is affected.
- **Vulnerability:** The central hub is a single point of failure; if it goes down, the entire network can be affected.



Explanation & Example:

- **How It Works:** All devices (PC1, PC2, PC3, Printer) are individually connected to a central device (Router/Switch).
- **Real-Life Example:** A typical home network where computers, smartphones, and a printer connect to a Wi-Fi router.

3.2 Bus Topology

- **Description:**

In a **bus topology**, all devices share a single communication line (the bus) to send and receive data.

- **Key Points:**

- **Simplicity:** Easy to implement and extend.
- **Cost-Effective:** Uses less cable compared to some other topologies.
- **Limitations:** If the main cable (bus) fails, the entire network is disrupted. Also, performance may suffer as more devices share the same communication line.

[PC1]----[PC2]----[PC3]----[PC4]

Explanation & Example:

- **How It Works:** All devices share a single communication line (the bus). Data travels along this main cable from one device to the next.
- **Real-Life Example:** An older office network where several computers are connected along a single coaxial cable. (Note: This topology is less common today.)

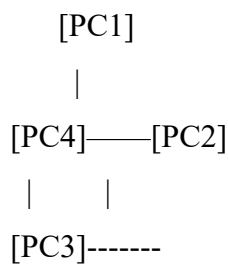
3.3. Ring Topology

- **Description:**

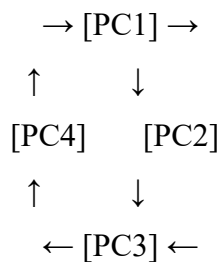
In a **ring topology**, each device is connected to exactly two other devices, forming a circular data path.

- **Key Points:**

- **Data Flow:** Data typically travels in one direction around the ring (or can be bidirectional in some cases).
- **Predictable Performance:** Each device gets a fair chance to communicate.
- **Disruption Risk:** If one device or connection fails, it can break the loop, potentially disrupting the entire network (though some networks use dual rings for redundancy).



Alternate diagram with directional flow:



Explanation & Example:

- **How It Works:** Each device is connected to two others, forming a closed loop. Data travels in one (or sometimes both) directions around the ring.
- **Real-Life Example:** Some local area networks (like token ring networks) or certain types of industrial control networks use a ring topology for predictable data circulation

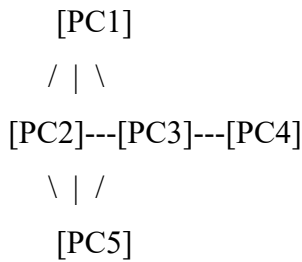
3.4. Mesh Topology

- **Description:**

In a **mesh topology**, every device is connected directly to every other device.

- **Key Points:**

- **High Redundancy:** There are multiple paths for data to travel, making the network very resilient.
- **Reliability:** If one connection fails, data can be routed through another path.
- **Complexity and Cost:** This topology requires a lot of cables and can be expensive to implement, especially as the number of devices increases.



Explanation & Example:

- **How It Works:** Every device is connected directly to every other device, offering multiple paths for data to travel.
- **Real-Life Example:** A fully meshed network in a data center or in mission-critical networks (like those used by military or emergency services) to ensure high redundancy and reliability.

4.0 Network Components

Understanding network components is crucial for knowing how data moves in a network. Below are the key components with explanations and real-life examples.

a. Router

- **Function:** Directs network traffic between different networks (e.g., your home network and the internet).
- **Example:** A Wi-Fi router in your home connects your devices to the internet.

b. Switch

- **Function:** Connects multiple devices within a LAN and directs data only to the intended recipient.
- **Example:** In an office network, a switch connects multiple computers and ensures they communicate efficiently.

c. Hub

- **Function:** A basic device that broadcasts data to all connected devices, whether they need it or not.
- **Example:** Used in older networks but replaced by switches for better efficiency.

d. Bridge

- **Function:** Connects two separate LANs and ensures they function as one network.
- **Example:** Used in large offices with multiple network segments.

e. Modem

- **Function:** Converts digital signals from your computer into signals that can travel over telephone lines or fiber optics.
- **Example:** The device your Internet Service Provider (ISP) gives you to connect to the internet.

5.0 Networking Protocols

Protocols define how data is sent and received across networks. Here are some essential ones:

a. TCP/IP (Transmission Control Protocol/Internet Protocol)

- **Function:** Ensures reliable data transmission across networks by breaking data into packets and reassembling it correctly.
- **Example:** The backbone of the internet—used for all online communication.

b. HTTP/HTTPS (HyperText Transfer Protocol / Secure)

- **Function:** Governs how web pages and data are transferred over the internet.
- **Example:** When you visit a website like <https://google.com>, your browser uses HTTPS.

c. FTP (File Transfer Protocol)

- **Function:** Enables file transfer between computers over a network.
- **Example:** Used by web developers to upload files to a website's server.

5.1 Demonstration: How Data Travels Through a Network

Step-by-Step Example (Sending an Email)

1. Typing an Email (Application Layer)

- A user types an email in Gmail and clicks "Send."
- The device uses **TCP/IP** to break the email into packets.

2. Data Sent to the Router (Network Layer)

- The router **directs** the packets to the recipient's mail server using the best path.

3. Internet Transmission (Using HTTP, FTP, or Other Protocols)

- The email travels through various routers across the internet.

4. Receiving the Email (Application Layer)

- The recipient's router receives the packets, and TCP/IP **reassembles** them into a readable email.

Class Activity: Simulating Network Communication

- Assign students roles: **Computer (Sender), Switch, Router, ISP, Server, Receiver.**
- Use paper notes to represent data packets.
- Show how packets move through each component before reaching the destination.

6.0. Network Security

Network security ensures the safety and integrity of data as it travels across networks. Below are key threats and protective measures.

a. Security Threats

1. **Malware** – Malicious software like viruses, worms, and ransomware that can damage or steal data.
 - *Example:* A Trojan virus disguised as a software update infects a computer.
2. **Hacking** – Unauthorized access to a network or system to steal or manipulate data.
 - *Example:* A hacker breaches a company's database and leaks customer information.
3. **Phishing** – Fraudulent attempts to obtain sensitive information (e.g., passwords) through deceptive emails or websites.
 - *Example:* A fake banking website tricks users into entering their credentials.
4. **DDoS (Distributed Denial of Service) Attack** – Overloading a network with excessive traffic to make services unavailable.
 - *Example:* A website is bombarded with fake requests, causing it to crash.

b. Security Measures

1. **Firewalls** – Monitor and block unauthorized network access.
 - *Example:* A company's firewall blocks suspicious incoming connections.
2. **Encryption** – Converts data into unreadable code that only authorized users can decrypt.
 - *Example:* WhatsApp uses end-to-end encryption for secure messaging.
3. **Antivirus Software** – Detects and removes malware from systems.
 - *Example:* Windows Defender scans for and removes viruses.

7.0. Troubleshooting Network Issues

When networks fail, it's essential to diagnose and fix problems using the following techniques:

a. Common Network Issues & Fixes

1. **No Internet Connection** – Check cables, restart the router, and ensure ISP services are working.
2. **Slow Internet Speed** – Disconnect unused devices, check for background downloads, and use speed test tools.
3. **Device Can't Connect to Wi-Fi** – Forget and reconnect to the network, update drivers, or check router settings.
4. **Network Congestion** – Too many users? Upgrade bandwidth or schedule internet-heavy tasks during off-peak hours.

b. Troubleshooting Techniques

- **Checking Physical Connections** – Ensure cables are properly plugged in and not damaged.
- **Restarting Devices** – Power cycle routers and computers to resolve temporary glitches.
- **Using Network Diagnostic Tools** – Ping tests, traceroute, and command-line tools to detect connection issues.

8.0. Case Study: Real-World Cyberattack

A great example to analyze is the **2017 WannaCry Ransomware Attack**:

- **What happened?** A global ransomware attack exploited Windows vulnerabilities, encrypting users' data and demanding Bitcoin ransom.
- **Who was affected?** Over 200,000 computers in 150+ countries, including hospitals and businesses.
- **How was it resolved?** Microsoft released emergency patches, and security agencies worked to contain the damage.
- **Lesson learned?** Regular software updates and cybersecurity awareness can prevent such attacks.

Class Activity: Cybersecurity Debate

- Split students into two groups: **Attackers** vs. **Defenders**.
- Attackers list strategies hackers use to exploit networks.
- Defenders propose security measures to counter these attacks.
- Discuss the best cybersecurity practices based on their arguments.

1. into providing sensitive information such as passwords or credit card details.

9.0 features and purposes of network communication protocols

providing sensitive information such

a. Wi-Fi

- **Purpose:**

Enables wireless connectivity in local area networks (LANs), allowing devices like laptops, smartphones, and tablets to access the internet and share data without cables.

- **Features:**

- **Standard:** Based on IEEE 802.11 standards.
- **Frequency Bands:** Operates mainly in 2.4 GHz and 5 GHz bands.
- **Range & Speed:** Offers a moderate range (typically tens of meters indoors) with varying speeds depending on the standard (e.g., 802.11n, 802.11ac, 802.11ax).
- **Security:** Uses protocols like WPA2/WPA3 to secure wireless communications.

b. ZigBee®

- **Purpose:**

Designed for low-power, low-data-rate applications such as home automation, industrial control, and sensor networks (often in the Internet of Things, IoT).

- **Features:**

- **Standard:** Based on IEEE 802.15.4.
- **Low Energy Consumption:** Optimized for devices that run on battery power for extended periods.
- **Short Range:** Typically used for communication within a room or small building.
- **Mesh Networking:** Supports mesh topology, allowing devices to relay data through each other to extend network range and reliability.

c. Bluetooth®

- **Purpose:**

Facilitates short-range wireless communication between personal devices (e.g., connecting a smartphone to a headset, keyboard, or speaker).

- **Features:**

- **Short-Range Communication:** Typically effective within 10 meters (though newer versions can extend further).
- **Low Energy Option:** Bluetooth Low Energy (BLE) is designed for minimal power consumption, ideal for wearable devices and sensors.
- **Data Exchange:** Suited for transmitting small amounts of data like audio, control commands, or simple file transfers.
- **Pairing Mechanism:** Devices must be paired to ensure secure and intended connections.

d. Cellular – Global System for Mobile (GSM) Communications (3G/4G)

- **Purpose:**

Provides wide-area mobile communication services, enabling voice, text, and data transmission for mobile phones and other mobile devices.

- **Features:**

- **Global Reach:** GSM networks are used worldwide, offering extensive coverage.
- **Generational Improvements:**
 - **3G:** Introduced better data speeds and multimedia support.
 - **4G:** Provides significantly faster internet speeds and supports high-definition streaming and advanced applications.
- **Mobility:** Designed for continuous connectivity while on the move.
- **Security & Standards:** Includes robust encryption and standardized protocols to protect communications.

e. Infrared

- **Purpose:**

Historically used for remote control devices and short-distance, line-of-sight data communication between devices.

- **Features:**

- **Line-of-Sight Requirement:** Infrared signals require a clear path between transmitter and receiver.

- **Short Range:** Typically effective over very short distances (a few meters).
- **Low Data Rates:** Suitable for simple commands or small data transfers, not for high-speed internet or large file transfers.
- **Interference:** Not subject to radio frequency interference but can be affected by physical obstacles.

f. Ethernet

- **Purpose:**

Provides high-speed, reliable wired connectivity within local area networks (LANs), such as in homes, offices, and data centers.

- **Features:**

- **Standard:** Based on IEEE 802.3 standards.
- **Wired Communication:** Uses cables (e.g., twisted pair, fiber optics) to connect devices, offering stable and secure connections.
- **High Data Rates:** Supports very high data transfer speeds, which are crucial for bandwidth-intensive tasks.
- **Low Latency:** Offers consistent, low-latency connections ideal for real-time applications and data-intensive operations.

Summary

- **Wi-Fi:** Wireless LAN standard for everyday connectivity, balancing speed and range.
- **ZigBee®:** Low-power, low-data-rate protocol for IoT and sensor networks with mesh networking.
- **Bluetooth®:** Short-range, low-energy protocol ideal for personal device connections.
- **Cellular (GSM/3G/4G):** Wide-area mobile communication providing voice and high-speed data on the move.
- **Infrared:** Short-range, line-of-sight communication mostly used in remote controls.
- **Ethernet:** Wired networking standard that provides reliable, high-speed connectivity for local networks.

Understanding these protocols helps students see how different technologies are optimized for various networking needs, from short-range personal communication to global mobile connectivity and robust wired networks.