GLS University

Faculty of Computer Application & IT

SY BCA
Semester - IV
2024-2025

210301404
Data Communication & Networks (DCN)
(Core Subject)

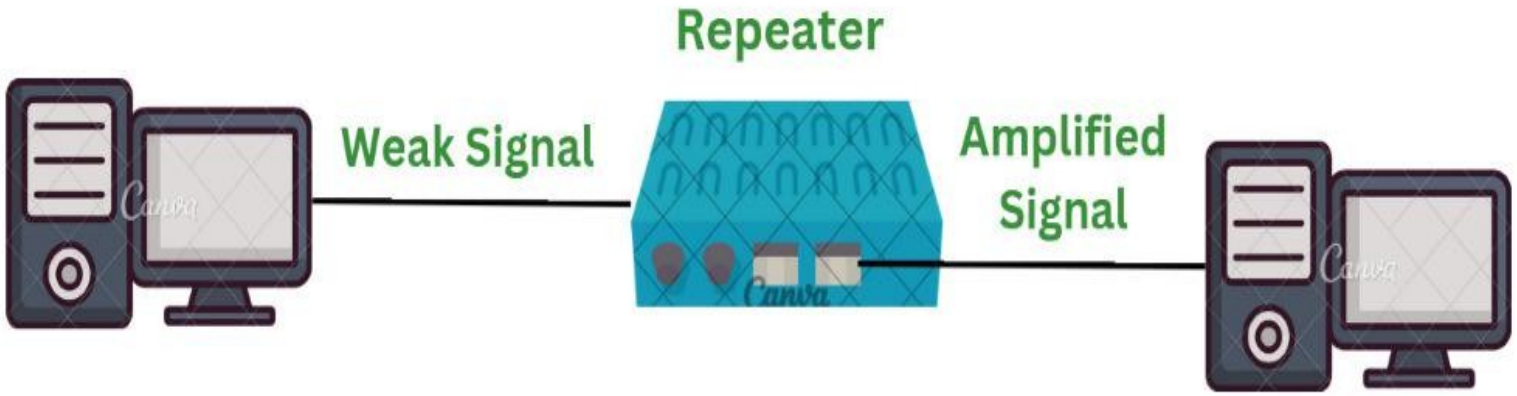
Unit 4 – Internetworking Devices

Internetworking Devices

Repeater:

- A repeater is a networking device that helps to amplify and regenerate signals to increase the reach of a network.
- Also operating at the physical layer of the OSI model, repeaters help overcome distance-related limitations by strengthening the strength and quality of the signal.
- They are instrumental in LANs and WANs as they minimize errors, reduce data loss, and ensure reliable delivery to specific locations.
- One of the primary benefits of repeaters is the error free transfer of data over longer distances. This will ensure efficient and safe communication.

Internetworking Devices



Internetworking Devices

Features of Repeater:

- Repeater can regenerate the signal without modifying it.
- Repeaters can be used in analog signals and digital signals.
- Repeaters can extend the range of networks.
- Dynamic networking is supported by repeater.
- Use of Repeaters reduces error and loss of data.
- Power is required for working of repeaters.
- Using repeater can add complexity in the network.

Internetworking Devices

Features of Repeater:

- Initially the source system transmits the signals. This source systems can be a mobile phone, laptop or radio.
- This transmitted signal from the source system travels in air if it’s wireless network or through the cable if it is wired network. As the signal goes away from the source it’s strength gets weak.
- The signal received to the repeater is not the actual signal sent by source system but a weak signal. Therefore repeater amplifies this weak signal to get it strengthen.

Internetworking Devices

Features of Repeater:

- The strengthen signal is now being sent from the repeater to its destination. This signal is more stronger and can travel at longer distance. In short, it extends the network without losing the quality of signal.
- Repeaters are therefore used in various wireless technologies such as Wi-Fi and wired technologies such as ethernet.

Internetworking Devices

Bridge:

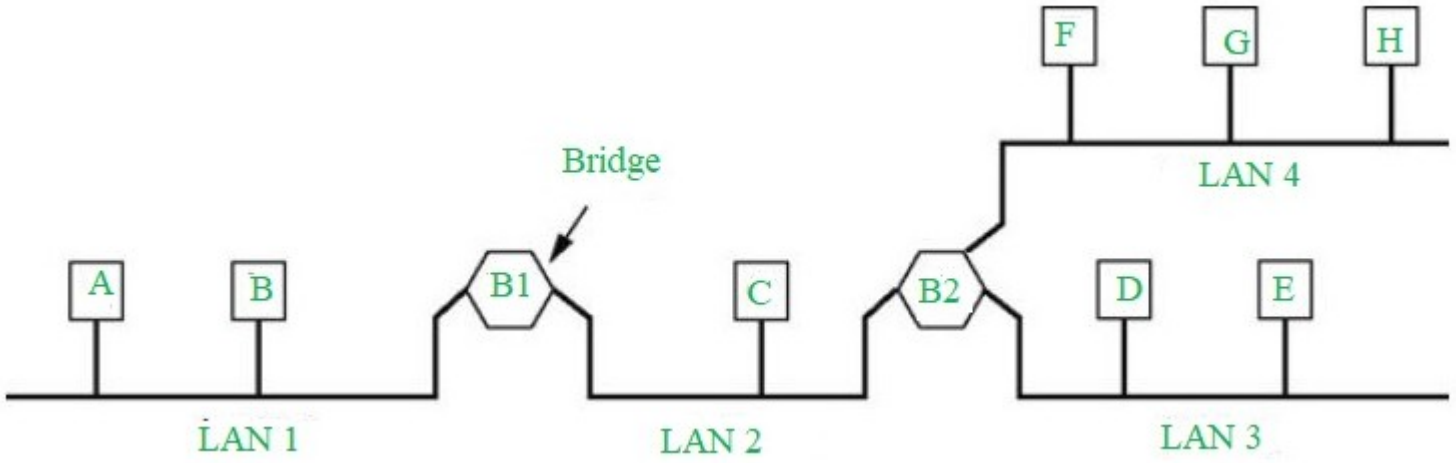
- A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN).
- The mechanism of network aggregation is known as bridging.
- The bridge is a physical or hardware device but operates at the OSI model’s data link layer and is also known as a layer of two switches.

Internetworking Devices

Bridge:

- The primary responsibility of a switch is to examine the incoming traffic and determine whether to filter or forward it.
- Basically, a bridge in computer networks is used to divide network connections into sections, now each section has a separate bandwidth and a separate collision domain.
- Here bridge is used to improve network performance.

Internetworking Devices



Internetworking Devices

Working of Bridges:

Receiving Data: The bridge gets data packets (or frames) from both network segments A and B.

- Building a Table: It creates a table of MAC addresses by looking at where the data is coming from to know which device is on which segment.
- Filtering Data: If the data from network A is meant for a device also on network A, the bridge stops it from going further.

Internetworking Devices

Working of Bridges:

- Forwarding Data: If the data from network A is meant for a device on network B, the bridge sends it to the correct place on network B.
- Repeating for Both Sides: The bridge does the same thing for data coming from network B.

Internetworking Devices

Router:

- A Router is a networking device that forwards data packets between computer networks.
- One or more packet-switched networks or subnetworks can be connected using a router.
- By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.
- Routers are the devices that are operated on the Network Layer of the OSI Model

husain

Internetworking Devices

Working of Router:

- A router determines a packet’s future path by examining the destination IP address of the header and comparing it to the routing database.
- The list of routing tables outlines how to send the data to a specific network location.

Internetworking Devices

Gateway:

- A gateway is a network connectivity device that connects two different configuration networks.
- Gateways are also known as protocol converters, because they play an important role in converting protocols supported by traffic on different networks.
- A gateway monitors and controls all the incoming and outgoing network traffic. Gateways are also known as protocol converters

Internetworking Devices

Features of Gateway:

- A gateway is situated at a network edge and manages all data that enters or exits the network.
- A gateway is distinct from other network devices in that it can operate at any layer of the OSI model.
- Gateways made the transmission more feasible as it queued up all the data and divided it into small packets of data rather than sending it bulk.
- Gateways provide security within the network.

Internetworking Devices

Working of Gateway:

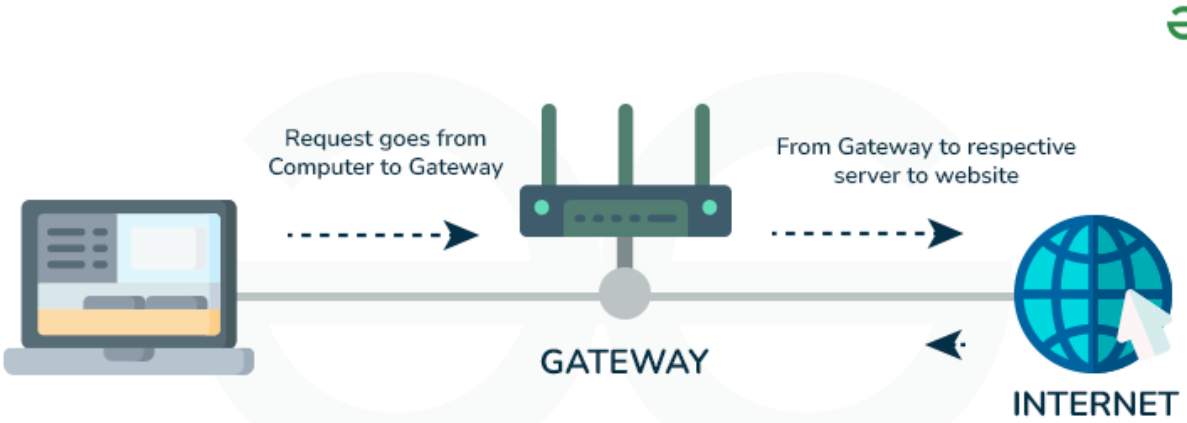
- The gateway receives data from devices within the network.
- After receiving data the gateway intercept and analyze data packets, which include analyzing packet header, payload etc.
- Based on the analysis of the data packets, the gateway calculate an appropriate destination address of data packet. It then routes the data packets to their destination address.

Internetworking Devices

Working of Gateway:

- In some cases, the gateway might also want to transform the format of the obtained data to ensure compatibility at the receiver.
- Once the data packets have been analyzed, routed, and converted, then the gateway sends the last packets to their respective destinations address inside the network.

Internetworking Devices



Introduction of Gateways

Internetworking Devices

Switch:

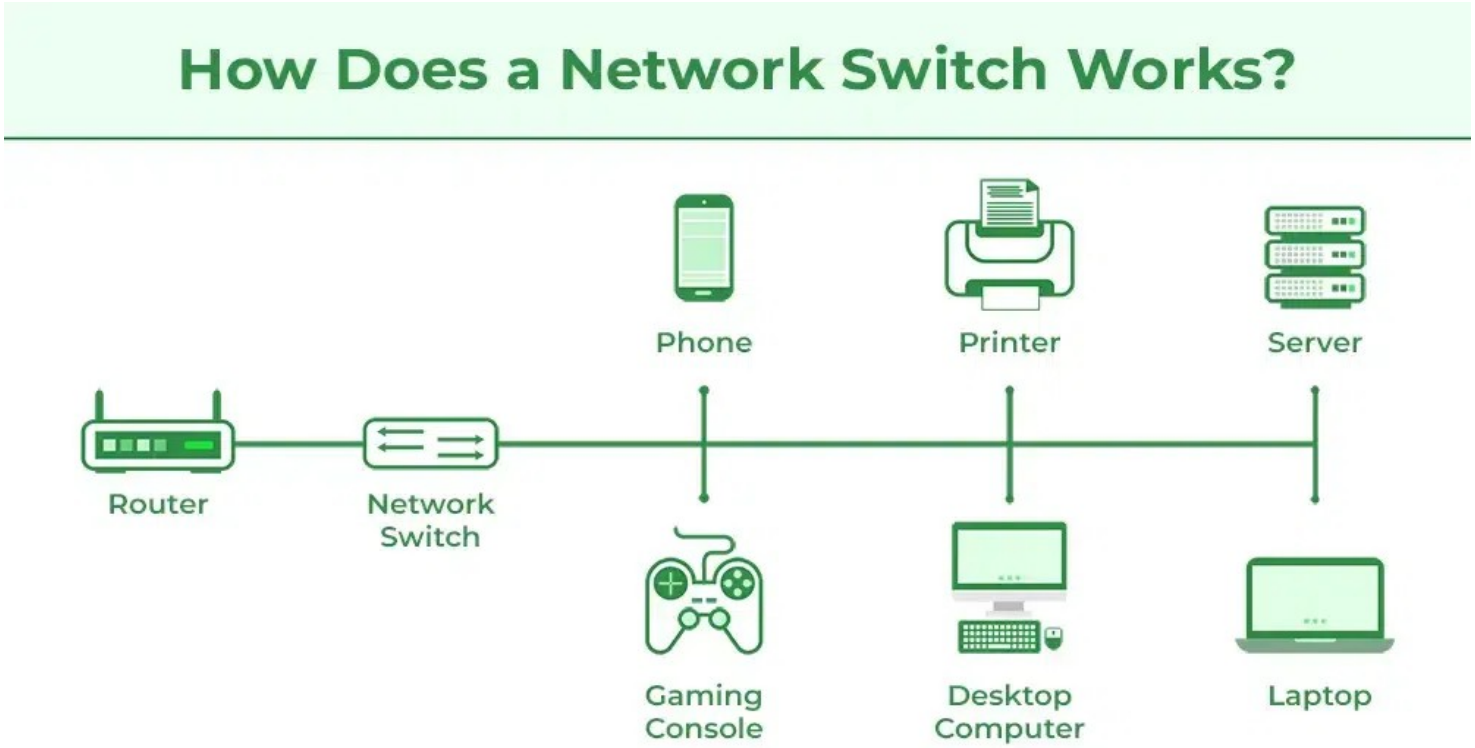
- The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments.
- It is responsible for filtering and forwarding the packets between LAN segments based on MAC address.

Internetworking Devices

Working of Switch:

- When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.
- Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done.

Internetworking Devices



What is Mobile Computing?

- Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.
- Mobile Computing is ability to compute remotely while on the move, it possible for people to access information from anywhere and at anytime.
- Mobility provides the capabilities to change location while
- communicating to invoke computing services at some remote computers .
- Mobile devices can be connected to a Local Area Network (LAN) or can take advantage of WiFi or wireless technology by connecting via a Wireless Local Area Network (WLAN).

Benefits of Mobile Computing

- Connectivity: You can stay connected to all sources at all times.
- Social Engagement: You can interact with a variety of users via the internet.
- Personalization: You can tailor your mobile computing to your individual needs.

Benefits of Mobile Computing

- Connectivity: You can stay connected to all sources at all times.
- Social Engagement: You can interact with a variety of users via the internet.
- Personalization: You can tailor your mobile computing to your individual needs.

Mobile Computing vs Wireless Networking

Mobile Computing	Wireless Networking
Mobile Computing refers to computing devices that are not restricted to a desktop.	Wireless networking refers to the method of transferring information between a computing devices and a data source without a physical connection
It refers to computing device that is not connected to a central network	It is simply data communication without the use of landline
Include laptop, smart phones, PDA	Involve cellular telephone, a two way radio, fixed wireless connection, a laser or satellite communication.
Communicate with base location, with or without a wireless connection	Computing device is continuously connected to the base network.
Uses mobile networks (airtel, idea,jio)	Routers
Uses GPRS, HSPA, EDGE, LTE	Wireless switches, Wireless HUBs
Can use wireless network also	This cannot use Mobile Networks directly(only through network sharing

Wired Networks vs Mobile Networks

Wired Networks	Mobile Networks
Speed of operation : Higher	Speed of operation : lower compare to wired networks
System Bandwidth : High	System Bandwidth : Low, as Frequency Spectrum is very scarse resource
Cost : Less as cables are not expensive	Cost : More as wireless subscriber stations, wireless routers, wireless access points and adapters are expensive
Installation : Wired network installation is cumbersome and it requires more time	Installation : Wireless network installation is easy and it requires less time
Transmission medium : copper wires, optical fiber cables, ethernet	Transmission medium : EM waves or radiowaves or infrared
Applications : LAN (Ethernet), MAN	Applications : WLAN, WPAN(Zigbee, bluetooth), Infrared, Cellular(GSM,CDMA, LTE)
Quality of Service : Better	Quality of Service : Poor due to high value of jitter and delay in connection setup

Applications for mobile computing

- There are several applications for mobile computing including wireless remote access by travelers and commuters, point of sale, stock trading, medical emergency care, law enforcement, package delivery, education, insurance industry, disaster recovery and management, trucking industry, intelligence and military.
- Most of these applications can be classified into:
  - wireless and mobile access to the Internet
  - wireless and mobile access to private Intranets
  - wireless and adhocly mobile access between mobile computers.

Charactersitics of Mobile Computing

- Portability :-
  The Ability to move a device within a learning environment or to different environments with ease.
- Social Interactivity :-
  The ability to share data and collaboration between users.

- Context Sensitivity :-
  The ability to gather and respond to real or simulated data unique to a current location , environment or time.

Characteristics of Mobile Computing

Connectivity :-

- The ability to be digitally connected for the purpose of communication of data in any environment.

Individual :-

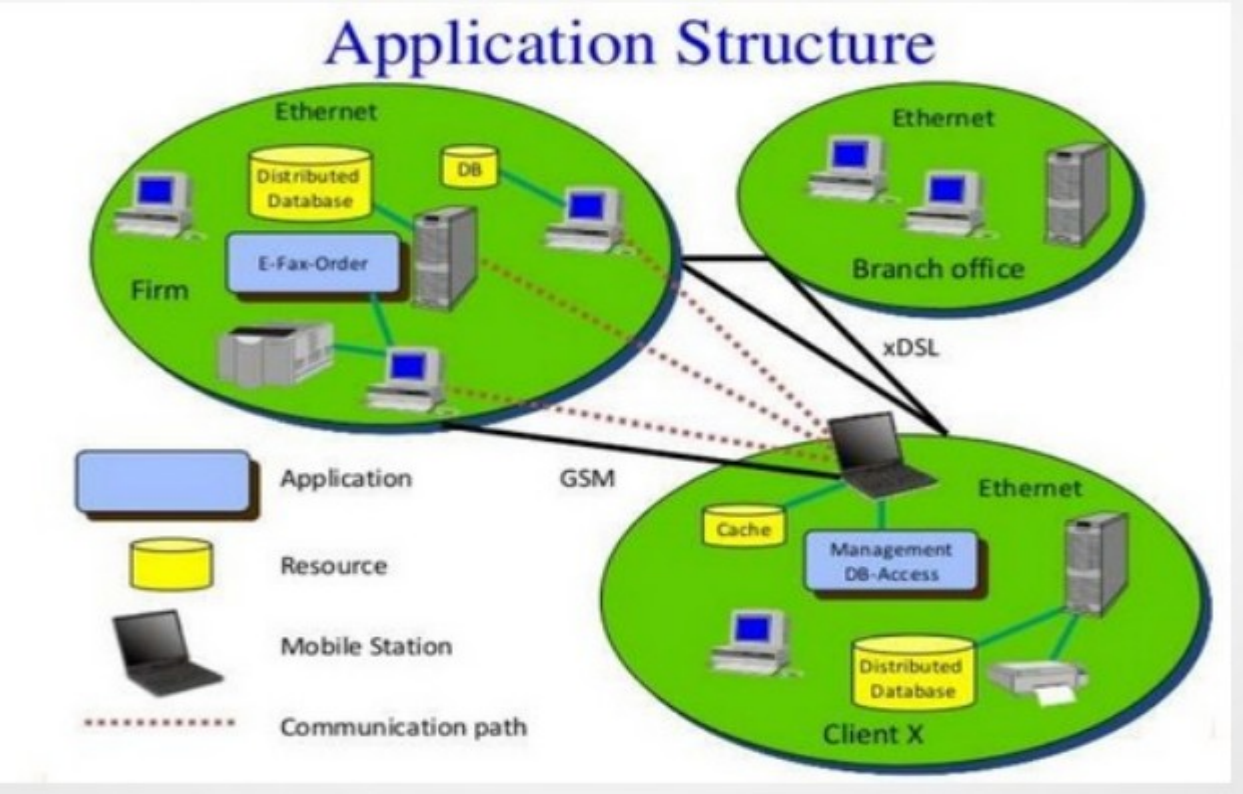
- The ability to use the technology to provide scaffolding on difficult activities and lesson customization for individual learners.

Characteristics of Mobile Computing

Wireless Communication :-

- Mobile devices are typically capable of communication with other similar devices , with stationary computers and portable phones.
- Base mobile devices are capable of accessing the Internet through Bluetooth or Wi- Fi networks, and many models are equipped to access data networks as well.

Structure of Mobile Computing



Characteristics of Mobile Computing

- Programming languages are used for mobile system software.
- Operating system functions to run the software components onto the hardware.
- Middleware components deployment.
- Layered structure arrangement of mobile computing components is used.
- Protocols and layers are used for transmission and reception.

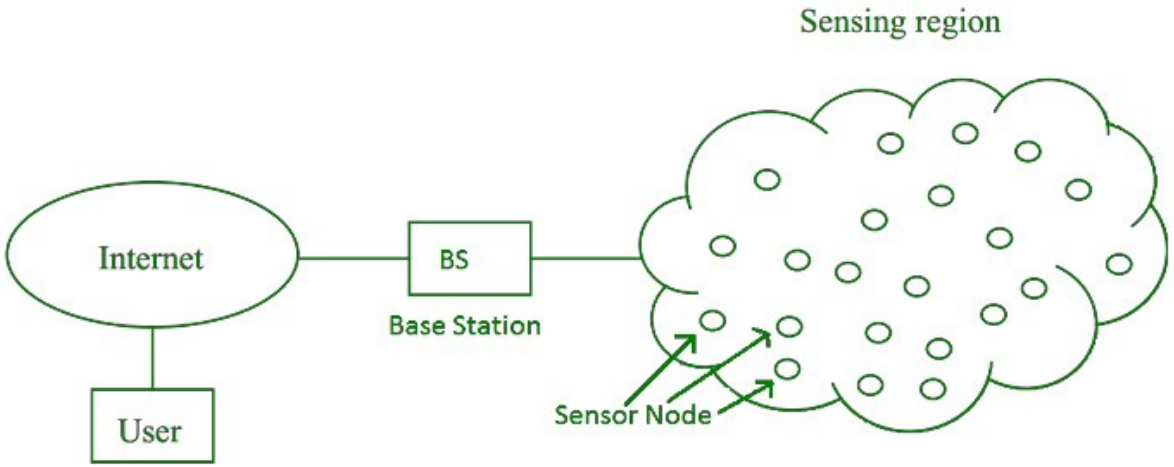
Introduction to WSN

- Wireless Sensor Network (WSN), is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical, or environmental conditions.

Introduction to WSN

- Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area.
- They are connected to the Base Station which acts as a processing unit in the WSN System.
- The base Station in a WSN System is connected through the Internet to share data.
- WSN can be used for processing, analysis, storage, and mining of the data.

Introduction to WSN



Architecture of WSN

- A Wireless Sensor Network (WSN) architecture is structured into three main layers:

Physical Layer:

- This layer connects sensor nodes to the base station using technologies like radio waves, infrared, or Bluetooth.
- It ensures the physical communication between nodes and the base station.

Architecture of WSN

Data Link Layer:

- Responsible for establishing a reliable connection between sensor nodes and the base station.
- It uses protocols such as IEEE 802.15.4 to manage data transmission and ensure efficient communication within the network.

Architecture of WSN

Application Layer:

- Enables sensor nodes to communicate specific data to the base station.
- It uses protocols like ZigBee to define how data is formatted, transmitted, and received, supporting various applications such as environmental monitoring or industrial control.

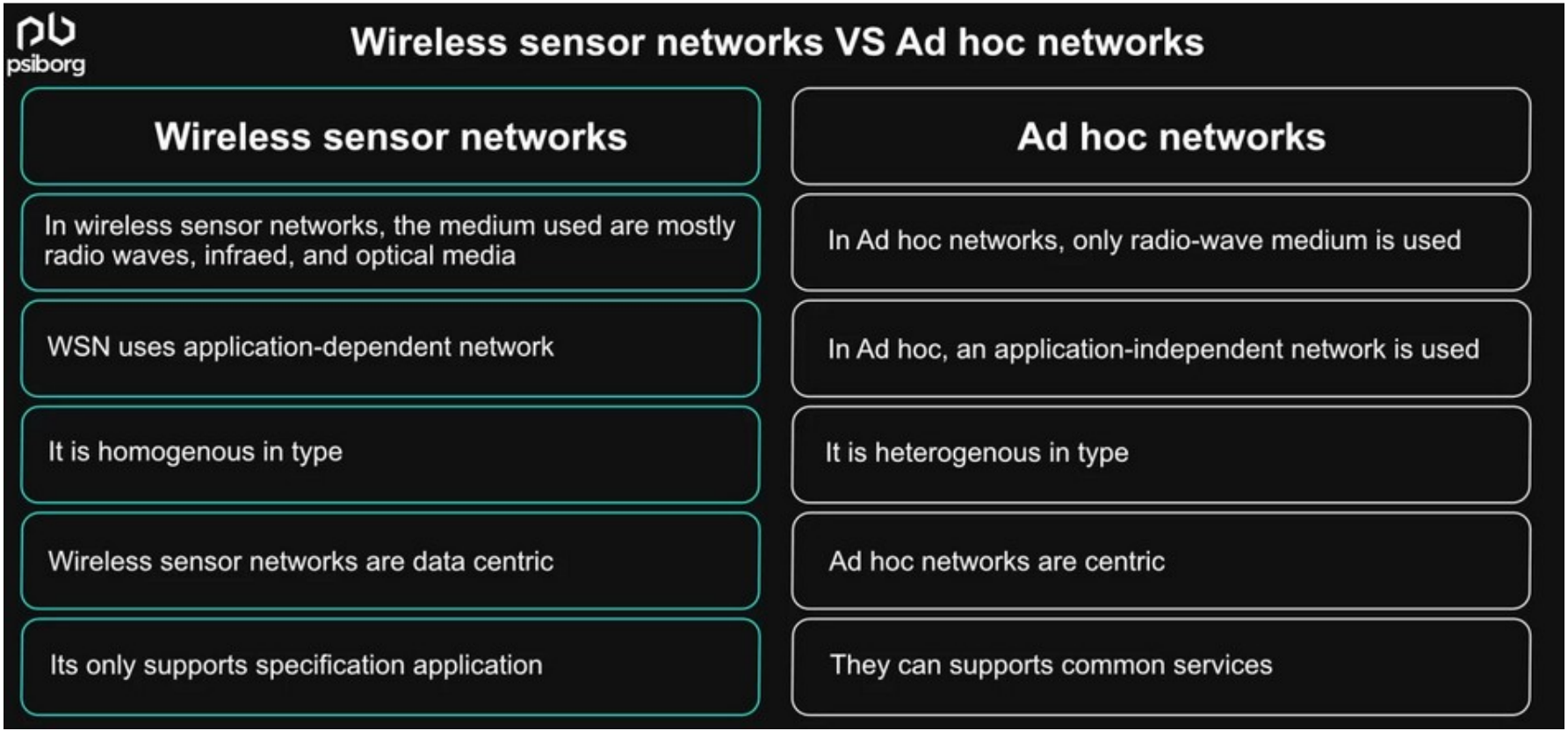
These layers work together to facilitate the seamless operation and data flow within a Wireless Sensor Network, enabling efficient monitoring and data collection across diverse applications.

MANET

MANET stands for Mobile Adhoc Network also called a wireless adhoc network or Adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.

- They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure.
- MANET nodes are free to move randomly as the network topology changes frequently.
- Each node behaves as a router as it forwards traffic to other specified nodes in the network.

WSN VS. MANET


psiborg
Wireless sensor networks VS Ad hoc networks
Wireless sensor networks
Ad hoc networks
In wireless sensor networks, the medium used are mostly radio waves, infraed, and optical media
In Ad hoc networks, only radio-wave medium is used
WSN uses application-dependent network
In Ad hoc, an application-independent network is used
It is homogenous in type
It is heterogenous in type
Wireless sensor networks are data centric
Ad hoc networks are centric
Its only supports specification application
They can supports common services

Characteristics of WSN

- **Resource constraints** – Nodes of WSN are smaller in size and get power from the batteries. It justifies that service provided by the nodes like communication and computation amount of memory is very limited.
- **Communication paradigm** – The data centric feature of WSN explains its data centric nature and justifies that the communication is restricted to nodes.
- **Application specific design** – WSN is application specific i.e. the architecture of WSN is based on application.
- **Node failure and unreliable communication** – Various factors like harsh operating conditions leading to instability, unpredictability, nodal mobility, environmental interferences makes typical WSN nodes to be error-prone.
- **Scalability and density** – The number of nodes in WSNs may be large and densely deployed to a higher degree in various applications.
- **Dynamic Topologies** – Nodes are free to travel randomly at different speeds in few applications and sometimes may fail to operate, to add or to replace. So there can be different network topology.
- **Communication models** – WSNs use different communication models – Flat/ hierarchical /distributed WSNs; or homogeneous/ heterogeneous WSNs.

Challenges of WSN

- **Limited power and energy:** WSNs are typically composed of battery-powered sensors that have limited energy resources. This makes it challenging to ensure that the network can function for long periods of time without the need for frequent battery replacements.
- **Limited processing and storage capabilities:** Sensor nodes in a WSN are typically small and have limited processing and storage capabilities. This makes it difficult to perform complex tasks or store large amounts of data.
- **Heterogeneity:** WSNs often consist of a variety of different sensor types and nodes with different capabilities. This makes it challenging to ensure that the network can function effectively and efficiently.

Challenges of WSN

- **Security:** WSNs are vulnerable to various types of attacks, such as eavesdropping, jamming, and spoofing. Ensuring the security of the network and the data it collects is a major challenge.
- **Scalability:** WSNs often need to be able to support a large number of sensor nodes and handle large amounts of data. Ensuring that the network can scale to meet these demands is a significant challenge.
- **Interference:** WSNs are often deployed in environments where there is a lot of interference from other wireless devices. This can make it difficult to ensure reliable communication between sensor nodes.
- **Reliability:** WSNs are often used in critical applications, such as monitoring the environment or controlling industrial processes. Ensuring that the network is reliable and able to function correctly in all conditions is a major challenge.

Advantages of WSN

- **Low cost:** WSNs consist of small, low-cost sensors that are easy to deploy, making them a cost-effective solution for many applications.
- **Wireless communication:** WSNs eliminate the need for wired connections, which can be costly and difficult to install. Wireless communication also enables flexible deployment and reconfiguration of the network.
- **Energy efficiency:** WSNs use low-power devices and protocols to conserve energy, enabling long-term operation without the need for frequent battery replacements.
- **Scalability:** WSNs can be scaled up or down easily by adding or removing sensors, making them suitable for a range of applications and environments.
- **Real-time monitoring:** WSNs enable real-time monitoring of physical phenomena in the environment, providing timely information for decision making and control.

Disdvantages of WSN

- **Limited range:** The range of wireless communication in WSNs is limited, which can be a challenge for large-scale deployments or in environments with obstacles that obstruct radio signals.
- **Limited processing power:** WSNs use low-power devices, which may have limited processing power and memory, making it difficult to perform complex computations or support advanced applications.
- **Data security:** WSNs are vulnerable to security threats, such as eavesdropping, tampering, and denial of service attacks, which can compromise the confidentiality, integrity, and availability of data.
- **Interference:** Wireless communication in WSNs can be susceptible to interference from other wireless devices or radio signals, which can degrade the quality of data transmission.
- **Deployment challenges:** Deploying WSNs can be challenging due to the need for proper sensor placement, power management, and network configuration, which can require significant time and resources.

UNIT 5 COMPLETED