IT8201
Information Technology Essentials

PROFESSIONAL CORE

Varun C.M.
Assistant Professor, Department of Information Technology, St. Xavier's Catholic College of Engineering

+91 770 888 5541 contactvaruncm@gmail.com /cmvarun /c/cmvarun

Unit 3 Network Essentials

Network Topology

Types of Computer Networks

Network Layers

Wireles LAN

WiFi

Network Components

Introduction

- A computer network consists of two or more computing devices that are connected in order to share the components of the network (its resources) and the information stored there.
- The real power of networking computers becomes apparent if the network is growing and then connecting it with other distinct networks, enabling communication and resource sharing across both networks.
- That is, one network can be connected to another network and become a more powerful tool because of the greater resources.

Network Topology

The topology of a network defines how the nodes of a network are connected.

Physical Topology defines how the nodes of the network are physically connected

Logical Topology is the dedicated connections between certain selected source destination pairs using the underlying physical topology

Network Topology

Bus Topology

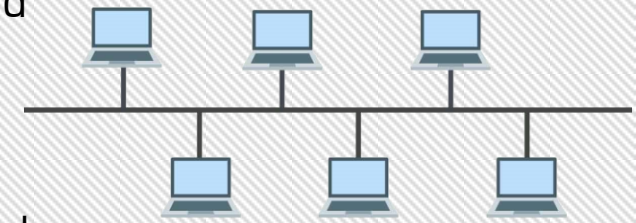
Linear local area network architecture in which all stations are attached to a single cable.

Advantages

- Easy to implement
- Good for temporary networks
- Failure of one station does not affect others

Disadvantages

- Difficult to troubleshoot
- Limited cable length and number of stations
- No redundancy
- The bus cable can be a bottleneck when network traffic gets heavy



Network Topology

Star Topology

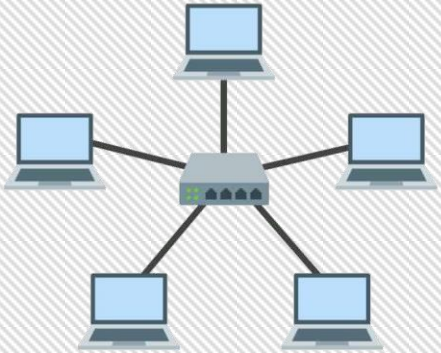
In star topology each station is connected via a point to point link to a central point. This central point is called hub.

Advantages

- Easy to connect new nodes or devices
- Centralized management which helps to monitor the network
- Failure of one node does not affect the rest of the network.

Disadvantages

- If the central hub fails, the whole network fails to operate.
- Each device requires its own cable segment.



Network Topology

Ring Topology

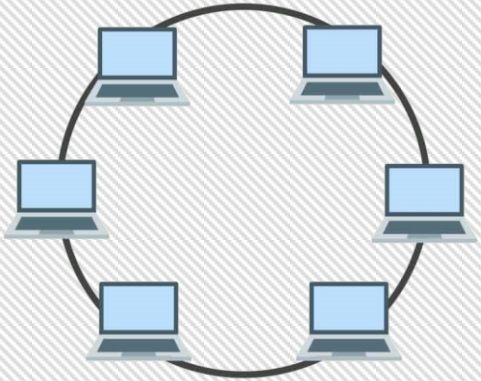
Each node is connected to the two nearest nodes so the entire network forms a circle.

Advantages

- Easier to manage
- Easier to locate defects
- Well suited for long distance transmission
- Handles high volume network traffic
- Enables reliable communication

Disadvantages

- Adding or removing nodes disrupts the network.
- Failure of one node on the ring can affect the whole network.
- Cost of cable is more in ring network



Network Topology

Mesh Topology

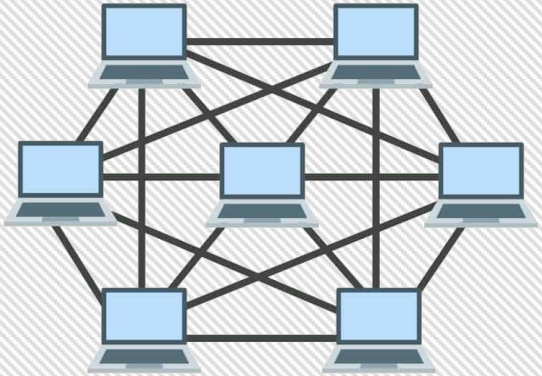
Every networked node is directly connected to every other node.

Advantages

- Provides redundant paths between devices
- Troubleshooting is easy

Disadvantages

- Difficulty in installation
- Costly because of maintaining redundant links
- Difficulty of reconfiguration



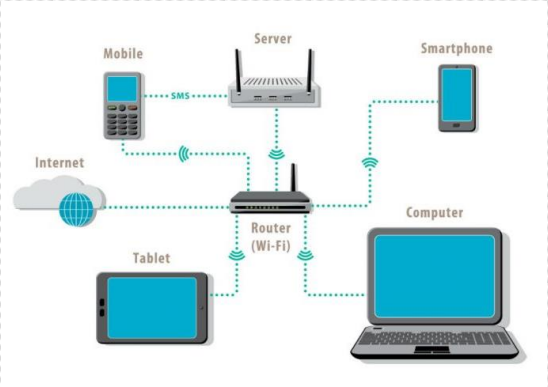
Types of Computer Networks

A computer network can be categorized by their size. A computer network is mainly of three types

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

Types of Computer Networks

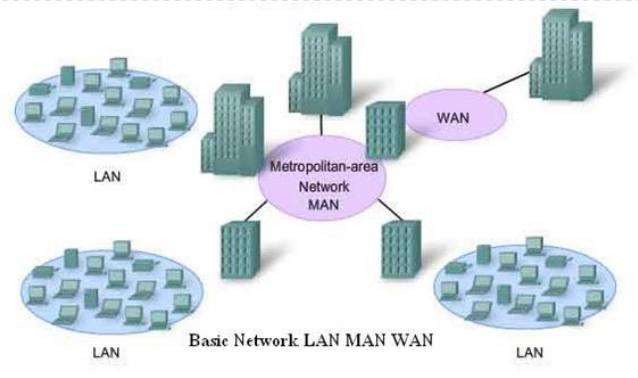
Local Area Network (LAN)



- LAN is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium
- It is less costly as it is built with inexpensive
- The data is transferred at an extremely faster rate
- It provides higher security.

Types of Computer Networks

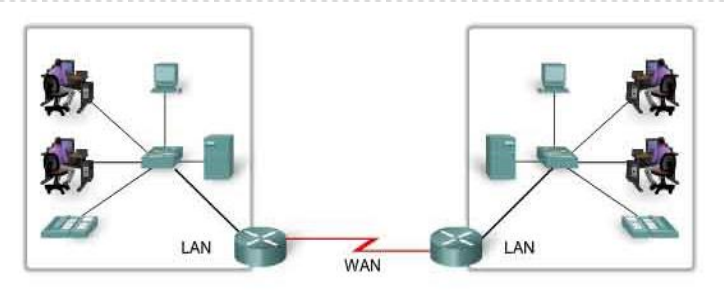
Metropolitan Area Network (MAN)



- MAN is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network(LAN).

Types of Computer Networks

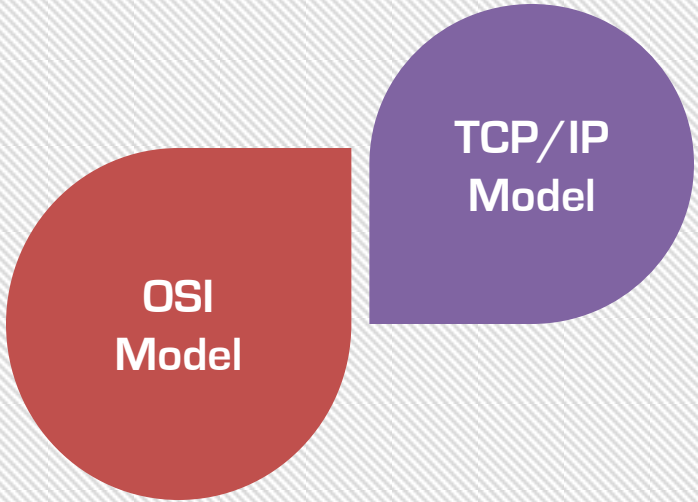
Wide Area Network (WAN)



- WAN is a network that extends over a large geographical area such as states or countries.
- WAN is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

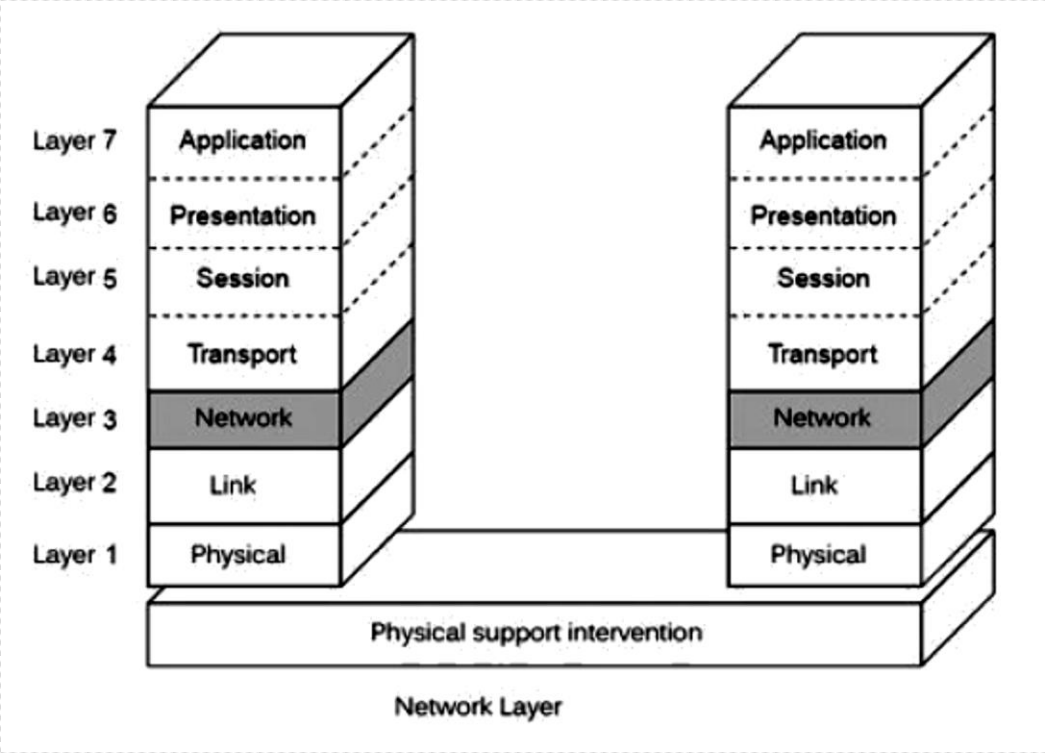
Network Layers

Network layer is responsible for addressing messages and data. It is used for translating logical addresses and names into physical addresses.



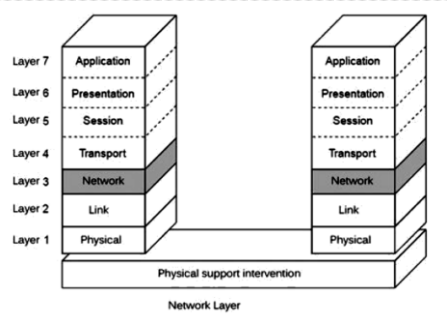
Network Layers

OSI Model



Network Layers

OSI Model

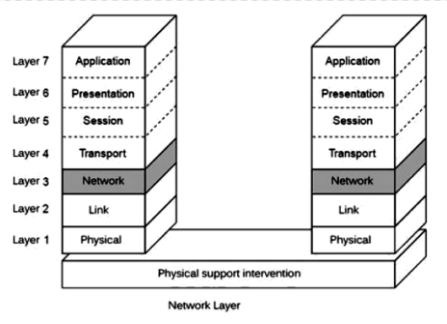


Layer 7 (Application Layer)

- Most of what the user actually interacts with is at this layer.
- Web browsers and other internet-connected applications (like Skype or Outlook) use Layer 7 application protocols.
- It contains all services or protocols needed by application software or operating system to communicate on the network
- Examples: Firefox web browser

Network Layers

OSI Model

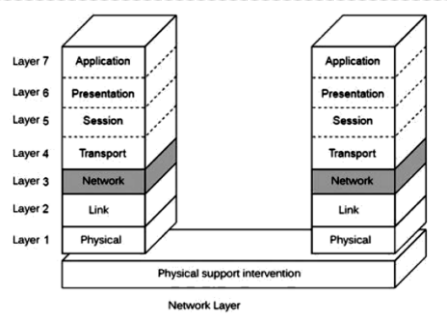


Layer 6 (Presentation Layer)

- This layer converts data to and from the Application layer.
- In other words, it translates application formatting to network formatting and vice versa.
- This allows the different layers to understand each other.
- It is concerned with how data is presented to the network.
- It handles three primary tasks: Translation, Compression and Encryption

Network Layers

OSI Model

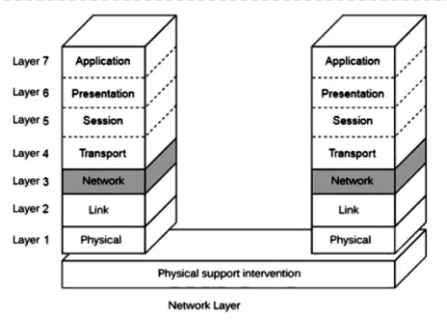


Layer 5 (Session Layer)

- This layer establishes and terminates connections between devices.
- It also determines which packets belong to which text and image files.
- It is responsible for managing the dialog between networked devices.
- It establishes, manages, and terminates connections.
- Also it provides procedures for establishing checkpoints, adjournment, termination, and restart or recovery procedure.

Network Layers

OSI Model



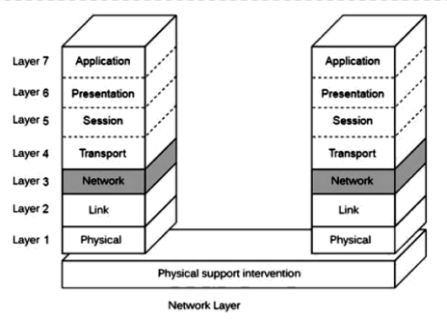
Layer 4 (Transport Layer)

- This layer coordinates data transfer between system and hosts, including error-checking and data recovery.
- It takes data from higher levels and breaks it into segments that can be sent to lower-level layers for data transmission.
- It conversely, reassembles data segments into data that higher-level protocols and applications can use.
- It also puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination.

Continues...

Network Layers

OSI Model

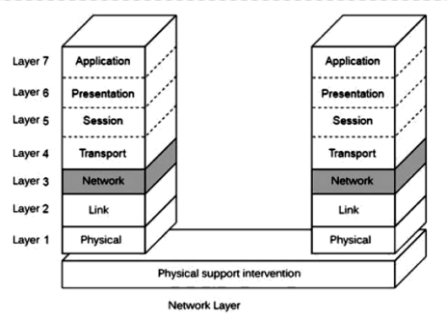


Layer 4 (Transport Layer)

- It is concerned with the reliability of the transport of sent data.
- It may use a connection-oriented protocol such as TCP to ensure destination received segments.
- It may use a connectionless protocol such as UDP to send segments without assurance of delivery.
- It also uses port addressing.

Network Layers

OSI Model

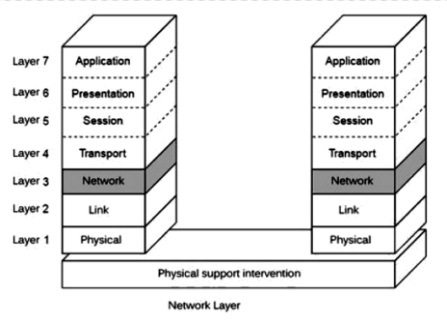


Layer 3 (Network Layer)

- This layer determines how data is sent to the receiving device.
- It's responsible for packet forwarding, routing, and addressing.
- It is responsible for moving packets (data) from one end of the network to the other, called end-to-end communications.
- It requires logical addresses such as IP addresses.
- Device example: Router

Network Layers

OSI Model

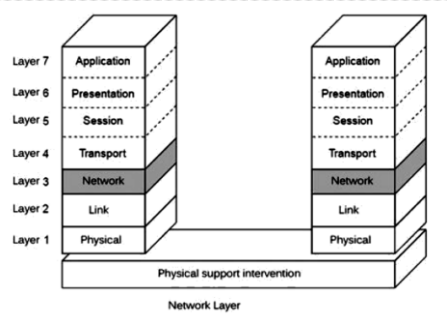


Layer 2 (Data Link Layer)

- Translates binary (or BITs) into signals and allows upper layers to access media.
- It is responsible for moving frames from node to node or computer to computer.
- It can move frames from one adjacent computer to another, cannot move frames across routers.
- It requires MAC address or physical address. Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP).

Network Layers

OSI Model

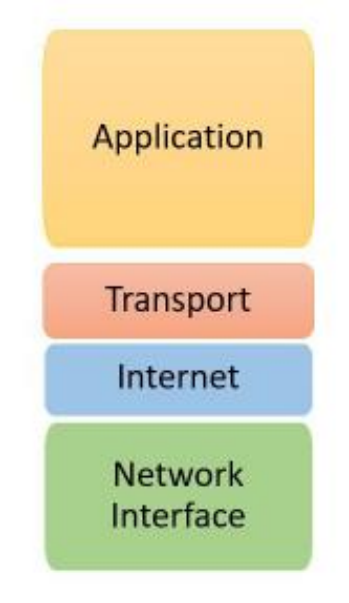


Layer 1 (Physical Layer)

- Actual hardware sits at this layer.
- It transmits signals over media.
- It deals with all aspects of physically moving data from one computer to the next.
- It converts data from the upper layers into 1s and 0s for transmission over media.
- It defines how data is encoded onto the media used to transmit the data.
- Device example: Hub

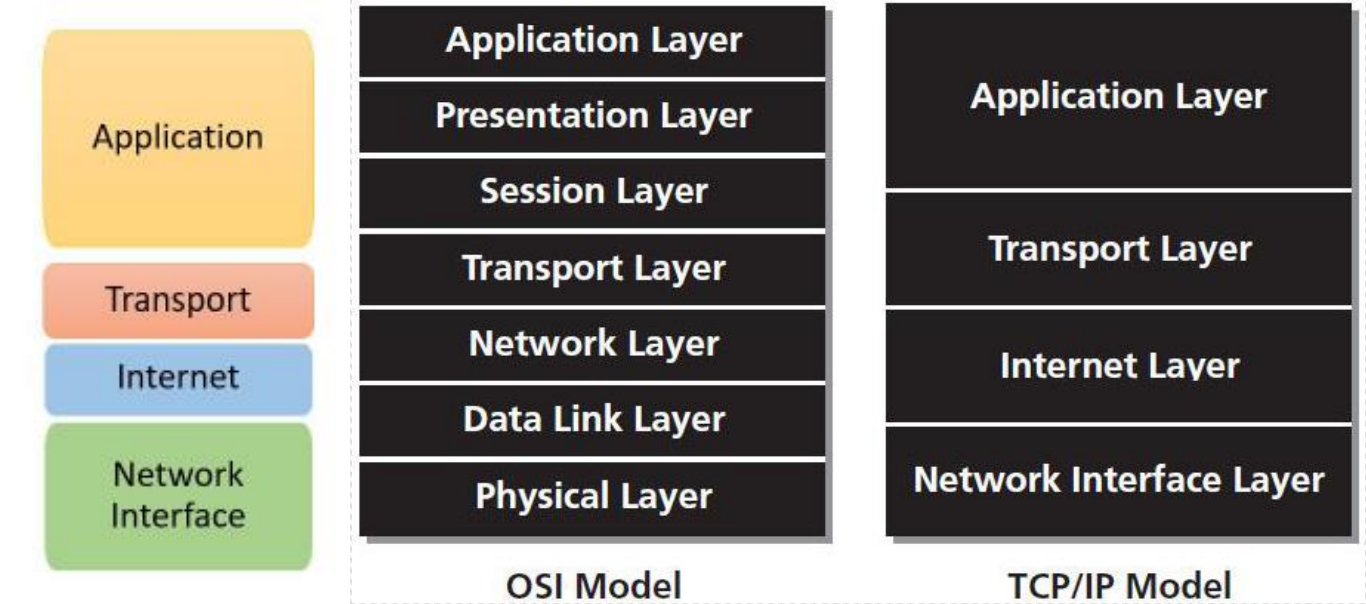
Network Layers

TCP/IP Model



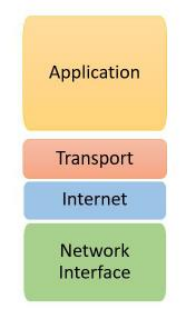
Network Layers

TCP/IP Model



Network Layers

TCP/IP Model



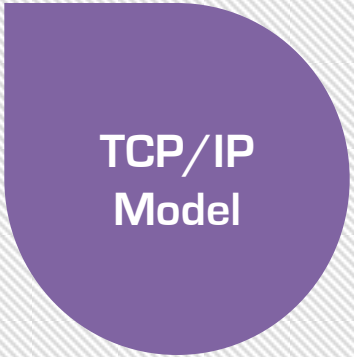
Application Layer

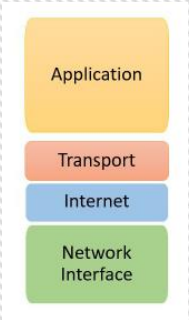
- It does the same functions of Application, Presentation and Session layers in OSI Model.

Transport Layer

- It functions as same as the Transport layer in OSI Model and part of Session layer.
- TCP and other similar protocols take on some of the function of the Session layer.
- It synchronizes source and destination computers to set up the session between the respective computers.

Network Layers





Internet Layer

- It performs the same functions as Network Layer in OSI Model. Primary protocol is Internet Protocol (IP)

Network Interface Layer

- It performs much of the job of the Data Link and Physical layers of the OSI Model.
- TCP/IP protocol suite relies on standards created by the various standards organizations concerning how to encode bits onto media to do the work on this layer.

Wireless Local Area Network

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building.

This gives users the ability to move around within a local coverage area and yet still be connected to the network.

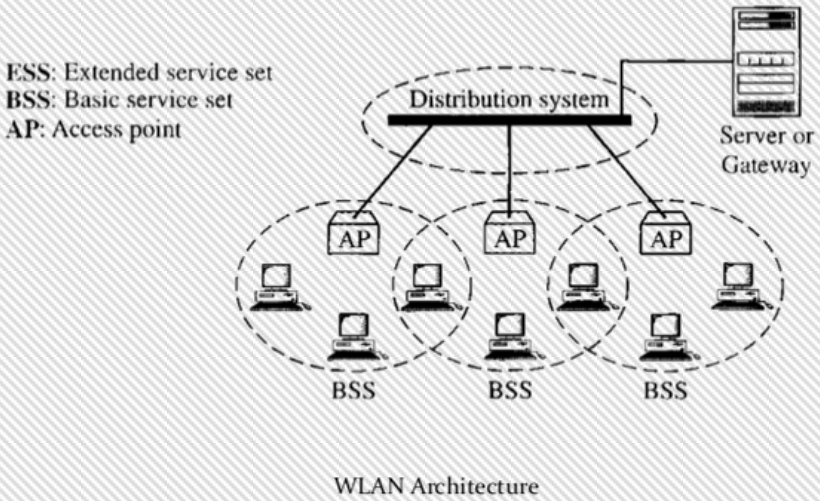
Through a gateway, a WLAN can also provide a connection to the wider Internet.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Wireless LANs have become popular for use in the home, due to their ease of installation and use.

Wireless Local Area Network

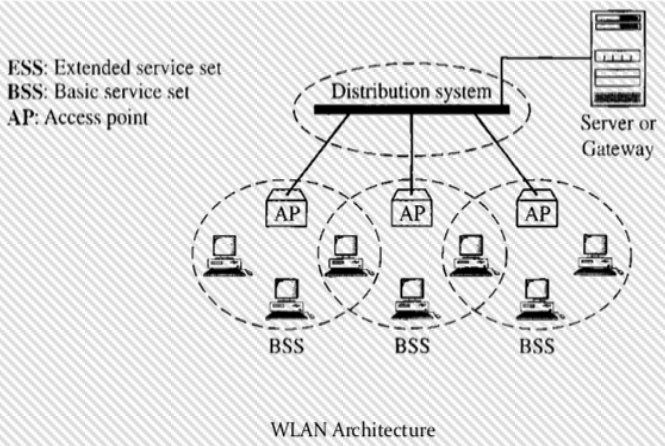
Wireless LAN Architecture



WLAN Architecture

Wireless Local Area Network

Wireless LAN Architecture



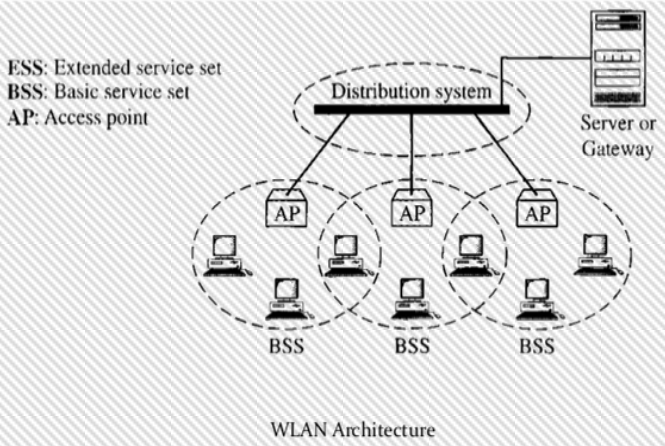
WLAN Architecture

Stations

- All components that can connect into a wireless medium in a network are referred to as stations (STA).
- All stations are equipped with wireless network interface controllers (WNICs).
- Wireless stations fall into two categories: wireless access points, and clients.

Wireless Local Area Network

Wireless LAN Architecture



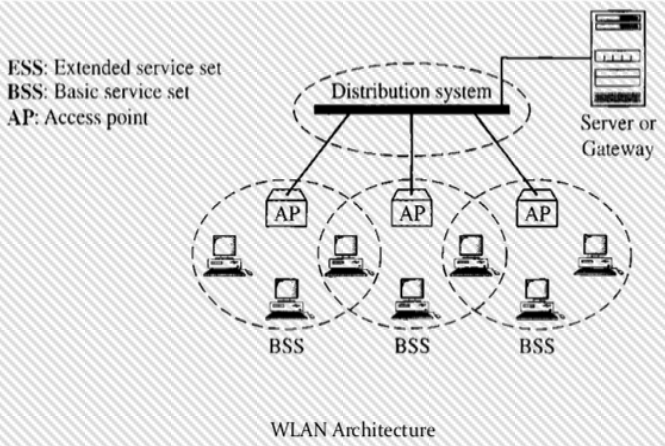
WLAN Architecture

Basic Service Set

- The basic service set (BSS) is a set of all stations that can communicate with each other at PHY layer.
- Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.
- There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS.

Wireless Local Area Network

Wireless LAN Architecture



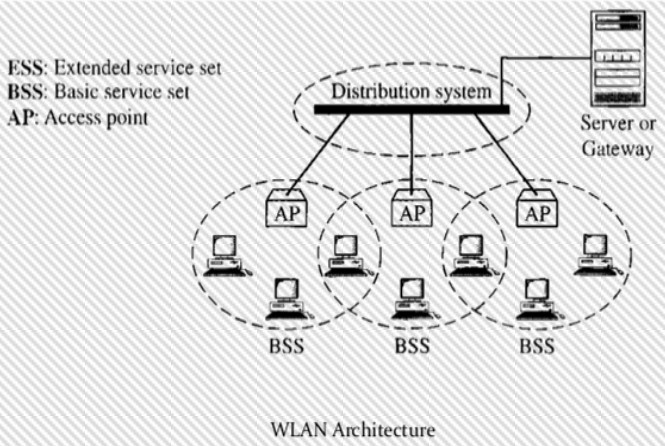
WLAN Architecture

Extended Service Set

- An extended service set (ESS) is a set of connected BSSs.
- Access points in an ESS are connected by a distribution system.
- Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

Wireless Local Area Network

Wireless LAN Architecture



WLAN Architecture

Distribution System

- A distribution system (DS) connects access points in an extended service set.
- The concept of a DS can be used to increase network coverage through roaming between cells.
- DS can be wired or wireless.

Ethernet

- Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).
- It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3, and has since been refined to support higher bit rates and longer link distances.
- The original 10BASE5 Ethernet uses coaxial cable as a shared medium, while the newer Ethernet variants use twisted pair and fiber optic links in conjunction with hubs or switches.

Wireless Fidelity (WiFi)

- Wi-Fi or WiFi is technology for radio wireless local area networking of devices based on the IEEE 802.11 standards.
- Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones and tablets, digital cameras, smart TVs, digital audio players and modern printers.
- Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point.
- Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors.

Wireless Fidelity (WiFi)

- Anyone within range with a wireless network interface controller can attempt to access a network; because of this, Wi-Fi is more vulnerable to attack (called eavesdropping) than wired networks.
- Wi-Fi Protected Access is a family of technologies created to protect information moving across Wi-Fi networks and includes solutions for personal and enterprise networks.
- Security features of Wi-Fi Protected Access have included stronger protections and new security practices as the security landscape has changed over time.

Routing

- Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.
- Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

Switching

- Switching is process to forward packets coming in from one port to a port leading towards the destination.
- When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress.
- At broad level, switching can be divided into two major categories:
- Connectionless: The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- Connection Oriented: Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

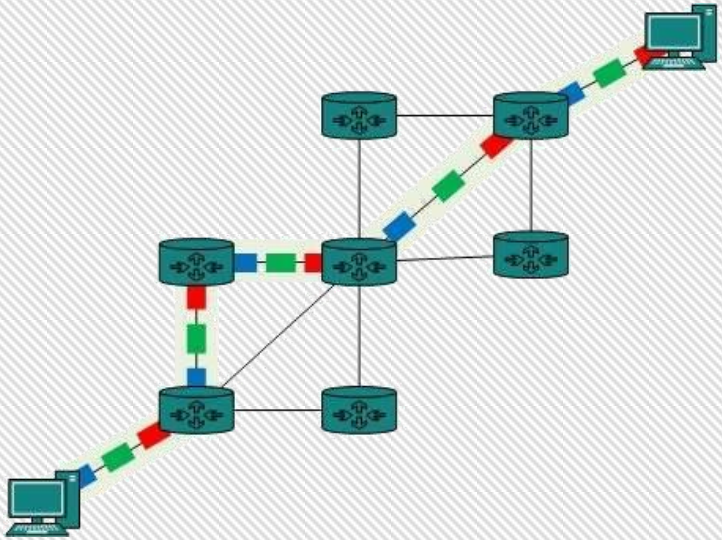
Switching

Circuit Switching

- When two nodes communicate with each other over a dedicated communication path, it is called circuit switching.
- There is a need of pre-specified route from which data will travels and no other data is permitted.
- In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.
- Circuits can be permanent or temporary.
- Applications which use circuit switching may have to go through three phases:
    1. Establish a circuit
    2. Transfer the data
    3. Disconnect the circuit

Switching

Circuit Switching



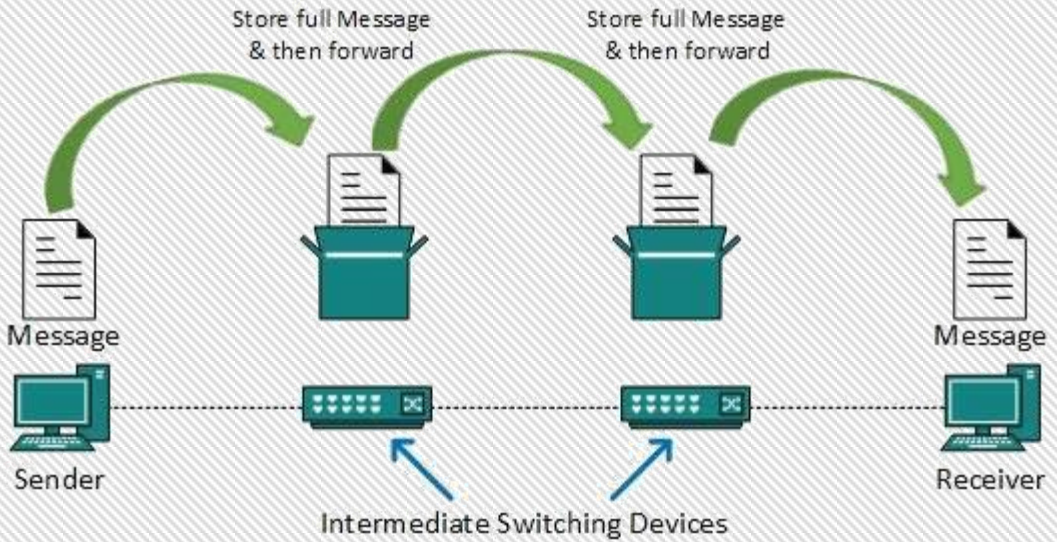
Switching

Message Switching

- This technique was somewhere in middle of circuit switching and packet switching.
- In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.
- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

Switching

Message Switching



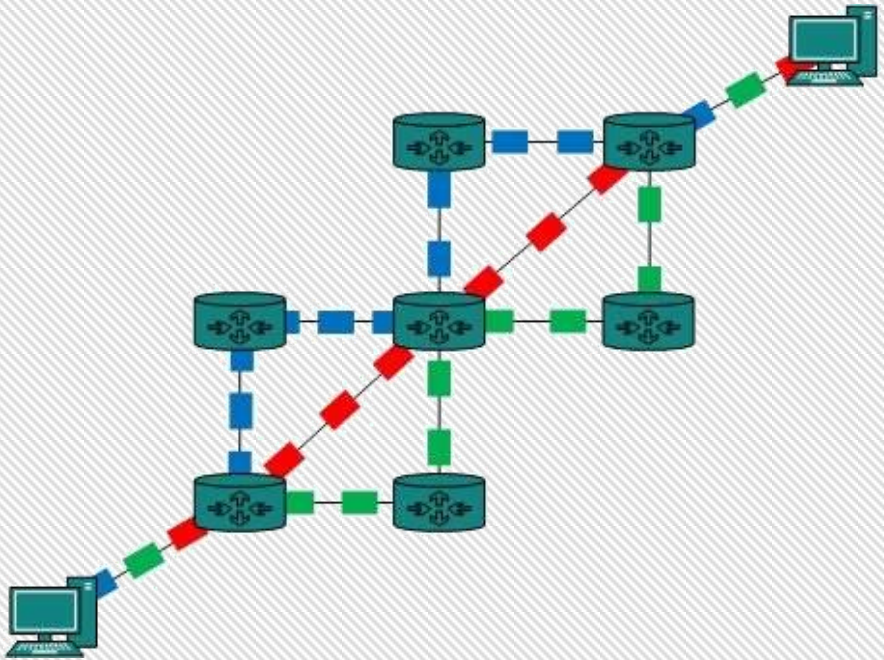
Switching

Packet Switching

- Shortcomings of message switching gave birth to an idea of packet switching.
- The entire message is broken down into smaller chunks called packets.
- The switching information is added in the header of each packet and transmitted independently.
- It is easier for intermediate networking devices to store small size packets and they do not take many resources either on carrier path or in the internal memory of switches.

Switching

Packet Switching



Network Components

NIC

- NIC stands for network interface card.
- It is a hardware component used to connect a computer with another computer onto a network.
- It can support a transfer rate of 10,100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely.
- The MAC address is stored in the PROM (Programmable read-only memory).

Network Components

HUB

- A Hub is a hardware device that divides the network connection among multiple devices.
- When computer requests for some information from a network, it first sends the request to the Hub through cable.
- Hub will broadcast this request to the entire network.
- All the devices will check whether the request belongs to them or not.
- If not, the request will be dropped.

Network Components

Switch

- A switch is a hardware device that connects multiple devices on a computer network.
- The Switch contains the updated table that decides where the data is transmitted or not.
- Switch delivers the message to the correct destination based on the physical address present in the incoming message.
- It provides a direct connection between the source and destination.
- It increases the speed of the network.

Network Components

Router

- A router is a hardware device which is used to connect a LAN with an internet connection.
- It is used to receive, analyze and forward the incoming packets to another network.
- It works in a Layer 3 (Network layer) of the OSI Reference model.
- It forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.

Network Components

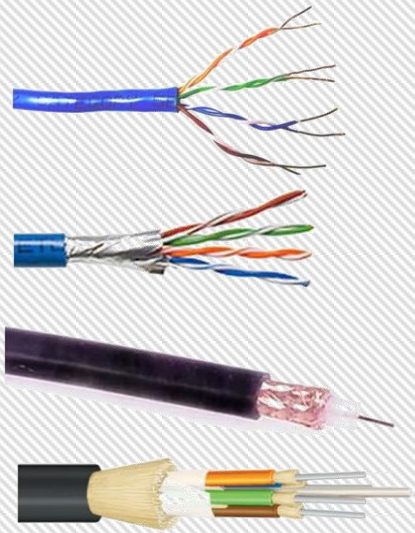
Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- It is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard.
- It stands for Modulator/Demodulator.
- It converts the digital data into an analog signal over the telephone lines.

Network Components

Cables

- Cable is a transmission media used for transmitting a signal.
- There are three types of cables used in transmission:
    1. Twisted pair cable
    2. Coaxial cable
    3. Fibre-optic cable



Varun C.M.

Assistant Professor, Department of Information Technology, St. Xavier's Catholic College of Engineering

+91 770 888 5541 contactvaruncm@gmail.com /cmvarun /c/cmvarun