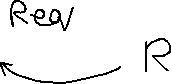
NETWORKING

Syllabus [7 layers of OSI model]:

1. Physical Layer – Cables, Topology, Transmission modes, encoding, lan, devices, modulation
2. Data Link – Stop & wait, go back and Selective Repeat, MAC Protocols, Switching, Error control, Ethernet frame format
3. Network – IP Addressing, routing protocols, IPV4 Header, IPV6 Header
4. Transport – TCP, UDP, Headers
5. Session
6. Presentation
7. Application
8. Network Security

INTRODUCTION

* **Computer Network**: Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. Computer network is a collection of two or more computers. It helps users to communicate more easily.



Computer network generally contains two components – Sender (Client) and Receiver (Server)

When Sender and Receiver are in the same machine (like keyboard and monitor in a laptop), it is called inter-process communication and is controlled by the OS.

When the sender and receiver exist separately, the communication and data exchange is controlled by computer networks.

Functionalities:

* Mandatory – The functions that cannot be neglected when client is sending a request to the server.

Error control, Flow control, MUX DeMUX

* Optional – The functions that cannot be neglected when client is sending a request to the server.

Encryption/Decryption(cryptography), Checkpoint

So that all of these functionalities are properly maintained and implemented, a standardized model called OSI model is created.

Basic Terminologies:

* Network – A network is collection of computers and devices that are connected together to enable communication and data exchange.
* Nodes – Nodes are devices that are connected to a network. These include Printers, Servers, Routers, Switches, etc.
* Protocol – A protocol is a set of rules and standards that governs how data is transmitted over a network. E.g. TCP/IP, HTTP, and FTP.
* Topology – Network topology refers to the physical and logical arrangement of nodes over a network. The common network topologies include bus, star, mesh, ring, tree.
* Service Provider Network – These types of networks give permission to take network capacity and functionality on lease from the provider.
* IP Network – An IP address is a unique numerical identifier that is assigned to every device on a network.
* DNS – The Domain Name System (DNS) is a protocol that is used to translate human readable domain names into IP addresses that computers can understand.
* Firewall – A firewall is a security device that is used to monitor and control incoming and outgoing network traffic.
* OSI Model – Open Systems Interconnection (OSI) model is a reference model that specifies standards for communication protocols and also the functionalities of each layer. The OSI, developed by the International Organization of Standardization, is a 7-layer architecture where each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are physical layer, data-link layer, network layer, transport layer, session layer, presentation layer, application layer.
* Types of Enterprise Computer Networks:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PAN | LAN | CAN | MAN | WAN |
| Full Form | Personal Area Network | Local Area Network | Campus Area Network | Metropolitan Area Network | Wide Area Network |
| Technology | Bluetooth, IrDA, Zigbee | Ethernet and WIFI | Ethernet | FDDI, CDDI, ATM | Leased Line, Dial-Up |
| Range | 1-100 m | Up to 2 km | 1-5km | 5-50 km | Above 50km |
| Transmission Speed | Very High | Very High | High | Average | Low |
| Area | Within a Room | Within office, building | Within University, Corporate Offices | Within a city | Within countries |
| Ownership | Private | Private | Private | Private or Public | Generally Public |
| Maintenance | Very Easy | Easy | Moderate | Difficult | Very Difficult |
| Error Rate and Cost | Very Low | Low | Moderate | High | Very High |

PAN

LAN

CAN

MAN

WAN

* Physical Layer in OSI Model:

The physical layer is the bottom-most layer in the Open System Interconnection (OSI) model which is a physical and electrical representation of the system.

It consists of various network components such as power plugs, connectors, receivers, cable types, etc.

Functionalities ->

* Cables and Connectors
* Physical Topology
* Hardware
* Transmission mode
* Multiplexing
* Encoding
* Topology:

Network topology is the way that defines the structure, and how different components are connected together.

In other words, the arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology.

* Point to Point Technology

Point to point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point to Pint provides high bandwidth.

* Mesh Topology

In a Mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



* Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active hub which have repeaters in them.



* Bus Topology

Bus topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional, a multipoint connection and a non-robust topology because if the backbone fails, the topology crashes.



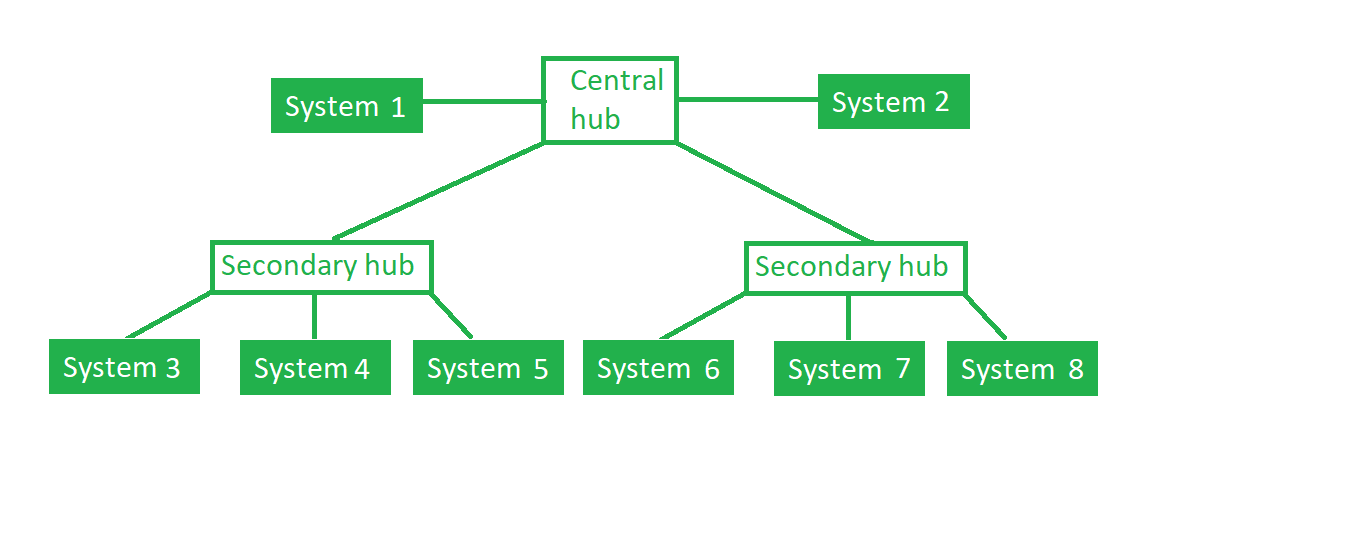
* Ring Topology

In a Ring topology, it forms a ring connecting devices with exactly two neighboring nodes. A number of repeaters are used for ring topology with a large number of nodes, because if someone wants to send data to the last node in a ring topology with 100 nodes, the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss, repeaters are used in the network.



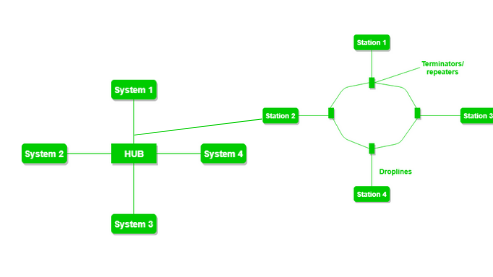
* Tree Topology

Tree topology is a variation of Star topology which has a hierarchical flow of data. In tree topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.

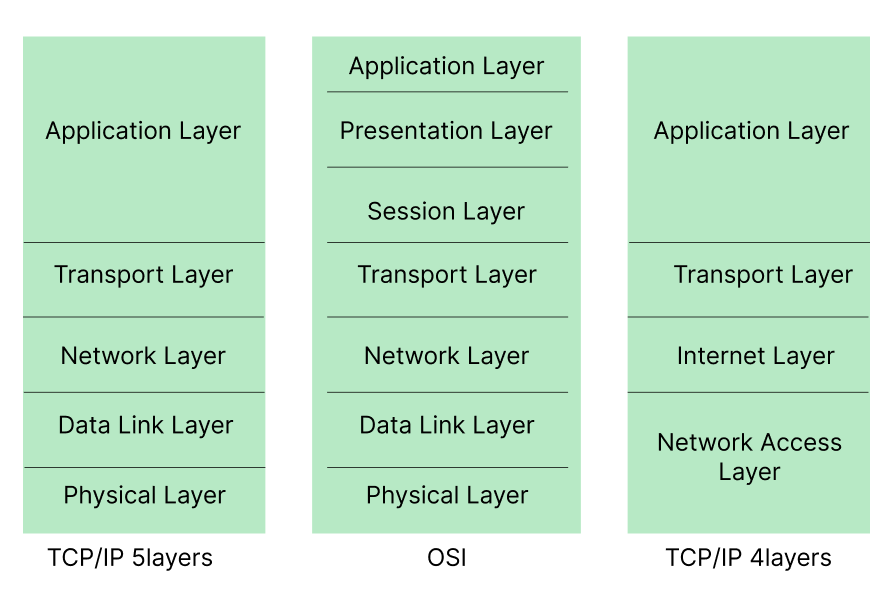


* Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied earlier. Hybrid topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above.



* **TCP/IP Protocol: [TCP/IP vs. OSI]**

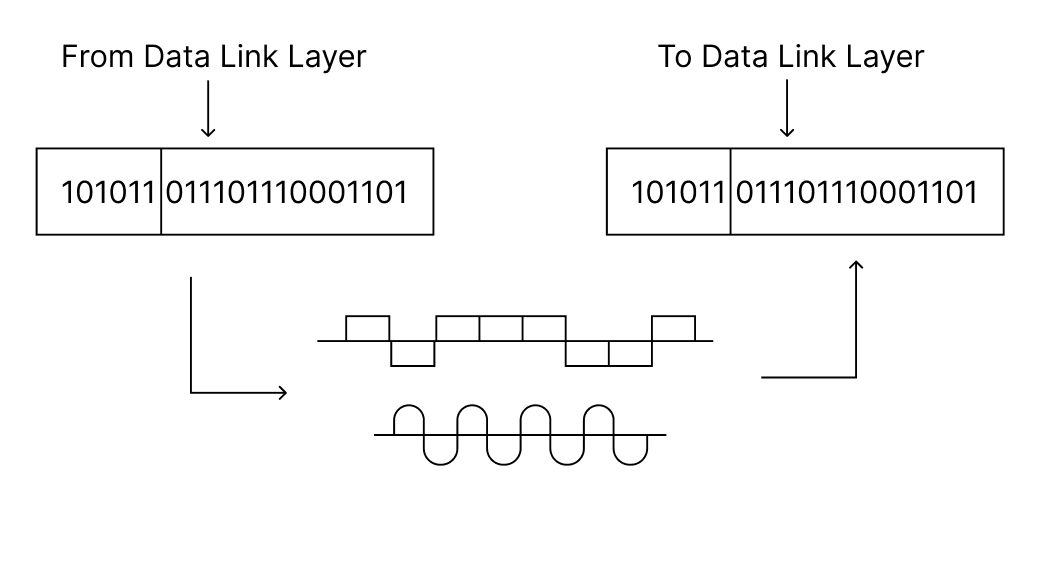


TCP/IP protocol is the practical approach of Networking while OSI is the theoretical approach.

TCP/IP Protocol Suit [Transport Control Protocol or Internet Protocol] was developed by ARPANET and supports client-server and peer to peer.

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining accuracy of the data while transferring from one end to another end.

PHYSICAL LAYER



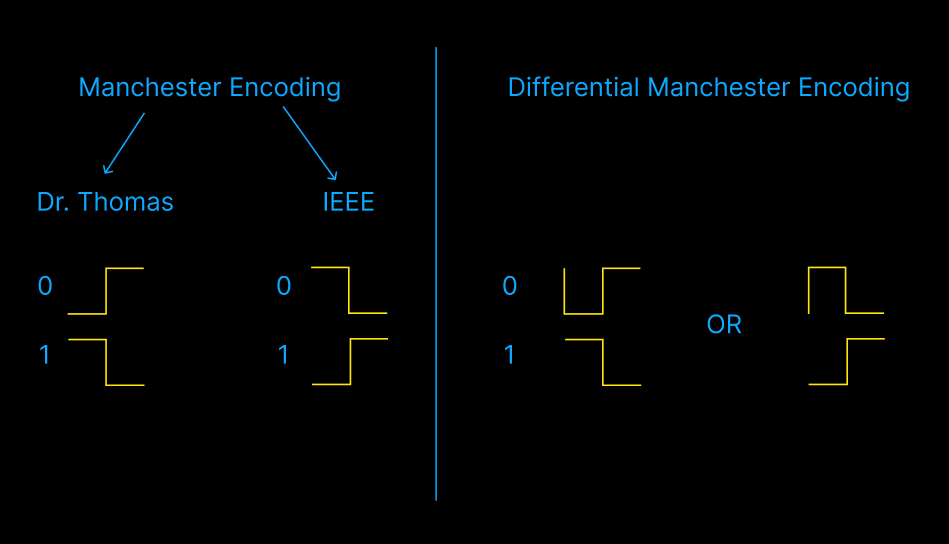
The physical layer is the bottom-most layer in the Open System Interconnection (OSI) model which is a physical and electrical representation of the system. The physical layer consists of various hardware components such as connectors, switches, power plugs, cable types, receivers, etc.

The physical layer sends **data bits** from one device to another device. The physical layer is responsible for the communication for unstructured raw data streams over a physical medium.

Functions performed by the physical layer:

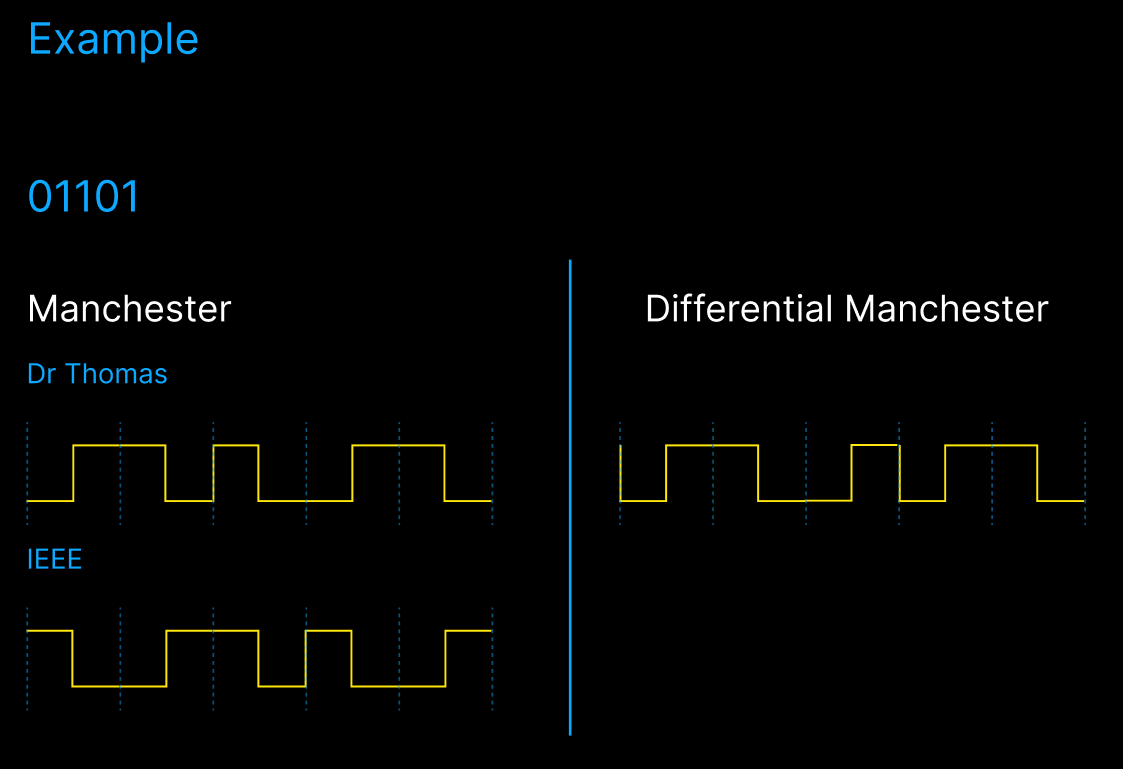
* Cables and connectors
* Physical topology (Mesh, Star, Bus, Ring)
* Hardware (Repeaters, hubs)
* Transmission mode
* Multiplexing
* Encoding

Manchester Encoding and Differential Manchester encoding



Remembering:

Manchester: 0 (Zero) looks like a Z in IEEE convention.

Differential Manchester: 0 means edge and 1 means continuous. 

Various devices in Computer Networks

1. Cables (H/W):

* **Unshielded Twisted Cable:** UTP cable is commonly used in networking for connecting devices in the Local Area Network (LAN). It consists of pairs of insulated copper wires twisted together.
* **Coaxial Cable:** Coaxial cables are commonly used for cable television distribution, broadband internet access and some Ethernet networks. They offer better shielding against interference compared to UTP cables, making them suitable for longer distance transmissions and environments with higher interference levels.
* **Fiber Optic:** Fiber optic cable uses light to transmit data instead of electrical signals like UTP and coaxial cables. It contains a core of glass or plastic fibers, surrounded by a cladding layer that reflects light inward, and outer protective layer.
* **100 Base T:** 100 means 100 mbps, Base means Baseband or broadband, T means the distance (attenuation). After T\*100 meters, the signal starts to dissipate.

1. Repeaters (H/W):

Repeater regenerates the input signal and forwards it. For e.g. if we have a 10Base2 signal, the signal starts losing its strength after 200m. We can use a repeater after 200m to conserve the signal strength.

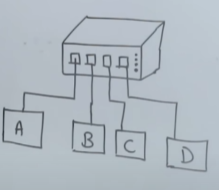
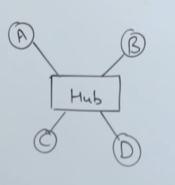
Characteristics:

* 2 Port Device
* Forwarding
* No Filtering
* Collision Domain is n (maximum).

1. Hubs (H/W):

A hub is basically a **multi-port repeater**.

Hub in networking plays a vital role in data transmission and broadcasting. A hub is a hardware device used at the physical layer to connect multiple devices in the network. Hubs are widely **used to connect** **LANs**. A hub has multiple ports and unlike a switch, it **cannot filter the data** so it broadcasts or sends the message to each port.



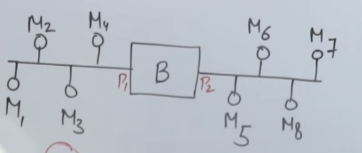
Collision domain is n (maximum)

1. Bridges (H/W and S/W)

Bridges are used to **connect two different LANs**. E.g. we can connect a Token Ring LAN (using ring topology) and a Token Bus LAN (using Bus topology) using a bridge. They work on both Physical layer and Data-link layer.

Each packet should have the source MAC address and destination MAC address which the bridge can check to determine whether message should be forwarded across the bridge or not. Hence **bridges offer filtering**.

E.g. If M1 packet sends a message to M3 packet, the bridge decides that the message doesn’t need to be forward across.



Bridges use their own buffer which uses the “store and forward” technique. Hence there are **rarely any collisions**.

Bridges are of two types:

* Static Bridge: The MAC-Port table is maintained manually by a network administrator.
* Dynamic/Transparent Bridge: The MAC-Port table gets set automatically after making a few mistakes at first.

1. Switches (H/W and S/W):

A switch is basically a **multiport bridge** and it’s a data-link layer device.

Traffic is minimal.

Full-duplex links and collision domain in 0.

1. Routers (H/W and S/W):

A router is a networking device that forwards data packets between computer networks. One or more packet-switched networks or sub-networks 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.

COLLISION DOMAIN VS BROADCAST DOMAIN:

|  |  |  |  |
| --- | --- | --- | --- |
| SL NO | Device Name | Collision Domain | Broadcast Domain |
| 1 | Repeater (Layer 1) | No change | No change |
| 2 | Hub (Layer 1) | No change | No change |
| 3 | Bridge (Layer 1 & 2) | Reduced | No change |
| 4 | Switch (Layer 1 & 2) | Reduced | No change |
| 5 | Router (Layer 2) | Reduced | Reduced |