CMR INSTITUTE OF TECHNOLOGY

* UGC AUTONOMOUS *

* Approved by AICTE * Accredited by NAAC with 'A' Grade * All B.Tech programs Accredited by NBA*

(Kandlakoya (v),Medchal Road,Hyderabad - 501 401)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

II – B.Tech – II – Sem (CSE 'C' & CSE – DS 'A')

COMPUTER NETWORKS (20-CS-PC-224)
(R20 Regulations)

By

Dr.A.Nirmal Kumar

COMPUTER NETWORKS

SYLLABUS

Unit	Title/Topics	Hours
I	**Overview of the Internet, Physical layer and Data link layer**	10
Overview of the Internet: Protocols and standards, Layering scenario, TCP/IP Protocol Suite, The OSI model, Internet history and administration, Comparison of the OSI and TCP/IP reference model. **Physical layer:** Transmission Media, Guided Media, wireless transmission Media. **Data link layer**: Design issues, CRC Codes, Elementary Data Link layer Protocols, sliding Window Protocol. ***Task:*** *Write a program to compute CRC code for the polynomials.*		
II	**Multiple Access protocols**	9
Multiple Access protocols-Aloha, CSMA, Collision free protocols, Ethernet –Physical layer, Ethernet Mac sub layer, Data link layer switching and use of bridges, learning bridges ,Spanning tree bridges, repeaters, hubs, bridges, switches ,routers and gateways. ***Task:*** *Write a program for 1 bit collision free protocol.*		
III	**Network layer and Routing Algorithms**	5+5=10
Part-A: Network layer: Network layer Design issues, store and forward packet switching connection less and connection oriented networks. ***Task:*** *Write a program to implement i) Character stuffing ii) Bit stuffing.*		
Part-B: Routing Algorithms: Optimality principle, shortest path, flooding, distance vector routing, count to infinity problem, hierarchical routing, congestion control algorithms and admission control. ***Task:*** *Implement distance vector routing algorithm for obtaining routing tables at each node.*		
IV	**Internetworking and Transport Layer**	9
Internetworking: Tunneling, internetwork Routing, Packet fragmentation, IPV4, IPV6 Protocol, IP addresses, CIDR, ICMP, ARP, RARP, DHCP. **Transport Layer**: Services provided to the upper layers elements of transport protocol-addressing connection establishment, connection release. ***Task:*** *Write a program to demonstrate ARP.*		
V	**TCP/IP and Application Layer**	10
TCP/IP: The internet Transport protocols UD-RPC, Real time Transport protocols, The internet Transport protocols-Introduction to TCP, The TCP services model ,The TCP segment Header, The connection Establishment, The TCP Connection release, The TCP Connection management modeling, The TCP Sliding Window, The TCP Congestion Control. **Application Layer**: Introduction, Providing services, Applications layer paradigms, HTTP, FTP, electronic mail, DNS, SSH. ***Task:*** *Write a program to implement RPC.*		

TEXT BOOKS & REFERENCES

Textbooks:
1. Data Communications and Networking – Behrouz A Forouzan, Fourth Edition, TMH. 2. Computer Networks - Andrew S Tanenbaum, 4th Edition. Pearson Education/PHI
References:
1. Introduction to Data communication and Networking, Tamasi, Pearson Education 2. Computer Networking: A Top-Down Approach Featuring the Internet, James F. Kurose, Keith W. Ross, 3rd Edition, Pearson.

COURSE OUTCOMES

Upon completion of the course, the student will be able

CO 1: To outline the basics of computer networks and various layers **(Unit – I)**

CO 2: To demonstrate multiple access protocols (Unit – II)

CO 3: To interpret network layer and routing algorithms **(Unit – III)**

CO 4: To illustrate internetworking and various transport protocols **(Unit – IV)**

CO 5: To make use of various protocols of application layer **(Unit – V)**

UNIT – II

Multiple Access protocols-Aloha, CSMA, Collision free protocols, Ethernet –Physical layer, Ethernet Mac sub layer, Data link layer switching and use of bridges, learning bridges ,Spanning tree bridges, repeaters, hubs, bridges, switches ,routers and gateways.

- ***Task:*** *Write a program for 1 bit collision free protocol.*

Multiple access protocol- ALOHA, CSMA, CSMA/CA and CSMA/CD

Data Link Layer

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as **media access control** or the multiple access resolutions.

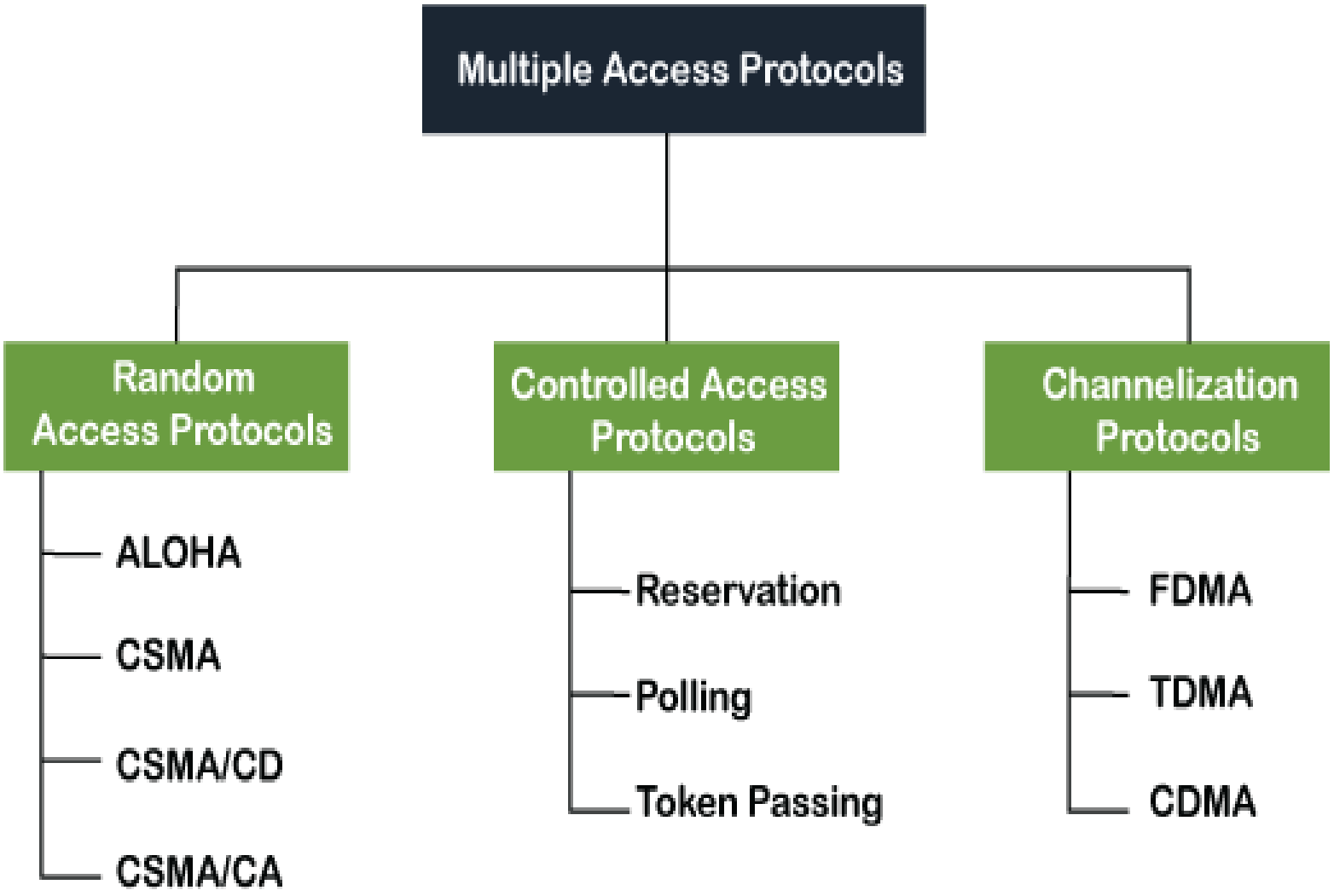
Data Link Control

A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

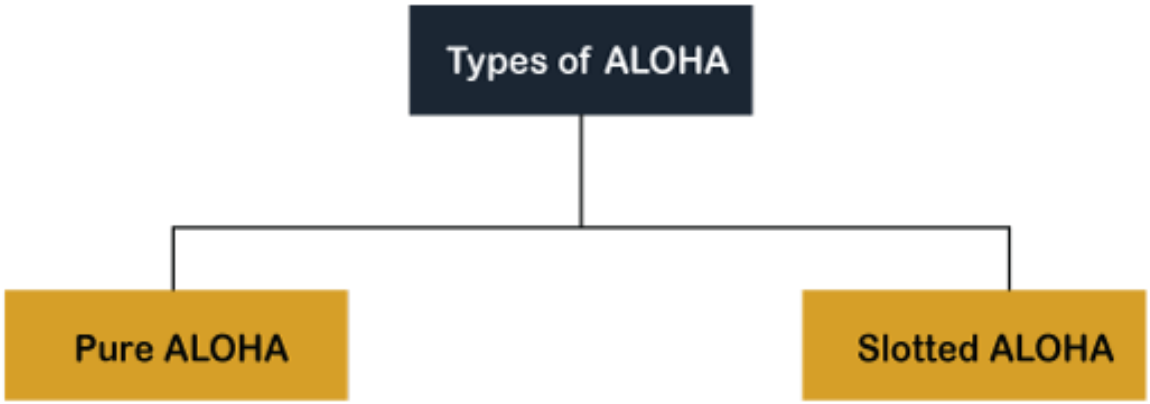

Multiple Access Protocols
Random Access Protocols
Controlled Access Protocols
Channelization Protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token Passing
FDMA
TDMA
CDMA

A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.



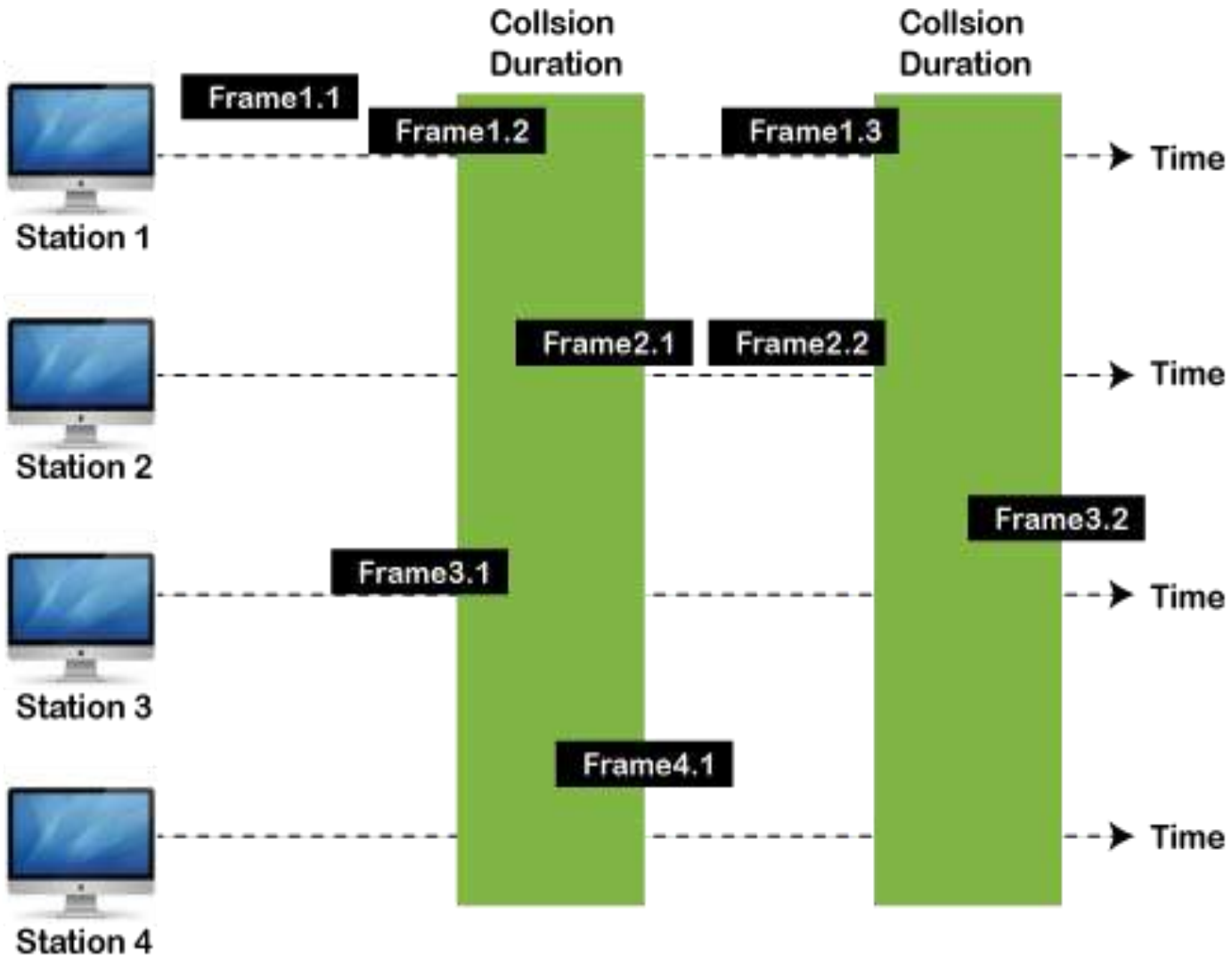
Aloha Rules

- Any station can transmit data to a channel at any time.
- It does not require any carrier sensing.
- Collision and data frames may be lost during the transmission of data through multiple stations.
- Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
- It requires retransmission of data after some random amount of time.

Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

- The total vulnerable time of pure Aloha is 2 * Tfr.
- Maximum throughput occurs when G = 1/ 2 that is 18.4%.
- Successful transmission of data frame is S = G * e ^ - 2 G.



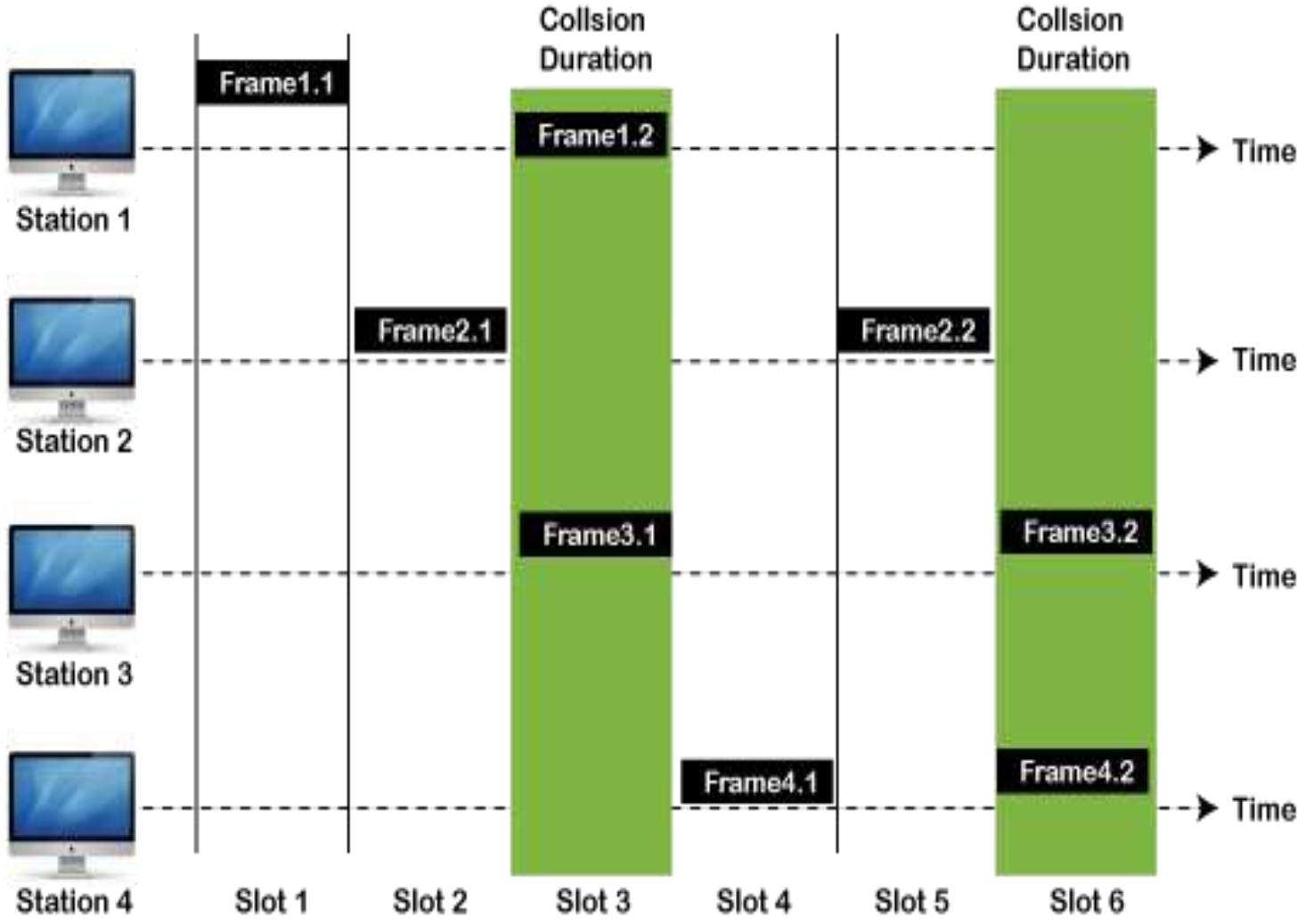
Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

- Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
- The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
- The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

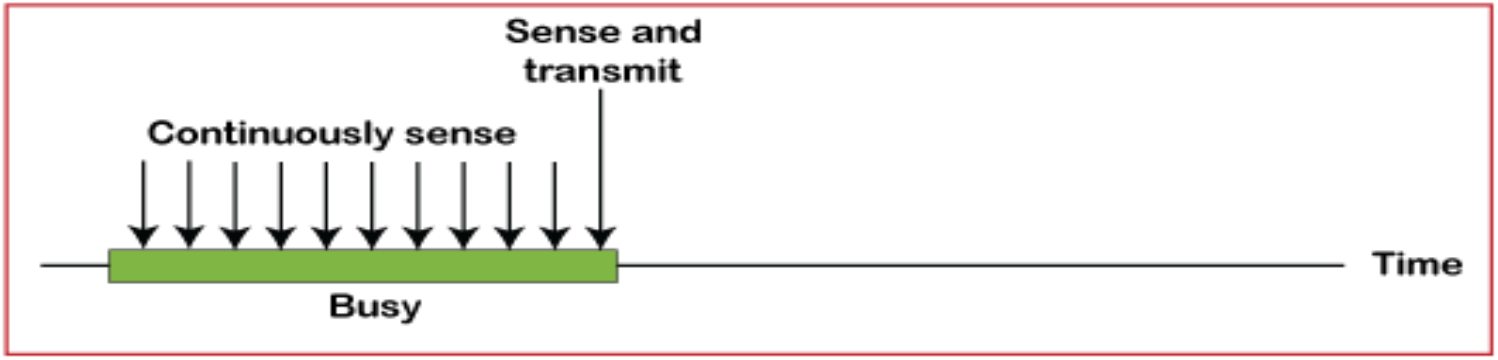
It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA Access Modes

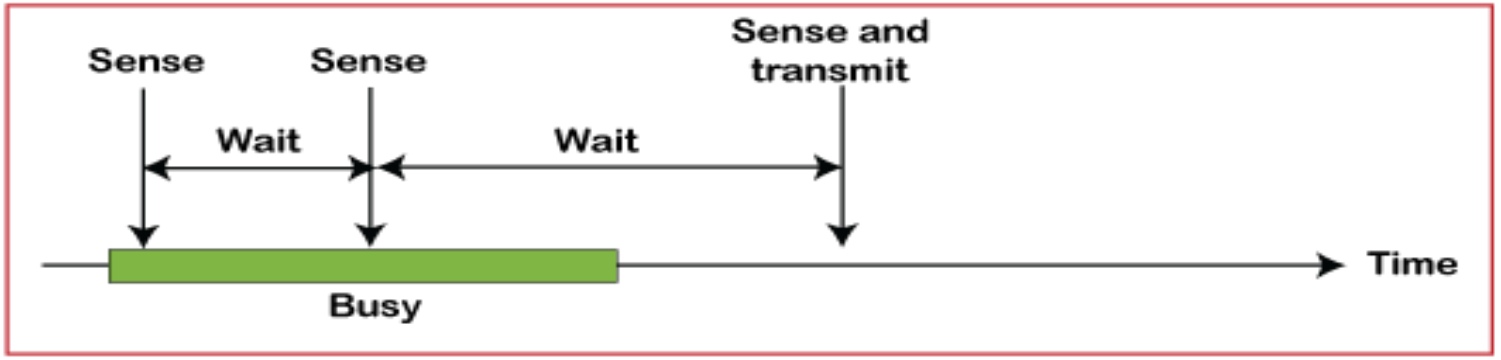
- **1-Persistent:** In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

- **Non-Persistent:** It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.
- **P-Persistent:** It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

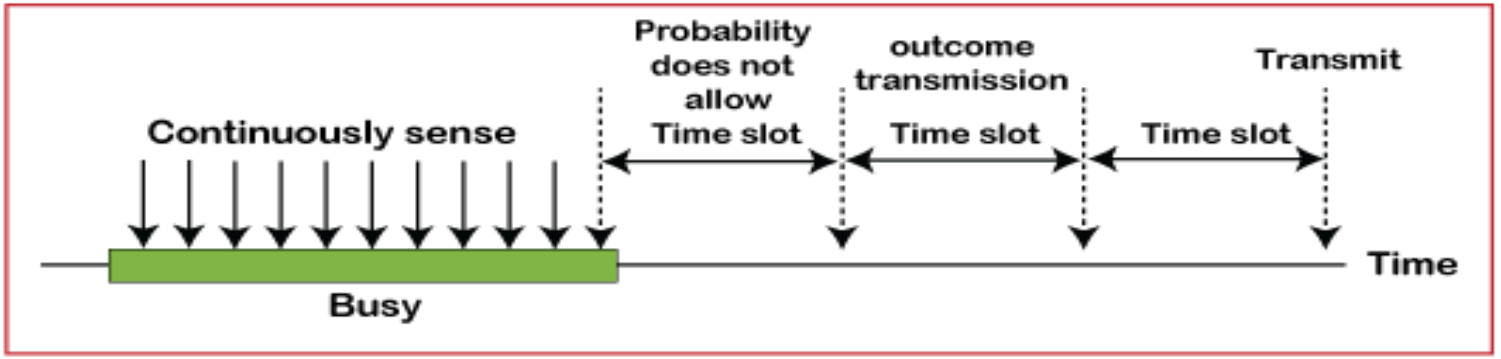
O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

Collision Free Protocols

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

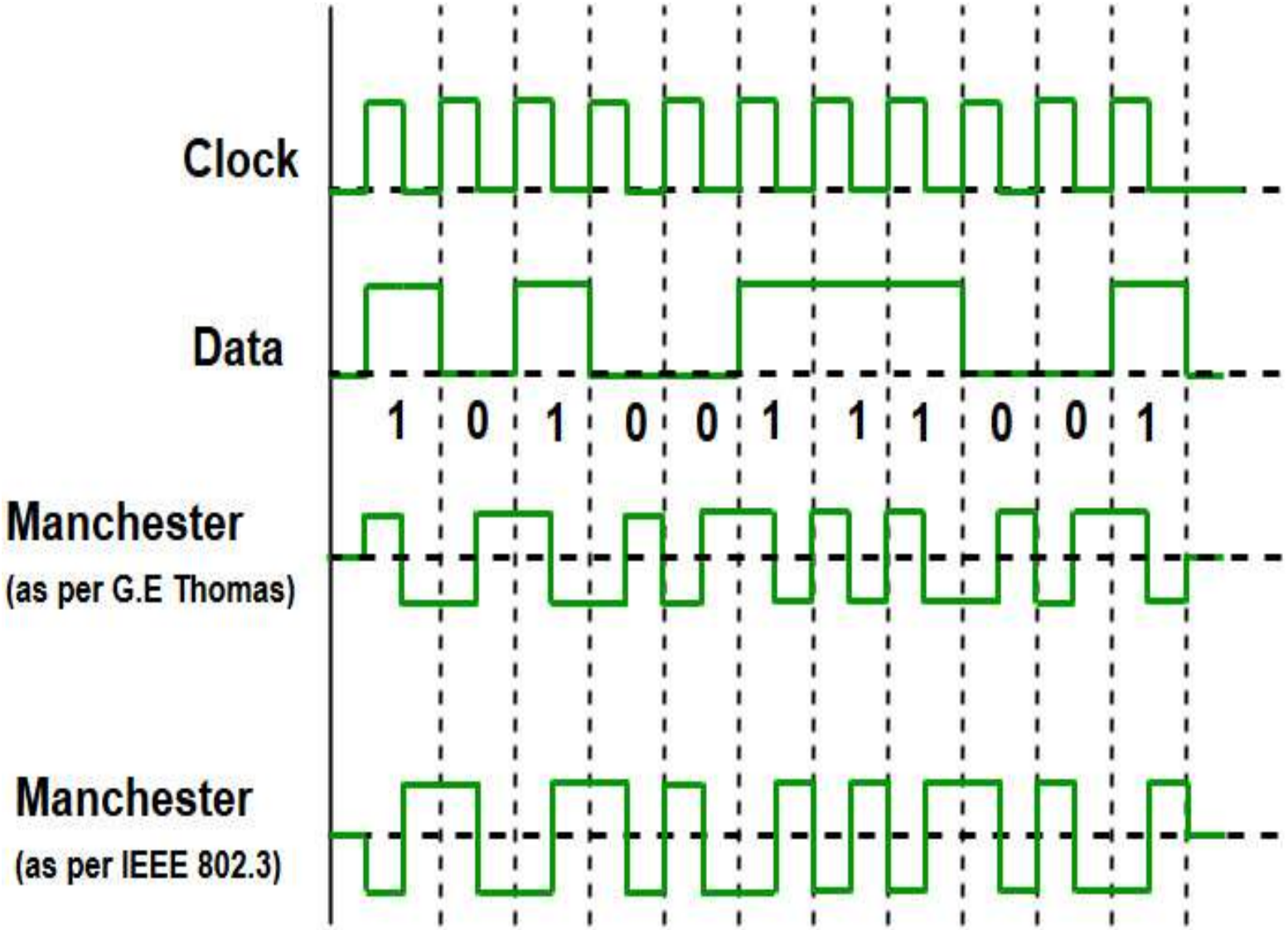
Following are the methods used in the CSMA/ CA to avoid the collision:

- **Interframe space**: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

- **Contention window**: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.
- **Acknowledgment**: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

Ethernet – Physical Layer

Ethernet is the most widely used LAN technology, which is defined under IEEE standards 802.3. The reason behind its wide usability is Ethernet is easy to understand, implement, maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of topologies that are allowed. Ethernet generally uses Bus Topology. Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer. For Ethernet, the protocol data unit is Frame since we mainly deal with DLL. In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD. Manchester Encoding Technique is used in Ethernet.


Clock
Data
1 0 1 0 0 1 1 1 0 0 1
Manchester
(as per G.E Thomas)
Manchester
(as per IEEE 802.3)

Since we are talking about IEEE 802.3 standard Ethernet, therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition. In both Manchester Encoding and Differential Manchester, the Encoding Baud rate is double of bit rate.

Baud Rate = 2 * Bit Rate

Ethernet LANs consist of network nodes and interconnecting media or links. The network nodes can be of two types:

Data Terminal Equipment (DTE):- Generally, DTEs are the end devices that convert the user information into signals or reconvert the received signals. DTEs devices are: personal computers, workstations, file servers or print servers also referred to as end stations. These devices are either the source or the destination of data frames. The data terminal equipment may be a single piece of equipment or multiple pieces of equipment that are interconnected and perform all the required functions to allow the user to communicate. A user can interact with DTE or DTE may be a user.

Data Communication Equipment (DCE):-

DCEs are the intermediate network devices that receive and forward frames across the network. They may be either standalone devices such as repeaters, network switches, routers, or maybe communications interface units such as interface cards and modems. The DCE performs functions such as signal conversion, coding, and maybe a part of the DTE or intermediate equipment.

Currently, these data rates are defined for operation over optical fibers and twisted-pair cables:

i) Fast Ethernet

Fast Ethernet refers to an Ethernet network that can transfer data at a rate of 100 Mbit/s.

ii) Gigabit Ethernet

Gigabit Ethernet delivers a data rate of 1,000 Mbit/s (1 Gbit/s).

iii) 10 Gigabit Ethernet

10 Gigabit Ethernet is the recent generation and delivers a data rate of 10 Gbit/s (10,000 Mbit/s). It is generally used for backbones in high-end applications requiring high data rates.

Medium Access Control Sublayer (MAC sublayer)

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

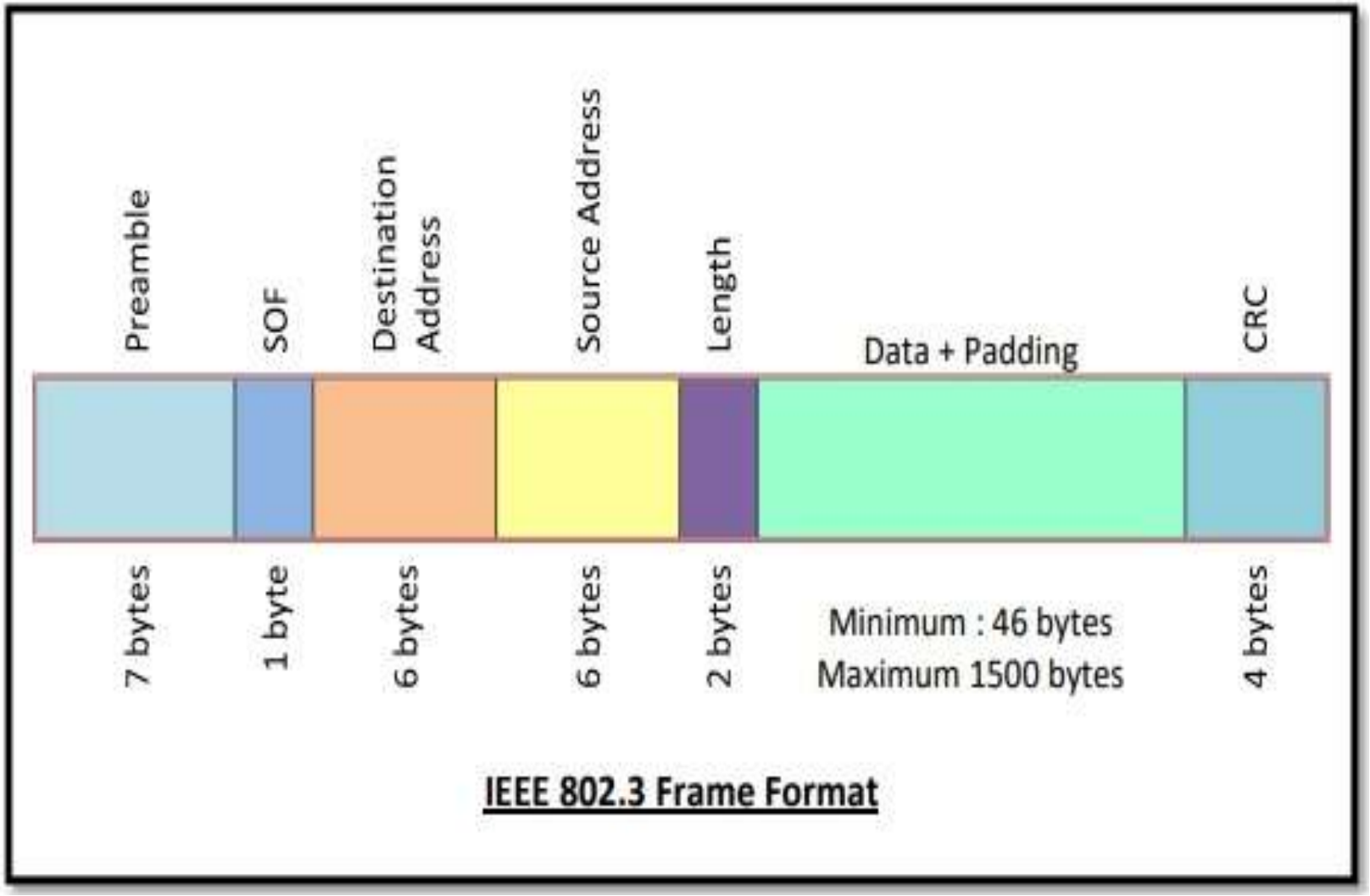
MAC Addresses

- MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.
- MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

What is Classic Ethernet MAC Sublayer Protocol?

- Classic Ethernet is the original form of Ethernet used primarily in LANs. It provides data rates between 3 to 10 Mbps.It operates both in the physical layer and in the MAC sublayer of the OSI model. In the physical layer, the features of the cables and networks are considered. In MAC sublayer, the frame formats for the Ethernet data frame are laid down.
- Classic Ethernet was first standardized in 1980s as IEEE 802.3 standard.

Frame Format of Classic Ethernet



- **Preamble** − It is the starting field that provides alert and timing pulse for transmission. In case of Ethernet (DIX) it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- **Start of Frame Delimiter (SOF)** − It is a 1 byte field in an IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address** − It is a 6 byte field containing physical address of destination stations.
- **Source Address** − It is a 6 byte field containing the physical address of the sending station.

- **Type/Length** − This is a 2 byte field. In case of Ethernet (DIX), the field is type that instructs the receiver which process to give the frame to. In case of IEEE 802.3, the field is length that stores the number of bytes in the data field.
- **Data** − This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding** − This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC** − CRC stands for cyclic redundancy check. It contains the error detection information.

Switching by Bridges

When a data frame arrives at a particular port of a bridge, the bridge examines the frame's data link address, or more specifically, the MAC address. If the destination address as well as the required switching is valid, the bridge sends the frame to the destined port. Otherwise, the frame is discarded.

The bridge is not responsible for end to end data transfer. It is concerned with transmitting the data frame from one hop to the next. Hence, they do not examine the payload field of the frame. Due to this, they can help in switching any kind of packets from the network layer above.

Bridges also connect virtual LANs (VLANs) to make a larger VLAN. If any segment of the bridged network is wireless, a wireless bridge is used to perform the switching.

There are three main ways for bridging −

- simple bridging
- multi-port bridging
- learning or transparent bridging

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.

- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Spanning Tree Bridges

Spanning Tree Protocol (STP) is a communication protocol operating at data link layer the OSI model to prevent bridge loops and the resulting broadcast storms. It creates a loop − free topology for Ethernet networks.

Working Principle

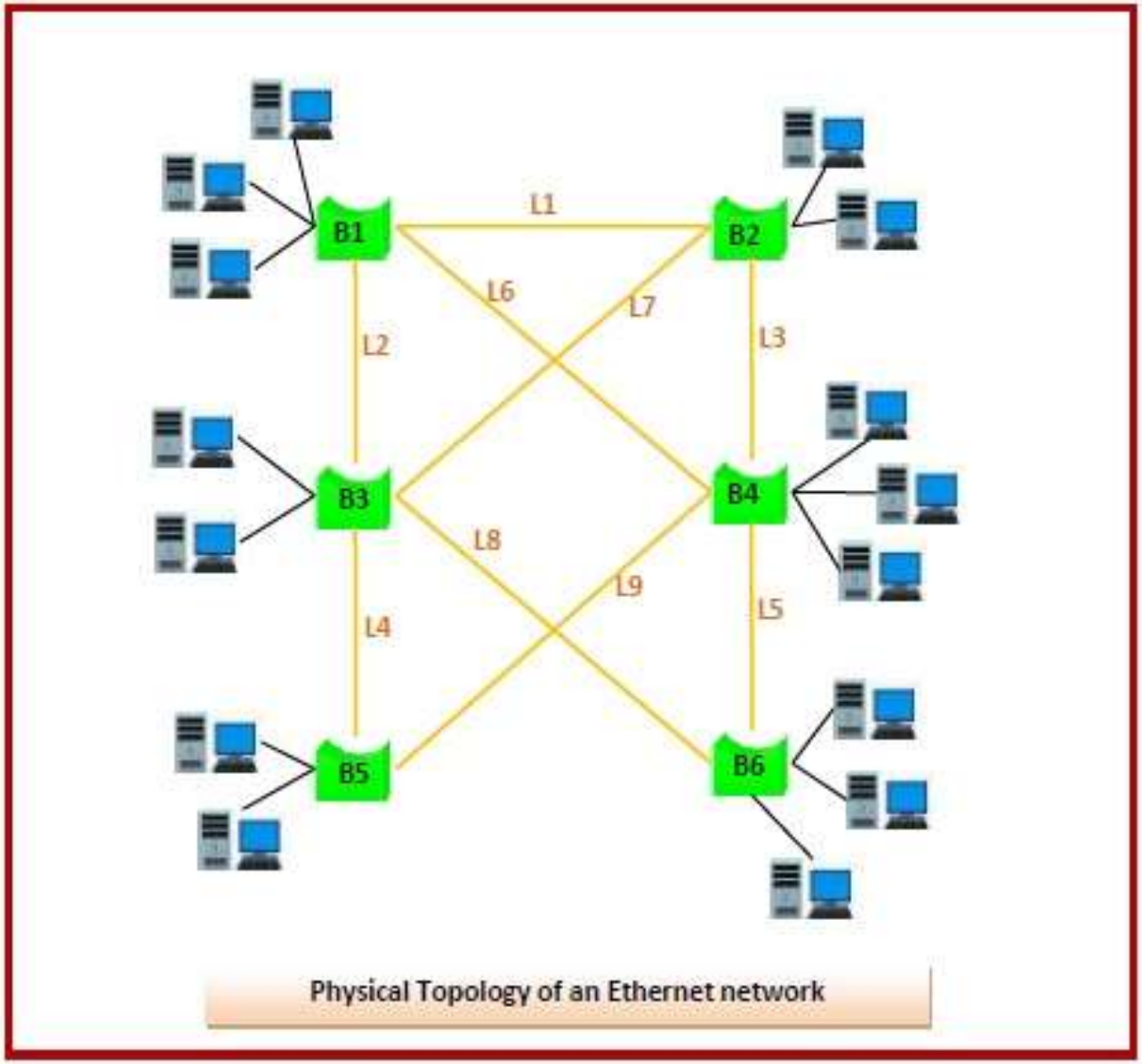
- A bridge loop is created when there are more than one paths between two nodes in a given network. When a message is sent, particularly when a broadcast is done, the bridges repeatedly rebroadcast the same message flooding the network.

- Since a data link layer frame does not have a time-to-live field in the header, the broadcast frame may loop forever, thus swamping the channels.
- Spanning tree protocol creates a spanning tree by disabling all links that form a loop or cycle in the network. This leaves exactly one active path between any two nodes of the network. So when a message is broadcast, there is no way that the same message can be received from an alternate path. The bridges that participate in spanning tree protocol are often called **spanning tree bridges**.

- To construct a spanning tree, the bridges broadcast their configuration routes. Then they execute a distributed algorithm for finding out the minimal spanning tree in the network, i.e. the spanning tree with minimal cost. The links not included in this tree are disabled but not removed.
- In case a particular active link fails, the algorithm is executed again to find the minimal spanning tree without the failed link. The communication continues through the newly formed spanning tree. When a failed link is restored, the algorithm is re-run including the newly restored link.

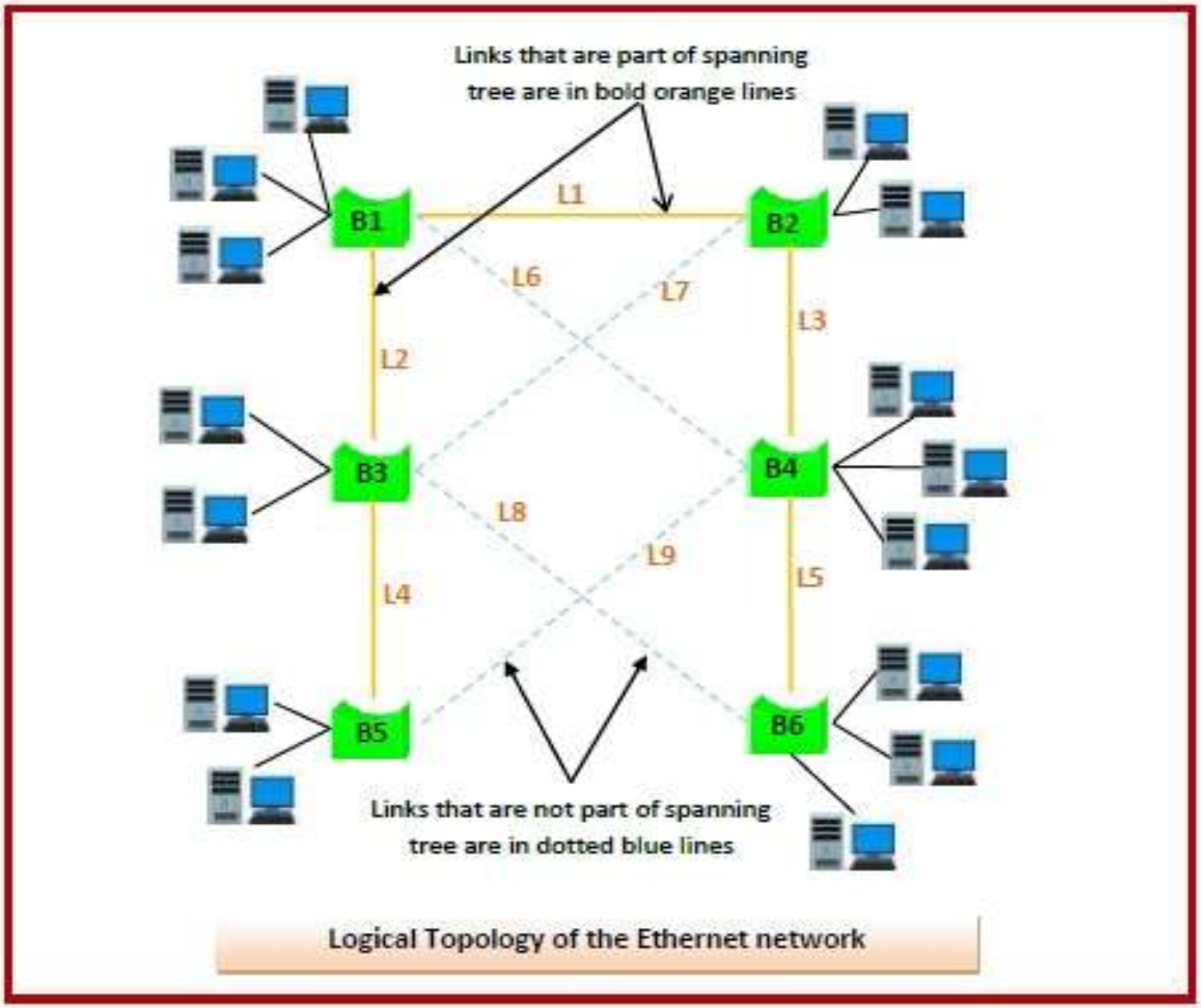
Example

- Let us consider a physical topology, as shown in the diagram, for an Ethernet network that comprises of six interconnected bridges. The bridges are named {B1, B2, B3, B4, B5, B6} and several nodes are connected to each bridge. The links between two bridges are named {L1, L2, L3, L4, L5, L6, L7, L8, L9}, where L1 connects B1 and B2, L2 connects B1 and B3 and so on. It is assumed that all links are of uniform costs. From the diagram we can see that there are multiple paths from a bridge to any other bridge in the network, forming several bridge loops that makes the topology susceptible to broadcast storms.



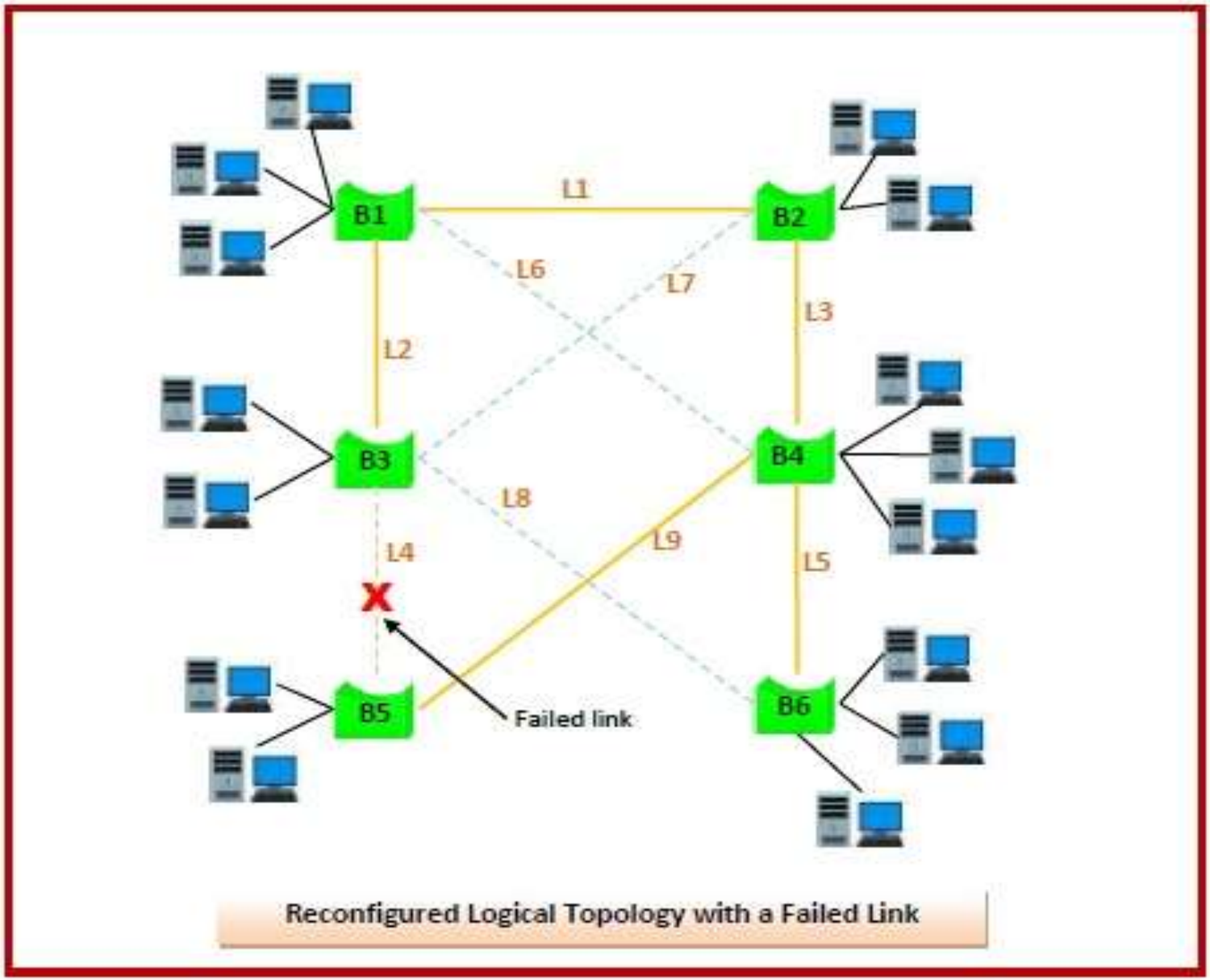
Physical Topology of an Ethernet network

According to spanning tree protocol, links that form a cycle are disabled. Thus,we get a logical topology so that there is exactly one route between any two bridges. One possible logical topology is shown in the following diagram below containing links {L1, L2, L3, L4, L5} –



Logical Topology of the Ethernet network

In the above logical configuration, if a situation arises such that link L4 fails. Then, the spanning tree is reconstituted leaving L4. A possible logical reconfiguration containing links {L1, L2, L3, L5, L9} is as follows −



Reconfigured Logical Topology with a Failed Link

Network Devices

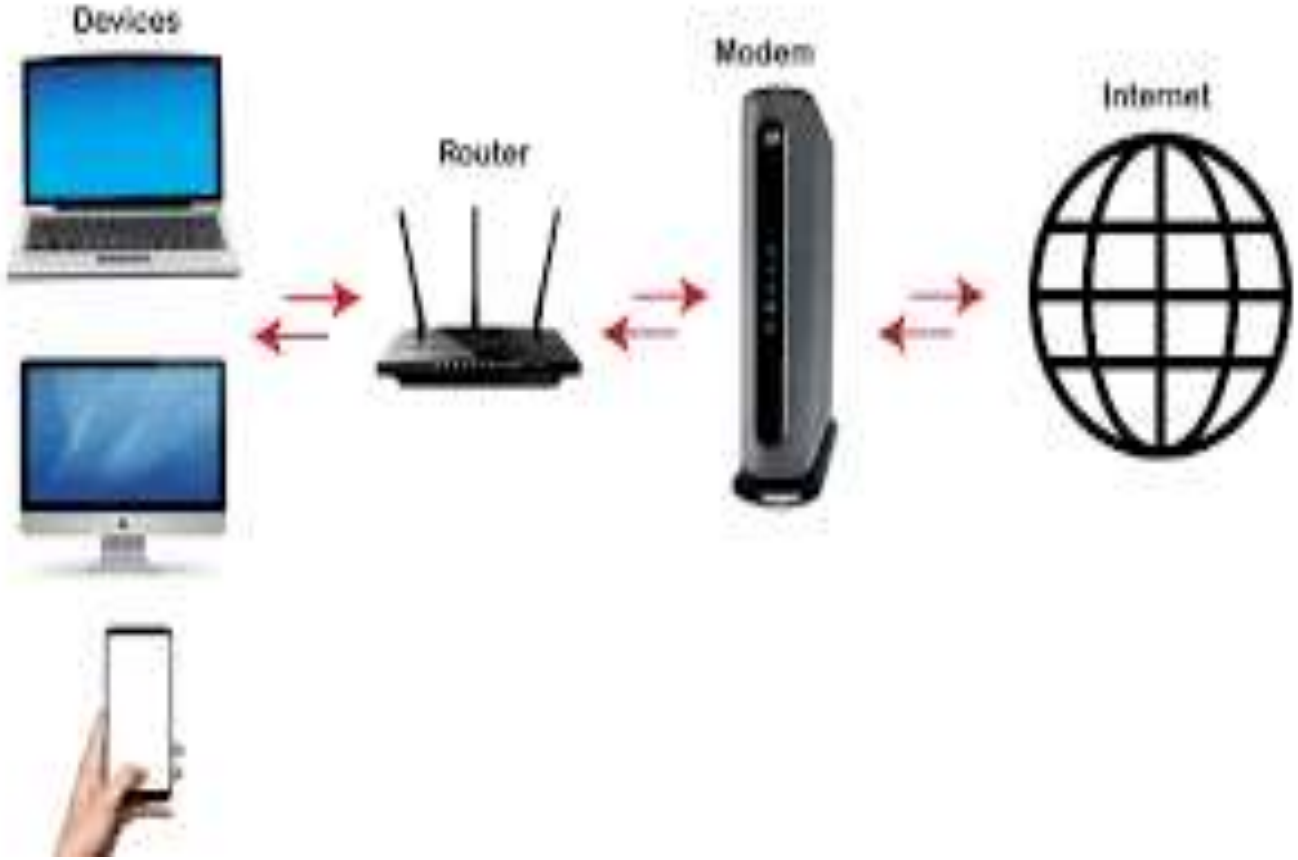
Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc.

Modem

- Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.
- The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − modulator and demodulator. The modulator converts digital data into analog data when the data is being sent by the computer. The demodulator converts analog data signals into digital data when it is being received by the computer.

Types of Modem

- **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
- **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

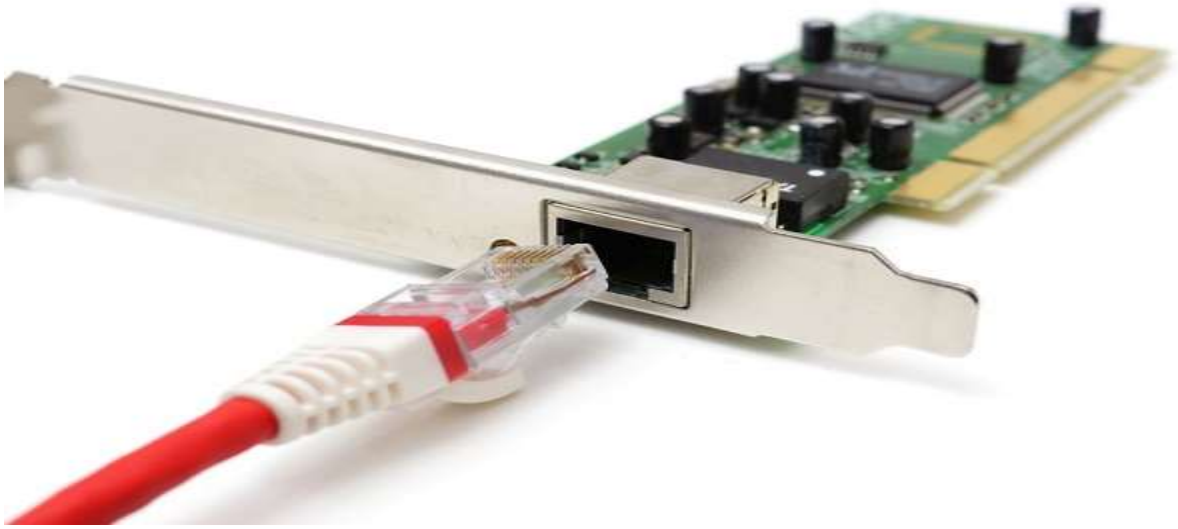

Devices
Router
Modem
Internet

RJ45 Connector

- RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an 8-pin jack used by devices to physically connect to **Ethernet** based **local area networks (LANs)**. **Ethernet** is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have **RJ45 connector pins** at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

Ethernet Card

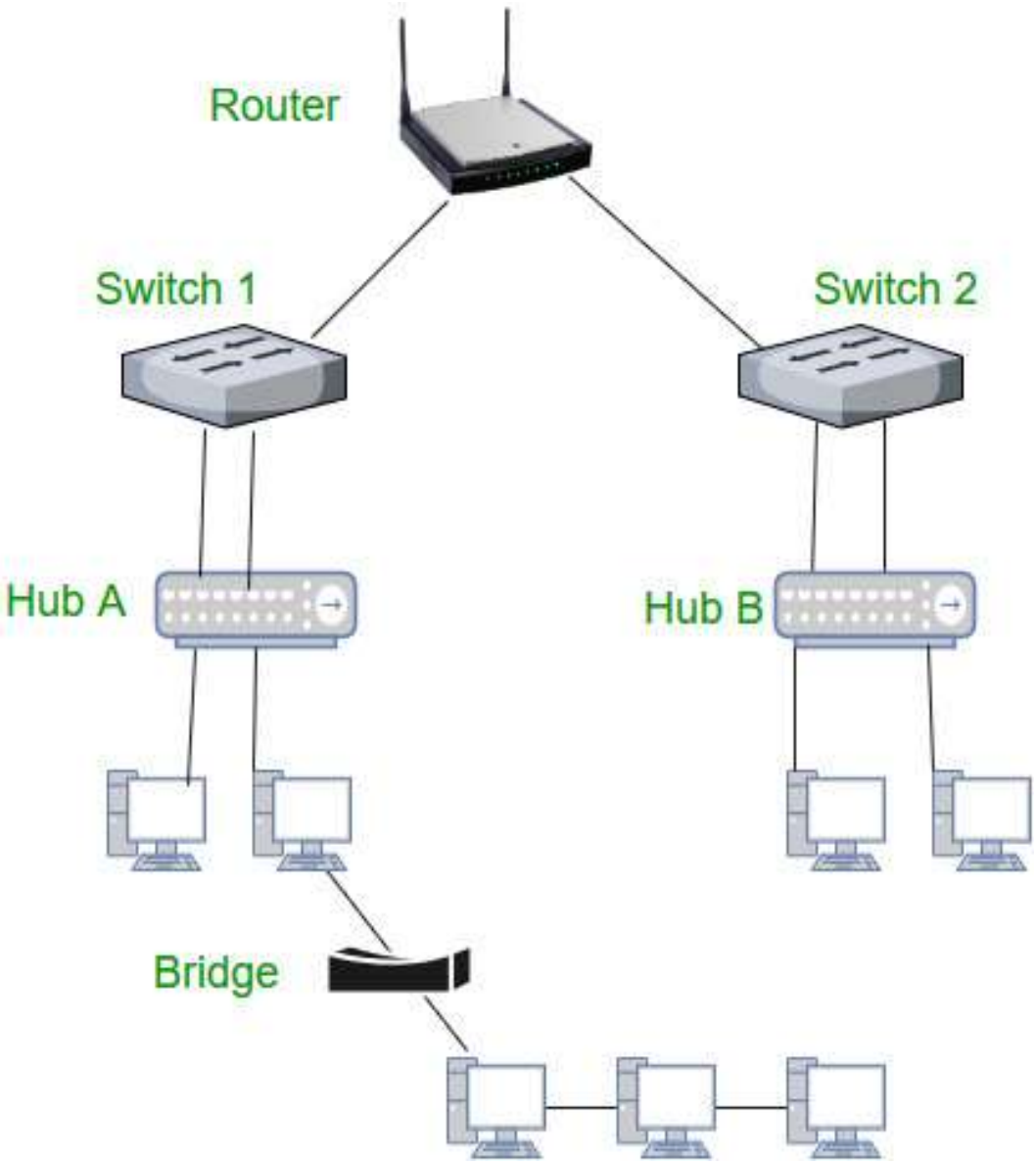
- **Ethernet card**, also known as **network interface card (NIC)**, is a hardware component used by computers to connect to **Ethernet LAN** and communicate with other devices on the LAN. The earliest **Ethernet cards** were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has **RJ45 socket** where network cable is physically plugged in.



Ethernet card speeds may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of 10 Mbps. However, modern cards support fast Ethernets up to a speed of 100 Mbps. Some cards even have capacity of 1 Gbps.

Router

- A **router** is a **network layer** hardware device that transmits data from one LAN to another if both networks support the same set of protocols. So a **router** is typically connected to at least two LANs and the **internet service provider** (ISP). It receives its data in the form of **packets**, which are **data frames** with their **destination address** added. Router also strengthens the signals before transmitting them. That is why it is also called **repeater**.


Router
Switch 1
Switch 2
Hub A
Hub B
Bridge

Switch

- **Switch** is a network device that connects other devices to **Ethernet** networks through **twisted pair** cables. It uses **packet switching** technique to **receive, store** and **forward data packets** on the network. The switch maintains a list of network addresses of all the devices connected to it.
- On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode


4510

Gateway

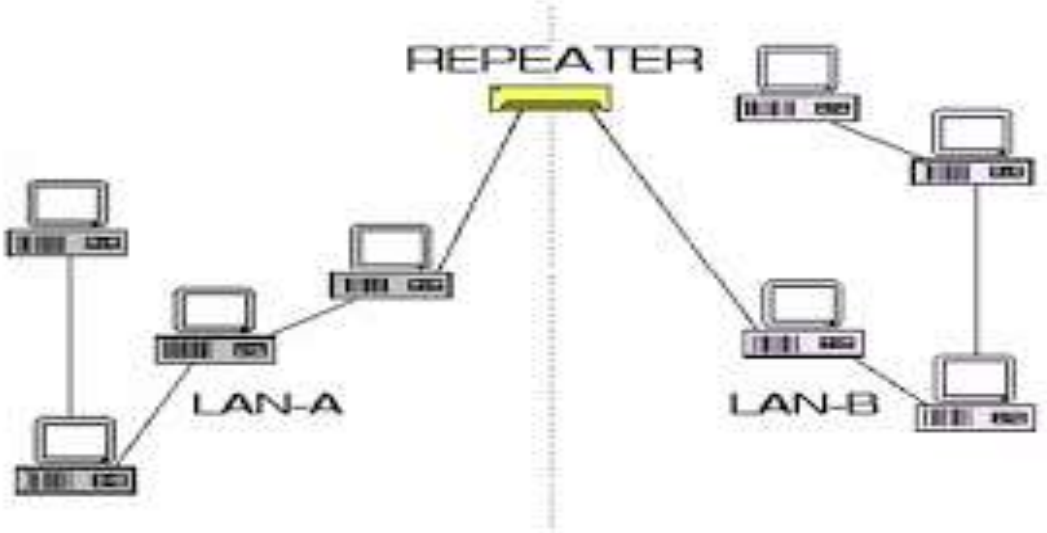
- **Gateway** is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are **dissimilar networks**. A gateway usually is a computer with multiple **NICs** connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.

Wi-Fi Card

- **Wi-Fi** is the acronym for **wireless fidelity. Wi-Fi technology** is used to achieve **wireless connection** to any network. **Wi-Fi card** is a **card** used to connect any device to the local network wirelessly. The physical area of the network which provides internet access through Wi-Fi is called **Wi-Fi hotspot**. Hotspots can be set up at home, office or any public space. Hotspots themselves are connected to the network through wires.

Repeater

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.


REPEATER
LAN-A
LAN-B

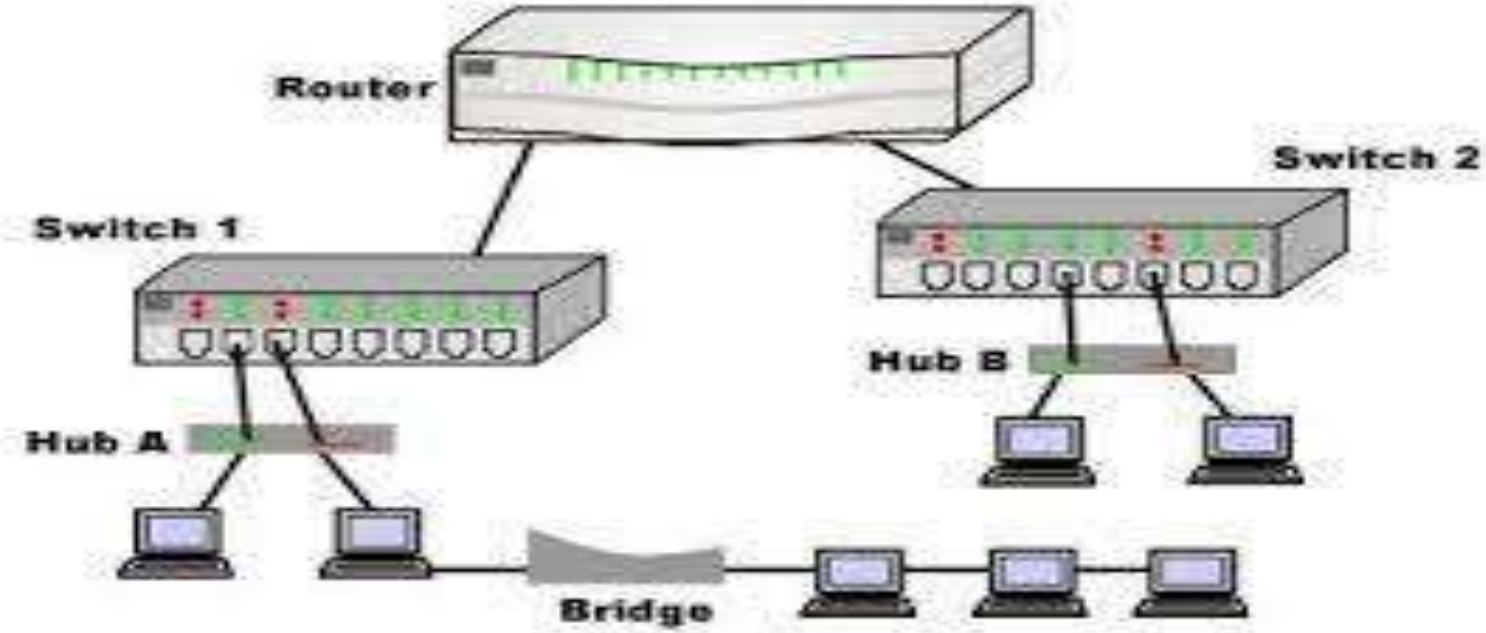

Matrox Veos Repeater

Hub

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:-** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
- **Intelligent Hub :-** It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

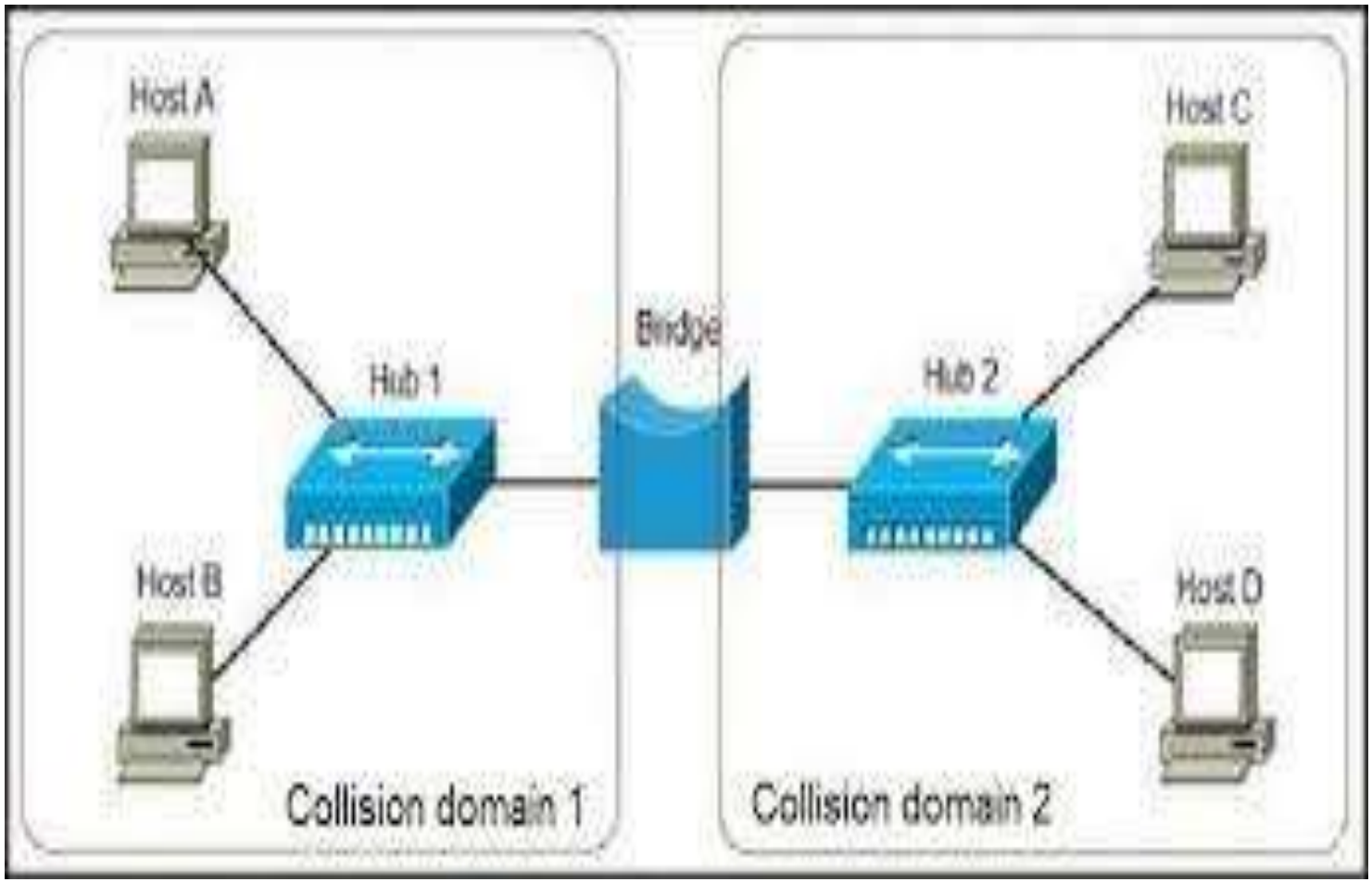

Router
Switch 1
Switch 2
Hub A
Hub B
Bridge

Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.


Host A
Host C
Bridge
Hub 1
Hub 2
Host B
Host D
Collision domain 1
Collision domain 2

Brouter

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.

Difference Between Hub, Switch and Router

Hub	Switch	Router
HUB work on Physical Layer of OSI Model	Switch work on Data Link Layer of OSI Model	Router work on Network Layer of OSI Model
HUB is Broadcast Device	Switch is Multicast Device	Router is a routing device use to create route for transmitting data packets
Hus is use to connect device in the same network	Switch is use to connect devices in the same network	Router is use to connect two or more different network.
Hub sends data in the form of binary bits	Switch sends data in the form of frames	Router sends data in the form packets
Hub only works in half duplex	Switch works in full duplex	Router works in full duplex
Only one device can send data at a time	Multiple devices can send data at the same time	Multiple devices can send data at the same time
Hub does not store any mac address or IP address	Switch store MAC Address	Router stores IP address

Routers	Bridges
Routers operates in network layer of OSI Model.	Bridge operates in data link layer of OSI Model.
Router is use to connect the LAN and WAN.	Bridge is use to connect two different LAN segments.
Router transmits data in the form of packets.	Bridge transmit data in the form frames.
Router reads the IP Address of a device.	Bridge reads the MAC Address of a device.
Router has more ports compare to bridge.	Bridge has only two ports.
Router uses routing table for sending data.	Bridge does not use any routing table for sending data.