CSE-3636 || **Computer Network** || Mid Note

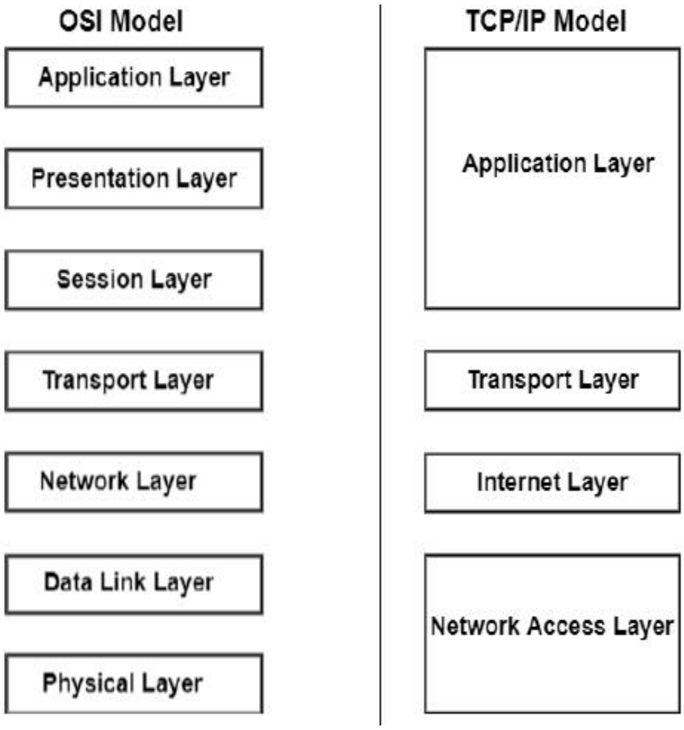
By **Sorowar Mahabub**, C201032

Can also read the miracle sheet from here!!

Autumn-22

1(a): Differentiate between TCP/IP model and OSI model.

Parameters	**OSI Model**	**TCP/IP Model**
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.



Class Suggestion || Why TCP has success?

TCP's remarkable success in computer networks is attributed to its reliability, adaptability, and wide-ranging benefits:

1. **Reliability:** TCP guarantees secure and accurate data delivery. Through sequence numbers, acknowledgments, and retransmissions, it ensures data integrity and order, making it ideal for tasks like file transfers and web browsing.
2. **Flow and Congestion Control:** TCP prevents bottlenecks by controlling data flow between sender and receiver. This averts congestion and optimizes performance by matching the receiver's capacity, enhancing overall network efficiency.
3. **Network Stability:** TCP's congestion control dynamically adjusts to varying network conditions, preventing gridlocks and promoting fairness in resource sharing among connections.
4. **End-to-End Philosophy:** By adhering to the end-to-end principle, TCP empowers edge devices with intelligence, fostering flexibility, innovation, and the seamless introduction of new services.
5. **Ubiquity:** Supported across devices, operating systems, and network equipment, TCP's compatibility ensures seamless communication and interaction across diverse network landscapes.
6. **Standardization:** As an IETF standard, TCP's robust specifications are publicly available, undergo community scrutiny, and benefit from collective improvements.
7. **Application Integration:** TCP forms the backbone for many applications and protocols like HTTP, SMTP, FTP, and SSH, cementing its status as a cornerstone for internet services.
8. **Adaptability:** TCP transcends IPv4 and IPv6 networks, ensuring compatibility with evolving network infrastructures and technology.
9. **Security and Privacy:** TCP synergizes with secure protocols and encryption methods, bolstering data confidentiality and safeguarding transmission.
10. **Continuous Advancements:** TCP's triumph also hinges on perpetual research, leading to innovations like TCP New Reno and TCP Cubic, catering to specific challenges and scenarios.

In essence, TCP's triumph in computer networks emanates from its unwavering reliability, ability to adapt, seamless integration with applications, pervasive support, and steadfast commitment to networking principles that prioritize efficient communication and resource management.

1(b): write down the name of corresponding layer in TCP/IP model for each of the following task: 1. detecting errors during the delivery of a message, 2. Representing of bits in a wire, 3. delivery of a message to an appropriate process or application of the destination host, 4. communication reliability achieved, 5. address keeps on changing during communication over internet?

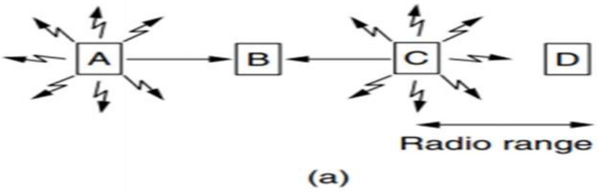
1. Detecting errors during the delivery of a message. Function of **Data Link Layer**
2.Representing bits on a wire. Function of **Physical Layer**
3.Delivery of a message to an appropriate process on the destination host. Function of **Transport Layer**
4.Communication reliability achieved. Function of **Transport Layer**
5.Address keeps on changing during communication over the internet. Function of **Network Layer**

2(a): Explain hidden node problem and exposed node problem with proper diagram for wireless communication.

The hidden node problem and the exposed node problem are two common issues that can occur in wireless communication networks. These problems are particularly relevant in scenarios where multiple wireless devices share the same communication medium, such as in a Wi-Fi network. Let's explore each problem and provide diagrams to illustrate them.

Hidden Node Problem:

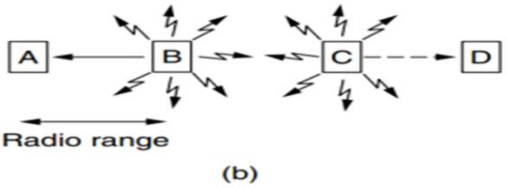
In the hidden node problem, three nodes A, B, and C are involved. Node B is the central node, and nodes A and C are out of each other's transmission range but within node B's transmission range. Nodes A and C are "hidden" from each other. This can lead to collisions when both nodes A and C transmit to node B simultaneously, causing interference at node B. Diagram:



Solution: *(Related to Q, tai Dea Hoice + Sir o Praice)*
Request to Send (RTS) / Clear to Send (CTS) Protocol: Nodes A and B can use an RTS /CTS protocol before transmitting data. Node A sends an ***RTS (Request to Send)*** packet to Node B, requesting permission to transmit. If Node B sends a ***CTS (Clear to Send)*** packet back, both Node A and Node C are aware of the transmission, and Node C can hold off its transmission until Node A is done.

Exposed Node Problem:

In the exposed node problem, nodes A, B, C and D are involved. Node B and C are within transmission range. Node B is transmitting data to node A. Node C also wants to transmit data and wants to communicate with node D. But Node C, fearing interference, refrains from transmitting to node D even though it could do so without causing any collision. This leads to inefficient use of the communication medium. Diagram:



Solution: *(Related to Q, tai Dea Hoice + Sir o Praice)*
Request to Send (RTS) / Clear to Send (CTS) Protocol: Node B sends an ***RTS (Request to Send)*** packet which contains that Node A will receive data from Node B. Then Node C knows that Node D is free for transmitting.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): CSMA/CA is a protocol used in wireless networks that includes mechanisms to address the exposed node problem. Nodes listen for ongoing transmissions and avoid transmitting if they sense ongoing activity. However, CSMA/CA uses backoff mechanisms to avoid overly long waits, allowing transmissions to resume after a certain idle period.

2(b): How does CSMA/CD improve performance over CSMA protocol? (**CSMA/CD =>** Career Sence multiple Access Collision Detection**)**

CSMA/CD is an improvement over the basic CSMA (Carrier Sense Multiple Access) protocol primarily in the context of wired Ethernet networks. CSMA/CD was specifically designed to address the issue of collisions that can occur in CSMA networks, thereby improving overall network performance.

CSMA/CD: CSMA/CD improves over basic CSMA by introducing collision detection. **Here's how it works:**

Carrier Sense: Devices still listen to the medium to check for its availability. If the medium is sensed as busy, the device waits until it becomes idle.

Collision Detection: Unlike basic CSMA, in CSMA/CD, devices continue monitoring the medium during their transmission. If a collision is detected while a device is transmitting, it stops immediately, sends a "jam" signal to indicate the collision, and then enters a "backoff" period.

Backoff and Randomization: During the backoff period, the device waits for a random amount of time before attempting to retransmit. This randomization helps reduce the chances of collisions happening again.

Explain non persistent and persistent CSMA protocols.

Non-persistent CSMA:

1.Device senses the channel.
2.If the channel is busy, the device waits for a random period of time.
3.After waiting, the device checks the channel again.
4.If the channel is still busy, the device continues to wait and retries later.
5.Once the channel is sensed as idle, the device starts transmitting.
6.Non-persistent CSMA helps reduce collisions by introducing randomness in the retransmission attempts.

Persistent CSMA:

1.Device senses the channel.
2.If the channel is busy, the device keeps checking the channel continuously.
3.Once the channel becomes idle, the device starts transmitting immediately.
4.If a collision is detected during transmission, collision detection mechanisms are employed, and collision resolution occurs.

Persistent CSMA is more aggressive in trying to transmit as soon as the channel becomes available, which can result in quicker access to the medium. However, it can also lead to more frequent collisions compared to non-persistent CSMA, as devices may attempt to transmit simultaneously.

Or 2(b): In a multiple access network the average frame size is 200 bits and the channel capacity 200 kbps. Evaluate the throughput if the system generates 800 frames per second for the aloha system and for the slotted aloha system.

Given data: Average frame size = 200 bits, Channel capacity = 200 kbps (kilobits per second), System generates 800 frames per second

Frame transmission time = Frame size / Channel capacity Frame transmission time

= 200 bits / 200,000 bits per second Frame transmission time = 0.001 seconds = 1 ms

For ALOHA system:

G= traffic load = (frames per second * frame transmission time) = **800** frames per second * **0.001** seconds = **0.8**

Throughput = G * e$^{(-2G)}$

= 0.8 * e$^{-2*0.8}$ = 0.162 or 16.2%

For slotted ALOHA system:

Throughput = G * e^{-G}

= 0.8 * e$^{-0.8}$ = 0.3595 or 35.95%

So, the throughput for the ALOHA system is approximately 16.2%, and the throughput for the Slotted ALOHA system is approximately 35.95%.

3(b): Write down the comparison between ipv4 and ipv6.

Feature	**IPv4**	**IPv6**
Address Length	32 bits	128 bits
Address Notation	Dotted Decimal (e.g., 192.168.1.1)	Colon-Hexadecimal (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address Space	Limited (4.3 billion addresses)	Vast (340 undecillion addresses)
Address Configuration	Manual, DHCP	Stateless, Stateful DHCPv6
Fragmentation	Routers and hosts perform fragmentation	Fragmentation not done by intermediate routers
NAT (Network Address Translation)	Commonly used due to address scarcity	Discouraged due to ample address space
IPSec (Security)	Optional	Mandatory
Header Checksum	Included in header (optional)	Removed; checksum at transport layer
Broadcast/Multicast	Broadcast supported	Multicast emphasized
QoS (Quality of Service)	Limited support	Improved support
Routing Protocols	RIP, OSPF, BGP, etc.	OSPFv3, BGP4+

Or 3(b): Write short note on the followings-

1. Network Address: The network address is a fundamental concept in networking that represents the starting point of a network segment. It is the first address within a subnet and is used to identify the network itself. In IP addressing, the network address is obtained by setting all host bits to 0 within a specific subnet. Devices use the network address to route packets to the correct network and to determine whether communication should occur within the same local network or be forwarded to another network.

Example: In **192.168.123.**132 the **bold part** is Network address and 132 is the host address.

2. Broadcast Address: The broadcast address is an address that is used to send a packet to all devices within a specific network segment. In IPv4, the broadcast address is obtained by setting all host bits to 1 within a subnet. When a device sends a packet to the broadcast address, all devices within that network receive the packet. Broadcasts are commonly used for tasks such as discovering devices, sending updates, or announcing network services. However, with the growth of networks and security concerns, the use of broadcasts has decreased in favor of more targeted communication methods.

Example: the broadcast address of a Class C 192.168. 16.0 network is 192.168. 16.255.

3. Bridge: A bridge is a networking device that operates at the Data Link Layer of the OSI model. Its primary function is to connect and filter traffic between two or more network segments to create a single larger network. Bridges operate based on MAC addresses and can effectively reduce network congestion and improve overall network performance by dividing network traffic into smaller segments. Modern bridges are often implemented as switches, which are more efficient and versatile devices for connecting and managing network segments.

4. Network Address Translation (NAT): Network Address Translation is a technique used to modify IP addresses within packets as they pass through a routing device. NAT is commonly used to allow multiple devices on a local network to share a single public IP address for communication over the internet. It enables private IP addresses on a local network to be translated into a single public IP address for external communication. NAT helps alleviate the shortage of IPv4 addresses and enhances security by hiding internal IP addresses from external networks.

5. Netmask: A netmask, also known as a subnet mask, is a binary pattern used to distinguish between the network and host portions of an IP address. It works in conjunction with IP addresses to determine which part of the address belongs to the network and which part identifies individual devices within the network. Netmasks are used in subnetting to divide IP address space into smaller segments. In CIDR notation, the netmask is represented as a slash followed by the number of bits set to 1 in the subnet mask. For example, a netmask of /24 represents a subnet with 24 bits reserved for the network and 8 bits for hosts.

*. Router: A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

Spring-22

1(a): Make a list of activities that a human does every day in which computer networks are used. how would our human life be altered if these networks were suddenly switched off? list the negative impacts of computer network.

Everyday Activities that human does Involving Computer Networks:

1.Communication: Sending emails, instant messaging, making calls, and using social media platforms.
2.Information Retrieval: Searching the internet for news, information, research, and educational resources.
3.Entertainment: Streaming videos, music, online gaming, and accessing digital content.
4.Online Shopping: Buying products and services from e-commerce websites.
5.Work and Collaboration: Remote work, video conferencing, file sharing, and collaborating on documents.
6.Banking and Financial Transactions: Online banking, fund transfers, and digital payments.
7.Navigation and Maps: Using GPS and navigation apps for directions and location-based services.
8.Smart Home Control: Managing smart devices, home automation, and security systems.
9.Healthcare: Telemedicine, online health records, and medical research.
10.Education: Online classes, e-learning platforms, and educational resources.
11.News and Media: Reading online news articles, watching live streams, and staying updated.

Computer networks has become integral part of our modern daily life, affecting various aspects of communication, work, entertainment, education, and more. If the networks were suddenly switched off, it would have widespread and significant negative impacts on individual, societal, and economic levels. It will cause many negative impact like Communication disruption, loss of information access, entertainment interruption, economic impact, work disruption, social isolation, education interruption, healthcare challenge, security concerns etc.

Negative impacts of computer networks:

1.Security Breaches: Networks are vulnerable to cyberattacks, data breaches, and hacking attempts, leading to unauthorized access, data theft, and financial loss.

2.Malware Spread: Networks can facilitate the rapid spread of viruses, worms, ransomware, and other malicious software, affecting multiple devices and systems.

3.Privacy Concerns: Personal and sensitive information can be exposed or compromised, leading to identity theft, stalking, and surveillance.

4.Dependency: Over reliance on networks can lead to significant disruptions when they fail or are compromised, affecting daily activities and critical services.

5.Social Isolation: Excessive use of computer networks, particularly social media, can lead to reduced face-to-face interactions, isolation, and detachment from real-world relationships.

6.Loss of Productivity: Network-related downtime, cyberattacks, or distractions from online activities can lead to decreased productivity in both personal and professional contexts.

7.Misinformation and Fake News: Networks can facilitate the rapid spread of false information, leading to misinformation, misunderstandings, and public manipulation.

8.Online Harassment and Bullying: Computer networks can provide platforms for cyberbullying, trolling, and online harassment, affecting individuals emotionally and psychologically.

9.Health Concerns: Excessive screen time and reliance on computer networks can contribute to physical health issues such as eye strain, sedentary behavior, and disrupted sleep patterns.

10.Loss of Traditional Skills: Reliance on computer networks for various tasks can lead to a decline in traditional skills and manual abilities.

11.Intellectual Property Theft: Networks can facilitate unauthorized sharing and distribution of copyrighted materials, leading to financial losses for content creators.

1(b): when a file is transferred between two computers two acknowledgment strategies are possible.in the first one the file is chopped up in packets which are, individually recognized by receiver, but the file transfer as a whole is not acknowledged. in the second one the packets are not acknowledged individually, but the entire file is acknowledged when it arrives. Discuss these two approaches.

The two acknowledgment strategies/approaches that is described pertains to different transport layer protocols, namely, Connectionless Transport and Connection-Oriented Transport.

1.Connectionless Transport:
In this approach, the file is divided into smaller packets, each containing a portion of the data along with a sequence number. These packets are then sent over the network individually. The receiver acknowledges the receipt of each packet by sending an acknowledgment (ACK) back to the sender. If a packet is lost or corrupted during transmission, the sender can detect this based on the lack of acknowledgment and retransmit the missing packet.

Advantages:
Individual acknowledgment provides higher reliability, as each packet's successful delivery is confirmed.

Disadvantages:
The overhead of sending individual acknowledgments for each packet can lead to increased network traffic. Sequence number management and acknowledgment handling can introduce complexity and overhead.

Uses:
Connectionless transport is commonly used in protocols like User Datagram Protocol (UDP), which is employed for applications where low latency is crucial, and some packet loss is acceptable (e.g., streaming media, online gaming).

2. Connection-Oriented Transport:
In this approach, the file is treated as a single unit, and the entire file is transmitted as a continuous stream of data. The receiver acknowledges the successful receipt of the complete file once it has been fully delivered. If any part of the file is lost or corrupted, the entire file might need to be re-transmitted.

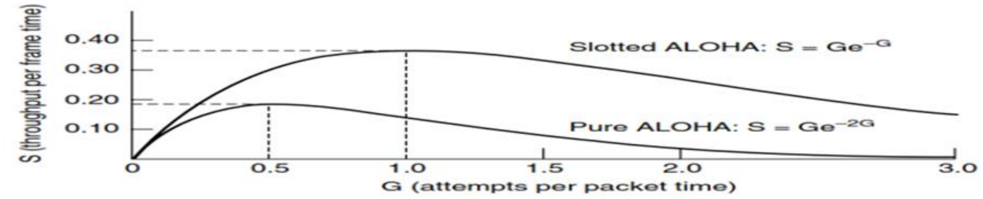
Advantages:
Simplicity in acknowledgment, as only one acknowledgment is required for the entire file.
Reduced overhead compared to individual acknowledgment for each packet.

Disadvantages:
Lack of granularity in acknowledgment, which may make it harder to identify which specific portions of the file need to be re-transmitted. Less suitable for error-prone networks, as a corrupted or lost packet might require re-transmitting the entire file.

Uses:
Connection-oriented transport is commonly used in protocols like Transmission Control Protocol (TCP), which ensures reliable, ordered, and error-checked data delivery. It is suitable for applications where data integrity is critical, such as web browsing, file downloads, and email communication.

2(a): Compare the characteristics and performance of pure and slotted Aloha.

Key	Pure Aloha	Slotted Aloha

Key	Pure Aloha	Slotted Aloha
Time Slot	In Pure Aloha, any station can transmit data at any time.	In Slotted Aloha, any station can transmit data only at the beginning of a time slot.
Time	In Pure Aloha, time is continuous and is not globally synchronized.	In Slotted Aloha, time is discrete and is globally synchronized.
Vulnerable time	The vulnerable time or susceptible time in Pure Aloha is equal to (2×Tt).	In Slotted Aloha, the vulnerable time is equal to (Tt).
Probability	The probability of successful transmission of a data packet $S=G\times e^{-2G}$	The probability of successful transmission of data packet $S=G\times e^{-G}$
Maximum efficiency	Maximum efficiency = 18.4%.	Maximum efficiency = 36.8%.
Number of collisions	Does not reduce the number of collisions.	Slotted Aloha reduces the number of collisions to half, thus doubles the efficiency.
Perfomence	Performance of Pure vs Slotted ALOHA  **Figure 4-3.** Throughput versus offered traffic for ALOHA systems.	

2(b): Explain non-persistent and different variation of persistent CSMA.

--- Same Q in Au’22 ---

+

There are different variations of persistent CSMA, including:

1-Persistent CSMA:

1.In 1-persistent CSMA, when a device senses the channel as busy, it continues to check the channel continuously until it becomes idle. Once the channel is idle, the device starts transmitting immediately.
2.If a collision occurs, it is detected, and the devices involved initiate collision resolution mechanisms.
3.This approach is commonly used in wired Ethernet networks.

p-Persistent CSMA:

1.In p-persistent CSMA, when a device senses the channel as busy, it transmits with a certain probability 'p' and defers with probability '1-p'.
2.If the device chooses to transmit and the channel is busy, it waits for the channel to become idle and then starts transmitting.
3.p-persistent CSMA is often used in wireless networks with slotted time.

Advantages of Persistent CSMA (1-persistent and p-persistent): Higher channel utilization compared to non-persistent CSMA. Particularly useful in scenarios where high channel utilization is desired.

Disadvantages: Increased likelihood of collisions due to aggressive transmission behavior. More complex to implement compared to non-persistent CSMA.

Or 2(b): Explain major characteristics of a collision free protocol.

Collision-Free Protocol - Bit Map:

The Bit Map protocol is designed to achieve collision-free communication in a network by carefully scheduling the transmission of devices. Here are its major characteristics:
1.Centralized Control: The Bit Map protocol requires a central controller, often referred to as a "master" or "scheduler," to manage the communication schedule of devices.
2.Time Division Multiplexing (TDM): The communication time is divided into fixed time slots, each corresponding to a specific device or communication channel. The schedule of these time slots is represented using a bit map.
3.Bit Map Structure: The bit map is a binary sequence, where each bit corresponds to a time slot. A "1" in the bit map indicates that the corresponding time slot is allocated for transmission, and a "0" indicates that the time slot is idle.

4.Synchronization: All devices synchronize their clocks with the master controller to ensure accurate timing and coordination of transmission.
5.Collision Avoidance: Collision avoidance is achieved by assigning non-overlapping time slots to different devices. Each device is allowed to transmit only during its allocated time slot, thus eliminating the possibility of collisions.
6.Efficiency and Fairness: The Bit Map protocol ensures efficient utilization of the communication channel, as no time slots are wasted on collisions. It also provides fairness by guaranteeing each device an equal share of the available bandwidth.

Or, Collision-Free Protocol - Binary Countdown:

The Binary Countdown protocol is another approach to achieving collision-free communication. It involves devices following a systematic countdown pattern to transmit without collisions. Here are its major characteristics:
1.Decentralized Approach: Unlike Bit Map, the Binary Countdown protocol does not require a central controller. Devices follow a predefined algorithm to determine their transmission time.
2.Countdown Sequence: Each device is assigned a unique binary countdown sequence based on its identity or priority. The sequence determines when the device can transmit.
3.Binary Exponential Backoff: When two or more devices attempt to transmit simultaneously, the device with the longest remaining countdown sequence wins the transmission right. The other devices pause their countdown and resume after the collision.
4.Collision Resolution: Collisions are resolved by the binary exponential backoff mechanism, where devices with lower countdown values take precedence over devices with higher countdown values.
5.Adaptability: Devices adjust their countdown values dynamically based on the network conditions and collisions, ensuring efficient and collision-free transmission.
6.Fairness and Efficiency: The Binary Countdown protocol offers fairness by giving devices with longer countdown values higher priority, ensuring that all devices have an opportunity to transmit. It also improves efficiency by reducing the likelihood of collisions.

3(a): Both virtual circuit and datagram have their supporter and their detractors. make comparison of datagram and virtual circuit subnets with highlighting advantage and disadvantages of each system.

Key	Virtual Circuits	Datagram Networks
Definition	Virtual Circuit is a connection-oriented service in which there is an implementation of resources like buffers, CPU, bandwidth, etc., used by virtual circuit for a data transfer session.	Datagram networks are a type of connectionless service where no such resources are required for data transmission.
Path	In Virtual circuits, as all the resources and bandwidth get reserved before the transmission, the path which is utilized or followed by first data packet would get fixed and all other data packets will use the same path and consume same resources.	In a Datagram network, the path is not fixed as data packets are free to decide the path on any intermediate router on the go by dynamically changing routing tables on routers.
Header	As there is same path followed by all the data packets, a common and same header is being used by all the packets.	Different headers with information of other data packet is being used in Datagram network.
Complexity	Virtual Circuit is less complex as compared to that of Datagram network.	Datagram network are more complex as compared to Virtual circuit.
Reliability	Due to fixed path and assurance of fixed resources, Virtual Circuits are more reliable for data transmission as compared to Datagram network.	Datagram networks, due to their dynamic resource allocation and dynamic path, are more error-prone and less reliable than Virtual circuits.
Example and Cost	Virtual circuits are costlier in installation and maintenance. They are widely used by ATM (Asynchronous Transfer Mode) Network, which is used for the Telephone calls.	Datagram networks are cheaper as compared to the Virtual Circuits. They are mainly used by IP network, which is used for Data services like Internet.

Need to know(Part-01)

An IP address has **two** parts. The **first part** of an IP address is used as a **network address**, the **last part as a host address**. If you take the example *192.168.123.132* and divide it into these two parts, you get **192.168.123 => Network** & **132 => Host** *or* 192.168.123.0 - network address & 0.0.0.132 - host address.

Subnet mask: The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

Network classes: Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

A. **Class A** networks use a default subnet mask of 255.0.0.0 and **have 0-127 as their first octet**. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

B. **Class B networks** use a default subnet mask of 255.255.0.0 and **have 128-191 as their first octet**. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

C. **Class C networks** use a default subnet mask of 255.255.255.0 and **have 192-223 as their first octet**. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

Subnetting: The **subnet mask 255.255.255.192 gives you four networks of 62 hosts each**. It works because in binary notation, 255.255.255.192 is the same as 1111111.11111111.1111111.11000000. The first two digits of the last octet become network addresses, so you get the additional networks 00000000 (0), 01000000 (64), 10000000 (128) and 11000000 (192). *In these four networks, the last six binary digits can be used for host addresses.*

Using a subnet mask of 255.255.255.192, your 192.168.123.0 (*for example*) network then becomes the four networks 192.168.123.0, 192.168.123.64, 192.168.123.128 and 192.168.123.192. These four networks would have as valid host addresses:

192.168.123.**1-62**, 192.168.123.**65-126**, 192.168.123.**129-190**, 192.168.123.**193-254**

3(b): An organization is using class C address 192.168.5.0. perform the subnetting for 4 different departments. How many hosts can connect in each department. Write the beginning and ending range of the IP address and broadcast address for all 4 departments.

To subnet the Class C address 192.168.5.0 into 4 different departments, we need to borrow bits from the host portion of the address to create subnets. Let's perform the **subnetting**:

Given Class C IP address: 192.168.5.0

Step 1: *Determine the number of bits needed to accommodate 4 subnets (2^2 = 4).* **Number of bits for subnets = 2**

Step 2: *Subtract the number of subnet bits from the total bits in the host portion of a Class C address (which is 8 bits).* **Remaining bits for hosts** = 8 - 2 **= 6 bits**

Step 3: *Calculate the number of hosts per subnet using the remaining bits in the host portion.* **Number of hosts per subnet = 2^6 - 2 (***subtract 2 for network address and broadcast address***) = 62 hosts per subnet**

Step 4: *Calculate the subnet mask based on the number of subnet bits.* **Subnet mask = 255.255.255.192** (CIDR notation: /26) (*e step kahini bujtecina, knob a kibabe eta hcce! **Apni jdi bujen kindly wp- 01521564157 te aktu diben**, obviously if possible)

Now, let's calculate the subnet ranges, beginning and ending IP addresses, and broadcast addresses for the 4 departments:

Departments	Subnet Range	Beginning IP	Ending IP	Broadcast Address
Dept 1	192.168.5.0 - 192.168.5.63	192.168.5.1	192.168.5.62	192.168.5.63
Dept 2	192.168.5.64 - 192.168.5.127	192.168.5.65	192.168.5.126	192.168.5.127
Dept 3	192.168.5.128 - 192.168.5.191	192.168.5.129	192.168.5.190	192.168.5.191
Dept 4	192.168.5.192 - 192.168.5.255	192.168.5.193	192.168.5.254	192.168.5.255

Or 3(b): In the given IP address FDEC::BBFF::0::FFFF/60, **how many bits can you use for host address? Expand the given address FDEC::BBFF::0::FFFF.**

In the given IPv6 address **FDEC::BBFF::0::FFFF**/60, we can determine the number of bits available for the host address and expand the address as follows:

1. **Number of Host Bits:** The subnet mask /60 indicates that the first 60 bits are used for the network prefix, leaving the remaining bits for the host address. **In IPv6, each hexadecimal digit represents 4 bits**. **Therefore, the number of host bits is:** *Total bits in an IPv6 address (**128 bits**) - Network bits (**60 bits**)* = **68 bits**

2. Expanded IPv6 Address: To expand the IPv6 address FDEC::BBFF::0::FFFF, we need to fill in the zeros between each segment. Here's the expanded address:

FDEC:0000:0000:0000:BBFF:0000:0000:0000:FFFF

Keep in mind that leading zeros within each segment can be omitted in IPv6 addresses. So, the expanded address can also be written as: **FDEC:0:0:0:BBFF:0:0:FFFF**

This represents the full 128-bit IPv6 address, with the network prefix and host bits included.

Need to know(Part-02)

Describe addressing techniques of Internet? Or, How many address techniques used in Internet? Describe.

(1) Physical address: The physical address, also known as the **link address**, also called **MAC (Machine Access Control) address**, is the address of a node as defined by its LAN or WAN. *Example: 2C:54:91:88:C9:E3*. The Logical/IP Address identifies a device in a network. But to reach and deliver data to the device, we need a MAC/Physical address.
[Never Changed; provided *by the hardware interface vendor***]**

(2) Logical address: Logical address, also called as **IP address**, is necessary for universal communications that are independent of underlying physical networks. Every device gets an IP address logically computed and this IP address acts as an identifier for that particular device in the network communication. *Example: 255.255.255.255*.

[Change *over time as well as from one network to another***; provided** *by the Internet service provider***]**

(3) Port address: In TCP/IP model, the level assigned to perform a process is called a port address. A port address in TCP/IP is 16-bits in length. Example:
(4) Specific address: Some application has user friendly address that are designed for that specific address. *Example: email address, URL etc.*

Overlap of Frames in media is called **Collision**. *Re-Transmit is required if collision occurred.* If collision occurs, frames need to go waiting state for different time- that is called **Backoff Time**. *Vulnerable Time (F_t) is when collision occurs.* **For calculation:** Frame time = Slot time= Transmission time = F_t.

Devices related to OSI Model Layers:

Session + Transport Layer: Gateway
Network Layer: Router

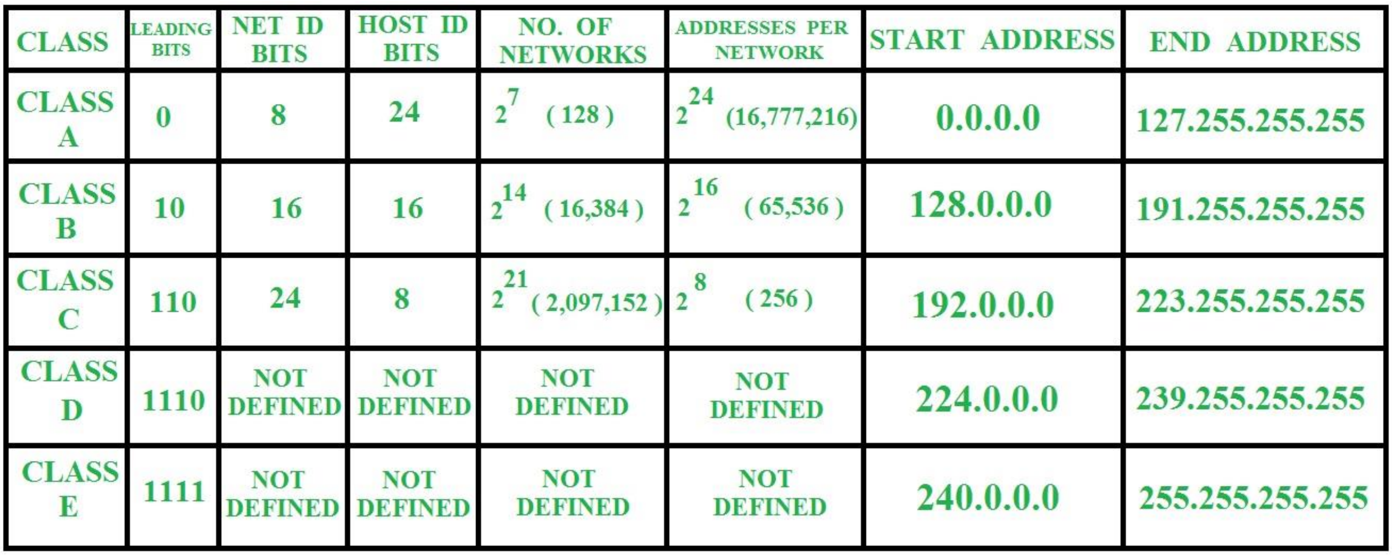
Data Link Layer: Bridge & Switch
Physical Layer: Repeater or Hub

Why is random access suitable for computer network systems? How?

Random access is a suitable access method for computer networks due to its efficiency and ability to handle multiple devices accessing the network simultaneously. Random access is a type of multiple access protocol where devices can transmit data whenever they have information to send, without waiting for a predetermined time slot. It enables efficient use of bandwidth, adapts well to varying traffic loads, doesn't require fixed time slots, handles collisions effectively, and is relatively simple to implement. One common example of a random-access protocol used in computer networks is the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol used in Ethernet networks.

ARPANET: APPA, the Advanced Research Projects Agency, was established by US President Eisenhower. The ARPA Network was an early Packet-switching network and the first network to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet. The ARPANET incorporated distributed computation, and frequent re-computation, of routing tables.

Classful Addressing: Classful addressing is a network addressing the Internet's architecture. This addressing method divides the IP address into five separate classes based on four address bits. Here, classes A, B, C offers addresses for networks of three distinct network sizes. **Class D is only used for multicast**, and **class E reserved exclusively for experimental purposes**.



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Classless Addressing: At a high level, classless addressing works by allowing IP addresses to be assigned arbitrary network masks without respect to "class." That means /8 (255.0.0.0), /16 (255.255.0.0), and /24 (255.255.255.0) network masks can be assigned to any address that would have traditionally been in the Class A, B, or C range

Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

- For the 1-persistent method, throughput is 50% when G=1.
- For the non-persistent method, throughput can go up to 90%.

Data Link Layer generates Frame being requested by Network Layer. Bursty: A condition in which network activity rises suddenly for a short period of time (idle) but there are huge data to be transmitted.

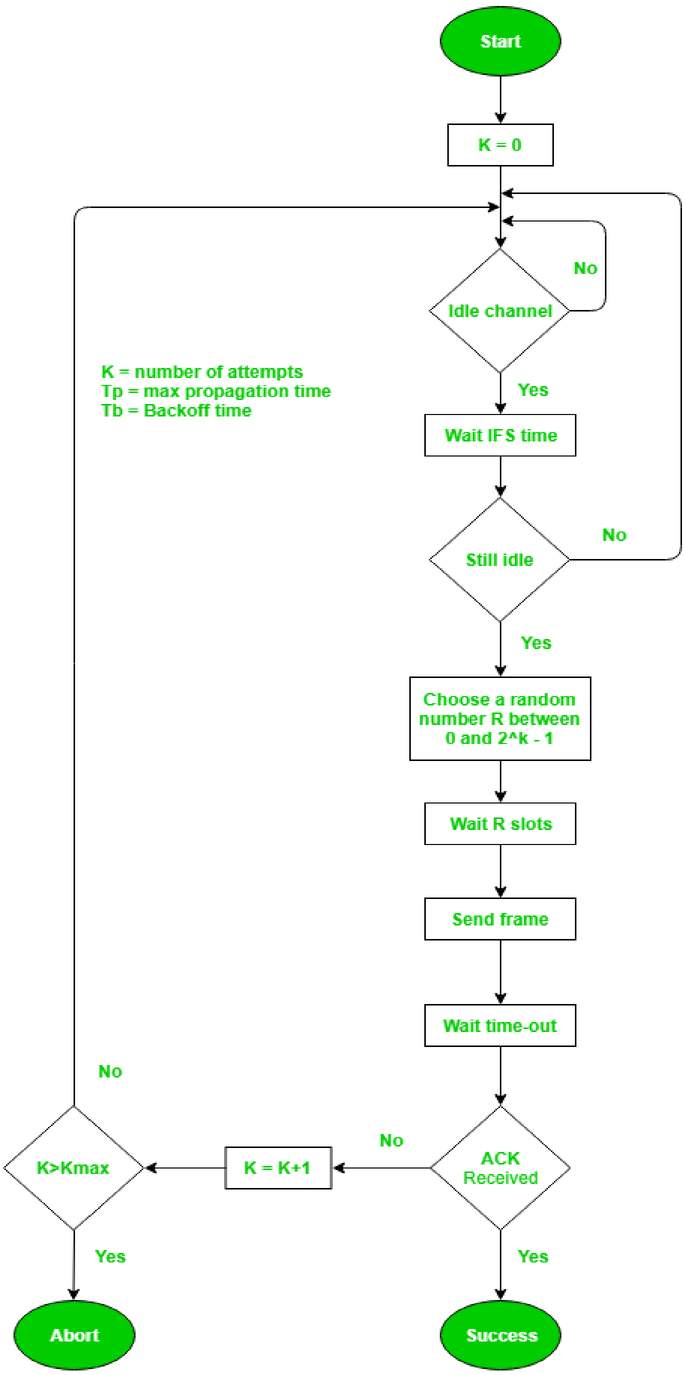
Propagation speed is the amount of time it takes for one particular signal to get from one point to another. **Transmission** Rate is the total amount of data that can be sent from one place to another in a given period of time.

*(**Sohoj Kathai:** IIUC 1ta bus e 1jn 1jn kre **x** jn students uthte ja time lage ta **Transmission** & By=us e kre apnar IIUC to Basai jaite j total time lage ta **Propagation**)*

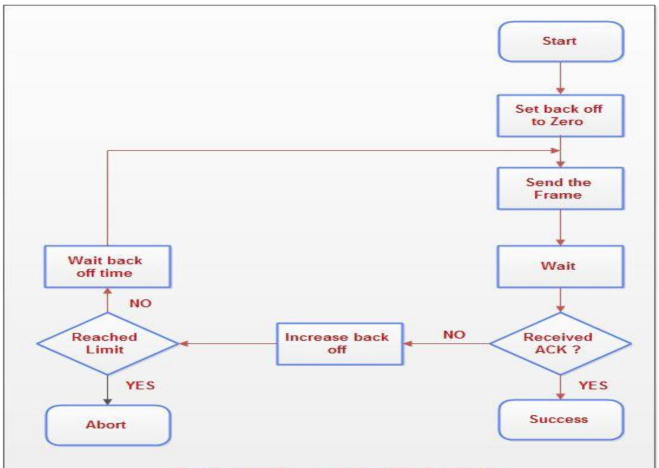
.

.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):

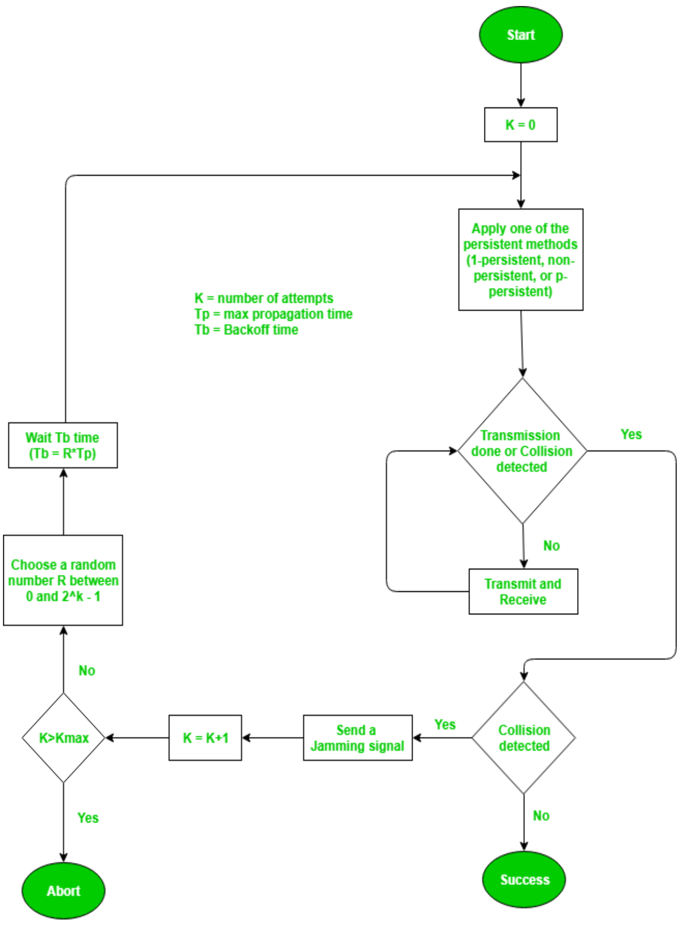


.



Protocol flow chart for ALOHA

Carrier Sense Multiple Access with Collision Detection (CSMA/CD):



Start
K = 0
Apply one of the persistent methods (1-persistent, non-persistent, or p-persistent)
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Transmission done or Collision detected
Yes
No
Transmit and Receive
Collision detected
Yes
Send a Jamming signal
K = K+1
K>Kmax
No
Choose a random number R between 0 and 2^k - 1
Wait Tb time (Tb = R*Tp)
Yes
Abort
No
Success

Range of Special IP Addresses

A. 169.254.0.0 – 169.254.0.16 **: Link-local addresses**

B. 127.0.0.0 – 127.0.0.8 **: Loop-back addresses**

C. 0.0.0.0 – 0.0.0.8 **: used to communicate within the current network.**

IP Address Types

There are 4 types of IP Addresses-

1. Public IP address– A public IP address is an Internet Protocol address, encrypted by various servers/devices. Ex.: DTCL, APMC (have to buy to use)

2. Private IP address– Everything that connects to your Internet network has a private IP address. 10.0.0.0 – 10.255.255.255 etc.

3. Static IP Address & **4. Dynamic IP Address.**