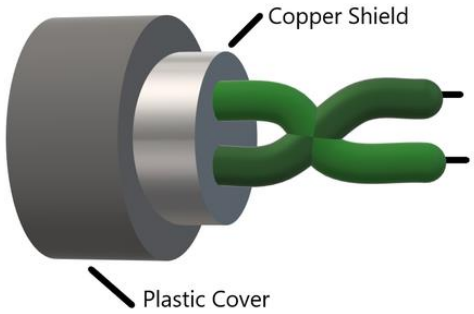
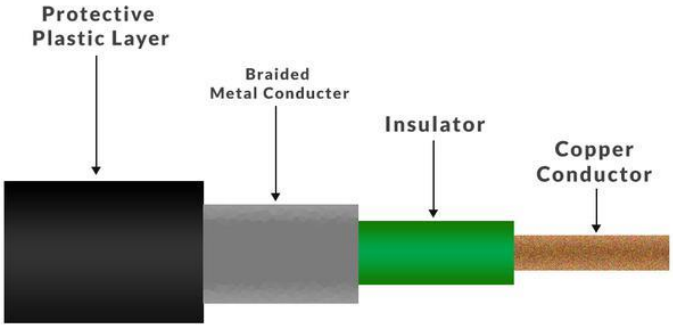
Various guided media

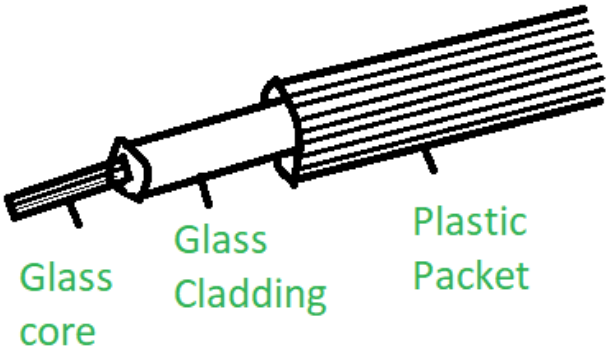
- **Twisted pair cable:** Twisted pair cable is the most common type of guided media. It consists of two insulated copper wires twisted together. Twisted pair cables are relatively inexpensive and easy to install. They are typically used for short-distance networks, such as Ethernet networks.



- **Coaxial cable** is a type of guided media that consists of a central copper core surrounded by a layer of insulation. The insulation is then surrounded by a braided metal shield. Coaxial cables are more expensive than twisted pair cables, but they can transmit data over longer distances and at higher speeds. They are typically used for cable television networks and high-speed Internet connections.



- **Fiber-optic cable:** Fiber-optic cable is a type of guided media that uses light to transmit data. It consists of a core of glass or plastic surrounded by a cladding layer. The core and cladding have different refractive indices, which allows light to be guided along the cable. Fiber-optic cables are the most expensive type of guided media, but they can transmit data over very long distances and at very high speeds. They are typically used for long-distance telecommunications networks and high-speed Internet connections.



Media Type	Cost	Distance	Speed
Twisted pair cable	Low	Short	100 Mbps
Coaxial cable	Medium	Medium	1 Gbps
Fiber-optic cable	High	Long	100 Gbps

Difference between guided and unguided media

Feature	Guided Media	Unguided Media
Transmission medium	Physical medium, such as copper wires, fiber optic cables, or waveguides	Air or vacuum
Signal propagation	In a specific path	In all directions
Security	More secure	Less secure
Interference	More susceptible to interference from other signals	Less susceptible to interference from other signals
Cost	More expensive	Less expensive
Distance	Can transmit data over shorter distances	Can transmit data over longer distances
Speed	Can transmit data at lower speeds	Can transmit data at higher speeds

Find out the subnet mask in each case also show the steps involved in calculation (a) 1024 subnets in class A (b) 256 subnets in class B (c) 32 subnets in class C (d) 4 subnets in class C (e) 64 subnets in class B

$x = n + \log_2 S$

(n=8,16 and 24 for class A,B and C respectively)

where:

- x is the number of bits required for the subnet mask
- n is the number of bits already allocated for the network portion of the address
- S is the number of subnets required

subnet mask = $255.255.(2^x - 1).0$

(a) 1024 subnets in class A

- Number of bits already allocated for the network portion of a class A address: 8
- Number of subnets required: 1024
- Number of bits required for the subnet mask: 8 + log2(1024) = 8 + 10 = 18
- Subnet mask: 255.255.192.0

(b) 256 subnets in class B

- Number of bits already allocated for the network portion of a class B address: 16
- Number of subnets required: 256
- Number of bits required for the subnet mask: 16 + log2(256) = 16 + 8 = 24
- Subnet mask: 255.255.255.192

(c) 32 subnets in class C

- Number of bits already allocated for the network portion of a class C address: 24
- Number of subnets required: 32
- Number of bits required for the subnet mask: 24 + log2(32) = 24 + 5 = 29
- Subnet mask: 255.255.255.240

(d) 4 subnets in class C

- Number of bits already allocated for the network portion of a class C address: 24
- Number of subnets required: 4

- Number of bits required for the subnet mask: 24 + log2(4) = 24 + 2 = 26
- Subnet mask: 255.255.255.252

(e) 64 subnets in class B

- Number of bits already allocated for the network portion of a class B address: 16
- Number of subnets required: 64
- Number of bits required for the subnet mask: 16 + log2(64) = 16 + 6 = 22
- Subnet mask: 255.255.255.128

Difference between broadcast, multicast and multiple unicast

Broadcast

- A broadcast is a message that is sent to all devices on a network.
- Broadcasts are used for network management purposes, such as sending ARP requests and RIP updates.
- Broadcasts can also be used for applications that need to reach all devices on a network, such as broadcasting a message to all users on a network.

Multicast

- A multicast is a message that is sent to a specific group of devices on a network.
- Multicasts are used for applications that need to reach a specific group of users, such as streaming video to a group of users or sending a file to a group of users.
- Multicasts are more efficient than broadcasts because they only send the message to the devices that are interested in receiving it.

Multiple unicast

- A multiple unicast is a message that is sent to multiple devices on a network, but each device receives a separate copy of the message.
- Multiple unicasts are used for applications that need to send different messages to different devices, such as sending a different message to each user in a chat room.
- Multiple unicasts are more efficient than sending multiple broadcasts because they only send the message once to each device.

Feature	Broadcast	Multicast	Multiple Unicast
Destination	All devices on the network	Specific group of devices	Multiple devices
Efficiency	Inefficient	Efficient	Efficient
Use cases	Network management, broadcasting messages	Streaming video, sending files	Chat rooms, sending different messages to different devices

Layers used for (a) combination of bits into bytes and bytes into frame (b) hop to hop delivery (c) process to process delivery (d) end to end delivery (e) segmentation and reassembly of data

(a) combination of bits into bytes and bytes into frame

- **Data Link Layer**

The Data Link Layer is responsible for combining bits into bytes and bytes into frames. It also adds error detection and correction bits to the frames to ensure that they are received correctly by the destination device.

(b) hop to hop delivery

- **Internet Layer**

The Internet Layer is responsible for routing data packets from the source device to the destination device. It does this by breaking the data into smaller packets and adding a header to each packet that contains the destination address. The packets are then routed through the network, one hop at a time, until they reach the destination device.

(c) process to process delivery

- **Transport Layer**

The Transport Layer is responsible for providing a reliable connection between two communicating processes. It does this by breaking the data into smaller segments and adding a header to each segment that contains the source and destination addresses, as well as the sequence number of the segment. The segments are then sent to the destination device, where they are reassembled into the original data.

(d) end to end delivery

- **Application Layer**

The Application Layer is responsible for providing services to the user. This includes things like file transfer, email, and web browsing. The Application Layer interacts with the Transport Layer to send and receive data.

(e) segmentation and reassembly of data

- **Transport Layer**

The Transport Layer is responsible for segmentation and reassembly of data. It breaks the data into smaller segments and adds a header to each segment that contains the source and destination addresses, as well as the sequence number of the segment. The segments are then sent to the destination device, where they are reassembled into the original data.

How is repeater different from amplifier? How is hub related to repeater? Explain four network devices

Repeater

- A repeater is a device that amplifies and regenerates signals on a network.
- Repeaters are used to extend the range of a network by amplifying the signal strength.
- Repeaters work on the Physical Layer of the OSI model.
- Repeaters do not have any intelligence, they simply amplify the signal.

Amplifier

- An amplifier is a device that increases the amplitude of a signal.
- Amplifiers are used to increase the signal strength, but they do not regenerate the signal.
- Amplifiers work on the Physical Layer of the OSI model.
- Amplifiers have some intelligence, they can amplify the signal based on the input signal strength.

Hub

- A hub is a device that connects multiple devices on a network.
- Hubs work on the Physical Layer of the OSI model.
- Hubs simply repeat the signal that they receive from one port to all of the other ports.
- Hubs do not have any intelligence, they simply repeat the signal.

The **main difference** between a repeater and an amplifier is that a repeater regenerates the signal, while an amplifier simply increases the amplitude of the signal. This means that a repeater can be used to extend the range of a network, while an amplifier can only be used to increase the signal strength.

Hubs are **related** to repeaters as they both work on the Physical Layer of the OSI model and simply repeat the signal that they receive. However, hubs are different from repeaters in that hubs can connect multiple devices on a network, while repeaters can only connect two devices.

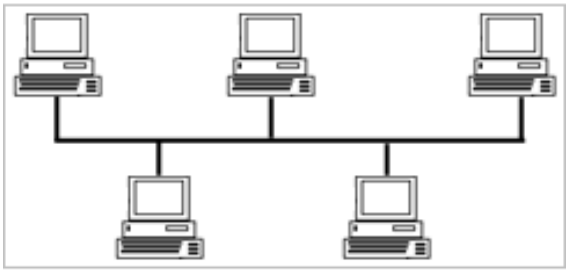
Here are four other network devices:

- **Bridge:** A bridge is a device that connects two separate networks. Bridges work on the Data Link Layer of the OSI model. Bridges forward frames based on the MAC addresses of the devices on the network.
- **Switch:** A switch is a device that connects multiple devices on a network. Switches work on the Data Link Layer of the OSI model. Switches forward frames based on the MAC addresses of the devices on the network. Switches are more intelligent than hubs, and they can forward frames more efficiently.
- **Router:** A router is a device that connects two or more networks. Routers work on the Network Layer of the OSI model. Routers forward packets based on the IP addresses of the devices on the network. Routers are the most intelligent network devices, and they can route packets through multiple networks.
- **Firewall:** A firewall is a device that protects a network from unauthorized access. Firewalls work on the Network Layer and Transport Layer of the OSI model. Firewalls filter packets based on a variety of criteria, such as IP addresses, ports, and protocols.

Name the four basic network topologies and cite an advantage of each type. Explain each topology with example.

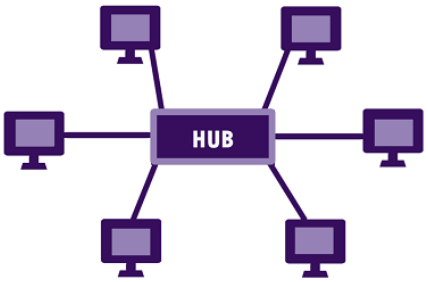
- **Bus topology:** A bus topology is a simple network topology in which all devices are connected to a single cable. For example, a bus topology could be used to connect a few computers in a small office.

  ✓ Advantage: Easy to set up and maintain.
  ✓ Disadvantage: Single point of failure.

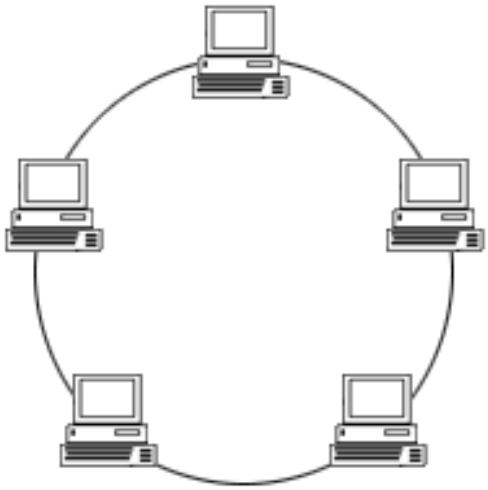


- **Star topology:** A star topology is a network topology in which all devices are connected to a central hub or switch. For example, a star topology could be used to connect all of the computers in a corporate office.

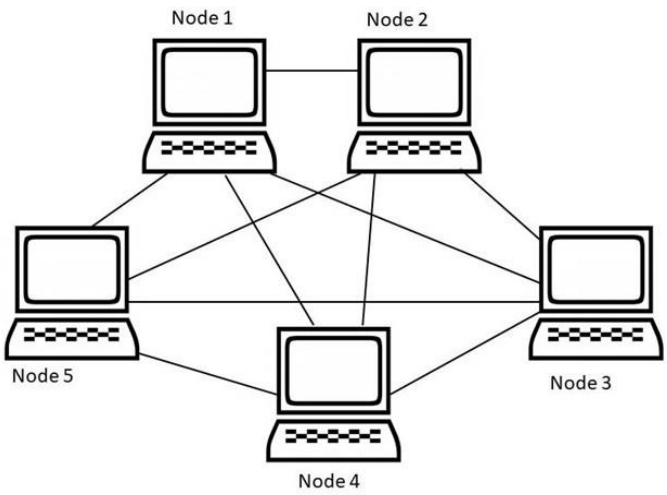
  ✓ Advantage: Easy to troubleshoot.
  ✓ Disadvantage: Centralized hub or switch is a single point of failure.



- **Ring topology:** A ring topology is a network topology in which all devices are connected in a loop. For example, a ring topology could be used to connect a few computers in a laboratory.
    - ✓ Advantage: Fault-tolerant.
    - ✓ Disadvantage: Difficult to troubleshoot.



- **Mesh topology:** A mesh topology is a network topology in which all devices are connected to each other. For example, a mesh topology could be used to connect all of the computers in a military base.
    - ✓ Advantage: Highly reliable.
    - ✓ Disadvantage: Expensive and difficult to manage.



Discuss the responsibilities of data link layer. Explain its design issues in detail.

The Data Link Layer (DLL) is the second layer of the Open Systems Interconnection (OSI) model. It is responsible for providing a reliable link between two nodes on a network. The DLL does this by providing services such as:

- **Framing:** The DLL breaks the data up into frames, which are the smallest unit of data that can be transferred between two nodes.
- **Addressing:** The DLL assigns addresses to each frame, so that the frames can be delivered to the correct destination node.
- **Error detection and correction:** The DLL detects and corrects errors that occur during transmission.
- **Flow control:** The DLL controls the flow of data between two nodes, so that one node does not overwhelm the other.

Design Issues:

- **How to frame data:** The DLL has to decide how to break the data up into frames. The size of the frames will affect the efficiency of the network, so the DLL has to choose a size that is appropriate for the network.
- **How to address frames:** The DLL has to assign addresses to each frame. The addresses have to be unique, so that the frames can be delivered to the correct destination node.
- **How to detect and correct errors:** The DLL has to detect and correct errors that occur during transmission. The DLL can use a variety of techniques to detect errors, such as checksums and cyclic redundancy checks (CRCs).
- **How to control the flow of data:** The DLL has to control the flow of data between two nodes, so that one node does not overwhelm the other. The DLL can use a variety of techniques to control the flow of data, such as sliding windows and stop-and-wait protocols.

Explain with the help of example why the window size is less than 2m in Go back NARQ if frames are numbered from from 0 to m-1. Also explain why the window size is less than or equal to 2m-1 in Selective Repeat ARQ if frames are numbered from 0 to m-1 with the help of example.

The window size in Go-Back-N ARQ is less than 2m because the sender has to wait for a NAK before it can retransmit the frames.

For example, let's say that the window size is 20 frames and that the frames are numbered from 0 to 19. If the receiver does not receive frame 10, it sends a NAK to the sender. The sender then retransmits frames 10 to 19. This means that the sender has to wait for 10 frames before it can send the next window of frames.

The window size in Selective Repeat ARQ is less than or equal to 2m-1 because the sender only has to retransmit the frames that have been received incorrectly.

For example, let's say that the window size is 20 frames and that the frames are numbered from 0 to 19. If the receiver receives frames 10, 11, and 12 incorrectly, it sends NAKs for those frames. The sender then retransmits frames 10, 11, and 12. This means that the sender only has to retransmit 3 frames, which is much better than having to retransmit all 20 frames in Go-Back-N ARQ.

Give two reasons why networks might use an error correcting code instead of error detection and retransmission.

1. **Performance:** Error correcting codes can often correct more errors than error detection and retransmission, which can improve the performance of the network. This is because error correcting codes can correct errors without having to retransmit the entire frame.
2. **Cost:** Error correcting codes can be less expensive than error detection and retransmission, especially in networks with a high error rate. This is because error correcting codes do not require the sender to retransmit the entire frame if an error is detected.

Suppose that an 11-Mbps 802.11 b LAN is transmitting 64-byte frames back to back over a radio channel with a bit error of 107. How many framed per second will be damaged on average?

Probability of error per bit = 10^{-7}

Probability of bit arriving correctly = $1 - 10^{-7}$

Probabiilty of a 64 B frame arriving correctly = $(1 - 10^{-7})^{64*8} = 0.9999488$

Probability of a frame being damaged = $1–0.9999488 = 5.12 * 10^{-5}$

Since data-rate is 11-Mbps, no. of frames transmitted per second =
$(11 * 10^6)/(64 * 8) = 21484.375$ frames/sec

No. of damaged frames per second = no. of frames/sec * prob. of a frame being damaged
$= 21484.375 * (5.12 * 10^{-5}) = 1.0999 = 1.1$ frames/sec (approx.)

Explain five key assumptions for formulating the dynamic channel allocation in LANs and MANs

1. **Independent traffic:** The traffic generated by each station is independent of the traffic generated by other stations. This means that the probability of a station generating a frame for transmission is not affected by the transmissions of other stations.
2. **Single channel:** All stations share a single channel for communication. This means that only one station can transmit at a time.
3. **Observable collision:** When two or more stations transmit at the same time, a collision occurs. All stations are able to detect collisions.

4. **Continuous or slotted time:** Time can be either continuous or slotted. In continuous time, frames can be transmitted at any time. In slotted time, frames can only be transmitted at the beginning of a slot.
5. **Carrier sensing:** Stations are able to sense if the channel is busy before transmitting. This means that stations will not transmit if the channel is already in use.

An ISP is granted a block of addresses starting with 120.60.4.0/20. The ISP wants to distribute these blocks to 100 organizations with each organization receiving 8 addresses only. Design the subblocks and give the slash notation for each sub block. Find out how many addresses are still available after these allocations.

The site has $2^{32-20} = 2^{12} = 4096$ addresses. We need to add 7 more 1s to the site prefix ($2x \geq 100$; $x = 7$). $2^{32-27} = 2^5 = 32$. Each of the 100 organizations has 32 addresses, but only 8 are needed. We add 2 more 1s to the site prefix. $2^{32-29} = 8$.

1st subnet: 120.60.4.0/29 to 120.60.4.7/29

... ...

32nd subnet: 120.60.4.248/29 to 120.60.4.255/29

33rd subnet: 120.60.5.0/29 to 120.60.5.7/29

... ...

64th subnet: 120.60.5.248/29 to 120.60.5.255/29

... ...

99th subnet: 120.60.7.16/29 to 120.60.7.23/29

100th subnet: 120.60.7.24/29 to 120.60.7.31/29

Subnets:

4096 − 800 = 3296 addresses left

A computer on a 6-Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 1 Mbps. It is initially filled to capacity with 8 megabits. How long can the computer transmit at the full 6 Mbps?

Max transmission rate, M=6 Mbps

Token arrival rate, R=1 Mbps

Capacity of token bucket, C=8 Mb

Time duration in which a computer will transmit in full speed= $\frac{C}{M-R} = \frac{8}{6-1} = \frac{8}{5} = 1.6$ sec

Give an argument why the leaky bucket algorithm should allow just one packet per tick, independent of how large the packet is.

- **The leaky bucket algorithm is a rate limiter.** It is designed to ensure that the sender does not transmit data at a rate that exceeds the maximum allowed rate. If the leaky bucket algorithm allowed more than one packet per tick, then it would not be able to effectively limit the rate of the sender.
- **Allowing more than one packet per tick would favor large packets over small packets.** This is because a large packet would be able to occupy the bucket for a longer period of time, allowing it to transmit more data before being blocked. This would give large packets an unfair advantage over small packets.
- **Allowing more than one packet per tick would make the algorithm more complex.** The algorithm would need to keep track of the size of each packet in order to ensure that only one packet was transmitted per tick. This would add unnecessary complexity to the algorithm.