What is Signaling System-7 ? and its characterstics

Signaling System 7 (SS7) is a set of protocols used for communication among various elements of telecommunication networks. It's a signaling network used to set up, manage, and tear down telephone calls and other telecommunication services.

Characteristics of SS7:

1. **Signaling:** SS7 is primarily a signaling system, facilitating the exchange of information necessary for call setup, routing, and termination in telecommunications networks.
2. **Common Channel Signaling:** It operates on a separate, dedicated out-of-band signaling channel, distinct from the voice/data channels used for actual communication. This separation ensures that signaling information doesn’t congest voice/data channels and allows for faster call setup.
3. **Point-to-Point Communication:** SS7 facilitates communication between two network elements in a point-to-point manner. This allows for direct and efficient signaling between different nodes in the network.
4. **Layered Architecture:** SS7 has a layered architecture, consisting of multiple levels (or layers) with specific functions, including Message Transfer Part (MTP), Signaling Connection Control Part (SCCP), and Transaction Capabilities Application Part (TCAP).
5. **Global Standard:** SS7 is a globally accepted standard for signaling in telecommunications networks, ensuring interoperability among different vendors' equipment and networks.
6. **Support for Various Services:** SS7 supports a wide range of telecommunication services beyond traditional voice calls, including SMS (Short Message Service), intelligent network services, and call forwarding.
7. **Reliability and Security:** SS7 is designed with robustness and security in mind. However, in recent years, there have been concerns about vulnerabilities within the SS7 protocol that could potentially be exploited for unauthorized access or tracking of mobile devices.
8. **Call Control and Network Management:** It handles call setup, teardown, and various network management functions, enabling efficient operation and control of telecommunications networks.

SS7 has been a foundational component in telecommunications for decades, playing a crucial role in establishing and managing communication services across different networks and services. However, as technology evolves, newer signaling systems and protocols, such as Diameter and IP-based signaling, have emerged to address the requirements of modern telecommunications networks and services.

Difference between IEEE 802.3, 802.4 and 802.5

EEE 802 specifies to a group of IEEE standards. IEEE standards 802 are used for controlling the Local Area Network and Metropolitan Area Network. The user layer in IEEE 802 is serviced by the two layers- the data link layer and the physical layer. The generally uses specifications of IEEE 802 are:

- **IEEE 802.3** The IEEE 802.3 standard determines the CSMA/CD access control protocol. The best known scheme for controlling a local area network on a bus structure is carrier sense multiple action with collision detection(CSMA/CD).
- **IEEE 802.4** IEEE 802.4 describes a token bus LAN standards.In token passing methods, stations connected on a bus are arranged in a logical ring. In this method only the station having token(token holder)is being permitted to transmit frames.
- **IEEE 802.5** IEEE 802.5 describes the token ring standards. In a token ring a special bit pattern, called the token, circulates around the ring whenever all stations are idle.The sequence of token is determined by the physical locations of the stations on the ring.

Let's see the difference between IEEE 802.3, 802.4 and 802.5 :-

S.No.	IEEE 802.3	IEEE 802.4	IEEE 802.5
1.	Topology used in IEEE 802.3 is Bus Topology.	Topology used in IEEE 802.4 is Bus or Tree Topology.	Topology used in IEEE 802.5 is Ring Topology.
2.	Size of the frame format in IEEE 802.3 standard is 1572 bytes.	Size of the frame format in IEEE 802.4 standard is 8202 bytes.	Frame format in IEEE 802.5 standard is of the variable size.
3.	There is no priority given in this standard.	It supports priorities to stations.	In IEEE 802.5 priorities are possible
4.	Size of the data field is 0 to 1500 bytes.	Size of the data field is 0 to 8182 bytes.	No limit is on the size of the data field.

S.No.	IEEE 802.3	IEEE 802.4	IEEE 802.5
5.	Minimum frame required is 64 bytes.	It can handle short minimum frames.	It supports both short and large frames.
6.	Efficiency decreases when speed increases and throughput is affected by the collision.	Throughput & efficiency at very high loads are outstanding.	Throughput & efficiency at very high loads are outstanding.
7.	Modems are not required.	Modems are required in this standard.	Like IEEE 802.4, modems are also required in it.
8.	Protocol is very simple.	Protocol is extremely complex.	Protocol is moderately complex.
9.	It is not applicable on Real time applications, interactive Applications and Client-Server applications.	It is applicable to Real time traffic.	It can be applied for Real time applications and interactive applications because there is no limitation on the size of data.

routing techniques in circuit switching network

In circuit-switched networks, routing techniques differ significantly from those used in packet-switched networks. In circuit switching, the established path remains dedicated for the entire duration of the communication session. Here are the primary routing techniques used in circuit-switched networks:

1. **Fixed Routing:**
   - In circuit-switched networks, fixed routing establishes predetermined paths between nodes. These paths are established during the setup phase and remain dedicated for the duration of the call.
   - Fixed routing doesn’t involve dynamic adjustments or considerations of network congestion or varying traffic patterns.
2. **Static Routing:**
   - Similar to fixed routing, static routing involves predetermined paths. However, these paths might be manually configured or adjusted occasionally.

- Static routing can offer a bit more flexibility compared to fixed routing, as administrators can manually alter routes if necessary.

3. **Dynamic Routing (Adaptive Routing):**
   - Dynamic routing techniques, though less common in traditional circuit-switched networks, involve real-time adjustments to the established paths based on current network conditions.
   - Dynamic routing allows for adapting to changes in the network, such as failures or congestion, by dynamically rerouting connections to available paths.
   - Some circuit-switched networks might incorporate basic dynamic routing capabilities to adapt to changes, but this isn't as prevalent as in packet-switched networks like IP networks.
4. **Least Cost Routing:**
   - This technique involves selecting the least costly or most efficient path based on predefined metrics such as distance, cost, or quality.
   - Paths are chosen at the setup phase based on these metrics and remain fixed for the duration of the call.

Circuit-switched networks focus on establishing and maintaining a dedicated path for the entire duration of a communication session, hence emphasizing the need for a predetermined route that remains constant throughout the call. As a result, routing techniques in circuit switching are more static and less dynamic compared to packet-switched networks, where routers dynamically determine the best path for each packet based on real-time network conditions.

- **GEO (Geostationary Earth Orbit)** at about 36,000km above the earth's surface.
- **LEO (Low Earth Orbit)** at about 500-1500km above the earth's surface.
- **MEO (Medium Earth Orbit)** or **ICO (Intermediate Circular Orbit)** at about 6000-20,000 km above the earth's surface.

The primary differences among Medium Earth Orbit (MEO), Geostationary Orbit (GEO), and Low Earth Orbit (LEO) satellites lie in their altitudes, orbital characteristics, coverage areas, and applications:

1. **Altitude:**
   - **MEO (Medium Earth Orbit):** MEO satellites orbit at intermediate altitudes, generally ranging from 2,000 to 35,786 kilometers (1,243 to 22,236 miles) above the Earth's surface.
   - **GEO (Geostationary Orbit):** GEO satellites orbit at an altitude of approximately 35,786 kilometers (22,236 miles) above the equator.
   - **LEO (Low Earth Orbit):** LEO satellites orbit at lower altitudes, usually ranging from 160 to 2,000 kilometers (100 to 1,243 miles) above the Earth's surface.
2. **Orbital Characteristics:**
   - **MEO:** These satellites orbit the Earth in elliptical paths, providing moderate coverage and a compromise between coverage area and latency.
   - **GEO:** GEO satellites orbit the Earth directly above the equator and rotate at the same speed as the Earth's rotation, making them appear stationary from the ground. They offer continuous coverage of a fixed geographic area.

- **LEO:** LEO satellites orbit closer to the Earth's surface and complete orbits more frequently, resulting in quicker coverage changes and lower latency.

3. **Coverage Area:**
   - **MEO:** Moderate coverage area compared to GEO and LEO satellites.
   - **GEO:** Provides continuous coverage over a specific geographic area, making them ideal for global communication services.
   - **LEO:** Offers global coverage but with quicker passes over any given point on the Earth's surface.
4. **Applications:**
   - **MEO:** Used in navigation systems like GPS (Global Positioning System) and communication services requiring moderate latency.
   - **GEO:** Ideal for applications that require continuous coverage of a specific area, such as broadcasting, weather monitoring, and global communication services.
   - **LEO:** Suited for applications demanding low latency and high-speed communication, such as internet services, Earth observation, and scientific research.

Given that the signal is 200 mW, you will convert this into Wats;

200/1000 = 0.2W

Noise = $10 \times 2 \times 10^{-6} = 2 \times 10^{-5}$

Therefore the SNR = Average signal power÷Average noise power

$0.2/2 \times 10^{-5} = 10000$

Thus:

SNR db = 10 $\log_{10}$ (SNR)

So in this case 10 $\log_{10}$ (10000) = **40.**

haracteristics	Twisted pair cable	Co-axial cable	Optical fiber cable
Signal transmission	Takes place in the electrical form over the metallic conducting wires.	Takes place in the electrical form over the inner conductor of the cable.	Takes place in an optical form over glass fiber.
Consists of	Pair of insulated copper wires	Requires 4 components from inner to outer-	Bundling of very thin optical fibers made up of glass

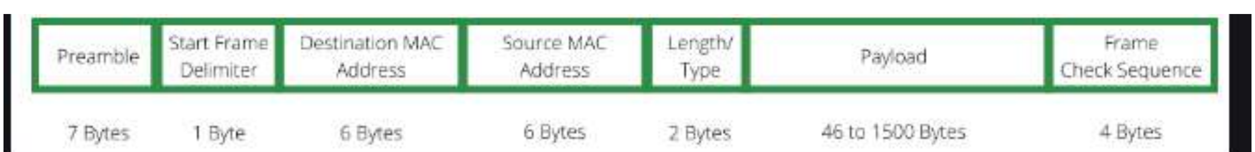
haracteristics	Twisted pair cable	Co-axial cable	Optical fiber cable
		• Solid conductor wire • Layer of insulation • Grounding conductor • Layer of exterior insulation.	or plastic in a single cable.
Installation and Implementation	Simple and easy	Relatively difficult	Difficult
External magnetic field	Affected due to external magnetic field.	The external magnetic field is less affected.	The external magnetic field is not affected.
Cause of power	Power loss due to conduction and radiation.	Power loss due to conduction.	power loss due to absorption, scattering, and bending.
Diameter	Large diameter than Optical fiber cable.	Large diameter than Optical fiber cable.	Small diameter
Bandwidth	The twisted-pair cable has low bandwidth.	Co-axial cable has moderately high bandwidth.	Optical fiber cable has a very high bandwidth.
Electromagnetic interference(EMI)	EMI can take place.	EMI is reduced to shielding.	EMI is not present.
Installation	Easy installation.	Fairly easy installation.	Difficult to install.

haracteristics	Twisted pair cable	Co-axial cable	Optical fiber cable
Attenuation	In twisted pair cable has very high attenuation.	In coaxial cable has low attenuation.	In optical fiber cable has very low attenuation.
Data rate	Twisted pair cable supports a low data rate.	Moderately high data rate.	Very high data rate.
Noise immunity	Twisted pair cable has low noise immunity.	Co-axial cable has higher noise immunity.	Optical fiber cable has the highest noise immunity.
Cost	The cost is very low.	Cost is moderate	Cost is expensive.
Repeater Spacing	Repeater spacing is 2-10 km.	Repeater spacing is 1-10 km.	Repeater spacing is 10-100 km.
Security	Security is not guaranteed of the transmitted signal.	Security is not guaranteed of the transmitted signal.	Security is guaranteed of the transmitted signal.
Types	• Unshielded Twisted Pair (UTP) • Shielded Twisted Pair (STP)	• RG59 • RG6	• Single mode fiber (SMF) • Multimode fiber (MMF)
Power loss	Reasons- conduction and radiation	Reasons- absorption, scattering	Reasons- conduction

haracteristics	Twisted pair cable	Co-axial cable	Optical fiber cable
		dispersion and bending	

Category	FHSS	DSSS
Abbreviation	FHSS is Frequency-Hopping Spread Spectrum	DSSS is Direct-Sequence Spread Spectrum
Definition	FHSS is a type of spread spectrum technology in which the frequency of the transmitted signal changes according to a specific pattern.	DSSS is a type of spread spectrum technology in which the transmitted signal is spread across multiple frequency bands.
Pattern	In FHSS, the data transmission is encoded and decoded using a specific pattern called **hopset**.	In DSSS, the data transmission is encoded and decoded using a pseudo-random binary sequence or **chip** code.
Frequency band	FHSS transmits data using a narrowband carrier that hops among different frequency channels.	DSSS transmits data using a wider frequency band.
Interference resistant	FHSS is more resistant to interference because it uses frequency hopping, which makes it difficult to intercept the signal.	DSSS is more vulnerable to interference because it uses a wider frequency band.

Category	FHSS	DSSS
Susceptibility	FHSS is less susceptible to multipath fading, it is a phenomenon in which the transmitted signal arrives at the receiver via multiple paths, resulting in a loss of signal quality.	DSSS is more susceptible to multipath fading because it uses a wider frequency band.
Transmission speed	FHSS has low transmission rates (up to 3 Mbps).	DSSS has high transmission rates (up to 11 Mbps).
Modulation techniques used	Multilevel Frequency Shift Keying (FSK) was used.	BPSK (Binary Phase-Shift Keying) was used.
Efficiency	FHSS is generally more efficient than DSSS in terms of bandwidth utilization.	DSSS is less efficient because it uses a wider frequency band.
Application areas	It is widely used in a variety of applications, including wireless networking like Bluetooth, mobile communications, and military communications.	It is well-suited for particular applications where the signal must travel over long distances like GPS, and WIFI



The Ethernet Frame

In the context of Ethernet frames, the smallest Ethernet frame, known as the Minimum Ethernet Frame, consists of the following components:

1. **Preamble:** 7 bytes

2. **Start Frame Delimiter (SFD):** 1 byte
3. **Destination MAC Address:** 6 bytes
4. **Source MAC Address:** 6 bytes
5. **EtherType/Length:** 2 bytes
6. **Data (Payload):** Variable length (46 to 1500 bytes)
7. **Frame Check Sequence (FCS):** 4 bytes

The useful data refers to the payload or the actual data being transmitted, excluding the header (Destination MAC, Source MAC, EtherType/Length) and trailer (Preamble, SFD, FCS) information.

Calculating the ratio of useful data to the entire packet for the smallest Ethernet frame:

Useful Data = Data Payload Entire Packet = Data Payload + Header + Trailer

For the minimum Ethernet frame:

Useful Data = Data Payload = 46 bytes (minimum payload for Ethernet frame) Entire Packet = Data Payload (46 bytes) + Header (Preamble: 7 bytes + SFD: 1 byte + Destination MAC: 6 bytes + Source MAC: 6 bytes + EtherType/Length: 2 bytes) + Trailer (FCS: 4 bytes) = 72 bytes

Ratio of Useful Data to Entire Packet: Useful Data / Entire Packet = 46 bytes / 72 bytes ≈ 0.638 or approximately 63.8%

Please note that this calculation considers the smallest Ethernet frame, and in practical scenarios, larger Ethernet frames are often used to improve efficiency by maximizing the useful data-to-overhead ratio.

Characteristics of FDDI

- FDDI gives 100 Mbps of information throughput.

- FDDI incorporates two interfaces.
- It is utilized to associate the equipment to the ring over long distances.
- FDDI could be a LAN with Station Management.
- Allows all stations to have broken even with the sum of time to transmit information.
- FDDI defines two classes of traffic viz. synchronous and asynchronous.

Advantages of FDDI

- Fiber optic cables transmit signals over more noteworthy separations of approximately 200 km.
- It is conceivable to supply the need to the work stations associated within the chain. Consequently, based on the prerequisite a few stations are bypassed to supply speedier benefit to the rest.
- FDDI employments different tokens to make strides organize speed.
- It offers a higher transmission capacity (up to 250 Gbps). Thus, it can handle information rates up to 100 Mbps.
- It offers tall security because it is troublesome to spy on the fiber-optic link.
- Fiber optic cable does not break as effectively as other sorts of cables.

Disadvantages of FDDI

- FDDI is complex. Thus establishment and support require an incredible bargain of expertise.
- FDDI is expensive. Typically since fiber optic cable, connectors and concentrators are exceptionally costly.

FDDI defines various field formats in its frame structure:

1. **Preamble**: This is a set bit pattern used for synchronization and identification of the start of the frame.
2. **Start Delimiter (SD)**: Marks the beginning of the frame following the preamble.
3. **Frame Control (FC)**: Contains control information about the frame, such as frame type, priority, and token information.
4. **Destination Address (DA)**: Specifies the MAC address of the intended recipient device.
5. **Source Address (SA)**: Indicates the MAC address of the sender device.
6. **Frame Check Sequence (FCS)**: A field used for error detection and ensuring the integrity of the frame.
7. **Frame Status (FS)**: Includes information about successful receipt of the frame.
8. **Data**: This field carries the actual data being transmitted.
9. **End Delimiter (ED)**: Marks the end of the frame.
10. **Frame Status (FS)**: Contains information about the status of the frame transmission.

S.No.	Synchronous TDM	Statistical TDM
1.	The data flow of each input connection is divided into units and each input control one output time slot.	The slots are allotted dynamically. Input line is given slots in output frame only if it has data to send.
2.	In this, number of slots in each frame are equal to number of input lines.	In this, number of slots in each frame are less than the number of input lines.
3.	The maximum bandwidth utilization is done when all inputs have data to send.	The volume of link is normally is less than the sum of the volume of each channel.
4.	In this de-multiplexer at receiving end decomposes each frame, discards framing bits and draw out data unit in turn. This draw out data unit from frame is then passed to destination device.	In this de-multiplexer at receiving end decomposes each frame, by checking local address of each data unit. This draw out data unit from frame is then passed to destination device.
5.	It uses synchronization bits at the beginning of each frame.	It does not used synchronization bits.
6.	Slots in this carry data only and there is no need of addressing.	Slots in this contain both data and address of the destination.
7.	In this, buffering is not done, frame is sent after a specific interval of time whether it has data to send or not.	In this, buffering is done and only those inputs are given slots in output frame whose buffer contains data to send.

cuit Switching	Packet Switching
In-circuit switching has there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In-circuit switching, each data unit knows the entire path address which is provided by the source.	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase because there might be	Congestion can occur during the data transfer phase, a large

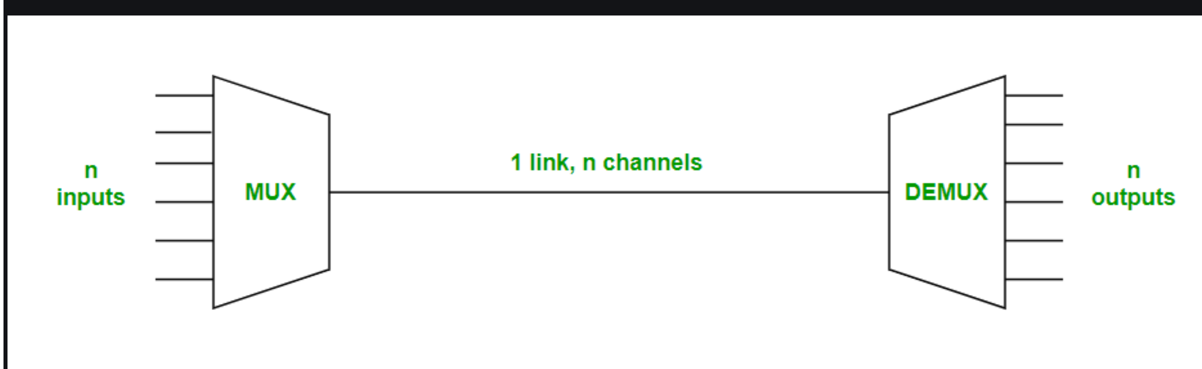
cuit Switching	Packet Switching
a case where a request is being made for a channel but the channel is already occupied.	number of packets comes in no time.
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.
In-Circuit switching, the charge depends on time and distance, not on traffic in the network.	In Packet switching, the charge is based on the number of bytes and connection time.
Recording of packets is never possible in circuit switching.	Recording of packets is possible in packet switching.
In-Circuit Switching there is a physical path between the source and the destination	In Packet Switching there is no physical path between the source and the destination
Circuit Switching does not support store and forward transmission	Packet Switching supports store and forward transmission
Call setup is required in circuit switching.	No call setup is required in packet switching.
In-circuit switching each packet follows the same route.	In packet switching packets can follow any route.
The circuit switching network is implemented at the physical layer.	Packet switching is implemented at the datalink layer and network layer
Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.

Basics	Circuit Switching	Message Switching	Packet Switching
Connection Creation	Connection is created between the source and destination by establishing a dedicated path between source and destination.	Links are created independently one by one between the nodes on the way.	Links are created independently one by one between the nodes on the way.
Queuing	No queue is formed.	Queue is formed.	Queue is formed.
Message and Packets	There is one big entire data stream called a message.	There is one big entire data stream called a message.	The big message is divided into a small number of packets.
Routing	One single dedicated path exists between the source and destination.	Messages follow the independent route to reach a destination.	Packets follow the independent path to hold the destination.
Addressing and sequencing	Messages need not be addressed as there is one dedicated path.	Messages are addressed as independent routes are established.	Packets are addressed, and sequencing is done as all the packets follow the

Basics	Circuit Switching	Message Switching	Packet Switching
			independent route.
Propagation Delay	No	Yes	Yes
Transmission Capacity	Low	Maximum	Maximum
Sequence Order	Message arrives in Sequence.	Message arrives in Sequence.	Packets do not appear in sequence at the destination.
Use Bandwidth	Wastage	Bandwidth is used to its maximum extent.	Bandwidth is used to its maximum extent.

What is Multiplexing?

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.



Types of Multiplexing

There are Five types of Multiplexing :

1. Frequency Division Multiplexing (FDM)
2. Time-Division Multiplexing (TDM)
3. Wavelength Division Multiplexing (WDM)
4. Code-division multiplexing (CDM)
5. Space-division multiplexing (SDM):

Aspect	Wired Ethernet	Wireless LAN (Wi-Fi)	ATM LAN
Medium	Uses physical cables (e.g., twisted pair, coaxial)	Wireless radio waves (no physical cables)	Uses fiber optics or twisted pair
Speed	Typically faster (varies, but can reach high speeds)	Slower compared to wired, affected by signal strength and interference	High-speed, capable of very high data rates
Security	Generally more secure due to physical connection	Vulnerable to interception, encryption essential for security	Offers robust security features
Installation	Requires physical cables and ports	No cables, flexible installation	Requires specific infrastructure setup
Mobility	Stationary, limited mobility	Offers mobility, can connect from different locations	Primarily for fixed installations
Interference	Less susceptible to interference	Susceptible to interference from various sources	Less susceptible to interference
Reliability	More reliable due to stable physical connections	Slightly less reliable due to potential signal disruptions	Highly reliable due to dedicated connections
Standards	Defined by IEEE standards (e.g., 802.3 for Ethernet)	Governed by IEEE 802.11 standards	Governed by ITU-T standards
Cost	Generally less expensive for cabling and equipment	Equipment costs can be moderate to high	Infrastructure setup cost can be significant
Scalability	Scalable, but additional cabling may be necessary	Scalable within range of access points	Scalable, supports high bandwidth for multiple users

UNIT-I

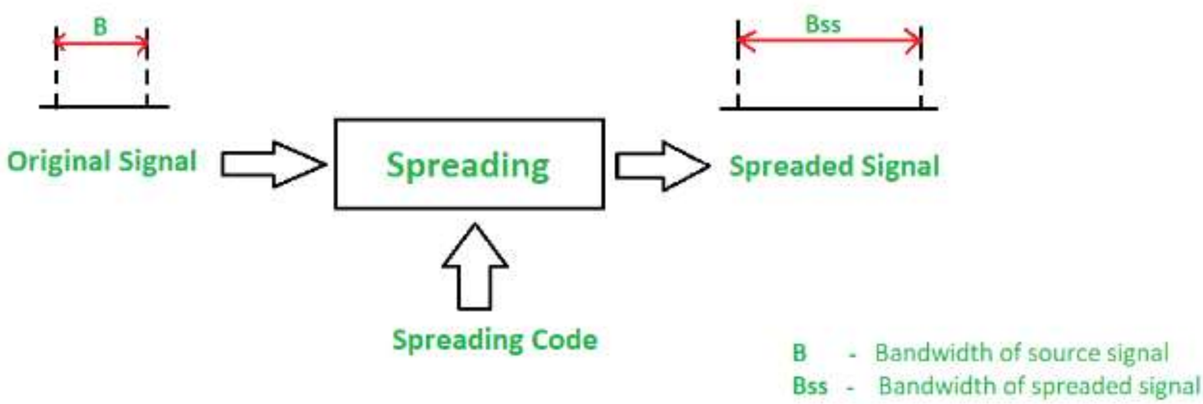
II. Compare and contrast circuit switching, virtual circuit switching, message switching and packet (Datagram) switching with suitable examples. (10)

III. What is multiplexing? Describe various multiplexing methods with examples. (10)

IV. Explain and compare wired Ethernet LAN, wireless LAN and ATM LAN. (10)

LAN	WLAN
LAN stands for Local Area Network.	WLAN stands for Wireless Local Area Network.
LAN connections include both wired and wireless connections.	WLAN connections are completely wireless.
LAN network is a collection of computers or other such network devices in a particular location that are connected together by communication elements or network elements.	WLAN network is a collection of computers or other such network devices in a particular location that are connected together wirelessly by communication elements or network elements.
LAN is free from external attacks like interruption of signals, cyber criminal attacks and so on.	Whereas, WLAN is vulnerable to external attacks.
LAN is secure.	WLAN is not secure.
LAN network has lost its popularity due to the arrival of latest wireless networks.	WLAN is popular.
Wired LAN needs physical access like connecting the wires to the switches or routers.	Work on connecting wires to the switches and routers are neglected.
In LAN, devices are connected locally with Ethernet cable.	For WLAN Ethernet cable is not necessary.

LAN	WLAN
Mobility limited.	Outstanding mobility.
It may or may not vary with external factors like environment and quality of cables.	It varies due to external factors like environment and quality of cables. Most of the external factors affect the signal transmission.
LAN is less expensive.	WLAN is more expensive.
Example: Computers connected in a college.	Example: Laptops, cellphones, tablets connected to a wireless router or hotspo



Spread Spectrum is a technique used in telecommunications and signal processing to spread the bandwidth of a signal over a wider frequency range than the original information signal. It's primarily employed in wireless communication systems to achieve various objectives such as improved reliability, security, and resistance to interference.

There are two primary types of Spread Spectrum:

1. **Direct Sequence Spread Spectrum (DSSS)**:
   - DSSS spreads the signal over a wider bandwidth by multiplying it with a higher data-rate bit sequence known as a spreading code or chip sequence.

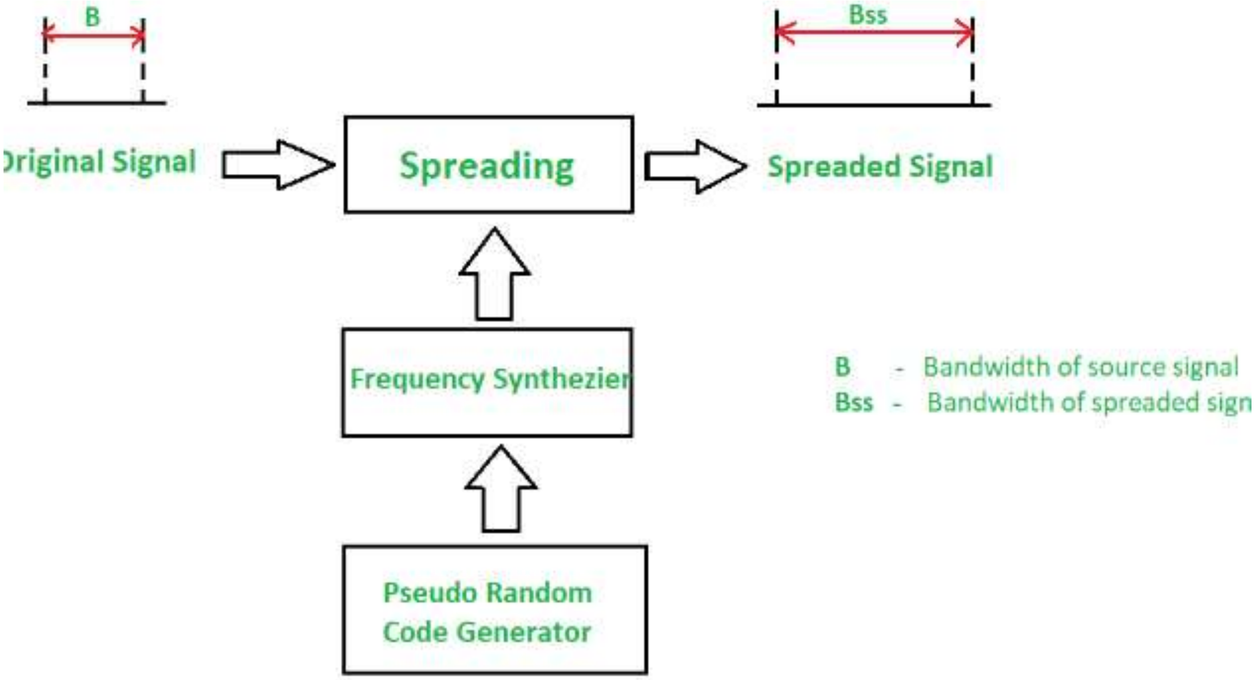
- This spreading code is unique to the transmitter-receiver pair and allows the signal to be recovered at the receiver end by using the same code to despread the received signal.
- DSSS provides resistance to interference and jamming because the signal appears as noise to an unintended receiver without the correct spreading code.

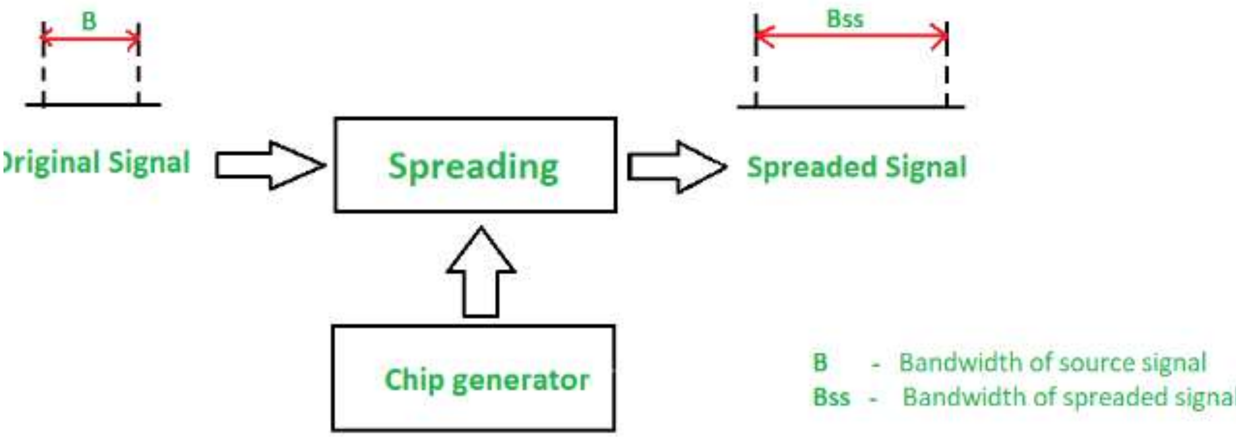
2. **Frequency Hopping Spread Spectrum (FHSS)**:
    - FHSS works by rapidly switching frequencies in a predetermined sequence.
    - It divides the signal into small pieces and transmits each piece at different frequencies within the available bandwidth.
    - This hopping pattern is synchronized between the transmitter and receiver, allowing them to follow the same sequence and reassemble the transmitted signal.

Spread Spectrum offers several advantages:

- **Resistance to Interference**: Spread Spectrum signals appear as noise to unauthorized receivers, making them more resistant to interference and jamming.
- **Security**: The unique spreading codes used in Spread Spectrum systems enhance security by making it difficult for unauthorized users to intercept the signal.
- **Robustness**: Spread Spectrum systems can provide robust and reliable communication, especially in environments with high interference or noise.

These advantages have led to the widespread adoption of Spread Spectrum techniques in various wireless communication systems, including Wi-Fi networks, Bluetooth devices, and some military and satellite communication systems.


B
Bss
riginal Signal
Spreading
Spreaded Signal
Frequency Synthezier
B - Bandwidth of source signal
Bss - Bandwidth of spreaded sign
Pseudo Random
Code Generator


B
Bss
riginal Signal
Spreading
Spreaded Signal
Chip generator
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

Key	Fast Ethernet	Gigabit Ethernet
Successor	Fast Ethernet is the successor of 10-Base-TEthernet.	Gigabit Ethernet is successor of Fast Ethernet.
Network speed	The maximum speed of Fast Ethernet is 100 Mbps.	Gigabit Ethernet speed can reach up to 1 Gbps.
Complexity	Fast Ethernet is simple to configure.	Gigabit Ethernet is quite complex to configure.
Delay	Fast Ethernet generates ore delay.	Gigabit Ethernet generates less delay than Fast Ethernet.
Coverage Limit	The maximum coverage distance for Fast Ethernet is 10 kilometers.	The maximum coverage distance for Gigabit Ethernet is 70 kilometers.
Round trip delay	The round trip delay in Fast Ethernet is 100 to 500 bit times.	The round trip delay in Gigabit Ethernet is 4000 bit times.

Aspect	Ethernet	Fast Ethernet	Gigabit Ethernet
Speed	10 Mbps	100 Mbps	1000 Mbps (1 Gbps)
Physical Media	Typically uses coaxial or twisted-pair cables	Uses twisted-pair cables (Cat 5 or better)	Uses twisted-pair cables (Cat 5e or Cat 6)
Frame Format	Uses the Ethernet frame format (802.3)	Uses the same Ethernet frame format (802.3u)	Uses the same Ethernet frame format (802.3ab)
Maximum Cable Length	100 meters	100 meters	100 meters
Backward Compatibility	Can communicate with Fast Ethernet devices	Can communicate with Ethernet and Gigabit Ethernet devices	Can communicate with Ethernet and Fast Ethernet devices
Interoperability	Interoperable with other Ethernet devices	Interoperable with other Fast Ethernet devices	Interoperable with other Gigabit Ethernet devices
Throughput	Lower throughput compared to Fast and Gigabit Ethernet	Higher throughput than Ethernet	Highest throughput among the three

Aspect	Ethernet	Fast Ethernet	Gigabit Ethernet
Network Standard	Defined by IEEE 802.3	Defined by IEEE 802.3u	Defined by IEEE 802.3ab
Market Availability	Initially prevalent, older technology	Commonly used in the 1990s and early 2000s	Widely used in modern networks

Aspect	Channel	Common Channel
Definition	Medium used for data transmission between devices	Dedicated/shared path for signaling/control
Purpose	Transmits data between sender and receiver	Used for signaling, control, and management
Usage	Carries actual data or information	Carries signaling information separate from data
Examples	Ethernet cables, Wi-Fi frequencies, fiber-optic links	SS7 signaling system, separate signaling channels
Characteristics	Transmits user data or payload	Handles call setup, routing, network management
Functionality	Provides the transmission path for data	Manages and controls communication setup and routing
Role	Facilitates communication by carrying information	Controls and manages communication network functions

In Channel	Common Channel
Trunks are held up during signalling.	Trunks aren't required for Signalling
Signal repertoire is limited.	Extensive signal repertoire is possible.
Interference between voice and Control signals may occur.	No interference as the two Channels are physically separate.
Separate signalling	Only one set of signalling

Equipment is needed for each trunk and thus expensive.	equipments is essential for a whole group of trunk Circuits and hence CCS is economical
Voice channel being the control channel, there is a possibility of potential misuse by the customers.	Control Channel is in general in accessible to users.
Signalling is comparatively slow.	Signalling is significantly fast.
It is difficult to change or add signals.	There is flexibility to change or add signals.
It is difficult to handle signalling during speech period.	Signals during speech. There is freedom to handle
Reliability of signalling path is not Critical.	Reliability of the signalling Path is critical.
Speech circuit reliability is assured.	There is no automatic test of speech circuit.

Common channel signalling is better than In-channel signalling.

Aspect	In-Band Signaling	Out-of-Band Signaling
Definition	Control information transmitted within the same channel used for data transmission.	Control information transmitted through a separate dedicated channel or medium.
Transmission	Control signals share the same path as the data being transmitted.	Control signals have a separate dedicated path or medium from the data path.
Data/Signaling Path	Uses the same channel or frequency spectrum as the actual user data.	Utilizes a distinct channel or frequency spectrum specifically reserved for signaling.
Examples	Using part of the data bandwidth for control information in a communication channel.	Using a separate network or dedicated channels for signaling (e.g., SS7 in telephony).
Efficiency	Utilizes the available data channel efficiently but may affect data throughput.	Provides a separate, dedicated path, reducing interference with data transmission.
Flexibility	Limited flexibility for separate control and data functions.	Offers greater flexibility for managing signaling separately from data.
Interference	Prone to interference affecting both data and signaling transmission.	Less prone to interference as signaling operates on separate channels.
Robustness	Susceptible to data and signaling conflicts affecting performance.	Offers greater robustness as signaling remains independent of data transmission.

In-band signaling integrates control or signaling information within the same communication channel used for transmitting user data. Conversely, out-of-band signaling involves a separate and dedicated channel for signaling, keeping it distinct from the data path. Each method has its advantages and limitations, impacting factors like efficiency, interference, and system complexity. The choice between in-band and out-of-band signaling often depends on the specific requirements of the communication system and the desired trade-offs between data efficiency, reliability, and flexibility.

S.NO	Serial Transmission	Parallel Transmission
1.	In this type, a single communication link is used to transfer data from one end to another	In this type, multiple parallels links used to transmit the data
2.	In serial transmission, data(bit) flows in bi-direction.	In Parallel Transmission, data flows in multiple lines.
3.	Serial Transmission is cost-efficient.	Parallel Transmission is not cost-efficient.
4.	In serial transmission, one bit transferred at one clock pulse.	In Parallel Transmission, eight bits transferred at one clock pulse.
5.	Serial Transmission is slow in comparison of Parallel Transmission.	Parallel Transmission is fast in comparison of Serial Transmission.
6.	Generally, Serial Transmission is used for long-distance.	Generally, Parallel Transmission is used for short distance.
7.	The circuit used in Serial Transmission is simple.	The circuit used in Parallel Transmission is relatively complex.

S.NO	Serial Transmission	Parallel Transmission
8.	Serial Transmission is full duplex as sender can send as well as receive the data	Parallel Transmission is half-duplex since the data is either send or receive
9.	Converters are required in a serial transmission to convert the data between internal and parallel form	No converters are required in Parallel Transmission
10.	Serial transmission is reliable and straightforward.	Parallel transmission is unreliable and complicated.

In Frame Relay networks, congestion control is essential to manage and alleviate network congestion, ensuring efficient data transmission. Frame Relay uses a form of congestion control known as "forward explicit congestion notification" (FECN) and "backward explicit congestion notification" (BECN). Here's an overview of congestion control in Frame Relay:

1. **Forward Explicit Congestion Notification (FECN)**:
    - When congestion occurs in a Frame Relay network at a switch (also known as a Frame Relay access device), the switch can set a "Congestion Indication" bit in the header of the frame as it forwards it towards its destination.
    - The Congestion Indication bit set to 1 indicates to the receiving device that congestion was encountered on the path.
2. **Backward Explicit Congestion Notification (BECN)**:
    - When a Frame Relay switch experiences congestion on its outgoing interface, it sets the Congestion Indication bit in the frames leaving that interface.
    - These frames travel back towards the originating device, informing it about the congestion.
3. **Action at the Receiving Device**:
    - Upon receiving frames with the Congestion Indication bit set (either through FECN or BECN), the receiving device can take actions to manage the situation.
    - Typically, the device can respond by throttling its transmission rate by either reducing the window size (for instance, in TCP sliding window protocols) or implementing other flow control mechanisms.
4. **Traffic Management**:

- Frame Relay networks might also implement traffic shaping and admission control mechanisms to prevent excessive traffic from entering the network, thus controlling congestion at its source.
- Traffic shaping regulates the flow of data to ensure it complies with the agreed-upon traffic parameters (committed information rate, excess burst size, etc.).

Frame Relay networks primarily rely on these explicit congestion notification mechanisms, along with traffic shaping and admission control, to manage and respond to congestion events. The goal is to maintain optimal performance and prevent network degradation caused by congestion.

The maximum data rate supported by a communication channel can be calculated using the Shannon-Hartley theorem, which relates the maximum data rate to the channel's bandwidth and signal-to-noise ratio (SNR).

The formula for maximum data rate (R) in a channel with bandwidth (B) and SNR (S/N) is given by:

$$R = B \cdot \log_2(1 + \mathrm{S/N})$$

There are two types of Time Division Multiplexing :

1. Synchronous Time Division Multiplexing
2. Statistical (or Asynchronous) Time Division Multiplexing

Advantages of Radio Transmission +

- Focal points of radio transmission incorporate the drawn-out encounters made with radio transmission for wide region organizations (for example microwave connections) and versatile mobile phones.
- Radio transmission can cover bigger territories and can infiltrate (more slender) dividers, plants, furniture and so forth
- Extra inclusion is picked up by reflection.
- Radio regularly needn't bother with a LOS (Line of Site) if the frequencies are not very high.
- Higher transmission rates (for example 54 Mbit/s) than infrared (coordinated laser joins, which offer information rates well over 100 Mbit/s).
- It helps in conveying radio publicizing to the clients. This will help in expanding income for the publicizing organizations.
- It uses adjustment plans, for example, AM and FM to use points of interest >> of the two of them.
- Cost is less in contrast with different administrations.

- Radio waves are untouched by clouds and earths atmosphere radio telescope can receive signals even though the sky is cloudy exception is strong winds, thunderstorm, large dish.
- Radio telescope can be used 24 hours.
- Radio waves can offers mobility at a lower price.
- It has low set up cost as it does not need any cables.
- No land acquisition right is required.

Disadvantages of Radio Transmission

- Radio transmission can meddle with different senders, or electrical gadgets can decimate information communicated by means of radio.
- Bluetooth is more basic than infrared.
- Radio is just allowed in certain recurrence groups.
- Protecting isn't so basic.
- Limited scopes of permit free groups are accessible worldwide and those that are accessible are not the equivalent in all nations.
- A ton of harmonization is going on because of market pressure.
- The radio waves that reach earth are very small and poor in strength.
- It get affected by strong winds and thunderstorm.
- It is uncertain and simple tap communication.

Applications of Radio Waves:

1. **Wireless Communication:** Applications include cellular networks, Wi-Fi, Bluetooth, and satellite communication, enabling voice and data transmission over wireless links.
2. **Broadcasting:** Radio waves are used for AM/FM radio broadcasting, allowing entertainment, news, and information dissemination.
3. **Radar Systems:** Radar systems use radio waves for various purposes, including air traffic control, weather monitoring, and military applications.
4. **Wireless Sensing:** They are used in RFID (Radio-Frequency Identification) systems for tracking and identification, as well as in wireless sensor networks for monitoring and control in various industries.
5. **Satellite Communication:** Radio waves enable communication between satellites and ground stations, facilitating global connectivity for telecommunications, GPS, weather forecasting, and more.

mircrowaves waves adv disadv application

Microwaves have distinct advantages and disadvantages, and they find application across various fields due to their unique characteristics.

Advantages of Microwaves:

1. **High Bandwidth:** Microwaves offer a higher bandwidth compared to lower frequency radio waves, enabling faster data transmission rates.
2. **Directional Transmission:** They can be easily focused into narrow beams, allowing for more targeted and directed transmission, reducing interference and enhancing security.
3. **Low Atmospheric Attenuation:** Microwaves experience relatively low attenuation when passing through the Earth's atmosphere compared to higher frequency waves like infrared or visible light.
4. **Shorter Wavelengths:** Their shorter wavelengths allow for the construction of smaller antennas, making them practical for various devices and applications.
5. **Line of Sight Communication:** They operate on line-of-sight propagation, suitable for point-to-point communication over long distances.

Disadvantages of Microwaves:

1. **Susceptibility to Obstructions:** Microwaves are easily obstructed by physical obstacles such as buildings, trees, and geographical features, which can limit their range and coverage.
2. **Weather Interference:** Certain weather conditions like heavy rain, fog, or snow can attenuate microwave signals, affecting signal quality and reliability.
3. **Cost of Infrastructure:** Building and maintaining microwave communication infrastructure, including specialized antennas and transmission equipment, can be costly.
4. **Interference and Noise:** Microwaves can experience interference from other microwave sources, leading to signal degradation and noise.

Applications of Microwaves:

1. **Communications:** Used in point-to-point and point-to-multipoint communication systems, including long-distance telephone, data transmission, and satellite communication.
2. **Radar Systems:** Microwaves are central to radar systems used in aviation, weather monitoring, defense, and navigation (such as air traffic control and vehicle collision avoidance).
3. **Wireless Networks:** Microwave technology is used in wireless local loop (WLL), fixed wireless broadband access, and microwave backhaul for cellular networks.
4. **Microwave Ovens:** Utilizing the ability of microwaves to heat water molecules, microwave ovens cook food quickly and efficiently.
5. **Medical Imaging:** In fields like radiology, microwaves are used in technologies like microwave imaging for diagnostic purposes.

The high data rates, directional transmission, and suitability for line-of-sight communication make microwaves invaluable in long-distance communication, radar systems, and various applications requiring high-speed data transmission. However, their susceptibility to obstruction and weather interference requires careful consideration in deployment and management.

infrared waves adv disadv and application

ChatGPT

ChatGPT

Infrared waves have specific advantages and disadvantages, and they find applications in various fields due to their unique properties.

Advantages of Infrared Waves:

1. **Safety:** Infrared waves are non-ionizing and generally considered safe for human exposure, unlike higher-energy electromagnetic waves like X-rays or ultraviolet radiation.
2. **Remote Sensing:** Infrared waves allow for remote sensing and imaging in applications such as thermal imaging cameras, night vision devices, and infrared astronomy.
3. **Wireless Communication:** Used in short-range wireless communication systems like infrared data transmission (IrDA), remote controls, and some wireless keyboards.
4. **Heating Applications:** Infrared radiation is utilized in heat lamps, infrared saunas, and industrial heating processes due to its ability to efficiently transfer heat.

Disadvantages of Infrared Waves:

1. **Limited Range and Penetration:** Infrared waves have limited range and are easily absorbed or scattered by materials, limiting their ability to penetrate obstacles.
2. **Environmental Factors:** Environmental factors such as humidity and atmospheric conditions can affect the transmission and quality of infrared signals.
3. **Interference:** They are susceptible to interference from other sources emitting infrared radiation, which can disrupt communication or sensing systems.
4. **Line of Sight Requirement:** Infrared communication typically requires a direct line of sight between the transmitter and receiver, limiting its applicability for longer-range communication.

Applications of Infrared Waves:

1. **Thermal Imaging:** Infrared cameras capture heat radiation to produce images used in various fields, including medical diagnosis, building inspections, and military applications.
2. **Remote Controls:** Used in devices like TV remotes, IR-based remote controls communicate commands via infrared signals.
3. **Security Systems:** Infrared motion detectors and sensors are used in security systems for intrusion detection.
4. **Medical Applications:** Infrared radiation is used in physiotherapy for pain relief and healing, as well as in medical imaging techniques like infrared spectroscopy.
5. **Consumer Electronics:** Infrared technology is integrated into various consumer electronics for data transmission, such as printers, smartphones, and some gaming devices.

Infrared waves offer unique advantages in terms of safety, remote sensing, and heating applications. However, their limitations regarding range, penetration, and line of sight requirements influence their suitability for specific applications and necessitate consideration of these factors during implementation.

You
global positioning system

ChatGPT
ChatGPT

The Global Positioning System (GPS) is a satellite-based navigation system that provides location and time information anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

Key Components of GPS:

1. **Satellite Constellation:** The GPS constellation consists of multiple satellites orbiting the Earth, continually transmitting signals containing precise timing and positioning data.
2. **Ground Control Stations:** These stations manage and monitor the satellite constellation, ensuring accurate positioning information and maintaining the system's integrity.
3. **User Devices:** GPS receivers, found in various devices like smartphones, cars, aircraft, and wearables, receive signals from the satellites and calculate their positions on Earth based on the time it takes for signals to reach them from multiple satellites.

How GPS Works:

- At least four GPS satellites are needed to determine a receiver's three-dimensional position (latitude, longitude, and altitude) and time. Each satellite broadcasts signals containing its location and the precise time the signal was transmitted.
- The GPS receiver determines its distance from each satellite by measuring the time it takes for the signals to reach the receiver.
- Using trilateration (a mathematical method that measures distances), the receiver uses the signals from multiple satellites to calculate its own position and time.

Applications of GPS:

1. **Navigation and Mapping:** GPS is extensively used for navigation in vehicles, ships, aircraft, and for outdoor activities like hiking and geocaching. It's integral to creating accurate maps and routing systems.
2. **Time Synchronization:** GPS provides highly accurate time signals, used in various applications requiring precise timing, such as telecommunications, banking, and scientific research.
3. **Surveying and Geodesy:** In surveying and geodesy, GPS is used to determine precise positions and elevations for mapping, construction, and land management.
4. **Emergency Services:** It assists emergency services in locating individuals in distress, providing precise coordinates for search and rescue operations.
5. **Military and Defense:** Originally developed for military use, GPS remains vital for military navigation, reconnaissance, and targeting.

GPS has become an integral part of modern life, offering accurate positioning and timing information for a wide array of applications across industries and everyday activities. Additionally, advancements in GPS technology continue to expand its capabilities, making it more accurate, accessible, and versatile.

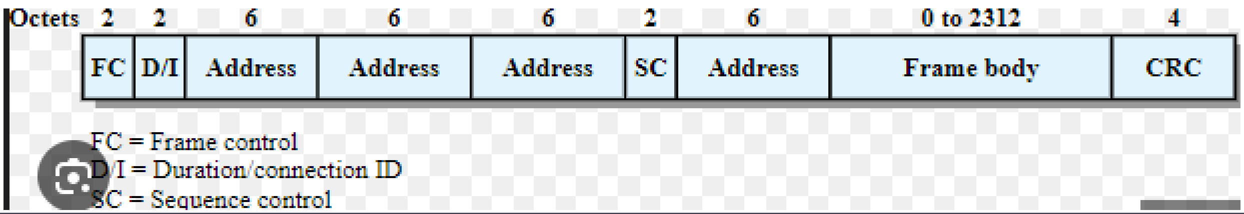
S.NO	Bridge	Router
1.	Bridge works in data link layer.	While Router works in network layer.
2.	Through bridge, data or information is not store and sent in the form of packet.	While through router, data or information is store and sent in the form of packet.
3.	There are only two ports in bridge.	While there are more than two ports in router.
4.	Bridge connects two different LANs.	While router is used by LAN as well as MAN for connection.
5.	In bridge, routing table is not used.	While in routers, routing table is used.
6.	Bridge works on single broadcast domain.	While router works on more than single broadcast domain.
7.	Bridges are easy to configure.	While Routers are difficult to setup and configure.
8.	Bridge focuses on MAC address .	While Router focuses on protocol address.
9.	Bridge is comparatively inexpensive.	While Router is relatively expensive device.
10.	Bridges are good for segment network and extends the existing network.	While Routers are good for joining remote networks.

Several congestion control protocols are used in computer networks to manage and mitigate congestion. Some notable ones include:

1. **Transmission Control Protocol (TCP) Congestion Control:**
    - TCP includes various congestion control algorithms like Slow-Start, Congestion Avoidance, Fast Recovery, and Fast Retransmit.
    - Slow-Start gradually increases the sending rate until congestion is detected.
    - Congestion Avoidance reduces the sending rate upon congestion detection and gradually increases it.
    - Fast Recovery and Fast Retransmit help recover from packet loss without waiting for a timeout.
2. **Explicit Congestion Notification (ECN):**
    - ECN allows routers to mark packets instead of dropping them when congestion is detected.
    - Routers and endpoints use ECN to signal congestion, allowing for more nuanced congestion control without immediate packet loss.
3. **Random Early Detection (RED):**
    - RED randomly drops or marks packets before the network becomes heavily congested.
    - It aims to prevent congestion collapse by reducing the transmission rate before severe congestion occurs.
4. **Forward Explicit Congestion Notification (FECN) and Backward Explicit Congestion Notification (BECN) in Frame Relay:**
    - These protocols provide explicit notification of congestion in Frame Relay networks.
    - FECN signals congestion at the forward direction, while BECN signals it backward toward the source.
5. **Resource Reservation Protocol (RSVP):**
    - RSVP allows hosts to request specific qualities of service (QoS) from the network for data flows.
    - It sets up and maintains reservations in routers to ensure adequate resources for certain traffic flows.
6. **Controlled Delay (CoDel) and Active Queue Management (AQM):**
    - CoDel and various AQM algorithms like CoDel and PIE (Proportional Integral controller Enhanced) aim to maintain low queuing delays and reduce bufferbloat by managing queue lengths and dropping packets before buffers become full.
7. **Bufferbloat Mitigation with FQ-CoDel:**

- Fair Queuing Controlled Delay (FQ-CoDel) combines fair queuing with CoDel to manage congestion and reduce latency in modern networking environments.

These congestion control protocols and algorithms are designed to ensure efficient network operation, prevent congestion collapse, manage traffic flow, and maintain network stability and performance under varying conditions. Each protocol or algorithm may be suited to specific network types or scenarios.



he field format for a wireless LAN (Local Area Network) frame typically follows the IEEE 802.11 standard, which defines the specifications for wireless communication. A basic frame structure in a Wi-Fi network includes several key fields:

1. **Frame Control Field:** This field contains various subfields specifying the frame type, duration, addressing, and control information.
2. **Duration/ID Field:** Indicates the duration of time required for transmission of the frame and is used by the receiver to reserve the medium for a specific duration.
3. **Address Fields:** Includes the MAC (Media Access Control) addresses of both the source and destination devices.
4. **Sequence Control Field:** Manages frame sequencing and fragmentation control for large frames.
5. **Frame Body:** Contains the actual data being transmitted (e.g., IP packets, TCP segments).
6. **Frame Check Sequence (FCS):** A checksum field used for error detection. It ensures the integrity of the data by allowing the receiver to verify if the frame was received without errors.
7. **Header Fields:** Depending on the frame type (e.g., management, control, data), additional fields may be included for specific purposes, such as QoS (Quality of Service) control, encryption, fragmentation, or reassembly.

The frame structure might vary depending on the specific IEEE 802.11 standard, such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, or 802.11ax (Wi-Fi 6 and Wi-Fi 6E), each introducing enhancements and modifications to the field format to accommodate higher speeds, improved efficiency, and additional features.

These fields collectively form the structure of a wireless LAN frame, facilitating the exchange of data between devices in a Wi-Fi network.

Answer:

13.53 percent

Explanation:

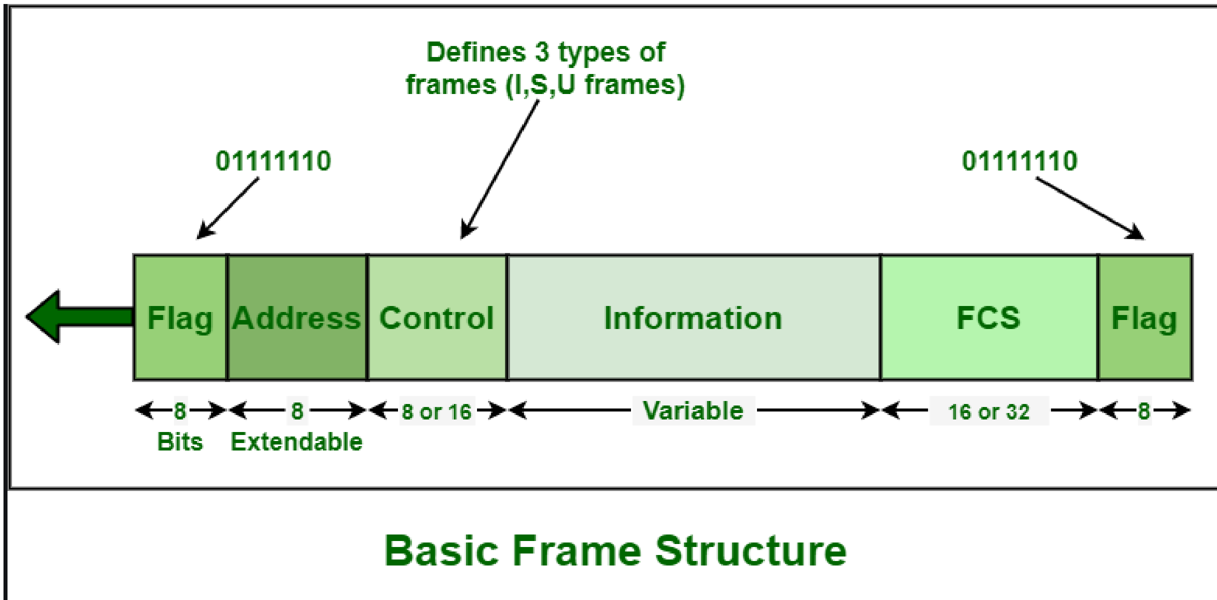
We can first calculate Tfr and G, and then the throughput. Tfr = (1000 bits) / 1 Mbps = 1 ms

G = ns × nfs × Tfr = 100 × 10 × 1 ms = 1

For pure ALOHA → S = G × e−2G ≈ 13.53 percent.

This means that each station can successfully send only 1.35 frames per second.

High-Level Data Link Control (HDLC) generally uses term “frame” to indicate and represent an entity of data or a protocol of data unit often transmitted or transferred from one station to another station. Each and every frame on link should begin and end with Flag Sequence Field (F). Each of frames in HDLC includes mainly six fields. It begins with a flag field, an address field, a control field, an information field, an frame check sequence (FCS) field, and an ending flag field. The ending flag field of one frame can serve as beginning flag field of the next frame in multiple-frame transmissions.
The basic frame structure of HDLC protocol is shown below :



Size of Different Fields :

Field Name	Size (bits)
Flag Field	8 bits
Address Field	8 bits
Control Field	8 or 16 bits
Information Field	Variable (not used in some type of HDLC frames)
FCS (Frame Check Sequence) Field	16 or 32 bits
Closing Flag Field	8 bits

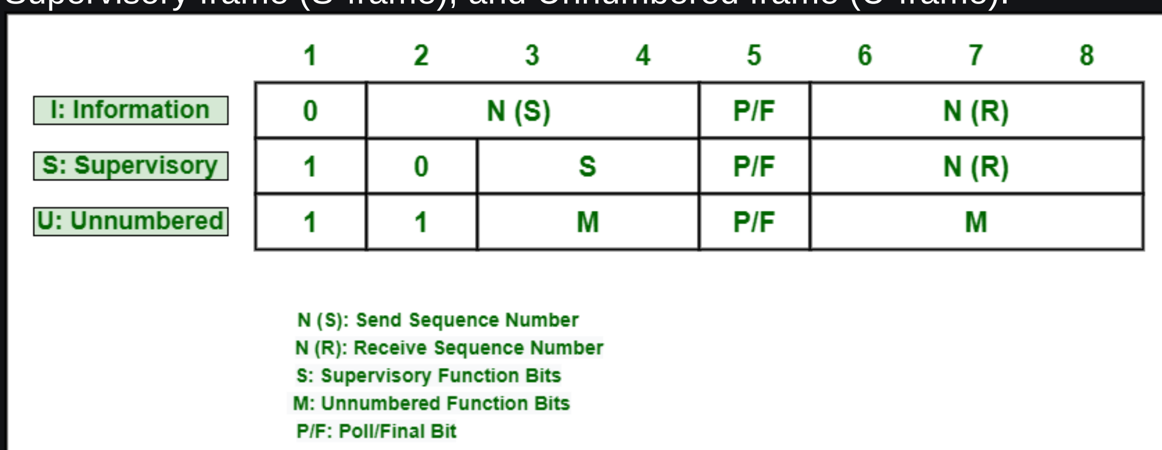
Let us understand these fields in details :

1. **Flag Field –**
   The flag field is generally responsible for initiation and termination of error checking. In HDLC protocol, there is no start and stop bits. So, the flag field is basically using delimiter 0x7e to simply indicate beginning and end of frame.

It is an 8-bit sequence with a bit pattern 01111110 that basically helps in identifying both starting and end of a frame. This bit pattern also serves as a synchronization pattern for receiver. This bit pattern is also not allowed to occur anywhere else inside a complete frame.

2. **Address Field –**
The address field generally includes HDLC address of secondary station. It helps to identify secondary station will sent or receive data frame. This field also generally consists of 8 bits therefore it is capable of addressing 256 addresses. This field can be of 1 byte or several bytes long, it depends upon requirements of network. Each byte can identify up to 128 stations.
This address might include a particular address, a group address, or a broadcast address. A primary address can either be a source of communication or a destination that eliminates requirement of including address of primary.

3. **Control Field –**
HDLC generally uses this field to determine how to control process of communication. The control field is different for different types of frames in HDLC protocol. The types of frames can be Information frame (I-frame), Supervisory frame (S-frame), and Unnumbered frame (U-frame).



	1	2	3	4	5	6	7	8
I: Information	0	N (S)			P/F	N (R)		
S: Supervisory	1	0	S		P/F	N (R)		
U: Unnumbered	1	1	M		P/F	M		

N (S): Send Sequence Number
N (R): Receive Sequence Number
S: Supervisory Function Bits
M: Unnumbered Function Bits
P/F: Poll/Final Bit

Control Field Format

This field is a 1-2-byte segment of frame generally requires for flow and error control. This field basically consists of 8 bits but it can be extended to 16 bits. In this field, interpretation of bits usually depends upon the type of frame.

4. **Information Field –**
   This field usually contains data or information of users sender is transmitting to receiver in an I-frame and network layer or management information in U-frame. It also consists of user’s data and is fully transparent. The length of this field might vary from one network to another network.
   Information field is not always present in an HDLC frame.

5. **Frame Check Sequence (FCS) –**
   FCS is generally used for identification of errors i.e., HDLC error detection. In FCS, CRC16 (16-bit Cyclic Redundancy Check) or CRC32 (32-bit Cyclic Redundancy Check) code is basically used for error detection. CRC calculation is done again in receiver. If somehow result differs even slightly from value in original frame, an error is assumed.

   This field can either contain 2 byte or 4 bytes. This field is a total 16 bit that is required for error detection in address field, control field, and information field. FCS is basically calculated by sender and receiver both of a data frame. FCS is used to confirm and ensure that data frame was not corrupted by medium that is used to transfer frame from sender to receiver.

$T_t = 1\mu s$

And for max efficiency, $G = \frac{1}{2}$

So,

$$\frac{1}{2} = \frac{\text{frames}}{T_f}$$

$$\text{frames} = 5 \times 10^5 \,/\text{sec}$$

This means that 5×10^5 frames must be produced each second to achieve maximum efficiency.

And,

There are 100 stations.

So,

Each station has to produce $= \frac{5 \times 10^5}{100} = 5 \times 10^3$

$= 5000$ frames/sec

Parameter	Narrowband	Broadband
Transmit power efficiency	High	Low
Frequency accuracy	Good	Even better than narrowband
Noise and interference	Affects the signals	Low noise and not an issue
Infrastructure	Good, as the narrowband is used for short-range communication	Infrastructure to be established widely
Bandwidth efficiency	Very high	Low
Range	Short	Long
Data transfer rate	Low	High
Coverage	Narrow coverage	Wide coverage
Security	Highly secured	Highly secured
Environmental penetration	High penetration	Low penetration

Aspect	ISDN	Broadband
Technology	Uses existing copper telephone lines	Utilizes various technologies (DSL, cable, fiber-optics, wireless)
Speed	Relatively lower speeds (up to 128 Kbps or 2 Mbps)	Offers significantly higher speeds (from Mbps to gigabit speeds)
Functionality	Simultaneous voice, data, and video transmission	Primarily high-speed internet access
Usage	Used as a dedicated digital service for businesses and some households	Standard internet connectivity for homes, businesses, industries
Deployment	Required specific ISDN-compatible hardware and infrastructure	Deploys various technologies for widespread availability
Connection	Dial-up connection, digital data and voice transmission	"Always-on" connection, high-speed internet access
Availability	Limited availability due to infrastructure constraints	More widespread availability