Mobile Computing refers a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device. It is free from having a connection with a fixed physical link. It facilitates the users to move from one physical location to another during communication.

Spread spectrum is a technique used for wireless communications in telecommunication and radio communication. In this technique, the frequency of the transmitted signal, i.e., an electrical signal, electromagnetic signal, or acoustic signal, is deliberately varied and generates a much greater bandwidth than the signal would have if its frequency were not varied.

Frequency Hopping Spread Spectrum (FHSS): Different carrier freq. are modulated by the source signal i.e. M carrier freq. are modulated by the signal. At one moment signal modulates one carrier frequency and at the subsequent moments, it modulates other carrier frequencies.

Direct Sequence Spread Spectrum (DSSS): The bandwidth of the original signal is also expanded by a different technique. Here, each data bit is replaced with n bits using a spreading code called chips, and the bit rate of the chip is called as chip-rate. The chip rate is n times the bit rate of the original signal.

Mobile Computing Application

1. **Business:** Business Owner can access the keep track of all activities of their travelling employees, to keep databases consistent etc.
2. **Infotainment:** Mobile computing performs a major role to provide uninterrupted internet connection to digital devices for streaming media.
3. **Emergencies:**An ambulance with a high-quality wireless connection to a hospital can carry vital information about injured persons to the hospital from the scene of the accident and specialists can be consulted for an early diagnosis.

Mobile Computing Application

4. **Education**: Wireless communication and digital devices are the backbone for distance learning concept.
5. **Manage Personal Records :**Some mobile applications allows user to manage their personal records such as day to day activities, some useful notes, etc.
6. **Social Media :** Some mobile applications allows user to keep in touch with their friends and relatives by sending messages, images, audio and video clips.
7. **Transaction :**Some mobile applications allow the facility of transaction such as recharge mobile, pay bills etc.

Issues in mobile computing

5. **Network Issues:** discovery of the connection-service to destination and connection stability
6. **Interoperability issues:** the varying protocol standards
7. **Security constraints:** Not only can portable devices be stolen more easily, but the radio interface is also prone to the dangers of eavesdropping. Wireless access must always include encryption, authentication, and other security mechanisms that must be efficient and simple to use.

Issues in mobile computing

1. **Resource constraints**: Battery
2. **Interference**: Radio transmission cannot be protected against interference using shielding and result in higher loss rates for transmitted data or higher bit error rates respectively
3. **Bandwidth**: Although they are continuously increasing, transmission rates are still very low for wireless devices compared to desktop systems.
4. **Dynamic changes in communication environment**: variations in signal power within a region, thus link delays and connection losses.

Advantages of FHSS:

Synchronization is not greatly dependent on distance.

Processing Gain is higher than DSSS.

Disadvantages of FHSS:

The bandwidth of the FHSS system is too large (in GHz).

Complex and expensive Digital frequency synthesizers are required.

Advantages of DSSS:

The DSSS System combats the jamming most effectively.

The performance of DSSS in presence of noise is superior to FHSS.

Interference is minimized against the signals.

Disadvantages of DSSS:

Processing Gain is lower than DSSS.

Channel Bandwidth is less than FHSS.

Synchronization is affected by the variable distance between the transmitter and receiver.

Multiple access techniques is multiplexing technique used to allow a large number of mobile users to share the allocated spectrum in the most efficient manner.

FDMA	TDMA	CDMA
FDMA stands for Frequency Division Multiple Access.	TDMA stands for Time Division Multiple Access.	CDMA stands for Code Division Multiple Access.
In this, sharing of bandwidth among different stations takes place.	In this, only the sharing of time of satellite transponder takes place.	In this, there is sharing of both i.e. bandwidth and time among different stations takes place.
There is no need of any codeword.	There is no need of any codeword.	Codeword is necessary.
In this, there is only need of guard bands between the adjacent channels are necessary.	In this, guard time of the adjacent slots are necessary.	In this, both guard bands and guard time are necessary.
Synchronization is not required.	Synchronization is required.	Synchronization is not required.
The rate of data is low.	The rate of data is medium.	The rate of data is high.
Mode of data transfer is continuous signal.	Mode of data transfer is signal in bursts.	Mode of data transfer is digital signal.
It is little flexible.	It is moderate flexible.	It is highly flexible.

CSMA/CA	It is a form of CSMA that is used to avoid collisions on a shared channel.
	It is a collision avoidance protocol.
	CSMA/CA is used in the Ethernet 802.11 network.
	It is compatible with wireless networks.
	This is useful prior to collision detection on a network.
	The CSMA CA, on the other hand, waits until the channel is congested and does not recover after a collision.
	It reduces the possibility of a collision.
	The efficiency of CSMA CA is comparable to that of CSMA.
	It is less well-known than CSMA CD.
CSMA/CD	It is the CSMA type used to detect a collision on a shared channel.
	The collision detection methodology is what it is.
	CSMA/CD found in 802.3 Ethernet network cables.
	It is compatible with wired networks.
	This is effective after a network's collision detection.
	When a data packet clashes on a shared channel, the data frame is resent.
	It cuts down on recovery time.
	When compared to CSMA, CSMA CD has a higher efficiency.
	It is more widely used than the CSMA CA protocol.

CSMA/CD cannot be implemented in Wireless LAN because of following reasons:-

In CSMA/CD, if a collision is detected on the medium, end-devices would have to wait a random amount of time before they can start the retransmission process. But in wireless LAN, there is no way for the sender to detect collisions the same way CSMA/CD does in wired networks since the sender is only able to transmit and receive packets on the medium but is not able to sense data traversing that medium. Thus CSMA/CD cannot be implemented in Wireless LAN.

But CSMA/CA can be used in wireless LAN because CSMA/CA doesn't detect collisions but rather avoids them through the use of control message. The control message collide with another control message from another node, it means that the medium is not available for transmission and the back-off algorithm needs to be applied before attempting retransmission.

Techniques to expand the capacity ad coverage area of cellular systems:

Cell Splitting : It is process of subdividing a congested cell into smaller cells, each with its own base station and a corresponding reduction in antenna height and transmitter power. Cell splitting increases capacity of cellular system since it increases number of times that channels are reused, it preserves frequency reuse plan.

Sectoring: The technique for decreasing co-channel interference and thus increasing system capacity by using directional antennas is called sectoring. The factor by which the co-channel interference is reduced depends on the amount of sectoring used. Sectoring improves Signal to Interference ratio.

Microcell Zone Concept : This approach was presented by Lee to solve the problem of an increased load on the switching and control link elements of the mobile system due to sectoring. It is based on a microcell concept for 7 cell reuse. In this scheme, each of the three zone sites are connected to a single base station and share the same radio equipment. Multiple zones and a single base station make up a cell. As a mobile travels within the cell, it is served by the zone with the strongest signal.

A **hexagon** is a tessellating cell shape in that cells can be laid next to each other with no overlap; therefore, they can cover the entire geographical region without any gaps.

Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources.

A contention-based access protocol is a protocol where data packet collisions may occur. Eg: Aloha protocol. Carrier Sense Multiple Access (CSMA) Multiple Access with Collision Avoidance.

A MAC protocol is **contention-free** if messages do not collide during its execution. Contention- free MAC protocols are typically based on time division multiplexing access (TDMA) of the wireless medium.

Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse. Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.

Slow start prevents a network from becoming congested by regulating the amount of data that's sent over it. It negotiates the connection between a sender and receiver by defining the amount of data that can be transmitted with each packet, and slowly increases the amount of data until the network's capacity is reached.

Fast retransmit is an enhancement to TCP that reduces the time a sender waits before retransmitting a lost segment. A TCP sender normally uses a simple timer to recognize lost segments.

1. **MS :** MS stands for Mobile System. MS comprises user equipment and software needed for communication with a mobile network

2. **BTS :** BTS stands for Base Transceiver Station which facilitates wireless communication between user equipment and a network. Every tower has BTS.

3. **BSC :** BSC stands for Base Station Controller. BSC has multiple BTS. You can consider the BSC as a local exchange of your area which has multiple towers and multiple towers have BTS.

4. **MSC :** MSC stands for Mobile Switching Center. MSC is associated with communication switching functions such as call setup, call release and routing

VLR : VLR stands for Visitor Location Register. VLR is a database which contains the exact location of all mobile subscribers currently present in the service area of MSC. If you are going from one state to another state then your entry is marked into the database of VLR.

HLR : HLR stands for Home Location Register. HLR is a database containing pertinent data regarding subscribers authorized to use a GSM network.. If you purchase SIM card from in the HLR. HLR is like a home which contains all data like your ID proof, which plan you are taking, which caller tune you are using etc.

In cellular system, **frequency re use** is the ability to use the same frequencies repeatedly across a cellular system. As each cell uses radio frequencies only within its boundaries, the same frequencies can be reused in other cells not far away with a limited possibility of interference.

Cells using the same set of frequencies are called co channel cells, and the interference between signals from these cells is called **Co-Channel interference.**

System capacity is formally defined as the maximum of the product of the number of users per cell times the user spectral efficiency for a given maximum outage probability.

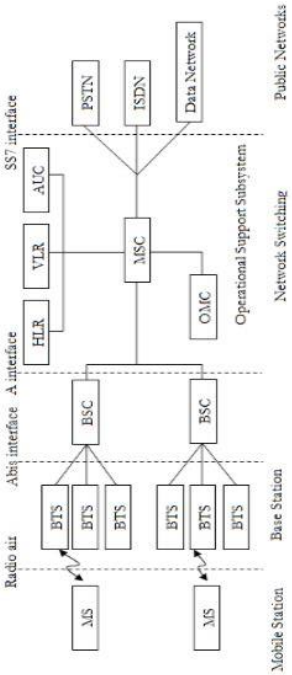


Fig: GSM Architecture

Mobility management in Global System for Mobile Communications **(GSM)** is used to trace physical user and subscriber locations to provide mobile phone services, like calls and Short Message Service (SMS).UMTS and GSM are each made up of separate cells (base stations) that cover a specific geographical area. All base stations are integrated into one area, allowing a cellular network to cover a wider area (location area).The location update procedure allows a mobile device to notify a cellular network when shifting between areas. When a mobile device recognizes that an area code differs from a previous update, the mobile device executes a location update, by sending a location request to its network, prior location and specific Temporary Mobile Subscriber Identity (TMSI).

Handoff is the process of transferring an active call or data session from one cell in a cellular network or from one channel to another. In satellite communications, it is the process of transferring control from one earth station to another. Handoff is necessary for preventing loss of interruption of service to a caller or a data session user.

Hard Handoff – An actual break in the connection occurs while switching from one cell to another. The radio links from the mobile station to the existing cell is broken before establishing a link with the next cell. It is generally an inter-frequency handoff. It is a "break before make" policy.

Soft Handoff – At least one of the links is kept when radio links are added and removed to the mobile station. This ensures that during the handoff, no break occurs. This is generally adopted in co-located sites. It is a "make before break" policy.

GSM has defined three different categories of services :

1. Telephony (also referred as tele-services) Services: Voice calls, video, sms, location
2. Data (also referred as bearer services) Services.
3. Supplementary Services: Call waiting, call hold, call forwarding, conferencing, Barring of Outgoing Calls, Barring of Incoming Calls, Multiparty service.

A mobile device provides updated network location information for several reasons, including reselecting cell location coverage due to a faded signal.

Location area includes a group of base stations assembled collectively to optimize signaling. Base stations are integrated to form a single network area known as a base station controller (BSC). The BSC manages allocation of radio channels, acquires measurements from cell phones, and handles handovers from one base station to another.

Roaming is among the basic procedures of mobility management. It enables subscribers to use mobile services when moving outside of the geographical area of a specific network.

Serial No.	GSM	CDMA
1. Signal Detection	GSM signals can be detected since they are focused in a narrow bandwidth.	CDMA transmissions are difficult to detect.
2. Technology used	FDMA(Frequency Division Multiple Access) and TDMA (Time Division Multiple Access).	CDMA(Code Division Multiple Access).
3. Availability	GSM is globally widely used and available.	CDMA is available in fewer countries and carriers.
4. Data speed rate	42Mbps in HSPA (3G).	3.6Mbps in CDMA.
5.Features	GSM supports transmitting data and voice both at once.	CDMA does not support this feature.
6. Customer Information	Stored in a SIM card.	Stored in a headset or phone.

Advantage of soft handoff is that the chances of call termination due to handoff failure are very less.Soft handoff is some what complex and technical implementation is expensive compared to hard handoff.

Disadvantage of soft handoff is that it uses a number of channels for just a single mobile station.Thus the number of free available channels are reduced which further reduce the capacity of the system.

Advantage of hard handoff is that the mobile user uses only channel at a given time. Also hard handover are cheaper and simpler because the mobile station does not need to be capable of receiving two or more channels.

Disadvantage of hard handoff is that if the handover fails then call may be temporarily disrupted or even terminated sometimes.

The uplink (mobile station to BTS) uses the frequencies between 890 MHz and 915 MHz and **the downlink** (BTS to mobile station) uses the frequencies between 935 MHz and 960 MHz. The duplex spacing, the spacing between the uplink and downlink channel, is 45 MHz.

Encapsulation is a network protocol technique where one IP packet consisting of packet header and data, often known as the inner packet, is inserted within another IP packet called the outer or tunneling packet. The main goals of this technique are to connect various network segments via a secure communication channel and to safely transport data through untrusted networks.

Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. It takes place to forward an IP datagram from the home agent to the care-of-address. Whenever the home agent receives a packet from the correspondent node, it encapsulates the packet with source address as home address and destination as care-of-address.

Security Issues in Mobile IP

Authentication and Authorization: Without proper authentication, unauthorized devices may gain access to the network, leading to security breaches.

Privacy Concerns: Mobile IP reveals the home network address of the mobile device, which can be a privacy concern. If this information falls into the wrong hands, it could be exploited for various malicious activities.

DoS Attacks : Attackers can flood the network with a high volume of packets, exhausting network resources and rendering the service unavailable to legitimate users.

Security Issues in Mobile IP

Spoofing and Man-in-the-Middle Attacks: Mobile IP relies on IP address information to route packets to mobile devices. This makes it vulnerable to IP spoofing attacks, where an attacker impersonates a legitimate mobile device by using its IP address.

Home Agent Vulnerabilities: The home agent, which serves as the anchor point for a mobile device's home network, can be a single point of failure and a potential target for attacks.

Location Tracking: Mobile IP reveals the current location of a mobile device, which can be a privacy concern for users

Multiple-Input Multiple-Output (MIMO) is a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time.

MIMO is often used for high-bandwidth communications where it's important to not have interference from microwave or RF systems.

The Care- of- address defines the current location of the mobile node from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the mobile node is done using a tunnel.

A **wireless LAN (WLAN)** is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building.

Bluetooth	IrDA
Point to multi-point	Point to Point
Data and voice	Data only
Omnidirectional antenna	Line-of-Sight
Devices can be Mobile	Both devices are Stationary
Range (upto 100m)	1m(range)

Network Architecture is the most universal, high-level, and persistent elements of structure and organization(or principles of structuring and organizing a complex system).**Network Protocols** define how diverse modules interact, and architecture defines how sets of protocols are organized. Architecture usually involves specification of protocols (rules of interaction) more than modules (which obey protocols). In engineering, system architecture must facilitate system level functionality as well as robustness and evolvability to uncertainty and change in components, function, and environment.

A mobile ad hoc network (**MANET**) is a collection of mobile nodes that act as both routers and hosts in an ad hoc wireless network and that dynamically self-organize in a wireless network without using any pre-established infrastructure. Nodes typically transmit in broadcast messages that reach only nearby nodes.

Home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist.

Foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN. Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

Co-located COA: The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the mobile node. Co-located address can be acquired using services such as DHCP. One problem associated with this approach is need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

Soft Hand-off	Soft hand-off is defined as a hand-off where a new connection is established before old one is released	It allocates same frequency	Soft hand-off used in CDMA and some TDMA systems	More complex than hard hand-off	Communicate up to three or four radio link at the same time
Hard Hand-off	The definition of a hard-hand off is one where an existing connection must be broken when the new one is established	It allocates Different frequency	Hard hand-off typically used in TDMA and FDMA	Hard hand-off is not very complicated	In hard hand-off handset always communicated with one BS at a time

Reverse tunneling is a tunneling from mobile host to home agent, and makes it possible for the mobile host from foreign network to communication in the network whose router has access filters.

The home agent encapsulates the correspondent host's packets and correctly forwards them to the mobile host. The mobile host's replies will however fail to reach the CH if it uses the home address as the source address due to ingress filtering at the CH. To avoid this problem, the MH should use reverse tunneling to send replies to CH. This is called **Bidirectional tunneling**.

In a **standard distance vector routing algorithm**, routers exchange their routing tables periodically with their neighboring routers. Each router calculates the best path to each destination based on the information received from its neighbors and updates its own routing table accordingly. The routing decision is typically based on the shortest path or the least cost metric, such as hop count or link bandwidth.

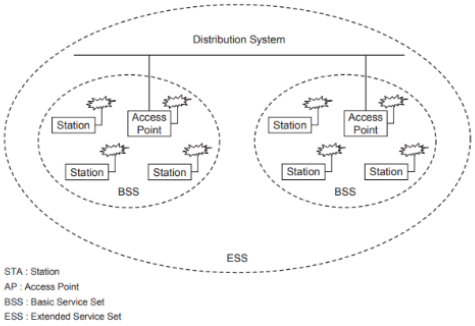
The destination sequence distance vector routing algorithm maintains routing tables at each mobile node, similar to the standard distance vector algorithm. However, DSDV introduces a sequence number for each destination entry in the routing table. The sequence number is used to track the freshness of routing information and to determine the most recent routing update for a particular destination.

Illustrate the system architecture of IEEE 802.11 WLAN

The IEEE 802.11 WLAN system architecture is divided into two layers: the physical layer (PHY) and the data link layer (DLL). The PHY layer is responsible for the transmission and reception of data over the air, while the DLL layer provides services for reliable data delivery.

The PHY layer is further subdivided into two sublayers: the physical medium dependent (PMD) sublayer and the medium access control (MAC) sublayer. The PMD sublayer is responsible for the physical implementation of the wireless medium, such as modulation and coding. The MAC sublayer is responsible for managing access to the shared wireless medium.

The DLL layer is further subdivided into two sublayers: the logical link control (LLC) sublayer and the service data unit (SDU) sublayer. The LLC sublayer provides services for reliable data delivery, such as error detection and correction. The SDU sublayer is responsible for encapsulating data from the upper layers into frames that can be transmitted over the wireless medium.



Here is a brief overview of the management functions in the IEEE 802.11 protocol architecture:

1. Association: A station associates with an access point to join a BSS.
2. Reassociation: A station reassociates with an access point to change the BSS it is associated with.
3. Disassociation: A station disassociates from an access point to leave a BSS.
4. Authentication: A station authenticates with an access point to prove its identity.
5. Deauthentication: An access point deauthenticates a station to revoke its access to the BSS.
6. Power management: Stations can enter a low-power mode to conserve energy when they are not actively transmitting or receiving data.
7. QoS: The IEEE 802.11 standard defines a number of quality of service (QoS) mechanisms to ensure that data is delivered in a timely and reliable manner.

The IEEE 802.11 protocol architecture provides a comprehensive set of features for managing wireless networks. These features can be used to ensure the reliable and efficient operation of wireless networks.

What are the different functions of L2CAP layer of Bluetooth?

The L2CAP layer of Bluetooth provides the following functions:

1. Protocol multiplexing: L2CAP allows multiple higher-layer protocols to coexist on the same Bluetooth link. This is done by assigning each protocol a unique channel identifier (CID).
2. Segmentation and reassembly: L2CAP segments large data packets from higher-layer protocols into smaller packets that can be transmitted over the Bluetooth link. The packets are reassembled at the receiving end.
3. Flow control: L2CAP provides flow control to prevent higher-layer protocols from sending data too quickly for the Bluetooth link to handle.
4. Quality of service (QoS): L2CAP can provide different levels of QoS to different higher-layer protocols. This allows applications that require real-time data delivery, such as voice and video, to get priority over applications that do not.

How does the data transfer occur between master and multiple slaves in the baseband layer of Bluetooth?

The data transfer between master and multiple slaves in the baseband layer of Bluetooth occurs using a technique called Time Division Duplex (TDD). In TDD, the master and slaves share the same frequency band, but they take turns transmitting and receiving data. The master is responsible for scheduling the transmissions.

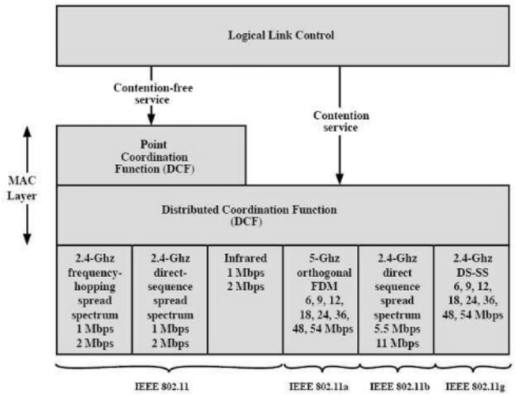
The baseband layer of Bluetooth divides each time slot into two equal parts: a master transmit part and a slave transmit part. The master transmits in the master transmit part, and the slaves transmit in the slave transmit part.

The master can transmit to any slave in any time slot. However, the slaves can only transmit to the master in the slave transmit part of the time slot that they are assigned.

The baseband layer of Bluetooth uses a technique called frequency hopping spread spectrum (FHSS) to improve the security and reliability of data transmission. FHSS involves rapidly changing the frequency of the Bluetooth signal over a wide range of frequencies. This makes it difficult for eavesdroppers to intercept the signal, and it also helps to reduce interference from other devices.

The baseband layer of Bluetooth is a complex and sophisticated protocol that is essential for the reliable and efficient transfer of data between Bluetooth devices.

Diagram of the IEEE 802.11 protocol architecture:



The IEEE 802.11 protocol architecture can be used to implement a variety of wireless networks, including:

1. Independent basic service set (IBSS): An IBSS is a wireless network that consists of a group of stations that communicate directly with one another without the use of an access point.
2. Basic service set (BSS): A BSS is a wireless network that consists of a single access point and a group of stations that communicate with the access point.
3. Extended service set (ESS): An ESS is a wireless network that consists of two or more BSSs that are connected together using a distribution system (DS). The DS can be a wired network, such as an Ethernet network, or a wireless network, such as another ESS.

What is the basic unit of networking in Bluetooth ?

A piconet is the basic unit of networking in Bluetooth. A piconet consists of one master device and up to seven active slave devices. The master device controls the communication within the piconet and schedules the time slots for each slave device to transmit data.

Briefly discuss the Bluetooth protocol stack.

The Bluetooth protocol stack is a set of protocols that define how Bluetooth devices communicate with each other. It is divided into four layers:

1. Physical layer: This layer is responsible for the physical transmission of data between Bluetooth devices. It uses radio waves to transmit data at a frequency of 2.4 GHz.
2. Data link layer: This layer is responsible for establishing and maintaining connections between Bluetooth devices. It also provides error detection and correction.
3. Logical link control and adaptation protocol (L2CAP): This layer provides a logical connection between Bluetooth devices. It allows multiple applications to share a single connection.
4. Application layer: This layer is responsible for providing services to applications. It includes protocols for file transfer, voice communication, and gaming.

Define WLAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building.

What you mean by adhoc piconet ?

An ad hoc piconet is a wireless network that is created on an ad hoc basis, meaning that it is not pre-planned. Ad hoc piconets are typically small, with only a few devices connected. They are often used for short-range communications, such as between a mobile phone and a headset or between a computer and a printer.

Mention the different criteria of WPAN.

Here are some of the criteria of WPAN:

1. Short range: WPANs are designed to operate over short ranges, typically less than 10 meters. This makes them ideal for use in personal and home environments.
2. Low power consumption: WPAN devices are designed to consume low power, which helps to extend their battery life. This is important for portable devices that are used on the go.
3. Low cost: WPAN devices are typically relatively inexpensive, which makes them accessible to a wide range of users.
4. Ease of use: WPAN devices are designed to be easy to use, which makes them ideal for users with limited technical expertise.
5. Security: WPAN devices can be secured using a variety of techniques, such as encryption and authentication. This helps to protect data from unauthorized access.

Discuss the advantages and limitations of Bluetooth as a wireless standard.

Bluetooth is a wireless technology that allows devices to communicate with each other over short distances. It is used in a wide variety of devices, including smartphones, tablets, laptops, and headsets.

Bluetooth has a number of advantages, including:

1. Ease of use: Bluetooth is easy to set up and use. There is no need to install drivers or configure settings.
2. Low power consumption: Bluetooth devices consume very little power, which helps to extend their battery life.
3. Security: Bluetooth devices can be secured using a variety of techniques, such as encryption and authentication.
4.

However, Bluetooth also has some limitations, including:

1. Short range: Bluetooth has a short range of up to 10 meters. This means that devices must be within close proximity of each other in order to communicate.
2. Low bandwidth: Bluetooth has a low bandwidth of up to 3 Mbps. This means that it is not suitable for applications that require high-speed data transfer, such as streaming video or audio.
3. Interference: Bluetooth can be susceptible to interference from other devices that use the same frequency band, such as microwaves and cordless phones.

What do you mean by satellite network.

A satellite network is a group of satellites that are used to provide a particular service. For example, the Globalstar satellite network is used to provide mobile phone communication. The Iridium satellite network is also used to provide mobile phone communication.

Discuss the IRIDIUM and GLOBAL STAR Satellite system.

The Iridium satellite network is a constellation of 66 satellites that are used to provide mobile phone communication around the world. The satellites are arranged in a polar orbit, which means that they pass over every point on Earth twice a day. This allows Iridium phones to make and receive calls from anywhere in the world, even in remote areas.

The Globalstar satellite network is a constellation of 48 satellites that are used to provide mobile phone communication around the world. The satellites are arranged in a low Earth orbit, which means that they are closer to Earth than Iridium satellites. This makes Globalstar phones more affordable than Iridium phones, but it also means that Globalstar phones have a shorter range.

Both the Iridium and Globalstar satellite networks are reliable and provide good quality of service. However, the Iridium network has a wider coverage area than the Globalstar network.

WAP 1.X architecture consists of the following components:

1. WAP Gateway: The WAP gateway is a server that acts as a bridge between the WAP network and the Internet. It converts WAP messages into HTTP messages, which can then be understood by web servers.
2. WAP Stack: The WAP stack is a software layer that is installed on the mobile device. It converts HTTP messages into WAP messages, which can then be understood by the WAP gateway.
3. WAP Browser: The WAP browser is a software application that is installed on the mobile device. It allows users to view WAP content.

WAP 1.X defines two interfaces:

1. User Agent Profile (UAProf): The UAProf is a file that is used to describe the capabilities of a WAP device. It includes information such as the device's screen size, supported markup languages, and supported protocols.
2. Wireless Markup Language (WML): WML is a markup language that is used to create WAP content. It is a simplified version of HTML, which is the markup language that is used to create web pages.

WML document modes

WML document modes are used to specify how WML documents should be displayed on different types of mobile devices. There are three WML document modes:

1. Card mode: Card mode is the default WML document mode. It displays WML documents as a series of cards. Each card can contain a different piece of information, such as a news article, a weather forecast, or a stock quote.
2. List mode: List mode displays WML documents as a list of items. Each item in the list can be clicked on to display more information about that item.
3. Form mode: Form mode is used to create interactive WML documents. Forms can be used to collect information from users, such as their name, address, or email address.

Parameters	BLUETOOTH	HIPERLAN-2
Application	Wireless network	Access to ATM fixed network
Frequency, Band	2.45GHz	5 GHz
Maximum Data rate	1 Mbps	54 Mbps
Topology	Ad-hoc	Cellular, centralized
Error control	Arq/fec mac layer	Arq/fec phy layer
Range	Upto 10m	50-100m
Interface	low	high
Medium Access methods	Master is responsible for medium	AP centralized
Connectivity	Connection less and Oriented	Connection oriented
QoS (Quality of Service)	Statistical	ATM /802.1p/RSVP
Frequency Selection	Frequency hopping	dynamic frequency selection (DSS)

Briefly explain different types of satellites.

There are many different types of satellites, each with its own unique purpose. Some of the most common types of satellites include:

1. Communication satellites: These satellites are used to transmit data and voice signals between different points on Earth. They are used for a variety of applications, including television broadcasting, internet access, and mobile phone communication.
2. Navigation satellites: These satellites are used to provide location information to GPS receivers. They are used for a variety of applications, including navigation, surveying, and mapping.
3. Earth observation satellites: These satellites are used to collect data about Earth's surface and atmosphere. They are used for a variety of applications, including weather forecasting, environmental monitoring, and disaster relief.
4. Scientific research satellites: These satellites are used to conduct scientific research about Earth, space, and the universe. They are used for a variety of applications, including studying climate change, tracking asteroids, and searching for exoplanets.

What is WAP? Why is it used?

WAP stands for Wireless Application Protocol. It is a set of communication protocols that allow users of mobile devices to access information and services on the Internet. WAP was developed by the Wireless Application Protocol Forum (WAPF), which is a group of companies that work together to develop and promote WAP standards.

WAP is used to access a variety of information and services on the Internet, including:

- Email
- Web browsing
- News
- Weather
- Stock quotes
- Games
- Entertainment

WAP is a convenient way for users of mobile devices to access information and services on the Internet. It is especially useful for users who are not always in a location where they have access to a wired internet connection.

WAP security

WAP security is a set of measures that are used to protect WAP data from unauthorized access. These measures include:

- Wireless Transport Layer Security (WTLS): WTLS is a security protocol that is used to encrypt WAP data as it is transmitted between the mobile device and the WAP gateway.
- User Authentication: User authentication is a process that is used to verify the identity of a user before they are allowed to access WAP services.
- Password Protection: Password protection can be used to protect WAP content from unauthorized access.

There are a number of different protocols that can be used in WLL networks. Some of the most common protocols include:

1. GSM: GSM is a cellular radio technology that is used in many parts of the world.
2. CDMA: CDMA is another cellular radio technology that is used in many parts of the world.
3. WiMAX: WiMAX is a wireless broadband technology that can be used to provide high-speed internet access to mobile devices.

WLL networks can provide a variety of services, including:

1. Internet access: WLL networks can provide high-speed internet access to mobile devices.
2. Voice calls: WLL networks can be used to make and receive voice calls.
3. Video calls: WLL networks can be used to make and receive video calls.
4. Data transfer: WLL networks can be used to transfer data between mobile devices and other devices, such as computers and printers.
5. Streaming media: WLL networks can be used to stream media content, such as music and video, to mobile devices.

Key	LAN	WLAN
Stands for	LAN stands for Local Area Network.	WLAN stands for Wireless Local Area Network.
Connection Type	LAN connections include wired as well as wireless connection technologies.	WLAN connections are completely based on wireless technology.
Cost	LAN connections are less expensive and more secure than the wireless connections of WLAN.	WLAN connections are more expensive and considered less secure than wired connections.
Complexity	It is relatively complex to set up a LAN. One needs to connect several network devices such as routers and switches with the help of Ethernet cables.	It is relatively simple to configure and set up a WLAN.
Performance	LANs provide good performance and the impact of weather is limited.	WLAN provides high performance but may get impacted in bad weather.
Mobility	A LAN has limited mobility. It needs Ethernet to connect devices.	WLAN is highly mobile in nature. No Ethernet is required to connect the devices to a WLAN.

What is HiperLAN? What are the four different versions of HiperLAN.

HIPERLAN stands for High Performance Radio LAN. It is a wireless LAN standard. It is a European alternative for the IEEE 802.11 standards (the IEEE is an international organization). It is defined by the European Telecommunications Standards Institute (ETSI). In ETSI the standards are defined by the BRAN project (Broadband Radio Access Networks).

The HiperLAN standard family has four different versions:

1. HIPERLAN/1: The first version of the standard was approved in 1997. It has a data rate of up to 23.5 Mbps.
2. HIPERLAN/2: The second version of the standard was approved in 2000. It has a data rate of up to 54 Mbps.
3. HIPERLAN/3: The third version of the standard was approved in 2005. It has a data rate of up to 100 Mbps.
4. HIPERLAN/4: The fourth and final version of the standard was approved in 2011. It has a data rate of up to 1 Gbps.

Type of wave	Data rate	Transmission distance	Interference	Cost
Radio waves	Low to high	Long	Low	Low
Microwaves	High	Medium	Medium	Medium
Infrared waves	Low	Short	High	Low

- As we can see, radio waves have the lowest data rates but the longest transmission distances. Microwaves have the highest data rates but the shortest transmission distances. Infrared waves have the lowest data rates and the shortest transmission distances.
- In terms of interference, radio waves are the least susceptible to interference. Microwaves are more susceptible to interference, and infrared waves are the most susceptible to interference.
- In terms of cost, radio waves are the least expensive. Microwaves are more expensive, and infrared waves are the most expensive.

What are the hidden station problem and exposed station problem? How the problem is solved?

>>> In wireless networks, a hidden station problem occurs when two stations that are within range of a common receiver are not within range of each other. This means that each station can hear the receiver, but not each other. As a result, it is possible for both stations to transmit at the same time, which can cause a collision.

>>> An exposed station problem occurs when a station is within range of a transmitting station, but not within range of any other stations that are also within range of the transmitting station. In this case, the exposed station could transmit data, but it chooses not to do so because it knows that its transmission would interfere with the transmission of the other station.

>>> There are a number of ways to solve the hidden station problem and the exposed station problem. One common solution is to use a protocol called Request to Send/Clear to Send (RTS/CTS). In RTS/CTS, a station that wants to transmit data sends an RTS frame to the intended receiver. The receiver then sends a CTS frame back to the sender, which grants permission to transmit. Any stations that hear the RTS frame know that they should not transmit data until the CTS frame has been sent.

Another solution to the hidden station problem is to use a protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In CSMA/CA, stations listen to the channel before transmitting data. If the channel is sensed to be idle, the station can transmit. If the channel is sensed to be busy, the station waits a random amount of time before trying again.

Advantages:(WLAN)

1. Mobility: WLANs allow users to move around freely while still being connected to the network.
2. Flexibility: WLANs can be easily expanded to accommodate new users or devices.
3. Cost-effectiveness: WLANs can be a cost-effective way to provide internet access to a large number of users.
4. Security: WLANs can be secured using a variety of methods, such as encryption and passwords.

Disadvantages:

1. Security: WLANs are more vulnerable to security attacks than wired networks.
2. Limited coverage: WLANs have a limited range, which means that users must be within a certain distance of the access point in order to connect to the network.
3. Interference: WLANs can be susceptible to interference from other devices that use radio waves, such as microwaves and cordless phones. This can cause signal degradation and dropped connections.
4. Bandwidth: WLANs can have limited bandwidth, which can slow down the transfer of data. This is especially a problem in areas with a lot of users.

The following are the values of the addresses in the 802.11 frames for the three transmissions:

Station A to AP1:

- Address 1: AP1
- Address 2: A
- Address 3: BSSID of BSS1

AP1 to AP2:

- Address 1: AP2
- Address 2: AP1
- Address 3: BSSID of BSS2
- Address 4: BSSID of BSS1

AP2 to station C:

- Address 1: C
- Address 2: AP2
- Address 3: BSSID of BSS2

The BSSID is the basic service set identifier, which is a unique identifier for each wireless network. The BSSID is used to distinguish between different wireless networks that may be overlapping in the same area.