CDMA vs. GSM | Difference between CDMA and GSM

Cellular mobile services have been used all over the world for a long time and still evolving day by day. With these services, various communication services also evolved, and **CDMA and GSM** are two of them. CDMA and GSM are the two most important technology standards that are known for mobile communication. Both the GSM and CDMA converts the data from the mobile phone into radio waves. *But these technologies are differentiated in the way in which the calls & data transfer takes place over a network*. One of the key differences between CDMA and GSM is that ***GSM uses SIM cards to connect a mobile phone with its network, whereas CDMA does not need any SIM card and operates on ESNs (Electronic Serial Number).*** In this topic, we will understand what GSM and CDMA technologies are and how they differentiate from each other in detail.

What is GSM?

- GSM or **Global System for Mobile Communication** is a digital mobile communication standard, which is used for transmitting and receiving data and voice signals over a network.
- It is also known as the **second-generation standard** for mobile networks or telecommunication, and it operates on a **wedge spectrum.**
- GSM uses the **TDMA** (Time Division Multiple Access) and **FDMA** (Frequency Division Multiple Access) for separating the users & cells and transmitting the signals.
- Due to the GSM standard, various other wireless services such as **GPRS(General Packet Radio Service), UMTS(Universal Mobile Radio System), and EDGE(Enhanced Data Rates for GSM Evolution) have also evolved.**
- It operates on three different radio frequencies, which are **900MHz, 1800MHz, and 1900MHz.**
- Among these three frequencies, the 900MHz band frequency is used by the Original GSM system, and the 1800 MHz band frequency is used to provide the added support for increasing customers. The 1900MHz band is specifically used in the US (United States).

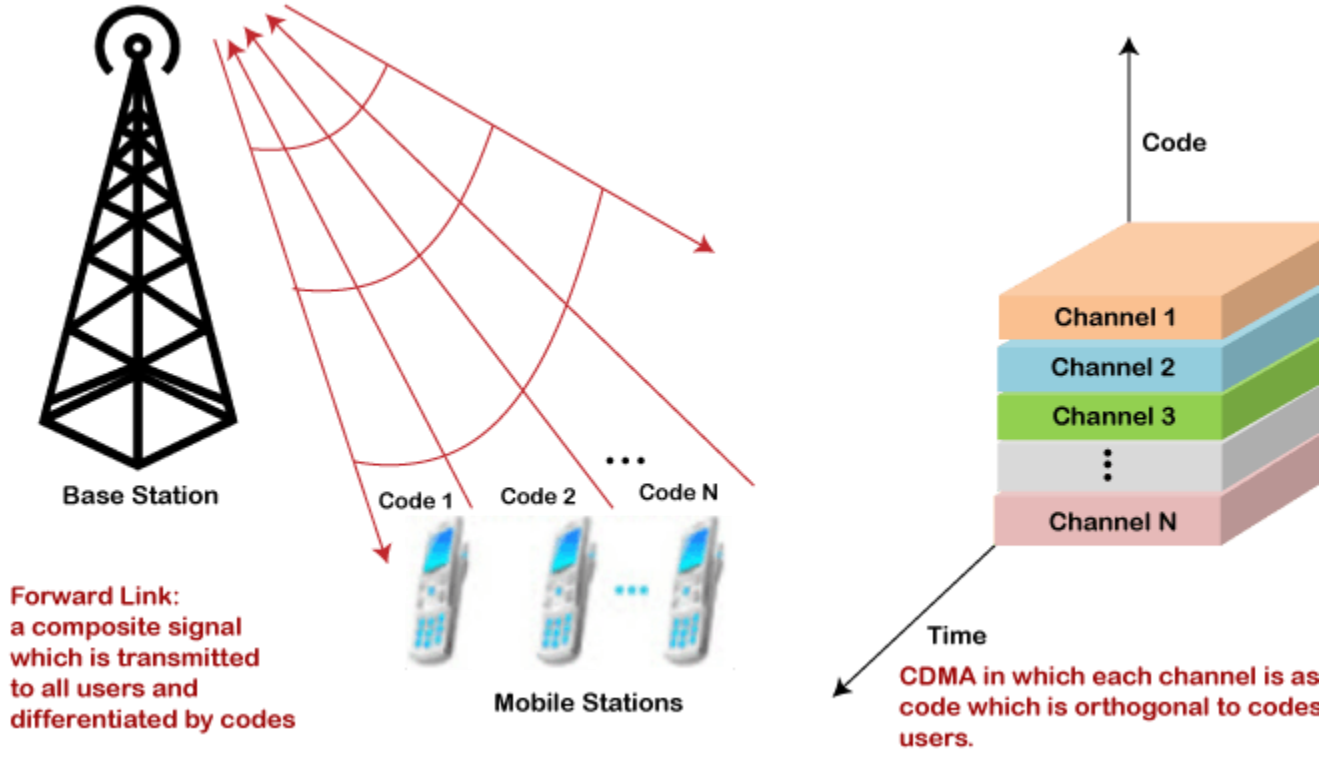
- The GSM users have first taken advantage of the **service Short Message System (SMS)**, by which the users can communicate with each other using text messages over the given network.

Advantages of GSM

- With GSM technology, we can have a low-cost mobile set and base stations.
- It improves spectrum efficiency.
- The data or voice signals are of high quality in GSM.
- The GSM is compatible with **ISDN** (Integrated Services Digital Network)

What is CDMA?

- CDMA is an acronym for **Code Division Multiple Access,** which is also a radio telecommunication standard similar to GSM.



- The CDMA came into existence in 2G and 3G generation as the protocol of wireless communication.

- It is based on the **spread spectrum technology** and makes optimal use of the available bandwidth. Since it uses the spread spectrum technology, hence allows each user to transmit the data over the entire frequency spectrum at any time.
- The CDMA provides one of the most secure modes of communication due to its spread spectrum property.
- It is used in **UHF or Ultra high-frequency cellular systems**, with frequency bands ranging from **800MHz to 1900MHz.**

Advantages of CDMA:

- It uses a fixed frequency spectrum in an efficient way.
- There is no limit on the number of Users.
- It provides a flexible allocation of resources.
- It is compatible with other cellular technologies; hence it allows nation-wide roaming.

Differences Between GSM and CDMA

1. Technology Used

The GSM is based on the wedge spectrum technology, also known as a carrier. This carrier is split into various time slots on the basis of TDMA technology, and each time slots are assigned to each user. Due to this, until one outgoing call is finished, no other user can access that slot. It uses FDMA to provide multiuser access by dividing the user frequencies.

On the other hand, CDMA uses the spread spectrum technology and hence it makes optimal use of the available bandwidth. It enables each user to transfer the data over the entire frequency spectrum at any time.

2. SIM Cards

SIM (Subscriber Identity Module) is a smart card that contains the user identification information to identify the subscriber on a telephony device. In a GSM-based phone, a SIM card is required to make the data or call transmission. These cards can be easily replaced from one mobile phone to another with saved information.

the other hand, CDMA based devices do not require a SIM card; instead, it uses ESN (Electronic Serial Number). Since it does not use a SIM card, hence changing a device from another is difficult and required a proper procedure.

3. Flexibility

The GSM standard is more flexible as compared to CDMA. It is because, in GSM, the SIM card can be inserted into any device and can be used. Whereas, CDMA mobile phone can only be used if ESN is registered in its database.

If a CDMA stops working on a phone, we need to buy the new phone, whereas if a SIM stops working, we can use another SIM rather than changing the phone.

4. Spectrum frequencies

The GSM works on the frequency spectrum ranging from **850 MHz to 1900 MHz**, whereas CDMA also operates in the frequency range of **850MHz and 1900MHz.**

5. Radiation Exposure

In GSM phones, there is **28 times more radiation exposure** takes place as compared to CDMA phones.

GSM phone continuously transmits wave pulses, whereas CDMA phones do not continuously produce such pulses.

6. Global Reach

GSM is more used globally as compared to CDMA technology. Approx. 80% of the mobile networks across 210 countries use GSM compared to CDMA. The CDMA-based mobile phones are mostly used in the US, Canada, and Japan.

7. Security

The CDMA provides more security as compared to GSM technology because it has inbuilt encryption and uses the spread spectrum for data transmission.

In CDMA, the signal detection is much difficult than in GSM. Hence it is more secure.

8. Data Transfer Rate

The data transfer rate is high in CDMA compared to GSM technology. In CDMA, **EVDO data transfer technology** is used, which provides a maximum download speed of **2 Mbps.**

On the other hand, GSM uses **EDGE data transfer technology** that provides a maximum download speed of 384 Kbps, which is much slower than CDMA.

How to check if the phone is based on GSM or CDMA technology?

To check if your mobile phone is GSM-based or CDMA based, check the below points:

1. Check from your Phone Settings:

- **For iPhone users:** Go to Settings→General→About→ check for the ***MEID, ESN, or IMEI number*** near the bottom of the menu.

Comparison Chart between CDMA and GSM

CDMA	GSM
It stands for Code Division Multiple Access.	It stands for Global System for Mobile Communication.
It uses a CDMA mechanism for data & call transmission.	It uses TDMA and FDMA mechanism for data & voice transmission.
The transmission rate is fast compared to GSM.	The transmission rate is slow compared to CDMA.
It uses EVDO data transfer technology.	It uses EDGE data transfer technology.
It is handset specific and does not require any	It is SIM specific, hence requires a SIM card for

SIM for communication.	communication.
During transmission, it is much prone to radiation emission.	During transmission, it is comparatively less prone to radiation emission.
It offers more secure communication compared to GSM.	It offers less secure communication compared to CDAM.
The signal detection is difficult in CDMA.	The signal detection is easy in GSM.
It provides built-in encryption.	It requires additional encryption as no built-in encryption is available.
It enables limited roaming.	It enables worldwide roaming.

- **For Android users:** Go to Settings→ System→About Phone→Click to Status, and check for the *MEID, ESN, or IMEI number.*

In both cases, if you see the MEID or ESN number, then your phone is CDMA based. If you see the IMEI number, then your phone is a GSM-based phone. If you see both options, it means your device supports both technologies.

2. Check for SIM card Slot on the Phone:

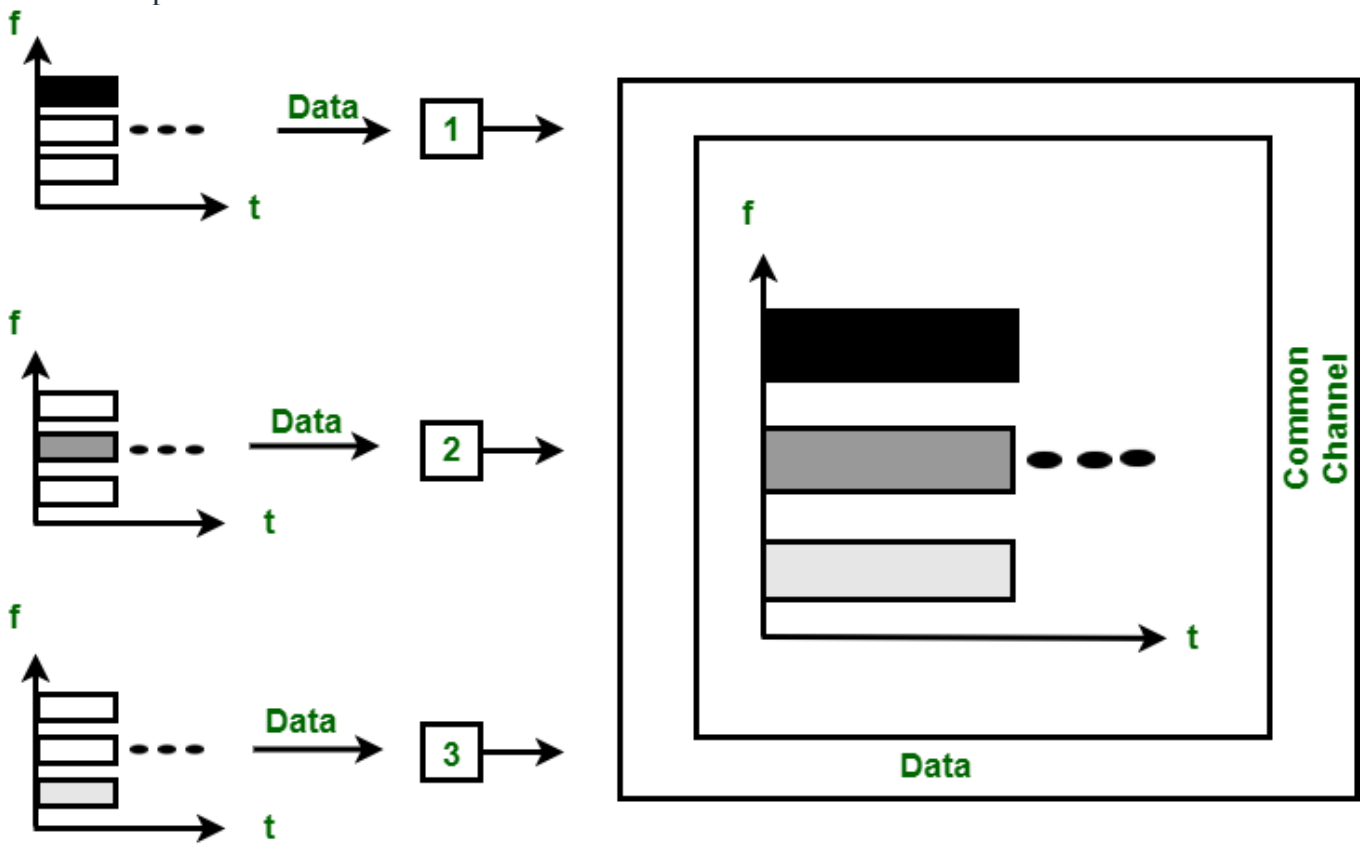
As discussed above, the GSM phone makes use of SIM cards, whereas CDMA not. So, you can check on your mobile phone whether it contains a SIM slot or not. But due to widely spread of 4G LTE technology, most CDMA devices also use SIM cards, so this way of checking is less helpful now.

Conclusion:

Both GSM and CDMA have their own importance and depends on how both technologies are being used. Approximately 80% of the world uses GSM, and CDMA is used mostly in the US and somewhere in Canada and Japan.

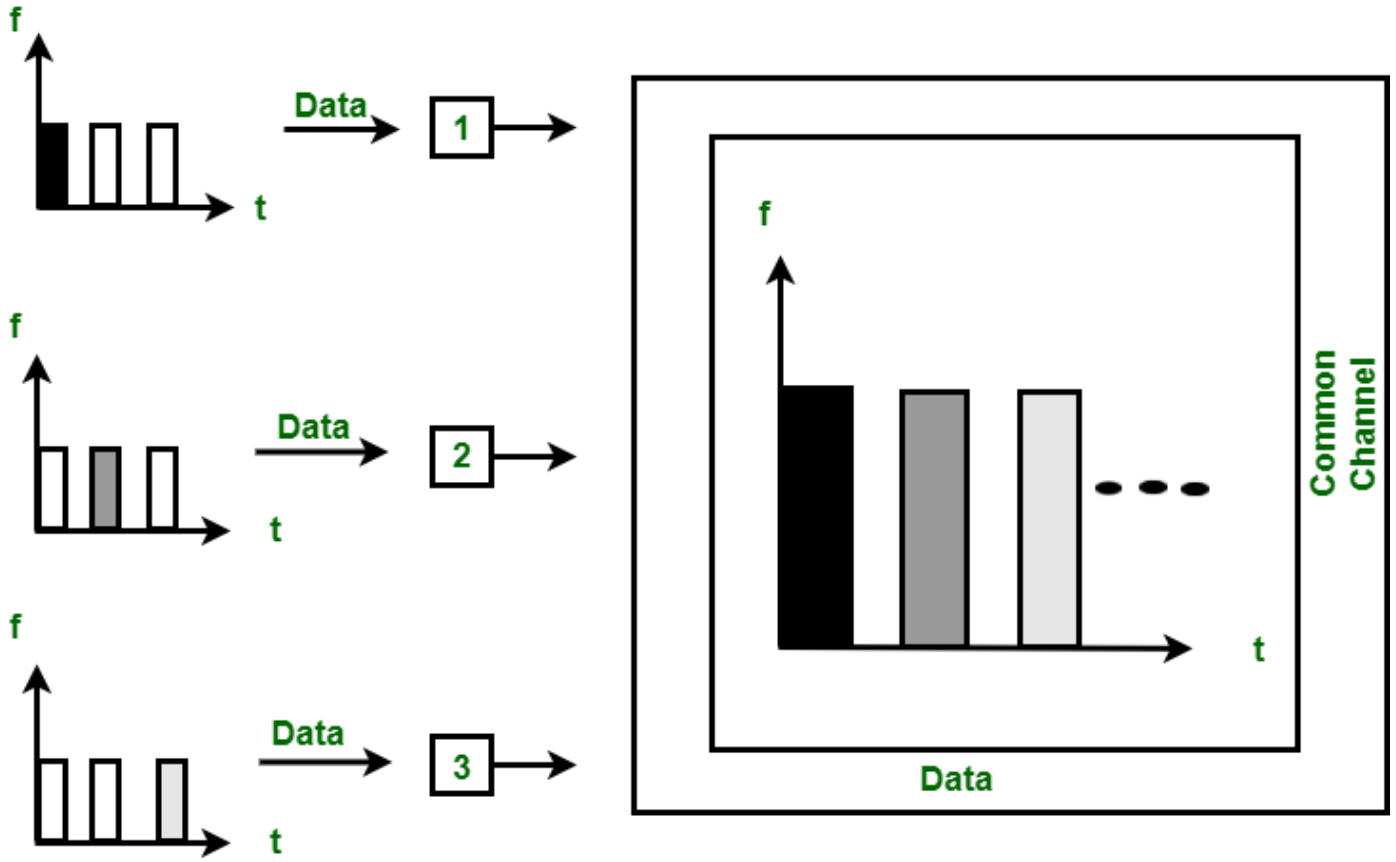
Difference between FDMA and TDMA

1. Frequency Division Multiple Access (FDMA) :
FDMA is the channelization protocol in which bandwidth is divided into various frequency bands. Each station is allocated with band to send data and that band is reserved for particular station for all the time which is as follows:



The frequency bands of different stations are separated by small band of unused frequency and that unused frequency bands are called as guard bands that prevent interference of stations. It is like access method in data link layer in which data link layer at each station tells its physical layer to make bandpass signal from data passed to it. The signal is created in allocated band and there is no physical multiplexer at physical layer.

2. Time Division Multiple Access (TDMA) :
TDMA is channelization protocol in which bandwidth of channel is divided into various stations on time basis. There is time slot given to each station, station can transmit data during that time slot only which is as follows:



Each station must aware of its beginning of time slot and location of the time slot. TDMA requires synchronization between different stations. It is type of access method in data link layer. At each station data link layer tells station to use allocated time slot.

Difference between FDMA and TDMA :

Sr. No.	FDMA	TDMA
1.	FDMA stands for Frequency Division Multiple Access.	TDMA stands for Time Division Multiple Access.
2.	Overall bandwidth is shared among number of stations.	Time sharing of satellite transponder takes place.
3.	Guard bands between adjacent channels is necessary.	Guard time between adjacent slots is necessary.

Sr. No.	FDMA	TDMA
4.	Synchronization is not required.	Synchronization is necessary.
5.	Power efficiency is less.	Power efficiency is high.
6.	It requires stability of high carrier efficiency.	It does not require stability of high carrier efficiency.
7.	It is basically used in GSM and PDC.	It is basically used in advanced mobile phone systems.

Wireless LAN overview

WLAN stands for **Wireless Local Area Network.** WLAN is a local area network that uses radio communication to provide mobility to the network users, while maintaining the connectivity to the wired network. A WLAN basically, extends wired local area network. WLAN's are built attaching a device called the access point(AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter which is similar in function to a ethernet adapter. It is also called a LAWN that is Local area wireless network.
The performance of WLAN is high compared to other wireless networks. The coverage of WLAN is within a campus or building or that tech parks. It is used in the mobile propagation of wired networks. The standards of WLAN are HiperLAN, Wi-Fi, and IEEE 802.11. It offers service to the desktop laptop, mobile application and all the devices works on the Internet. WLAN is an affordable method and can be set up in 24 hours. WLAN gives users the mobility to move around within a local coverage area and still be connected to the network. Most latest brands are based on IEE 802.11 standards, which are the WI-FI brand name.

History :
A professor at University of Hawaii who's name was Norman Abramson, developed the world's first wireless computer communication network. In 1979, Gfeller and u.Bapst published a paper in the IEE proceedings reporting an experimental wireless local area network using diffused infrared communications. The first of the IEEE workshops on Wireless LAN was held in 1991.
Characteristics :

- Seamless operation.

- Low power for battery use.
- Simple management, easy to use for everyone.
- Protection of investment in wired networks.
- Robust transmission technology

Advantages :

- Installation speed and simplicity.
- Installation flexibility.
- Reduced cost of ownership.
- Reliability.
- Mobility.
- Robustness.

Disadvantages :

- Slower bandwidth.
- Security for wireless LAN's is the prime concern.
- Less capacity.
- Wireless networks cost four times more than wired network cards.
- Wireless devices emit low levels of RF which can be harmful to our health.

What is Bluetooth?

Bluetooth simply follows the principle of transmitting and receiving data using radio waves. It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

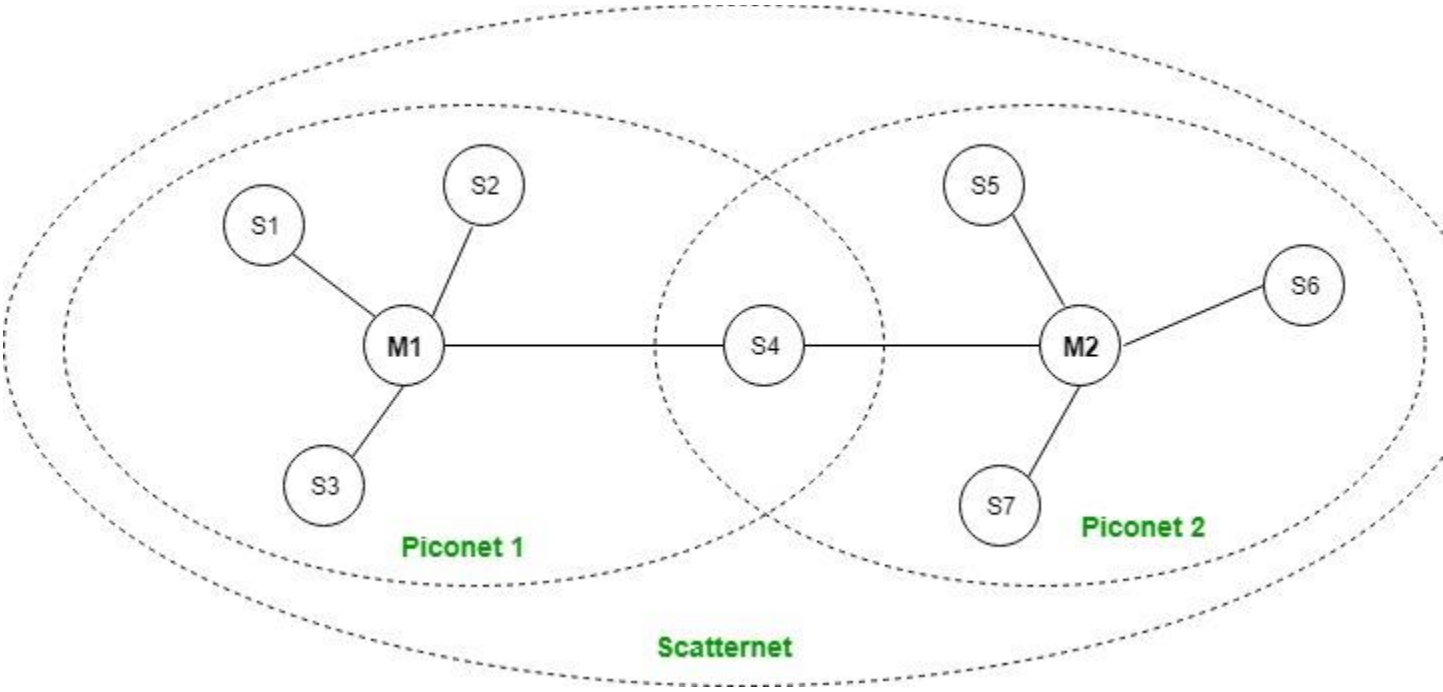
Points to remember for Bluetooth:

- Bluetooth Transmission capacity 720 kbps.
- Bluetooth is Wireless.
- Bluetooth is a Low-cost short-distance radio communications standard.
- Bluetooth is robust and flexible.
- Bluetooth is cable replacement technology that can be used to connect almost any device to any other device.
- The basic architecture unit of Bluetooth is a piconet.

Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1. Piconet
2. Scatternet



Piconet:

Piconet is a type of Bluetooth network that contains **one primary node** called the master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet:

It is formed by using **various piconets**. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

Types of Bluetooth

Various types of Bluetooth are available in the market nowadays. Let us look at them.

- In-Car Headset: One can make calls from the car speaker system without the use of mobile phones.
- Stereo Headset: To listen to music in car or in music players at home.
- Webcam: One can link the camera with the help of Bluetooth with their laptop or phone.
- Bluetooth-equipped Printer: The printer can be used when connected via Bluetooth with mobile phone or laptop.
- Bluetooth Global Positioning System (GPS): To use GPS in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

Advantage:

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.

Applications:

- It can be used in laptops, and in wireless PCs, printers.
- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wirelessly to a mobile phone.
- It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
- It is used in the sectors of Medical health care, sports and fitness, Military.

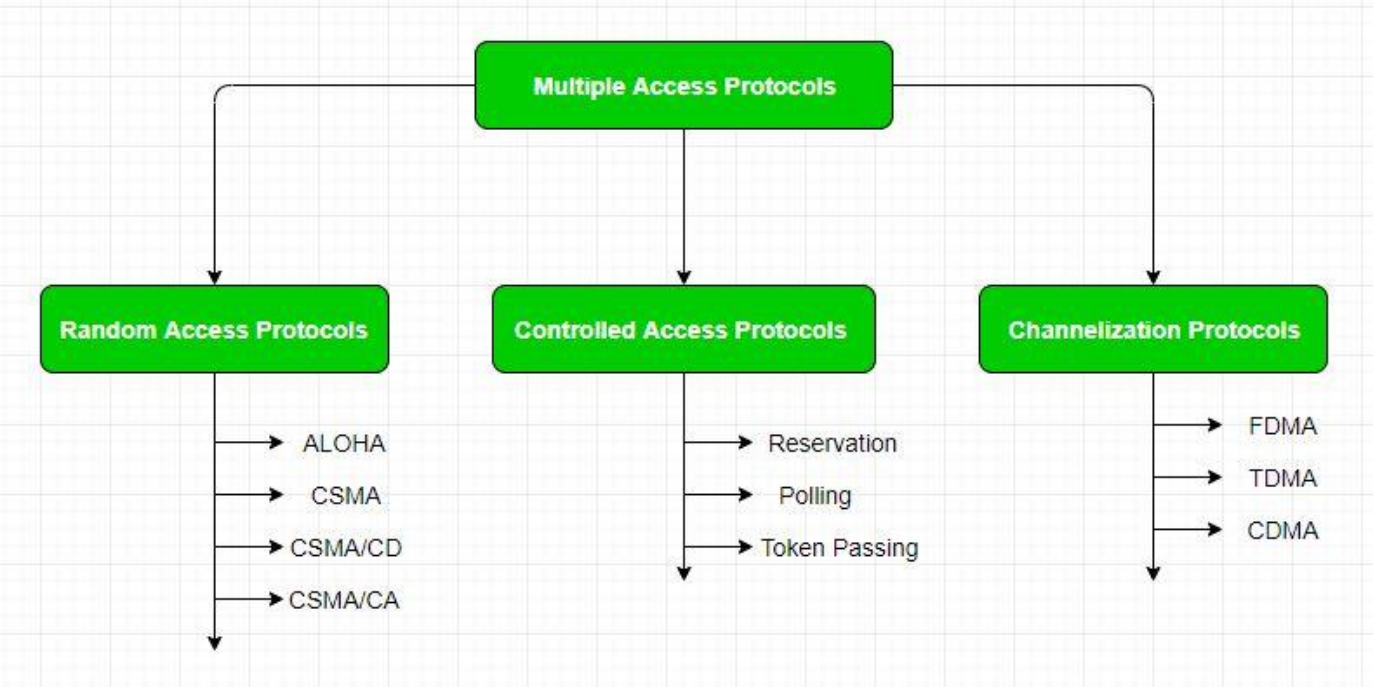
Multiple Access Protocols in Computer Network

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

- Data Link Control
- Multiple Access Control

Data Link control –
The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control. For Data link control refer to – Stop and Wait ARQ

Multiple Access Control –
If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.
Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as –



1. Random Access Protocol: In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

(a) ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

```
Vulnerable Time = 2* Frame transmission time

Throughput =  G exp{-2*G}

Maximum throughput = 0.184 for G=0.5
```

- **Slotted Aloha:**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

```
Vulnerable Time =  Frame transmission time

Throughput =  G exp{-*G}
```

```
Maximum throughput = 0.368 for G=1
```

For more information on ALOHA refer – LAN Technologies

(b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

(c) CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.

(d) CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case. CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:

In this, the data is sent by that station which is approved by all other stations. For further details refer – Controlled Access Protocols

3. Channelization:

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each

station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
For more details refer – Circuit Switching

- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- **Orthogonal Frequency Division Multiple Access (OFDMA) –** In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.

Advantages:

- Increase in efficiency
- High data rates
- Good for multimedia traffic

Disadvantages:

- Complex to implement
- High peak to power ratio

- **Spatial Division Multiple Access (SDMA) –** SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Advantages :

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

Disadvantages :

- It is complex to implement
- It require the accurate information about the channel

Features of multiple access protocols:

Contention-based access: Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.

Carrier Sense Multiple Access (CSMA): CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.
Collision Detection (CD): CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.
Collision Avoidance (CA): CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.
Token passing: Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel. Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.
Bandwidth utilization: Multiple access protocols can affect the overall bandwidth utilization of a network. For example, contention-based protocols may result in lower bandwidth utilization due to collisions, while token passing protocols may result in higher bandwidth utilization due to the controlled access to the communication channel.

Applications of Wireless Communication

Following is a list of applications in wireless communication:

Vehicles

Many wireless communication systems and mobility aware applications are used for following purpose:

- Transmission of music, news, road conditions, weather reports, and other **broadcast information** are received via digital audio broadcasting (DAB) with 1.5Mbit/s.
- For **personal communication,** a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384kbit/s.
- For **remote areas,** satellite communication can be used, while the current position of the car is determined via the GPS (Global Positioning System).
- A local ad-hoc network for the fast **exchange of information** (information such as distance between two vehicles, traffic information, road conditions) in emergency situations or to help each other keep a safe distance. Local ad-hoc

network with vehicles close by to prevent guidance system, accidents, redundancy.

- Vehicle data from buses, trucks, trains and high speed train can be transmitted in advance for **maintenance.**
- In ad-hoc network, car can comprise personal digital assistants (PDA), laptops, or mobile phones connected with each other using the Bluetooth technology.

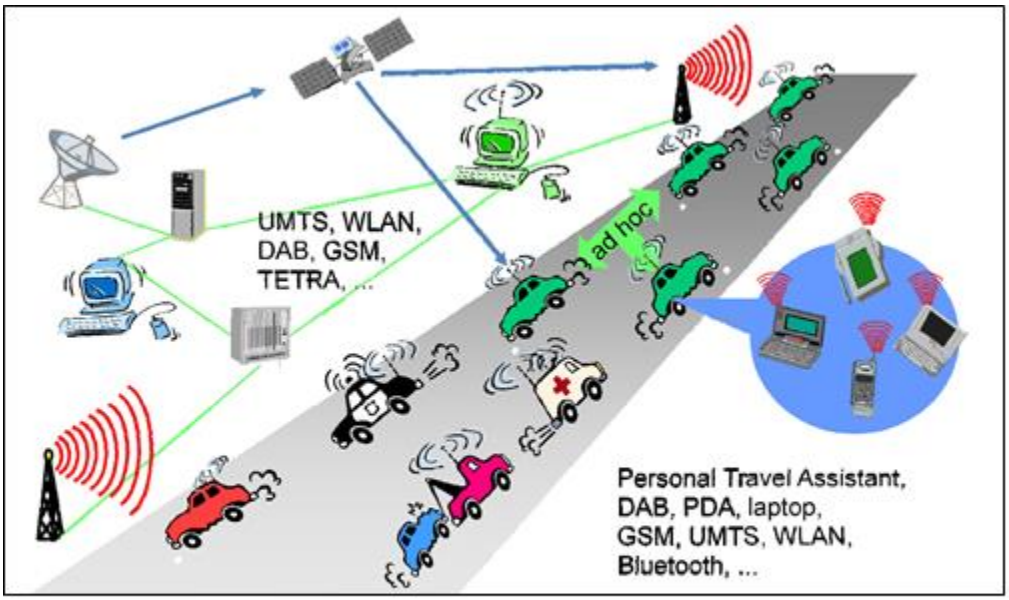


Fig: A Typical Application of Mobile Communication in Road Traffic

Emergency

Following services can be provided during emergencies:

- **Video communication:** Responders often need to share vital information. The transmission of real time situations of video could be necessary. A typical scenario includes the transmission of live video footage from a disaster area to the nearest fire department, to the police station or to the near NGOs etc.
- **Push To Talk (PTT):** PTT is a technology which allows half duplex communication between two users where switching from voice reception mode to the transmit mode takes place with the use of a dedicated momentary button. It is similar to walkie-talkie.

- **Audio/Voice Communication:** This communication service provides full duplex audio channels unlike PTT. Public safety communication requires novel full duplex speech transmission services for emergency response.
- **Real Time Text Messaging (RTT):** Text messaging (RTT) is an effective and quick solution for sending alerts in case of emergencies. Types of text messaging can be email, SMS and instant message.

Business

Travelling Salesman

- Directly access to customer files stored in a central location.
- Consistent databases for all agents
- Mobile office
- To enable the company to keep track of all the activities of their travelling employees.

In Office

- **Wi-Fi** wireless technology saves businesses or companies a considerable amount of money on installations costs.
- There is no need to physically setup wires throughout an office building, warehouse or store.
- **Bluetooth** is also a wireless technology especially used for short range that acts as a complement to Wi-Fi. It is used to transfer data between computers or cellphones.

Transportation Industries

- In transportation industries, GPS technology is used to find efficient routes and tracking vehicles.

Replacement of Wired Network

- Wireless network can also be used to replace wired network. Due to economic reasons it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information, wireless connections via satellite, can help in this situation.
- Tradeshows need a highly dynamic infrastructure, since cabling takes a long time and frequently proves to be too inflexible.
- Many computers fairs use WLANs as a replacement for cabling.
- Other cases for wireless networks are computers, sensors, or information displays in historical buildings, where excess cabling may destroy valuable walls or floors.

Location dependent service

It is important for an application to know something about the location because the user might need location information for further activities. Several services that might depend on the actual location can be described below:

- **Follow-on Services:**
- **Location aware services:** To know about what services (e.g. fax, printer, server, phone, printer etc.) exist in the local environment.
- **Privacy:** We can set the privacy like who should get knowledge about the location.
- **Information Services:** We can know about the special offers in the supermarket. Nearest hotel, rooms, cabs etc.

Infotainment: (Entertainment and Education)

- Wireless networks can provide information at any appropriate location.
- Outdoor internet access.
- You may choose a seat for movie, pay via electronic cash, and send this information to a service provider.
- Ad-hoc network is used for multiuser games and entertainment.

TCP over wireless

Wireless networks are becoming more widely deployed and more often used to access services in the Internet. Internet technology has been successful in providing services to users in fixed networks. In wireless networks, on the other hand, the performance of the Internet protocols has been reported to be much lower than in fixed networks[7, 11]. The main reason for the performance degradation is that the Transmission Control Protocol (TCP) works less efficiently in wireless networks. This problem is important, since TCP is used by many popular Internet applications, such as e-mail, web browsing, and remote login. TCP was designed for networks with wired links and stationary hosts. In these networks, data is lost mainly due to congestion. TCP interprets all data loss as congestion in the network, and in case of data loss TCP slows down its transmission rate in order to reduce the congestion. In a wireless network, it is no longer appropriate to assume that most losses are caused by congestion. Data loss is often caused by the relatively low quality of the wireless link. Terminal mobility, which is supported by many wireless networks, may also result in data loss. If data gets lost for some other reason than congestion, then performance is unnecessarily degraded as TCP reduces its transmission rate in response to the loss.

What is a Mobile IP?

Mobile IP is a communication protocol (developed by extending Internet Protocol, IP) that enables users to travel from one network to another network while maintaining the same IP address. It assures that communication will not be interrupted by the user's sessions or connections, which is one of the major motivations for using mobile IP.

In simple words, **Mobile IP** is an IETF (Internet Engineering Task Force) standard communications protocol that allows users of mobile devices (such as laptops, PDAs, mobile phones, and so on) to move from one network to another network while keeping their permanent IP (Internet Protocol) address.

Components of a Mobile IP Network

The components of a mobile IP are as follows:

Mobile Node

The **mobile node** is an end system or hand-held device, such as a laptop, Personal Digital Assistant(PDA), or cell phone, with network roaming software.

Home Network

It is the network to which the mobile node was assigned initially based on its IP address (home address).

Home Agent(HA)

The **home agent**(HA), which is located in the home network, provides numerous services to the mobile node. The packet tunnel towards the mobile node begins at the home agent. The house agent maintains a location record, which is updated with the current COA's location (care-of address).

Foreign Agent(FA)

The mobile node can receive various services from the foreign agent while connected to the foreign network. The foreign agent can use the COA (Care of Address) to forward packets to the mobile node and act as a tunnel endpoint. The foreign agent may serve as the MN's default router. It can also provide security services because they are part of the foreign network, in contrast to the mobile node, which is merely visiting.

Care-of-Address(COA)

The Care-of-address specifies the mobile node's current IP location. All IP packets directed to the mobile node are routed to the COA rather than directly to the mobile node's IP address. A tunnel is used to transport packets to the mobile node. To be more specific, the COA denotes the tunnel's endpoint or the address where packets exit the tunnel. The care-of-address has two possible locations:

- **Foreign agent Care-of-Address:-** The COA could be at the foreign agent's IP address. The tunnel endpoint is the foreign agent, which passes traffic to the mobile node. This COA is shared by many mobile nodes that use a foreign agent.
- **Co-located Care-of-Address:-** If the mobile node temporarily obtained an additional IP address that serves as a COA, the COA is co-located. The tunnel endpoint is now at the mobile node, and the address is topologically correct. Services like DHCP can be used to obtain a co-located address. One issue with this strategy is the requirement for extra addresses if MNs desire a COA. Given the scarcity of IPv4 addresses, this is not necessarily a brilliant idea.

Foreign Network

It is the current network that the mobile node is visiting (away from its home network).

Correspondent Node

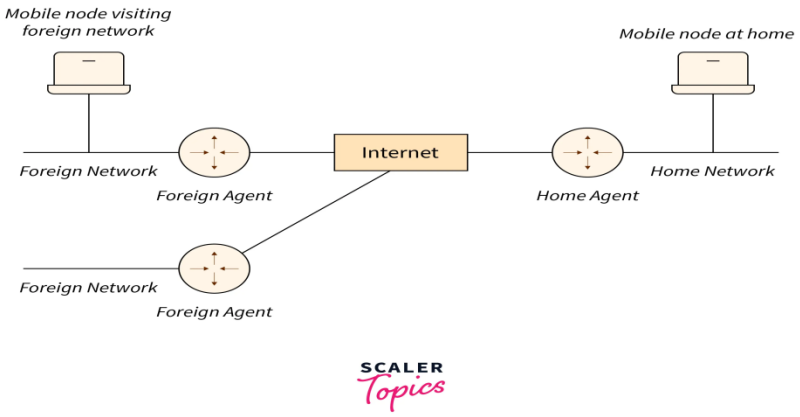
Communication requires at least one partner. For the MN, the correspondent node symbolizes this partner. The correspondent node can be either permanent or mobile.

Home Address

The mobile node's home address is its permanent IP address (within its home network).

The Architecture of Mobile IP

The architecture of Mobile IP can easily be understood by the diagram given below.



Let’s understand the architecture of Mobile IP step by step.

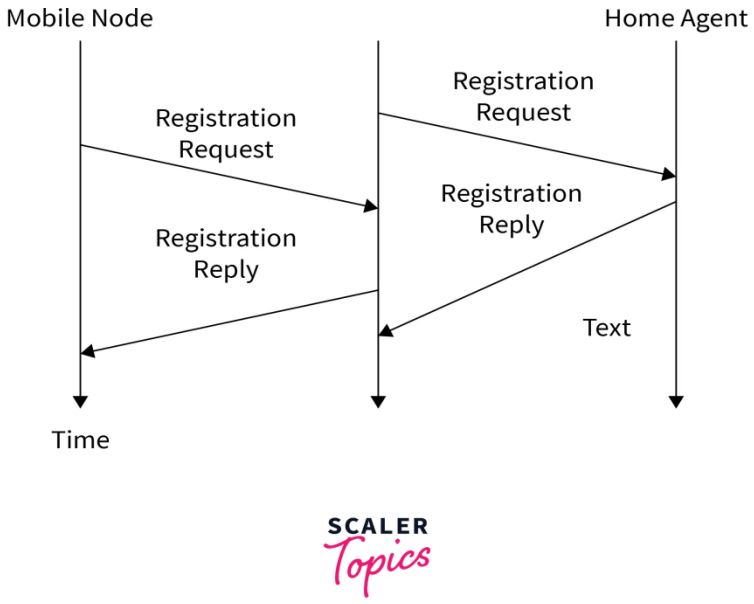
- First, the internet host transmits a datagram to the mobile node using the home address of the mobile node (using the standard IP routing process).
- If the MN(mobile node) is connected to its home network, the datagram is delivered via the standard IP (Internet Protocol) process. Otherwise, the datagram is received by the home agent.
- If the mobile node is on a foreign network, the datagram is forwarded to the foreign agent by the home agent.
- The foreign agent then delivers the datagram(or data packet) to the mobile node.
- **Datagrams** are transferred from the MN to the Internet host using standard IP routing techniques. The datagrams are delivered to the foreign agent if the mobile node is in a foreign network. Finally, the datagram is forwarded by the foreign agent to the Internet host.

Working on Mobile IP

Agent Discovery

Agents periodically broadcast their agent advertisement messages to promote their existence. The mobile node getting these agent advertisements messages checks to see if the message is coming from its home agent and then evaluates whether it is in the local or foreign network.

Agent Registration



When the mobile node identifies the foreign agent, the mobile node sends a registration request (RREQ) to the foreign agent. In turn, the foreign agent submits the registration request to the home agent, including the care-of-address. The home agent sends the foreign agent a registration reply (RREP). The registration response is then forwarded to the mobile node, completing the registration process.

Tunneling

Tunneling, also known as port forwarding, is the transmission of data intended for use only within a private, usually corporate, network across a public network. It creates a virtual pipe for available packets between a tunnel entrance and an endpoint. It is the process of transmitting a packet through a tunnel, which is accomplished using an encapsulating technique. It takes place to pass an IP datagram from the home agent to the care-of-address. Every packet the home agent gets from the correspondent node is encapsulated with the source address serving as the home address and the destination serving as the care address.

Applications of Mobile IP

- It is utilized in various wired and wireless scenarios where users must carry mobile devices across different LAN subnets.
- Mobile IP technology is employed in many applications where unexpected network connectivity and IP address changes can cause problems. It was created to provide continuous and seamless Internet connectivity.
- It is frequently used in cellular networks(such as 3G, 4G) to enable seamless IP mobility between various packet data serving node (PDSN) domains.

Conclusion

- **Mobile IP** is a communication protocol (developed by extending Internet Protocol, IP) that enables users to travel from one network to another network while maintaining the same IP address.
- Generally, there are **eight components** of the Mobile IP, and there are:
    - Mobile Node
    - Home Network
    - Home Agent
    - Foreign Agent
    - Care-of-Address
    - Correspondent Node
    - Foreign network
    - Home Address
- There are **three significant steps** involved in working Mobile IP, i.e., agent discovery, agent registration, and tunneling.
- Mobile IP is widely used in various wired and wireless scenarios where users must carry mobile devices across different networks.