1. History of Wireless Communications

- The first indication of wireless networking dates back to the 1800s and earlier. For examples, sent information to each other via smoke signals from a burning fire.
- This smoke signal system was a true network. People working intermediate fires would relay messages if a great distance separated the source of the message and the destination. The world has seen much progress since those days.
- Wireless communication system includes cellular phones, satellite phones and cordless phones in its early communication network. These systems transmit information over line of sight (LOS) distance.
- Early radio systems transmit analog signals. Today most of radio signals transmit digital signals composed of binary bits, where the bits are obtained directly from data signal or by digitizing the analog signal.
- Radio technology advances rapidly to enable transmissions over large distances with better quality, less power used with cheaper devices, thus enabling public and private radio wireless communications.
- Evolution of wireless communication systems can be described in the form of table.

Table 1: Evolution of Wireless Communication Systems

Generation	Cellular Systems	Satellite Systems	Cordless Systems	WLANs
1G	AMPS	INMARSAT	CT	IEEE 802.11
2G	GSM	LEO	DECT	Bluetooth
3G	CDMA	Iridium-66LEO	PACS	-
4G	PDC	Global Star-44	PHS	-
5G	DCS	-	-	-

Abbreviations defined as:

- AMPS: Advance mobile phone systems
- CDMA: Code division multiple access
- DCS: Digital Cellular System
- LEO: Low earth orbit satellite
- DECT: Digital enhanced cordless telephone
- PHS: Personal handy systems
- GSM: Global system for mobile
- PDC: Personal digital cellular
- INMARSAT: International marine satellite
- CT: Cordless telephone
- PACS: Personal access comm. systems
- WLAN: Wireless LAN

2. Types of Networks

- Mobile computing used various types of networks. For Example fixed telephone network, GSM, GPRS, ATM, Frame Relay, ISDN, CDMA, Dial-up, WiFi, Bluetooth, Ethernet, Broadband etc.
- Basic three types of networks are:
    1. **Wired Network**
        - It uses Ethernet cable to connect the computers to the network router.
        - Wired networks are less expensive, faster, and more secure than wireless networks.

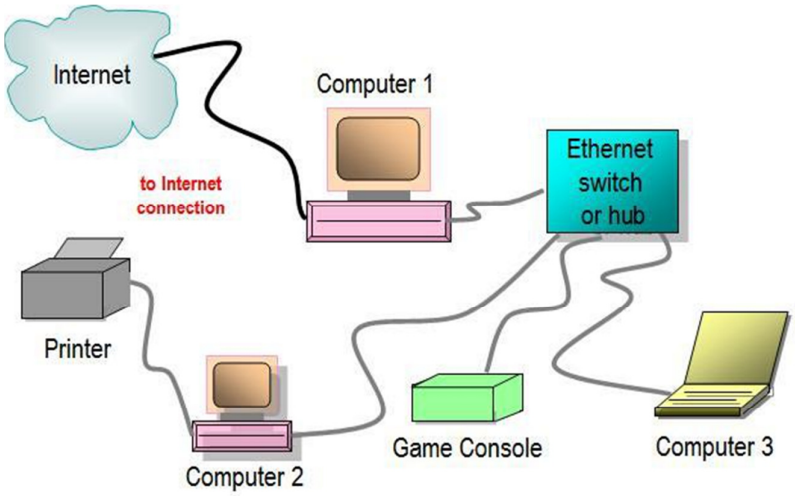


Figure 1: Wired Network

- This network is called fixed line or wire-line network. Fixed telephone over copper or fiber optic and broadband network over DSL or cable will also include in wired network.
- Wired networks generally covers public and wide area.

2. Wireless Network

- A mobile network generally refers as wireless networks.
- A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications.

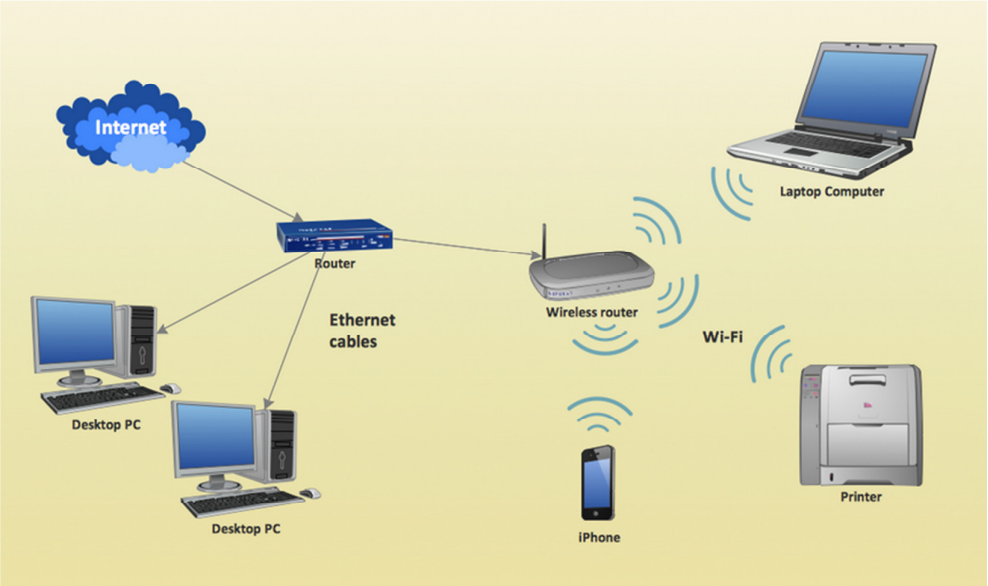


Figure 2: Wireless Network

- When you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, you're connecting to that business's wireless network.

- Wireless network used by radio taxies, cellphone, one or two way pager, GSM, CDMA, AMPS, GPRS, WiLL(Wireless Local Loop) etc.

3. Ad-hoc Network

- Ad-hoc network referred as "for this purpose only".
- An Ad-hoc network is a collection of mobile nodes, which forms a temporary network without the aid of centralized administration or standard support devices regularly available as conventional networks.
- These nodes generally have a limited transmission range and, so, each node seeks the assistance of its neighboring nodes in forwarding packets and hence the nodes in an Ad-hoc network can act as both routers and hosts.

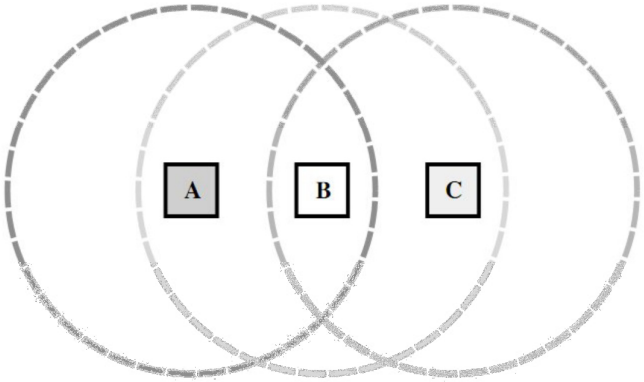


Figure 3: Ad-hoc Network

- For example, in Figure, to establish communication between nodes A and C the network must enlist the aid of node B to relay packets between them.
- The circles indicate the nominal range of each node's radio transceiver. Nodes A and C are not in direct transmission range of each other, since A's circle does not cover C.
- By nature these types of networks are suitable for situations where either no fixed infrastructure exists or deploying network is not possible.
- Examples of Ad-hoc mobile networks are military, emergency, conferencing and sensor networks.

3. Explain various Propagation Modes in Wireless Communication

- In the earth environment, electromagnetic waves propagate in ways that depend an own properties but also on those of the environment itself.
- The various methods of propagation depends largely on frequency, the complete electromagnetic spectrum is now shown in figure-4.
- Wave in straight lines, except where the earth and its atmosphere alter their path. Except in unusual circumstances, frequencies above the HF generally travel in straight lines.

- They propagate by means of so called **space waves**. They are sometimes called **tropospheric waves.** Since they travel in the troposphere, the portion of the atmosphere closest to the ground.

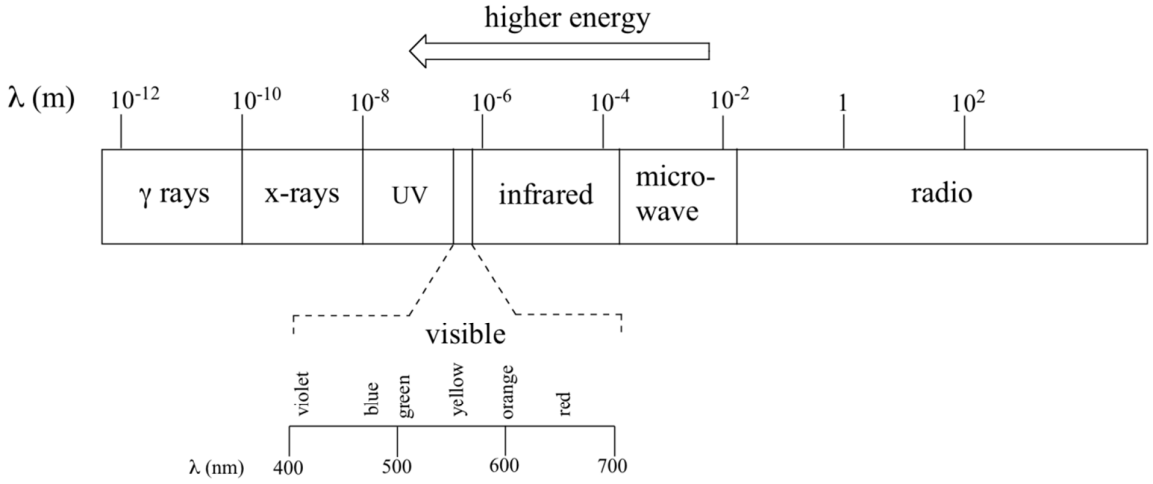


Figure 4: Electromagnetic spectrum

- Frequencies below the HF range travel around the curvature of the earth, sometimes right around the globe. The means are probably a combination of diffraction and a type of **waveguide** effect which uses the earth's surface and the lowest **ionized** layer of the atmosphere as the two waveguide walls.
- These **ground waves** or **surface wave** as they are called, are one of the two original means of propagation. All broadcast radio signals received in daytime propagate by means of surface waves.
- Waves in the HF range, and sometimes frequencies just above or below it, are reflected by ionized layers of the atmosphere and they are called **sky waves**. Such signals are beamed into the sky and come down again reflection. Returning to earth well beyond the horizon.
- To reach receivers on the opposite side of the earth, these waves must be reflected by the ground and the ionosphere several times.

Ground Wave

- Radio waves in the VLF band propagate in a ground, or surface wave. The wave is connected at one end to the surface of the earth and to the ionosphere at the other.
- The ionosphere is the region above the troposphere (where the air is), from about 50 to 250 miles above the earth.
- It is a collection of ions, which are atoms that have some of their electrons stripped off leaving two or more electrically charged objects. The sun's rays cause the ions to form which slowly modified.

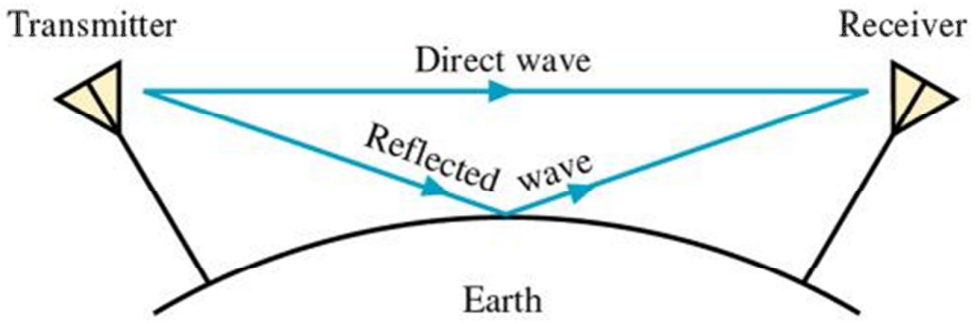


Figure 5: Ground Wave Propagation

- The propagation of radio waves in the presence of ions is drastically different than in air, which is why the ionosphere plays an important role in most modes of propagation.
- Ground waves travel between two limits, the earth and the ionosphere, which acts like a channel. Since the channel curves with the earth, the ground wave will follow. Therefore very long range propagation is possible using ground waves.

Sky Waves

- Radio waves in the LF and MF ranges may also propagate as ground waves, but suffer significant losses, or are attenuated, particularly at higher frequencies. But as the ground wave mode fades out, a new mode develops: the sky wave.
- Sky waves are reflections from the ionosphere. While the wave is in the ionosphere, it is strongly bent, or refracted, ultimately back to the ground.
- From a long distance away this appears as a reflection. Long ranges are possible in this mode also, up to hundreds of miles.
- Sky waves in this frequency band are usually only possible at night, when the concentration of ions is not too great since the ionosphere also tends to attenuate the signal.

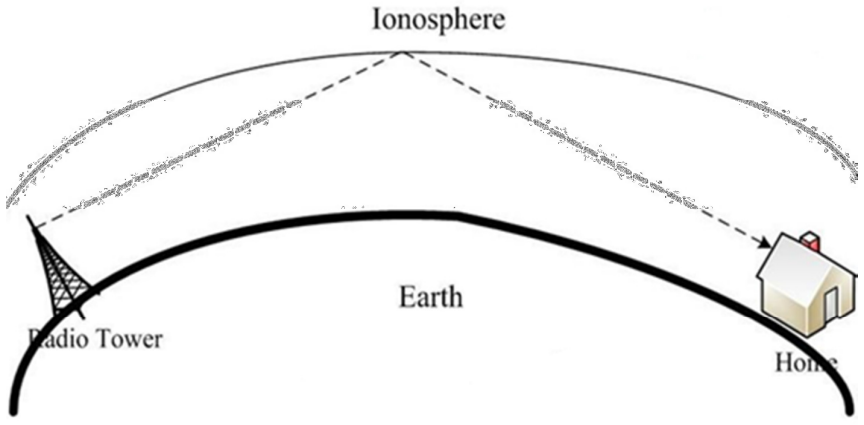


Figure 6: Sky Wave Propagation

- However, at night, there are just enough ions to reflect the wave but not reduce its power too much.

4. Explain Wireless Network Architecture

- In general, networks perform many functions to transfer information from source to destination.
- The medium provides a bit pipe (path for data to flow) for the transmission of data.
- Medium access techniques facilitate the sharing of a common medium.
- Synchronization and error control mechanisms ensure that each link transfers the data intact.
- Routing mechanisms move the data from the originating source to the intended destination.
- A good way to depict these functions is to specify the network's architecture.
- This architecture describes the protocols, major hardware, and software elements that constitute the network.
- Network architecture, whether wireless or wired, may be viewed in two ways, logically and physically.

Logical architecture of wireless network

- A logical architecture defines the network's protocols rules by which two entities communicate. People observe protocols every day. Individuals participating in a business meeting, for example, interchange their idea and concerns while they avoid talking at the same time.
- They also rephrase a message if no one understands it. Doing so ensures well managed and effective means of communication. Likewise, PCs, Servers, routers, and other active devices must conform to very strict rules to facilitate the proper coordination and transformation.
- A popular standard logical architecture is the 7 layer Open System Interconnection (OSI) Reference Model, developed by the International Standards Organization (ISO).
- OSI specifies a complete set of network function, grouped into layers Figure illustrate the OSI Reference Model.

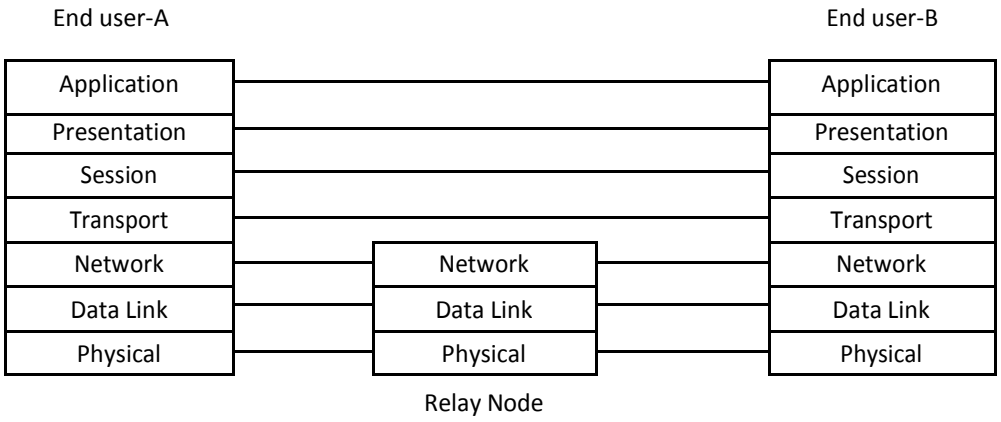


Figure 7: The Open System Interconnection Reference Model

The OSI layers provide the following network functionality:

Layer 7 - Application layer

- Establishment communication with other users and provides services such as file transfer and email to the end uses of the network.

Layer 6 - Presentation layer

- Negotiates data transfer syntax for the application layer and performs translations between different data types, if necessary.

Layer 5 - Session layer

- Establishes manages, and terminates sessions between applications.

Layer 4 - Transport layer

- Provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits, while shielding the higher layers from the network implementation details.

Layer 3 - Network layer

- Provides the routing of packets from source to destination.

Layer 2 - Data Link layer

- Ensures synchronization and error control between two entities.

Layer 1 - Physical layer

- Provides the transmission of bits through communication channel by defining electrical, mechanical and procedural specifications.

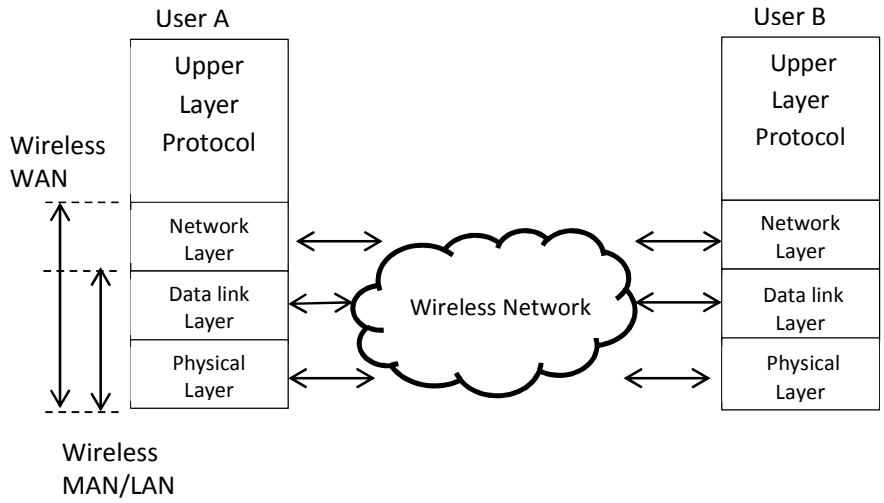


Figure 8: Logical Architecture of Wireless Network

- In figure, wireless LANs and MANs function only within the physical and data link layers, that is provide the medium, link synchronization, and error control mechanism.
- Wireless WANs provide these first two layers, as well as network layer architecture needs to include function such as end to end connection establishment and application services.
- In addition to the wireless network functions, complete network architecture needs to include functions such as end-to-end connection establishment and application services.

Physical Architecture of a Wireless Network

- The physical components of a wireless network implement the Physical, Data Link, and Network Layer functions.
- The **network operating system** (NOS) of a network, such as Novell Netware, supports the shared use of applications, printers, and disk space.
- The NOS, located on client and server machines, communicates with the wireless **Network Interface Card** (NIC) via driver software, enabling applications to utilize the wireless network for data transport.

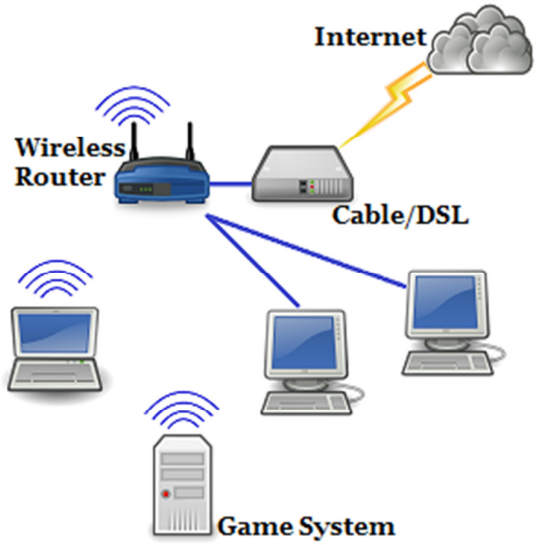


Figure 9: Physical Wireless Network

- The NIC prepares data signals for propagation from the antenna through the air to the destination comprised of the same set of components.
- **End-User Appliances:** As with any system, there must be a way for users to interface with applications and services. Whether the network is wireless or wired, an end-user appliance is a visual interface between the user and the network.
- Following are the classes of user appliances:
  - Desktop workstations
  - Laptops
  - Palmtops

  - Pen-based computers
  - Personal Digital Assistants (PDA)
  - Pagers
- Many households connect to the Internet through a cable or DSL connection, and from there a wireless router connects the rest of the equipment (some cable or DSL modems have wireless capabilities, thus eliminating the need for a separate device as shown).
- Laptops usually connect to the network wirelessly, as do game consoles.
- Desktops can connect to the network either via a cable or a wireless adapter.

5. List various applications of Wireless Communication

- Vertical industries where mobile technology has already been successfully adopted include Consumer Goods, Delivery and Rout Sales, Government, Healthcare, Market Research, Pharmaceuticals, Transportation, and Utilities.

Consumer Goods

- Typical applications include inventory, merchandising, order entry, and sales automation.
- Features found in these applications usually provide access to stock and pricing information, monitor promotions, and perform shelf space analysis including number of facings and product age. Customer detail helps reps to act more as consultants than order takers.

Delivery & Route Sales

- With fierce competition and an increasing inventory, having timely and accurate information is more important than ever.

Government

- Applications center on assessments, inspections, and work orders. Most of these applications involve auditing some sort of facility or process (food service, restaurant, nursing home, child care, and schools, commercial and residential buildings).

Healthcare

- The focus in this industry has been on automating patient records, medication dispensing, and sample collection.
- A common goal is to leverage mobile computing in the implementation of positive patient identification.

Market Research

- Automating the survey process has enabled these companies to get their data more accurately and quickly while being able to customize their queries at will.

Pharmaceuticals

- In addition to the reps need to perform account management and call reporting functions, the FDA's requirement for physician signatures for all drug samples dispensed was an added

complication that was eliminated through the use of mobile technology.

Transportation

- Transforming freight damage inspections from paper to mobile computing greatly expedites the process and reduces costs by providing on-line pre-shipment inspections.
- This technology also offers a more efficient means of storing and transmitting maintenance inspection reports.
- In conjunction with GPS (global positioning systems), mobile computing allows companies to provide better customer service by being continually aware of exactly where any given shipment is when in transit.

Utilities

- Eliminating the rekeying of data and providing a means to perform on site analysis are instrumental to an industry that is required to perform inspections on a routine basis.

Business

- Today's typical travelling salesman needs instant access to the company's database: to ensure that files on her laptop reflect the actual state, to enable the company to keep track of all activities of their travelling employees, to keep database consistent etc. With wireless access, the laptop can be turned into a true mobile office.

6. Security in Wireless Communication

- Security and privacy are specific concerns in wireless communication because of the ease of connecting to the wireless link anonymously.
- Common problems are impersonation, denial of service and tapping.
- The main technique used is encryption. In personal profiles of users are used to restrict access to the mobile units.
- Secures connection between client device and origin server should handle:
    - Confidentiality (managed by encryption)
    - Integrity (managed by algorithms)
    - Availability (relates to peripheral security)
    - Non – repudiation (managed by digital signatures)

7. Explain Concerns and Standards of Wireless Communication

- The standards of a wireless network are certainly defined by companies and organizations. Few of standards are like IETF, IEEE, EIA, W3C, Bluetooth, DECT etc.
- Network managers and engineers should be aware, however, of the following concerns that surround the implementation and use of wireless networking:
    - Radio signal interference
    - Power management
    - System interoperability
    - Network security

- Installation issues
- Health risks

Radio Signal Interference

- The purpose of radio-based networks is to transmit and receive signals efficiently over airwaves.
- This process, though, makes these systems vulnerable to atmospheric noise and transmissions from other systems.
- In addition, these wireless networks could interfere with other radio wave equipment. Interference may be inward or outward.

Inward Interference

- Most of us have experienced radio signal interference while talking on a wireless telephone, watching television, or listening to a radio.
- Someone close by might be communicating with another person via a short-wave radio system, causing harmonic frequencies that you can hear while listening to your favorite radio station. Or, a remote control car can cause static on a wireless phone while you are attempting to have a conversation.
- These types of interference might also disturb radio-based wireless networks in the form of inward interference.

Outward Interference

- Inward interferences is only half of the problem. The other half of the issue, outward interference, occurs when a wireless network's signal disrupts other systems, such as adjacent wireless LANs, navigation equipment on aircraft, and so on.
- This disruption results in the loss of some or all of the system's functionality. Interference is uncommon with ISM band products because they operate on such little power.
- The transmitting components must be very close and operating in the same bandwidth for either one to experience inward or outward interference.

Power Management

- If you are using a portable computer in an automobile, performing an inventory in a warehouse, or caring for patients in a hospital, it might be cumbersome or impossible to plug your computer into an electrical outlet.
- Thus, you will be dependent on the computer's battery. The extra load of the wireless NIC in this situation can significantly decrease the amount of time you have available to operate the computer before needing to recharge the batteries.
- Your operating time, therefore, might decrease to less than an hour if you access the network often.
- To counter this problem, vendors implement power management techniques in wireless NICs.

- Without power management, radio-based wireless components normally remain in a receptive state waiting for any information. Proxim incorporates two modes to help conserve power: the Doze Mode and the Sleep Mode.
- **The Doze Mode**, which is the default state of the product, keeps the radio off most of the time and wakes up periodically to determine if any messages wait in a special mailbox.
- This mode alone utilizes approximately 50 percent less battery power.
- **The Sleep Mode** causes the radio to remain in a transmit-only standby mode.
- In other words, the radio wakes up and sends information if necessary, but is not capable of receiving any information. Other products offer similar power management features.

System Interoperability

- When implementing an Ethernet network, network managers and engineers can deploy NICs from a variety of vendors on the same network.
- Because of the stable IEEE 802.3 standard that specifies the protocols and electrical characteristics that manufacturer must follow for Ethernet, these products all speak exactly the same language.
- This uniformity allows you to select products meeting your requirements at the lowest cost from a variety of manufacturers. Today, this is not possible with most wireless network products, especially wireless LANs and MANs.
- The selection of these wireless products is predominantly single vendor, sole-source acquisitions. Products from one vendor will not interoperate with those from a different company. This raises a problem when deploying the network.
- Once you decide to buy a particular brand of wireless network component, you must continue to purchase that brand to ensure that the components can talk the same language as the existing ones.

Installation Issues

- A well-designed plan can point the way to better security decisions about configuring and implementing wireless devices and network infrastructure.
- The plan will support decisions concerning the tradeoffs between usability, performance, and risk.

Health Risk

- Wireless Internet routers or Wi-Fi modems use dangerous electromagnetic radiation to send their signals to your computer through walls.
- If you have a wireless Internet router set up in your home or office.
- You are receiving massive EMF exposure, and living or working in a dangerous soup of radiation. These antenna radiation patterns have been shown to lead to numerous health problems.

8. Give Benefits & Future of Wireless Communication

The benefits of automating data collection applications with mobile computing are the reduction of hard and soft costs, enhancement of revenue potential, and a distinct competitive advantage through:

- Improving the data collection process
- Improving data accuracy
- Reducing paperwork
- Enforcing collection of more complete information
- Facilitating collection of more useful information
- Eliminating redundant data entry
- Reducing administrative costs
- Reducing billing errors
- Reducing data backlog
- Improving information flow
- Allowing faster adaptation to changing business conditions
- Increasing responsiveness and customer satisfaction
- Providing access to previously unavailable information

Future

- There's more happening than many people suspect. The difficulty, though, is to provide the right network, the right device, the right price and the right applications.
- Wireless is not wired, and there are numerous advantages and disadvantages. The wireless industry "mindset" is different from the computer community's.
- These different philosophies produce what we call a "wireless-Web culture clash." Also, much of the information we obtain via the Internet isn't worth paying for in a mobile environment.
- The Internet will change is already changing the way mobile companies and computer companies offer products and services, and deal with customers.
- Indeed, many wireless subscribers will demand these changes, ranging from online customer service to electronic bill-paying to creating profiles that automatically transmit personalized information via the Internet to wireless devices.
- We are in a period of tremendous change. Its mobile computing jungle where old technologies must evolve to survive and where proponents of new technologies are jockeying for dominance. It is a dangerous and exciting time where existing business models can crumble and more nimble, innovative companies can usurp established institutions.
- Uncovering these developments, analyzing their impact and recommending solutions to corporations is what Wireless Internet & Mobile Computing consulting is all about.

9. What Mobile Users Need

- Mobile business users need mobile technology that is easy to use and easy to carry with them. They will not tolerate anything less in their demanding jobs.
- Mobile workers may be working indoors or outdoors, have limited access to corporate networks and typically have many interactions with people and information throughout their workday.
- Mobile workers need practical mobility, ease of use, data access, and personalization of data.

Practical mobility

- Devices must be small in many mobile work situations to be useful. Small for most mobile workers means that the device fits in their mobile devices while they are standing and without the need to set the device down on a supporting surface.
- Mobile workers need fast access to information without having to wait for the device to "boot up".

Ease of use

- User interfaces have to be designed so that they can be manipulated easily and intuitively using interaction capabilities such as a stylus drop down lists, and thumb keyboards.
- Data collection is a practical mobile computing application as long as it is designed around the users' task and minimizes unnecessary data entry, keystrokes and stylus strokes.
- PDAs (Personal Digital Assistants such as Palm and PocketPC) and tablet computers are examples of mobile computing devices that can work effectively for data entry.
- Today's phones are not practical for data collection due to very small displays and cumbersome alpha keys.

Data access

- Mobile workers require useable information at the point of need. This includes email as a starting point, but more effectively such as product specifications, services descriptions, and inventory availability.

Personalization of data

- Mobile users will avoid using devices if they cannot easily obtain the information and only the relevant information they need. They don't have the time for extensive searches.
- Mobile device screen size limits the amount of information that can be displayed at one time. Successful mobile technology solution personalize the information for each user and take advantage of the screen "real estate" that is available on the mobile device.
- For example, information relevant to an upcoming meeting with a customer is presented based on a customer profile database.
- Another example is filtering a large catalog based for a given customer's needs so that catalog searches are limited to what the customer will likely order.

Anytime and anywhere capability

- Mobile users need to have solutions that can be used effectively at any time during their workday and used whenever their work takes them.
- For example, customer orders should be entered on the mobile device at the point of need. Having to write down order information for entry later inefficient and more prone to errors.

10. AOC and SOC Client

SOC – Sometimes On Connectivity	AOC – Always On Connectivity
• Whenever SOC clients are available they can work effectively in a disconnected mode and take advantage of wireless or wired connections	• To be effective AOC clients must be always connected to all or most of the time.
• SOC clients have the ability to store large amounts of data on the mobile device and provide the user with a complete application solution even when the user does not have a wireless or wired data connection.	• While AOC clients have to be connected or getting the solutions. Also they are not able to store large amount of data.
• Regardless of connectivity, productive work can proceed.	• Nothing useful can be done without connectivity.
• SOC technology typically requires a Pocket PC or WinCE device in order to have sufficient processing power and data storage capability.	• AOC clients have small amounts of data or no data on board the device. They require a wireless connection that is always on to be able to access data and the user interface, or screen image.

11. Give brief about Mobile Computing OS

- A mobile operating system, also known as a mobile OS, a mobile platform, or a handheld operating system, is the operating system that controls a mobile device or information appliance—similar in principle to an operating system.
- Such as Windows, Mac OS, or Linux that controls a desktop computer or laptop.
- However, they are currently somewhat simpler, and deal more with the wireless versions of broadband and local connectivity, mobile multimedia formats, and different input methods.
- Typical examples of devices running a mobile operating system are smart phones, personal digital assistants (PDAs), and information appliances, or what are sometimes referred to as smart devices, which may also include embedded systems, or other mobile devices and wireless devices.

Symbian OS

- Symbian OS has become a standard operating system for smartphones, and is licensed by more than 85 percent of the world's handset manufacturers. The Symbian OS is designed for the specific requirements of 2.5G and 3G mobile phones.

Windows Mobile

- The Windows Mobile platform is available on a variety of devices from a variety of wireless operators. You will find Windows Mobile software on Dell, HP, Motorola, Palm and i-mate products. Windows Mobile powered devices are available on GSM or CDMA networks.

Palm OS

- Since the introduction of the first Palm Pilot in 1996, the Palm OS platform has provided mobile devices with essential business tools, as well as capability to access the Internet or a central corporate database via a wireless connection.

Mobile Linux:

- The first company to launch phones with Linux as its OS was Motorola in 2003. Linux is seen as a suitable option for higher-end phones with powerful processors and larger amounts of memory.

MXI

- MXI is a universal mobile operating system that allows existing full-fledged desktop and mobile applications written for Windows, Linux, Java, and Palm are enabled immediately on mobile devices without any redevelopment.
- MXI allows for interoperability between various platforms, networks, software and hardware components.

Android OS

- Android is a mobile operating system (OS) based on the Linux kernel and currently developed by Google.
- With a user interface based on direct manipulation, Android is designed primarily for touchscreen mobile devices such as smartphones and tablet computers, with specialized user interfaces for televisions (Android TV), cars (Android Auto), and wrist watches (Android Wear).
- The OS uses touch inputs that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard.

iOS

- iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.
- It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod touch.

12. What are the different tiers in 3 tier architecture of mobile computing? Describe the functions of these tiers.

- The 3-tier architecture contains the following layers as given below:-

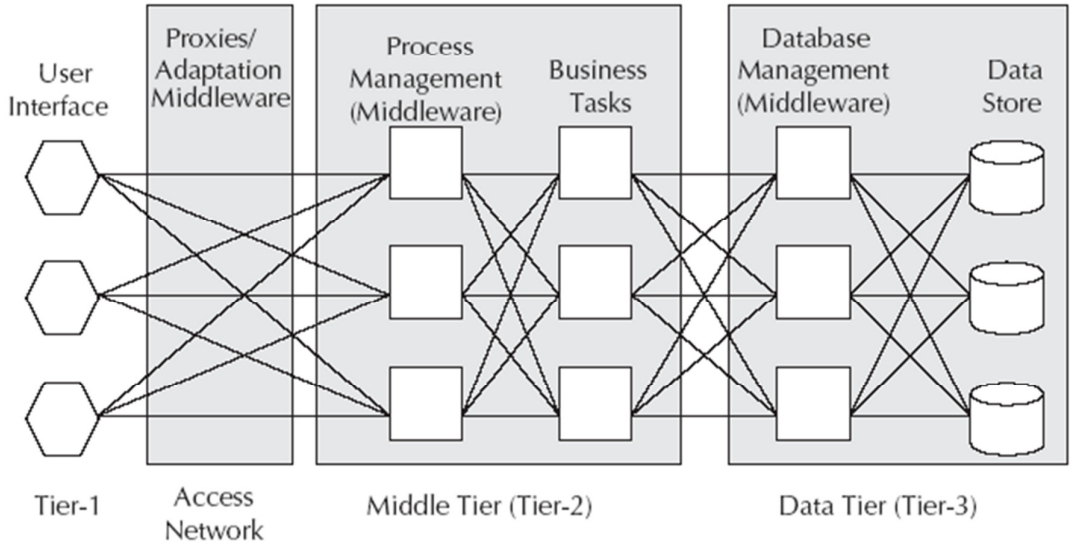


Figure 10: Three-tier Architecture for Mobile Computing

Presentation Tier (Tier-1)

- This is the layer of agent applications and systems. These applications run on the client device and offer all the user interfaces.
- This tier is responsible for presenting the information to the end user. The visual presentation will relate to rendering on a screen. 'Presentation Tier' includes web browsers, WAP browsers and customized client programs.

Application Tier (Tier-2)

- The application tier or middle tier is the "engine" of a ubiquitous application. It performs the business logic of processing user input, obtaining data and making decisions.
- In certain cases, this layer will do the transcoding of data for appropriate rendering in the Presentation Tier. The application tier may include technology lie CGIs, Java, JSP, .NET Services, PHP, etc. deployed in Apache, WebSphere, WebLogic, Pramati, etc.
- The application tier is presentation and database independent. A middleware framework is defined as a layer of software, which sits in the middle between the OS and the user facing software.
- We can group middleware into the following major categories:

Message-Oriented Middleware (MOM)

- It is the middleware framework that loosely connects different applications through asynchronous exchange of messages.
- It works over a networked environment without having to know what platform or processor the other application is resident on.

Transaction Processing (TP) Middleware

- It provides tools and an environment for developing transaction-based distributed applications. TP is used in data management, network access, security systems, delivery order processing, airline reservations, customer service, etc.

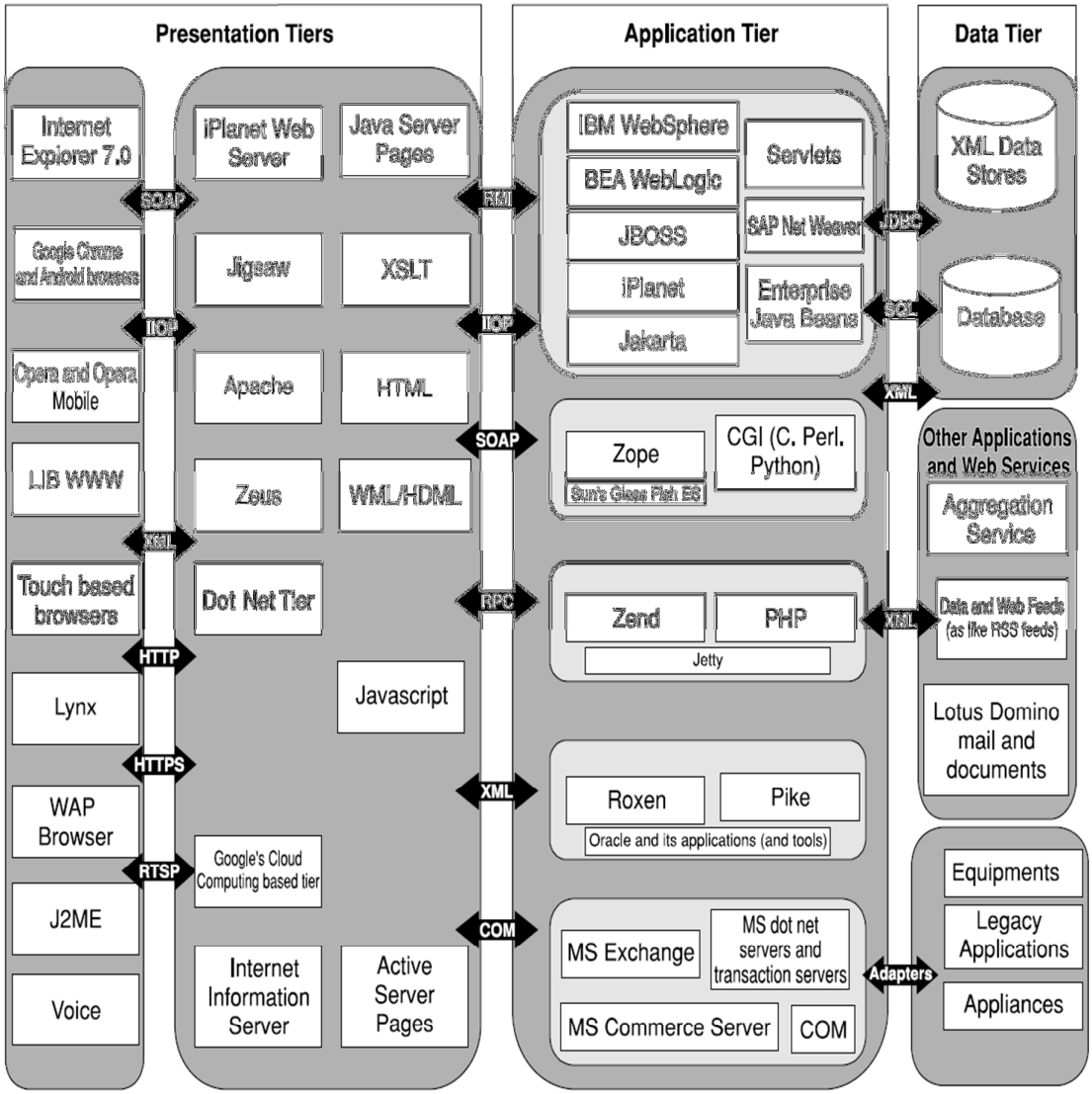


Figure 11: Mobile Computing Architecture

Communication Middleware

- It is used to connect one application to another through some communication middleware, like connecting one application to another through telnet.
- These types of middleware are quite useful in the telecommunication world.

Distributed Object and Components

- An example of distributed objects and components is COBRA (Common Object Request Broker Architecture).
- COBRA is an open distributed object computing infrastructure being standardized by the Object Management Group.

Transcoding Middleware

- It is used to transcode one format of data to another to suit the need of the client. Technically transcoding is used for content adaptation to fit the need of the device.

Data Tier (Tier-3)

- It is used to store data needed by the application and acts as a repository for both temporary and permanent data. The data can be stored in any form of data store or database.
- These can range from sophisticated relational database, legacy hierarchical database, to even simple text files.
- The data can also be stored in XML format for interoperability with other systems and data sources.
- A legacy application can also be considered as a data source or document through a communication middleware.

13. Explain various Multiplexing Techniques.

Frequency Division Multiple Access (FDMA)

- It is one of the most common multiplexing procedures. FDMA is a channel access technique found in multiple-access protocols as a channelization protocol.
- FDMA permits individual allocation of single or multiple frequency bands, or channels to the users.

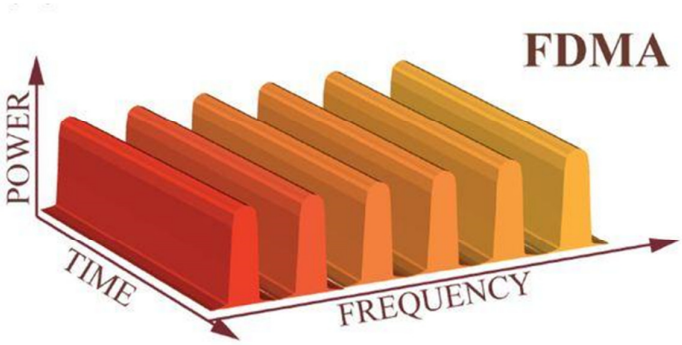


Figure 12: Frequency Division Multiple Access

- FDMA permits multiple users to simultaneously access a transmission system.
- In FDMA, every user shares the frequency channel or satellite transponder simultaneously; however, every user transmits at single frequency.

- FDMA is compatible with both digital and analog signals.
- FDMA demands highly efficient filters in the radio hardware, contrary to CDMA and TDMA.
- FDMA is devoid of timing issues that exist in TDMA.
- As a result of the frequency filtering, FDMA is not prone to the near-far problem that exists in CDMA.
- All users transmit and receive at different frequencies because every user receives an individual frequency slot.
- One disadvantage of FDMA is crosstalk, which can cause interference between frequencies and interrupt the transmission.

Space Division Multiple Access (SDMA)

- SDMA utilizes the spatial separation of the users in order to optimize the use of the frequency spectrum.
- A primitive form of SDMA is when the same frequency is reused in different cells in a cellular wireless network.
- The radiated power of each user is controlled by Space division multiple access.
- SDMA serves different users by using spot beam antenna. These areas may be served by the same frequency or different frequencies.
- However for limited co-channel interference it is required that the cells are sufficiently separated. This limits the number of cells a region can be divided into and hence limits the frequency re-use factor. A more advanced approach can further increase the capacity of the network. This technique would enable frequency re-use within the cell. In a practical cellular environment it is improbable to have just one transmitter fall within the receiver beam width. Therefore it becomes imperative to use other multiple access techniques in conjunction with SDMA.

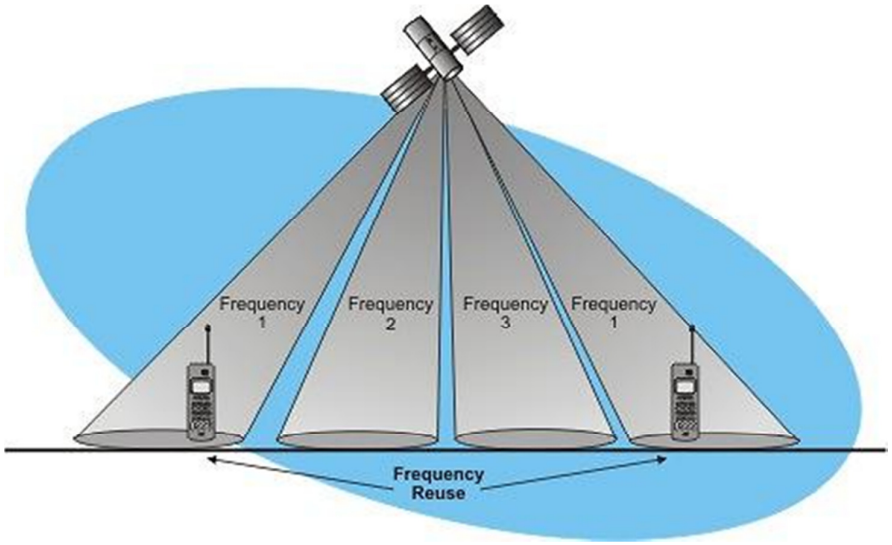


Figure 13: Space Division Multiple Access

- When different areas are covered by the antenna beam, frequency can be re-used, in which case TDMA or CDMA is employed, for different frequencies FDMA can be used.

Time Division Multiple Access (TDMA)

- It is a multiplexing technique where multiple channels are multiplexed over time.
- In TDMA, several users share the same frequency channel of higher bandwidth by dividing the signal into different time slots.
- Users transmit their data using their own respective time slots in rapid succession; to synchronize, the transmitter and the receiver need to synchronize using a global clock.
- It is divided into two types:-

Fixed TDMA

- In this, connections between time slots in each frame and data streams assigned to a user remain static and switched only when large variations in traffic are required.
- In this variant, the slot sizes are fixed at T/N (T is time in seconds and N is the number of users).

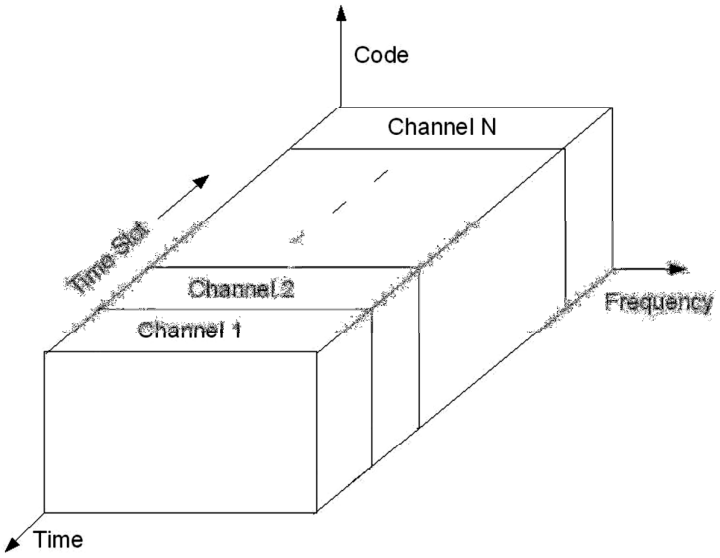


Figure 14: Time Division Multiple Access

Dynamic TDMA

- In this, a scheduling algorithm is used to dynamically reserve a variable number of time slots in each frame to variable bit-rate data streams.
- This reservation algorithm is based on the traffic demand of each data stream.

Code Division Multiple Access (CDMA)

- Short for Code-Division Multiple Access, a digital cellular technology that uses spread-spectrum techniques. It is a broadband system.
- CDMA uses spread spectrum technique where each subscriber uses the whole system bandwidth.

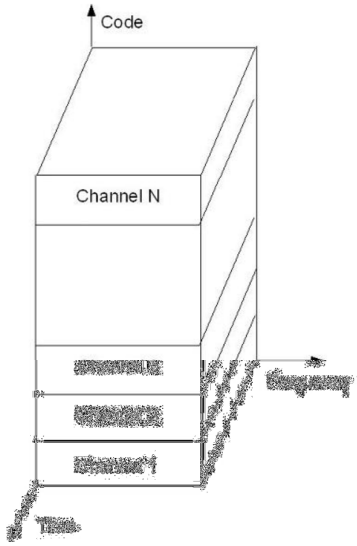


Figure 15: Code Division Multiple Access

- Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user.
- Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence.
- CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which 3G technologies are built.
- For example, CDMA is a military technology first used during World War II by English allies to foil German attempts at jamming transmissions.
- Unlike the FDMA or TDMA where a frequency or time slot is assigned exclusively to a subscriber, in CDMA all subscribers in a cell use the same frequency band simultaneously.
- To separate the signals, each subscriber is assigned an orthogonal code called “chip”.

14. Various aspects of mobility with respect to Mobile Computing and list the variants of Mobile Computing.

We can define a computing environment as mobile if it supports one or more of the following characteristics:-

- **User Mobility**
  - User should be able to move from one physical location to another location and use the same service.
  - For Example, User moves from London to New York and uses the Internet in either place to access the corporate application.
- **Network Mobility**

- User should be able to move from one network to another network and use the same service.
- For Example, User moves from Hong Kong to Singapore and uses the same GSM phone to access the corporate application.

- **Bearer Mobility**
  - User should be able to move from one bearer to another while using the same service.
  - For Example, User is unable to access the WAP bearer due to some problem in the GSM network then he should be able to use voice or SMS bearer to access that same corporate application.
- **Device Mobility**
  - User should be able to move from one device to another and use the same service.
  - For Example, User is using a PC to do his work. During the day, while he is on the street he would like to use his Palmtop to access the corporate application.
- **Session Mobility**
  - A user session should be able to move from one user - agent environment to another.
  - For Example, An unfinished session moving from a mobile device to a desktop computer is a good example.
- **Service Mobility**
  - User should be able to move from one service to another.
  - For Example, User is writing a mail. Suddenly, he needs to refer to something else. In a PC, user simply opens another service and moves between them. User should be able to do the same in small footprint wireless devices.
- **Host Mobility**
  - User should be able to move while the device is a host computer.
  - For Example, The laptop computer of a user is a host for grid computing network. It is connected to a LAN port. Suddenly, the user realizes that he needs to leave for an offsite meeting.
  - He disconnects from the LAN and should get connected to wireless LAN while his laptop being the host for grid computing network.

15. Define various mobile computing functions.

The mobile computing functions can be divided into the following major segments:-

User with Device

- This means that this could be a fixed device like a desktop computer in an office or a portable device like mobile phone. Example: Laptop computers, desktop computers, fixed telephone,

mobile phones, digital TV with set-top box, palmtop computers, pocket PCs, two-way pagers, handheld terminals, etc.

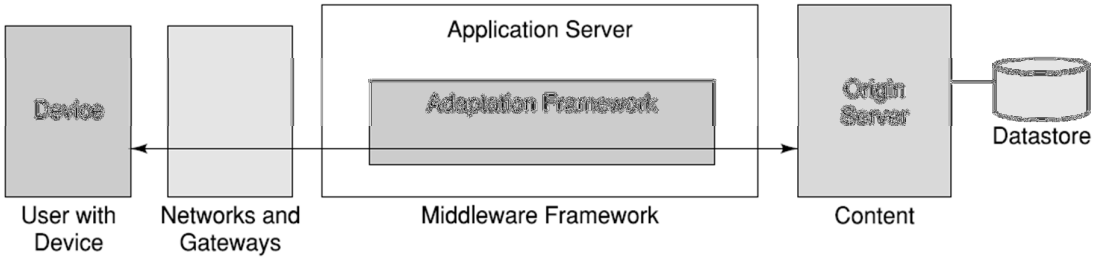


Figure 16: Mobile Computing Functions

Network

- Whenever a user is using a mobile, he will use different networks at different locations at different times. Example: GSM, CDMA, iMode, Ethernet, Wireless LAN, Bluetooth, etc.

Gateway

- This acts as an interface between different transports bearers. These gateways convert one specific transport bearer to another.
- Example, from a fixed phone we access a service by pressing different keys on the telephone. These key generates DTMF (Dual Tone Multi Frequency).
- These analog signals are converted into digital data by the IVR (Interactive Voice Response) gateway to interface with a computer application.

Middleware

- This is more of a function rather than a separate visible node. In the present context, middleware handles the presentation and rendering of the content on a particular device.
- It may optionally also handle the security and personalization for different users.

Content

- This is the domain where the origin server and content is. This could be an application, system, or even an aggregation of systems.
- The content can be mass market, personal or corporate content. The origin server will have some means of accessing the database and storage devices.

16. Explain design consideration for mobile computing.

- Mobile computing is basically the use of portable devices that are capable of use wireless network communication.
- It is divided into mobile devices and wireless communication.
- For designing mobile applications have altogether different challenges than designing desktop application. It requires different mind-set.

- On mobile platform everything is limited to make balance between design principles and resources at hand such changes shall mean that content and behavior of applications should be adapted to suit the current situation.
- Few of design consideration parameter for mobile computing:

Native vs. Mobile Web

- If your application requires local processing, access to local resources and can work in occasionally connected scenario or no connectivity consider designing a native application.
- A native application is hard to maintain, requires separate distribution and upgrade infrastructure, are compatible only with target device/platform, requires more effort (sometimes huge) to port on different devices.
- A mobile web application is compatible with all devices with internet connection and a browser.

Target device

- Target device and platform (OS) play a key role throughout design decisions making process.
- Design decisions are influenced by target device's screen size, resolution, orientations, memory, CPU performance characteristics, Operating systems capabilities, OEM (device vendor) specific OS changes/limitations, device hardware, user input mechanism (touch/non-touch), sensors (such as GPS or accelerometer) etc.

User experience

- User experience, for mobile applications, needs utmost importance (may be more than desktop).
- User interface should be rich, intuitive and responsive. While using mobile application user is often distracted by external or internal (e.g. incoming call when user is in middle of a wizard) events.

Resource Constraint

- In design decision should take into account the limited CPU, memory and battery life.
- Reading and writing to memory, wireless connections, specialized hardware, and processor speed all have an impact on the overall power usage.
- For example using notification or app directed SMS instead of polling to monitor a value/flag on server.

Multiple Platform

- An application will target not only one platform or only one device.
- In near future, requirement like same code base should support iPhone and iPad or Android Phone and Android tablet will arise.
- Design Architect should consider portability, technology agnostic with platform specific implementation. To make design with reuse across the platforms.

Security

- Devices are more vulnerable than desktop, primarily due to lack of awareness.
- It may device can be lost easily. It needs to secured device – server communication and server accepts request only from authentic source (device).
- If you are storing any confidential application or configuration data locally, ensure that the data is encrypted.

Network Communication

- Network communication on device is very significant parameter.
- To reduce network traffic by combining several commands in one request.
- For example, committing added, updated and deleted records in one request instead of firing separate request on each add/update/delete.

17. What is ICAP? Explain the typical data flow scenario in ICAP environment.

- ICAP, the Internet Content Adaption Protocol, is a protocol aimed at providing simple object-based content vectoring for HTTP services.
- ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages.
- It allows ICAP clients to pass HTTP messages to ICAP servers for some sort of transformation or other processing ("adaptation").
- The server executes its transformation service on messages and sends back responses to the client, usually with modified messages.
- Typically, the adapted messages are either HTTP requests or HTTP responses.

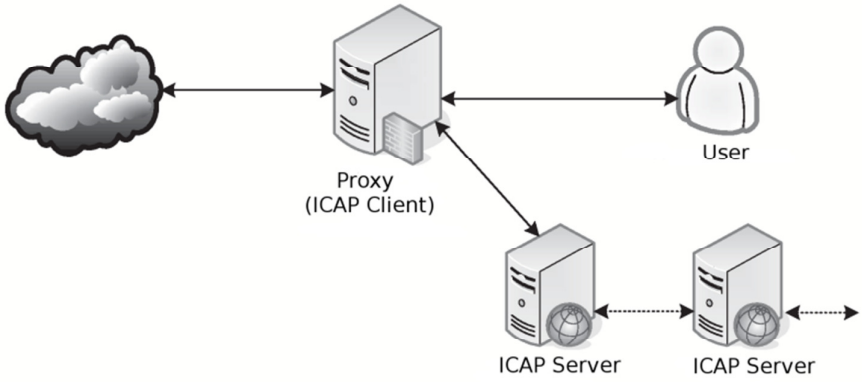


Figure 17: Typical dataflow in ICAP

- In figure, typical data flow scenario of ICAP environment is:
    1. A user agent makes a request to an ICAP client for an object on an origin server.

2. The client sends the request to the ICAP server.
3. The ICAP server executes the ICAP resource's service on the request and sends the possibly modified request or a response to the request back to the ICAP client.
4. The client sends the request, possibly different from the original client's request, to the origin server.
5. The origin server responds to the request.
6. The client sends the reply (from either the ICAP or the origin server) to the client.

18. Define mobile computing through Internet.

- A network can be divided into three major functional areas like core, edge and access. Out of this three, the core and edge are likely to be Internet and internet.
- By internet we define a network which is combination of various networks and interworks with one another, whereas Internet is the Internet we know.
- For mobile computing and ubiquitous, the access network will be both wireless and wired networks.
- In this case, infrared, Bluetooth, WiFi, GSM, GPRS, IS-95, CDMA, etc. For wired network, it is expected to be some kind of LAN.

19. Making existing application mobile-enabled in mobile computing.

- In mobile computing, there are many applications that are now being used within the intranet or the networks that need to be ubiquitous.
- These are different productivity tools like e-mail or messaging applications, workflow systems, etc.
- For example Information systems are like sales force automation need to be made ubiquitous and mobile computing capable. There are many ways by which this can be achieved.
    1. **Enhance existing application:** Take the current application and enhance it to support mobile computing.
    2. **Rent an application from an ASP:** There are many organizations which develop ubiquitous application and rent the same at a fee.
    3. **Write a new application:** Develop a new application to meet the new business requirements of mobile computing.
    4. **Buy a packaged solution:** There are many companies which are offering packaged solutions for various business areas starting from manufacturing to sales and marketing. Buy and install one of these which will also address the mobile computing needs of the enterprise.
    5. **Bridge the gap through middleware:** Use different middleware technique to face-lift and mobile computing enable the existing application.

- By using any of combinations can be used to make an application ubiquitous. If the enterprise has a source code for the application, enhancement of the existing application may be a choice.
- Writing a new application by taking care of all the aspects described above may also be a possibility.
- Buying a package or renting a solution from ASP can also be a preferred path for some business situations.

20. Explain the differences between 1G, 2G, 2.5G and 3G mobile communications.

1G

- It is the first generation cellular network that existed in 1990's.
- It transfer data in analog wave, it has limitation because there are no encryption, the sound quality is poor and the speed of transfer is only 9.6 kbps.

2G

- It is the second generation, improved by introducing the concept of digital modulation, which means converting the voice into digital code and then into analog signals.
- Being over limitation 1G, such as it omits the radio power from handsets making life healthier, and it has enhanced privacy.

2.5G

- It is a transition of 2G and 3G.
- In 2.5G, the most popular services like SMS, GPRS, EDGE, high speed circuit switched data and more had been introduced.

3G

- It is the current generation of mobile telecommunication standards.
- It allows use of speech and data services and offers data rates up to 2 mbps, which provide services like video calls, mobile TV, mobile internet and downloading.
- There are bunch of technologies that fall 3G, like WCDMA, EV-DO, and HSPA etc.

4G

- It is the fourth generation of cellular wireless standards. It is a successor to the 3G and 2G families of standards.
- In 2008, the ITU-R organization specifies the IMT Advanced (International Mobile Telecommunication Advanced) requirements for 4G standards, setting peak speed requirements for 4G service at 100 Mbit/s for high mobility communication and 1 Gbit/s for low mobility communication.

4G system

- It is expected to provide a comprehensive and secure all-IP based mobile broadband solution to laptop computer wireless modems, smart phones, and other mobile devices.

- Facilities such as ultra-broadband Internet access, IP telephony, gaming services and streamed multimedia may be provided to users.

PRE-4G

- This technology such as mobile WiMax and Long term evolution (LTE) has been on the market since 2006 and 2009 respectively, and are often branded as 4G.

Table 2: Comparison of Generation of Network

Gen.	Definition	Throughput/ Speed	Technology	Features
1G (1970 to 1980)	Analog	14.4 Kbps (peak)	AMPS,NMT, TACS	• During 1G Wireless phones are used for voice only.
2G (1990 to 2000)	Digital Narrow band circuit data	9.6/14.4 Kbps	TDMA,CDMA	• 2G capabilities are achieved by allowing multiple users on a single channel via multiplexing. • During 2G Cellular phones are used for data also along with voice.
2.5G (2001 to 2004)	Packet Data	171.2 Kbps(peak) 20-40 Kbps	GPRS	• In 2.5G the internet becomes popular and data becomes more relevant.2.5G Multimedia services and streaming starts to show growth. • Phones start supporting web browsing through limited and very few phones have that.
3G (2004 to 2005)	Digital Broadband Packet Data	3.1 Mbps (peak) 500-700 Kbps	CDMA 2000 (1xRTT, EVDO) UMTS, EDGE	• 3G has Multimedia services support along with streaming are more popular.In 3G, Universal access and portability across different device types are made possible. (Telephones, PDA's, etc.)
3.5G (2006 to 2010)	Packet Data	14.4 Mbps (peak) 1-3 Mbps	HSPA	• 3.5G supports higher throughput and speeds to support higher data needs of the consumers.
4G (Now (Read more on Transitioning to 4G)	Digital Broadband Packet All IP Very high throughput	100-300 Mbps (peak) 3-5 Mbps 100 Mbps (Wi-Fi)	WiMax LTE Wi-Fi	• Speeds for 4G are further increased to keep up with data access demand used by various services. • High definition streaming is now supported in 4G. New phones with HD capabilities surface. It gets pretty cool. • In 4G, Portability is increased further. World-wide roaming is not a distant dream.

1. What is piconet and scatternet in Bluetooth? How many maximum numbers of devices can communicate within one piconet?

- **Bluetooth** allows users to make ad hoc wireless connections between devices like mobile phones, desktop or notebook computers wirelessly.
- Bluetooth operates in a globally available frequency bad ensuring interoperability. Bluetooth uses the unlicensed 2.4GHz ISM (Industrial Scientific and Medical) frequency band.
- There are 79 available Bluetooth channels spaced 1MHz apart from 2.402 GHz to 2.480 GHz.
- The Bluetooth standard is managed and maintained by Bluetooth Special Interest Group.
- Data transfer at a speed of about 720 Kbps within 50 meters (150 feet) of range or beyond through walls, clothing and even luggage bags.

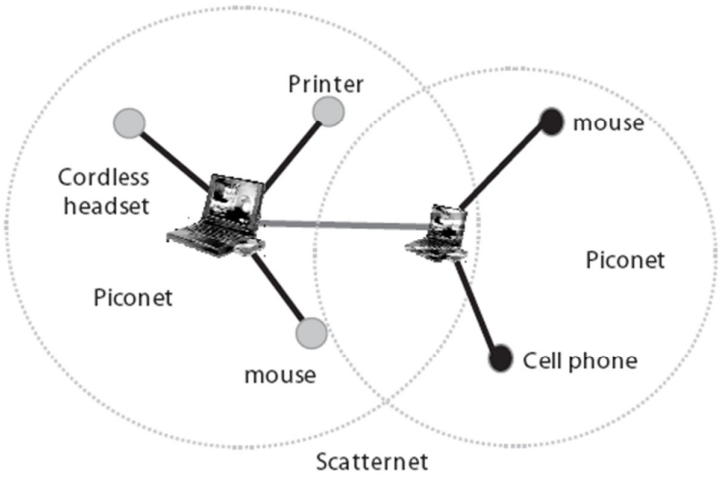


Figure 1: Scatternet and Piconet in Bluetooth

- Bluetooth protocol uses the concept of master and slave. In a master-slave protocol a device cannot talk as and when they desire. They need to wait till the time the master allows them to talk.
- The master and slaves together form a **piconet**. Up to seven “slave” devices can be set to communicate with a “master”.
- Several of these piconets can be linked together to form a larger network in an ad-hoc manner.
- The topology can be thought as a flexible, multiple piconet structure. This network of piconets is called **scatternet**.
- A scatternet is formed when a device from one piconet also acts as a member of another piconet. In this scheme, a device being a master in one piconet can simultaneously be a slave in the other one.

2. Explain Bluetooth Protocol Stack in detail.

- Bluetooth uses spread spectrum technologies at the Physical Layer while using both direct sequence and frequency hopping spread spectrum technologies.
- It uses connectionless (ACL–Asynchronous Connectionless Link) and connection-oriented (SCO–Synchronous Connection-oriented Link) links.
- Bluetooth protocol stack can be divided into four basic layers according to their functions.

Bluetooth Core Protocols:

- This comprises of baseband, Link Manager Protocol (LMP), Logical Link Control and Adaption Protocol (L2CAP), and Service Discovery Protocol (SDP).
- **Baseband**: It enables the physical RF link between Bluetooth units forming a piconet.
- This layer uses inquiry and paging procedures to synchronize the transmission with different Bluetooth devices. Using SCO and ACL link different packets can be multiplexed over the same.
- **Link Manager Protocol:** When two Bluetooth devices come within each other's range, link managers of either device discover each other.
- LMP then engages itself in peer-to-peer message exchange. These messages perform various security functions starting from authentication to encryption.
- It also controls the power modes, connection state, and duty cycles of Bluetooth devices in a piconet.
- **Logical Link Control and Adaption Protocol (L2CAP):** This layer is responsible for segmentation of large packets and the reassembly of fragmented packets.
- L2CAP is also responsible for multiplexing of Bluetooth packets from different applications.

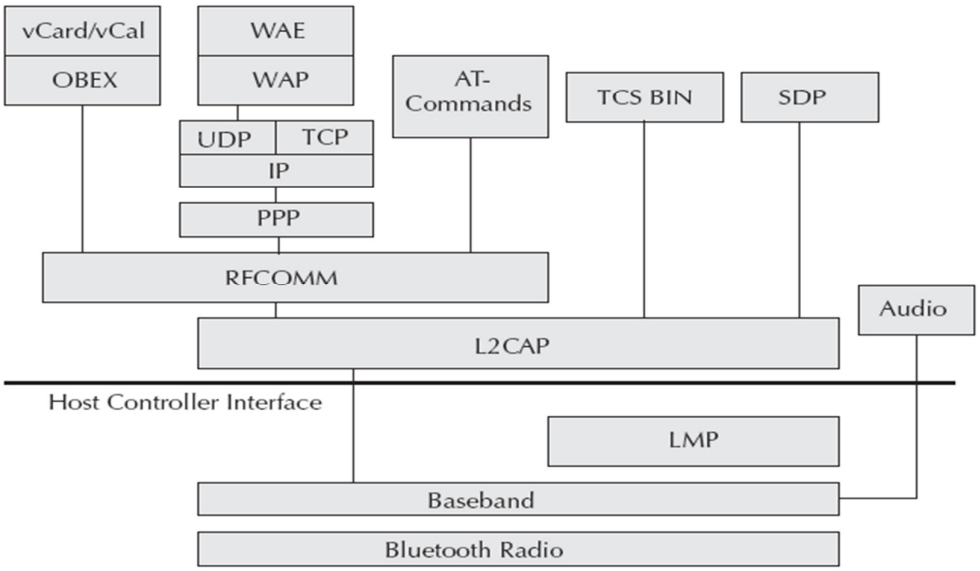


Figure 2: Bluetooth Protocol Stack

- **Service Discovery Protocol (SDP):** It enables a Bluetooth device to join a piconet. Using SDP a device inquires what services are available in a piconet and how to access them.
- SDP uses a client-server model where the server has a list of services defined through service records.
- In Bluetooth device there is only one SDP server. If a device provides multiple services, one SDP server acts on behalf of all of them.

Cable Replacement Protocol:

- This protocol has only one member which is Radio Frequency Communication (RFCOMM).
- **RFCOMM:** It is a serial line communication protocol and is based on ETSI 07.10 specification.
- The "cable replacement" protocol emulates RS-232 control and data signals over Bluetooth Baseband Protocol.

Telephony Control Protocol:

- It comprises of two protocol stacks, viz., Telephony Control Specification Binary (TCS BIN), and the AT-commands.
- **Telephony Control Specification Binary (TCS BIN):** It is a bit-oriented protocol. It defines all the call control signaling protocol for set up of speech and data calls between Bluetooth devices.
- It also defines mobility management procedures for handling groups of Bluetooth TCS devices. It is based on the ITU-T Recommendation Q.931.
- **AT-Commands:** It defines a set of AT-commands by which a mobile phone can be used and controlled as a modem for fax and data transfers.
- AT commands are used from a computer or DTE to control a modem or DC. They are based on ITU-T Recommendation V.250 and GSM 07.07.

Adopted Protocols:

- This has many protocols stacks like Point-to-Point Protocol (PPP), TCP/IP Protocol, OBEX (Object Exchange Protocol), Wireless Application Protocol (WAP), vCard, vCalender, Infrared Mobile Communication (IrMC), etc.
- **PPP Bluetooth:** This offers PPP over RFCOMM to accomplish point-to-point connections. Point-to-Point Protocol is the means of taking IP packets to/from the PPP layer and placing them onto the LAN.
- **TCP/IP:** This protocol is used for communication across the Internet. TCP/IP stacks are used in numerous devices including printers, handheld computers, and mobile handsets.
- TCP/IP/PPP is used for the all Internet bridge usage scenarios.
- **OBEX Protocol:** OBEX is a session protocol developed by the Infrared Data Association (IrDA) to exchange objects.

- OBEX provides the functionality of HTTP in a much lighter fashion. It defines a folder listing object, which can be used to browse the contents of folders on remote devices.
- **Content Formats:** vCard and vCalender specifications define the format of an electronic business card and personal calendar entries developed by the Versit consortium.
- These content formats are used to exchange messages and notes. They are defined in the IrMC specification.

3. Give Application of Bluetooth.

Model	Description
File Transfer	Refers to object transfer or transfer of files between devices.
Internet Bridge	In this model, a cordless modem acts as a modem to a PC and provides dial-up networking and faxing facilities.
LAN Access	Multiple data terminals use a LAN access point (LAP) as a wireless connection to an Ethernet LAN.
Synchronization	The synchronization model enables a device-to-device synchronization of data.
Headset	It is wirelessly connected and can act as an audio input-output interface of remote devices.

4. Define active RFID and passive RFID? Describe applications of active & passive RFID.

- **RFID** is a radio transponder carrying and ID (Identification) that can be read through radio frequency (RF) interfaces.
- These transponders are commonly known as RFID tags or simply tags.
- To assign an identity to an object, a tag is attached to the object. A RFID system comprises different functional areas like:
    - Means of reading or interrogating the data in the tag.
    - Mechanism to filter some of the data.
    - Means to communicate the data in the tag with a host computer.
    - Means for updating or entering customized data into the tag.
- RFID tags are categorized on three basic criteria. These are based on frequency, application area and the power level.
    1. **On Frequency:** There are six basic frequencies on which RFID operates.
    - These are 132.4 KHz, 13.56 MHz, 433 MHz, 918 MHz, 2.4GHz and 5.8GHz. Low frequency systems have short reading ranges and lower system costs.
    - The higher the frequency, the higher the data transfer rates.
    2. **On Application:** RFIDs are also grouped according to application and usage.
    - Speed of the object and distance to read determines the type of tag to be used.
    - The significant advantage of all types of RFID systems is the contactless, non-line-of-sight nature of the technology.

- However, RFID has become indispensable for a wide range of automated data collection and identification applications that would not be possible otherwise.
- **Power Based Grouping:** RFIDs can be grouped into two types based on power requirements. These are active and passive tags.
  a) **Active RFID Tags**: Active tags are powered by an internal battery and are typically read/write.
     - The life of an active tag is limited by the life of the battery. An active tag's memory can vary from a few bytes to 1MB.
     - Depending upon the battery type and temperatures, the life of such tags could be 10 years.
     - Some active tags can also be smart and do not send their information all the time.
  b) **Passive RFID Tags:** They operate without a power source of its own.
  - Passive tag obtains operating power from the reader's antenna. The data within a passive tag is read only and generally cannot be changed during operation.
  - Passive tags are lighter, less expensive and offer a virtually unlimited operational lifetime.
  - Passive tags contain data usually 32 to 128 bits long.

Two applications of active RFID are as follows:-

- **Access Control:** RFID tags are widely used in identification badges, replacing earlier magnetic stripe cards.
- These badges need only be held within certain of the reader to authenticate the holder.
- Tags can also be placed on vehicles, which can be read at distance, to allow entrance to controlled areas without having to stop the vehicle and present a card or enter an access code.
- **Transportation Payments:** In many countries, RFID tags can be used to pay for mass transit fares on bus, trains, or subways, or to collect tolls on highways.
- Some bike lockers are operated with RFID cards assigned to individual users.
- A prepaid card is required to open or enter a facility or locker and is used to track and charge based on how long the bike is parked.
- The Zipcar car-sharing service uses RFID cards for locking and unlocking cars and for member identification.

5. Why conventional network IP is not suitable for mobile environment? How Mobile IP works? OR Explain the Tunneling Operation in Mobile IP.

- A data connection between two end-points through TCP/IP network requires a source IP address, source TCP port and a target IP address with a target TCP port.

- The combination of one IP address of the host system combined with a TCP port as the identification of a service becomes a point of attachment for an end-point.
- TCP port number is application-specific and remains constant. IP address, on the other hand, is network-specific and varies from network to network.
- IP addresses are assigned to a host from a set, of addresses assigned to a network. This structure works well as long as the client is static and is using a desktop computer.
- Let us assume that the user is mobile and is using a laptop with Wi-Fi. As the user moves, the point of attachment will change from one sub-net to another subnet resulting in a change of IP address.
- This will force the connection to terminate. Therefore, the question is how we allow mobility while a data, connection is alive.
- The technology to do so is **'Mobile IP'**. The term 'mobile' in 'Mobile IP' signifies that, while a user is connected to applications across the Internet and the user's point of attachment changes dynamically, all connections are maintained despite the change in underlying network properties. This is similar to the handoff/roaming situation in cellular network.

Working of Mobile IP

- In a cellular network, when a user is mobile, the point of attachment (base station) changes. However, in spite of such changes the user is able to continue the conversation.
- Mobile IP allows the mobile node to use 2 IP addresses. These IP addresses are called home address and care-of address.
- **Home address** is the original static IP address of the node and is known to everybody as the identity of the node.
- The **care-of addresses** changes at each new point of attachment and can be thought of as the mobile node's location specific address. These are similar to MSISDN number and the MSRN (Mobile Station Roaming Number) as in GSM network.
- Let us take an example of IP datagrams being exchanged over a TCP connection between the mobile node (A) and another host (server X) as in the above given figure. The following steps occur:-
    1. Server X wants to transmit an IP datagram to node A. The home address of the A is advertised and known to X. X does not know whether A is in the home network or somewhere else. Therefore, X sends the packet to A with A's home address as the destination IP address in the IP header. The IP datagram is routed to A's home network.
    2. At the A's home network, the incoming IP datagram is intercepted by the home agent. The home agent discovers that A is in a foreign network. A care-of address has been allocated to A by this foreign network and available with the home agent.
    3. The home agent encapsulates the entire datagram inside a new IP datagram, with A's care-of address in the IP header. This new datagram with the care-of address as the destination address is retransmitted by the home agent. At the foreign network, the

incoming IP datagram is intercepted by the foreign agent. The foreign agent is the counterpart of the home agent in the foreign network. The foreign agent strips off the outer IP header, and delivers the original datagram to A.

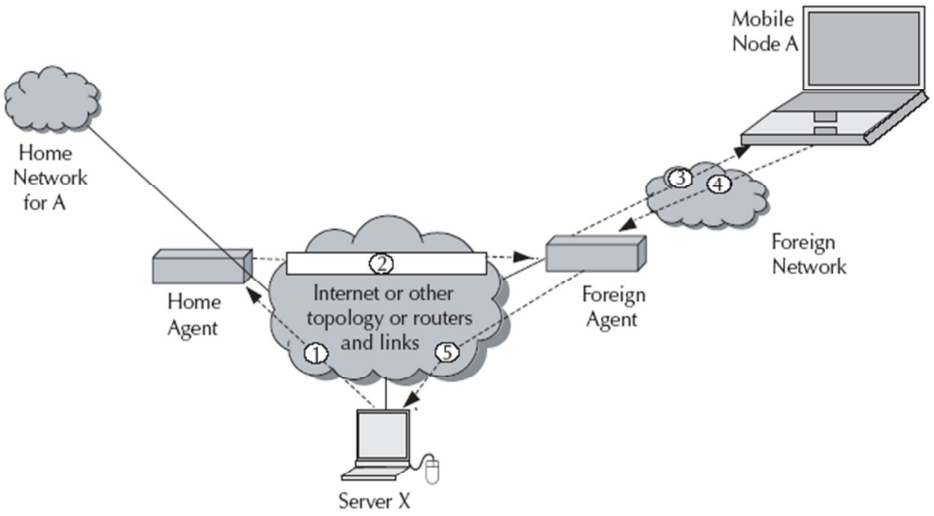


Figure 3: Mobile IP Architecture

4. A intends to respond to this message and sends traffic to X. In this example, X is not mobile; therefore X has a fixed IP address. For routing A's IP datagram to X, each datagram is sent to some router in the foreign network. Typically, this router is the foreign agent. A uses X's IP static address as the destination address in the IP header.
5. The IP datagram from A to X travels directly across the network, using X's IP address as the destination address.

- To support the operations, mobile IP needs to support 3 basic capabilities:-
- **Discovery**: A mobile node uses a discovery procedure to identify prospective home and foreign agents.
- **Registration:** A mobile node uses a registration procedure to inform its home agent of its care-of address.
- **Tunneling**: Tunneling procedure is used to forward IP datagrams from a home address to care-of address.

Discovery

- During the agent discovery phase, the home agent and foreign agent advertise their services on the network by using the ICMP Router Discovery Protocol (IRDP).
- The mobile node listens to these advertisements to determine if it is connected to its home network or foreign network. If a mobile node determines that it is connected to a foreign network, it acquires a care-of address.

Registration

- Once a mobile node obtained a care-of address from the foreign network, the same needs to be registered with the home agent.
- The mobile node sends a registration request to the home agent with the care-of address information.
- When the home agent receives this request, it updates its routing table and sends a registration reply back to the mobile node. The registration process involves the following 4 steps:-
    1. The mobile node requests for forwarding service from the foreign network by sending a registration request to the foreign agent.
    2. The foreign agent relays this registration request to the home agent of that mobile node.
    3. The home agent either accepts or rejects the request and sends a registration reply on the foreign agent.
    4. The foreign agent relays this reply to the mobile node.

Tunneling

1. The above figure shows the tunneling operations in mobile IP. In the mobile IP, an IP-within-IP encapsulation mechanism is used.
2. Using IP-within-IP, the home agent, adds a new IP header called tunnel header. The new tunnel header uses the mobile node's care-of address as the tunnel destination IP address.
3. The tunnel source IP address is the home agent's IP address. The tunnel uses 4 as the protocol number indicating that the next protocol header is again an IP header.
4. In IP-within-IP, the entire original IP header is preserved as the first part of the payload of the tunnel header. The foreign agent after receiving the packet drops the tunnel header and delivers the rest to the mobile node.

6. What is cellular IP? Establish its relationship with mobile IP.

- None of the nodes know the exact location of a mobile host. Packets addressed to a mobile host are routed to its current base station on a hop-by-hop basis where each node only needs to know on which of its outgoing ports to forward packets.
- This limited routing information (referred as mapping) is local to the node and does not assume that nodes have any knowledge of the wireless network topology. Mappings are created and updated based on the packets transmitted by mobile hosts.
- Uses two parallel structures of mappings through Paging Caches (PC) and Routing Caches (RC).

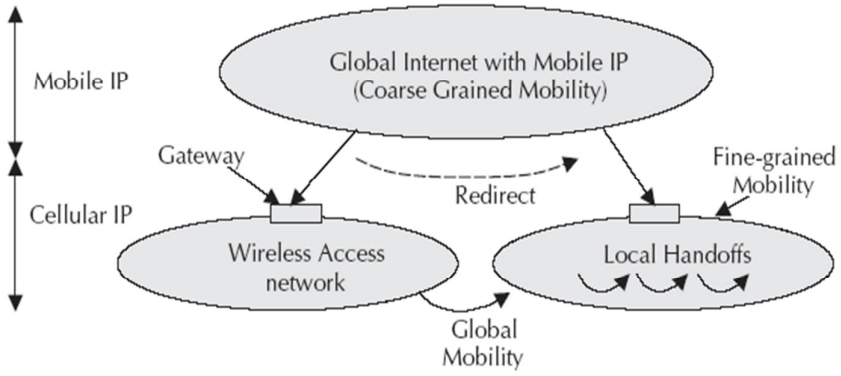


Figure 4: Relation between Mobile IP and Cellular IP

- PCs maintain mappings for stationary and idle (not in data communication state) hosts.
- RC maintains mappings for mobile hosts.
- Mapping entries in PC have a large timeout interval, in the order of seconds or minutes. RCs maintain mappings for mobile hosts currently receiving data or expecting to receive data.

7. Explain routing in MANET.

- In wireless networks with infrastructure support a base station always reaches all mobile nodes.
- But in adhoc network a destination node might be out of range of a source node transmitting packets, routing is needed to find a path between source and destination.
- In an infrastructure wireless networks cell have been defined and within cell the base station can reach all mobile modes without routing via broadband.
- In above given example dark lines define the good link and light lines defining the bad links between the nodes.
- Five nodes N1 to N5 are connected with each other defining the dependency on the current transmission between them.

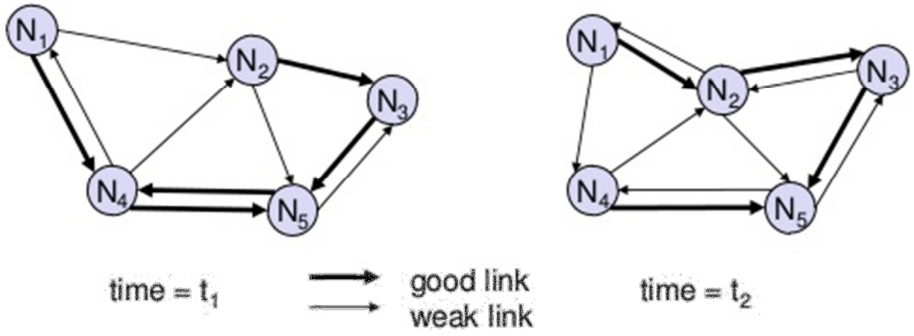
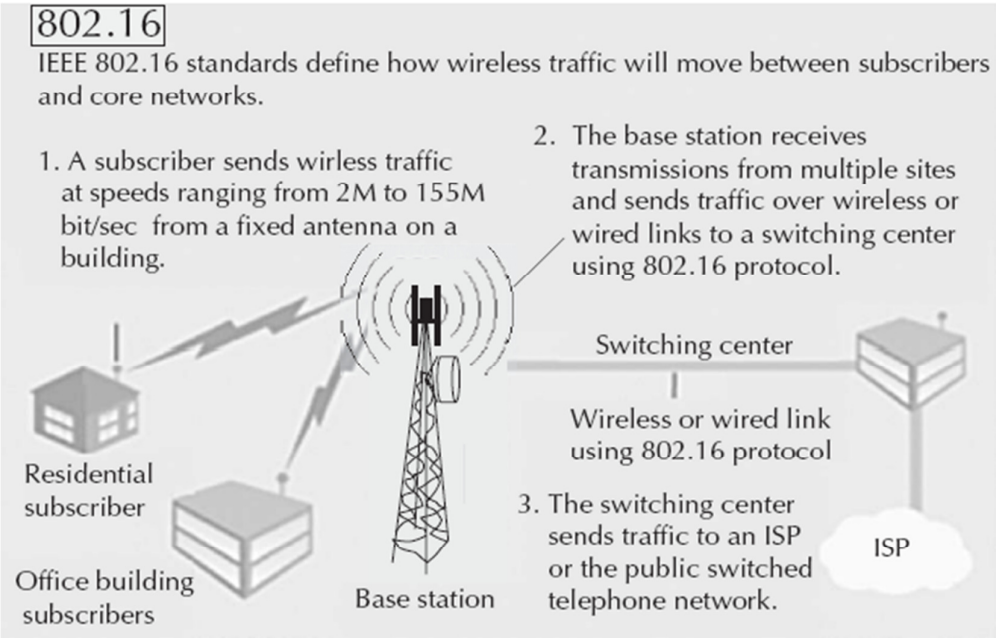


Figure 5: Routing at time t1 & t2

- N4 can receive N1 over good link but N1 receives N4 via a weak link.
- Links do not necessarily have the same characteristics in both directions. N1 cannot receive N2 at all therefore N1 has an asymmetric connection.
- This defines that the situation changes when the snapshot changes at time t2.

8. Explain architecture of IEEE 802.16 standard. (OR) Explain WiMAX three layer architecture.



- IEEE 802.16 standardizes the air interface and related functions associated with WLL.
- IEEE 802.16 standards are concerned with the air interface between a subscriber's transceiver station and a base transceiver station. The 802.16 standards are organized into 3-layer architecture.
    - **The Physical Layer**: This layer specifies the frequency band, the modulation scheme, error-correction techniques, synchronization between transmitter and receiver, data rate and the multiplexing structure.
    - **The MAC (Media Access Control) Layer**: This layer is responsible for transmitting data in frames and controlling access to the shared wireless medium through media access control layer. The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel.
    - Above the MAC layer is a **convergence layer** that provides functions specific to the service is being provided.
    - For IEEE 802.16.1, bearer services include digital audio/video multicast, digital telephony, ATM, internet access, wireless trunks in telephone networks and frame relay.

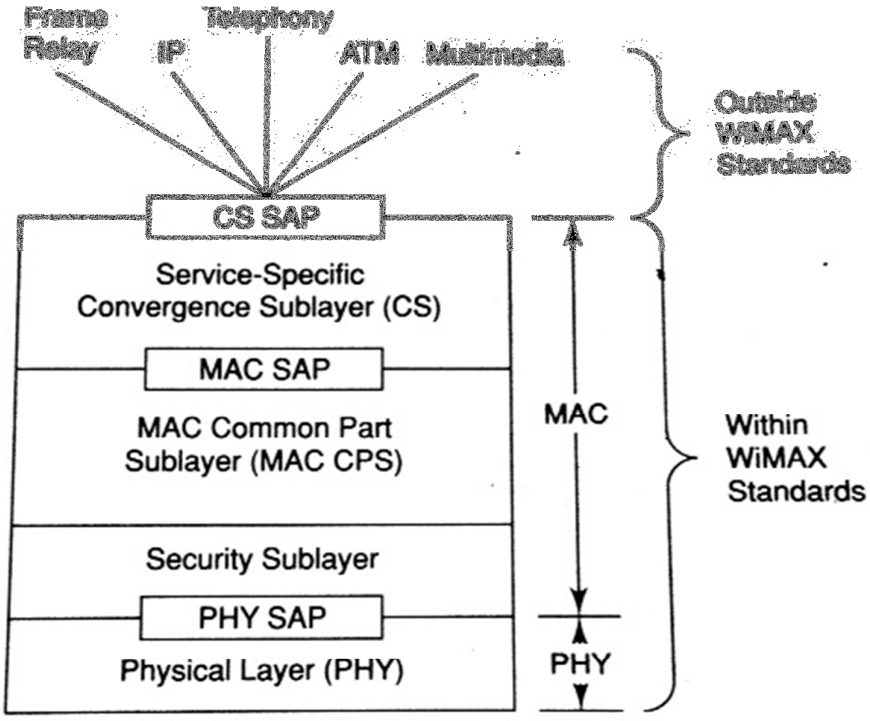


Figure 6: WiMAX Protocol Stack

9. Compare and contrast WiMAX and WiFi technologies.

	WiMAX	Wi-Fi
Released In	It was released in 2004.	It was released in 1997.
IEEE Standards	It is standardized under 802.16 family of wireless networking where y refers to various WiMAX versions.	It has been defined under IEEE 802.11x where x is various Wi-Fi versions.
Frequency Band	There is no bar on frequency usage in WiMAX.	It has been defined under ISM bands where user has to pay no extra charge for utilizing those bands.
Range	Ideal WiMAX network can reach about 80-90 kms in terms of range.	Ideal Wi-Fi based network can reach 100m in terms of range.
Channel Bandwidth	It has a flexible bandwidth option which ranges from 1.25MHz to 20MHz.	They have a channel bandwidth of 20MHz.
Data Transfer Rates	WiMAX networks exchange data at speeds up to 40mbps.	Wi-Fi networks can transfer data at speeds up to 54mbps.
MAC Layer	WiMAX MAC layer is connection oriented.	Wi-Fi MAC layer uses CSMA/CA protocol which is connection less protocol.

10. Explain the following TCP variants 1) Indirect TCP, 2) Selective Repeat Protocol 3) Snooping TCP 4) Mobile TCP

Indirect TCP

- Indirect TCP suggests splitting of the TCP layer into two TCP sub-layer. Figure. Shows the Indirect TCP sub-layer between the base transceiver (BTS) and the other between the BTS and a FN.
- The BTS has an access point at an agent TCPm for TCP connection TCPm sends and receives the packets to and from the MN through the BTS. Indirect TCP function in the following manner:

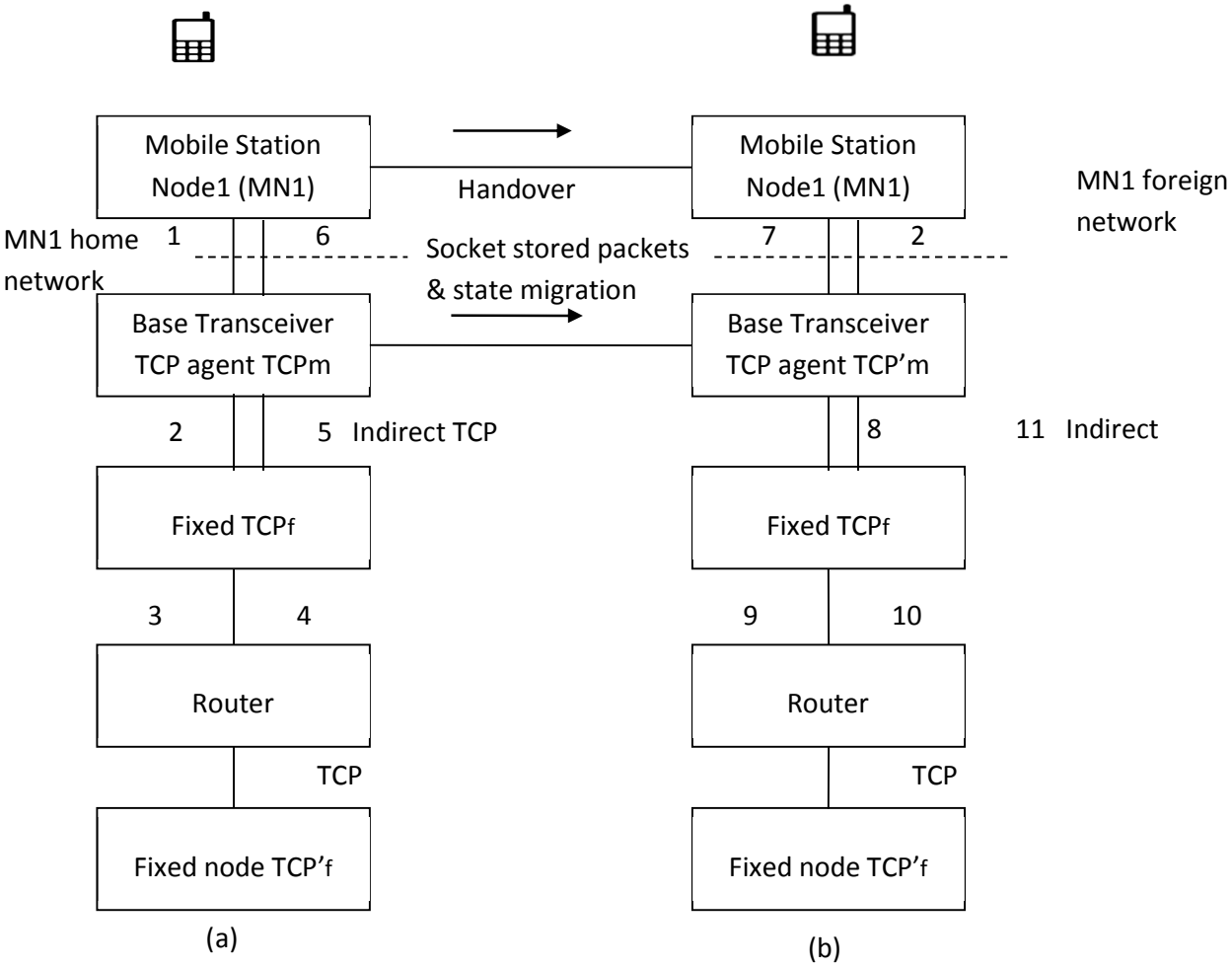


Figure 7: Indirect TCP

- TCPm sends and receives the packets to and from the TCPf layer at the fixed node.
- The transfer mechanism is simple as there is only one hope. Retransmission delay between TCPm and TCPf is very small. Unlike that between the fixed nodes.

- TCPf layer at the fixed node sends and receives the packets to and from another fixed node TCP'f. The transfer mechanism is standard using multiple hops through the routers.
- The data stream are received from the service access point (application) at the MN and buffered at TCPm.
- Figure shows the handover mechanism. When there is handover when the MN visits a foreign network, the packets for transmission, buffred at TCPm, are transferred to TCP'm.
- On handover, the socket (port and IP address) and its present state migrate from TCP, to TCP'm. The transfer from TCPm to TCP'm has latency period. (The states of a socket during a TCP connection are described).
- **Advantage of Indirect TCP** is that mobile part of the network is isolated from the conventional network and thus there is no change in the existing TCP network.
- **Disadvantage of Indirect TCP** bare the high latency period during handover of packet, possible loss of the data at the base, and guarantees reliable packet delivery.
- As an example an acknowledgement to a sender may be lost during handover latency.

Snooping TCP

- The main drawback of I-TCP is the segmentation of the single TCP connection into two TCP connections, which loses the original end-to-end TCP semantic.
- A new enhancement, which leaves the TCP connection intact and is completely transparent, is Snooping TCP. The main function is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss.

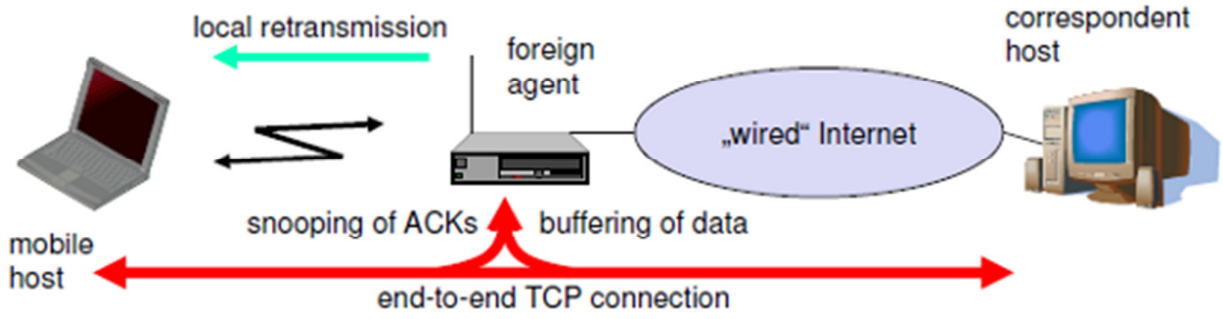


Figure 8: Snooping TCP

- Here, the foreign agent buffers all packets with **destination mobile host** and additionally 'snoops' the packet flow in both directions to recognize acknowledgements.
- The foreign agent buffers every packet until it receives an acknowledgement from the mobile host.
- If the FA does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost.
- Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet.
- Now, the FA retransmits the packet directly from the buffer thus performing a faster

retransmission compared to the CH. For transparency, the FA does not acknowledge data to the CH, which would violate end-to-end semantic in case of a FA failure.

- The foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host.
- If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission.
- The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host. This avoids unnecessary traffic on the wireless link.
- For data transfer from the mobile host with **destination correspondent host**, the FA snoops into the packet stream to detect gaps in the sequence numbers of TCP.
- As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host. The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the correspondent host by TCP.

Advantages:

- The end-to-end TCP semantic is preserved.
- Most of the enhancements are done in the foreign agent itself which keeps correspondent host unchanged.
- End-to-End semantics is preserved.
- Handover is easy. I-TCP requires a careful handover of the system state. Here it falls back to the standard solution if no enhancements.

Disadvantages:

- Snooping TCP does not isolate the behavior of the wireless link as well as I-TCP. Transmission errors may propagate till CH.
- Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host. This approach is no longer transparent for arbitrary mobile hosts.
- Snooping might be useless depending on encryption schemes.
- Data is transmitted twice in case of a packet loss. Once from the FA to the MH and the second time when the ACK finally reaches the CN.

Mobile TCP

- A TCP sender tries to retransmit data controlled by a retransmission timer that doubles with each unsuccessful retransmission attempt, up to a maximum of one minute (the initial value depends on the round trip time).
- This means that the sender tries to retransmit an unacknowledged packet every minute and will give up after 12 retransmissions.
- What happens in the case of I-TCP if the mobile is disconnected? The proxy has to buffer more and more data, so the longer the period of disconnection, the more buffers is needed. If a

handover follows the disconnection, which is typical, even more state has to be transferred to the new proxy. The snooping approach also suffers from being disconnected. The mobile will not be able to send ACKs so, snooping cannot help in this situation.

- The M-TCP (mobile TCP) approach has the same goals as I-TCP and snooping TCP: to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems.
- M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover.
- Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections
- M-TCP splits the TCP connection into two parts as I-TCP does. An unmodified TCP is used on the standard host-supervisory host (SH) connection, while an optimized TCP is used on the SH-MH connection.
- The M-TCP approach assumes a relatively low bit error rate on the wireless link. Therefore, it does not perform caching/retransmission of data via the SH.
- If a packet is lost on the wireless link, it has to be retransmitted by the original sender. This maintains the TCP end-to-end semantics.

Advantages of M-TCP

- It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
- If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0.
- Since it does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH. Lost packets will be automatically retransmitted to the new SH.

Dis-advantages of M-TCP

- The lack of buffers and changing TCP on the wireless part also has some disadvantages.
- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption.
- A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager.

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	"snoops" data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Transmission/ time-out freezing	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant
Selective retransmission	retransmit only lost data	very efficient	slightly more complex receiver software, more buffer needed
Transaction oriented TCP	combine connection setup/release and data transmission	Efficient for certain applications	changes in TCP required, not transparent

11. Explain the IPv6

- IPv6 addresses both a short term and long term concern for network service providers and users.
- IPv6 uses two types of addresses: Global and Local addresses.
- Global addresses are used for routing of global internet.
- Link Local addresses are available within subnet.
- IPv6 uses hierarchical addressing with three levels of address:
    - Public Topology(48-bit external routing prefix)
    - Site Topology(16-bit subnet number)
    - Interface Identifier(automatically generated unique 64-bit number)
- Hierarchical addressing of IPv6 is shown in figure.

Limitation of IPv6

- Expanded addressing capabilities
- Structured hierarchy to manage routing table growth
- Server less auto-configuration and reconfiguration.
- Streamlined header format and flow identification.
- Source address selection
- Mobility – more efficient and robust mechanism
- Security – Built-in, strong IP layer encryption and authentication

- Quality of service
- Privacy extensions for stateless address auto-configuration
- Improved support for options

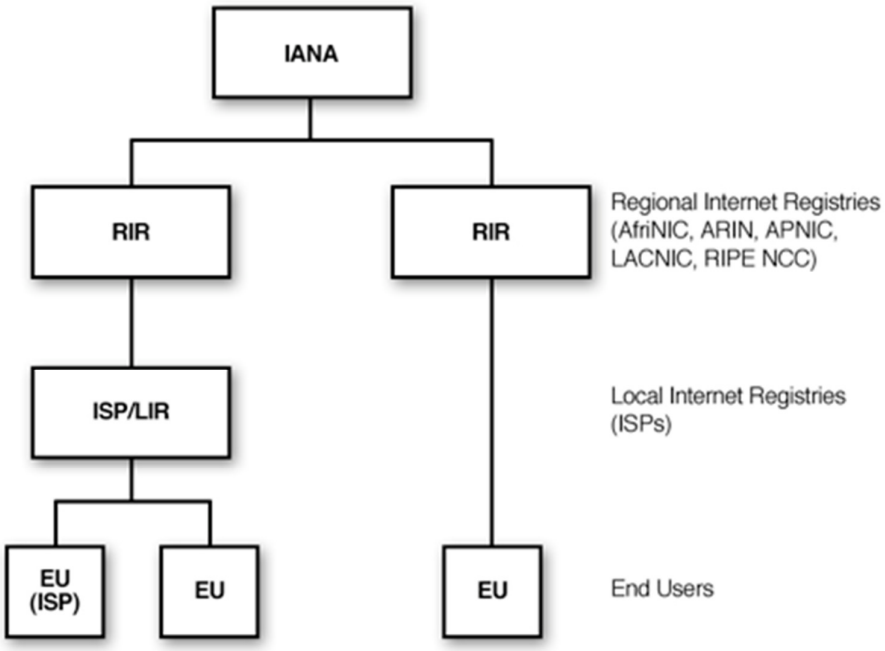


Figure 9: IPv6

12. List out GSM specification and explain functional architecture of GSM.

GSM Specification

- Uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access).
- Allocation of 50 MHz (890–915 MHz and 935–960 MHz) bandwidth in the 900 MHz frequency band and using FDMA further divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz.
- Using TDMA, each of the above mentioned channels is then further divided into 8 time slots
- So, with the combination of FDMA and TDMA, a maximum of992 channels for transmit and receive can be realized.

Frequency reuse in GSM

- To serve hundreds of thousands of users, the frequency must be reused and this is done through cells.

- The area to be covered is subdivided into radio zones or cells. Though in reality these cells could be of any shape, for convenient modeling purposes these are modeled as hexagons. Base stations are positioned at the center of these cells.

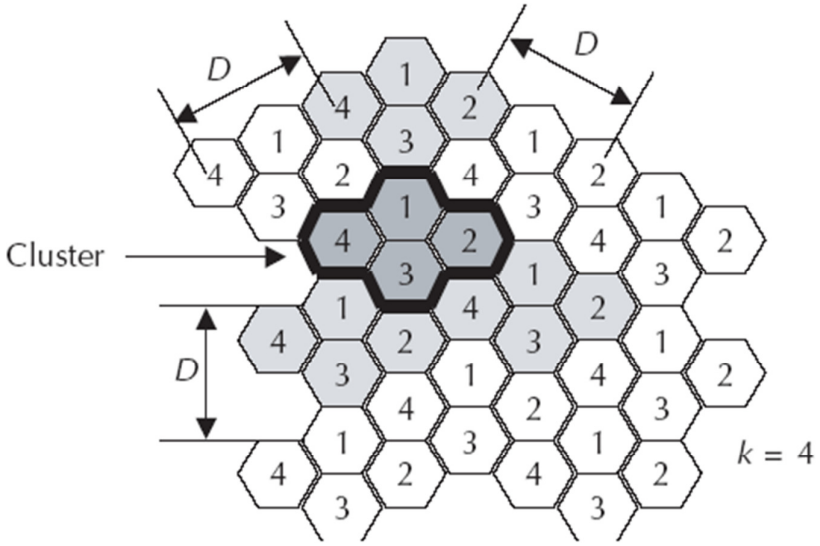


Figure 10: Cell Structure in GSM

- Each cell i receive a subset of frequencies fbi from the total set assigned to the respective mobile network.
- To avoid any type of co-channel interference, two neighboring cells never use the same frequencies.
- Only at a distance of D (known as frequency reuse distance), the same frequency from the set fbi can be reused. Cells with distance D from cell i, can be assigned one or all the frequencies from the set fbi belonging to cell i.
- When moving from one cell to another during an ongoing conversation, an automatic channel change occurs. This phenomenon is called handover.
- Handover maintains an active speech and data connection over cell boundaries.
- The regular repetition of frequencies in cells results in a clustering of cells. The clusters generated in this way can consume the whole frequency band.
- The size of a cluster is defined by k, the number of cells in the cluster. This also defines the frequency reuse distance D. The figure in next slide shows an example of cluster size of 4.

GSM Architecture

- In System, It consists at the minimum one administrative region assigned to one MSC (Mobile Switching Centre).
- Administrative region is commonly known as PLMN (Public Land Mobile Network).
- Each administrative region is subdivided into one or many Location Area (LA).

- One LA consists of many cell groups and each cell group is assigned to one BSC (Base Station Controller).
- For each LA, there will be at least one BSC while cells in one BSC can belong to different LAs.

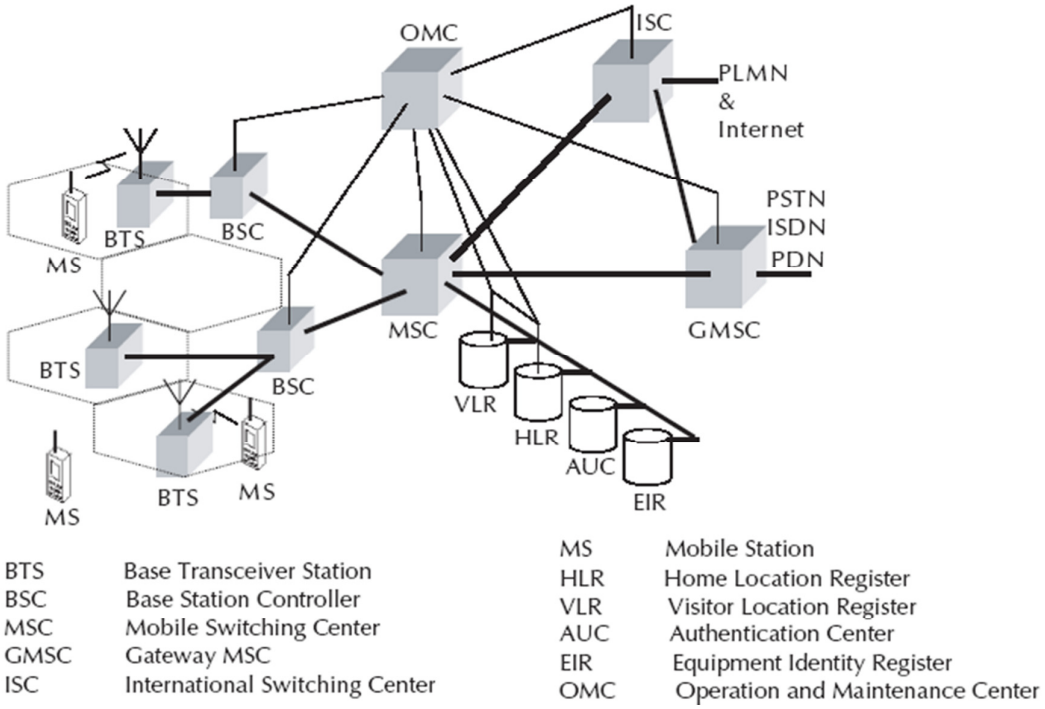


Figure 11: GSM Architecture

- Cells are formed by the radio areas covered by a **BTS** (Base Transceiver Station). Several BTSs are controlled by one BSC.
- Traffic from the **MS** (Mobile Station) is routed through **MSC**. Calls originating from or terminating in a fixed network or other mobile networks is handled by the **GMSC** (Gateway MSC)
- For all subscribers registered with a cellular network operator, permanent data such as the service profile is stored in the Home Location Register (**HLR**). The data relate to the following information:-
    - Authentication information like IMSI.
    - Identification information like name, address, etc., of the subscriber.
    - Identification information like MSISDN, etc.
    - Billing information like prepaid or postpaid customer.
    - Operator select denial of service to a subscriber.
    - Handling of supplementary services like for CFU (Call Forwarding Unconditional), CFB (Call Forwarding Busy), CFNR (Call Forwarding Not Reachable) or CFNA (Call Forwarding Not Answered)

- Storage of SMS Service Center (SC) number in case the mobile is not connectable so that whenever the mobile is connectable, a paging signal is sent to the SC
- Provisioning information like whether long distance and international calls allowed or not.
- Provisioning information like whether roaming is enabled or not
- Information related to auxiliary services like Voice mail, data, fax services, etc.
- Information related to auxiliary services like CLI (Caller Line Identification), etc.
- Information related to supplementary services for call routing. In GSM network, one can customize the personal profile to the extent that while the subscriber is roaming in a foreign PLMN, incoming calls can be barred. Also, outgoing international calls can be barred, etc.
- Some variable information like pointer to the VLR, location area of the subscriber, Power OFF status of the handset, etc.

- The GSM technical specifications define different entities that form the GSM network by defining their functions and interface requirements. The GSM network can be divided into 5 main groups:-
- **The Mobile Station (MS):** This includes the Mobile Equipment (ME) and the Subscriber Identity Module (SIM).
- **The Base Station Subsystem (BSS):** This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).
- **The Network and Switching Subsystem (NSS):** This includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AUC).
- **The Operation and Support Subsystem (OSS):** This includes the Operation and Maintenance Center (OMC).
- The data infrastructure that includes Public Switched Telephone Network (PSTN), Integrated System Digital Network (ISDN), and the Public Data Network (PDN).

13. Explain the handover procedure in GSM system OR What is handover/handoff? How handoff is different from roaming?

- The process of handover or handoff within any cellular system is of great importance.
- It is a critical process and if performed incorrectly handover can result in the loss of the call.
- Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network.

Types of GSM handover

- Within the GSM system there are four types of handover that can be performed for GSM only systems:

- **Intra-BTS handover:** This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons.
- In this form of GSM handover, the mobile remains attached to the same base station transceiver, but change the channel or slot.
- **Inter-BTS Intra BSC handover:** This GSM handover or GSM handoff occurs when the mobile is moved out of the coverage area of one BTS but into another controlled by the same BSC.
- In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.
- **Inter-BSC handover:** When the mobile is moved out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another.
- For this the handover is controlled by the MSC.
- **Inter-MSC handover:** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

GSM handover process

- Although there are several forms of GSM handover as detailed above, as far as the mobile is concerned, they are effectively seen as very similar. There are a number of stages involved in undertaking a GSM handover from one cell or base station to another.
- In GSM, which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight.
- As a result the RF section of the mobile could be idle for 6 slots out of the total eight.
- This is not the case because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable.
- In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radio channels of the beacon frequencies of neighboring BTSs via the Broadcast Channel (BCCH).
- The mobile scans these and reports back the quality of the link to the BTS. In this way the mobile assists in the handover decision and as a result this form of GSM handover is known as Mobile Assisted Hand over (MAHO).
- The network knows the quality of the link between the mobile and the BTS as well as the strength of local BTSs as reported back by the mobile.
- It also knows the availability of channels in the nearby cells. As a result it has all the information it needs to be able to make a decision about whether it needs to hand the mobile over from one BTS to another.

- If the network decides that it is necessary for the mobile to hand over, it assigns a new channel and time slot to the mobile. It informs the BTS and the mobile of the change.
- The mobile then retunes during the period it is not transmitting or receiving, i.e. in an idle period.
- A key element of the GSM handover is timing and synchronization. There are a number of possible scenarios that may occur dependent upon the level of synchronization.

Roaming

- In wireless telecommunications, roaming is a general term that refers to the extending of connectivity service in a location that is different from the home location where the service was registered. Roaming ensures that the wireless device keeps connected to the network, without losing the connection. The term "roaming" originates from the GSM (Global System for Mobile Communications) sphere; the term "roaming" can also be applied to the CDMA technology.

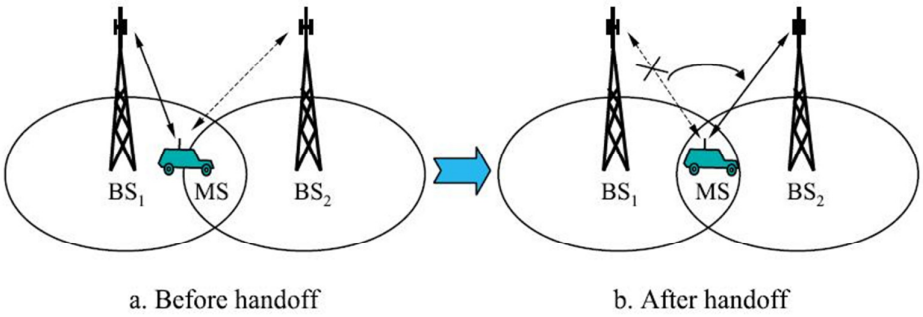


Figure 12: Handoff Process

Handoff

- In cellular telecommunications, the term handover or handoff refers to the process of transferring an ongoing call or data session from one channel connected to the core network to another.
- In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service.

14. Explain the importance of following identifiers with that GSM deals with: - 1) IMEI 2) IMSI 3) MSISDN

- **International Mobile Station Equipment Identity (IMEI):** It uniquely identifies a mobile station internationally. It is a kind of serial number.
- The IMEI is allocated by the equipment manufacturer and registered by the network operator, who stores it in the EIR.

- By means of IMEI one can recognize obsolete, stolen or non-functional equipment. The following are the parts of an IMEI:
    - Type Approval Code (TAC):- 6 decimal places, centrally assigned.
    - Final Assembly Code (FAC):- 6 decimal places, assigned by the manufacturer.
    - Serial Number (SNR):- 6 decimal places, assigned by the manufacturer.
    - Spare (SP):- 1 decimal place.
- **International Mobile Subscriber Identity (IMSI):** Each registered user is uniquely identified by its international mobile subscriber identity (IMSI).
- It is stored in the subscriber identity module (SIM). A mobile station can only be operated if a SIM with valid IMSI is inserted into equipment with a valid IMEI.
- The following are the parts of IMSI:-
    - Mobile Country Code (MCC):- 3 decimal places, internationally standardized.
    - Mobile Network Code (MNC):- 2 decimal places, for unique identification of mobile network within the country.
    - Mobile Subscriber Identification Number (MSIN):- Maximum 10 decimal places, identification number of the subscriber in the home mobile network.
- **Mobile Subscriber ISDN Number (MSISDN):** The real telephone number of a mobile station is the mobile subscriber ISDN number (MSISDN).
- It is assigned to the subscriber, such that a mobile station set can have several MSISDNs depending on the SIM.
- The MSISDN categories follow the international ISDN number plan and therefore have the following structure:-
    - Country Code (CC):- Up to 3 decimal places.
    - National Destination Code (NDC):- Typically 2-3 decimal places.
    - Subscriber Number (SN):- Maximum 10 decimal places.

15. What is SMS? Explain the strengths of SMS.

- Short message service-SMS is one of the most popular data bearer/service within GSM.
- More than one billion SMS messages interchanged every day with a growth of more than half a billion every month on an average
- Runs on SS7 signaling channels, which are always present but mostly unused, be it during an active user connection or in the idle state
- Each short message is up to 160 characters in length when 7-bit English characters are used and 140 octets when 8-bit characters are used

Strength of SMS

- Various characteristics of SMS make it as an attractive bearer for mobile computing.
- **Omnibus nature of SMS:** SMS uses SS7 signaling channel which is available throughout the world.

- **Stateless:** SMS is session-less and stateless as every SMS message is unidirectional and independent of any context. This makes SMS the best bearer for notifications, alerts and paging.
- **Asynchronous:** SMS is completely asynchronous. In case of SMS, even if the recipient is out of service, the transmission will not be abandoned and hence, SMS can be used as message queues.
- SMS can be used as a transport bearer for both synchronous (transaction oriented) and asynchronous (message queue and notification) information exchange.
- **Self-configurable and last mile problem resistant:** SMS is self-configurable and subscriber is always connected to the SMS bearer irrespective of the home and visiting network configurations.
- **Non-repudiable:** SMS message carries the Service Center (SC) and the source MSISDN as a part of the message header through which any SMS can prove beyond doubt its origin.
- **Always connected:** As SMS uses the SS7 signaling channel for its data traffic, the bearer media is always on. Users cannot switch OFF, BAR or DIVERT any SMS message. SMS message is delivered to the Mobile Station (MS) without any interruption to the ongoing call.

16. Explain Operator-centric Pull and Operator-independent Push.

Operator Centric Pull

- Operators offer different information on demand and entertainment services through connecting an Origin server to the SC via a SMS gateway.
- Such service providers are known as Mobile Virtual Network Operator(s) (MVNO).
- MVNOs develop different systems, services and applications to offer data services using SMS.
- Many enterprises use MVNOs to make their services available to mobile phone users.
- Let's say few banks offer balance enquiry and other low security banking services over SMS and customers need to register for the service.
- During the registration, the customer needs to mention the MSISDN of the phone which will be used for a banking service.
- Once a user is registered for the service, he enters 'BAL' and sends the message to a service number (like 333) as a MO message and then SC delivers this MO message to the SMS gateway (known as SME-Short Message Entity) connected to this service number.
- SMS gateway then forwards this message to the enterprise application and response from the enterprise application is delivered to the MS as a MT message from the SME.
- Even if the subscriber is in some remote region of a foreign network within GSM coverage, he can send the same SMS to the same service number in his home network and this makes the home services available in the foreign network.
- Hence, operator-centric SMS pull service is completely ubiquitous.

- Connectivity between SME and Origin server could be anything like SOAP (Simple Object Access Protocol), direct connection through TCP socket or through HTTP.
- There are applications where SMS is used in session oriented transactions as 'SMS chat' and 'SMS contests' need to remember the user context over multiple transactions.

Operator Independent Pull

- Any push, which may be an alert, notification or even response from a pull message generated by an application, can be serviced by any network and delivered to any GSM phone in any network without any difficulty.
- If appropriate roaming tie-ups are in place, an enterprise can use SMS to send business alerts or proactive notifications to its customer anywhere, anytime on his phone.

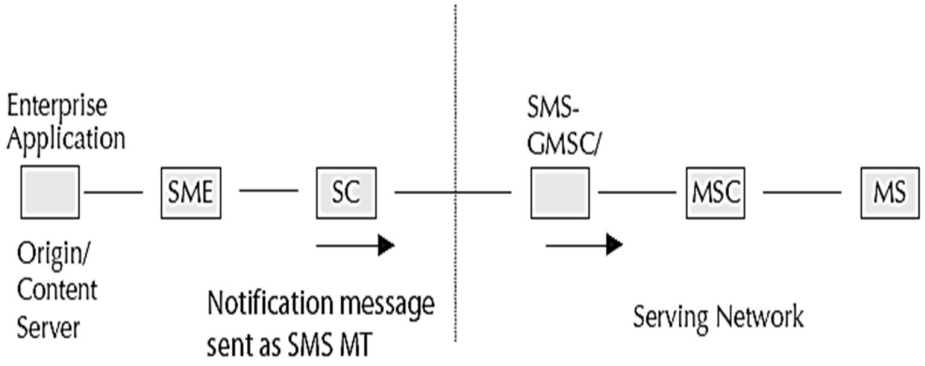


Figure 13: Basic Network Structure of the SMS Push

- For a SMS message to be routed to some enterprise SME connected to external SC, SAT is used.
- SAT application running on the SIM card changes the SC number during the transmission of the SMS and forces the SMS to recognize a different SC of a different network as its home SC.
- Here, too, SMS is sent to the SME connected to the home SC. If a SMS service is operator dependent, the cellular operator can use this to its advantage.
- Enterprises need operator independent pull as enterprises have customers around the world subscribing to different GSM networks
- Above scenario can also be achieved through Intelligent Network.

17. Challenges for SMS as Mobile computing bearer

- The major challenge for implementing ubiquitous service through SMS requires operator independent SM MO messages or operator independent pull services.
- The SMS routing needs to work exactly in the same fashion as 1-800 services.

18. Explain SMS Architecture and differentiate between SM MT and SM MO

- Two types of SMS - SM MT (Short Message Mobile Terminated Point-to-Point) and SM MO (Short Message Mobile Originated Point-to-Point)
- SM MT is an incoming short message from the network and is terminated in the MS
- SM MO is an outgoing message originated in the MS and forwarded to the network for delivery
- For an outgoing message, the path is from MS to SC via the VLR and the IWMSC (Inter Working MSC) function of the serving MSC whereas for an incoming message the path is from SC to the MS via HLR and the GMSC (Gateway MSC) function of the home MSC

Short Message Mobile Terminated (SMMT)

- SMMT is an incoming short message from the network and is terminated in the MS.
- Message is sent from SC to the MS.
- For the delivery of MT or incoming SMS messages, the SC of the serving network is never used which implies that a SMS message can be sent from any SC in any network to a GSM phone anywhere in the world.

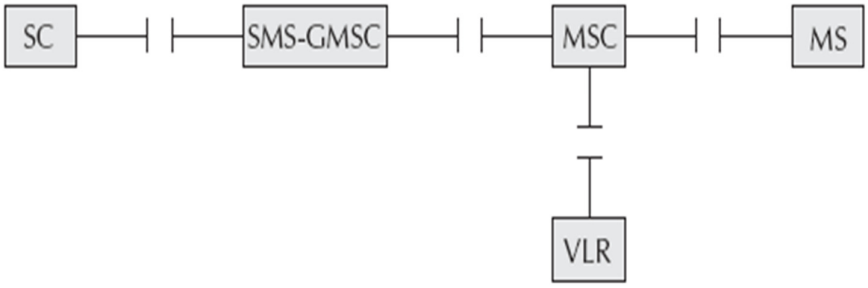


Figure 14: Interface in SMMT

Short Message Mobile Originated

- SMMO is an outgoing message originated in the MS and forwarded to the network for the delivery. For a MO message, the MSC forwards the message to the home SC.
- MO message works in two asynchronous phases. In the first phase, the message is sent from the MS to the home SC as a MO message.
- In the second phase, the message is sent from the home SC to the MS as a MT message.

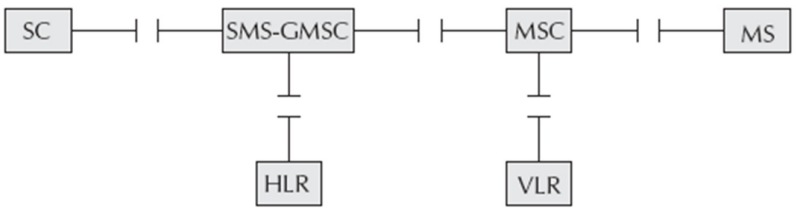


Figure 15: Interface in SMMO

19. Explain call routing in GSM with block diagram.

- Human interface is analog. However, the advancement in digital technology makes it very convenient to handle information in digital way.
- **Digitizer and source coding:** The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited–Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop where information from previous samples is used to predict the current sample.
- Each sample is then represented in signed 13-bit linear PCM value.
- This digitized data is passed to the coder with frames of 160 samples where encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech compressed into 1625 bytes and achieving a rate of 13 Kbits/sec.
- **Channel coding:** This introduces redundancy into the data for error detection and possible error correction where the gross bit rate after channel coding is 22.8 kbps (or 456 bits every 20 ms).
- These 456 bits are divided into eight 57-bit blocks and the result is interleaved amongst eight successive time slot bursts for protection against burst transmission errors.
- **Interleaving:** This step rearranges a group of bits in a particular way to improve the performance of the error-correction mechanisms.
- The interleaving decreases the possibility of losing whole bursts during the transmission by dispersing the errors.
- **Ciphering:** This encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS.
- **Burst formatting:** It adds some binary information to the ciphered block for use in synchronization and equalization of the received data.
- **Modulation:** The modulation technique chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK) where binary data is converted back into analog signal to fit the frequency and time requirements for the multiple access rules.
- This signal is then radiated as radio wave over the air.
- **Multipath and equalization:** An equalizer is in charge of extracting the 'right' signal from the received signal while estimating the channel impulse response of the GSM system and then it constructs an inverse filter.
- The received signal is then passed through the inverse filter.
- **Synchronization:** For successful operation of a mobile radio system, time and frequency synchronization are needed.
- Frequency synchronization is necessary so that the transmitter and receiver frequency match (in FDMA) while Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA).
- To avoid collisions of burst transmitted by MS with the adjacent timeslot such collisions, the Timing Advance technique is used where frame is advanced in time so that this offsets the delay due to greater distance.

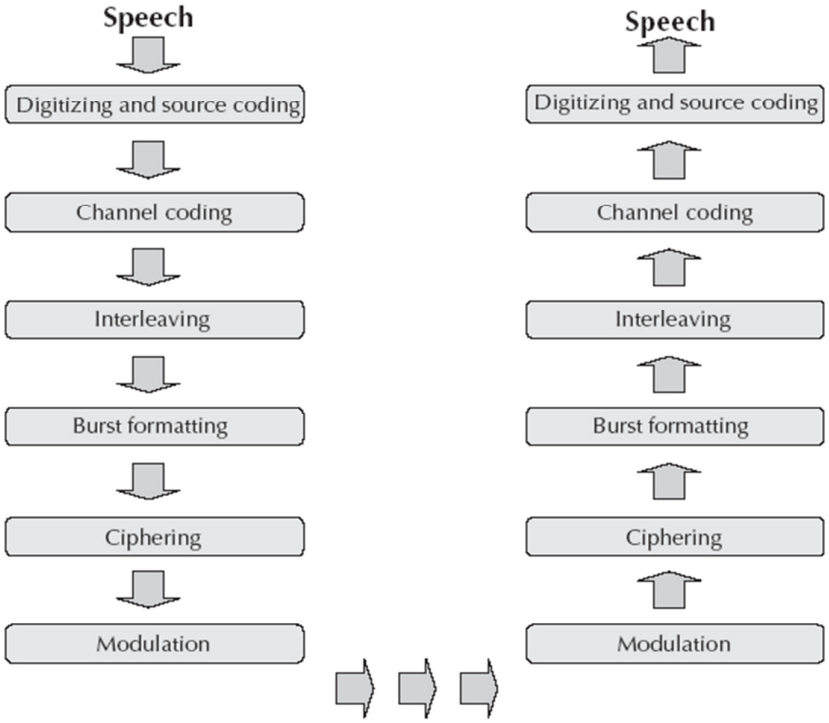


Figure 16: From speech to radio waves

- Using this technique and the triangulation of the intersection cell sites, the location of a mobile station can be determined from within the network.

Example

- The MSISDN number of a subscriber in Bangalore associated with Airtel network is +919845XYYYYY which is a unique number and understood from anywhere in the world.
- Here, + means prefix for international dialing, 91 is the country code for India and 45 is the network operator's code (Airtel in this case).
- X is the level number managed by the network operator ranging from 0 to 9 while YYYYY is the subscriber code which, too, is managed by the operator.
- The call first goes to the local PSTN exchange where PSTN exchange looks at the routing table and determines that it is a call to a mobile network.
- PSTN forwards the call to the Gateway MSC (GMSC) of the mobile network.
- MSC enquires the HLR to determine the status of the subscriber. It will decide whether the call is to be routed or not. If MSC finds that the call can be processed, it will find out the address of the VLR where the mobile is expected to be present.
- If VLR is that of a different PLMN, it will forward the call to the foreign PLMN through the Gateway MSC. If the VLR is in the home network, it will determine the Location Area (LA).

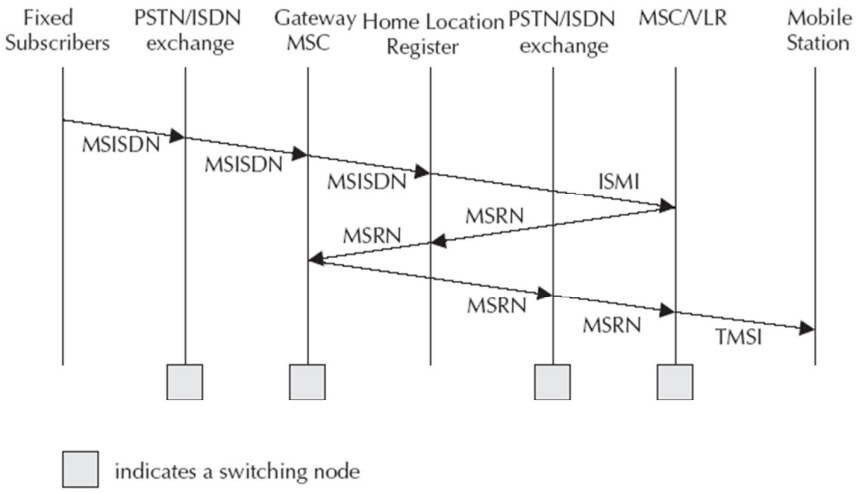


Figure 17: Call Routing for a mobile terminating call

- Within the LA, it will page and locate the phone and connect the call.

20. Write Note on Signaling Protocol Structure in GSM

- Layer 1 is the physical layer which uses the channel structures over the air interface.
- Layer 2 is the data link layer and across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN or X.25, called LAPDm.

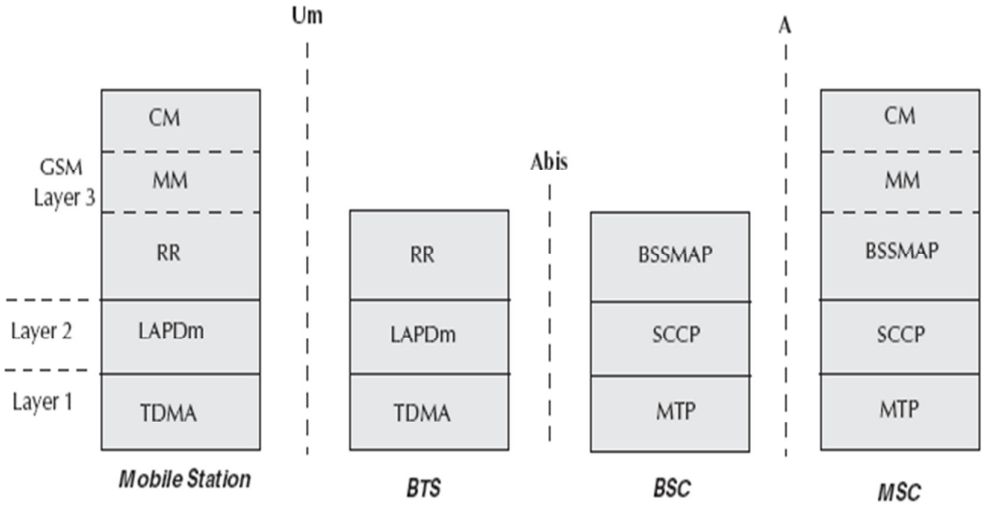


Figure 18: Signaling protocol structure in GSM

- Across the A interface, the Message Transfer Part layer 2 of Signaling System Number 7 is used.
- Layer 3 of the GSM signaling protocol is itself divided into three sub-layers:
    - **Radio Resources Management**: It controls the set-up, maintenance and termination of radio and fixed channels, including handovers.

- **Mobility Management:** It manages the location updating and registration procedures as well as security and authentication.
- **Connection Management:** It handles general call control and manages Supplementary Services and the Short Message Service.

21. Explain different GSM Services.

- There are three types of services offered through GSM which are:
  1. Telephony (also referred as tele-services) Services
  2. Data (also referred as bearer services) Services
  3. Supplementary Services

Teleservices or Telephony Services

- A teleservices utilizes the capabilities of a Bearer Service to transport data, defining which capabilities are required and how they should setup.
  - **Voice Calls:** The most basic teleservices supported by GSM is telephony. This includes full rate speech at 13 Kbps and emergency calls, where the nearest emergency service provider is notified by dialing three digits.
  - **Videotext and Facsimile:** Another group of teleservices includes Videotext access, Teletext transmission, and Facsimile alternate speech and facsimile Group 3, automatic facsimile Group 3 etc.
  - **Short Text Messages:** SMS service is a text messaging which allow you to send and receive text messages on your GSM mobile phones.

Bearer Services or Data Services

- Using your GSM phone to receive and send data is the essential building block leading to widespread mobile Internet access and mobile and mobile data transfer.
- GSM currently has a data transfer rate of 9.6k.
- New development that will push up data transfer rated for GSM users HSCSD are now available.

Supplementary Services

- Supplementary services are provided on top of teleservices or bearer services, and include features such as caller identification, call forwarding, call waiting, multi-party conversation. A brief description of supplementary services is given here:
  - **Multiparty Service or conferencing:** The multiparty service allows a mobile subscriber to establish multiparty conservations. That is, conservation between three or more subscribers to setup a conference calls. This service is only applicable to normal telephony.
  - **Call Waiting:** This service allows a mobile subscriber to be notified of an incoming call during a conversation. The subscriber can answer, reject or ignore the incoming call. Call

waiting is applicable to all GSM telecommunications services using circuit switched connection.

- **Call Hold:** This service allows a mobile subscriber to put an incoming call on hold and then resume this call. The call hold service is only applicable to normal telephony.
- **Call Forwarding:** The call forwarding supplementary service is used to divert calls from the original recipient to another number, and is normally set up by the subscriber himself.
- It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.
- A typical scenario would be a salesperson turns off his mobile phone during a meeting with customer, but does not wish to lose potential sales leads while he is unavailable.
- **Call Barring:** The concept of barring certain type of calls might seem to be a supplementary disservice rather than service.
- However, there are times when the subscriber is not the actual user of the Mobile Station, and as a consequence may wish to limit its functionality, so as to limit charges incurred.
- If the subscriber and users and one and same, the call barring may be useful to stop calls being routed to international destinations when they are route.
- The reasons for this are because it is expected that are roaming subscriber will pay the charges incurred for international re-routing of calls.
- So, GSM devised some flexible services that enable the subscriber to conditionally bar calls.

1. Introduction of GPRS

- GPRS is an abbreviation for General Packet Radio Service.
- GPRA is a means of providing packet switched data service with full mobility and wide area coverage on GSM networks.
- The GPRS service is designed to ultimately provide data transfer up to 14.4 kBps to 171.2 KBps.
- Deployment of GPRS networks allows a variety of new applications ranging from mobile e-commerce to mobile corporate VPN access.
- No dial-up modem connection is necessary.
- Offers fast connection set-up mechanism to offer a perception of being 'always on' or 'always connected'.
- Immediacy is one of the prime advantages of GPRS.

Basic Quality of Service in GPRS

- Allows definition of QoS profiles using the parameters of service precedence, reliability, delay and throughput.
- **Service precedence** is the priority of a service in relation to another service which can be high, normal or low.
- **Reliability** indicates the transmission characteristics required by an application and guarantees certain maximum values for the probability of loss, duplication, mis-sequencing and corruption of packets.
- **Delay** parameters define maximum values for the mean delay and the 95-percentile delay.
- **Throughput** specifies the maximum/peak bit rate and the mean bit rate.

2. Explain the GPRS functional architecture and its application.

- GPRS uses the GSM architecture for voice.
- GPRS support nodes are responsible for the delivery and routing of data packets between the mobile stations and the external packet data networks (PDN).
- There are 2 types of support nodes which are given below:

Serving GPRS Support Node (SGSN)

- A SGSN is at the same hierarchical level as the MSC. Whatever functions MSC does for the voice, SGSN does the same for packet data.
- SGSN's tasks include packet switching, routing and transfer, mobility management, logical link management, and authentication and charging functions.
- SGSN processes registration of new mobile subscribers and keeps a record of their location inside a given service area.
- The location register of the SGSN stores location information and uses profiles of all GPRS users registered with the SGSN.

- SGSN sends queries to HLR to obtain profile data of GPRS subscribers. The SGSN is connected to the base station system with Frame Relay.

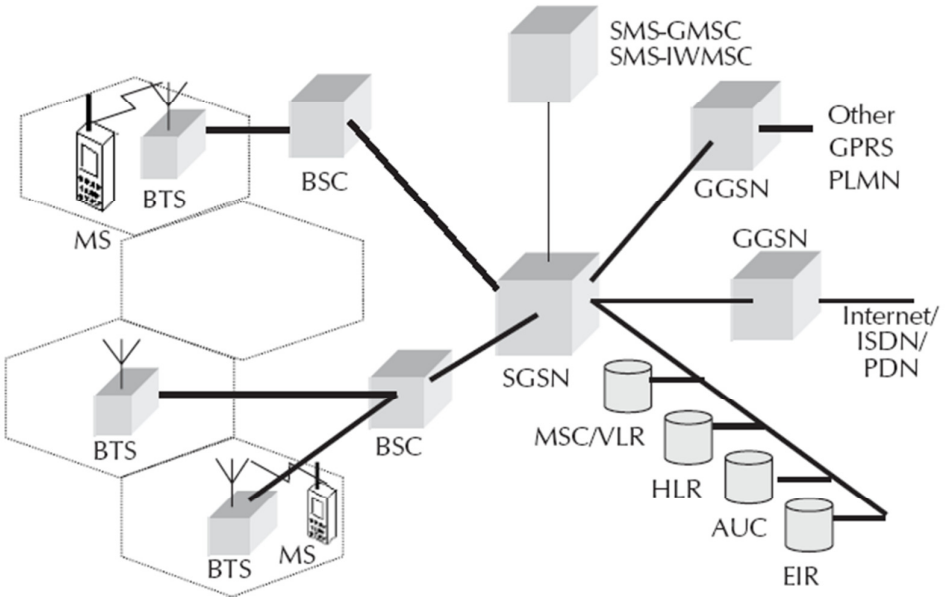


Figure 1: GPRS Architecture

Abbreviation:

AUC	**Authentication Center**	**MS**	**Mobile Station**
BSC	**Base Station Controller**	**MSC**	**Mobile Switching Center**
BTS	**Base Transceiver Station**	**PDN**	**Packet Data Network**
EIR	**Equipment Identity Register**	**PLMN**	**Public Land Mobile Network**
GGSN	**Gateway GPRS Support Node**	**SMSC**	**Short Message Service Center**
GPRS	**General Packet Radio Service**	**SMS-GMSC**	**SMS Gateway MSC**
HLR	**Home Location Register**	**SMS-IWMSC**	**SMS Inter-Working MSC**
ISDN	**Integrated System Digital Network**	**SGSN**	**Serving GPRS Support Node**

Gateway GPRS Support Node (GGSN)

- A GGSN acts as an interface between the GPRS backbone network and the external packet data network.
- GGSN's function is similar to that of a router in a LAN. GGSN maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations.
- It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like internet or X.25, PDP sends these packets out on the corresponding packet data network.
- The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register.
- GGSN also performs authentication and charging functions related to data transfer.

Some existing GSM network elements must be enhanced in order to support packet data. These are as following:

Base Station System (BSS)

- BSS system needs enhancements to recognize and send packet data.
- This includes BTS upgrade to allow transportation of user data to the SGSN.
- Also, the BTS needs to be upgraded to support packet data transportation between the BTS and the MS (Mobile Station) over the radio.

Home Location Register (HLR)

- HLR needs enhancement to register GPRS user profiles and respond to queries originating from GSNs regarding these profiles.

Mobile Station (MS)

- The mobile station or the mobile phone for GPRS is different from that of GSM.

SMS Nodes

- SMS-GMSCs and SMS-IWMSCs are upgraded to support SMS transmission via the SGSN.0
- Optionally, the MSC/VLR can be enhanced for more efficient coordination of GPRS and non-GPRS services and functionality.
- GPRS uses two frequency bands at 45 MHz apart; viz., 890-915 MHz for uplink (MS to BTS), and 935-960 MHz for downlink (BTS to MS).

Applications of GPRS

- **Communications:** E-mail, fax, unified messaging and intranet/internet access, etc.
- **Value-added services:** Information services and games, etc.
- **E-commerce**: Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications:** Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- **Vertical applications:** Freight delivery, fleet management and sales-force automation.
- **Advertising:** It may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

3. Draw and Explain Transmission Plane Protocol Architecture of GPRS.

- Figure shows the protocol architecture of the GPRS transmission plane, providing transmission of user data and its associated signaling.
- The transmission plane consists of a layered protocol structure providing user data transfer, along with associated procedures that control the information transfer such as flow control,

error detection, and error correction. Figure shows the layered protocol structure between the MS and the GGSN.

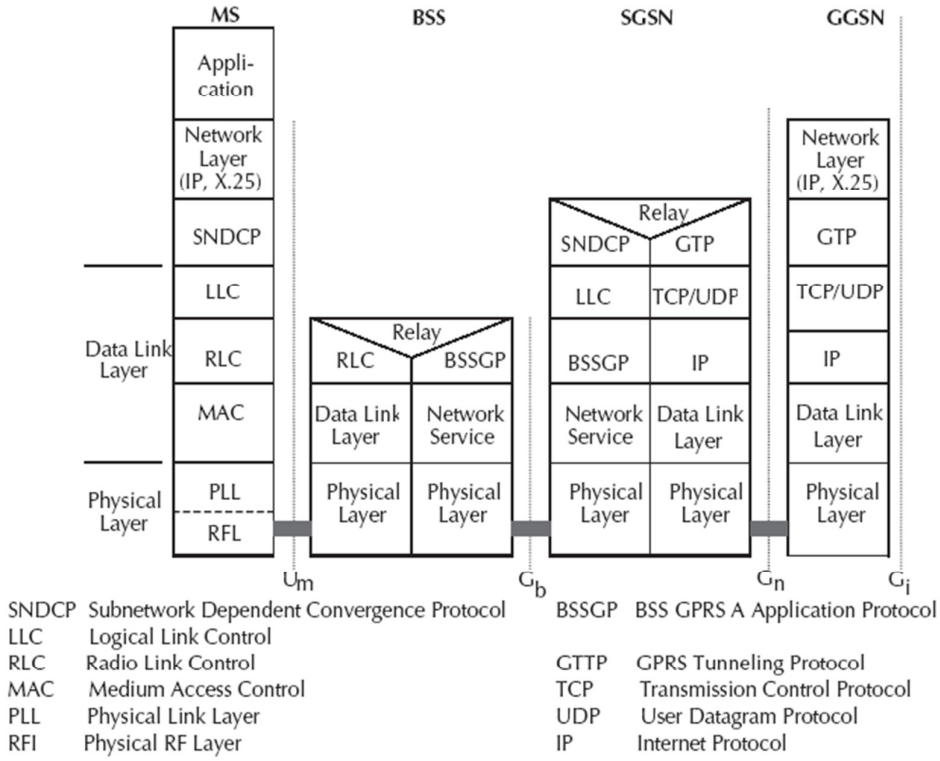


Figure 2: Transmission Plane and GPRS Protocol Stack

Air Interface

- The air interface is located between the MS and the BSS. The protocols used on the air interface are as follows:
    - **Radio link control/medium access control** (RLC/MAC): RLC provides a reliable radio link between the mobile and the BSS.
    - MAC controls the access signaling procedures to the GPRS radio channel, and the multiplexing of signaling and RLC blocks from different users onto the GSM physical channel.
    - **GSM-RF layer:** It is the radio subsystem that supports a certain number of logical channels.
    - This layer is split into two sub layers: the radio frequency layer (RFL), which handles the radio and baseband part (physical channel management, modulation, demodulation, and transmission and reception of radio blocks), and the physical link layer (PLL), which manages control of the RFL (power control, synchronization, measurements, and channel coding/decoding).
- A relay function is implemented in the BSS to relay the LLC PDUs between the air interface and the Gb interface.

Gb Interface

- The Gb interface is located between the SGSN and the BSS. It supports data transfer in the transmission plane. The Gb interface supports the following protocols:
    - **BSS GPRS protocol (BSSGP):** This layer conveys routing and QoS-related information between the BSS and SGSN.
    - **Network service (NS):** It transports BSSGP PDUs and is based on a frame relay connection between the BSS and SGSN.
- A relay function is implemented in the SGSN to relay the packet data protocol (PDP) PDUs between the Gb and Gn interfaces.

Gn/Gp Interface

- The Gn interface is located between two GSNs (SGSN or GGSN) within the same PLMN, while the Gp interface is between two GSNs in different PLMNs.
- The Gn/Gp interface is used for the transfer of packets between the SGSN and the GGSN in the transmission plane. The Gn/Gp interface supports the following protocols:
    - **GPRS tunnelling protocol (GTP):** This protocol tunnels user data between the SGSN and GGSN in the GPRS backbone network. GTP operates on top of UDP over IP. The layers L1 and L2 of the Gn interfaces are not specified in the GSM/GPRS standard.
    - **User datagram protocol (UDP):** It carries GTP packet data units (PDUs) in the GPRS Core Network for protocols that do not need a reliable data link (e.g., IP).
    - **Internet protocol (IP):** This is the protocol used for routing user data and control signaling within the GPRS backbone network.

Interface between MS and SGSN

- This interface supports the following protocols:
    - **Subnetwork-dependent convergence protocol (SNDCP):** This protocol maps the IP protocol to the underlying network. SNDCP also provides other functions such as compression, segmentation, and multiplexing of network layer messages.
    - **Logical link control (LLC):** This layer provides a highly reliable logical link that is independent of the underlying radio interface protocols. LLC is also responsible for the GPRS ciphering.

4. Write a note on PDP context activation procedure with respect to GPRS.

- In GPRS network, MS registers itself with SGSN through a GPRS attach which establishes a logical link between the MS and the SGSN.
- To exchange data packets with external PDNs after a successful GPRS attach, an MS must apply for an address which is called **PDP (Packet Data Protocol) address**.

- For each session, a PDP context is created which contains PDP type (e.g. IPv4), PDP address assigned to the mobile station (e.g. 129.187.222.10), requested QoS and address of the GGSN that will function as an access point to the PDN.
- Such a context is stored in MS, SGSN and GGSN while with an active PDP context; the MS is 'visible' to the external PDN.
- A user may have several simultaneous PDP contexts active at a given time and user data is transferred transparently between MS and external data networks.
- Allocation of the PDP address can be static or dynamic.
- In case of static address, the network operator permanently assigns a PDP address to the user while in other case, a PDP address is assigned to the user upon the activation of a PDP context.
- Using the message **"activate PDP context request"**, MS informs the SGSN about the requested PDP context and if request is for dynamic PDP address assignment, the parameter PDP address will be left empty.

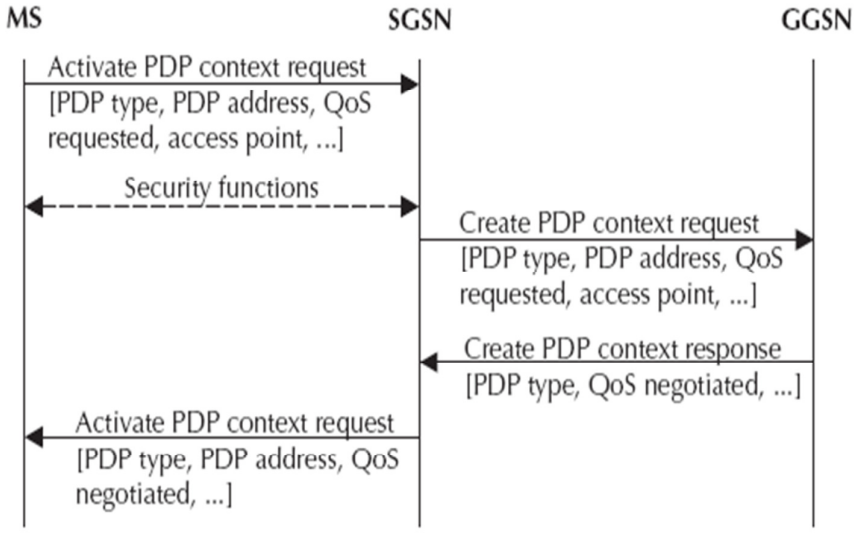


Figure 3: PDP Context Activation

- After necessary security steps, if authentication is successful, SGSN will send a 'create PDP context request' message to the GGSN, the result of which is a confirmation message 'create PDP context response' from the GGSN to the SGSN, which contains the PDP address.
- SGSN updates its PDP context table and confirms the activation of the new PDP context to the MS.
- Disconnection from the GPRS network is called GPRS detach in which all the resources are released.

5. How the packets are routed in GPRS. Explain GPRS packet routing for Inter & Intra PLMN.

- Routing is the process of how packets are routed in GPRS.

- Here, the example assumes two intra-PLMN backbone networks of different PLMNs. Intra-PLMN backbone networks connect GSNs of the same PLMN or the same network operator.
- These intra-PLMN networks are connected with an inter-PLMN backbone while an inter-PLMN backbone network connects GSNs of different PLMNs and operators. However, a roaming agreement is necessary between two GPRS network providers.

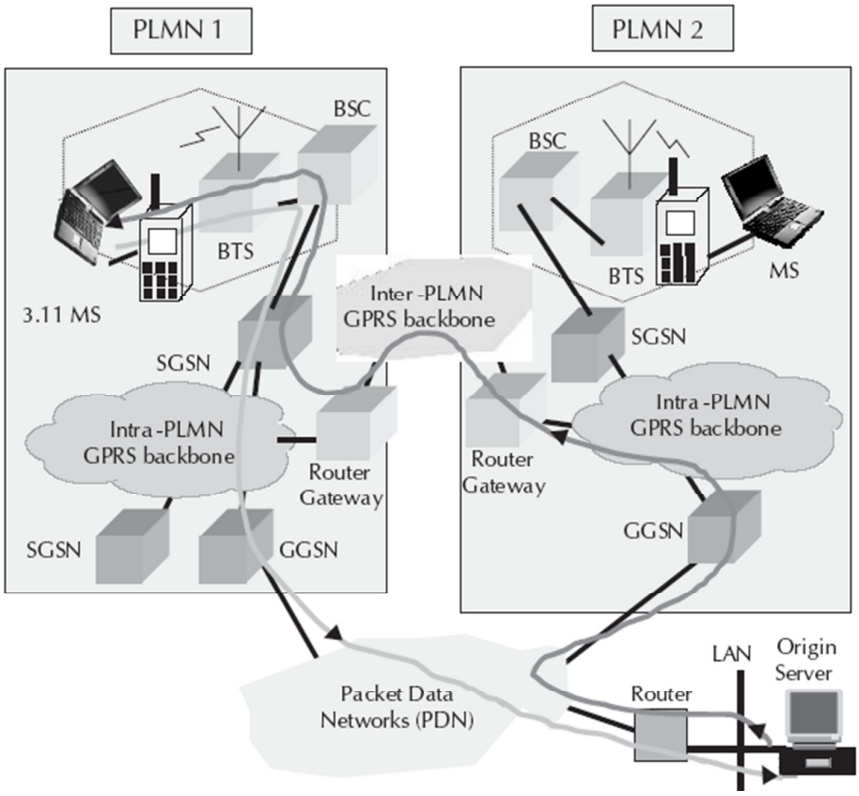


Figure 4: GPRA Packet Routing

- Gateways between PLMNs and external inter-PLMN backbone are called border gateways which perform security functions to protect the private intra-PLMN backbones against malicious attacks.
- Let's say that GPRS MS located in PLMN1 sends IP packets to a host connected to the IP network (e.g. to a Web server connected to the Internet).
- SGSN that the MS is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN.
- GGSN de-encapsulates the packets and sends them out on the IP network, where IP routing mechanisms are used to transfer the packets to the access router of the destination network and finally, delivers the IP packets to the host.
- Let us also say that home-PLMN of the mobile station is PLMN2.

- An IP address has been assigned to MS by the GGSN of PLMN2 and so, MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2.
- Correspondent host is now sending IP packets to the MS onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1.
- It encapsulates the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1 while the SGSN de-encapsulates the packets and delivers them to the MS.
- HLR stores the user profile, the current SGSN address and the PDP addresses for every GPRS user in the PLMN.
- When the MS registers with a new SGSN, HLR will send the user profile to the new SGSN.
- Signaling path between GGSN and HLR may be used by the GGSN to query a user's location and profile in order to update its location register.

6. Data services in GPRS

- Any user is likely to use either of the two modes of the GPRS network:
  - Application mode
  - Tunneling mode
- In **application mode**, user uses the GPRS mobile phone to access the applications running on the phone itself. The phone here acts as the end user device.
- In **tunneling mode**, user uses GPRS interface as an access to the network as the end user device would be a large footprint device like laptop computer or a small footprint device like PDA.
- The mobile phone will be connected to the device and used as a modem to access the wireless data network.

7. Billing and Charging in GPRS

- For voice networks tariffs are generally based on distance and time means that user pay more for long distance calls.
- On other hand, in data services, minimum charging information that must be collected are:
  - Destination and source addresses
  - Usage of radio interface
  - Usage of external Packet Data Networks
  - Usage of the packet data protocol addresses
  - Usage of general GPRS resources and location of the Mobile Station
- A GPRS network needs to be able to count packets to charging customers for the volume of packets they send and receive.
- Various business models exist for charging customers as billing of services can be based on the transmitted data volume, the type of service, the chosen QoS profile, etc.

- GPRS call records are generated in the GPRS Service Nodes.
- Packet counts are passed to a Charging Gateway that generates Call Detail Records that are sent to the billing system.

8. Write a short note on limitations of GPRS.

- A GPRS is a new enabling mobile data service which offers a major improvement in spectrum efficiency, capability and functionality compared with today's non-voice mobile services.
- However, it is important to note that there are some limitations with GPRS, which can be summarized as:

Limited Cell Capacity for All Users

- GPRS does impact a network's existing cell capacity.
- There are only limited radio resources that can be deployed for different uses - use for one purpose precludes simultaneous use for another.
- For example, voice and GPRS calls both use the same network resources. If tariffing and billing are not done properly, this may have impact on revenue.

Speeds Much Lower in Reality

- Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight timeslots without any error protection.
- Clearly, it is unlikely that a network operator will allow all timeslots to be used by a single GPRS user.
- Additionally, the initial GPRS terminals are expected be severely limited - supporting only one, two or three timeslots.
- The bandwidth available to a GPRS user will therefore be severely limited.
- The reality is that mobile networks are always likely to have lower data transmission speeds than fixed networks.

Transit Delays

- GPRS packets are sent in all different directions to reach the same destination.
- This opens up the potential for one or some of those packets to be lost or corrupted during the data transmission over the radio link.
- The GPRS standards recognize this inherent feature of wireless packet technologies and incorporate data integrity and retransmission strategies.
- However, the result is that potential transit delays can occur.

1. Explain the WAP Layered architecture and protocol stack.

- It is designed for access Internet and advanced telephony services from mobile phones
- Pays intelligent sensitivity to the constraints of these devices like small display, limited keys on the keypad, no pointer device like mouse, etc.
- WAP is designed in a layered fashion so that it can be extensible, flexible, and scalable.

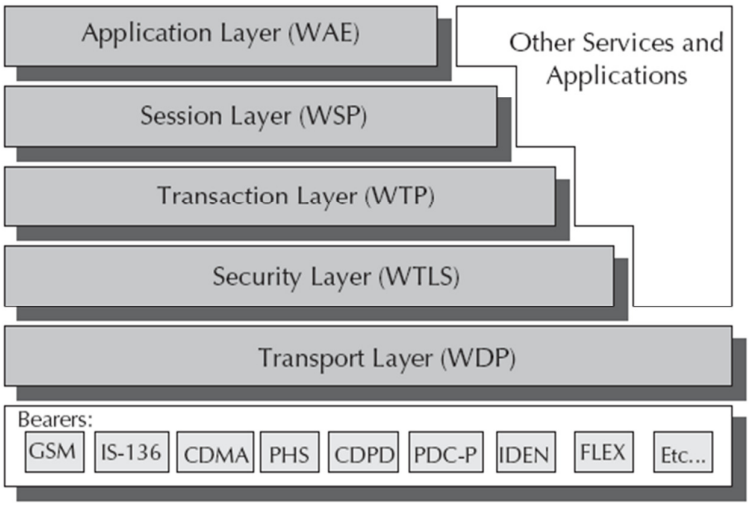


Figure 1: WAP Architecture

- WAP protocol stack is divided into five layers:
    1. Wireless Application Environment-WAE
    2. Wireless Session Protocol-WSP
    3. Wireless Transaction Protocol-WTP
    4. Wireless Transport Layer Security-WTLS
    5. Wireless Datagram Protocol-WDP

Wireless Application Environment

- This layer is of most interest to content developers because it contains, among other things, device specifications and the content development programming languages, WML and WMLScript.
- WAE architecture allows all content and services to be hosted on standard web servers when all content is located using WWW standard URLs.
- WAE consists of:
- **User agent** which is the browser or a client program.
- **Wireless Markup Language (WML)** which is a lightweight markup language optimized for use in wireless devices.
- **WMLScript** which is a lightweight client side scripting language.

- **Wireless Telephony Application:** Telephony services and programming interfaces.
- **WAP Push Architecture** which allow for mechanisms to allow origin servers to deliver content to the terminal without the terminal requesting for it.
- **Content formats:** Sets of data formats.

Wireless Session Protocol

- Unlike HTTP, WSP has been designed by the WAP forum to provide fast connection suspension and reconnection.
- WSP provides a consistent interface between two session services like client and server.
- WSP offers both connection oriented and connectionless service.

Wireless Transaction Protocol

- WTP runs on top of a datagram service such as user datagram protocol and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Wireless Transport Layer Security

- WTLS incorporates security features which are based upon the established transport layer security protocol standard.
- It includes data integrity checks, privacy, service denial of services protection.

Wireless Datagram Protocol

- The WDP is transport layer protocol in WAP architecture. WDP operates above data capable bearer services supported by various network type general transport services.
- The WDP allows WAP to be bearer independent by adapting the transport layer of the underlying bearer.
- The WDP presents a consistent data format to layer of the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

2. What is WAE? Draw its model with client, gateway and server.

- Primary objective of WAE is to provide an interoperable environment to build services in wireless space.
- Content is transported using standard protocols in the WWW domain and an optimized HTTP like protocol in the wireless domain.
- WAE architecture allows all content and services to be hosted on standard Web servers when all content is located using WWW standard URLs.
- WAE enhances some of the WWW standards to reflect some of the telephony network characteristics.
- User Agent is the user facing browser software, while in WAE this is generally referred to as micro-browser.

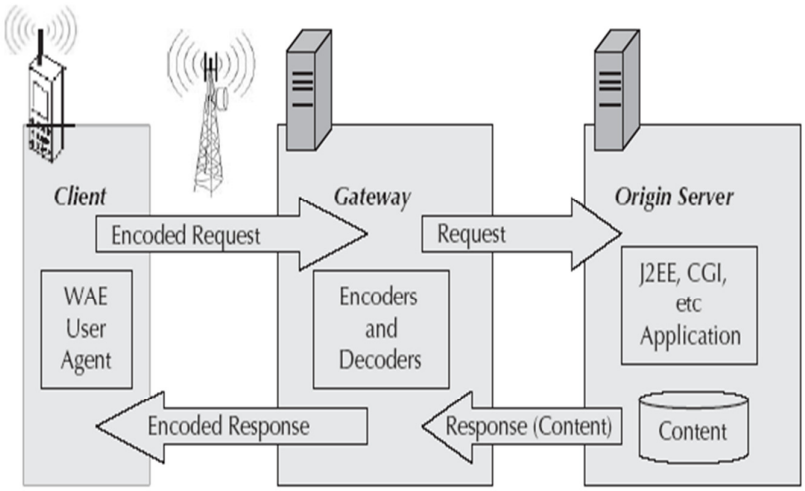


Figure 2: Wireless Application Environment

- WAE only defines fundamental services and formats that are needed to ensure interoperability among implementations and different layers.
- User Agent Profile (UAProf) specification allows WAP to notify the content server about the device capability.
- Devices that support UAProf architecture provide a URL in the WAP or HTTP session header which points to a XML file that describes the profile of that device which is used to deliver the content to best suit the terminal's capabilities.

3. Explain MMS architecture and transaction flow in MMS.

- Multimedia Messaging Service can contain formatted text, graphics, data, animations, images, audio clips, voice transmissions and video sequences.
- Two standards bodies producing specifications relating to MMS messages: WAP Forum and the 3GPP.
- Standards from the WAP Forum specify how messages are composed and packaged whereas standards from the 3GPP specify how messages are sent, routed and received.
- Layout and ordering of the slides are specified through a language called Synchronization Multimedia Integration Language (SMIL).
- Multimedia Message Service Environment (MMSE) encompasses various elements required to deliver a MMS and includes:
- **MMS Client** - This is the entity that interacts with the user. It is an application on the user's wireless device.
- **MMS Relay** - This is the system element that the MMS client interacts with. It provides access to the components that provide message storage services.
- It is responsible for messaging activities with other available messaging systems. The SMS relay along with the MMS content server is referred to as MMS Controller (MMSC).

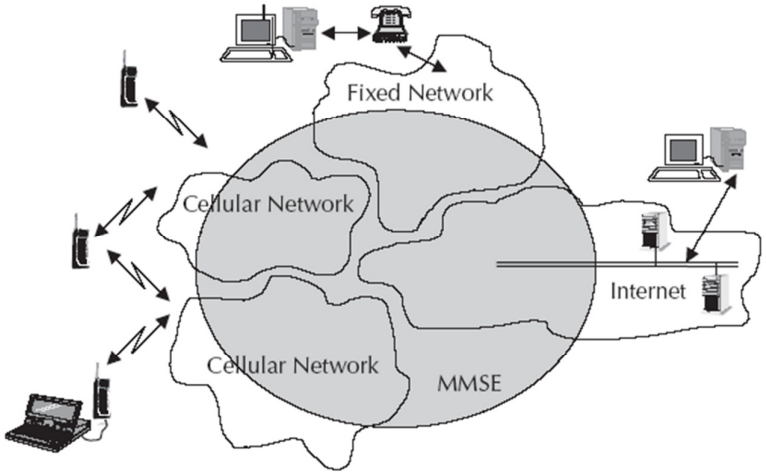


Figure 3: MMS Architecture

- **WAP Gateway** - It provides standard WAP services needed to implement MMS.
- **MMS Server** - This is the content server where the MMS content is generated.
- **Email Server** - MMS can integrate seamlessly to the email system of Internet.
- Messages that transit between the MMS Client and MMS Relay pass through WAP Gateway.
- Data is transferred between the MMS client and WAP gateway using WAP Session Protocol (WSP). Data is transferred between the WAP gateway and the MMS Relay using HTTP.

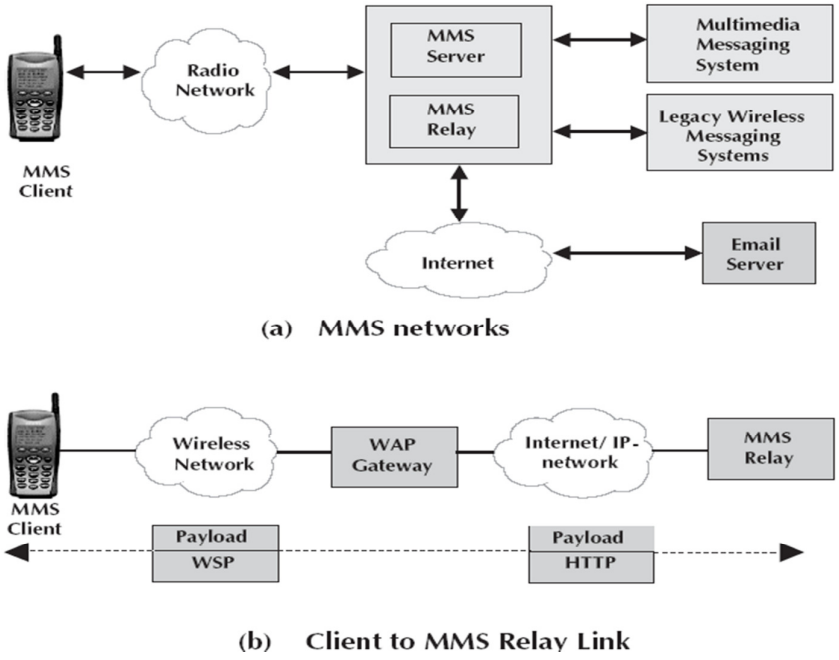


Figure 4: MMS Environment

- MMS service is realized by the invocation of transactions between the MMS Client and the MMS Relay.

- General transactions of sending and retrieving messages do not depend on what type of client the message is sent to or MMS service is realized by the invocation of transactions between the MMS Client and the MMS Relay.

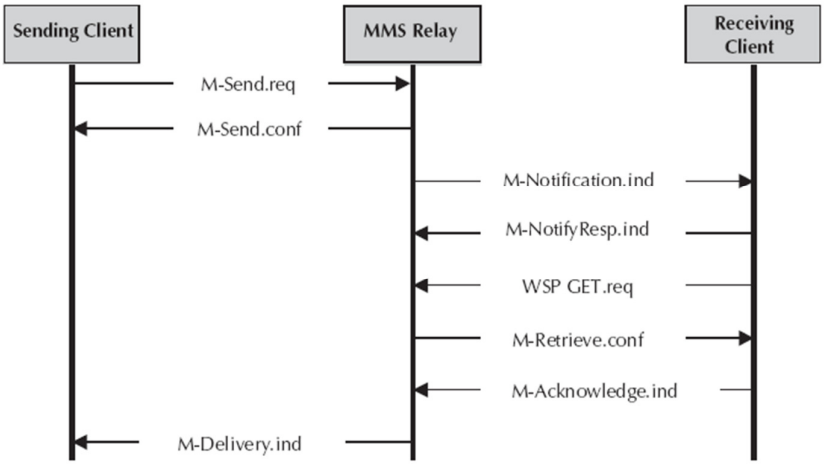


Figure 5: MMS Transaction Flow

- The general transactions of sending and retrieving messages do not depend on what type of client the message is sent to or received from.
- The other endpoint for the message may be another MMS Client or a client on a legacy wireless messaging system or it may even be an email server.

4. What is CDMA technology? Explain the Direct Sequence Spread Spectrum Techniques.

- Mobile phone technology had a reincarnation from first generation analogue (using FDMA) to second generation digital (using TDMA).
- The next incarnation is from second generation digital TDMA to third generation packet (using CDMA).
- CDMA is a specific modulation technique of Spread-Spectrum technology.
- Third generation or 3G is more of a generic term to mean mobile networks with high bandwidth.
- In a conventional transmission system, the information is modulated with a carrier signal and then transmitted through a medium.
- When that transmitted, all the power of the signal is transmitted centered around a particular frequency. This frequency represents a specific channel and generally has a very narrow band.
- In spread-spectrum we spread the transmission power over the complete band as shown in figure.

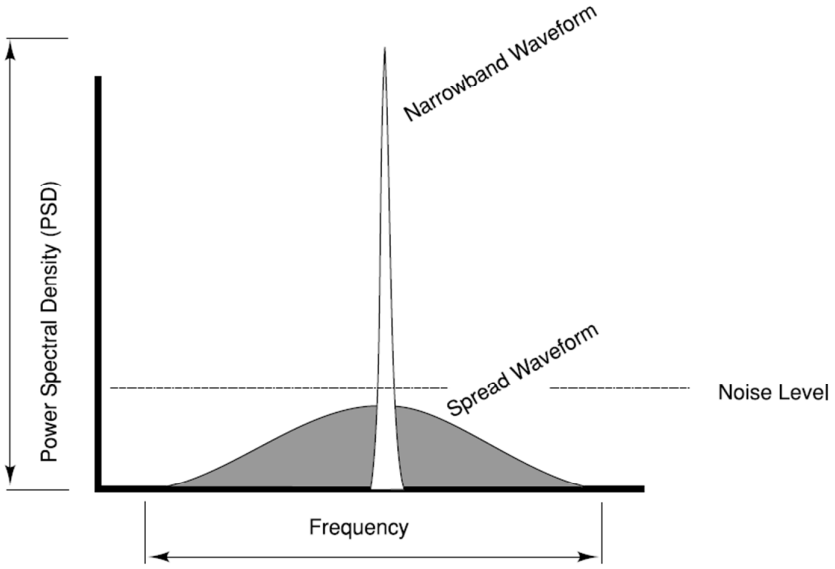


Figure 6: Spread Spectrum Technology

- In spread-spectrum the transmission signal bandwidth is much higher than the information bandwidth.
- There are numerous ways to cause a carrier to spread; however, all spread-spectrum systems can be viewed as two steps modulation processes.
- First, the data to be transmitted is modulated.
- Second, the carrier is modulated by the spreading code, causing it to spread out over a large bandwidth.

Different Spreading Techniques

- **Direct Sequence (DS):** DS spread spectrum is typically used to transmit digital information.
- A common practice in DS systems is to mix the digital information stream with a pseudo random code.
- **Frequency Hopping (FH):** Frequency hopping is a form of spreading in which the center frequency of a conventional carrier is altered many times within a fixed time period (like one second) in accordance with a pseudo-random list of channels.
- **Chirp**: The third spreading method employs a carrier that is swept over a range of frequencies.
- This method is called chirp spread spectrum and finds its primary application in ranging and radar systems.
- **Time Hopping**: The last spreading method is called time hopping. In a time-hopped signal, the carrier is on-off keyed by the pseudo-noise (PN) sequence resulting in a very low duty cycle.
- The speed of keying determines the amount of signal spreading.

- **Hybrid System:** A hybrid system combines the best points of two or more spread-spectrum systems. The performance of a hybrid system is usually better than can be obtained with a single spread-spectrum technique for the same cost.
- The most common hybrids combine both frequency-hopping and direct-sequence techniques.
- Amateurs and business community are currently authorized to use only two spreading techniques. These are frequency hopping and direct sequence techniques.
- Rest of the Spread-Spectrum technologies are classified and used by military and space sciences.

5. Define Direct Sequence Spread Spectrum DSSS.

- Direct Sequence Spread Spectrum (DSSS) is often compared to a party, where many pairs are conversing, each in a different language.
- Each pair understands only one language and therefore, concentrates on his or her own conversation, ignoring the rest.
- A Hindi-speaking couple just homes on to Hindi, rejecting everything else as noise.
- Its analogous to DSSS is when pairs spread over the room conversing simultaneously, each pair in a different language. The key to DSSS is to be able to extract the desired signal while rejecting everything else as random noise.
- The analogy may not be exact, because a roomful of people all talking at once soon becomes very loud.
- In general, Spread-Spectrum communications is distinguished by three key elements:
    1. The signal occupies a bandwidth much larger than what is necessary to send the information.
    2. The bandwidth is spread by means of a code, which is independent of the data.
    3. The receiver synchronizes to the code to recover the data. The use of an independent code and synchronous reception allows multiple users to access the same frequency band at the same time.
- In order to protect the signal, the code used is pseudo-random, which makes it appear random while being actually deterministic, which enables the receivers to reconstruct the code for synchronous detection. This pseudo-random code is also called pseudo-noise (PN).
- DSSS allows each station to transmit over the entire frequency all the time. DSSS also relaxes the assumption that colliding frames are totally garbled. Instead, it assumes that multiple signals add linearly.
- DSSS is commonly called Code Division Multiple Access or CDMA in short.
- Each station is assigned a unique m-bit code. This code is called the CDMA chip sequence. To transmit a 1 bit, the transmitting station sends its chip sequence, whereas to send 0, it sends the complement chip sequence.

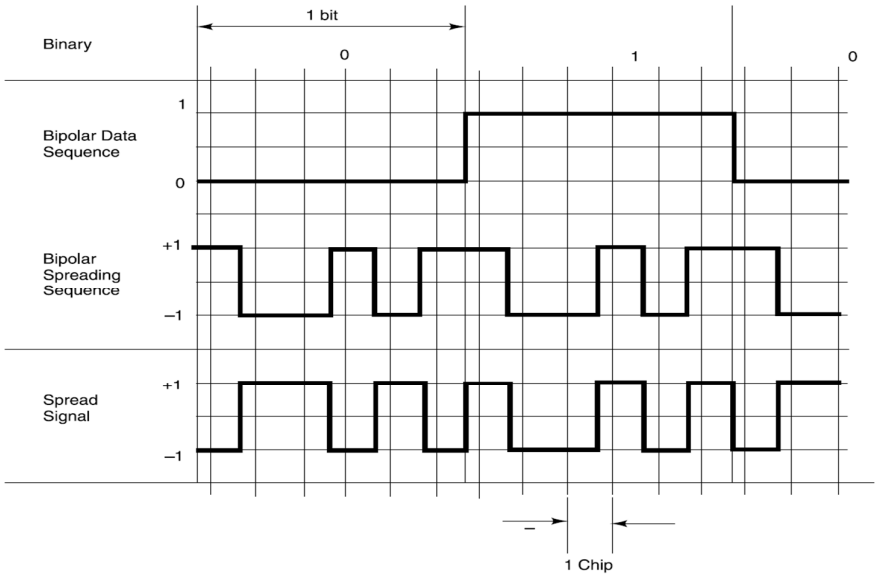


Figure 7: CDMA Chip Sequence

- Thus, if station A is assigned the chip sequence 00011011, it sends bit 1 by sending 00011011 and bit 0 by sending 11100100.

Using bipolar notations, we define bit 0 as +1 and bit 1 as –1. The bit 0 for station A will now become (–1, –1, –1, +1, +1, –1, +1, +1) and 1 becomes (+1, +1, +1, –1, –1, +1, –1, –1). The figure depicts this with 6 chips/bit (011010).

6. List and discuss at least seven functions where CDMA is different from GSM.

Functions	GSM	CDMA(IS-95)
Frequency	900MHz; 1800MHz;1900MHz	800MHz;1900MHz
Channel Bandwidth	Total 25 MHz bandwidth with 200 KHz per channels, 8 timeslots per channel with frequency hopping.	Total 12MHz with 1.25 MHz for the spread spectrum.
Voice Codec	13Kbits/second	8Kbits/second or 13Kbps
Data bit rate	9.6 Kbits/second or expandable	9.6Kbits
SMS	160 characters of text supports	120 characters
SIM Card	Yes	No
Multipath	Causes interference and destruction to service	Used as an advantage
Radio Interface	TDMA	CDMA
Handoff	Hard	Soft
System Capacity	Fixed and limited	Flexible and higher than GSM

7. Discuss 3G versus Wifi

Functions	3G	Wi-Fi
Radio Interface	Uses spread spectrum as the modulation technique.	Uses spread spectrum as the modulation technique.
Genesis	Evolved from voice network where QoS is a critical success factor.	Evolved from data network where QoS is not a critical success factor.
Bandwidth	It supports broadband data service of up to 2Mbps.	Wi-Fi supports broadband data service of up to 54Mbps.
Status of standards	For 3G, there is a relatively small family of internationally sanctioned standards, collectively referred to as IMT-2000.	It is one of the families of continuously evolving 802.11x wireless standards that are under development.
Access Technologies	Access or edge-network facility. The wireless link is from the end-user device to the cell base station, which may be at a distance of up to a few kilometers.	Access or edge-network facility. The wireless link is a few hundred feet from the end-user device to the base station.
Business models/deployment are different	Service providers own and manage the infrastructure. End customers typically have a monthly service contract with the 3G service provider to use the network.	Users' organization owns the infrastructure. Following the initial investment, the usage of the network does not involve an access fee.
Roaming	It will offer well-coordinated continuous and ubiquitous coverage.	Seamless ubiquitous roaming over Wi-Fi cannot be guaranteed as network growth is unorganized.

8. What is 3G? List applications on 3G

- The term 3G internet refers to the third generation of mobile phone standards, as set by the International Telecommunications Union (ITU).
- 3G technologies allow mobile operators to offer more service options to their users, including mobile broadband.
- 3G broadband offers greater flexibility and services by making more efficient use of mobile bandwidth than its predecessor 2G.
- Devices in 3G can work in multiple ways. They can run in a tunneling mode or in an application mode.
- **In tunneling mode**, the device works more as a pass through device or a modem. In this mode, the mobile phone is connected to another device like a laptop and functions as a wireless media interface. The intelligence of the phone is not used, only the communication interface of the phone is used.

- **In an application mode**, applications run on the phone itself. A 3G mobile phone will support, SMS, WAP, Java, etc. (MExE classmark 3). A MExE classmark 3 mobile device will have an execution environment that will allow application development for the client device.

Applications on 3G

- In 3G, there will be different types of client applications: Local, Occasionally connected, Online and Real-time.
- Games, cartoons and similar applications are examples of local applications. These applications can be downloaded over the air and used offline.
- In an occasionally connected computing (OCC) environment, the user will connect to the network occasionally. Downloading and uploading of emails are the best examples of OCC.
- Online applications will be the corporate applications. Examples of such applications will be online order booking or updating of inventory status.
- Real-time applications could be real-time stock updates or applications for law-enforcement agents for real-time tracking or navigational systems.
- Few 3G specific applications are:
    - **Virtual Home Environment (VHE)** – Virtual Home Environment can be defined as a concept where an environment is created in a foreign network (or home network outside the home environment).
    - So, that the mobile users can experience the same computing experience as they have in their home or corporate computing environment while they are mobile and roaming.
    - **Personal Communication Networks (PCN)** – These are digital telephone networking infrastructures, which supports personal numbering, individual service selection, and moves towards unified billing and call anytime, anywhere through wireless digital telephony.
    - **Universal Subscriber Identity Module (USIM)** – This is the smart card for third generation mobile phones. A SIM card in the mobile phone offers portability, security and individuality.
    - **Audio/Video** – Third generation applications will be used to download music, multimedia, news, etc.
    - **VoIP**
    - **Electronic Agents** – Electronic agents are defined as “mobile programs that go places in the network to carry out their owners’ instructions. They can be thought of as extensions of the people who dispatch them.”
    - **Downloading of Software and Content**
    - **ENUM** – ENUM is a protocol that is emerging from work of Internet Engineering Task Force’s (IETF’s) Telephone Number Mapping working group.

9. What is Wireless LAN? Give advantages and dis-advantage. Also mention goal of WLAN

- Wireless is a local area data network without any physical connectivity like without wires.
- WLAN is implemented as an extension to a wired LAN within a building or campus.
- Wireless LAN is referred as Wireless Fidelity(Wi-Fi)
- Typically restricted in their diameter: buildings, campus, single room etc...
- The global goal is to replace office cabling and to introduce high flexibility for ad hoc communication (e.g. Group meetings).

Wireless LAN advantages:

- **Mobility:** WLAN offers wire-free access within operating range.
- **Low Implementation Costs:** WLAN is easy to setup, relocate, change and low cost.
- **Installation Speed and Simplicity:** Fast and simple installation of WLAN.
- **Network Expansion:** Easy expansion of WLAN possible.
- **Higher**
- **Flexibility**: within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls.
- **Planning**: wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.
- **Robustness**: wireless networks can survive disasters; if the wireless devices survive people can still communicate.

Wireless LAN disadvantages

- **QoS**: WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission (1- 10 Mbit/s) and higher error rates due to interference.
- **Cost**: Ethernet adapter vs. wireless LAN adapters.
- **Proprietary solutions**: slow standardization procedures lead to many proprietary solutions only working in a homogeneous environment.
- **Safety and security**: using radio waves for data transmission might interfere with other high-tech equipment.

Wireless LAN: Main Design Goals

- **Global operation**: LAN equipment may be carried from one country to another and this operation should be legal (frequency regulations national and international).
- **Low power**: take into account that devices communicating via WLAN is typically running on battery power. Special power saving modes and power management functions.
- **Simplified spontaneous co-operation**: no complicated setup routines but operate spontaneously after power.

- **Easy to use**: WLANs are made for simple users; they should not require complex management but rather work on a plug-and-play basis.
- **Protection of investment**: a lot of money has been invested for wired LANs; WLANs should be able to interoperate with existing network (same data type and services).
- **Safety and security**: safe to operate. Encryption mechanism, do not allow roaming profiles for tracking people (privacy)
- **Transparency for applications**: existing applications should continue to work.

10. List types of wireless LAN. Differentiate between Ad hoc verses infrastructure mode.

- Types of Wireless LAN are:
  - 802.11
  - HyperLAN
  - HomeRF
  - Bluetooth
  - MANET

Adhoc vs. Infrastructure Mode

- In Adhoc mode, there is no access point or infrastructure.
- A number of mobile stations from a cluster communicate with each other.

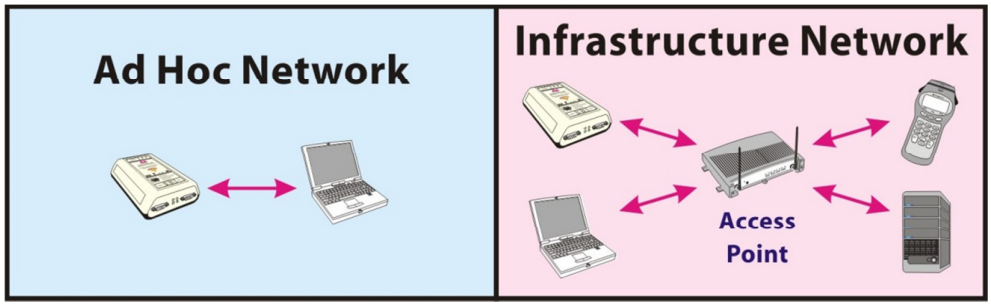


Figure 8: Adhoc Mode vs. Infrastructure Mode

- In infrastructure mode, the mobile station-MS are connected to a abase station or access point.
- This is similar to a star network where all the mobile stations are attached to the base station.
- Through a protocol the base station manages the dialogue between the AP and MS.

11. List Wireless LAN security issues and what do you understand by hidden & exposed terminal problem in wireless LAN.

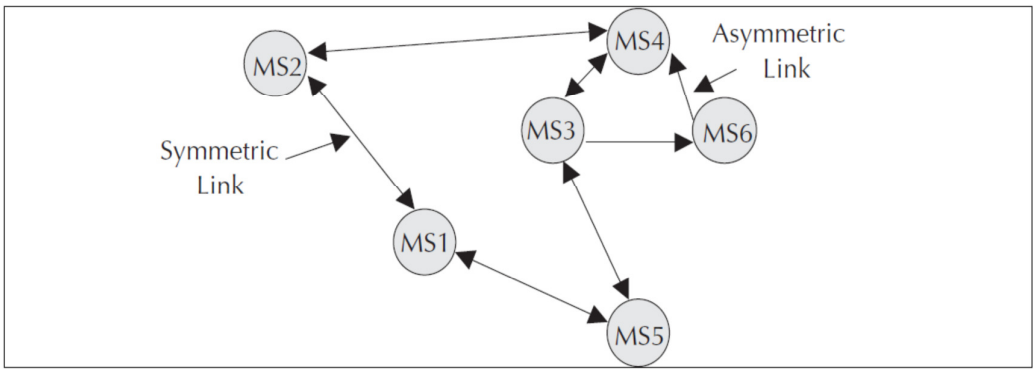
- IEEE 802.11 includes several security features:

  - Open system and shared key authentication modes
  - Service set identifiers-SSID
  - Wired Equivalent Privacy-WEP
- Security: A message transferred through wireless communication can be intercepted without physical access by any one.
- Any person, sitting in the vicinity of a WLAN with a transceiver with a capability to listen/talk, can pose a threat.
- Unfortunately, the same hardware or algorithms that are used for WLAN communication can be employed for such attacks. To make the WLANs reliable the following security goals were considered:
  - Confidentiality
  - Data Integrity
  - Access Control

- And following security measures are a part of the 802.11 IEEE protocol:
  - Authentication
  - Association
  - Encryption
- For communication purpose in wireless environment, the client should be authenticated person, and then only he or she may be able to associate with other client and the data that is to be transferred between two clients should be sent in encrypted form.

12. Explain MANET (Mobile ad-hoc Network) and issues with moving node in network. OR Define mobile ad-hoc networks. Discuss its characteristics and limitations.

- A Mobile ad-hoc Network (MANET) is an autonomous system of mobile stations connected by wireless links to form a network.
- This network can be modeled in the form of an arbitrary graph.
- Ad-hoc networks are peer-to-peer, multihop networks where data packets are transmitted from a source to destination via intermediate nodes.
- Intermediate nodes serve as routers in this case. In an ad-hoc network there will be situations when some of the nodes could be out of range with respect to some other nodes.
- When this happens, the network needs to reconfigure itself and ensure that the paths between two nodes are available.
- In an ad-hoc network, communication links could be either symmetric or asymmetric.
- To design a good wireless ad-hoc network be it a sensor network or an information network, we need to account for various issues and challenges. These are:-



- **Limited Security**: Wireless networks are vulnerable to attack. Mobile ad-hoc networks are more vulnerable as by design any node should be able to join or leave the network any time. This requires flexibility and higher openness.
- **Bandwidth Limited**: Wireless networks in general are bandwidth limited. In an ad-hoc network it is all the more so because there is no backbone to handle or multiplex higher bandwidth.
- **Routing**: Routing in a mobile ad-hoc network is complex. This depends on many factors, including finding the routing path, selection of routers, topology, protocol, etc.

13. Define Wireless Sensor Network

- Wireless sensor networks are a class of ad hoc networks.
- Sensor networks are very useful in unpredictable, unreliable environments.
- Sensor networks are primarily data collection points.
- They are widely used in defense, environmental, meteorological, and study of nature.
- A wireless sensor network is a collection of low-cost, low-power disposable devices.
- Each of these devices holds sensing, memory, and communication modules.
- Study of the movement of glaciers is done through wireless ad hoc networks. Sensor networks are generally unmanned.
- Sensors may not have any power source other than small batteries. Therefore, power control is a major challenge in sensor networks to ensure long life of the network.

14. Explain the H.323 Framework for Voice over IP (VoIP). OR Do the Comparison between H.323 and SIP.

VoIP

- Voice-over-Internet-Protocol (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
- Other terms commonly associated with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB).

- VoIP systems employ session control and signaling protocols to control the signaling, set-up, and tear-down of calls.
- The transport audio streams over IP networks using special media deliver protocols that encode voice, audio, video with audio codecs, and video codecs as Digital audio by streaming media.
- VoIP is available on many smartphones, PC's, and on Internet access devices. Calls and SMS text messages may be sent over 3G or Wi-Fi.

H.323

- The H.323 is a set of protocol standards that provide a foundation for multipoint conferencing of audio, video and data communications over IP networks standardized by the ITU.

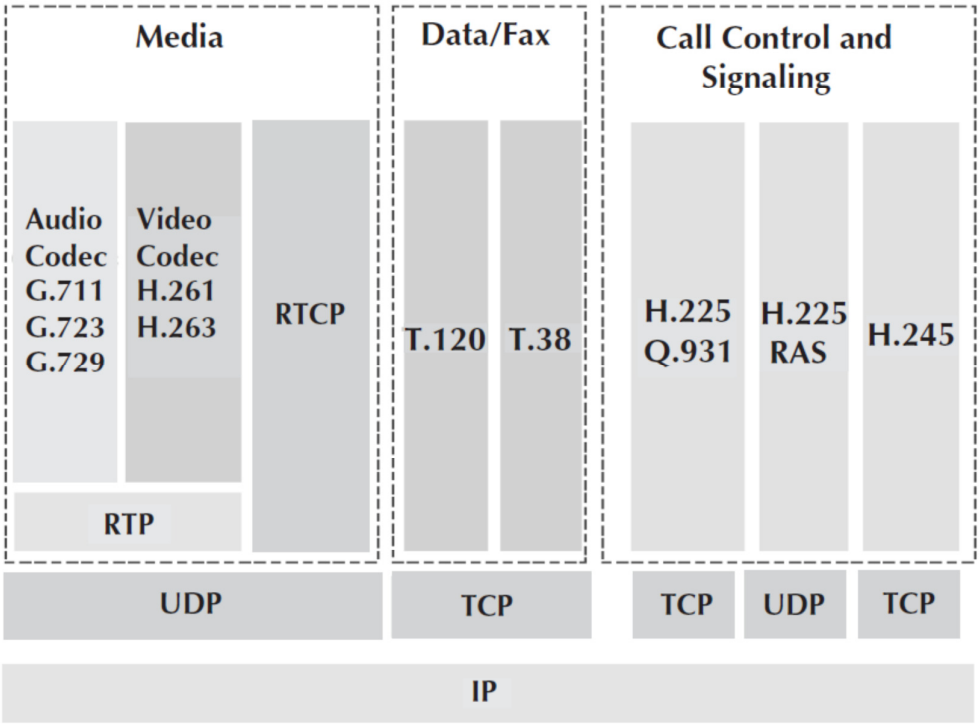


Figure 9: H.323 Umbrella Specification

- It is used for peer-to-peer, two-way delivery of real-time data. The scope of H.323 includes parts of H.225.0—RAS, Q.931, H.245 RTP/RTCP and audio/video codecs, such as the audio codecs G.711, G.723.1, G.728, etc. and video codecs like H.261, H.263 that compress and decompress media streams.
- It includes codecs for data conferencing through T.120 and fax through T.38. H.235 Specifies security and encryption for H.323 and H.245 based terminals.
- H.450.N recommendation specifies supplementary services such as call transfer, call diversion, call hold, call park, call waiting, message waiting indication, name identification, call completion, call offer, and call intrusion.
- H.246 specifies internetworking of H Series terminals with circuit switched terminals.

- In a H.323 implementation, along with the end-user devices three logical entities are required. These are Gateways, Gatekeepers and Multipoint Control Units (MCUs).
- Terminals, Gateways, and MCUs are collectively known as endpoints. It is possible to establish an H.323-enabled network with just terminals, which are H.323 clients.

Gateway

- The purpose of the gateway is to do the signal and media translation from IP to circuit switch network and vice versa.
- This includes translation between transmission formats, translation between audio and video codecs, call setup and call clearing on both the IP side and the circuit-switched network side.

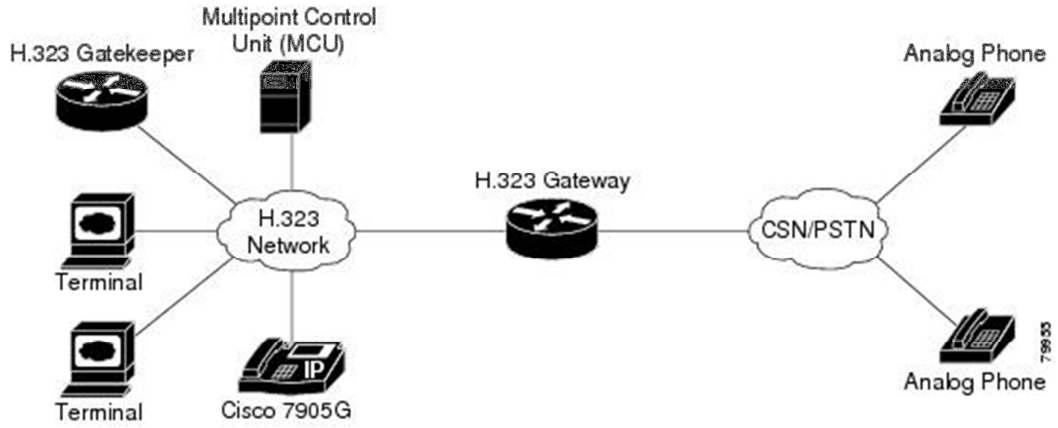


Figure 10: The H.323 Architecture

Gatekeeper

- A gatekeeper acts as the central point of control for all calls within its zone for all registered endpoints. A gatekeeper is not mandatory in an H.323 system. However, if a gatekeeper is present, terminals must use the services offered by gatekeepers. Gatekeepers perform functions like address translation and bandwidth management.
- For example, if a network has a threshold for the number of simultaneous conferences on the LAN, the gatekeeper can refuse to make any more connections once the threshold is reached.
- An optional feature of a gatekeeper is its ability to route H.323 calls. By routing a call through a gatekeeper, service providers can meter a call with an intention of charging.
- A gateway could use a gatekeeper to translate incoming E.164 addresses into IP addresses.

Multipoint Control Unit

- The Multipoint Control Unit (MCU) supports conferences between three or more endpoints. An MCU consists of a Multipoint Controller (MC) and a Multipoint Processor (MP).
- The MC handles H.245 negotiations between all terminals to determine common capabilities for audio and video processing. An MCU optionally may have one or more MPs to deal with the media streams.

- MP mixes, switches, and processes audio, video, and/or data bits.

SIP

- SIP is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.
- SIP can be used for creating, modifying and terminating sessions consisting of one or several media streams.
- SIP can be used for two-party or multiparty sessions. SIP works on conjunction with several other application layer protocols that identify and carry the session media.
- For secure transmissions of SIP messages, the protocol may be encrypted with Transport Layer Security (TLS).

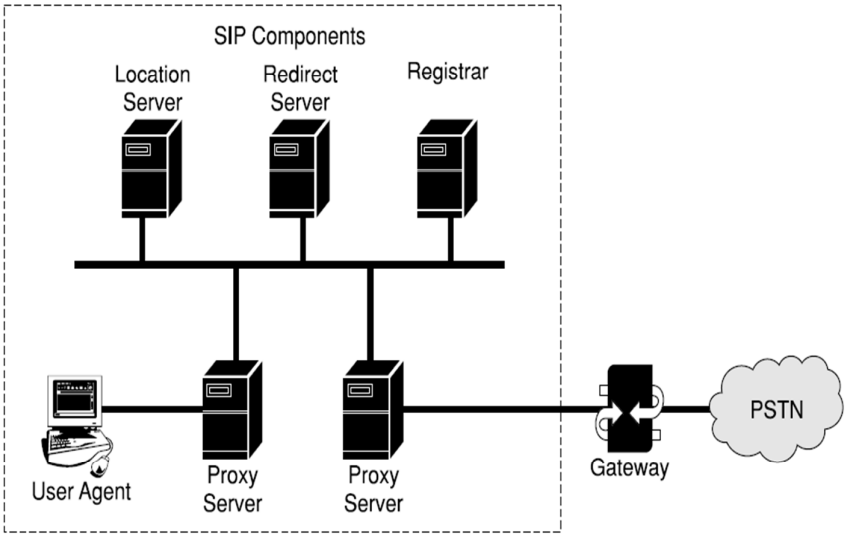


Figure 11: SIP in VoIP

- A motivating goal for SIP was to provide a signaling and call setup protocol for IP-based communications that can support a superset of the call processing functions and features present in the Public Switched Telephone Network (PSTN).
- SIP by itself does not define these features; rather, its focus is call-setup and signaling.
- SIP is primarily used in setting up and tearing down voice or video calls. It also allows modification of existing calls. The modification can involve changing addresses or ports, inviting ore participants, and adding or deleting media streams.
- SIP supports the following facets of establishing and terminating multimedia communications: User location; User capabilities; User availability; Call setup; Call handling, and Call teardown.
- The previous figure depicts the VoIP architecture with respect to SIP. In such a VoIP setup, the end-user device can be either an IP phone or a computer in an IP network.

- The conversation can be IP-to-IP, PSTN-to-IP, IP-to-PSTN. In a SIP environment along with the endpoint devices, five entities are required. These are (as described ahead):
    1. Proxy server
    2. Registrar server
    3. Redirect server
    4. Location server
    5. Gateways

Proxy Server

- SIP proxies are elements that route SIP requests to user agent servers (UAS) and SIP responses to user agent clients (UAC).
- A request may traverse several proxies on its way to a UAS. Each will make routing decisions, modifying the request before forwarding it to the next element.
- Responses will route through the same set of proxies traversed by the request in the reverse order.
- In the SIP context, UAC is the endpoint initiating a call and UAS is the endpoint receiving the call. SIP proxies function similar to routers and make routing decisions, modifying the request before forwarding it to the next element.
- SIP standard make provision for proxies to perform actions such as validate requests, authenticate users, resolve addresses, fork requests, cancel pending calls, etc.

Registrar Server

- The Registrar server in a VoIP network can be defined as the server maintaining the whereabouts of a domain.
- It accepts REGISTER requests from nodes in the VoIP network. It places the information it receives as a part of those requests into the location service for the domain it handles.
- REGISTER requests are generated by clients in order to create or remove a mapping between their externally known SIP address and the IP address they wish to be contacted at.
- It uses the location service in order to store and retrieve location information.
- The location service may run on a remote machine and may be contacted using any appropriate protocol (such as LDAP).

Redirect Server

- The Redirect server does similar functions as in case of call forwarding in a PSTN or cellular network.
- A redirect server receives SIP requests and responds with redirection responses. This enables the proxy to contact an alternate set of SIP addresses.
- The alternate addresses are returned as contact headers in the response SIP message.

Presence Server

- Presence is a service that allows the calling party to know the ability and willingness of the other party to participate in a call.
- A user interested in receiving presence information for another user (Presented) can subscribe to his/her presence status and receive Presence status notifications from the Presence system. This is achieved through an Event Server.
- An Events Server is a general implementation of specific event notification, as described in RFC3265. RFC3265 provides a framework that allows an entity to subscribe for notifications on the state change of other entities.

	H.323	SIP
Reliability	It has defined a number of features to handle failure of intermediate networks entities, and a means of recovering from connection failures	It has not defined procedures for handling device failure.
Message Encoding	It encodes messages in a compact binary format that is suitable for narrowband and broadband connections.	SIP messages are encoded in ASCII text format, suitable for humans to read. As a consequence, the messages are large and less suitable for networks where bandwidth is a concern.
Extensibility	It is extended with non-standard features in such a way as to avoid conflicts between vendors.	It is extended by adding new header lines or message bodies that may be used by different vendors to serve different purposes, thus rising interoperability problems.
Scalability-Load Balancing	It has the ability to load balance endpoints across a number of alternate gatekeepers in order to scale a local point of presence.	It has no option of load balancing, except “trial and error” across pre-provisioned devices or devices learned from DNS SRV records.
Scalability-Statelessness	An H.323 gatekeeper can be stateless using the direct call model.	A SIP proxy can be stateless if it does not fork, use TCP, or use multicast.
Addressing	Flexible addressing mechanisms, including URIs, e-mail addresses, and E.164 numbers.	It only understands URI-style addresses. This works fine for SIP-SIP devices, but causes some confusion when trying to translate various dialed digits.
Codecs	It supports any codec, standardized or proprietary. No registration authority is required to use any codec in H.323.	It supports any IANA-registered codec or other codec whose name is mutually agreed upon.

15. Short note about SAP and SDP

- **Session Announcement Protocol (SAP)** is an announcement protocol that is used by session directory clients.
- A SAP announcer periodically multicasts an announcement packet to a known multicast addresses and port.
- The scope of multicast announcement is same as the session it is announcing. This ensures that the recipients of the announcement can also be potential recipients of the session the announcement describes.
- **The Session Description Protocol (SDP)** describes multimedia sessions for the purpose of session announcement, session invitation and other types of multimedia session initiation.
- SDP communicates the existence of a session and conveys sufficient information to enable participation in the session.
- Many of the SDP messages are sent using SAP. Messages can also be sent using email or the WWW (World Wide Web).

16. Explain Real Time Protocol

- To allow real-time data transmission over TCP/IP, various protocols have been developed.
- These include protocols for real-time data, audio, video, movie, and streaming data in a unicast or multicast situation.
- Examples of such protocols are:
    - Real-time Transport Protocol (RTP – RFC1889)
    - Real-time Control Protocol (RTCP – RFC3605)
    - Real-time Streaming Protocol (RTSP – RFC 2326)
- **Real-time Transport Protocol** (RTP) is both an IETF and ITU standard (H.225.0). It defines the packet format for multimedia data.
- RTP is used by many standard protocols, such as RTSP for streaming applications, H.323 and SIP for IP telephony applications, and by SAP/SDP for pure multicast applications.
- It provides the data delivery format for all of these protocols.
- **Real-time Control Protocol** (RTCP) is based on the periodic transmission of control packets to all participants in the session. RTCP uses the same distribution mechanism as RTP data packets.
- RTCP can deliver information such as the number of packets transmitted and received, the round-trip delay, jitter delay, etc., that can be used to measure Quality-of-Service in the IP network.
- This facility allows monitoring of the data delivery in a manner scalable to large multicast networks, to provide minimal control and identification functionality.
- For RTCP to work effectively, the underlying protocols must provide multiplexing of the data and control packets.

- **Real-time Streaming Protocol** (RTSP) is a client-server protocol, designed to address the needs for efficient delivery of streamed multimedia over IP networks. Interoperability on streaming media systems involves many components.
- These are players in the client device, servers that store the content, encoders that transform or compress the data and tools that create the content.
- All these must share common mechanisms for interoperability. Encoders and tools must store data types in files in formats that will be understood by players.
- Encoders and content-creation tools must be able to store content in files that servers can read. Servers must be able to stream content using protocols that players in the client device can understand.

17. What is convergence technology? Explain their elements in details.

- To make convergence and interworking between PSTN and IP networks possible, three functional gateway elements are defined.
- These are interface elements:
  - The Media Gateway
  - The Signaling Gateway
  - Media Gateway Controller.
- **Signaling gateway** (SG) is responsible for interfacing to the SS#7 network and forwarding the signaling message to the IP network.
- **The Media Gateway** (MG) is responsible for packetization of voice and other real-time traffic (media).
- **The Media Gateway Controller** (MGC) plays the role of the mediator to enable and control access and resource usage between the IP and PSTN network.
- Together, these elements form the building blocks for a distributed architecture approach to providing voice, fax and a set of digital data services over IP networks.
- In figure, we can see an IP SCP (Service Control Point). The functionality of the SCP is similar to Intelligent Networks (IN). However, an IP SCP is addressable from the SS#7 network.

Media Gateway

- The primary responsibilities of the Media Gateway (MG) are to allow media of various types, e.g., voice, fax, video, and modem data to be transported from one type of network to another.
- These media must be transportable, both as packets in the IP network and as digital or analog streams in the circuit-switched network.
- They must also be able to move without loss of integrity or degradation of quality. These criteria are met through the use of various coding, compression, echo cancellation, and decoding schemes.

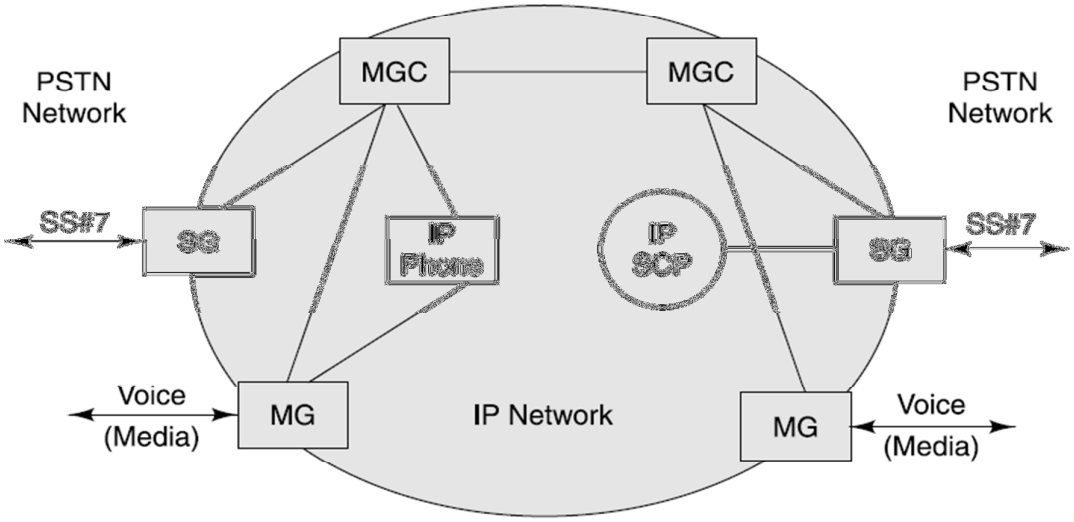


Figure 12: Interface between IP and PSTN Networks

- Media Gateways can implement a variety of physical interfaces to the PSTN.
- For example, highly scalable Media Gateway systems can implement high speed Time Domain Multiplexing (TDM) trunk interfaces.

Media Gateway Controller

- The key responsibilities of the Media Gateway Controller (MGC) are to make decisions based on flow-related information, and to provide associated instructions on the interconnecting of two or more IP elements so that they can exchange information.
- Media Gateway Controllers maintain current status information of all media flows, and they generate the administrative records necessary for charging and billing.
- A media gateway controller exchanges ISUP (ISDN User Part) messages with central office switches via a signaling gateway.
- In H.323, significant Media Gateway Controller functions are performed in network elements called Gatekeepers.
- Because media gateway controllers are built primary through software using off-the-shelf computer platforms, a media gateway controller is sometimes called a soft switch.

Signaling Gateway

- The Signaling Gateway (SG) function implements a bi-directional interface between an SS#7 network and various call control-related elements in an IP network.
- The key responsibilities of the Signaling Gateway are to repackage SS#7 information into formats understood by elements in each network, and to present an accurate view of the elements in the IP network to the SS#7 network.

- By definition, Signaling Gateways need to implement reliable SS#7 messaging that obeys all the rules of the SS#7 network, while also accommodating a variety of behaviors in the IP network.
- It is necessary for Signaling Gateways to understand all of SS#7 protocols and messaging standards.
- Finally, since an IP network is a shared medium lacking physical security, Signaling Gateways must filter out the inappropriate traffic that shows up at the Signaling Gateway.

18. What is IP Multimedia Subsystem (IMS)? Explain Architecture

- IP Multimedia Subsystem (IMS) is an emerging international standard, which looks at total convergence of voice and multimedia.
- Some literatures even refer IMS as "All IP network".
- IMS was specified by the Third Generation Partnership Project (3GPP/3GPP2) and is now being embraced by other standards bodies including ETSI. It specifies interoperability and roaming.
- It provides bearer control, charging and security. It is well integrated with existing voice and data networks.
- This makes IMS a key enabler for fixed-mobile- multimedia convergence with value-based charging.
- For a normal user, IMS-based services enable are as:
    - person-to-person and person-to-content communications in a variety of modes that include traditional telephony services
    - Non-telephony services such as instant messaging, unified messaging, push-to-talk, video streaming, multimedia messaging, text, fax, pictures and video, or any combination of these in a personalized and controlled way.
- For a network operator, IMS takes the concept of layered architecture one step further by defining a horizontal architecture, where service enablers and common functions can be reused for multiple applications.

IMS Architecture

- The IMS services architecture is a unified architecture that supports a wide range of services enabled by the flexibility of SIP.
- The IMS architecture is a collection of logical horizontal functions, which can be divided into three major layers:
    1. Communication Layer
    2. Session Control Layer
    3. Applications or Service Layer
- The session control layer contains the Call Session Control Function (CSCF), which provides the registration of the endpoints and routing of the SIP signaling messages to the appropriate application server.

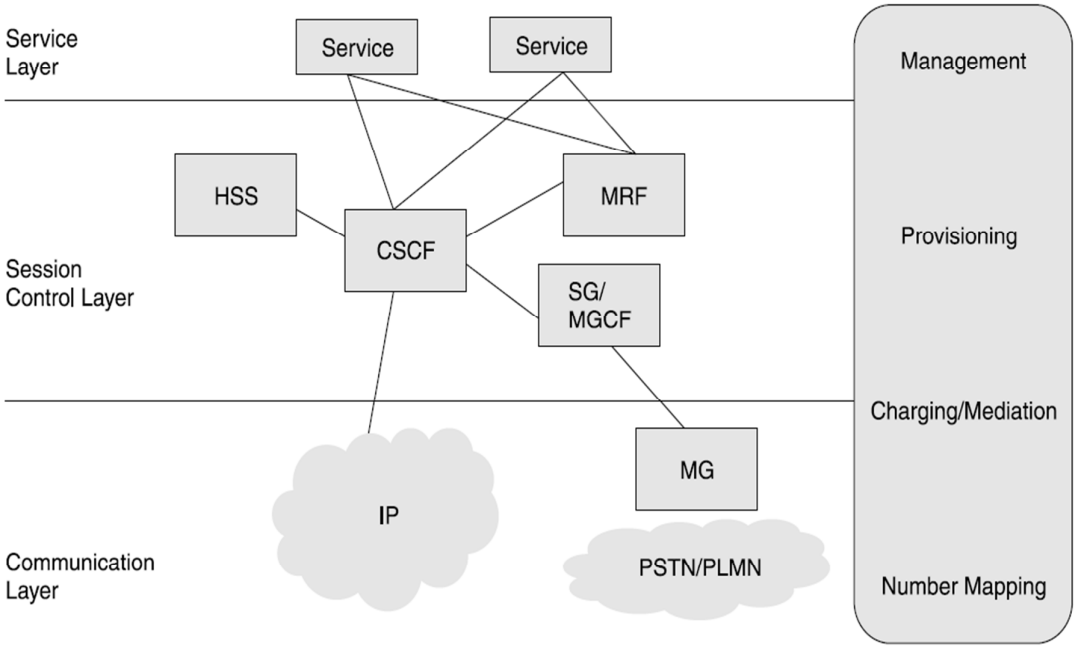


Figure 13: IMS Architecture

- The session control layer includes the **Home Subscriber Server** (HSS) database that maintains the unique service profile for each end user.
- The end user's service profile stores all of the user service information and preferences in a central location.
- This includes an end user's current registration information (i.e., IP address), roaming information, telephony services (i.e., call forwarding information), instant messaging service information (i.e., buddies list), voice mail box options (i.e., greetings), etc.
- **Media resource function** (MRF) includes functions related to conference booking and floor management.
- Conference booking provides booking information like start time, duration, list of participants, etc.
- Through floor control, end users (participants or chairman of the conference) can influence floor and provide information to the MRF Controller on how incoming media streams should be mixed and distributed.

19. What is Mobile VoIP? Explain

- While mobility has been considered to some extent within SIP, it has not been addressed comprehensively within H.323.
- In a VoIP application, mobility may include terminal mobility, user mobility, and service mobility.

- **Terminal mobility** refers to the ability for a terminal to change physical location while the ongoing voice connection is maintained.
- **User mobility** is defined as the ability for communications of the mobile user irrespective of the terminal type in use.
- **Service mobility** is the ability of a user to access a particular service independent of user and terminal mobility.
- In the context of VoIP, roaming refers to the ability that connectivity between endpoints is assured even while one or both endpoints are moving. Such reachability can either be discrete or continuous.
- Discrete reachability is service portability, implying no online reachability and communications taking place while moving.
- Continuous reachability is the service mobility allowing seamless communication continuity while roaming. Obviously, mobility encompasses portability, and requires the ongoing connection to be handed off when a mobile terminal is on the move.
- Upon crossing a region boundary, a handoff must be initiated; otherwise, the connection is broken and the ongoing conversation is interrupted.
- Mobility management is the key to enabling mobile Internet telephony service over connectionless IP networks.

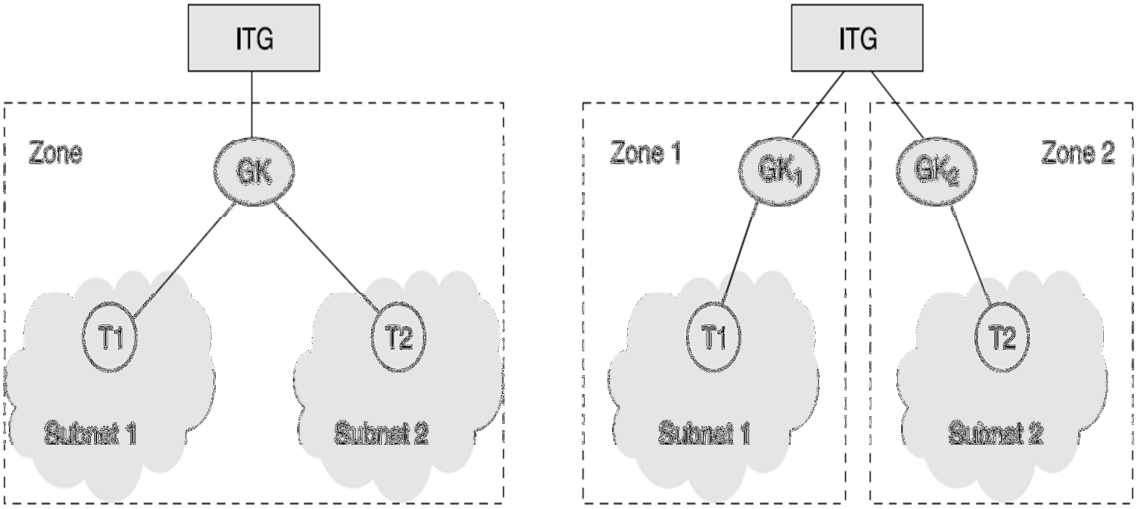


Figure 14: Intrazone and Inter Zone Handoff

- The core operations include registration, call establishment, roaming, and handoff. In H.323 or SIP there is no provision for support for roaming or handoff handling, and called location tracking and location update.
- When an H.323 terminal moves across different subnets during a call, it causes the IP address to change. This results in the ongoing connection to be broken.

- In the intrazone handoff, both subnets are under the management of the same GK (Gatekeeper), whereas in the interzone roaming, they are under the management of different GKs within the same ITG (Internet Telephony Gateway).

20. How authentication is possible in wireless LAN? List and discuss the possible attacks on such networks.

- WLAN specify two authentication mechanisms:
  - Open system authentication
  - Shared key authentication
- **Open system authentication** for successful association client SSID is used. And if any new client that comes in an extended basic service set (EBSS) area is provided with an SSID.

Figure 15: Open System Authentication

- **Shared system authentication** the client cannot authenticate him if he doesn't have the WEP shared secret key. WEP protocol is used for encryption.

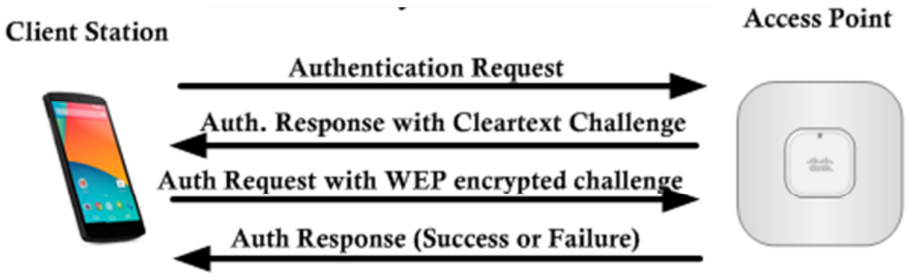


Figure 16: Shared Key Authentication

Attack

- Where the vulnerability is exploited, there is a loss. Loss can be either of static information asset (**static asset**) or an information asset in transit (**dynamic asset**)
- If we look at an information system, static assets cover a large portion of the asset base
- All the databases, files, documents, etc. in the computers/networks fall in this category
- Examples of an attacks on static asset are virus deleting files in a computer or jamming a network
- Example of an attack on a dynamic asset is the theft of a credit card number while a user is doing a credit card transaction on the web

Attacks on Static Assets

- **Virus and Worms:** These are a type of program that replicates and propagates from one system to another doing malicious functions in the system.
- **Denial of Service:** These are attacks on the system to prevent legitimate users from using the service.
- **Intrusion Attacks:** These are people or software which enter into computer systems and perform function without the knowledge of the owner of the asset.
- **Replay Attacks:** In a replay attack, the opponent passively captures the data without trying to analyze the content. At a later time, the same is used in the same sequence to impersonate an event and gain unauthorized access to resource.
- **Buffer Overflow Attacks:** In a buffer overflow attack, the vulnerability of an executable program is exploited to force a stack overflow condition inducing the program counter of the process to change. The program counter is then manipulated to do the work for the attacker.
- **Trapdoor Attacks:** These are exploitations of some undocumented features of a system. Undocumented functionality is designed to debug, service, and support or take control of the system.

Attacks on Dynamic Assets

- **Interception**: An unauthorized party gaining access to an asset will be part of this attack.
- This is an attack on confidentiality like unauthorized copying of files or tapping a conversation between parties. Some of the sniffing attacks fall in this category.
- **Modification**: An unauthorized party gaining control of an asset and tampering with it is part of this attack.
- This is an attack on integrity like changing the content of a message being transmitted through the network. Different types of man-in-the-middle attacks are part of this type of attack.
- **Fabrication**: An unauthorized party inserts counterfeited objects into the system. For example, impersonating someone and inserting a spurious message in a network.
- **Interruption**: An asset is destroyed or made unusable. This is an attack on availability. This attack can be on a static asset or a dynamic asset.
- An example could be cutting a communication line or making the router so busy that a user cannot use a server in a network. These are all denial of service attacks.

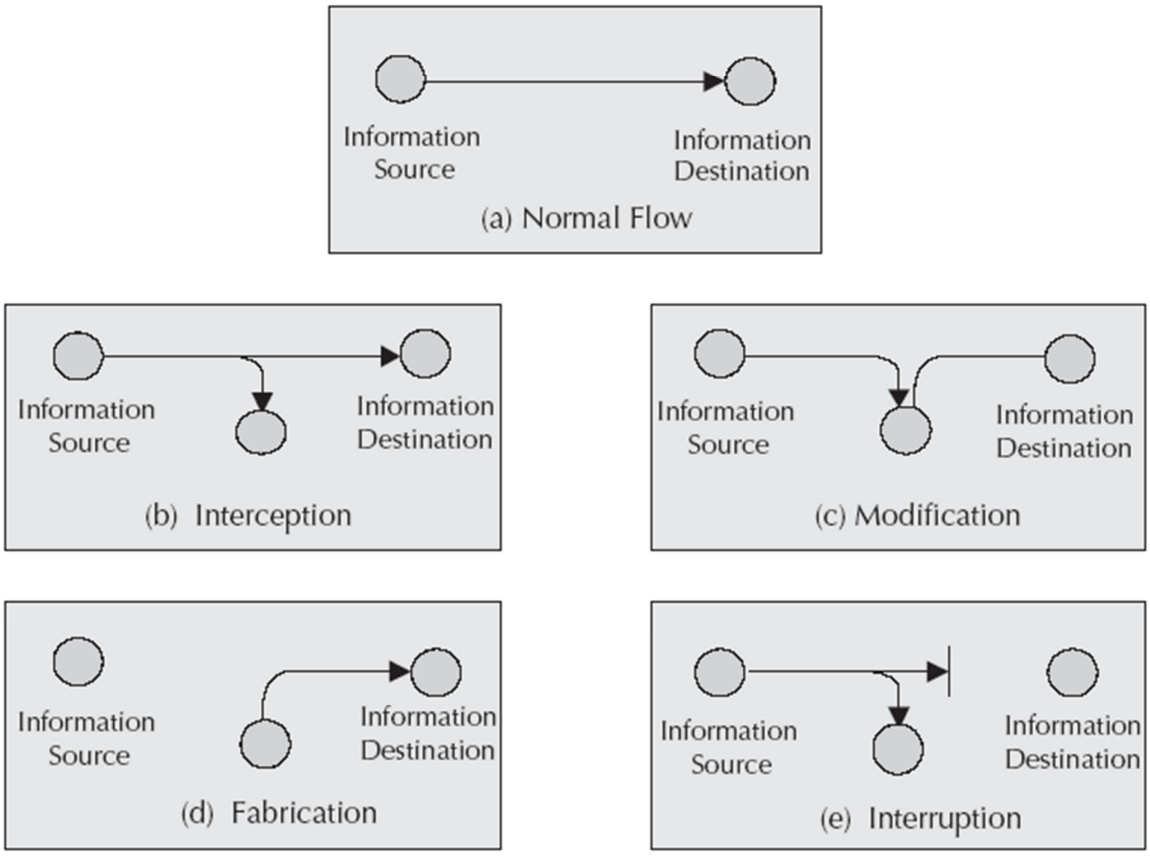


Figure 17: Attacks on Dynamic Assets

21. What is Information Security? Component of Information Security.

- **Confidentiality** is the property where the information is kept secret so that unauthorized persons cannot get the information.
- **Cryptography** helps achieve confidentiality.
- Cryptography is a process of making a message un-intelligible to un-intended users.
- Through encryption (or encipher), we disguise plaintext message in such a fashion that it is no longer understandable by either a person or a machine.
- Plaintext need not be a written text as it can even be an audio or video message as well.
- An encrypted message is called cipher text.
- The process of converting a cipher text back into plaintext is called decryption (or deciphering).
- In cryptography, there are two components - algorithms and protocols.
- A cryptographic algorithm is a mathematical function used for encryption and decryption while protocol relates to the process and procedure of using algorithms.
- A protocol is the way algorithms are used to ensure that the security is ensured and the system is less prone to attack.

- In a security system, the plaintext message is encrypted by using a key KEY(E).
- The encrypted message is then sent from the sender to the received through a media (wired, wireless or even postal) using some protocol. The encrypted message is then decrypted using a key KEY(D) to extract the original message.

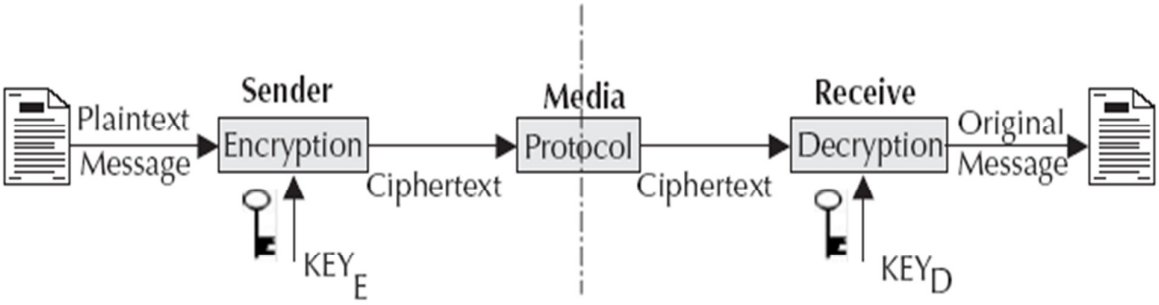


Figure 18: Cryptography

- A cryptographic key is generally a large number. The range of possible values of a key is called key space.
- The larger the keys pace is, the more difficult it is for an attacker to guess the key and restore the original message.
- People who practice cryptography are called cryptographers.
- People who try to break the secrecy of the cryptography are called cryptanalysts and the practice of cryptanalyst is called cryptanalysis.
- Steganography is the science of hiding secret message in other messages so that the existence of the secret message is concealed.
- For example, sending some secret message by changing some bits in a large picture message.
- **Integrity** is to ensure the integrity of the message.
- Integrity is achieved by adding additional information in to the message through checksums, message digests, and digital signatures.
- In a crypto system, the receiver of the message checks the extra information to verify whether the message has been tampered with.
- Integrity check is advised for both static asset and asset on transit.
- **Availability** is the property of a system by which the system is be available to its legitimate users.
- If an attacker manipulates the media to make sure that the message does not reach the destination, then he has attacked availability.
- Attack on availability happens for industrial espionage or from political motivation.
- This field of research area is called Censorship-resistant publishing.
- Censorship-resistant publishing is achieved through document entanglement.
- **Non-repudiation**, the identity of transacting parties are confirmed beyond any point of doubt.

- Non-repudiation can be considered as authentication with formal record which shall have legal bindings.
- Like a signature in a cheque, digital signatures can be used to achieve non-repudiation.
- **Authorization** deals with privileges.
- The privilege to an object is defined through ACL or Access Control List. ACL is used while allowing access to the object. The privilege on an object can be read, write or execute.
- Authorization is implemented through policy based resource accessibility.
- Privilege management infrastructure together with the role based authorization allows the administration and enforcement of user privileges and transaction entitlements.
- In the authorization process, users are checked to see if they have the required rights to access the resource.
- **Trust** is the property of expectation, confidence and belief over time.
- Trust involves developing a security policy, assigning credentials to entities and verifying that the credentials fulfill the policy.
- **Accounting** is the property of calculating the fee for a service rendered.
- Accounting is the process by which the usage of the service is metered.
- Based upon the usage, the service provider collects the fee either directly from the customer or through the home network.
- This is true even if the user is roaming in a foreign network and using the services in the foreign network.
- Remote Authentication Dial In User Service (RADIUS) has been in use for a long time for the Authentication, Authorization and Accounting (AAA) functions in Internet.

22. Explain security frameworks for mobile environment.

- To offer secured environment in a mobile environment, security procedure will be a combination of many procedure and functions.
- Some of vulnerabilities and techniques to offer security in mobile environment.

3GPP

- Its changes were made to defeat the false base station attack. The extended security mechanism is now capable of identifying the network.
- Key lengths are increased to allow stronger algorithms for encryption and integrity.
- Mechanisms are included to support security within and between networks.
- Security is based within the switch rather than the base station to ensure that links are protected between the base station and switch.
- The authentication algorithm has not been defined but guidance on choice shall be given.

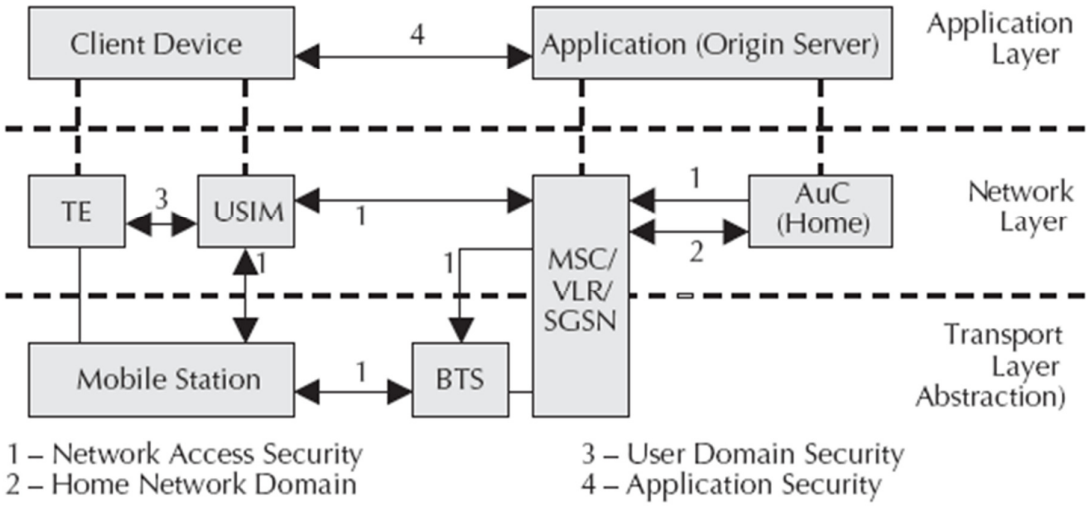


Figure 19: 3GPP Security

Mobile VPN

- Mobile VPN is a private network over a public network to connect two endpoints. Instead of using a dedicated physical connection such as leased line, a VPN uses virtual connections routed through the Internet from the enterprise's private network to the remote mobile device.
- VPN implements this through an encrypted private connection between nodes. It generally uses IPSec and other PKI frameworks to offer confidentiality, authentication, non-repudiation (through digital signature) and integrity.
- With mobile VPN, mobile workers have the freedom to safely use wireless applications on their PDAs, smart phones and other handheld devices in the field as if they are in a private network.

Smartcard Security

- Smart cards offer data encryption and the ability to store secret information for the purpose of authenticating the cardholder.
- To counter brute force attack, a smartcard processor does not allow more than 10 attempts to read a file data with wrong password.
- Therefore, a user can make use of the card as a security factory.
- Using this security factory is quite easy through Java card interfaces. In Java card technology, a Java interface is provided on the SIM card.
- Java Cryptographic Architecture (JCA) and Java programs running on the smartcard can do all these things quite easily.

Mutual and Spatial Authentication

- Using SIM card, we can do client authentication over wireless wide area networks.
- This is called mutual authentication because using GSM procedures, a client can authenticate the server while server can also authenticate the client.

- Location information then can be used to implement spatial authentication.
- For example, if the user is in a neighborhood which is insecure, access to some critical applications can be prevented.

Mobile Agent Security

- Mobile agent technology results in significant security threats from both malicious agents and malicious hosts.
- For example, as the mobile agent traverses multiple hosts that are trusted to different degrees, its state may be changed in a way that an adversely can impact the decision making process of the agent.

23. Give details about security risks.

- **Eavesdropping**: This is the capability through which the adversary eavesdrops signaling and data traffic associated with a user.
- **Impersonation of a user**: This is the capability whereby the adversary sends signaling and user data to the network in an attempt to make the network believe that they originate from a genuine (target of the impersonation) user.
- **Compromising authentication vectors in the network**: The adversary possesses a compromised authentication vector which may include challenge/response pairs, cipher keys and integrity keys.
- This data may have been obtained by compromising network nodes or by intercepting signaling messages on network links and then through brute force attack.
- **Impersonation of the network:** This is the capability whereby the adversary sends signaling and user data to the target user in an attempt to make the target user believe that the data originate from a genuine network.
- **Man-in-the-middle:** This is the capability whereby the adversary puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signaling and user data messages exchanged between the sender and the receiver.