MOBILE COMPUTING
ASSIGNMENT-1

SUBMITTED BY-

AKJOTSINGH

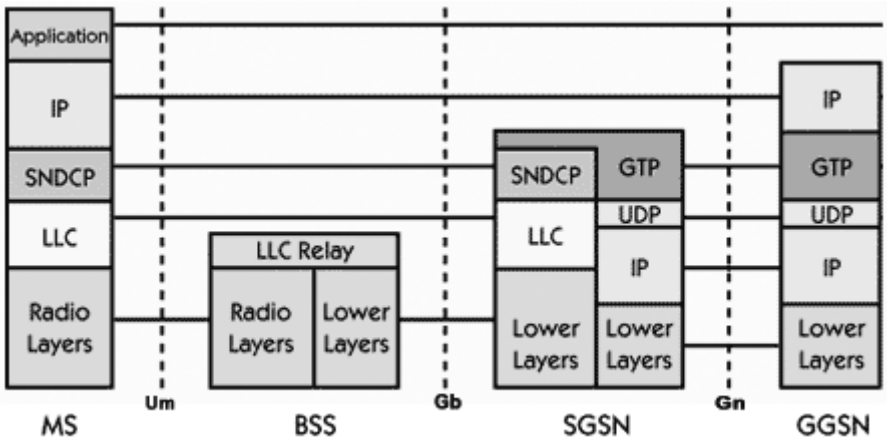
00213202717

CSE-1

Ques 1: Discuss the GPRS protocol stack with a diagram.

Answer:

The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunneling protocol.



The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.

SubNetwork Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling

protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.

SubNetwork Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

Reference: https://www.tutorialspoint.com/gprs/gprs_protocol_stack.htm#:~:text=The%20flow%20of%20GPRS%20protocol,a%20Layer%203%20tunneling%20protocol.

Ques 2: Describe the GSM architecture and its service detail. Explain about GSM authentication and security.

Answer:

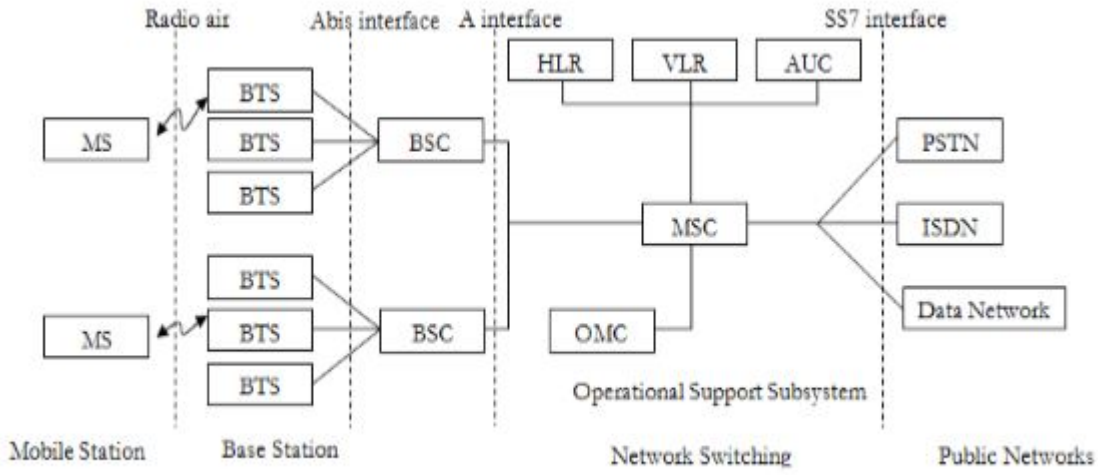


Fig: GSM Architecture

The GSM architecture consists of three major interconnected subsystems that interact with themselves and with users through certain network interface. The

subsystems are Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Operational Support Subsystem (OSS). Mobile Station (MS) is also a subsystem but it is considered as a part of BSS.

1. Mobile Station (MS): Mobile Station is made up of two entities.

A. Mobile equipment (ME):

- It is a portable, vehicle mounted, hand held device.
- It is uniquely identified by an IMEI number.
- It is used for voice and data transmission. It also monitors power and signal quality of surrounding cells foe optimum handover. 160 characters long SMS can also be sent using Mobile Equipment.

B. Subscriber Identity module (SIM):

- It is a smart card that contains the International Mobile Subscriber Identity (IMSI) number.
- It allows users to send and receive calls and receive other subscriber services. - It is protected by password or PIN.
- It contains encoded network identification details. it has key information to activate the phone.
- It can be moved from one mobile to another.

2. Base Station Subsystem (BSS): It is also known as radio subsystem, provides and manages radio transmission paths between the mobile station and the Mobile Switching Centre (MSC). BSS also manages interface between the mobile station and all other subsystems of GSM. It consists of two parts.

A. Base Transceiver Station (BTS):

- It encodes, encrypts, multiplexes, modulates and feeds the RF signal to the antenna.
- It consists of transceiver units.
- It communicates with mobile stations via radio air interface and also communicates with BSC via Abis interface.

B. Base Station Controller (BSC):

- It manages radio resources for BTS. It assigns frequency and time slots for all mobile stations in its area.
- It handles call set up, transcoding and adaptation functionality handover for each MS radio power control.
- It communicates with MSC via A interface and also with BTS.

3. Network Switching Subsystem (NSS): it manages the switching functions of the system and allows MSCs to communicate with other networks such as PSTN and ISDN. It consist of

A. Mobile switching Centre:

- It is a heart of the network. It manages communication between GSM and other networks.
- It manages call set up function, routing and basic switching.
- It performs mobility management including registration, location updating and inter BSS and inter MSC call handoff.
- It provides billing information.
- MSC does gateway function while its customers roam to other network by using HLR/VLR.

B. Home Location Registers (HLR): - It is a permanent database about mobile subscriber in a large service area. - Its database contains IMSI, IMSISDN, prepaid/post-paid, roaming restrictions, supplementary services.

C. Visitor Location Registers (VLR): - It is a temporary database which updates whenever new MS enters its area by HLR database. - It controls mobiles roaming in its area. It reduces number of queries to HLR. - Its database contains IMSI, TMSI, IMSISDN, MSRN, location, area authentication key.

D. Authentication Centre: - It provides protection against intruders in air interface. - It maintains authentication keys and algorithms and provides security triplets (RAND, SRES, Ki).

E. Equipment Identity Registry (EIR):

- It is a database that is used to track handset using the IMEI number.
- It is made up of three sub classes- the white list, the black list and the gray list.

4. Operational Support Subsystem (OSS): It supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose and troubleshoot all aspects of GSM system. It supports one or more Operation Maintenance Centres (OMC) which are used to monitor the performance of each MS, Bs, BSC and MSC within a GSM system. It has three main functions:

- To maintain all telecommunication hardware and network operations with a particular market.
- To manage all charging and billing procedures
- To manage all mobile equipment in the system.

Interfaces used for GSM network: (ref fig 2)
1) UM Interface –Used to communicate between BTS with MS
2) Abis Interface— Used to communicate BSC TO BTS
3) A Interface-- Used to communicate BSC and MSC
4) Singling protocol (SS 7)- Used to communicate MSC with other network.

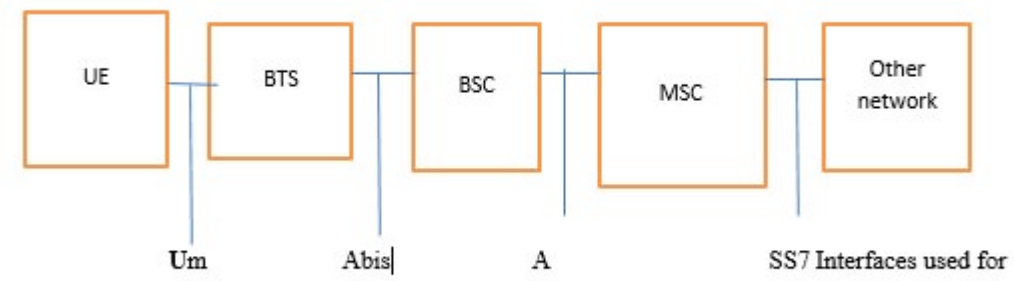


Fig 2 GSM network Interfaces

Reference:- https://www.tutorialspoint.com/gsm/gsm_security.htm

Ques 3: Discuss the feature of HiperLAN.

Answer:

A high-performance local area network (HIPERLAN) is an alternative wireless LAN standard to the IEEE 802.11. It is one of four standards (HIPERLAN 1 through 4) specified by the European telecommunications standards institute (ETSI) to link interoperable technologies from different locations instead of cable.

	HIPERLAN 1	HIPERLAN 2	HIPERLAN 3	HIPERLAN 4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.1-5.3GHz			17.2-17.3GHz
Topology	decentralized ad-hoc/infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50 m	50-100 m	5000 m	150 m
QoS	statistical	ATM traffic classes (VBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Data rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

HIPERLAN protocol family

Reference:- https://www.brainkart.com/article/HIPERLAN(high-performance-local-area-network)_9933/

Features:

- QoS (to build multiservice network)
- Strong security
- Handoff when moving between local area and wide areas
- Increased throughput
- Ease of use, deployment, and maintenance
- Affordability
- Scalability

Ques 4: Explain the following:

a. Zigbee

b. WiMax

c. RFID.

Answer:

Zigbee is based on the IEEE's 802.15.4 personal-area network standard. All you need to know is that Zigbee is a specification that's been around for more than a decade, and it's widely considered an alternative to Wi-Fi and Bluetooth for some applications including low-powered devices that don't require a lot of bandwidth - like your smart home sensors. Hence, Zigbee is a low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.

A typical example is when you have a Zigbee-enabled light bulb and a Zigbee-enabled light switch and you want the light switch to control the light bulb. With Zigbee, the two devices - even if they're from different manufacturers - speak a common language, so there's no barrier to communication.

With Zigbee, the two devices - even if they're from different manufacturers - speak a common language, so there's no barrier to communication. Zigbee does not focus on point-to-point communication, such as Bluetooth, but it operates in a mesh network, which is why it's great for the smart home.

Reference: https://homey.app/en-us/wiki/what-is-zigbee/

b) WiMAX is

- Acronym for **Worldwide Interoperability for Microwave Access**.
- Based on Wireless MAN technology.
- A wireless technology optimized for the delivery of IP centric services over a wide area.
- A scalable wireless platform for constructing alternative and complementary broadband networks.
- A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models −
    - A fixed usage model (IEEE 802.16-2004).
    - A portable usage model (IEEE 802.16e).

WiMAX would operate similar to WiFi, but at higher speeds over greater distances and for a greater number of users. WiMAX has the ability to provide

service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure.

WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the WiFi Alliance is to 802.11

WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way.

Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.

More strictly, WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards.

Reference: https://www.tutorialspoint.com/wimax/what_is_wimax.htm

c) RFID

Radio Frequency Identification (RFID) is the application of radio waves to read and capture information stored on tags affixed to objects. RFID readers are installed at tracking points and can read information from tags when they come into range, which can be of several feet radius. A tag need not be within direct line-of-sight of the reader to be tracked. RFID is used to check identities and track inventory, assets and people. RFID tags can be attached to a variety of objects like cash, clothing, baggage, parcels, and even implanted in animals and people.

Working Principle

There are two parts in a RFID system−

- a tag or label
- a reader

RFID tags are affixed on the object and have a transmitter and a receiver embedded on it. It contains the serial number that uniquely identifies a specific object. The tags have two parts−

- a microchip to store and process information, and

- an antenna to receive and transmit a signal.

The RFID reader (also called interrogator) captures the information encoded on the tag using an antenna. It is a two-way radio transmitter-receiver that emits a signal for the tag. The tag responds by sending the information embedded in its memory. The reader captures the results and transmits to the RFID computer program, which then performs the necessary processing.

Types of RFID tags

RFID tags are categorized into three types according to power−

- **Passive tags**− They use the radio wave energy of the reader to transmit its ID to the reader.
- **Active tags**− They are equipped with an on-board battery and transmit their ID periodically.
- **Battery – assisted Passive**− They have a small battery on-board and are activated only within the range of an RFID reader.

Types of RFID readers

RFID readers are categorized into two types according to power−p>

- **Passive readers**− They can only receive signals from active tags.
- **Active readers**− They can transmit interrogator signals to both passive, active as well as battery-assisted tags and also receives replies from them.

Reference: https://www.tutorialspoint.com/radio-frequency-identification-rfid

Ques 5: Explain the WAP architecture in brief.

Answer:

WAP stands for Wireless Application Protocol. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices. It uses the mark-up language WML (Wireless Markup Language and not HTML), WML is defined as XML 1.0 application.

Layers of WAP Protocol

Application Layer

Wireless Application Environment (WAE). 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.

Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer

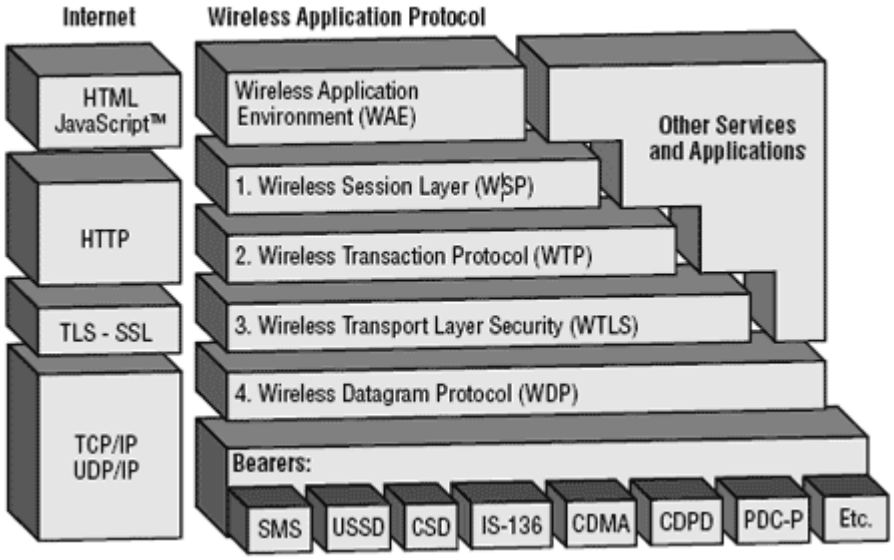
Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer

Wireless Datagram Protocol (WDP). 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 the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The **WAP protocol architecture** is shown below alongside a typical Internet Protocol stack.



Reference: tutorialspoint.com/wap/wap_architecture.htm