Subject Name: Mobile Computing and Wireless Communication
Subject Code: 3170710

Faculties: Ms. Alpa Rupala, Ms. Kinjal Parmar

TOPIC 3. General packet radio Service(GPRS)

DESCRIPTIVE QUESTIONS

- GPRS is an abbreviation for General Packet Radio Service.
- GPRS 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.

1.	Explain functional architecture of GPRS system. What is the frequency range of uplink and downlink in GPRS network? **(Nov-2011)[L.J.I.E.T]** Explain the GPRS system architecture. **(June-2012)[L.J.I.E.T]** Draw and explain GPRS architecture. **[New] (June-2014)[L.J.I.E.T]** Explain GPRS operations with its architecture. **(Summer-2014) (Winter-2015)[[L.J.I.E.T]** Draw GPRS System Architecture. Discuss GPRS network enhancement over GSM. **[New](May-2017)[L.J.I.E.T]** Explain GPRS system architecture. Also discuss limitations of GPRS. **[New](May-2018) [L.J.I.E.T]** What kind of changes need in GSM to Convert it into GPRS explain that? Explain application of GPRS? **(May-2017)[L.J.I.E.T]** Discuss the network elements in GPRS that are different from GSM. Also discuss applications and limitations of GPRS. **[New] (Nov-2016)[L.J.I.E.T]** Define SGSN and GGSN. **[New] (Dec-2013)[L.J.I.E.T]**	7, 8, 7, 7, 7, 7, 7

GPRS architecture:

- 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.

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

- Some Nodes of GSM Network needs to be upgraded to support the GPRS system.

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.

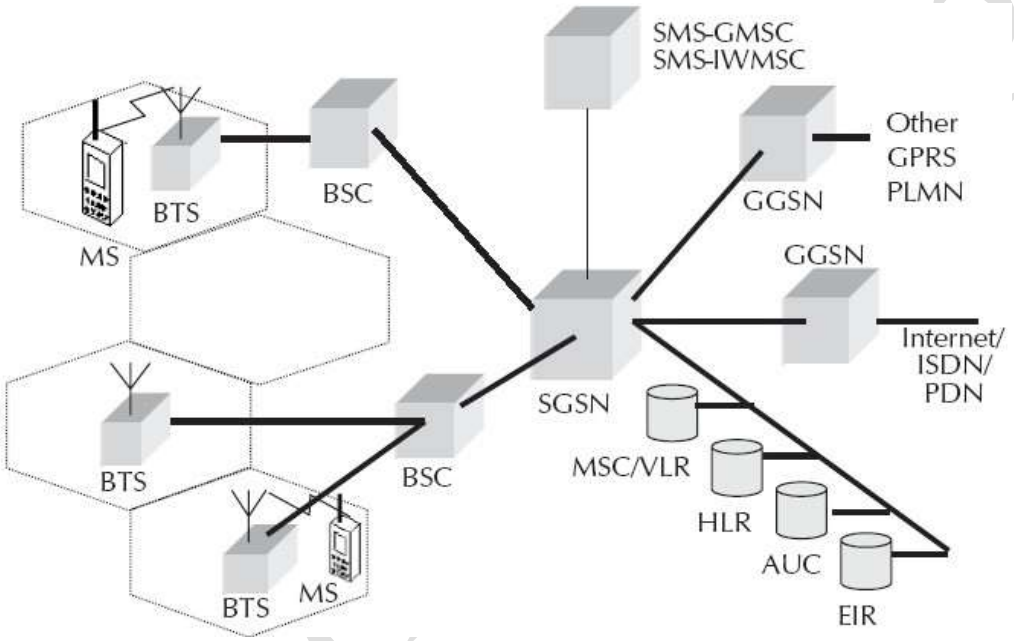
Mobile Station (MS)

- 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).

Figure 11: 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**

Uplink: 890 to 915 Mhz
Downlink: 935 to 960 Mhz

2. Describe what are the limitations of GPRS? **(Dec-2012)[L.J.I.E.T]**
Limitations of GPRS**(Winter-2013)[L.J.I.E.T]**
Write a short note on limitations of GPRS **[New](Dec-2013)[L.J.I.E.T]**
Explain the limitations of GPRS. **[New] (Dec-2016)[L.J.I.E.T]**

3, 3, 3, 7

Limitation 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 171.2 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.

Support of GPRS Mobile Terminate Connection for a Mobile Server not Supported:

- As of date a GPRS terminal can only act as a client device. There are many services for which the server needs to be mobile.
- An example could be a mobile healthcare center for rural population. For such application the server needs to be on the mobile network and user needs to be connect to the server. Using GPRS network, such communication is not possible.

3.	Explain the GPRS functional architecture and application. **[New] (Winter-2012) [New] (Dec-2014) [L.J.I.E.T]** Discuss GPRS-Specific Applications. **[New] (Dec-2013)[L.J.I.E.T]** Describe the applications for GPRS. **(Nov-2011) [New] (Dec-2016)[L.J.I.E.T]** Discuss GPRS specific applications along with limitations of GPRS. **[New](May-2017) [L.J.I.E.T]** Explain Term: Application and tunneling modes in GPRS **[New] (June-2014)[L.J.I.E.T]** Discuss data services in GPRS. Describe applications suitable for GPRS. **(Winter-2014) (Summer-2015)[[L.J.I.E.T]**	7, 7, 7

Applications:

- Any user is likely to use either of the two modes of the GPRS network:
  - Application mode
  - Tunneling mode
- **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. All GPRS phones have WAP Browser as an embedded application. This browser allows browsing of WAP sites. The device operating execution environment supported are Symbian and J2ME. Applications can be developed in C/C++ or JAVA.
- **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.

APPLICATIONS FOR GPRS

There are many applications suitable for GPRS. Many of them are of generic type, some of them are specific to GPRS.

- **Generic Applications:** Generic applications are applications like information services, Internet access, email, Web Browsing, which are very useful while mobile. These are generic mass market applications offering contents like sports scores, weather, flight information, news headlines, prayer reminders, lottery results, jokes, horoscopes, traffic information and so on. Banking over wireless is another generic application. Some Indian banks are offering banking over GPRS/WAP

- **GPRS-Specific Applications:**
  - **Chat:** chat is a very popular service in Internet and GSM (over SMS). Groups of like-minded people. use chat services as a means to communicate and discuss matters of interest. Generally, people use different chat services; one, through Internet and the other, using SMS (offered by mobile operator)

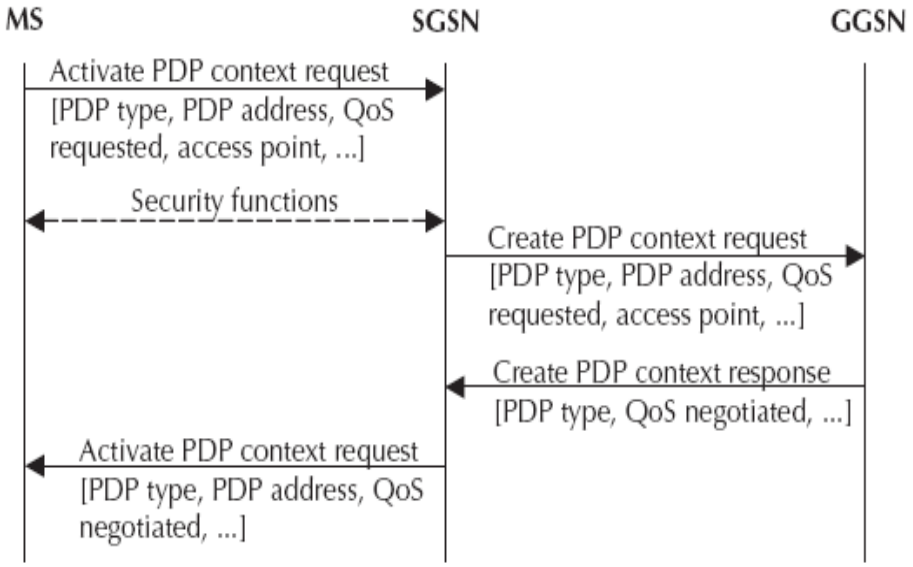
  - **Multimedia Services:** Multimedia objects like photographs, pictures, postcards, greet ng cards and presentations, static web pages can be sent and received over the mobile network. There are many phones available in the marketplace where a digital camera is integrated with the phone. These pictures can be sent as an electronic object or a printed one. Sending moving images in a mobile environment has several vertical market applications including monitoring parking lots or building sites for intruders or thieves. This can also be used by law enforcement agents, journalists, and insurance agents for sending images of accident site. Doctors can use these applications to send pictures of patients from a health center for expert help.

  - **Virtual Private Network:** GPRS network can be used to offer VPN services. Many Bank ATM machines use VSAT (Very Small Aperture Terminal) to connect the ATM system with the banks server. As the bandwidth in GPRS is higher, many banks in India are migrating from VSAT to GPRS-based networks. This is expected to reduce the transaction time by about 25%

	• **Personal Information Management:** Personal diary, address book, appointments, engagements etc. are very useful for a mobile individual. Some of these are kept in the phone some in the organizer and some in the Intranet. UsingJ2ME and WTAI (Wireless Telephony Application Interface) the address book, the diary of the phone can be integrated with the diary at the home office. GPRS and other bearer technology will help achieve this. • **Job Sheet Dispatch:** GPRS can be used to assign and communicate job sheets from office-based staff to mobile field staff. Customers typically telephone a call center whose staff takes the call and categorize it. Those calls requiring a visit by field sales or service representative can then be escalated to those mobile workers. Job dispatch applications can optionally be combined with vehicle positioning applications so that the ne available suitable personnel can be deployed to serve a customer • **Unified Messaging:** Unified messaging uses a single mailbox for all messages, including voice mail, fax, e-mail, SMS, MMS, and pager messages. With the various mailbox in one place, unified messaging systems then allow for a variety of access methods to recover messages of different types. Some will use text-to-voice systems to read e-mail and, less commonly, faxes over a normal phone line, while most will allow the interrogation of the contents of the various mailboxes through data access, such as the Internet. Others may be configured to alert the user on the terminal type of their choice when messages are received • **Vehicle Positioning:** This application integrates GPS (Global Positioning System) that tell people where they are. GPS is a free-to-use global network of 24 satellites run by the US Department of Defence. Anyone with a GPS receiver can receive their satellite position and thereby find out where they are. Vehicle-positioning applications can be used to deliver several services including remote vehicle diagnostics, ad hoc stolen vehicle tracking and new rental car fleet tariffs. In India this application is becoming popular in logistics industry • **Location-based Services and Telematics:** Location-based services provide the ability to link push or pull information services with a user's location. Examples include hotel and restaurant finders, roadside assistance, and city-specific news and information. All systems developed for Intelligent Transportation System (ITS) are built around GPRS and GPS technology. Location can be determined either through GPS or cell id from the operator. This technology also has vertical applications such as workforce management and vehicle tracking.	
4.	Write a note on PDP context activation procedure with respect to GPRS. **[New] (Dec-2013) [L.J.I.E.T]** What is PDP Address? Explain PDP Context Activation in GPRS. **[New] (May-2016)[L.J.I.E.T]** • 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.	4, 7

- 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 13: 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.	Explain call routing in the context of GPRS networks. **(Summer-2013)[L.J.I.E.T]** Explain call routing in the context of GPRS networks. **(Summer-2015)[L.J.I.E.T]** Explain the PLMN Interface. **(May-2018)[L.J.I.E.T]** What is a PLMN? How is a PLMN connected to PSTN and PDN? **[New] (Dec-2016)[L.J.I.E.T]** How the packets are routed in GPRS. Explain GPRS packet routing for Inter & Intra PLMN. **[New] (Dec-2014) [L.J.I.E.T]** Explain routing between PLMNs for GPRS system. **[New] (June-2014)[L.J.I.E.T]** Establish the relationship between PLMN and GPRS. Explain it using block diagram. **[New] (Dec-2015)[L.J.I.E.T]** Explain Routing between PLMNs of GPRS. **[New] (May-2016) [L.J.I.E.T]** Explain the data routing in GPRS. **[New] (Dec-2016)[L.J.I.E.T]**	7, 7, 3, 7, 7, 7

ANS: , 7

Call Routing , 7 , 7

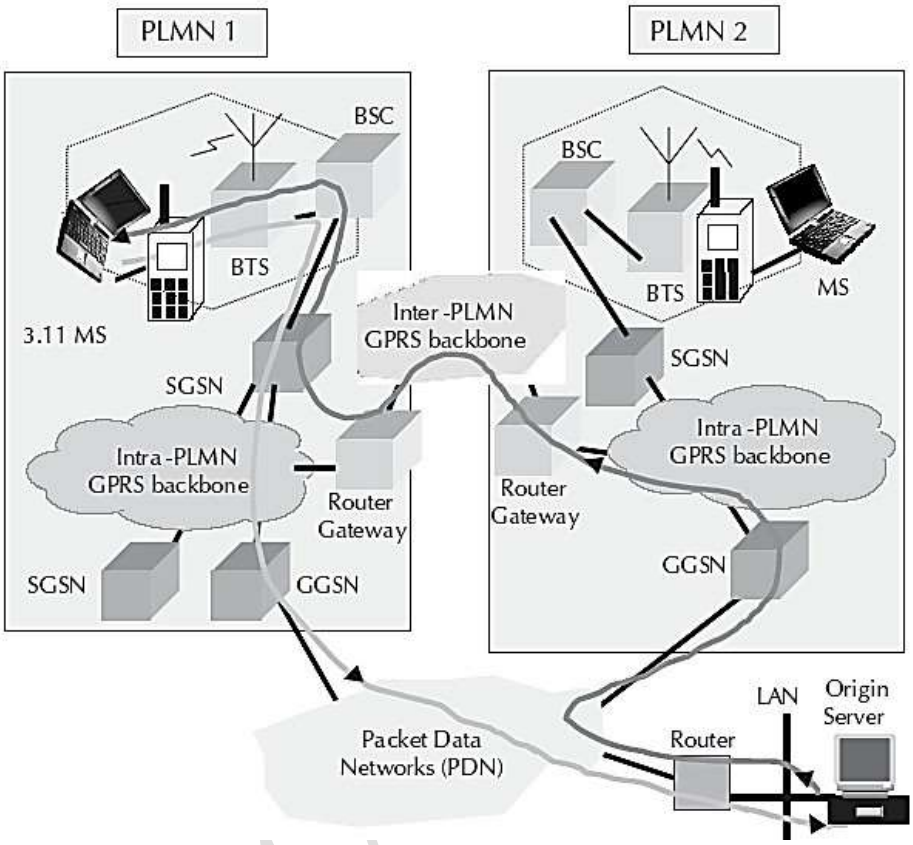


Figure 14: GPRA Packet Routing

- 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.
- 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.	Discuss Billing and Charging in GPRS network. **(Summer-2014) (Summer-2015) (Winter- 2015) [L.J.I.E.T]** What is GPRS? How billing and charging is done in GPRS? **(Nov-2017)[L.J.I.E.T]** **Billing:** Tariffing of data in wireless network has always been a challenges. • For voice networks tariffs are generally based on distance and time means that user pay more for long distance calls. They also pay more if they keep the circuit busy by talking for a longer period of time. So charging is fundamental part of the architecture. • On other hand, in data services charging with circuit busy does not have any meaning. Also, charging a customer by the distance traversed by a packet does not make any sense. • It is Believed that the optimal GPRS pricing model will be based on two variables, Time and Packet. • Network operators will levy a nominal per packet charge during peak time plus a flat rate. There will be no per packet charge during non-peak times. • Time and packet related charging will encourage application such as Remote monitoring, meter reading and chat to use GPRS at night when spare network capacity is available. • Simultaneously, nominal per packet charge during the day will help to allocate scarce radio resources, and charge radio heavy application such as file and image transfer more than application with lower data intensity. • It has the advantage of automatically adjusting customer charging according to their application usage. • **Minimum charging information that must be collected are:** o Destination and source addresses o Usage of radio interface o Usage of external Packet Data Networks o Usage of the packet data protocol addresses o 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	7, 7, 7, 4

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.
- The Charging for GPRS services dependent on following parameters:

1. **Duration:** the duration of a PDP context session.
2. **Time:** date time of the day, day of week, (low tariffs for happy hours at night).
3. **Volume:** the amount of data bites sent and received.
4. **Location:** the location of the subscribers
5. **Flat rate:** a fixed monthly change a rental.
6. **Free Charge:** data subscribed should be free from charge.
7. **Quality of Service:** More charge for high network priority and data rate.
8. **SMS:** Specific CDRs will be generated by SGSN for SMS.
9. **Reverse charging:** the subscriber sending the data is charged. The subscriber receiving the data is not charged for the data received.
10. **Bearer services:** charges depending on different bearer services like SMS, MMS.

7. Draw and Explain Transmission Plane Protocol Architecture of GPRS**. [New] (Dec-2014) [L.J.I.E.T]** Explain the GPRS Transmission Protocol Stack with the neat diagram. **(May-2018)[L.J.I.E.T]** — 7, 7

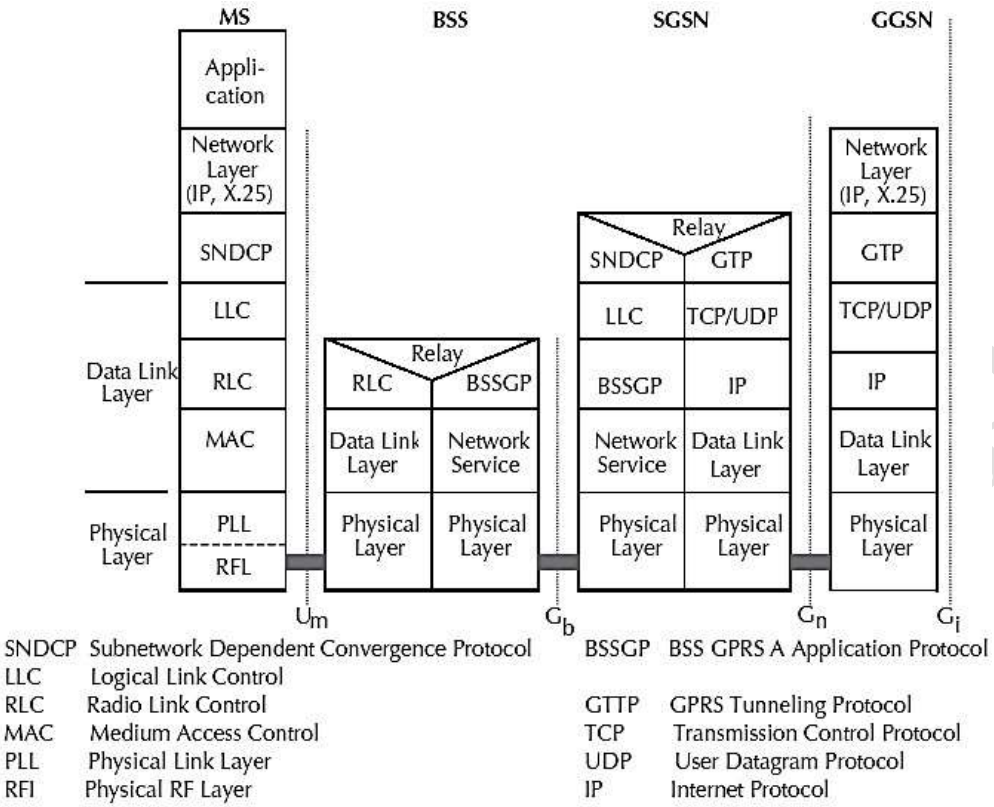
Protocol Architecture of GPRS:

- 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.

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 tunneling 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.

Figure 12: Transmission Plane and GPRS Protocol Stack

Interface between MS and SGSN

- This interface supports the following protocols:
  - **Sub network-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.

8. What is the difference between GSM and GPRS? What are the network elements in GPRS that area different from GSM? What are the limitations of GPRS. **(Summer-2013)[L.J.I.E.T]** — 7
What is the difference between GSM and GPRS? What are the network elements in GPRS that are different from GSM? **[New](Dec-2015)[L.J.I.E.T]** — 7
Differentiate the GSM and GPRS. **(May-2018) [L.J.I.E.T]** — 4
What is the difference between GSM and GPRS? How is data routing done in GPRS? **[New] (May-2015) [L.J.I.E.T]**
Compare the Following : (i) GSM and GPRS (ii) Wimax and WiFi **(May-2017) [L.J.I.E.T]**

Parameters	GSM	GPRS
Technology used	2G	2.5G
Base System	TDMA	GSM
Carrier Channel	200 kHz	200kHz
Users per Channel	8	8
Type of switching used	Circuit switching	Packet switching
Multiple Access	TDMA	TDMA
Data Rates	9.6 kbps	14.4 to 171.2 kbps
SIM Card Required	Yes	Yes
Frequency separation	45 MHz	45 MHz
Modulation	0.3 GMSK	GMSK
Uplink Frequency (MS to BS)	890-915 MHz	890-915 MHz
Downlink Frequency (MS to MS)	935-960 MHz	935-960 MHz
Frequency Hopping	217 Hops/Sec	217 Hops/Sec
Frame Period	4.615 ms	4.615 ms
Time slot period	576.92 µs	576.92 µs
Billing	Connection duration	Amount of data transferred
SMS	160 characters of Text Support	It is used as Bearer service
Applications	Mobile Telephony, Value added services, Telemetry system for toll connection	Emails, web browsing, broadcast service
Telematics	E commerce	VPN

TOPIC 4. Wireless system operations and standards

DESCRIPTIVE QUESTIONS

1.	Write a note on DECT frame format. **[New] (Nov-2016) [L.J.I.E.T]** Explain DECT Protocol Architecture. (**Nov-2017) [L.J.I.E.T]** **For DECT frame format: explain DECT in brief, Draw DECT protocol architecture and write physical layer in detail.**	4, 3

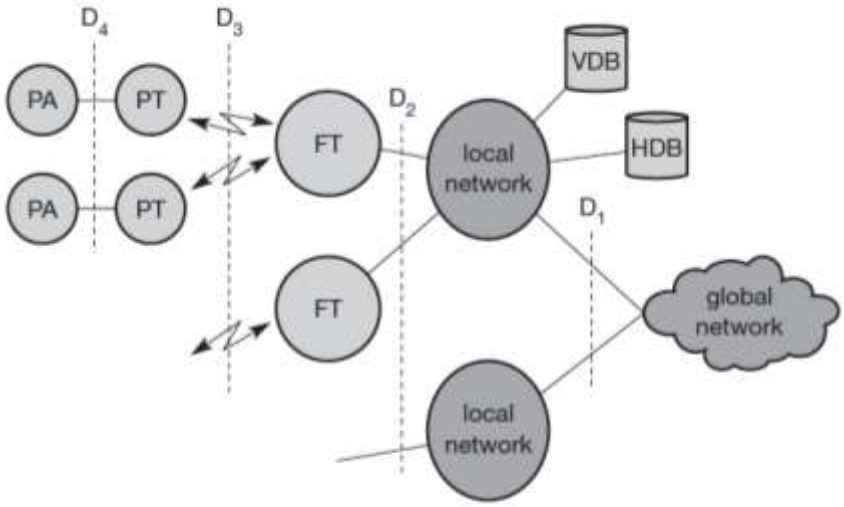
DECT

- Fully digital cellular network is the **digital enhanced cordless telecommunications (DECT)** system specified by ETSI (2002, 1998). Formerly also called **digital European cordless telephone and digital European cordless telecommunications**, DECT replaces older analog cordless phone systems such as CT1 and CT1+.
- These analog systems only ensured security to a limited extent as they did not use encryption for data transmission and only offered a relatively low capacity. DECT is also a more powerful alternative to the digital system CT2, which is mainly used in the UK (the DECT standard works throughout Europe), and has even been selected as one of the 3G candidates in the IMT-2000 family.
- DECT is mainly used in offices, on campus, at trade shows, or in the home. Furthermore, access points to the PSTN can be established within, e.g., railway stations, large government buildings and hospitals, offering a much cheaper telephone service compared to a GSM system.
- DECT could also be used to bridge the last few hundred meters between a new network operator and customers. Using this 'small range' local loop, new companies can offer their service without having their own lines installed in the streets. DECT systems offer many different interworking units, e.g., with GSM, ISDN, or data networks. Currently, over 100 million DECT units are in use (DECT, 2002).
- A big difference between DECT and GSM exists in terms of cell diameter and cell capacity. While GSM is designed for outdoor use with a cell diameter of up to 70 km, the range of DECT is limited to about 300 m from the base station (only around 50 m are feasible inside buildings depending on the walls).
- Due to this limited range and additional multiplexing techniques, DECT can offer its service to some 10,000 people within one km2. This is a typical scenario within a big city, where thousands of offices are located in skyscrapers close together.
- DECT also uses base stations, but these base stations together with a mobile station are in a price range of €100 compared to several €10,000 for a GSM base station. GSM base stations can typically not be used by individuals for private networks.
- One reason is licensing as all GSM frequencies have been licensed to network operators. DECT can also handle handover, but it was not designed to work at a higher speed (e.g., up to 250 km/h like GSM systems).
- Devices handling GSM and DECT exist but have never been a commercial success.
- DECT works at a frequency range of 1880–1990 MHz offering 120 full duplex channels. Time division duplex (TDD) is applied using 10 ms frames. The frequency range is subdivided into 10 carrier frequencies using FDMA, each frame being divided into 24 slots using TDMA. For the TDD mechanism, 130 Mobile communications 12 slots are used as uplink, 12 slots as downlink (see Figure 1).
- The digital modulation scheme is GMSK – each station has an average transmission power of only 10 mW with a maximum of 250 mW.

System architecture

- A DECT system may have various different physical implementations depending on its actual use.
- Different DECT entities can be integrated into one physical unit; entities can be distributed, replicated etc.

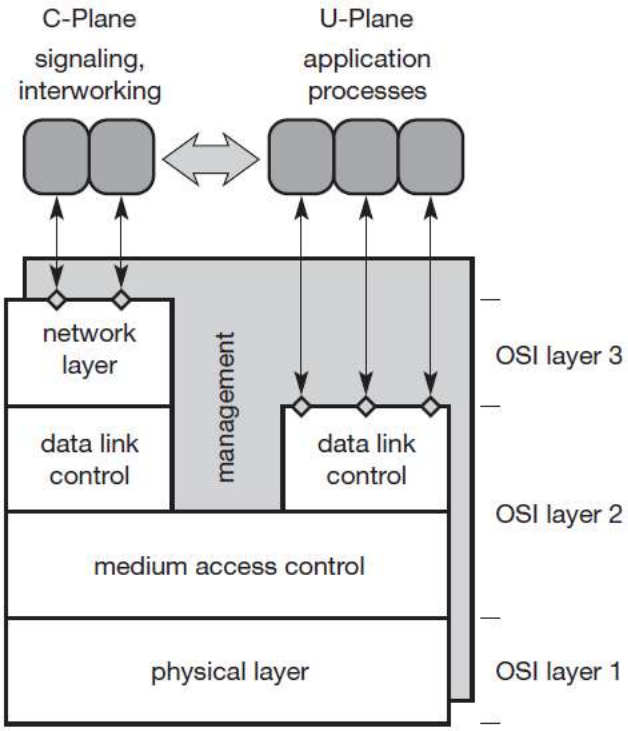
- However, all implementations are based on the same logical reference model of the system architecture as shown in Figure 1.
- A global network connects the local communication structure to the outside world and offers its services via the interface D1.
- Global networks could be integrated services digital networks (ISDN), public switched telephone networks (PSTN), public land mobile networks (PLMN), e.g., GSM, or packet switched public data network (PSPDN).
- The services offered by these networks include transportation of data and the translation of addresses and routing of data between the local networks.
- Local networks in the DECT context offer local telecommunication services that can include everything from simple switching to intelligent call forwarding, address translation etc. Examples for such networks are analog or digital private branch exchanges (PBXs) or LANs, e.g., those following the IEEE 802.x family of LANs.



- As the core of the DECT system itself is quite simple, all typical network functions have to be integrated in the local or global network, where the databases home data base (HDB) and visitor data base (VDB) are also located.
- Both databases support mobility with functions that are similar to those in the HLR and VLR in GSM systems. Incoming calls are automatically forwarded to the current subsystem responsible for the DECT user, and the current VDB informs the HDB about changes in location.
- The DECT core network consists of the fixed radio termination (FT) and the portable radio termination (PT), and basically only provides a multiplexing service.
- FT and PT cover layers one to three at the fixed network side and mobile network side respectively. Additionally, several portable applications (PA) can be implemented on a device.

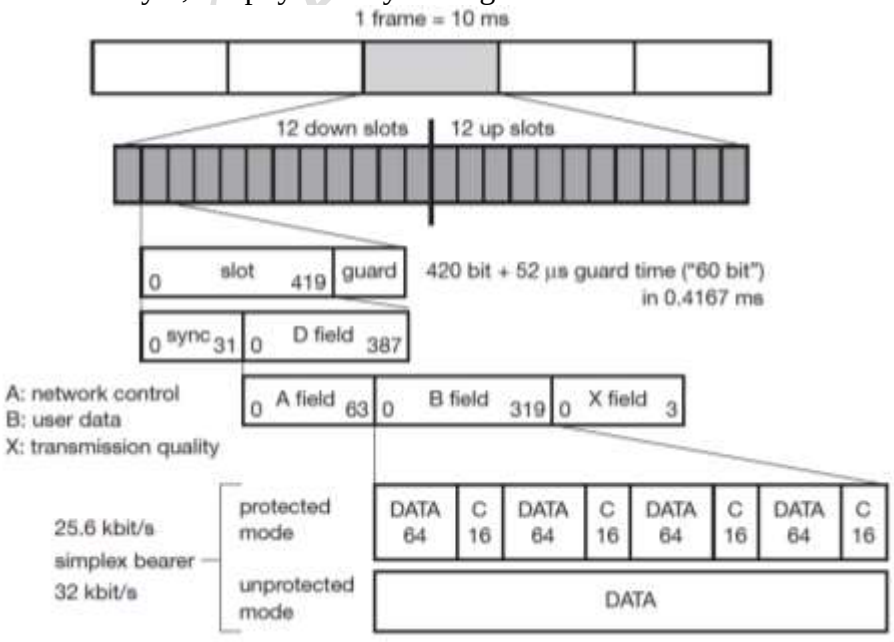
Protocol architecture

- The DECT protocol reference architecture follows the OSI reference model. Figure 2 shows the layers covered by the standard: the physical layer, medium access control, and data link control for both the control plane (C-Plane) and the user plane (U-Plane).
- An additional network layer has been specified for the C-Plane, so that user data from layer two is directly forwarded to the U-Plane. A management plane vertically covers all lower layers of a DECT system.



Physical layer

- As in all wireless networks, the physical layer comprises all functions for modulation/ demodulation, incoming signal detection, sender/receiver synchronization, and collection of status information for the management plane.
- This layer generates the physical channel structure with a certain, guaranteed throughput. On request from the MAC layer, the physical layer assigns a channel for data transmission.



- Figure 3 shows the standard TDMA frame structure used in DECT and some typical data packets. Each frame has duration of 10 ms and contains 12 slots for the downlink and 12 slots for the uplink in the basic connection mode.

- If a mobile node receives data in slot s, it returns data in slot s+12. An advanced connection mode allows different allocation schemes. Each slot has duration of 0.4167 ms and can contain several different physical packets.
- Typically, 420 bits are used for data; the remaining 52 µs are left as guard space. The 420 data bits are again divided into a 32 bit synchronization pattern followed by the data field D.
- The fields for data transmission now use these remaining 388 bits for network control (A field), user data (B field), and the transfer of the transmission quality (X field).
- While network control is transmitted with a data rate of 6.4 kbit/s (64 bit each 10 ms), the user data rate depends on additional error correction mechanisms.
- The simplex bearer provides a data rate of 32 kbit/s in an unprotected mode, while using a 16 bit CRC checksum C for a data block of 64 bit in the protected mode reduces the data rate to 25.6 kbit/s.
- A duplex bearer service is produced by combining two simplex bearers. DECT also defines bearer types with higher throughputs by combining slots, e.g., the double duplex bearer offers 80 kbit/s full-duplex.

Medium access control layer

- The medium access control (MAC) layer establishes, maintains, and releases channels for higher layers by activating and deactivating physical channels.
- MAC multiplexes several logical channels onto physical channels. Logical channels exist for signaling network control, user data transmission, paging, or sending broadcast messages.
- Additional services offered include segmentation/reassembly of packets and error control/error correction.

Data link control layer

- The data link control (DLC) layer creates and maintains reliable connections between the mobile terminal and the base station.
- Two services have been defined for the C-Plane: a connectionless broadcast service for paging (called Lb) and a point-to-point protocol similar to LAPD in ISDN, but adapted to the underlying MAC (called LAPC+Lc).
- Several services exist for the U-Plane, e.g., a transparent unprotected service (basically a null service), a forward error correction service, rate adaptation services, and services for future enhancements.
- If services are used, e.g., to transfer ISDN data at 64 kbit/s, then DECT also tries to transfer 64 kbit/s. However, in case of errors, DECT raises the transfer rate to 72 kbit/s, and includes FEC and a buffer for up to eight blocks to perform ARQ.
- This buffer then introduces an additional delay of up to 80 ms.

Network layer

- The network layer of DECT is similar to those in ISDN and GSM and only exists for the C-Plane. This layer provides services to request, check, reserve, control, and release resources at the fixed station (connection to the fixed network, wireless connection) and the mobile terminal (wireless connection).
- The mobility management (MM) within the network layer is responsible for identity management, authentication, and the management of the location data bases.
- Call control (CC) handles connection setup, release, and negotiation.
- Two message services, the connection oriented message service (COMS) and the connectionless message service (CLMS) transfer data to and from the interworking unit that connects the DECT system with the outside world.

2. Explain WiMax **(Winter-2013)[L.J.I.E.T]**

- 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).

What is 802.16a ?

- WiMAX is such an easy term that people tend to use it for the 802.16 standards and technology themselves, although strictly it applies only to systems that meet specific conformance criteria laid down by the WiMAX Forum.
- The 802.16a standard for 2-11 GHz is a wireless metropolitan area network (MAN) technology that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.
- It can be used to connect 802.11 hot spots to the Internet, provide campus connectivity, and provide a wireless alternative to cable and DSL for last mile broadband access.

WiMax Speed and Range

- WiMAX is expected to offer initially up to about 40 Mbps capacity per wireless channel for both fixed and portable applications, depending on the particular technical configuration chosen, enough to support hundreds of businesses with T-1 speed connectivity and thousands of residences with DSL speed connectivity. WiMAX can support voice and video as well as Internet data.
- WiMax developed to provide wireless broadband access to buildings, either in competition to existing wired networks or alone in currently unserved rural or thinly populated areas. It can also be used to connect WLAN hotspots to the Internet. WiMAX is also intended to provide broadband connectivity to mobile devices. It would not be as fast as in these fixed applications, but expectations are for about 15 Mbps capacity in a 3 km cell coverage area.
- With WiMAX, users could really cut free from today's Internet access arrangements and be able to go online at broadband speeds, almost wherever they like from within a MetroZone.
- WiMAX could potentially be deployed in a variety of spectrum bands: 2.3GHz, 2.5GHz, 3.5GHz, and 5.8GHz

Why WiMax ?

- WiMAX can satisfy a variety of access needs. Potential applications include extending broadband capabilities to bring them closer to subscribers, filling gaps in cable, DSL and T1 services, WiFi, and cellular backhaul, providing last-100 meter access from fibre to the curb and giving service providers another cost-effective option for supporting broadband services.
- WiMAX can support very high bandwidth solutions where large spectrum deployments (i.e. >10 MHz) are desired using existing infrastructure keeping costs down while delivering the bandwidth needed to support a full range of high-value multimedia services.
- WiMAX can help service providers meet many of the challenges they face due to increasing customer demands without discarding their existing infrastructure investments because it has the ability to seamlessly interoperate across various network types.
- WiMAX can provide wide area coverage and quality of service capabilities for applications ranging from real-time delay-sensitive voice-over-IP (VoIP) to real-time streaming video and non-real-time downloads, ensuring that subscribers obtain the performance they expect for all types of communications.

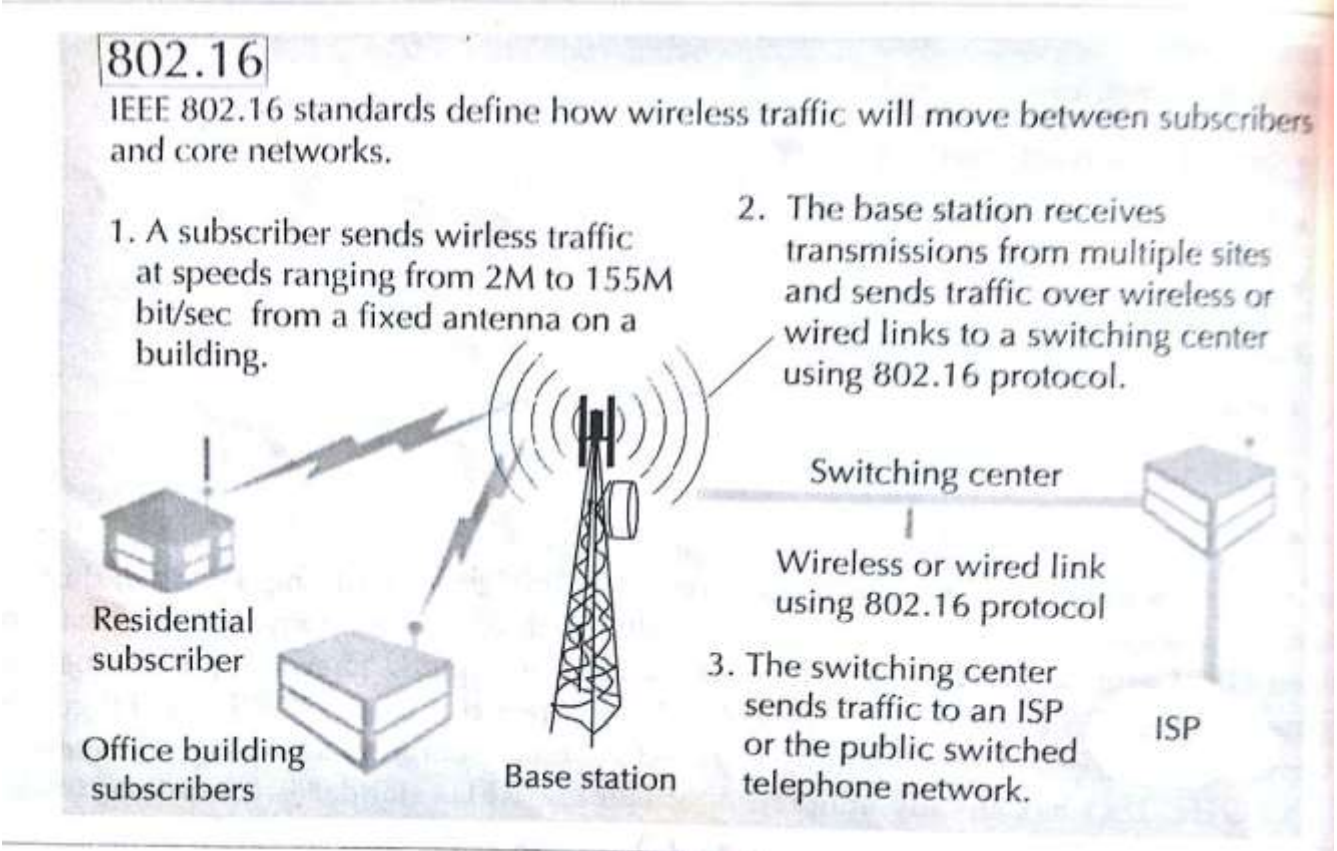
- WiMAX, which is an IP-based wireless broadband technology, can be integrated into both wide-area third-generation (3G) mobile and wireless and wireline networks allowing it to become part of a seamless anytime, anywhere broadband access solution.
- Ultimately, WiMAX is intended to serve as the next step in the evolution of 3G mobile phones, via a potential combination of WiMAX and CDMA standards called 4G.

WiMAX Goals

- A standard by itself is not enough to enable mass adoption. WiMAX has stepped forward to help solve barriers to adoption, such as interoperability and cost of deployment. WiMAX will help ignite the wireless MAN industry by defining and conducting interoperability testing and labeling vendor systems with a "WiMAX Certified™" label once testing has been completed successfully.

3. Explain architecture of IEEE 802.16 standard **[New] (Winter-2012)[L.J.I.E.T]** 7

- The World is moving towards a convergence of voice, data, and video. This convergence will demand interoperability and high data rate. Keeping this in mind, the IEEE 802 Committee set up the 802.16 working group in 1999 to develop wireless broadband or wirelessMAN (wireless metropolitan area network) standards.
- Wireless MAN offers an alternative to high bandwidth wireline access networks like fiber optic, cable modems and DSL (Digital Subscriber Line).



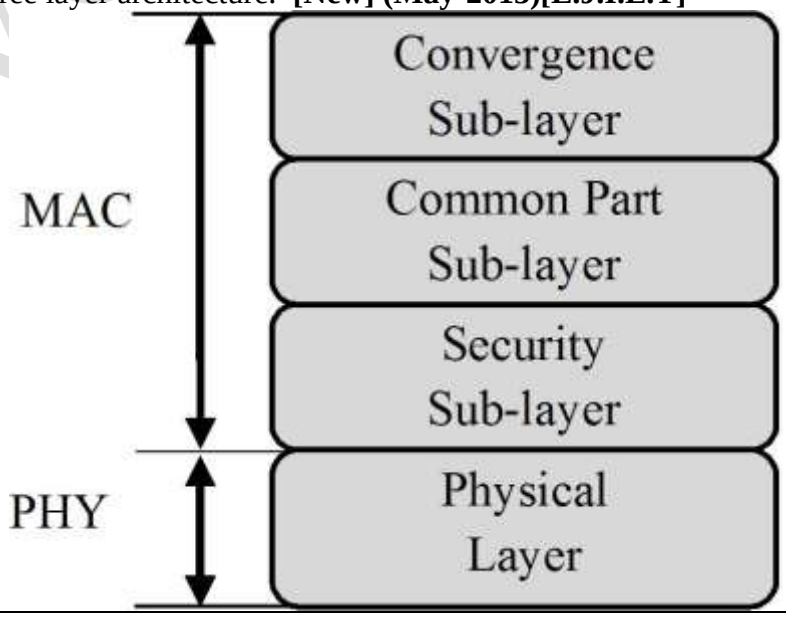
- The release of wirelessMAN (IEEE 802.16) standards in April 2002 has paved the way for the entry of broadband wireless access as a new bearer to link homes and businesses with core telecommunications network access to buildings through exterior antennas communicating with radio base stations.
- The technology is expected to provide less expensive access with more ubiquitous broadband access with integrated data, voice and video services.

- One of the most attractive aspects of wireless broadband technology is that networks can be created in just weeks by developing a small number of base stations on building or poles to create high-capacity wireless access systems.
- In a wired set up, one physical wire will connect the device with the network. Also, we need to keep many wires reserved for future growth. Therefore, the initial investment in wired infrastructure is very high. Wireless network can grow as the demand increases.
- At any point in time the numbers of active users are always a fraction of the number of subscribers. In a wireless environment the number of channels is always low compared to the number of subscribers. This makes wireless technologies very attractive to the service providers.

- IEEE 802.16 standardizes the air interface and related functions associated with WLL. Three working Groups have been chartered to produce following standards.
  - IEEE 802.16.1-Air interface for 10 to 66 GHz.
  - IEEE 802.16.2-Cpexistence of broadband wireless access systems.
  - IEEE 802.16.3-Air interface for licensed frequencies, 2 to 11 GHz.
  - Extensive radio spectrum is available in frequency bands from 10 to 66 GHz worldwide. In a business scenario, 802.16 can serve as a backbone for 802.11 networks. Other possibilities are using 802.16 within the enterprise along with 802.11a, b or g.

- 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 three-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 (MAC) 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 being provided. For IEEE 802.16.1, bearer services include digital audio/video multicast, digital telephony, ATM, Internet access, wireless trunks in telephone network and frame relay.

4. Explain WiMAX three layer architecture. **[New] (May-2013)[L.J.I.E.T]** 7



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 three-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 (MAC) 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 being provided. For IEEE 802.16.1, bearer services include digital audio/video multicast, digital telephony, ATM, Internet access, wireless trunks in telephone network and frame relay.

Physical Layer:

- To support duplexing, 802.16 adapted a burst design that allows both Time division duplexing (TDD) and Frequency division duplexing (FDD).
- In TDD the uplink and downlink share a channel but do not transmit simultaneously.
- In case of FDD the uplink and downlink operate on separate channels and sometimes simultaneously.
- Support for Half-duplex FDD subscriber stations is also supported in 802.16.
- Both TDD and FDD alternatives support adaptive burst profiles in which modulations and coding options may be dynamically assigned on a burst-by-burst basis.
- The 2-11 GHz bands, both licensed and unlicensed, are used in 802.16.
- Design of the 2-11 GHz physical layer is driven by the need for no line of sight operation.
- The draft currently specifies that complaint systems implement one of three air interface specifications, each of which provides for interoperability.
- The 802.16 standard specifies three physical layer for services:
    - Wireless MAN-SC2: This uses a single carrier modulation format. This is to support existing networks and protocols.
    - Wireless MAN-OFDM: This uses orthogonal frequency division multiplexing with 256 point transform. Access is by TDMA, This air interface is mandatory for license-exempt bands.
    - Wireless MAN-OFDMA: This uses orthogonal frequency division multiple access with a 2048 point transform. In this system, multiple access is provided by addressing a sub set of the multiple carriers to individual receivers.

Medium Access Control:

- The MAC layer is subdivided into three sub-layers, namely Service Specific Convergence Sub-layer (CS), Common Part Sub-layer (CPS) and Security Sub-layer (SS)
- The IEEE 802.16 MAC protocol was designed for point to multipoint broadband wireless access.
- It addresses the need for very high bit rates, both uplink and downlink.
- To support, a variety of services like multimedia and voice, the 802.16 MAC is equipped to accommodate both continuous and bursty traffic.
- To facilitate the more demanding physical environment and different service requirements of the frequencies between 2 and 11 GHz, the 802.16 project is upgrading the MAC to provide automatic repeat request (ARQ) and support for mesh, rather than only point-to-multipoint, network architectures.

	• The service specific convergence sub-layer communicates with higher layers and receives packets from them and then do some specific functions like packet/frame classification and header suppression. • Next, it encapsulates these packets into MAC Service Data Unit (MAC SDU) format, and then distributes MAC SDUs to common part sub-layer. Asynchronous Transfer Mode (ATM) convergence and packet convergence sub-layers are two types of service specific convergence sub-layer. • The ATM convergence sub-layer is used for ATM networks, and the packet convergence sub-layer is used for packet services like Ethernet, IPv4 and IPv6. • The main part of the IEEE 802.16 standard is common part sub-layer which is responsible for bandwidth allocation, connection management, scheduling, connection control, automatic repeat request and QoS enforcement. • The security sub-layer is responsible for providing authentication, authorization and secured key exchange. It is also used for encryption and decryption of data from the MAC layer to PHY layer and vice versa. Two main protocols of security sub-layer are: o Encapsulation Protocol, which is used for ciphering operations on data in the networks, o PKM protocol, which is used for secure key distribution between BS and MSs, and also it enables the BS to enforce conditional access to network services	
	TOPIC 5. Mobile IP and Wireless Application Protocol	
	DESCRIPTIVE QUESTIONS	
1.	What are limitations of traditional IP to support the mobile technology? How does Mobile IP works? **(June-2012) [L.J.I.E.T]** What is cellular IP? Establish its relationship with mobile IP. **[New] (June-2014)[L.J.I.E.T]** Why conventional network IP is not suitable for mobile environment? How Mobile IP works? **[New] (May-2013)[L.J.I.E.T]** Why conventional network IP is not suitable for mobile environment? Describe the way in which Mobile IP works? **[New] (Dec-2014)[L.J.I.E.T]** Explain how does mobile IP work? What are the challenges with mobile IP with respect to high speed mobility? How does cellular IP solve some of these challenges? **(Dec-2012)[L.J.I.E.T]** Compare: IP and Mobile IP. **(Summer-2014) (Winter-2015)[[L.J.I.E.T]** **Limitation of Traditional IP:** • When two devices use TCP/IP connection to establish a data connection they need a TCP port and target IP address. The TCP port number is fixed for an application and has a constant value. However, IP address is dependent on the network and modifies as the network changes. • Secondly if the user is operating a desktop device the IP address is static as the point of attachment is fixed. However, if the user is using a portable device like tablet, laptop, PDAs etc. configured with wi-fi as the user moves the point of attachment will modify. This change in point of attachment will require a new IP address and force the session to be terminated • To avoid these drawbacks and supporting mobility to the new devices "Mobile IP" was introduced • Mobile IP (or MIP) is a communications protocol to allow mobile device users to move from one network to another while maintaining a permanent IP address. • The Mobile IP allows location-independent routing of IP datagrams on the Internet • Every mobile terminal is identified by its own address irrespective of its current location in the Internet	8, 7, 7, 7, 7, 7, 7

- When user is away from its home network, its mobile node is associated with a proxy address which identifies its current location and its home address is linked with the local endpoint of a tunnel to its home network.
- Mobile IP specifies how a mobile node registers with its home network. It also specifies how the network routes the data to the mobile node.
- With the help of Mobile IP a user can send and receive the data from any point in the network irrespective of its location in network. But this poses a security problem of redirection attacks
- A redirection attack happens when a suspicious user provides wrong information to the home agent in the mobile IP network
- The home network is intimated that the user has new proxy address and thus all IP data addressed to the original user are redirected to the suspicious user
- Internet Protocol (IP) routes packets from a source endpoint to a destination endpoint through various routers.
- An IP address of a host can be considered to be a combination of network address and node address
- The network portion of an IP address is used by routers to deliver the packet to the last router in change to which the target computer is attached. This last router then uses the host portion of the IP address to deliver the other IP packet to the destination computer.
- In additional to IP addresses of the host for meaning full communication we need the TCP or UDP port of the application.
- A TCP connection is identified by a quadruplet that contains the IP addresses and port number of the sender and point along with the IP address and port number of the receiving end point.
- To ensured that an active TCP connection is not terminated while the user is mobile, it is essential that all of this four identifier remain constant.
- The TCP ports are application specific and generally constant.
- However, the IP address change from subnet to subnet. Therefore, to fix this problem mobile IP allows the mobile node to use two IP addresses. Which are given bellow.
  1. Home address
  2. Care-of address
- The home address is static and known to everybody as the identity of the host.
- The Care-of address changes at each new point of attachment and can be thought of as the mobile nodes location specific address.
- When the mobile node is roaming and is attached to a foreign network, the home agent receives all the packets for the mobile node and arranges to forward them to the mobile nodes current point of attachment.
- The network node that is responsible for forwarding and managing this transparency is known as the home agent.
- Whenever the mobile node moves, it registered its new care-of address with its home agent.
- The home agent forward the packet to the foreign network using the care-of address.
- The delivery requires that the packet header is modified so that the care-of address becomes the destination IP address.

2. How does Mobile IP works? Also briefly explain Mobile Computing OS. **(Winter-2014) [L.J.I.E.T]** 7
How does the Mobile IP work? Explain its architecture. **(Winter-2013) (Summer-2015) [L.J.I.E.T]**
What do you mean by mobile IP? How does mobile IP work? **[New] (Dec-2016)[L.J.I.E.T]**
Explain operation of Mobile IP. **[New] (Nov-2016) [L.J.I.E.T]**
Explain how the Mobile IP works. **(May-2018)[L.J.I.E.T]**
What are the needs of Mobile IP? Explain handoff operation in Mobile IP. **(May-2017)[L.J.I.E.T]**

How Mobile IP works / Architecture of Mobile IP:

- As the user moves, the point of attachment will change from one subnet to another subnet resulting in a change of IP address. This will force the connection to terminate. Therefore, the technology for allowable mobility while a data connection is alive is known as "Mobile IP".
- The Term 'Mobile' in 'Mobile IP' signifies that, while a user is connected to applications across the Internet and 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 system.
- In cellular network, when a user is mobile, the point of attachment changes. However, in spite of such changes the user is able to continue the conversation.

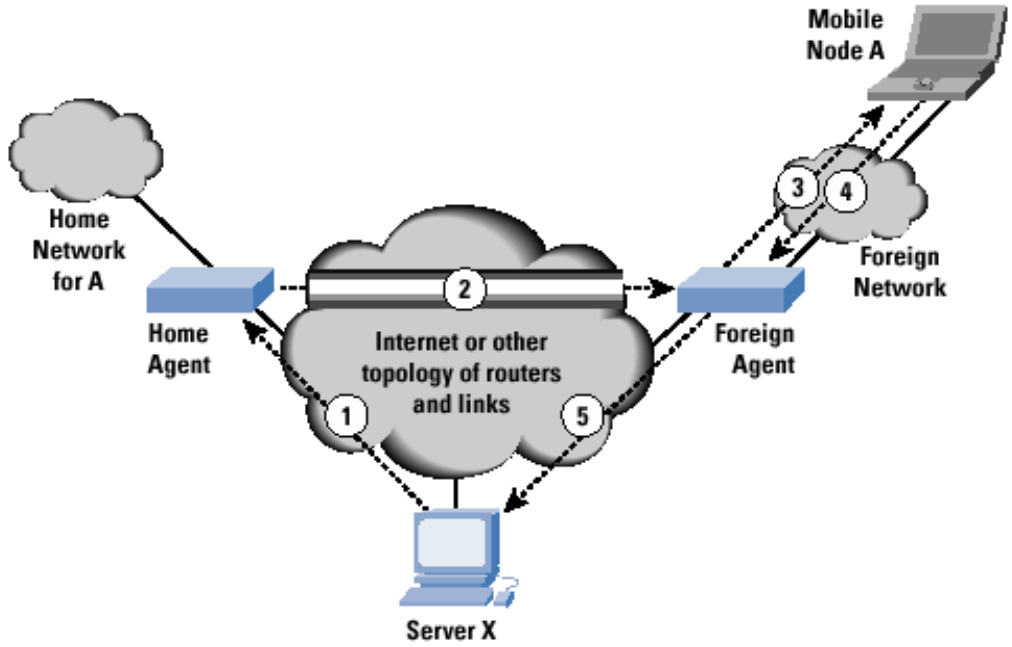
How Does Mobile IP Works?

- Internet Protocol (IP) routes packets from a source endpoint to a destination endpoint through various routers.
- An IP address of a host can be considered to be a combination of network address and node address
- The network portion of an IP address is used by routers to deliver the packet to the last router in change to which the target computer is attached. This last router then uses the host portion of the IP address to deliver the other IP packet to the destination computer.
- In additional to IP addresses of the host for meaning full communication we need the TCP or UDP port of the application.
- A TCP connection is identified by a quadruplet that contains the IP addresses and port number of the sender and point along with the IP address and port number of the receiving end point.
- To ensured that an active TCP connection is not terminated while the user is mobile, it is essential that all of this four identifier remain constant.
- The TCP ports are application specific and generally constant.
- However, the IP address change from subnet to subnet. Therefore, to fix this problem mobile IP allows the mobile node to use two IP addresses. Which are given bellow.
  1. Home address
  2. Care-of address
- The home address is static and known to everybody as the identity of the host.
- The Care-of address changes at each new point of attachment and can be thought of as the mobile nodes location specific address.
- When the mobile node is roaming and is attached to a foreign network, the home agent receives all the packets for the mobile node and arranges to forward them to the mobile nodes current point of attachment.
- The network node that is responsible for forwarding and managing this transparency is known as the home agent.
- Whenever the mobile node moves, it registered its new care-of address with its home agent.
- The home agent forward the packet to the foreign network using the care-of address.
- The delivery requires that the packet header is modified so that the care-of address becomes the destination IP address.
- This new header encapsulates the original packet, causing the mobile nodes home address to have no impact on the encapsulated packets routing. This phenomenon is called tunneling.

Figure shows in general terms how mobile IP deals with the problem of dynamic IP address.

- Let us take an example of IP datagrams being exchanged over a TCP connection between the mobile node (A) and another host (Server X), this following steps occurs

- **Step 1:** Server X wants to transmit an IP datagram to node A. the home address of A is advertised and known to X. X does not know whether A is in the home network or some ware else. Therefore, X send the packet to A with A's home address as the destination IP address in the IP header. The IP datagram is routed A's home network.
- **Step 2:** at 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 home agent. 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.
- **Step 3:** at the foreign network the IP datagram is intercepted by the foreign agent. The foreign agent is the counter part of the home agent in the foreign network. The foreign agent strips off the outer IP header, and delivers the original datagram to A.
- **Step 4:** A intends to response to this massage 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 send to some router in the foreign. Typically, this router is the foreign agent. A uses X's IP address as the destination address.



The mobile IP needs to support three basic capabilities,

1. **Discovery:** a mobile node uses discovery procedure to identifies prospective home agents and foreign agents.
2. **Registration:** a mobile node uses a registration procedure to inform its home agent of its care-of address.
3. **Tunnelling:** tunnelling procedure is used to forward IP datagram from a home address to a care-of address.

Mobile Operating Systems:

- 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, Palm be enabled immediately on mobile devices without any redevelopment. MXI allows for interoperability between various platforms, networks, software and hardware components.

3. Explain tunnelling and encapsulation in mobile IP. **(Nov-2011)[L.J.I.E.T]** 7
Explain tunnelling operation in Mobile IP. Discuss the new fields in Mobile IP other than IP. **[New](May-2017) [L.J.I.E.T]**
What is Mobile IP? Explain the tunnelling in context of Mobile IP. **(Summer-2013) [New] (May-2015) [L.J.I.E.T]**
Explain the tunnelling Operation in Mobile IP. **[New] (May-2013)[L.J.I.E.T]**
How mobile IP works? Explain tunnelling with mobile IP. **[New] (Dec-2015)[L.J.I.E.T]**
What is a mobile IP? Explain discovery, registration and tunnelling with mobile IP. **[New] (June-2014) [New] (May- 2016) (Nov-2017) [New](May-2018) [L.J.I.E.T]**

- **Discovery:**
  - This procedure is used to identify the home agents and foreign agents.
  - It the router detects any new mobile node, it sends a router advertisement message for knowing the point of attachment to internet.

- The discovery procedure is on top of existing router discovery
- The discovery procedure can be used to determine whether a node is home network or foreign network
- A router advertisement message is periodically sent to compare the address of the network part of the IP with router IP address assigned by the home network. If the data matches, mobile node is in the home network otherwise the mobile node is in foreign network

- **Registration:**
  - Once a mobile node gets a care of address from the foreign agent, it needs to be registered with the home agent using the care-of-address.
  - With the care-of address information the mobile node issues a registration request to the home agent.
  - The home agent responds by updating the routing table and sending a registration replay to the mobile node.

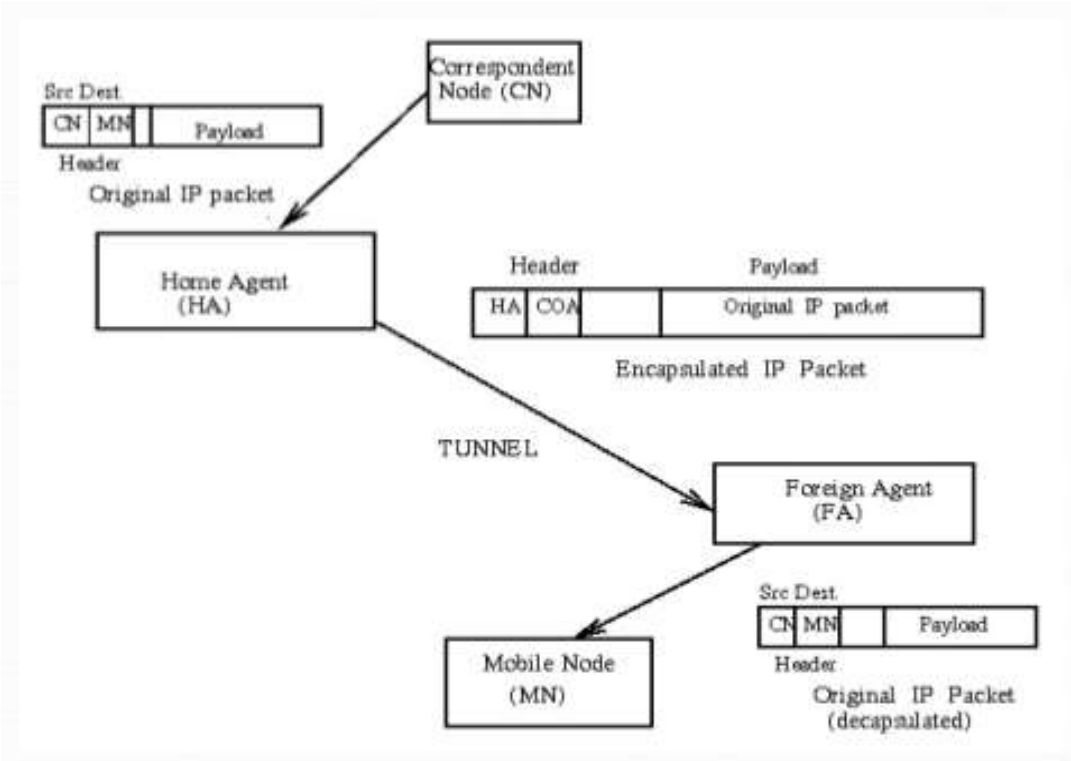
  Authentication:
  - Authentication is a necessary step for registration. Every mobile node needs to be authenticated
  - With the help of HMAC-MD5 hashing algorithm and 128 bit secrete key a digital signature is generated
  - The digital signature is unique. The home agent along with the mobile node share a common key for authentication so that it is unknown to hackers
  - The home agent contains a binding for the mobile node referred to as the triplet. It comprises the registration lifetime, home address and care of address
  - Following is the list of registration steps
    - **Step 1:** The mobile node sends a request for registration to the foreign agent. The mobile node request for forwarding service from the foreign agent.
    - **Step II:** The registration request is relayed by the of foreign agent to the mobile nodes home agent.
    - **Step III:** The registration request is accepted/rejected by the home agent. The home agent sends a registration reply to the foreign agent.
    - **Step IV:** The reply message is relayed by the foreign node to the mobile node that requested registration.
  - The mobile node can behave as its own foreign agent with a co-located care of address. This address is IP address got from mobile that relates to the foreign network. Registration is done directly with the home agent when the mobile node uses a co-located care of address

- **Tunnelling and Encapsulations:**

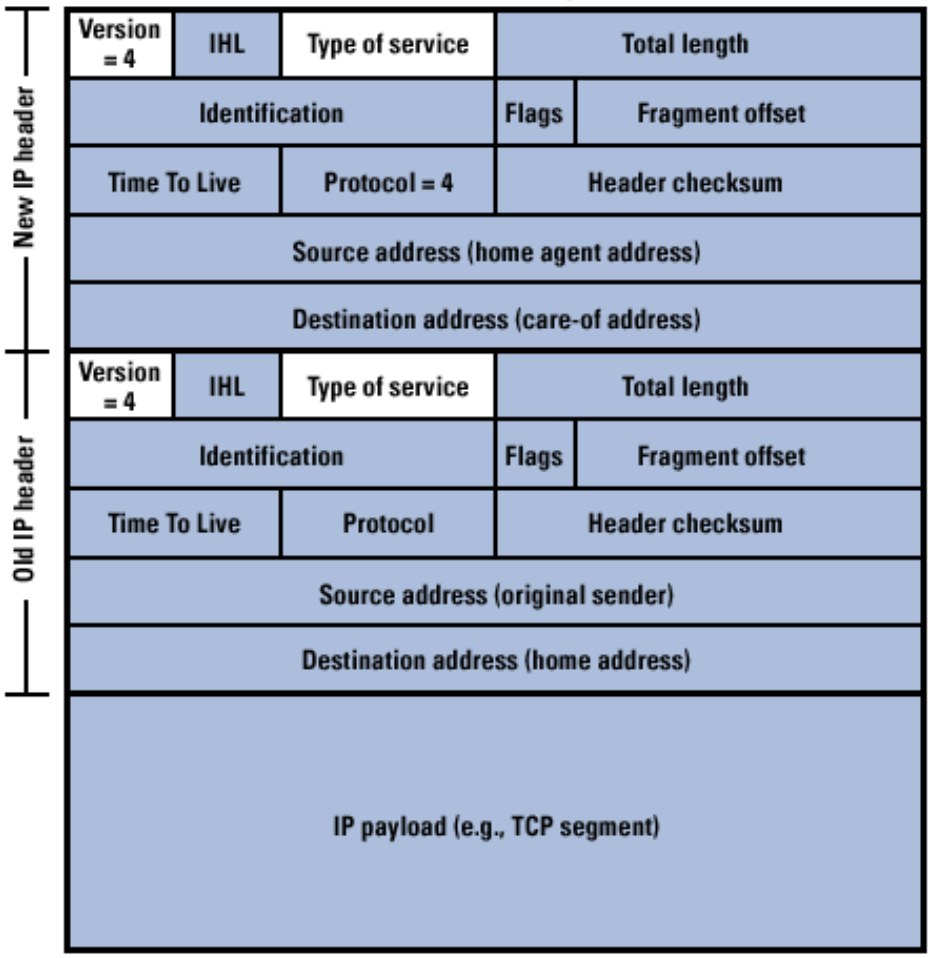
  Tunnelling:
  - A tunnel creates a virtual pipe so that data packets can travel from the start to the end of the tunnel. Tunnelling is done through IP within IP encapsulation.

  Encapsulation:
  - Encapsulation is a method where the data packet comprises a packet header and data and then a new packet is created by combining them. A reverse method is following for encapsulation.
  - 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.
  - The tunnel header uses 4 as the protocol number, indicating that the next protocol header is again an IP header.

- 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.s



(a) IP-within-IP encapsulation



Unshaded fields are copied from the inner IP header to the outer IP header.

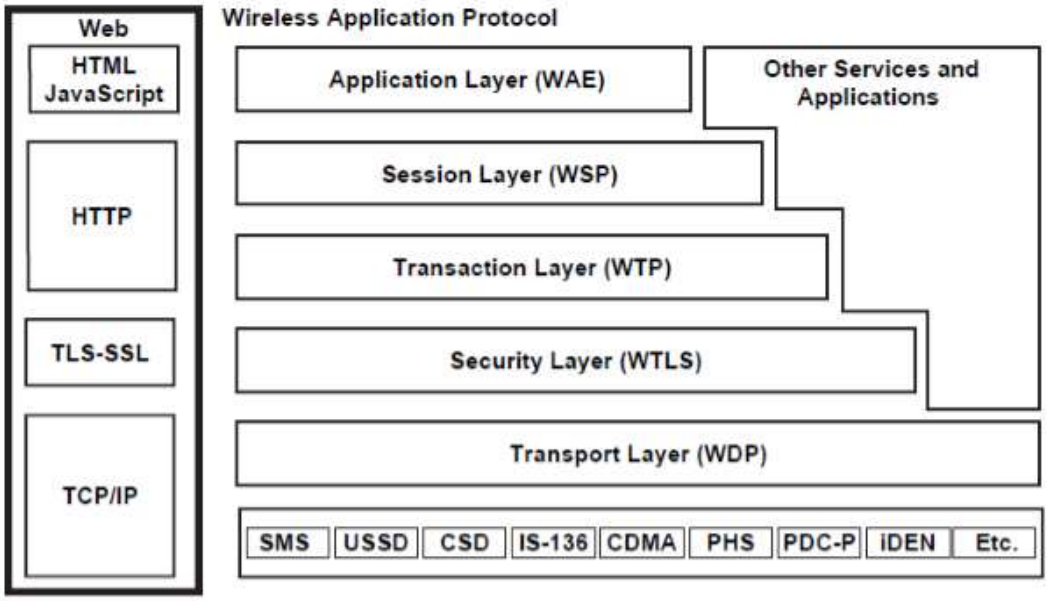
- Once the foreign agent receives the data packet, the tunnel header is dropped and remaining data packet is delivered to the mobile node.
- AN ARP (Address Resolution Protocol) is sued for providing notifications to all the mobile nodes in the home network.
- When the mobile node is in a foreign network, the data packets sent to the mobile should be available to the home agent so that they can be sent through tunnelling.

4. Describe the WAP protocol stack. What are the functions of different layers in this protocol stack? **(Dec-2012)[L.J.I.E.T]** — 7
Describe the WAP protocol stack while enumerating the functions of different layers. **(Summer-2013)[L.J.I.E.T]** — 7
Explain the WAP Layered architecture and protocol stack. **[New] (May-2013) [New] (Dec-2014) [L.J.I.E.T]** — 6
Explain Wireless Application Protocol (WAP) in detail. **(Nov-2017)[L.J.I.E.T]** — 7
Explain the WAP Stack with neat diagram. **(May-2018)[L.J.I.E.T]** — 7
Explain : Spread Spectrum and WAP. **(Summer-2014) (Winter-2015)[L.J.I.E.T]** — 7
Write a short note on: WAP **[New] (Dec -2016) [New](May-2018)[L.J.I.E.T]** — 3

WAP Architecture

- It provides a scalable and extensible environment for application development of mobile
- This is achieved using layered design of protocol stack. The layers resemble the layers of OSI model.

- Each layer is accessible by layers above as well as by other services and applications through a set of well-defined interface.
- External applications may access session, transaction, security and transport layers directly.



Wireless Application Environment

- WAE is the uppermost layer in the WAP stack. It is general purpose environment based on combination of WWW and mobile telephony technologies.
- Its primary objective is to achieve interoperable environment that allows operators and service providers to build applications that can reach wide variety of wireless platforms.
- It uses URL and URI for addressing. Language used is WML and WML script. WML script can be used for validation of user input.

User Agent

- Technically user agent significant who works on behalf of the users.
- In WWW and WAE context, user agent is the user facing browser software.
- In WAE this is generally referred to as micro-browser.
- WAE allows the integration of domain-specific user agents as well.

User Agent Profile (UAProf)

- The UAProf specification allows WAP to notify the content server about the device capability.
- UAProf is also referred to as Capability and preference information (CPI).
- CPI is passed from the WAP client to the origin server through intermediate network points.

Wireless Markup language (WML)

- WML is tag-based document manipulation language. It shares the heritage with HTML of W3C and HDML of Unwired planet.
- WML is designed to specify presentation and user interaction on mobile phones and other wireless devices.
- WML implements a deck and card metaphor.

WMLScript

- WMLScript is an extended subset of JavaScript and forms a standard means for adding

procedural logic to WML decks.

- WMLScript is used to do client side processing. Therefore, it can be used very effectively to add intelligence to the client and enhance the user interface.

Wireless Telephony Application

- WTA provides a means to create telephony services using WAP. It uses WTA Interface (WTAI) which can be evoked from WML and for WML script.
- The Repository makes it possible to store WTA services in device which can be accessed without accessing the network. The access can be based on any event like call disconnect, call answer etc.
- Sometimes, there can be notification to user based on which WTA services are accessed by users. The notification is called WTA service indication.

Wireless Session Protocol.

- WSP provides reliable, organized exchange of content between client and server.
- The core of WSP design is binary form of HTTP. All methods defined by HTTP 1.1 are supported.
- Capability negotiation is used to agree on common level of protocol functionality as well as to agree on a set of extended request methods so that full compatibility to HTTP applications can be retained.
- An idle session can be suspended to free network resources and can be resumed without overload of full-blown session establishment.
- WSP also supports asynchronous requests. Hence, multiple requests will improve utilization of air time.

Wireless Transaction Protocol

- WTP is defined as light-weight transaction-oriented protocol suitable for implementation in thin clients.
- Each transaction has unique identifiers, acknowledgements, duplicates removal and retransmission.
- Class 1 and Class 2 enable user to confirm every received message, however, in class 0, there is no acknowledgement.
- WTP has no security mechanisms and no explicit connection set-up or tear-down phases.

Wireless Transport Layer Security

- WTLS is security protocol based on industry standard transport layer security (TLS). It provides transport layer security between a WAP client and the WAP Gateway/ Proxy.
- The goals of WTLS are data integrity, privacy, authentication, Denial-of-service protection.
- It has features like datagram support, optimized handshake and dynamic key refreshing.

Wireless Datagram Protocol

- WDP provides application addressing by port numbers, optional segmentation and reassembly, optional error detection.
- It supports simultaneous communication instances from higher layer over a single underlying WDP bearer service. The port number identifies higher level entity above WDP.
- The adaptation layer of WDP maps WDP functions directly on to a bearer based on its specific characteristics.
- On the GSM SMS, datagram functionality is provided by WDP.

Optimal WAP Bearers

- The WAP is designed to operate over a variety of different service like SMS,' Circuit Switched Data (CSD)', GPRS,' Unstructured Supplementary Services Data(USSD)'.

5. What is WAE?

ANS:

Wireless Application Environment

- WAE is the uppermost layer in the WAP stack. It is general purpose environment based on combination of WWW and mobile telephony technologies.
- Its primary objective is to achieve interoperable environment that allows operators and service providers to build applications that can reach wide variety of wireless platforms.
- It uses URL and URI for addressing. Language used is WML and WML script. WML script can be used for validation of user input.

User Agent

- Technically user agent significant who works on behalf of the users.
- In WWW and WAE context, user agent is the user facing browser software.
- In WAE this is generally referred to as micro-browser.
- WAE allows the integration of domain-specific user agents as well.

User Agent Profile (UAProf)

- The UAProf specification allows WAP to notify the content server about the device capability.
- UAProf is also referred to as Capability and preference information (CPI).
- CPI is passed from the WAP client to the origin server through intermediate network points.

Wireless Markup language (WML)

- WML is tag-based document manipulation language. It shares the heritage with HTML of W3C and HDML of Unwired planet.
- WML is designed to specify presentation and user interaction on mobile phones and other wireless devices.
- WML implements a deck and card metaphor.

WMLScript

- WMLScript is an extended subset of JavaScript and forms a standard means for adding procedural logic to WML decks.
- WMLScript is used to do client side processing. Therefore, it can be used very effectively to add intelligence to the client and enhance the user interface.

Wireless Telephony Application

- WTA provides a means to create telephony services using WAP. It uses WTA Interface (WTAI) which can be evoked from WML and for WML script.
- The Repository makes it possible to store WTA services in device which can be accessed without accessing the network. The access can be based on any event like call disconnect, call answer etc.
- Sometimes, there can be notification to user based on which WTA services are accessed by users. The notification is called WTA service indication.

WAP Push Architecture

- The WAP push framework allows information to be sent to a client device without pervious user action.
- In a normal client/server model, a client requests for a service or information from a

server. The server then response to this request by transmitting information back to the client. This is referred to a PULL technology.

- Where the client Pulls information from the server. In addition to this type of synchronized request response transaction, WAP offers PUSH Technology.

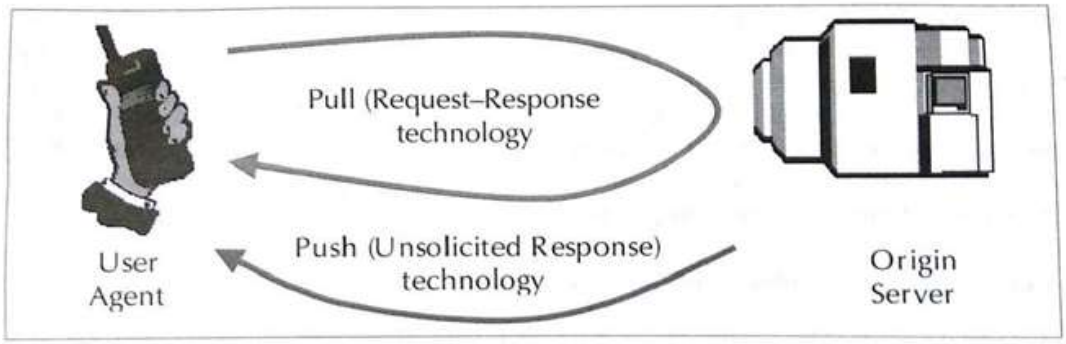
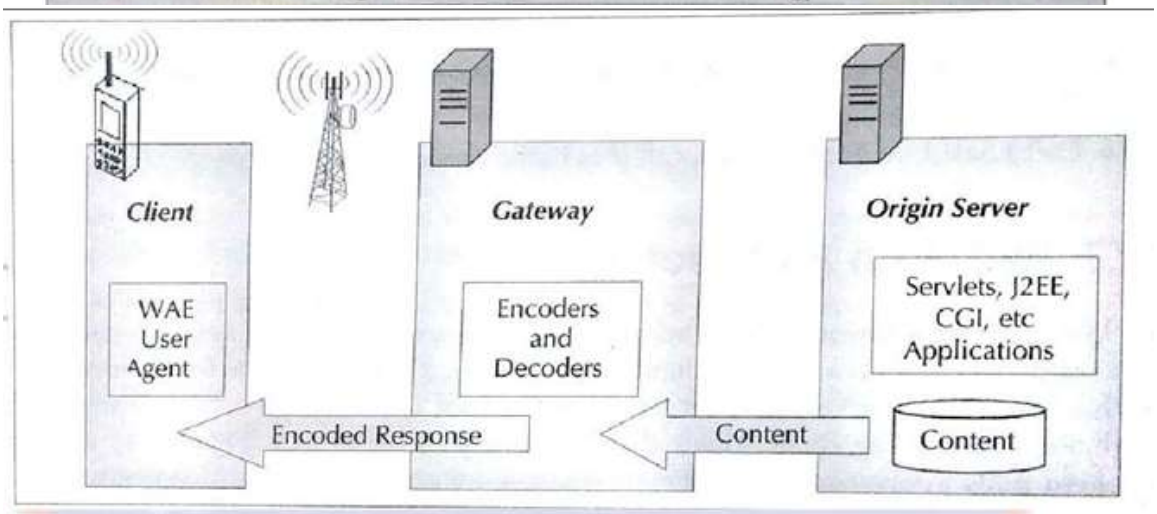


Figure 8.4 Pull versus Push technology



6. Explain the Wireless Session Protocol Primitives and Parameters. **(May-2018)[L.J.I.E.T]**

- WSP provides reliable, organized exchange of content between client and server.
- The core of WSP design is binary form of HTTP. All methods defined by HTTP 1.1 are supported.
- Applications provided by WSP:
  1. Establish a reliable session from client to server and close it in an orderly manner.
  2. Agree on a common level of protocol functionality using capability negotiation
  3. Exchange content between client and server using compact encoding
  4. Suspend and resume session.
- It provides connection oriented and connectionless services.
- Connectionless services is most suitable when do not need reliable delivery of data.
- Connection oriented categories are:
  - Session management facility
  - Method invocation facility
  - Exception reporting facility
  - Push facility
  - Session resume facility

7. Wireless Transaction Protocol (WTP). **(Winter-2013)[L.J.I.E.T]**

- The Wireless transaction Protocol (WTP) runs on top of the datagram service and provides a lightweight transaction-oriented protocol that is suitable for implementation in 'thin' client.

	• WTP allows for interactive browsing (request/response) applications and support three transaction classes: unreliable with no result message, reliable with no result message and reliable with one reliable result message.
	• WTP provides the following features:
	  ○ Class 0: Unreliable one-way requests
	  ○ Class 1: Reliable one-way requests
	  ○ Class 2: Reliable two-way request-reply transactions
	• Optional user-to-user reliability, WTP user triggers the confirmation of each received message.
	• Optional out-of-band data on acknowledgements.
	• PDU concatenation and delayed acknowledgement to reduce the number of message sent
	• Asynchronous transaction.
	• WTP has no security mechanisms and no explicit connection set-up or tear-down phases.
	• WTP supports peer-to-peer, Client/server and multicast applications
	• It requires Low memory.	

8.	State the requirements of WAP and explain different layers of WAP. What are the advantages of WML Script over WML**? (Nov-2011)[L.J.I.E.T]** **Requirement of WAP:** • To after easy, fast delivery of information and services to the mobile user. • To define a layered, extensible and scaled architecture. • To use the existing standards. • To support wireless networks • To support secure communication and secure application • To optimize narrow-band bearer with high latency • To use minimum resources for high efficiency **Advantages of WMLScript over WML:** • JavaScript-based scripting language: WMLScript is based on industry standard JavaScript solution and adapts it to the narrow-band environment • Procedural Logic: It adds the power of procedural logic to WML. • Compiled implementation: It can be compiled down to more space efficient bytecode that is transported to the client. • Event-based: It may be invoked in response to certain user or environment events. • Integrated into WAE: It is fully integrated with the WML browser. It has access to the WML state model and can set and get WML variable. • International support: It supports Unicode 2.0. • Efficient extensible library support: It can be used to expose and extend device functionality without changes to the device software. • Data Types: Following basic data types are supported in it: Boolean, integer, floating-point, string and invalid.	7
9.	Discuss the WAP gateway for coding and encoding. **[New] (June-2014)[L.J.I.E.T]** What is a WAP gateway? What are its functions**? (Dec-2012)[L.J.I.E.T]** **WAP Gateway:** • WAP gateway acts as a middleware which performs coding and encoding between cellular device and the web server.	7

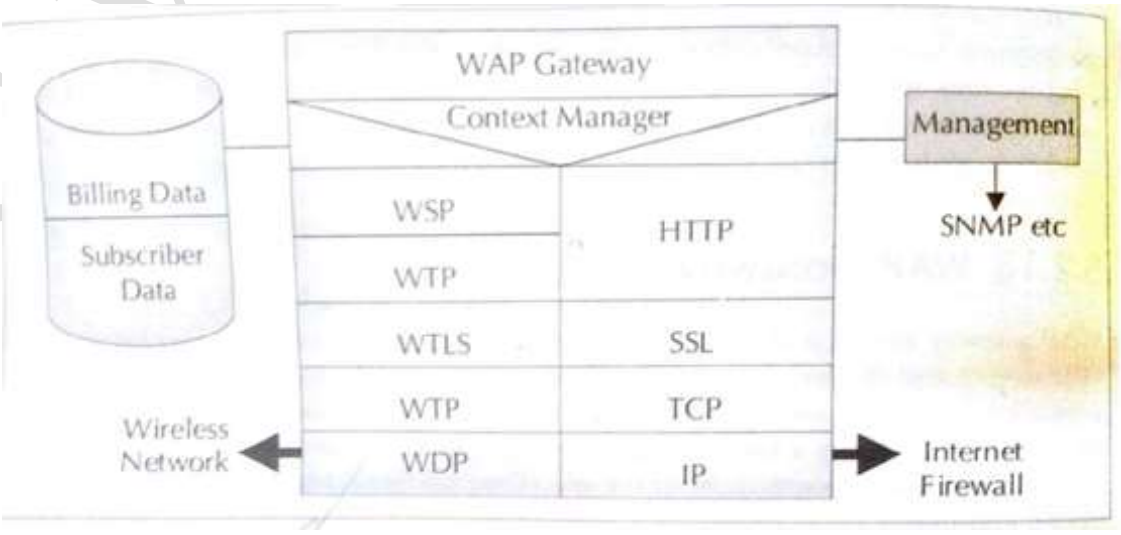
- The WAP gateway can be located either in a telecom network or within a computer data network.
- A user from a WAP device requests for a WAP page using a URL, the gateway establishes a connection to the target WAP site.
- It collects the document from the site. Then the WAP is compiled and converted into binary code.
- Binary code takes far less space compared to the WML source.
- This realizes quicker delivery. The code is then sent across to the phone or the wireless device over the air.
- When the phone receives the stream of octets, it 'de-compiles' it.
- The client browser does the reverse operation of compilation by decompiling the binary code.
- This will allow the client to regenerate the normal WML page and then displays it on the device.
- The WAP phones all have a maximum allowed size for a compiled WAP page.
- The WAP protocols are designed to operate over a variety of different bearer services, including Short message, circuit-switched data, and packet data.
- The bearer offer different levels of quality of service with respect to throughput, error rate, and delays.
- The WAP protocols are designed in such a fashion that it can compensate for or tolerate this varying level of QoS (Quality of Service).

External Interface of a gateway are:

- SMS Center, using various protocols
- HTTP servers, to fetch WML pages
- WAP device using WAP protocol stack

Basic Function of the WAP gateway are:

- Implementing WAP protocol stack
- Protocol translation between phone and server.
- Compress WML pages to save bandwidth.
- User authentication and billing
- To support wireless networks like GSM
- To provide data services to PDA and mobile user
- To support worldwide wireless communication and internet applications
- Together internet contents.



	• Many WAP gateways include additional functions. These relate to user authentication and charging. • For charging, it captures the usage data. The gateway does not actually include a billing system itself but it provides the user and the service provider the usage data. The usage data is given to the billing system of the operator. • From the user's point of view, the gateway is also responsible for optimizing WAP usage as far as possible. The gateway keeps the number of packets small to keep costs down and make the best use of available bandwidth. • WAP is not self-configurable as like Internet. This means that when we move from one network to another network, there may be a need to configure the client device to suit the network parameters of the serving network. • The configuration of WAP requires an IP address of the WAP gateway. Though the WAP gateway can be from home network, due to security and charging reasons, service providers do not allow the usage of external WAP gateways. • Therefore, at a minimum, two parameters needs to be changed. These are the telephone number for the WAP dial-up connection and the IP address of the WAP gateway. The rest can be configured once only.	
10	Explain WAE logical model. **(Winter-2013)[L.J.I.E.T]** What is WAE? Draw its model with client, gateway and server. **[New] (June-2014) [New] (Dec- 2015) [New] (May-2016) [L.J.I.E.T]** • The primary objective of the WAP application environment (WAE) is to provide an interoperable environment to build services in wireless space. • It covers system architecture relating to the user agents, networking schemes, content formats, programming languages and shared services based on WWW technologies. • 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 server. • All content are located using WWW standard URLs. • WAE enhances some of the WWW standard to reflect some of the telephony network characteristics. • A WAP request from the browser (User agent) is routed through a WAP gateway. • The gateway acts as an intermediary between the client and network through a wireless last mile (GSM, GPRS, CDMAs) • The gateway does encoding and decoding of data transferred from and to the mobile user agent. • The purpose of encoding is to minimize the size of data transacted over-the-air. • Reduced data size reduces the computational power required by the client to process that data. • In most cases the WAP gateway resides on TCP/IP network. • The gateway processes the request, retrieves contents from the server using Java servlets, J2EE, CGI scripts, or some other dynamic mechanism. • The data is formatted as WML and returned to the client. The client device can employ logic via embedded WMLScript for client-side processing of WML. • The major elements of the WAE model include: o **WAE User Agents:** User facing client software (Browser). User agents are integrated into the WAP architecture. They interpret network content referenced by a URL. WAE includes user agents for two primary standard contents: Encoded WML and Compiled WMLScript o **Content Generators:** Applications on origin server that extract standard content	7, 7, 7, 7

in response to requests from user agents. Content servers are typically HTTP severs as used in WWW.

- **Standard Content Encoding:** A set of well-defined content encoding, allowing a WAE user agent to navigate web content. Standard content encoding includes compressed encoding for WML, bytecode encoding for WMLScript, standard image formats, business, and calendar data formats.
- **Wireless Telephony Application (WTA):** A collection of telephony specific extensions for call and telephony features control.

- WAE defines a set of user agent capabilities that is exchanged between the client and the server using WSP.
- These capabilities include global device characteristics as WML version, WMLScript version, floating-point support, image formats and so on.

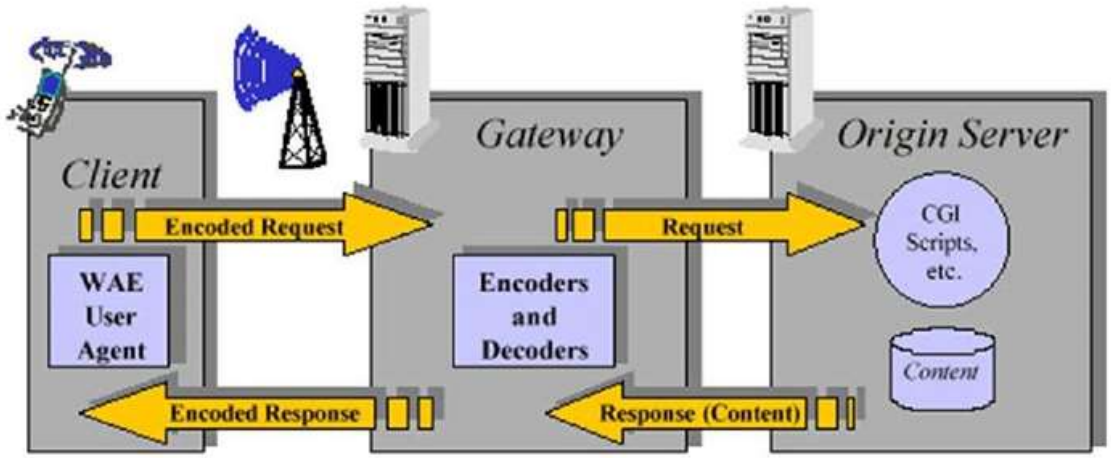


Figure 2: WAE Logical Model