



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 1/46

Important Instructions to examiners:

- 1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
- 2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
- 3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).
- 4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
- 5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
- 6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
- 7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q. 1) a) Attempt any THREE of the following:

12

- (i) List various mobile computing functions.**
(Each Function 1M, Any four)

Ans: Mobile computing can be defined as a computing environment over physical mobility.

The user of the mobile computing environment will be able to access data, information or logical objects from any device in any network while on move.

Functions of Mobile Computing:

1. **User mobility:** User should be able to move from one physical location to another location and use same service
2. **Network mobility:** User should be able to move from one network to another network and use same service
3. **Device mobility:** User should be able to move from one device to another and use same service
4. **Session mobility:** A user session should be able to move from one user-agent environment to another.
5. **Service mobility:** User should be able to move from one service to another
6. **Host mobility:** The user should be either a client or server.

(ii) State any four features of GSM.

(Each feature 1M, Any four)

Ans: Subscriber Identity Module: It is a memory device that stores info such as



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 2/46

subscriber identification no., the networks & countries where the subscriber is entitled for service, privacy keys and other user specific information. The SIM gives the GSM subscriber unit their identity

On –the- air privacy: The privacy is made possible by encrypting the digital bit stream sent by GSM transmitter, according to a secret cryptographic key that is known only to cellular carrier. This key changes with time for each user

The features of GSM are

1. **Call Waiting** - Notification of an incoming call while on the handset
2. **Call Hold**- Put a caller on hold to take another call
3. **Call Barring** - All calls, outgoing calls, or incoming calls
4. **Call Forwarding**- Calls can be sent to various numbers defined by the user
5. **Multi Party Call Conferencing**- Link multiple calls together
6. **Calling Line ID** - incoming telephone number displayed
7. **Alternate Line Service**
 - a. One for personal calls
 - b. One for business calls
8. **Closed User Group** - call by dialing last for numbers
9. **Advice of Charge** - Tally of actual costs of phone calls
10. **Fax & Data** - Virtual Office / Professional Office
11. **Roaming:** services and features can follow customer from market to market.

(iii) Describe GSM Location Update Procedure.

(Location Update Procedure 3M, Diagram: 1M)

Ans: GSM Location Update: The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next. Mobiles are responsible for detecting location area codes. When a mobile finds that the location area code is different from its last update, it performs another update by sending to the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI)

In order to make a mobile terminated call, The GSM network should know the location of the MS (Mobile Station), despite of its movement. For this purpose the MS periodically reports its location to the network using the Location Update procedure.

Location Area (LA)

A GSM network is divided into **cells**. A group of cells is considered a **location area**. A mobile phone in motion keeps the network informed about changes in the location area. If the mobile moves from a cell in one location area to a cell in another location area, the mobile phone should perform a location area update to inform the network about the exact location of the mobile phone.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

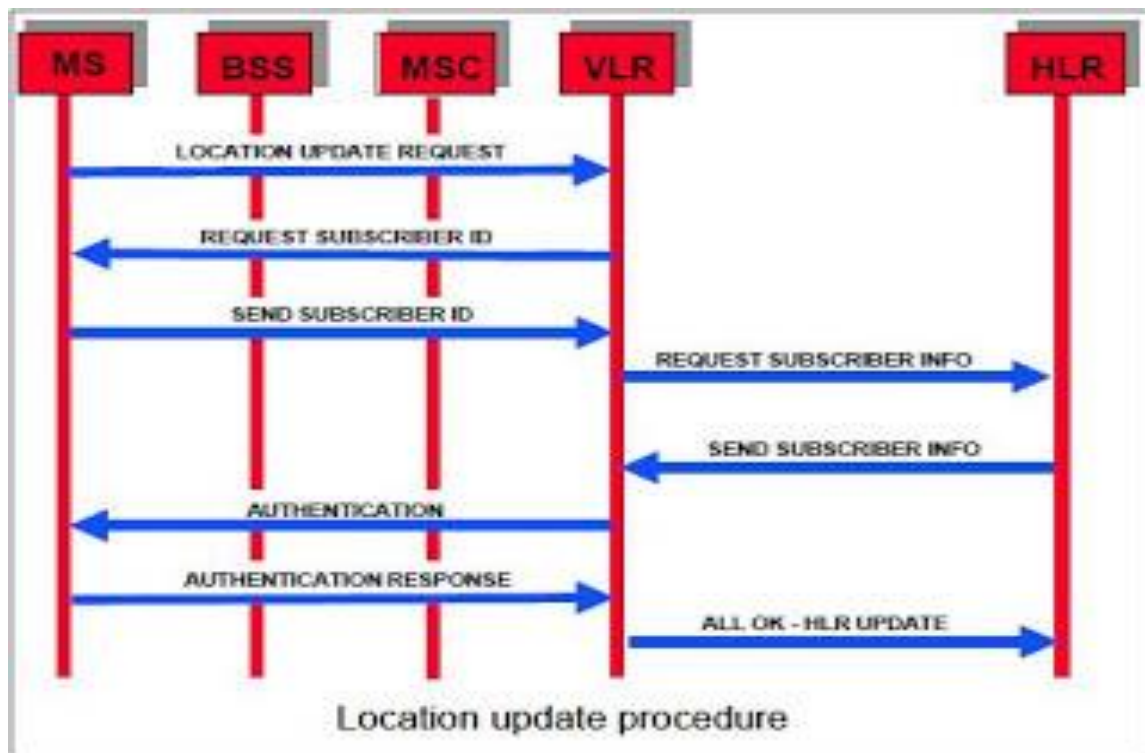
Subject Code: 17632

Model Answer

Page No: 3/46

The Location Update procedure is performed:

- When the MS has been switched off and wants to become active, or
- When it is active but not involved in a call, and it moves from one location area to another.
- After a regular time interval.



The **Location Update process** consists of the following phases

Request for service; the MS detects that it has entered a new Location Area and requests to update its location. The new MSC/VLR identifies the MS.

- Authentication - The new MSC/VLR requests to the AUC for authentication parameters (SRES). Using these parameters the MS is authenticated.
- Ciphering - Using the parameters which were made available earlier during the authentication the uplink and the downlink are ciphered.
- Update HLR/VLR - The new MSC/VLR requests to update the MS location in the HLR. The MS is de-registered in the old VLR.
- TMSI re-allocation - The MS is assigned a new TMSI.



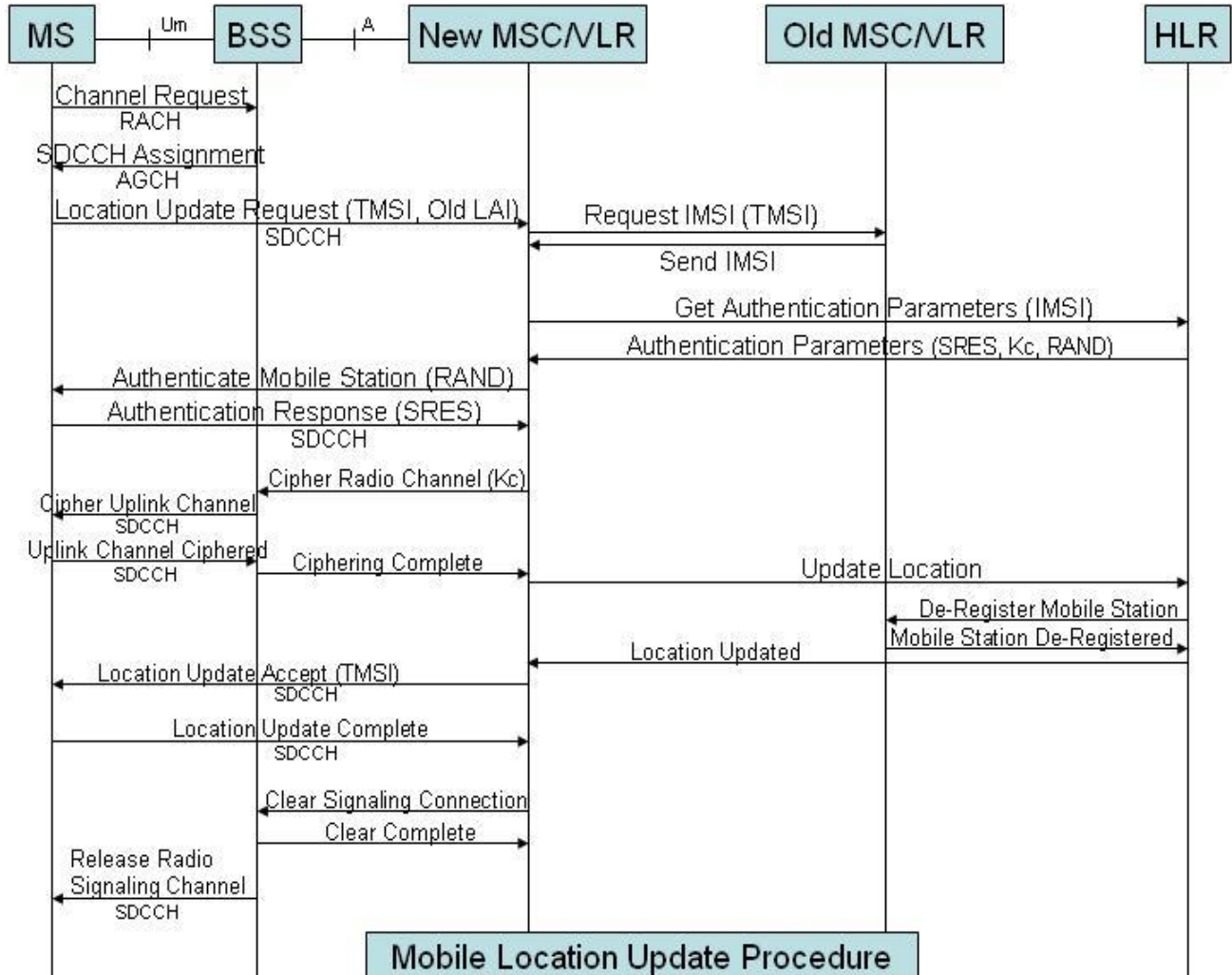
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 4/46



1. The MS detects that it has entered a new Location Area and transmits a Channel Request message over the Random Access Channel (RACH).
2. Once the BSS receives the Channel Request message, it allocates a Stand-alone Dedicated Control Channel (SDCCH) and forwards this channel assignment information to the MS over the Access Grant Channel (AGCH). It is over the SDCCH that the MS will communicate with the BSS and MSC.
3. The MS transmits a location update request message to the BSS over the SDCCH. Included in this message are the MS Temporary Mobile Subscriber Identity (TMSI) and the old Location Area Identification (oldLAI). The MS can identify itself either with its IMSI or TMSI. The BSS forwards the location update request message to the MSC.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 5/46

4. The VLR analyzes the LAI supplied in the message and determines that the TMSI received is associated with a different VLR (old VLR). In order to proceed with the registration, the IMSI of the MS must be determined. The new VLR derives the identity of the old VLR by using the received LAI, supplied in the location update request message. It also requests the old VLR to supply the IMSI for a particular TMSI.
5. The new VLR sends a request to the HLR/AUC (Authentication Center) requesting the “authentication triplets” (RAND, SRES, and Kc) available for the specified IMSI.
6. The AUC, using the IMSI, extracts the subscriber's authentication key (Ki). The AUC then generates a random number (RAND), applies the Ki and RAND to both the authentication algorithm (A3) and the cipher key generation algorithm (A8) to produce an authentication Signed Response (SRES) and a Cipher Key (Kc). The AUC then returns to the new VLR an authentication triplet: RAND, SRES, and Kc.
7. The MSC/VLR keeps the two parameters Kc and SRES for later use and then sends a message to the MS. The MS reads its Authentication key (Ki) from the SIM, applies the received random number (RAND) and Ki to both its Authentication Algorithm (A3) and Cipher key generation Algorithm (A8) to produce an authentication Signed Response (SRES) and Cipher Key (Kc). The MS saves Kc for later, and will use Kc when it receives command to cipher the channel.
8. The MS returns the generated SRES to the MSC/VLR. The VLR compares the SRES returned from the MS with the expected SRES received earlier from the AUC. If equal, the mobile passes authentication. If unequal, all signaling activities will be aborted.
9. The new MSC/VLR requests the BSS to cipher the radio channel. Included in this message is the Cipher Key (Kc), which was made available earlier during the authentication.
10. The BSS retrieves the cipher key, Kc, from the message and then transmits a request to the MS requesting it to begin ciphering the uplink channel.
11. The MS uses the cipher key generated previously when it was authenticated to cipher the uplink channel, and transmits a confirmation over the ciphered channel to the BSS.
12. The BSS upon ciphering the downlink channel sends a cipher complete message to the MSC. At this point, we are ready to inform the HLR that the MS is under control of a new VLR and that the MS can be de-registered from the old VLR.
13. The new VLR sends a message to the HLR informing it that the given IMSI has changed locations and can be reached by routing all incoming calls to the VLR address included in the message.
14. The HLR requests the old VLR to remove the subscriber record associated with the given IMSI. The request is acknowledged.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 6/46

15. The HLR updates the new VLR with subscriber data (mobiles subscriber's customer profile).
16. The MSC forwards the location update accept message to the MS. This message includes the new TMSI.
17. The MS retrieves the new TMSI value from the message and updates its SIM with this new value. The mobile sends then an update complete message back to the MSC.
18. The MSC requests from the BSS that the signaling connection be released between the MSC and the MS.
19. The MSC releases its portion of the signaling connection when it receives the clear complete message from the BSS.
20. The BSS sends a "radio resource" channel release message to the MS and then frees up the Stand-alone Dedicated Control Channel (SDCCH) that was allocated previously. The BSS then informs the MSC that the signaling connections has been cleared.

(iv) Explain in brief streams ciphering and block ciphering.
(Stream Cipher: 2M, Block Cipher: 2M)

Ans:

Stream Cipher: Stream ciphers are a special class of ciphers in which the encryption and decryption algorithm is applied to the individual bits or bytes of the plain-text. The algorithm works by combining the plain-text bits or bytes with a pseudo-random bit stream, one bit or byte at a time.

Stream ciphers are especially well suited for encrypting and decrypting the type of data that is used in network communication systems-data in transit.

Stream Ciphers

- Essentially meant to be pseudo random generators, used for stateful encryption.
- Examples: linear feedback shift registers (not secure, but used as component in better stream ciphers), RC4, SEAL.
- Extremely simple and fast

Block Cipher: Block ciphers are another special class of ciphers that perform their magic on blocks of plain-text instead of individual bits. When necessary, the plain-text can be divided into blocks and the algorithm is applied to the individual blocks.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 7/46

Block ciphers define different "operating modes." These operating modes serve as a sort of blueprint for the algorithm to perform the actual encryption or decryption. Following are some popular operating modes for block ciphers:

- Electronic codebook mode (ECB) This mode is quite simple and is also prone to several weaknesses. It relies on the use of a fixed "code" book for encrypting data blocks. The fact that a given plain-text and key combination will always yield the same cipher-text is one of its weaknesses.
- Cipher-block chaining mode (CBC) This mode operates by using (or chaining) the cipher-text extracted from the preceding block to encrypt the next block of data. This is probably the most popular and widely used mode of operation for block ciphers.
- Counter mode (CM) This mode operates by using an initialization vector (IV) counter that increments for every block of plain-text to be converted to cipher-text. Block ciphers that operate in this mode are generally very fast in executing.
- Output feedback mode (OFB) This mode is best suited for encrypting smaller chunks of plain-text at a time, because it can emulate the behavior of stream ciphers.

Block ciphers

- For every key $k \in \{0, 1\}^n$, $E_k : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is a permutation, and both E_k and E_k^{-1} can be computed quickly given k . (n =key length, n = block length)
- Examples: DES, AES/Rijndael, IDEA.
- Main tools for private-key encryption in practice. Have both stateless modes and stateful/stream-like modes.

Q. 1) b) Attempt any ONE of the following:

6

**(i) With neat diagram describe steps for VLR failure restoration procedure.
(2M Diagram, 4M Explanation)**

Ans: VLR Failure Restoration:

After VLR failure, the service information of VLR record is recovered by first contact between the VLR and the HLR of the corresponding MS. The location information is recovered by the first contact between the VLR and the MS. The mobile station information is recovered either from HLR or MS.

VLR restoration procedure is initiated by one of the following three events.

- MS registration.
- MS call origination.
- MS call termination.

1. MS registration:

Since the record in the VLR get erased due to the failure, then the normal registration procedure define in inter-VLR movement is applied to recover the VLR record. In this



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 8/46

case, TMSI sends from the MS to the VLR that is not recognized, and MS asked to send IMSI over the air.

2. MS call origination:

When VLR receives the call origination request MAP_SEND_INFO_FOR_OUTGOING_CALL from the MSC, then the VLR record for the MS is not found. VLR considers this situation as a system error, with cause "unidentified subscriber". Request is then rejected and MS indicate the location registration procedure, then the VLR record is recovered.

3. MS call termination:

The call termination message flow is illustrated in Fig.

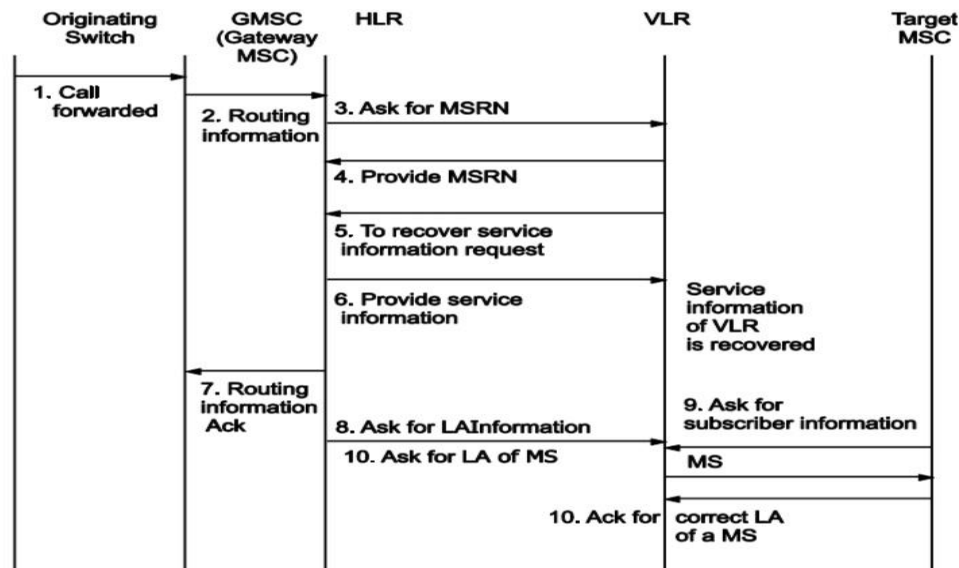


Fig. VLR failure restoration

Step 1: When the MS ISDN is dialed the call is forwarded to GMSC (Gateway Mobile Switching Centre), GMSC is a switch which ask the HLR for routing information. The HLR request to VLR of the MS to provide the routing address for the MSRN (Mobile Station Roaming Number).

Step 2: The VLR returns the MSRN to the GMSC through the HLR.

Step 3: The GMC uses the MSRN to route the call to the MS through the visited MSC (Mobile Switching Centre).

[Note that the IMSI - (International Mobile Subscriber Identity) and the MSC number are provided in the message which is send from HLR to VLR].



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 9/46

Then the VLR searches MS record, but the record is erased due to the failure because of this the search PS fails the VLR creates a new VLR record for the MS.

Neither the service nor the location information is available in this record. Steps 4 and 5 are executed parallelly.

Step 4 and 5:

VLR does not have routing information; it uses MSC number to create MSRN.

The number is sent back to gateway MSC to set up the call in Step 8.

Step 6 and 7:

The VLR recovers service information by sending MAP_RESTORE_DATA message To HLR. Then HLR sends service information to VLR by using MAP_INSERT_SUBSCRIBER_DATA message.

Step 8: After gateway MSC receive the MSRN in Step 7, the target MSC does not have LA information of the MS. In order to proceed to set up the call and asked for LAI information. Unfortunately VLR does not have LAI information. Hence, VLR ask MSC to determine the LA of MS by sending MAP_SEARCH_FOR_MOBILE_SUBSCRIBER message.

Step 9: The MSC initiate paging of MS in all LAS. If the paging is successful, the current LA address of MS is sent back to VLR. At this point LA information of VLR record is recovered.

(ii) Draw and Explain Life cycle of android activity.

(Diagram: 2M, Activities: 4 M (any 4))

Ans: Life Cycle of Android Activity:

As an activity transitions from state to state, it is notified of the change by calls to the following protected methods:

onCreate()	This is the first callback and called when the activity is first created.
onStart()	This callback is called when the activity becomes visible to the user.
onResume()	This is called when the user starts interacting with the application.
onPause()	The paused activity does not receive user input and cannot execute any code and called when the current activity is being paused and the previous activity is being resumed.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

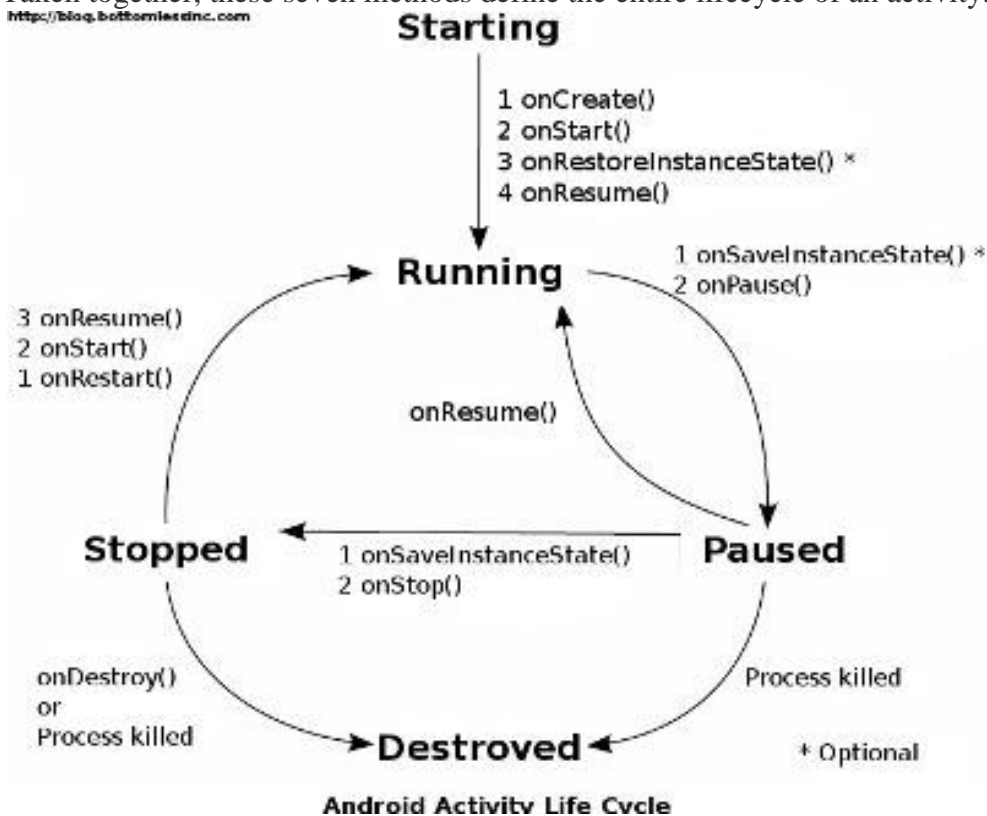
Model Answer

Page No: 10/46

onStop()	This callback is called when the activity is no longer visible.
onDestroy()	This callback is called before the activity is destroyed by the system.
onRestart()	This callback is called when the activity restarts after stopping it.

Taken together, these seven methods define the entire lifecycle of an activity.

<http://blog.bottomlineinc.com>



Q.2) Attempt any FOUR of the following:

16

**a) Write different channel assignment strategies in GSM. Explain in brief.
(Naming types of strategy 1M; explanation of each strategy 1 ½ M each)**

Ans: Types of Channel Assignment strategies:

- Fixed channel assignment
- Dynamic channel assignment



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 11/46

1. Fixed channel assignment

- Each cell is allocated a predetermined set of voice channel
- Any new call attempt can only be served by the unused channels in the cell.
- The call will be *blocked* if all channels in that cell are occupied
- Borrowing strategy is a type of fixed channel assignment strategy.
- In this the cell is allowed to borrow channels from neighboring cell if all of its own channels are already occupied.
- The MSC (Mobile switching center) supervises such borrowing procedures and ensures that borrowing of a channel does not disrupt or interfere with any of the calls in progress in the donor cell

2. Dynamic channel assignment

- Channels are not allocated to cells permanently.
- Mobile Switching center (MSC) allocates channels based on request.
- Reduce the likelihood of blocking, increase capacity.
- This requires the MSC to collect real time data on channel occupancy, traffic distribution & Radio Signal strength Indications (RSSI) of all channels on a continuous basis.

b) Define cell sectoring with its type.

(Definition: 2 M, Types 1 M, Diagram 1M)

Ans:

In cellular telephone system, co-channel interference can be decreased by replacing a single omnidirectional antenna with several directional antennas, each radiating within a smaller area. It is a method to increase capacity is to keep the cell radius unchanged and seek methods to decrease D/R ratio. Sectoring increases SIR, so that the cluster size may be reduced. First the SIR is improved using directional antennas, then capacity improvement is achieved by reducing the number of cell in the cluster; thus increasing the frequency reuse. To achieve this, it is necessary to reduce the relative interference without decreasing the transmit power.

In sectoring a cell has the same coverage space but instead of using a single Omnidirectional antenna that transmits in all directions, either 3 or 6 directional antennas are used these antennas provide coverage to a sector of the hexagon.

There are two types of sectoring in a cell

1. 3 directional antennas, 120° sectoring (each antenna covers 120°)
2. 6 directional antennas, 60° sectoring (each antenna covers 60°).



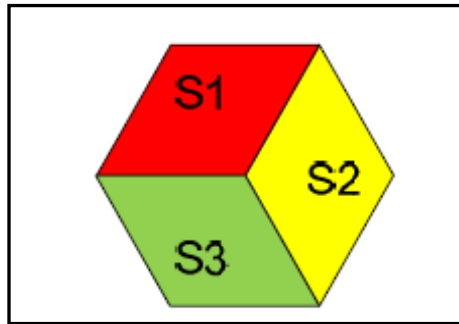
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

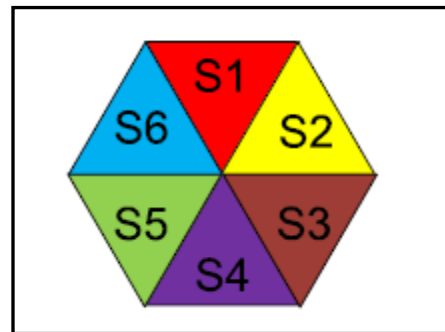
Subject Code: 17632

Model Answer

Page No: 12/46



120° Sectoring



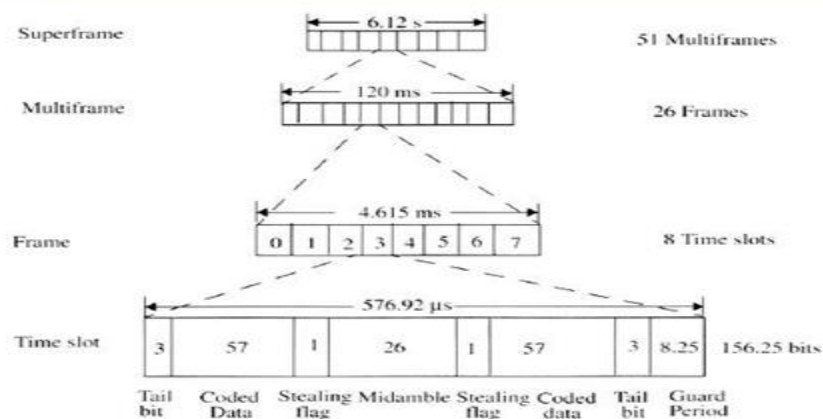
60° Sectoring

c) With neat diagram describe GSM frame structure.
(Explanation 2M, diagram 2M)

Ans: Frame structure in GSM:

- The length of GSM frame in a frequency channel is 4.615 ms.
- The frame is divided into 8 bursts of length of 0.577ms
- The timeslots in the uplink are derived from downlink by a time delay of time slots
- This arrangement prevents an MS from transmitting and receiving at the same time
- However, due to propagation delay (when MS is far away from BTS) the 3 TS delay cannot be maintained accurately

GSM Frame Structure



GSM frame structure.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 13/46

GSM Burst structure

- Each burst contains 148 bits (0.546ms) followed by 0.031ms guard time (8.25bits)
- The burst begins with 3 head bits and 3 tail bits (logical Zeroes)
- Two groups of data bits are separated by an equalizer Training sequence of 26 bits
- Each data group consists of 57 bit information bits and 1 flag that indicates whether the information bits are for user speech/ data or signaling.

d) Describe basic call originating procedure.

(Diagram: 1M, Steps: 3M)

Ans: Call Originating Procedure in GSM:

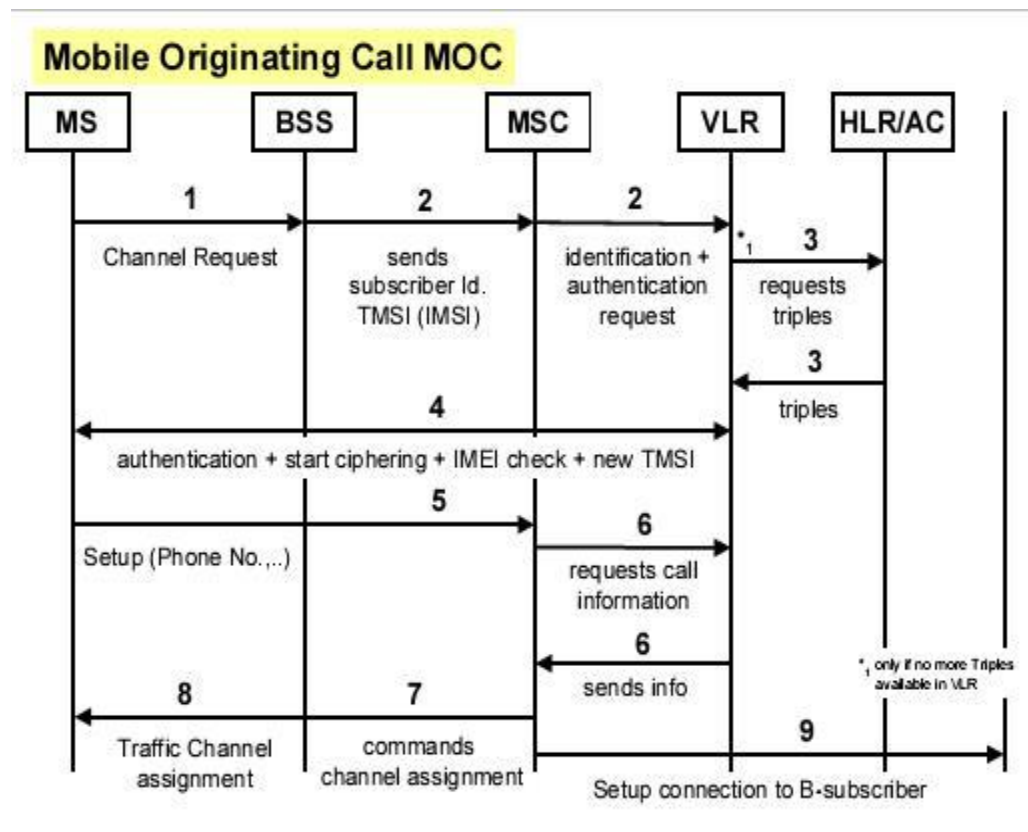


Fig: Call Originating in GSM



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 14/46

Mobile Originating Call (MOC): Call setup, which are initiated by an MS

1. Channel Request: The MS requests for the allocation of a dedicated signaling channel to perform the call setup.
2. After allocation of a signaling channel the request for MOC call setup, included the TMSI (IMSI) and the last LAI, is forwarded to the VLR
3. The VLR requests the AC via HLR for Triples (if necessary).
4. The VLR initiates Authentication, Cipher start, IMEI check (optional) and TMSI Re-allocation (optional).
5. If all this procedures have been successful, MS sends the Setup information (number of requested subscriber and detailed service description) to the MSC.
6. The MSC requests the VLR to check from the subscriber data whether the requested service an number can be handled (or if there are restrictions which do not allow further proceeding of the call setup)
7. If the VLR indicates that the call should be proceeded, the MSC commands the BSC to assign a Traffic Channel (i.e. resources for speech data transmission) to the MS
8. The BSC assigns a Traffic Channel TCH to the MS
9. The MSC sets up the connection to requested number (called party)

Request Access

- The MS sends a *Channel Request* (CHAN_REQ) message on the RACH.
- The BSS responds with a radio resource assignment (IMM_ASS_CMD) on the AGCH.
- The MS sends a *Service Request* (CM_SERV_REQ) message to the BSS on the SDCCH.

- e) List and explain in short types of bearers services in GPRS.**
(Any 4 Services: 1M Each)

Ans:

GPRS Services: GPRS is a wireless extension of data networks. It can access to data networks, such as IP-based networks (public internet, private intranet, IPv4 and IPv6 protocols) and X.25 based networks.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 15/46

GPRS upgrades GSM data services and provides the following services

1. Point-to-point (PTP) service: internetworking with the Internet (IP protocols) and X.25 networks.
2. Point-to-multipoint (PTM) service: point-to-multipoint multicast and point-to-multipoint group calls.
3. SMS service: bearer for SMS
4. Anonymous service: anonymous access to predefined services
5. Future enhancements: flexible to add new functions, such as more capacity, more users, new accesses, new protocols, new radio networks.

**f) With neat diagram describe the stepwise procedure to describe AES
(Diagram: 2 M, Steps: 2M)**

Ans:

Operation of AES:

AES is an iterative rather than Feistel cipher. It is based on 'substitution-permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Stepwise procedure in AES for encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so first it convert the 128 bits into 16 bytes.



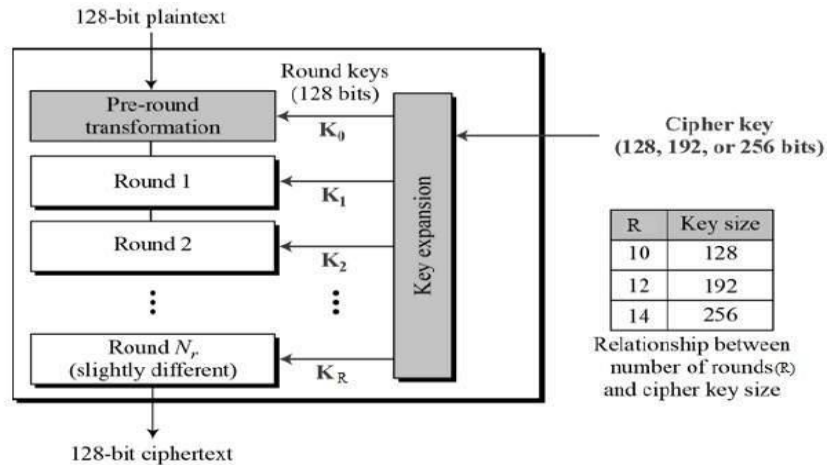
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 16/46

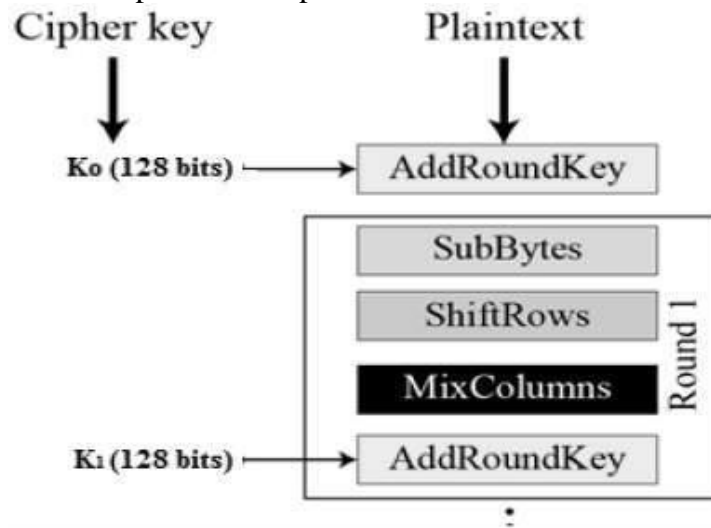


Diagrammatic Representation of AES is given below

Encryption Process

Each round in AES comprise of four sub-processes.

The first round process is depicted below



1. Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 17/46

2. Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3. MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4. Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Q.3) Attempt any FOUR of the following:

16

- a) Describe how repeaters are used in range extension.**
(2 M for Description 2 M for Diagram)

Ans:

The use of repeater in cellular mobile communication system is for extending the range of the reception of the receiver. Especially, the repeater is used when it is hard for the transmitted signal to reach up to the receiver set. Repeaters are bidirectional in nature and simultaneously send signals to and receive signals from a serving BS. Upon receiving signals from BSs in forward link, the repeater amplifies and reradiates the BS signals to the specific coverage region. Repeaters are being widely used to provide



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

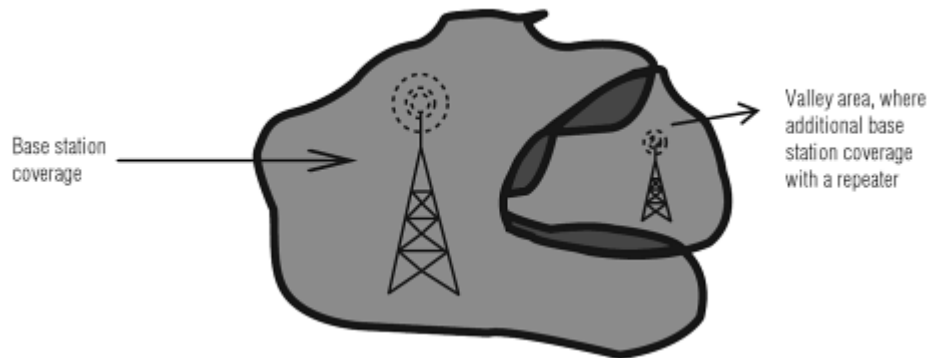
WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 18/46

coverage into and around buildings, where coverage has been traditionally weak. However, repeaters do not add any capacity to the system, they just increase the reach of a BS or MS into “shadowed” areas.



b) Describe GSM Traffic Channels with its type.
(Relevant description 4M)

Ans:

TRAFFIC CHANNELS In GSM system two types of traffic channels used: Full Rate Traffic Channels (TCHF): This channel carries information at rate of 22.8 Kbps. Half Rate Traffic Channels (TCHH): This channel carries information at rate of 11.4 Kbps.

Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the slow associated control channel (SACCH) and 1 is currently unused.

TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thereby simplifying the electronic circuitry. This method permits complex antenna duplex filters to be



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

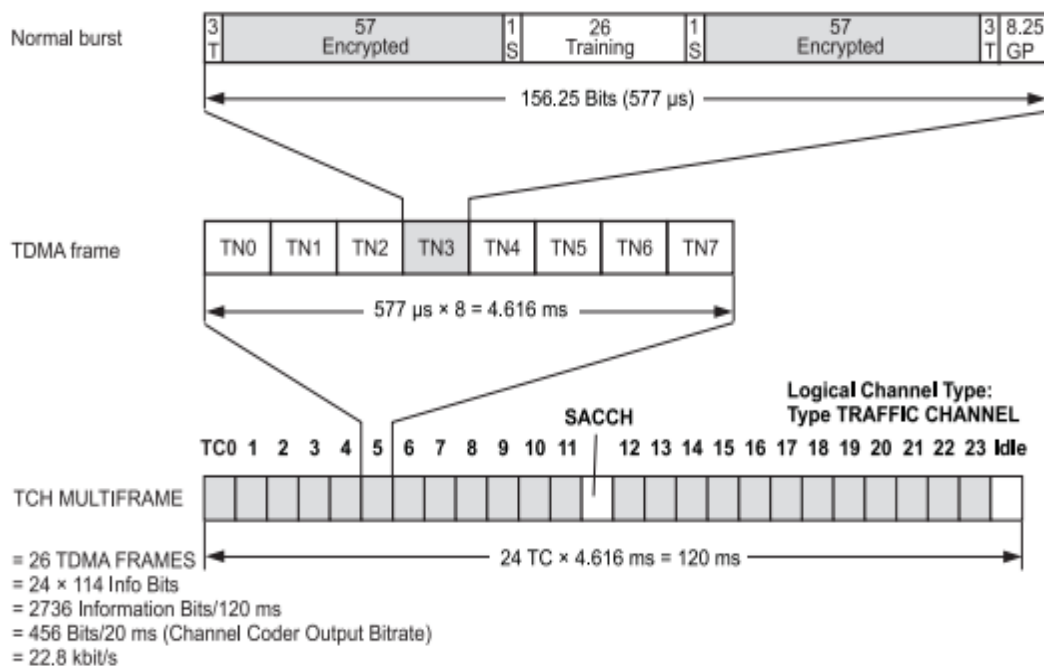
Subject Code: 17632

Model Answer

Page No: 19/46

avoided and thus helps to cut power consumption. In addition to these full-rate TCHs (TCH/F, 22.8 kbit/s), half-rate TCHs (TCH/H, 11.4 kbit/s) are also defined. Half-rate TCHs double the capacity of a system effectively by making it possible to transmit two calls in a single channel.

If a TCH/F is used for data communications, the usable data rate drops to 9.6 kbit/s (in TCH/H: max. 4.8 kbit/s) due to the enhanced security algorithms. Eighth-rate TCHs are also specified, and are used for signaling. In the GSM Recommendations, they are called stand-alone dedicated control channels (SDCCH).



c) Write major steps performed in inter-LA movement.
(Correct steps:4M)

Ans:

The MS moves from LA1 to LA2, where both Las are connected to same MSC. In GSM specification there are 9 messages exchanged between MS and MSC and 10 messages exchanged between MSC and VLR

Step1. A location update request message is sent from MS to MSC through BTS. This message includes the address of previous visited LA, MSC, and VLR. In this case, the



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

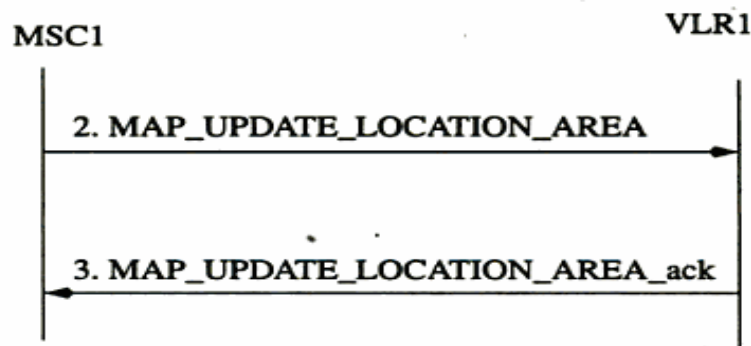
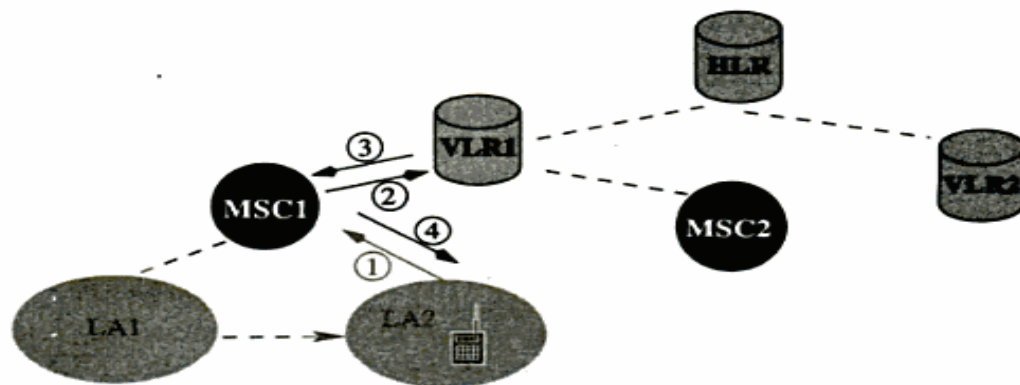
Page No: 20/46

addresses of previous MSC and VLR are same as those for new MSC and VLR. Furthermore, the MS identifies itself by the temporary mobile subscriber identity (TMSI).

Step2. The MSC forwards the location update request to the VLR by a TCAP message, MAP_UPDATE_LOCATION_AREA. This message includes:

- Address of the MSC
- TMSI of the MS
- Previous Location area Identification (LAI); for example, the ID for LA1
- Target LA1; for example, the ID for LA2
- Other related information related to GSM

Step 3 and Step 4 The VLR notices that both LA1 and LA2 belong to the same MSC. It updates the LA1 field of the VLR record and replies with an acknowledgement to the MS through the MSC.





MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 21/46

d) List strategies used in implementation of 4G technology.
(Any 4 Strategies: 1 mark each)

Ans:

Considerations in the Evolution to 4G:

The deployment of LTE is another step in the evolution of mobile broadband networks. While the deployment of 4G radio access networks receives considerable attention, the multimedia core network has emerged as a critical element in the delivery of next-generation mobile broadband services.

Communication services provider migration strategies in the evolution to 4G can be classified into three main categories:

1. Data-only services on 4G
2. Data-only services on 4G with 2G/3G voice
3. Voice and data services on 4G

To mitigate the risks of their 4G deployments, communication services providers may incorporate one or more of these strategies at different times. Therefore, the three migration strategies are not diametric to one another, but rather build upon their predecessor.

Evolution considerations for an integrated approach include:

- Does your existing 3G network support a software upgrade to 4G functions?
- Have you analyzed the optimization you can achieve by integrating functions when migrating from 3G to 4G and growing 4G networks?
- Does the platform chosen for 3G scale to support the capacity required for 4G?

Another potential near-term deployment model is a complete EPC overlay with separate functional elements handling LTE connections. This approach may mitigate some risk and allow slow migration to EPC.

Considerations for these deployments include:

- How will handover support be provided between 2G/3G and 4G?
- Will end customers be happy if their common applications - FTP, email, HTTP, and YouTube - do not have seamless service mobility?
- Are the existing platforms ready for the performance challenges of separate elements?

Multimedia Services

One of the biggest disruptions in the mobile industry is the movement to an open, IP-based architecture designed to deliver converged voice, data, and multimedia services. The emerging mobile packet technologies, High Speed Packet Access (HSPA) and LTE, provide an all-IP infrastructure from the mobile device, whether it is a handset, smartphone, data card, or other emerging intelligent device. With all-IP networks, the door is open to providing the traditional circuit-based services, including voice and video over the packet infrastructure.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 22/46

**e) Mention the features of Windows CE.
(Any four features 1M each)**

Ans:

- Features of Windows CE OS:
- Similar to windows 95.
- It is a Microsoft's mobile os used in smart phones and mobile devices
- It is a 32 bit multitasking, multithreading os that has scalable, open architecture design, providing support for variety of devices.
- Windows CE is compact, providing high performance in limited memory configurations
- Standard communication support is built into this OS enabling access of internet.
- Integrated power management enabling long battery life
- GUI facilitating ease of use for end users
- Subset of win 32 API : windows CE supports more than 700 of the most frequently used win 32 APIs , enabling developers to take advantage of vast amounts of third party programming resources, tools , documentation for their windows CE based development
- Low cost, familiar development tools
- Scalable , full featured OS
- Extensive and extensible device support- supports keyboard, mouse devices, touch panels, serial ports , Ethernet modems, USB devices, audio devices, parallel port, printer devices, storage devices
- Wide microprocessor support

Q.4) a) Attempt any THREE of the following:

12

**i) Define Frequency Reuse and Handoff.
(2 M each for Definition)**

Ans: Frequency Reuse: Frequency reuse is a technique of reusing frequencies and channels within a communication system to improve capacity and spectral efficiency. Frequency reuse is one of the fundamental concepts on which commercial wireless systems are based that involve the partitioning of an RF radiating area into cells.

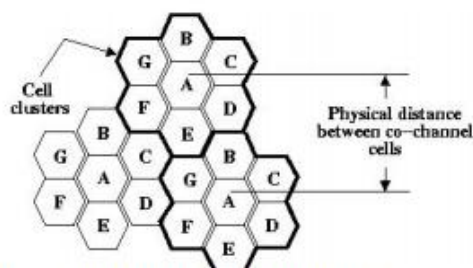


Figure: Frequency reuses technique of a cellular system.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

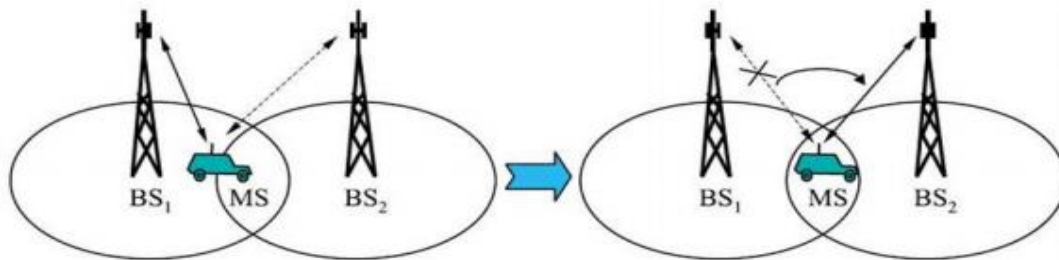
WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 23/46

Handoff: A handoff refers to the process of transferring an active call or data session from one cell in a cellular network to another or from one channel in a cell to another. A well-implemented handoff is important for delivering uninterrupted service to a caller or data session user. Fig: Handoff Handoffs may be classified into two types: Hard Handoff and Soft Handoff

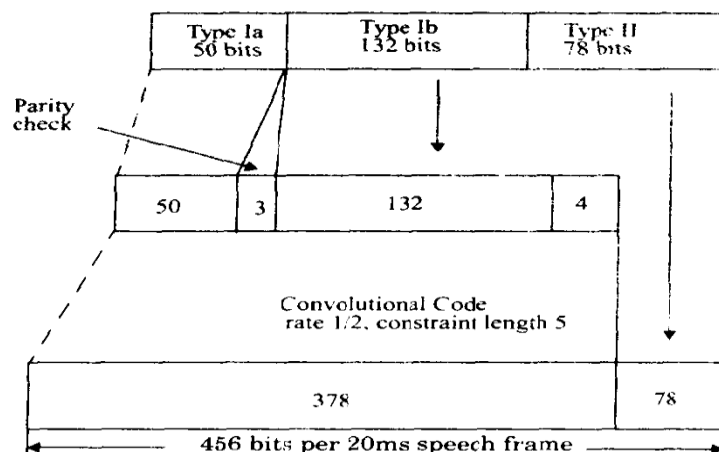


ii) Explain TCH Channel Coding in GSM signal Processing
(Relevant explanation 4M)

Ans:

The output bits of the speech coder are ordered into groups for error protection, based upon their significance in contributing to speech quality. Out of the total 260 bits in a frame, the most important 50 bits, called type Ia, have 3 parity check (CRC) bits added to them.

This facilitates the detection of non-correctable errors at the receiver. The next 132 bits along with the first 53 (50 type Ia bits + 3 parity bits) are recorded and appended by 4 trailing zero bits, thus providing a data block of 189 bits. This block is then encoded for error protection using a rate $\frac{1}{2}$ convolutional encoder with constraint $K=5$, thus providing a sequence of 378 bits. The least important 78 bits do not have any error protection and are concatenated to the existing sequence to form a block of 456 bits in a 20ms frame. The error protection coding scheme increases the gross data rate of the GSM speech signal, with channel coding, to 22.8 kbps.





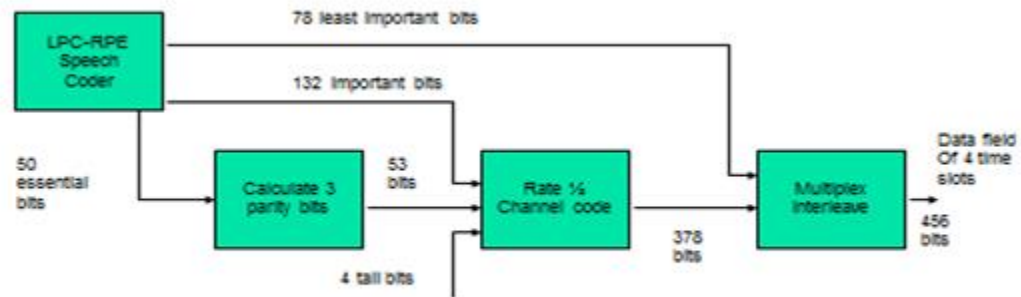
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 24/46



****consider the TCH coder transmitter and receiver block diagram as well instead of above frame diagram. Description is same as explanation given above.**

iii) Describe various types of attacks in Information Security
(Active attacks 2M, passive attacks 2M)

Ans:

ATTACK: An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, clickjacking, botnet, phishing, spamming, inside and outside. It is classified in two types

Active Attack: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data in route to the target.

Types of active attacks:

1. Masquerade Attack: In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

2. Session Replay Attack: In a session replay attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 25/46

3. Message Modification Attack: In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

4. DoS Attack: In a denial of service (DoS) attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

Passive Attack: A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target. Passive attacks include active reconnaissance and passive reconnaissance. In passive reconnaissance, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture. In active reconnaissance, the intruder engages with the target system through methods like port scans.

Types of passive attacks:

1. War driving: War driving detects vulnerable Wi-Fi networks by scanning them from nearby locations with a portable antenna. The attack is typically carried out from a moving vehicle, sometimes with GPS systems that hackers use to plot out areas with vulnerabilities on a map. War driving can be done just to steal an Internet connection or as a preliminary activity for a future attack.

2. Dumpster diving: In dumpster diving, intruders look for information stored on discarded computers and other devices or even passwords in trash bins. The intruders can then use this information to facilitate covert entry to a network or system.

3. Intruder attack: An intruder might masquerade as an authorized network user and spy without interaction. With that access, an intruder might monitor network traffic by setting the network adapter to promiscuous mode.

iv) Compare between symmetric key cryptography with public key cryptography
(Any 4 Points 1M each)

Ans:

Symmetric Key Cryptography	Public Key Cryptography
It is also known as private key cryptography	It is also known as asymmetric encryption
Only one key is used: Private key	Two Keys are used: Public and Private
The key is kept secret	Public key is freely available to all, while private key is a secret key



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 26/46

Same key is used for encryption and decryption	One key is used for encryption while other is decryption
Faster than Public key cryptography	Slower than symmetric key cryptography
It is used for encrypting small or large message	It is used for encrypting small messages

Q.4) b) Attempt any ONE of the following:

6

i) With neat Labelled diagram explain GSM architecture (3M description and 3M diagram)

Ans:

GSM system consists of three major components: (i) Base Station System (BSS). (ii) Operation and Maintenance Center (OMC). (iii) Network and Switching Subsystem (NSS).

(i) **Base Station System (BSS):** This system consists of Mobile Station (MS), Base Station Controller (BSC), Base Trans receiver Station (BTS). As shown in Fig. the BSS and NSS connected to each other via A interface (solid lines) and the connection to OMC via O interface (dashed lines).

Base Station Subsystem (BSS): GSM system consists of many BSS, each one is controlled by Base Station Controller (BSC). BSS performs all the functions which are required to maintain connection to MS, coding/decoding of voice etc. BSS also contains Base Trans receiver Stations (BTS).

Base Station Controller (BSC): BSC provides all the control functions and physical link between MSC and BTS. BSC is connected to BTS and MSC (Mobile Switching Center).

Base Trans receiver Station (BTS): BTS is responsible for handling radio interface to the mobile station. It is connected to MS via Um interface and it is also connected to BSC via the Abis interface.

The Um interface contains all mechanism for wireless interface (TDMA, FDMA etc.). The BTS is a radio equipment (trans receiver or antenna) needed to service each cell in the network.

(ii) **Operation and Maintenance Center (OMC):** OMC is connected to all equipments in switching system and to the BSC. It maintains operation of the GSM network by observing the handovers, system load, blocking rates etc. OMC



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 27/46

provides network overview and allow network engineers to monitor, diagnose and troubleshoot every aspect of GSM network.

- (iii) **Network and Switching Subsystem (NSS):** NSS is responsible for performing call processing and subscriber related functions. It also includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AUC), Equipment Identity Register (EIR) etc.

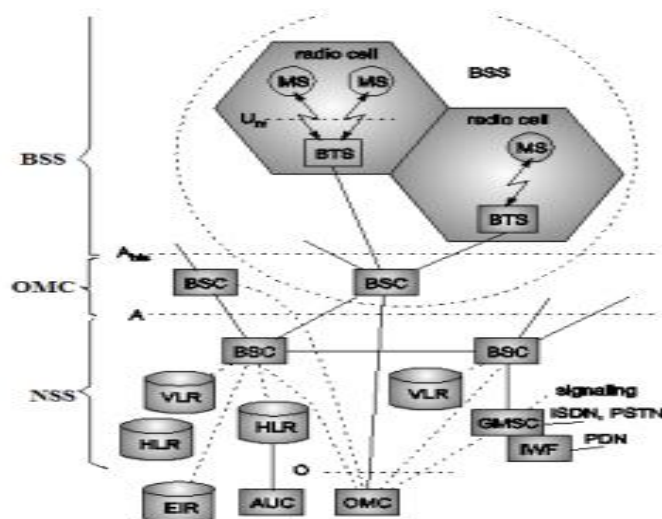
Mobile Switching Center (MSC): It is used to handle communication between different MS connected to different BSCs. The function of MSC is to locate different MS and associated BTS, call switching and authentication etc.

Home Location Register (HLR): It is a database for managing the mobile subscriber. HLR stores permanent data of subscriber which include subscribers service profile, location information and its activity. A home subscriber charges are less then the roaming subscriber. **Visitor Location Register (VLR):** It is a database which consists of temporary information about subscribers which is used by MSC in order to provide services to visiting subscriber. MSC updates the VLR by determining which users are in roaming. Once, the roaming mobile information is updated, and then MSC sends necessary information to roaming mobile subscribers so that roaming mobile call can be properly routed.

Authentication Center (AUC): This authentication center is used to provide authentication and encryption method that is used to verify the user identity and ensure the confidentiality and secrecy of each call.

Equipment Identity Register (EIR): It contains a list of all valid MS equipment within the network, where each MS is known by it's IMEI. This IMEI is divided into three groups.

1. White IMEI: All known IMEI.
2. Black IMEI: All stolen mobile handset.
3. Gray IMEI: Handset that is uncertain.





MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 28/46

- ii) Write steps to develop a User interface with two text box and two buttons.
(Relevant steps 6M)**

Ans:

Creating a User Interface

The graphical user interface for an Android app is built using a hierarchy of View and ViewGroup Objects. View objects are usually UI widgets such as buttons or textfields. ViewGroup objects are invisible view containers that define how the child views are laid out, such as in a grid or a vertical list.

Android provides an XML vocabulary that corresponds to the subclasses of View and ViewGroup so you can define your UI in XML using a hierarchy of UI elements.

Create a Linear Layout

1. In Android Studio, from the **res/layout** directory, open the **activity_my.xml** file.
The BlankActivity template you chose when you created this project includes the activity_my.xml file with a RelativeLayout root view and a TextView child view.
2. In the **Preview** pane, click the Hide icon to close the Preview pane.
In Android Studio, when you open a layout file, you're first shown the Preview pane. Clicking elements in this pane opens the WYSIWYG tools in the Design pane. For this lesson, you're going to work directly with the XML.
3. Delete the **<TextView>** element.
4. Change the **<RelativeLayout>** element to **<LinearLayout>**.
5. Add the android:orientation attribute and set it to "horizontal".
6. Remove the android:padding attributes and the tools:context attribute.

Creating a Text Field

A text field allows the user to type text into your app. It can be either single line or multi-line. Touching a text field places the cursor and automatically displays the keyboard. In addition to typing, text fields allow for a variety of other activities, such as text selection (cut, copy, paste) and data look-up via auto-completion.

Text fields can have different input types, such as number, date, password, or email address. The type determines what kinds of characters are allowed inside the field, and may prompt the virtual keyboard to optimize its layout for frequently used characters.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 29/46

You can add a text field to you layout with the EditText object. You should usually do so in your XML layout with a <EditText> element.

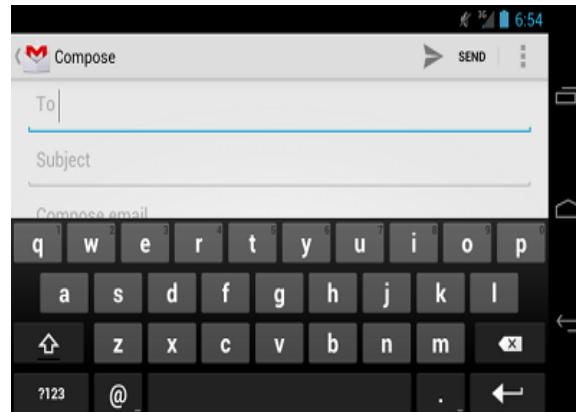


Fig: Text field with keyboard

As with every View object, you must define certain XML attributes to specify the EditText object's properties.

1. In the activity_my.xml file, within the <LinearLayout> element, define an <EditText> element with theid attribute set to @+id/edit_message.
2. Define the layout_width and layout_height attributes as wrap_content.
3. Define a hint attribute as a string object named edit_message.

Add a Button

A button consists of text or an icon (or both text and an icon) that communicates what action occurs when the user touches it. Depending on whether you want a button with text, an icon, or both, you can create the button in your layout in three ways:

1. With text, using the Button class:

<Button

android:layout_width="wrap_content"

android:layout_height="wrap_content"



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

Subject Code: 17632

WINTER – 2015 EXAMINATION
Model Answer

Page No: 30/46

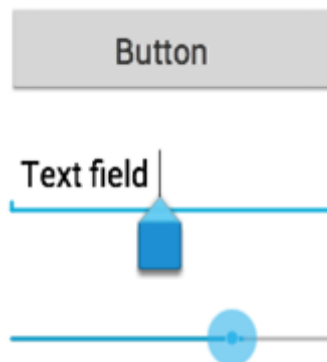
```
android:text="@string/button_text"  
... />
```

2. With an icon, using the ImageButton class:

```
<ImageButton  
    android:layout_width="wrap_content"  
    android:layout_height="wrap_content"  
    android:src="@drawable/button_icon"  
... />
```

3. With text and an icon, using Button class with the android:drawableLeft attribute:

```
<Button  
    android:layout_width="wrap_content"  
    android:layout_height="wrap_content"  
    android:text="@string/button_text"  
    android:drawableLeft="@drawable/button_icon"  
... />
```



1. In Android Studio, from the `res/layout` directory, edit the `activity_my.xml` file.
2. Within the `<LinearLayout>` element, define a `<Button>` element immediately following the `<EditText>` element.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

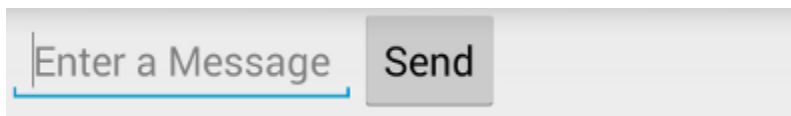
Model Answer

Page No: 31/46

3. Set the button's width and height attributes to "wrap_content" so the button is only as big as necessary to fit the button's text label.
4. Define the button's text label with the android:text attribute; set its value to the button_send string resource you defined in the previous section.

Note: This button doesn't need the android:id attribute, because it won't be referenced from the activity code.

The layout is currently designed so that both the EditText and Button widgets are only as big as necessary to fit their content, as shown in figure.



To configure how the Button control looks, adjust the control's properties by selecting the control (either in the Outline tab or the Preview window) and changing its properties in the Properties Tab.

Specific properties you will want to be aware of:

- Give the Button or ImageButton control a unique name using the id property.
- Set the text displayed on the Button control using the text property; set the image displayed on the ImageButton control using the src property.
- Set the layout height and layout width properties of the control to wrap_content.
- Set any other properties you desire to adjust the control's appearance.
For example, adjust the font of a Button using the Text color, text size, and text style properties.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 32/46

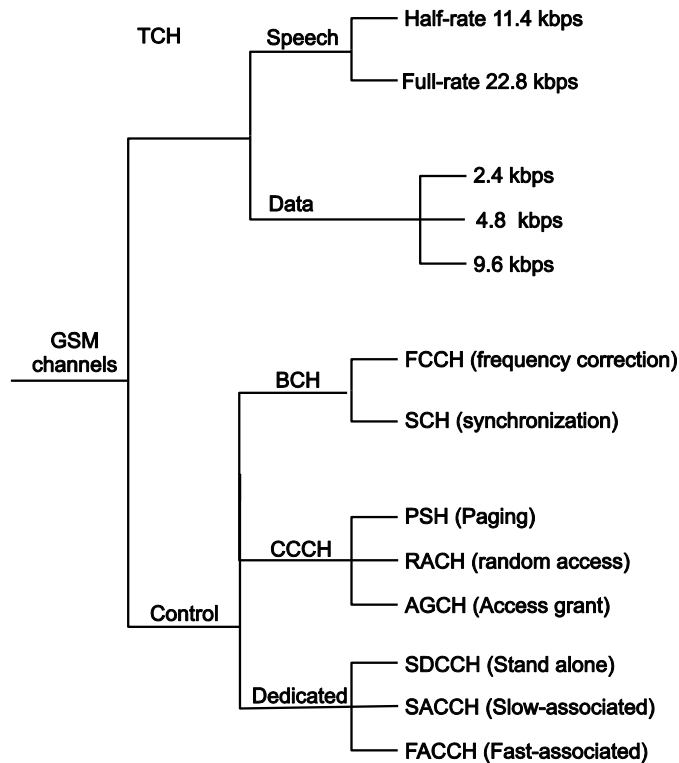
Q.5 Attempt Any TWO of the following:

16

a) State Various GSM control channel in brief.

(Each Channel Explanation-1Marks, total 8 Channel)

Ans:



GSM Control Channels (CCH):

There are three control channels in GSM:

1. Broadcast control channels.
2. Common control channels.
3. Dedicated control channels.

1. Broadcast control channels (BCH) :

The BTS uses this channel to give information to all MSs within a cell. Information uses by this channel is cell and network identity, current control channel structure, channel



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 33/46

availability and congestion. The broadcast control channel also sends the list of channels that are currently used within cell.

- (a) **Frequency Correction Channel (FCCH):** The BTS sends information for frequency correction via the Frequency Correction Channel (FCCH). The FCCH is special data burst, which occupies first frame (i.e. frame 0) and repeated after every ten frames in control channel multiframe.
- (b) **Synchronization Channel (SCH):** BTS broadcast information about time synchronization to all MSS via synchronization channel (SCH). If the mobile station is 30 km away from serving base station, it is often necessary to adjust the timing of particular mobile user. The SCH is transmitted once after every ten frames within the control channel multiframe.

2. Common Control Channels (CCCH):

All the information regarding setting up a connection between MS and BS is exchanged via the CCCH. The common control channel occupies TSO (frame) of GSM frame and that is not used by BCH and ideal channels.

- (a) **Paging Channel (PCH):** The PCH gives paging signal from the base station to all mobile stations within cell. It also notify particular mobile for an incoming call from PSTN. Alternatively, the PCH is used to provide cell broadcast ASCII text message to all subscriber, as a GSM SMS features.
- (b) **Random Access Channel (RACH):** If MS wants to setup a call, it uses Random Access Channel (RACH) to send data to BTS. All mobile must request access or respond to a PCH with TSO of GSM frame. At BTS, every frame will accept RACH transmission from mobile during TSO.
- (c) **Access Grant Channel (AGCH):** The AGCH channel is used by base station to provide forward link communication to mobile station and carries instructional data which tells mobile to operate in particular physical channel with particular control channel. The AGCH is the final common control channel message sent by the base station before subscriber is roaming or moving off the control channel.

3. Dedicated Control Channels (DCCH):

There are mainly three types of dedicated control channels in GSM, same as traffic channel, they are bidirectional. They have same format and function on both forward and reverse links.

- (a) **Stand-alone Dedicated Control Channels (SDCCH):** SDCCH carries signaling data which follows the connection of mobile with base station. The SDCCH ensures that the mobile and base station connection remains constant while the base



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 34/46

station and MSC verify the subscriber unit and resource allocation to mobile. The SDCCH is also used to send authentication and alert messages but not speech.

- (b) **Slow Associated Control Channel (SACCH):** The SACCH is always associated with traffic channel or SDCCH, the SACCH carries general information between the MS and BTS. On the forward link, the SACCH is used to send slow but regularly changing control information to the mobile, such as power level instruction, and specific timing advance instruction for each user. The reverse SACCH carries information about the received signal strength and quality of traffic channel as well as BCH measurement result from neighboring cell.
- (c) **Fast Associated Control Channels (FACCH):** FACCH carries urgent messages, and contain the same type of information as SDCCH. A FACCH is assigned to a particular user when SDCCH has not been dedicated to particular user. The FACCH access the time slots by taking frame from traffic channel, this is done by using two special bits, called stealing bits, in TCH channel.

b) Describe GPRS architecture with neat Diagram.

(4 marks-Diagram, 4-marks Explanation)

Ans. GPRS Architecture

- GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.
- GPRS usually attempts to reuse the existing GSM network elements as much as possible. There are new entities called GPRS that supports nodes (GSN) which are responsible for delivery and routing of data packets between mobile stations and external packets networks. There are two types of GSNs,
 - Serving GPRS Support Node (SGSN)
 - Gateway GPRS Support Node (GGSN)
- There is also a new database called GPRS register which is located with HLR. It stores routing information's and maps the IMSI to a PDN address. Thus, GPRS Reference Architecture is shown as:



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 35/46

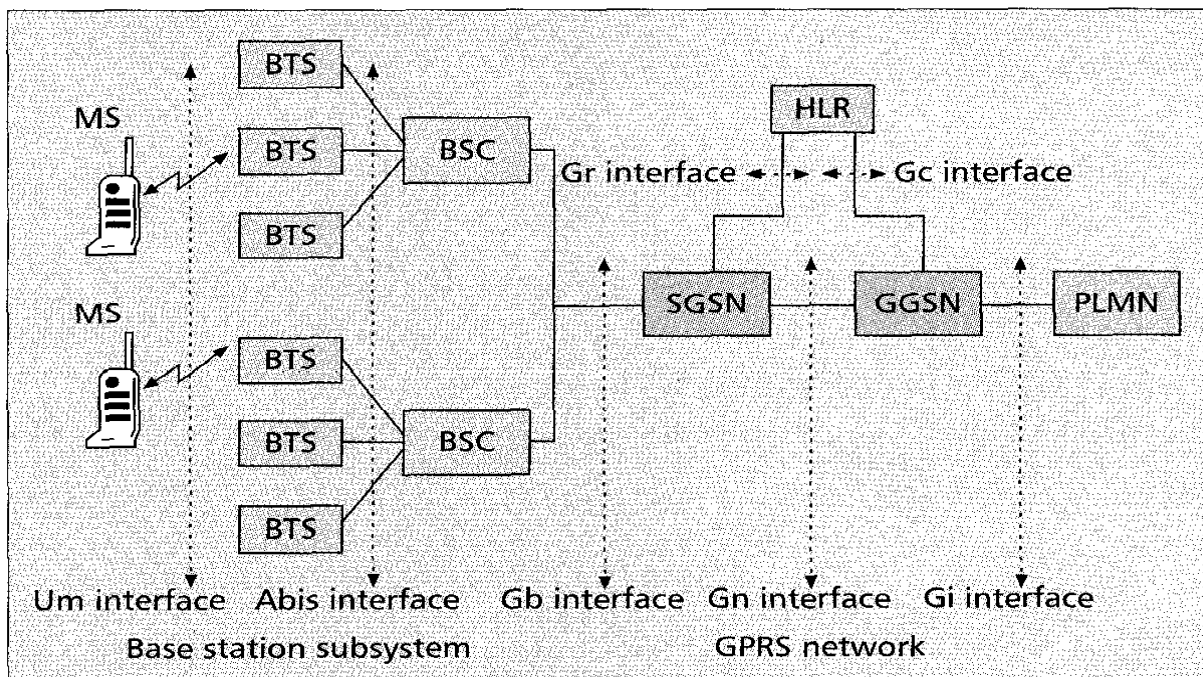
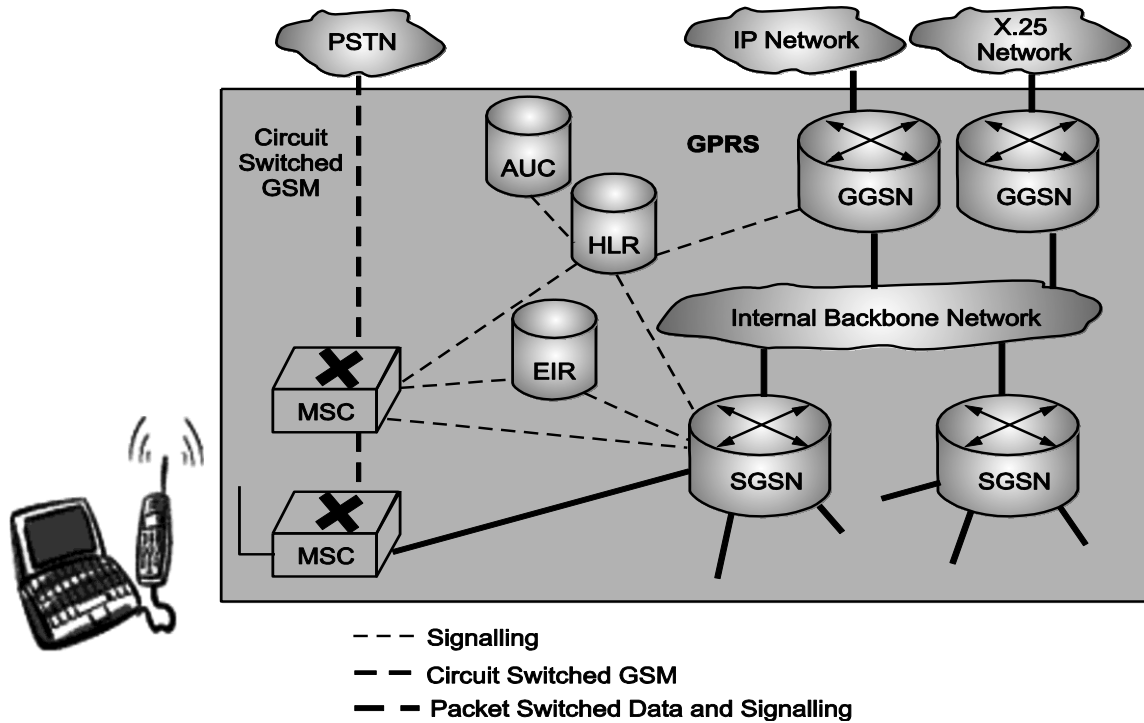


Fig: GPRS Architecture



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 36/46

- The MS and the BSS communicate via the Um interface. The BSS and the SGSN are connected by the Gb interface using frame relay. Within the same GPRS network, SGNS/GGSN are connected through the Gn interface. When SGSN and GGSN are in different GPRS networks, they are interconnected via the Gp interface. The GGSN connects to external networks through the Gi interface. The MSC/VLR communicates with the BSS using the existing GSM A interface, and with the SGSN using the Gs interface. The HLR connects to the SGSN via the Gr interface, and to the GGSN via the GC interface. Both Gr and GC follow the GSM Mobile Application Part (MAP) protocol. The HLR and the VLR are connected through the existing GSM D interface. Interfaces A, Gs, Gr, GC, and D are used for signaling, without involving user data transmission in GPRS. Note that the A interface is used for both signaling and voice transmission in GSM. Interfaces Um, Gb, Gn, Gp and Gi are used for both signaling and transmission in GPRS.

GSM Network Element	Modification or Upgrade Required for GPRS
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station (BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 37/46

c) Write Detail Procedure of DES algorithm.

(2 marks-Diagram, 6 Marks-Explanation)

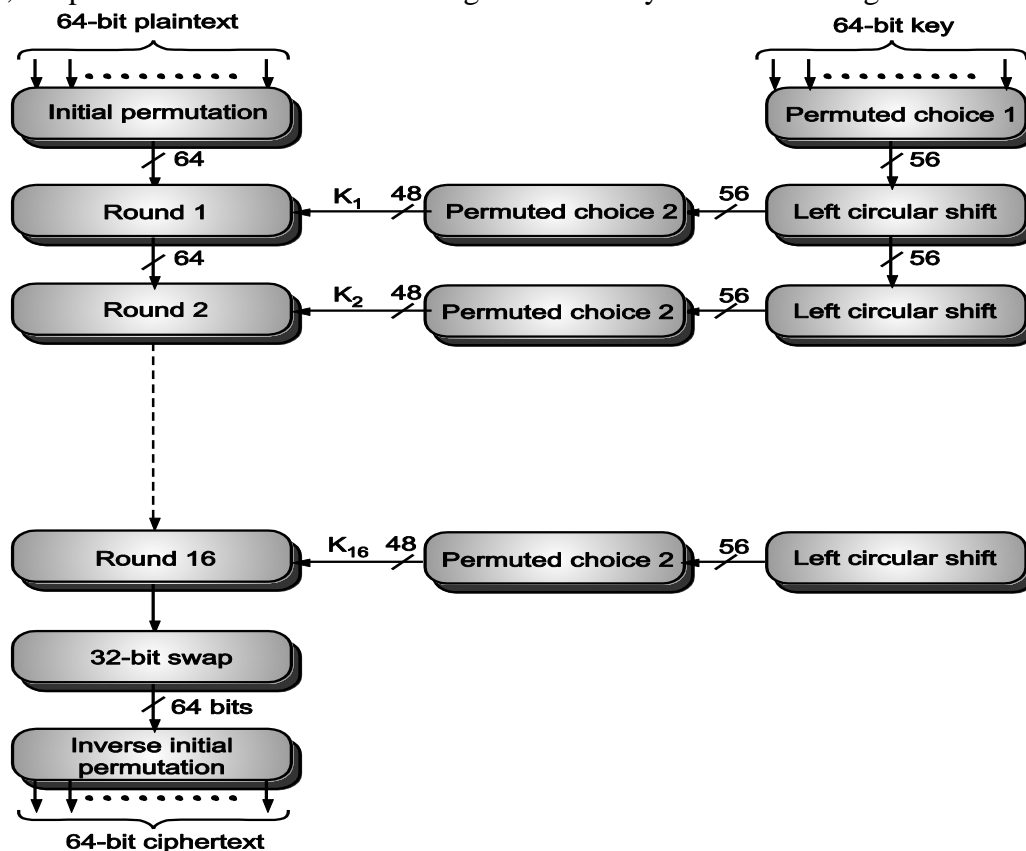
Ans. Data Encryption Standard (DES):

In 1977 NIST (National Institute of Standards and Technology) had adopted Feistel structure cryptography as Data Encryption Standard (DES).

For DES,

- It is Block cipher type.
- Data are encrypted in 64-bit blocks using a 56-bit key.
- The algorithm transforms 64-bit input in a series of steps into a 64-bit output.
- The same steps, with the same key, are used to reverse the encryption.
- It uses a Feistel structure.

The overall scheme for DES encryption is illustrated in following Fig. 5.7. There are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.



Overall scheme of DES



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 38/46

Looking at the left-hand side of the figure:

Processing of the plaintext proceeds in three phases.

1. The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the *permuted input*.
2. This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the **preoutput**.
3. Finally, the preoutput is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

The right-hand portion of Figure shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the sixteen rounds, a *subkey* (K_i) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

Q.6) Attempt Any FOUR of the following:

16

a) Describe microcell zone concept.

(2marks- Diagram, 2 Marks Explanation)

Ans.

- When sectoring is employed, lot of handoffs is required due to this load on switching and control link element of the mobile system increases.
- To solve this problem, a microcell concept for seven cell reuse is used.
- In this scheme, each of three (possibly more) zone sites are connected to single base station. The zone are connected by a co-axial, fiber optic cable or microwave link to a base stations.



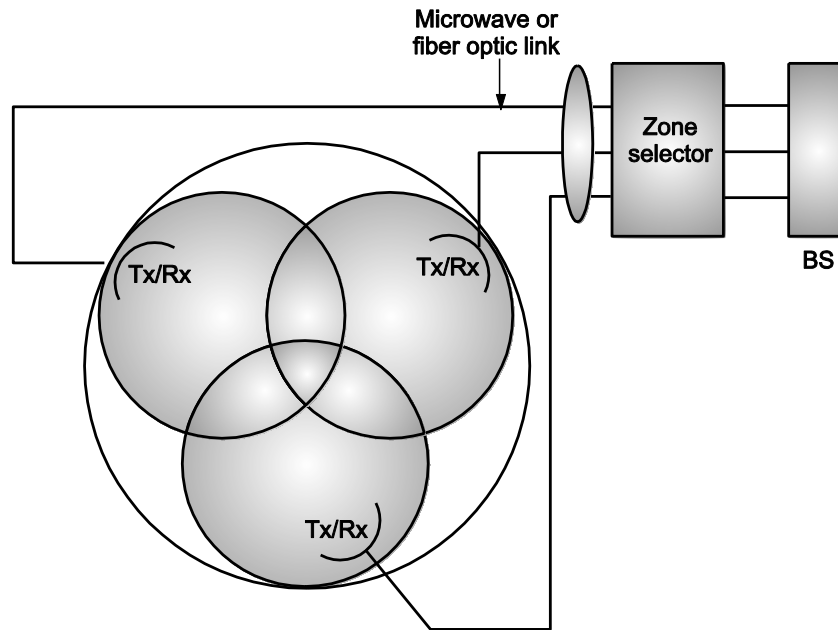
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 39/46



The Microcell concept, BS - Base station

- Multiple zones and single station make a cell. As mobile travels within a cell, it served by zone with strong signal, this approach is advantageous because of sectoring placed antenna at outer edges of cell, and base station channel is assigned to any zone by the base station.
- As mobile moves from one zone to another zone in same cell, it uses same channel, thus like a sectoring, handoff is not required at mobile switching centre (MSC) when mobile travels within the cell in different zone.
- The base station simply changes the channel from one zone to another zone, and channel is active in particular zone in which mobile is travelling, hence interference is reduced.
- The advantage of zone cell technique is that, cell maintains particular area of coverage, the co-channel interference in cellular system is reduced, as larger control base station is replaced by zone transmitter on edge of cell.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 40/46

**b) Write algorithm for call termination of VLR overflow.
(2 Marks-Diagram, 2 marks Explanation)**

Ans: Call termination

Step 1: Location query

Step 1.1: The calling party dials the phone number of u_1 , the request is sent to call originating switch to PSTN.

Step 1.2: The originating switch sends the location query message to HLR.

Step 1.3: The HLR determines that u_1 is an overflow user and send a query message to obtain its routing information. The user profile information is attached in this message.

Step 2: Location Response

Step 2.1: If V is not full, a record for u_1 is created. If V is full, a user record is deleted and is used to store u_1 's record. V creates routable address of u_1 and send back to HLR, if the VLR record is not available, then refer the detail of routable address. If the record is replaced (u_3 as shown in Fig.), the replacement information is included in the message.

Step 2.2: The HLR returns the routable address to the originating switch. If the record is replaced, the overflow flag are updated in HLR (for u_1 and u_3 as shown in Fig.).

Step 2.3: The originating switch set up the trunk to the MSC based on routable address.

Step 2.4: The MSC pages the mobile phone and the path for the call is established.



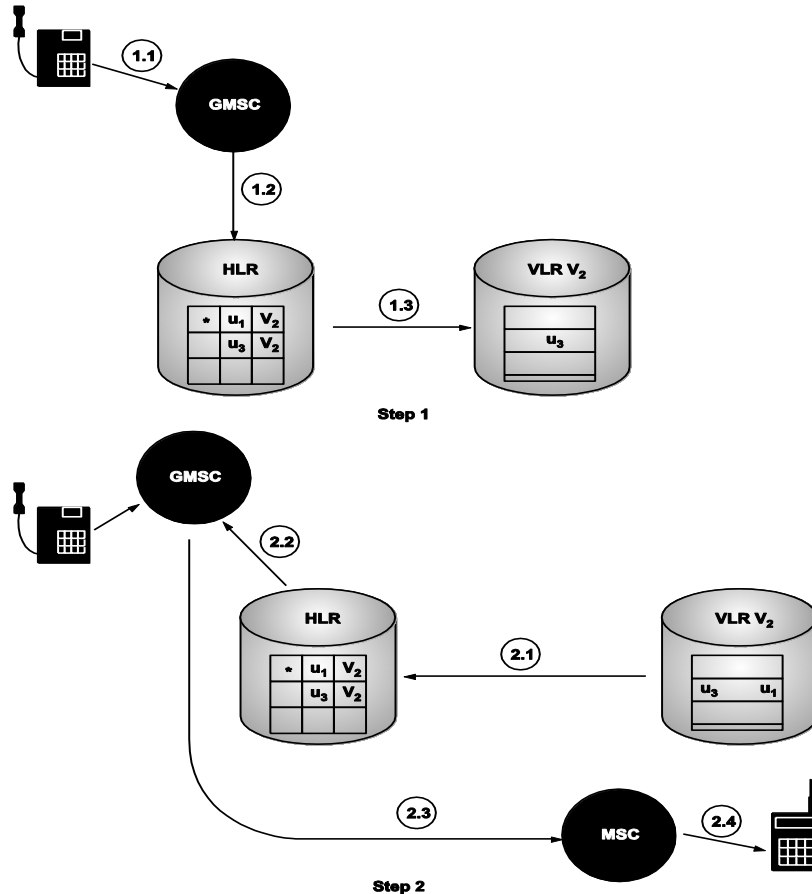
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 41/46



Call termination with overflow VLR

c) Describe HLR restoration procedure.

(Relevant procedure 4M)

Ans: HLR Failure Restoration:

In GSM HLR, it is compulsory to save the update into non-volatile storage. Changes of service information are backup immediately after every update and the location information is periodically transferred from HLR into backup. The service information is update infrequently because not all the subscriber changes their service profile after subscription.

After HLR failure, the data in the backup are reloaded into the HLR. We also have "uncovered period" as a time interval after last backup operation and before the restart of the HLR data that changed in the uncover period cannot be recovered. The following HLR restoration procedure is executed.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

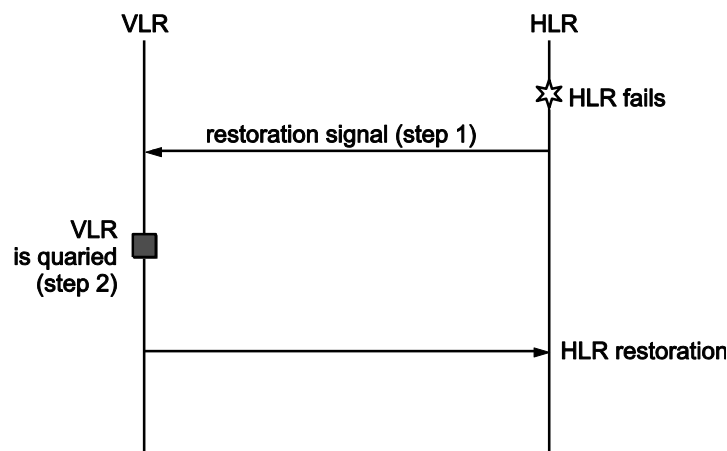
WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 42/46

- Step 1:** The HLR sends an signalling system 7 (SS7) TCAP (Transaction Capability Application Part) message. MAP_RESET to the all VLRs where its MSs are located (that is restoration signal).
- Step 2:** Each VLR that receives the restoration signal from HLR is queried to search the lost location information of user.
- Step 3:** All the VLRs derived all MSs of the HLR, and for each MS, they send an SS7 TCAP message, MAP_UPDATE LOCATION, to the HLR.



HLR restoration

d) With neat diagram explain any two data bus in GSM frame.

(1 marks for any burst diagram, any three burst explanation: 1 mark for each)

Ans:

Each user transmits data during the time slots which is assigned to them. These data have one of five specific formats, as defined in GSM. Fig. 2.3 illustrates the five types of data bursts used for various traffic and control channels. Normal bursts are used for traffic channels (TCH) and dedicated control channel (DCCH), on both forward and reverse link. The RACH channel burst is used by all mobiles to access services from any base station. FCCH and SCH burst are used for broadcasting of frequency and time synchronization control messages.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 43/46

Normal

3 start bits	58 bits of encrypted data	26 training bits	58 bits of encrypted data	3 stop bits	8.25 bits guard period
--------------	---------------------------	------------------	---------------------------	-------------	------------------------

FCCH burst

3 start bits	142 fixed bits of all zeroes	3 stop bits	8.25 bits guard period
--------------	------------------------------	-------------	------------------------

SCH burst

3 start bits	39 bits of encrypted data	64 bits of training	39 bits of encrypted data	3 stop bits	8.25 data bits guard period
--------------	---------------------------	---------------------	---------------------------	-------------	-----------------------------

RACH burst

8 start bits	41 bits of synchronization	36 bits of encrypted data	3 stop bits	68.25 bits extended guard period
--------------	----------------------------	---------------------------	-------------	----------------------------------

Dummy burst

3 start bits	58 mixed bits	26 training bits	58 mixed bits	3 stop bits	8.25 bits of guard period
--------------	---------------	------------------	---------------	-------------	---------------------------

Fig. : Time slot data bursts in GSM

Fig. illustrates the data structure within normal burst. It consists of 148 bits which is transmitted at a rate of 270.833333 kbps. Out of total 148 bits per TS, 114 contains information bits which are transmitted as two 57 bits sequences close to the beginning and end of the burst.

The midamble consists of 26 bits training sequence which allow mobile or base station receiver to analyse the characteristics of radio channel. On both the sides of midamble bits there are control bits called stealing flags. These two flags are used to distinguish between traffic channel or control (FACCH) data.

During a frame, a GSM subscriber uses one TS to transmit, one TS to receive and use the six spare time slots to measure on five adjacent base station as well as its own base station.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 44/46

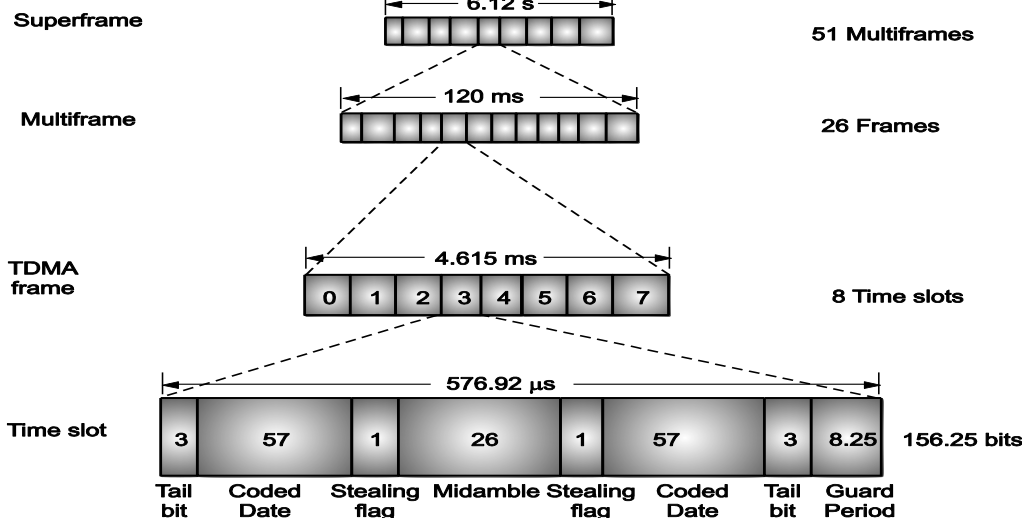


Fig.: GSM frame structure

As shown in Figure, there are eight time slots per TDMA frame, and frame period is 4.615 ms. As frame contains $8 \times 156.25 = 1250$ bits.

These each normal speech frames are grouped into larger structure called multiframes which in turn are grouped into superframe.

One multiframe contain 26 TDMA frame and one superframe contain 51 multiframes or 1326 TDMA frames a hyperframe which is not shown in Fig. 2.4 which contains 2048 superframes or 2,715,648 TDMA frames. A hyperframe is sent about every 3 hours, 28 minutes and 54 seconds, it is important to GSM, sufficient security can be obtained by using large number of frames provided by the hyperframe.

FCCH Burst

- The most simple format of all the bursts is used for the frequency correction burst, which is transmitted only in the frequency correction channel (FCCH).
- The frequency correction burst is also used by MSs as a frequency reference for their internal time bases.
- All 148 bits (142 bits + 6 tail bits) are coded with 0 and frequency a pure sinewave is transmitted which is the frequency with which MS has to tune with.

SCH Burst

- The synchronization burst is used to transmit synchronization channel information (SCH).



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 45/46

- As its name suggests, this burst carries details of the GSM frame structure and allows an MS to fully synchronize with the BTS.
- The synchronization burst is the first burst that the MS has to demodulate and, for this reason, the training sequence is extended to 64 bits. It also allows larger multipath delay spreads to be resolved.

RACH Burst

- Used to send RACH Burst.
- In contrast to the bursts described so far, the access burst comes in a rather unique format because of its special tasks.
- A mobile station uses the access burst only for the initial access to a BTS.
- MS does not know the current distance to the BTS. It generally is uncertain if the access burst arrives within specified time frame and there exists chances of overlapping with other bursts.
- To ensure that an access burst arrives at the BTS during the proper time period the number of bits for the access burst was set to only 88 bits along with increased guard band bits of 68.25.
- The purpose of this extra free space is to measure the distance between MS and BTS at the beginning of a connection.

Dummy Burst

- Used to fill up unused timeslots, which transmits the BCCH channel.
- No real information.

e) Write note on UMTS in 3G and 4G technology.

(Any four points 1 Mark each)

Ans:

- UMTS (Universal Mobile Telecommunications Service) is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps).
- Universal Mobile Telecommunications System (UMTS) is a air interface standard and has evolved since late 1996 under the European Telecommunications Standards Institute (ETSI). European carriers, manufacturers, and government regulators collectively developed, the early versions of UMTS as a competitive open air-interface standard for 3G wireless telecommunications.
- UMTS offers a consistent set of services to mobile computer and phone users, which is not depend on the location. UMTS is based on the Global System for Mobile (GSM)



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2015 EXAMINATION

Subject Code: 17632

Model Answer

Page No: 46/46

communication standard. Once UMTS is available, computer and phone users can be continuously connected to the Internet wherever they travel, will have the same set of capabilities. Users will get access to internet via combination of terrestrial wireless and satellite transmissions.

- Earlier cellular telephone systems were using circuit-switched connection, where the connections were always dependent on circuit availability. A packet-switched connection uses the Internet Protocol (IP), meaning that a virtual connection is always available.
- The 3G W-CDMA air interface standard had been designed for “always-on” packet based wireless service, so that computers, entertainment devices, and communication device all share the same wireless network and be connected to the Internet, anytime, anywhere. W-CDMA is used to transfer packet up to 2.048 Mbps per user (if the user is stationary), thereby allowing high quality data, multimedia, streaming audio, streaming video, and broadcast-type services to consumers. Future versions of W-CDMA will support stationary user data rates in excess of 8 Mbps. W-CDMA provides public and private network features, as well as video conferencing and virtual home entertainment (VHE). W-CDMA designers contemplate that broadcasting, mobile commerce (m-commerce), games, interactive video, and virtual private networking will be possible throughout the world, all from a small portable wireless device.
- UMTS also makes it possible to provide new services like alternative billing methods or calling plans. For instance, users can choose to pay-per-bit, pay-per-session, flat rate, or asymmetric bandwidth options.
- The higher bandwidth of UMTS also enables other new services like video conferencing. UMTS may allow the Virtual Home Environment (VHE) to fully develop, where a roaming user can have the same services to either at home, in the office or in the field through a combination of transparent terrestrial and satellite connections.

LTE(Long-Term Evolution):

- LTE, an abbreviation for Long-Term Evolution, commonly marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals.
- It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using a different radio interface together with core network improvements. The standard is developed by the 3GPP (3rd Generation Partnership Project).
- LTE is the natural upgrade path for carriers with both GSM/UMTS networks and CDMA2000 networks. The different LTE frequencies and bands used in different countries will mean that only multi-band phones will be able to use LTE in all countries where it is supported.