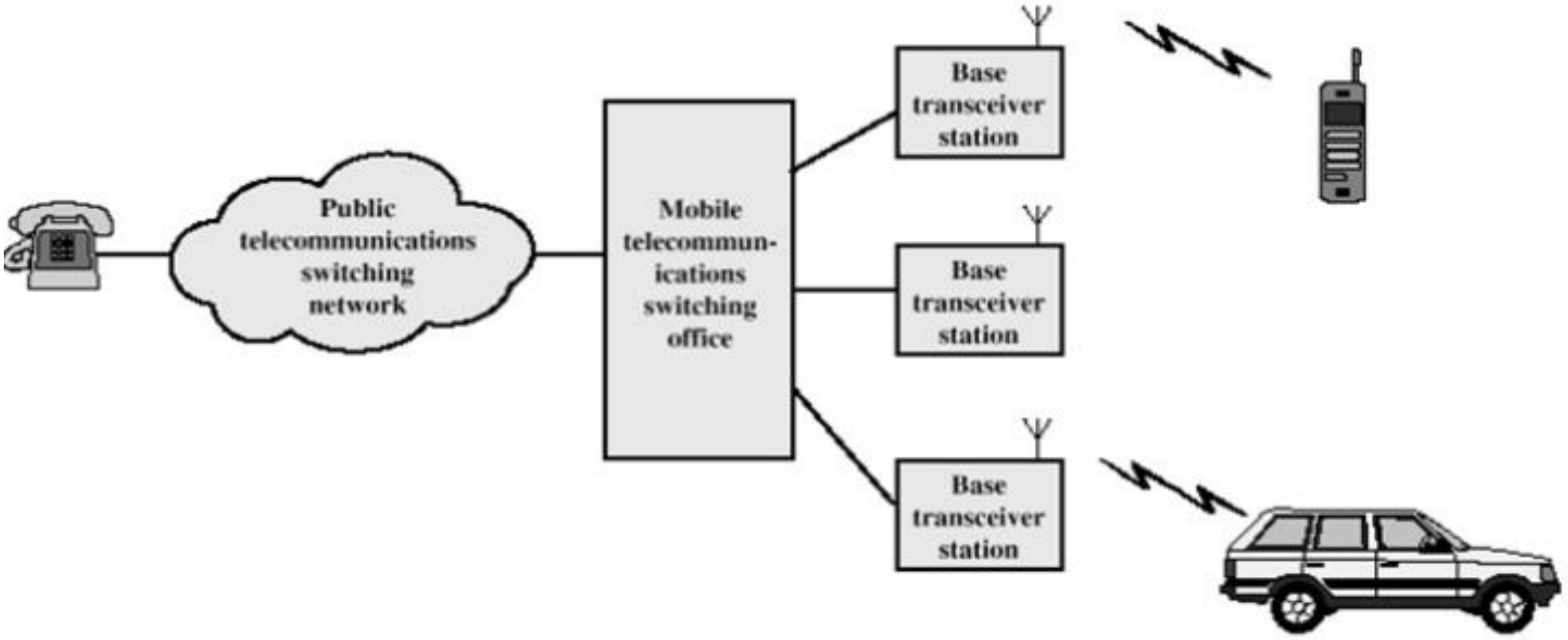
Module 2
Wide Area Wireless Networks

Principle of Cellular Communication – Frequency Reuse concept, cluster size and system capacity, co-channel interference and signal quality; GSM – System Architecture, GSM Radio Subsystem, Frame Structure; GPRS and EDGE – System Architecture; UMTS – Network Architecture; CDMA 2000 – Network Architecture; LTE – Network Architecture; Overview of LoRa & LoRaWAN.

Self-learning Topics:- IS-95

Principle of Cellular Communication

- Cellular system overview



Principle of Cellular Communication

- Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc.
- The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems.
- Cellular networks use lower power, shorter range and more transmitters for data transmission.

Features of Cellular Systems

- Offer very high capacity in a limited spectrum.
- Reuse of radio channel in different cells.
- Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region.
- Communication is always between mobile and base station (not directly between mobiles).
- Each cellular base station is allocated a group of radio channels within a small geographic area called a cell.
- Neighboring cells are assigned different channel groups.
- By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells.
- Keep interference levels within tolerable limits.
- Frequency reuse or frequency planning.
- Organization of Wireless Cellular Network.

Shape of Cells

- The coverage area of cellular networks are divided into **cells**, each cell having its own antenna for transmitting the signals. Each cell has its own frequencies. Data communication in cellular networks is served by its base station transmitter, receiver and its control unit.
- The shape of cells can be either square or hexagon –

Square

- A square cell has four neighbors at distance **d** and four at distance Root **2 d**
- Better if all adjacent antennas equidistant
- Simplifies choosing and switching to new antenna

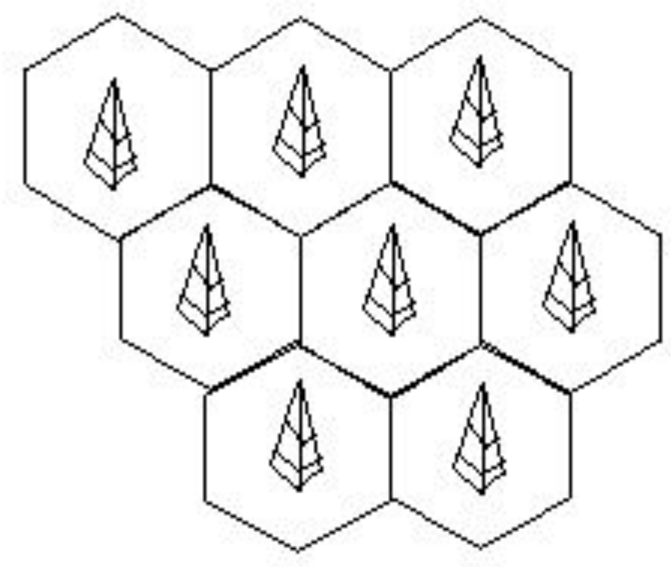
Hexagon

- A hexagon cell shape is highly recommended for its easy

coverage and calculations.

It offers the following advantages –

- Provides equidistant antennas
- Distance from center to vertex equals length of side

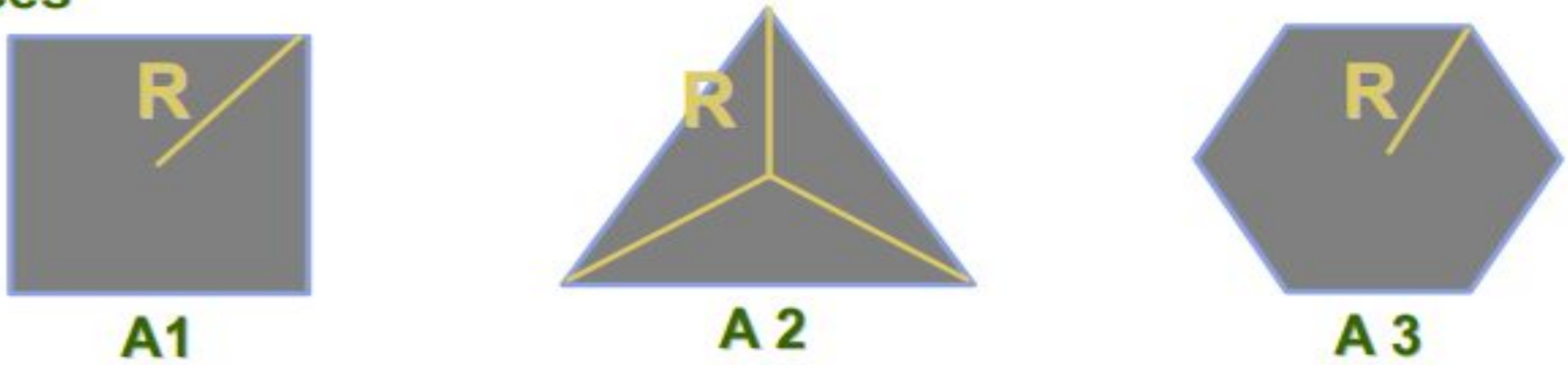


Choices of Hexagonal Cell Geometry

Factors

- Equal area
- No overlap between cells

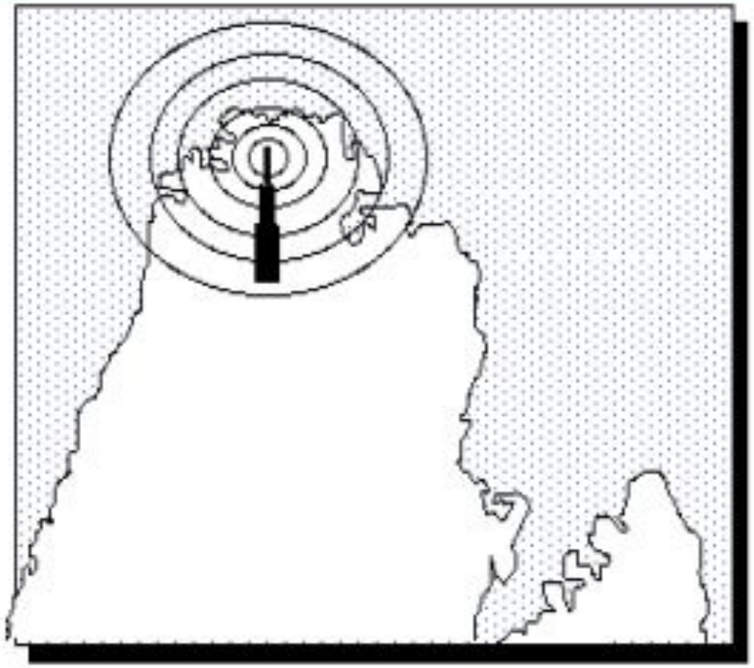
Choices

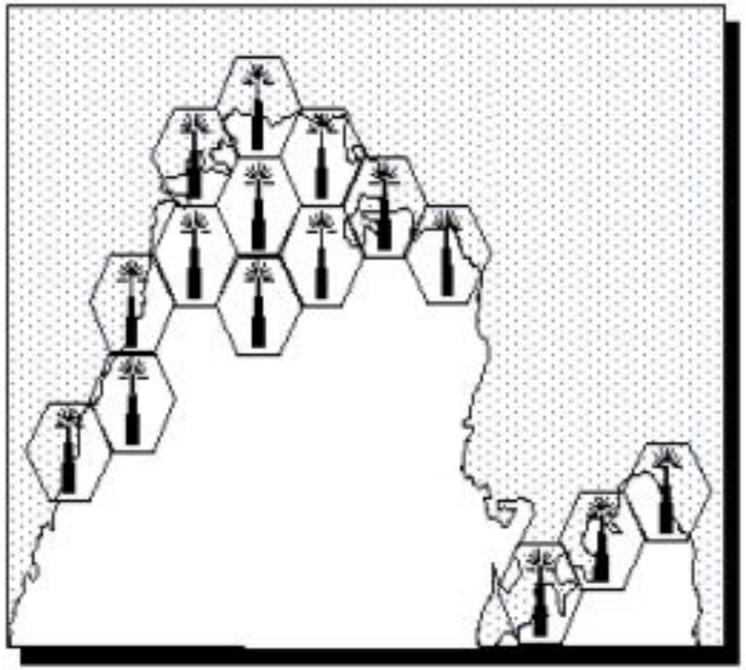


For a given R, A3 provides **maximum coverage area**.

By using hexagon geometry, the fewest number of cells covers a given geographic region.

Frequency Reusing





Early Mobile Telephone System

Traditional mobile service was similar to radio/TV broadcasting: One very powerful transmitter located at the highest spot in a large area.

Cellular System

In a cellular system, instead of using one powerful transmitter, many low-power transmitters were placed throughout a coverage area.

Frequency Reusing

Early Mobile Telephone System

Low Capacity: Consider that the assigned frequency band can afford 100 simultaneous conversations (channels).

Cellular System

High Capacity: Consider that the assigned frequency band is reused in 10 cells, the system may afford 1000 simultaneous conversations (channels).

- The cellular concept was a major breakthrough in solving the problem of spectral congestion and user capacity.

- It offered very high capacity in a limited spectrum allocation without any major technological changes.

Frequency Reuse

- **Technique for using a specified range of frequencies more than once in the same radio system so that the total capacity of the system is increased without increasing its allocated bandwidth**.

Frequency reuse offers the following benefits −

- Allows communications within cell on a given frequency
- Limits escaping power to adjacent cells
- Allows re-use of frequencies in nearby cells
- Uses same frequency for multiple conversations
- 10 to 50 frequencies per cell

For example, when **N** cells are using the same number of frequencies and **K** be the total number of frequencies used in systems. Then each **cell frequency** is calculated by using the formulae **K/N**.

In Advanced Mobile Phone Services (AMPS) when K = 395 and N = 7, then frequencies per cell on an average will be 395/7 = 56. Here, **cell frequency** is 56.

Consider a cellular system

Total duplex channels : S

Cluster size : N cells

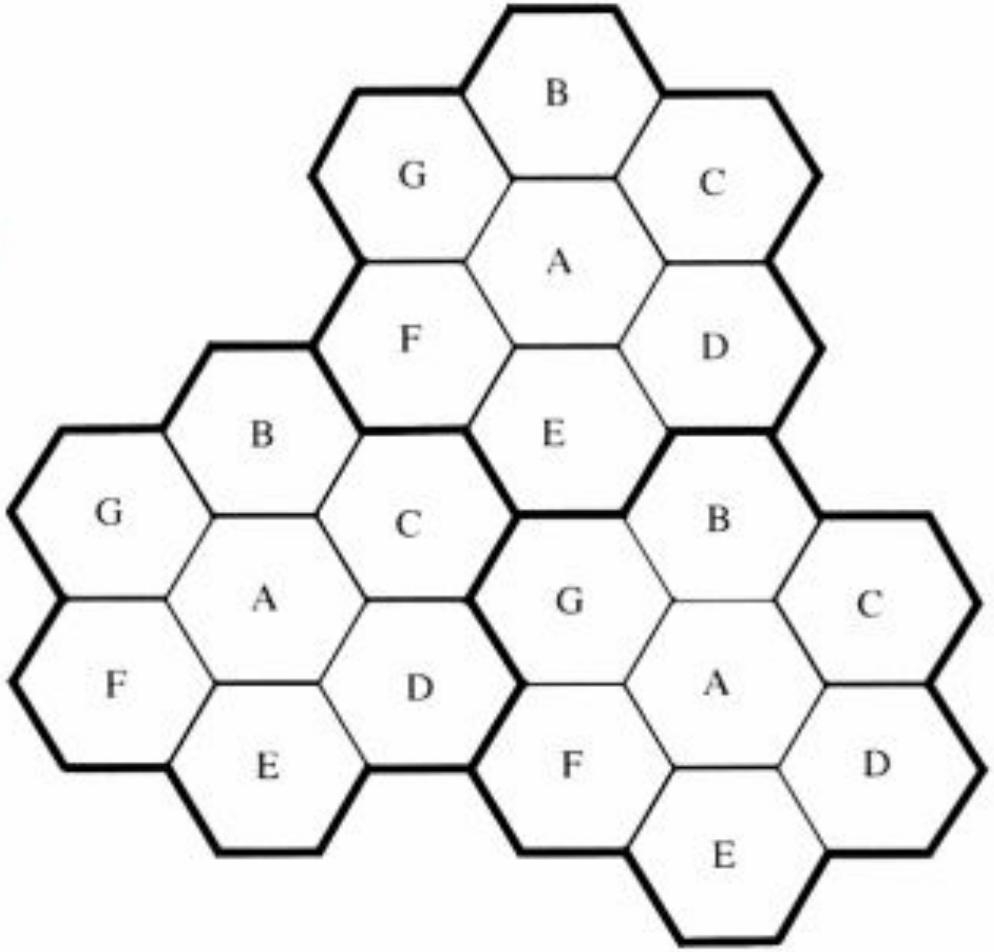
No. of channels in each cell : $k = S/N$

Capacity in a cluster : $C = kN = S$

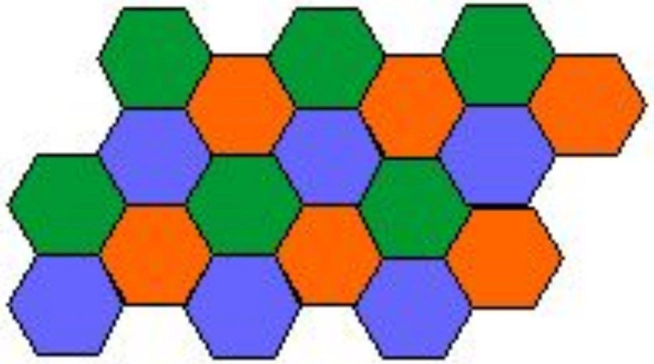
If a cluster is replicated M times

Total capacity : $C = MkN = MS$

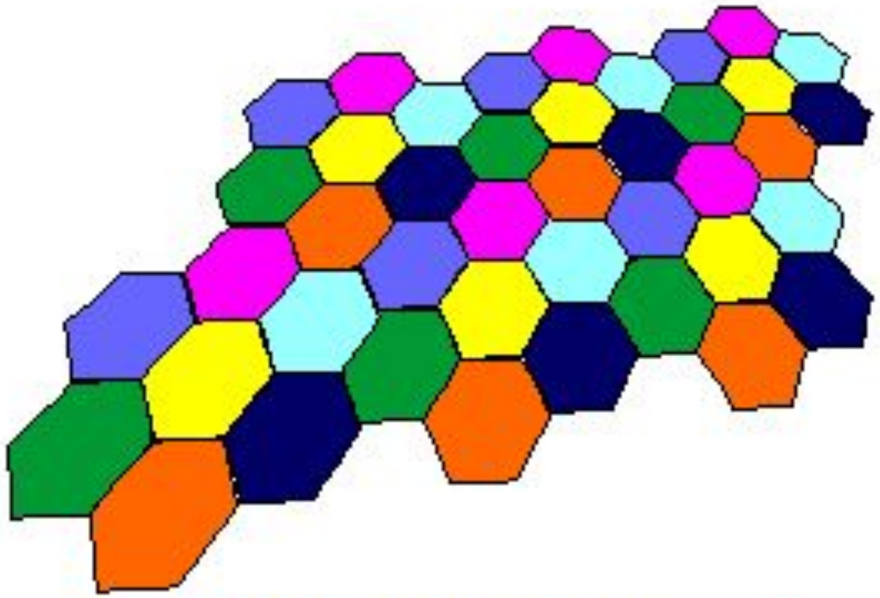
→ The capacity is increased by M.



- To ensure that the mutual interference between users remains below a harmful level, adjacent cells use different frequencies.
- In fact, a set of *C* different frequencies $\{f_1, ..., f_C\}$ are used for each cluster of *C* adjacent cells. Cluster patterns and the corresponding frequencies are re-used in a regular pattern over the entire service area.



Frequency reuse plan for $C = 3$, with hexagonal cells. (i=1, j =1)



Frequency reuse plan for $C = 7$ (i=2, j =1).

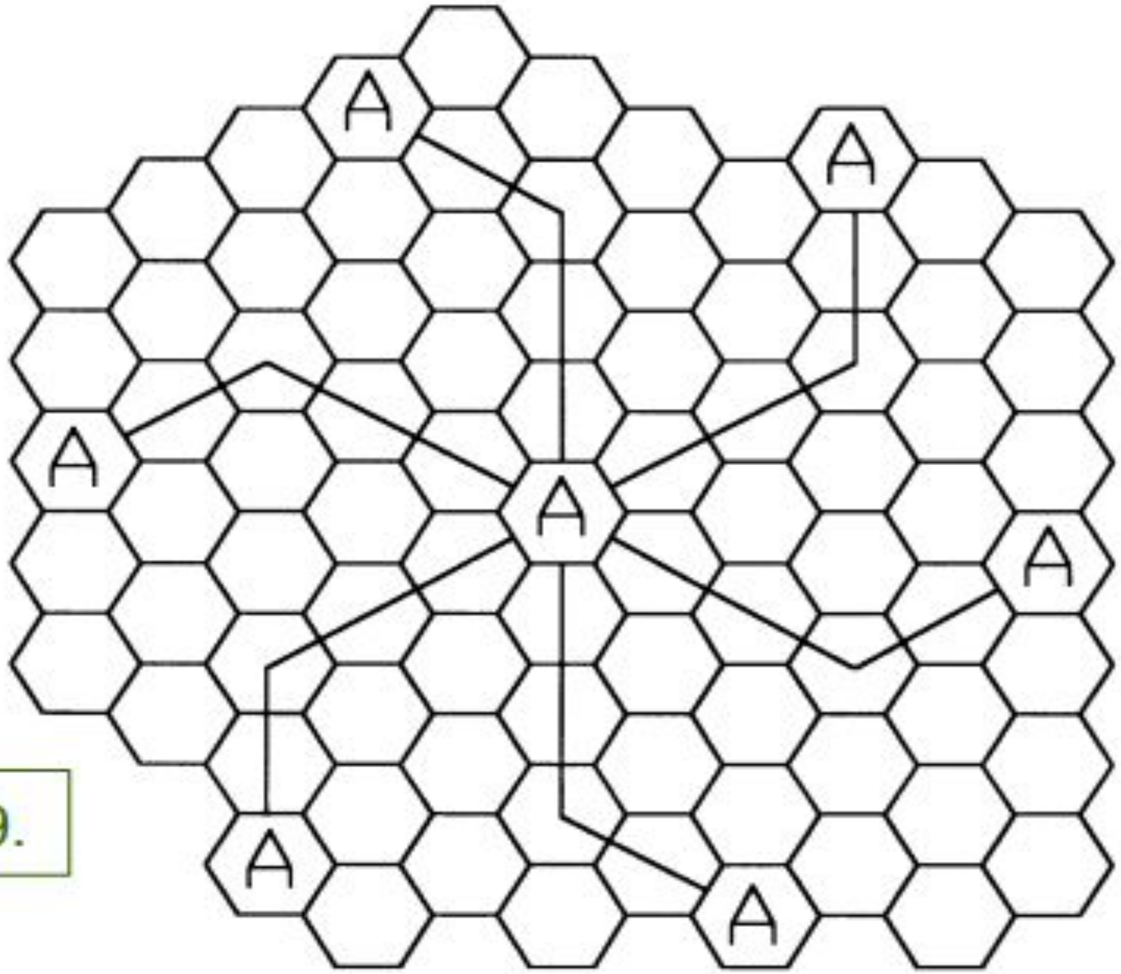
The total bandwidth for the system is *C* times the bandwidth occupied by a single cell.

Design of Cluster Size

To Find the Nearest Co-channel Neighbor of Particular Cell:

Move i cells along any chain or hexagon.

Then turn 60 degrees counterclockwise and move j cells.



In this example, i=3, j=2, N=19.

Design of Cluster Size

In order to connect without gaps between adjacent cells

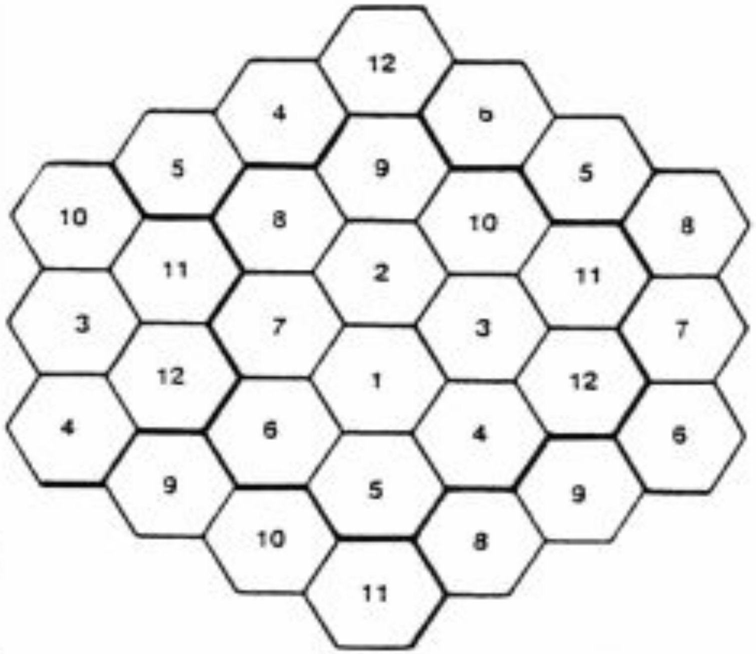
$$N = i^2 + ij + j^2$$

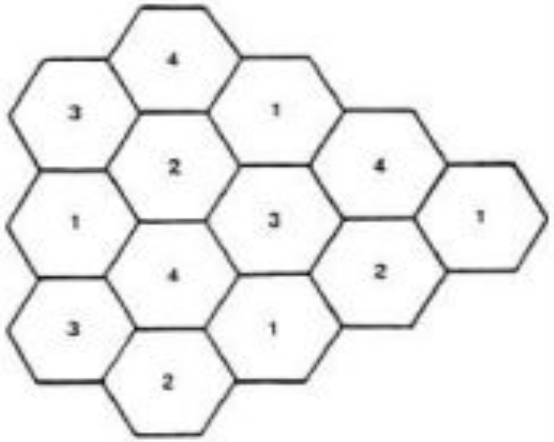
where i and j are non-negative integers.

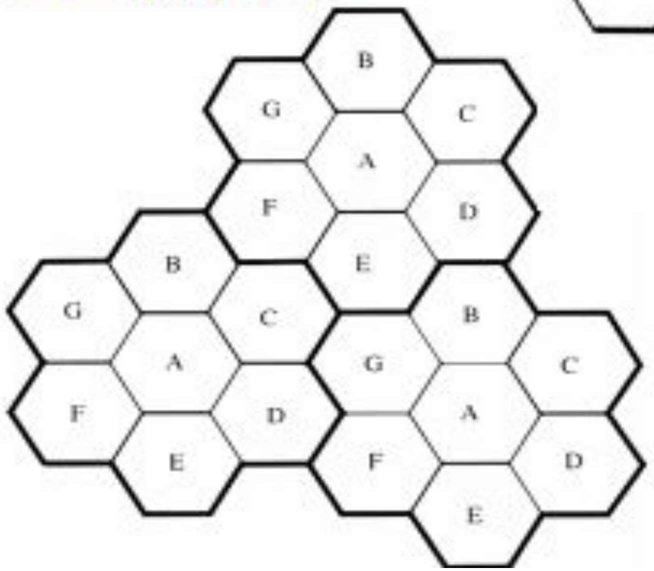
Example: When $i = 2$, $j = 1$

$$N = 2^2 + 2(1) + 1^2 = 4 + 2 + 1 = 7$$

Commonly used cluster size $N = 4, 7, 12$.



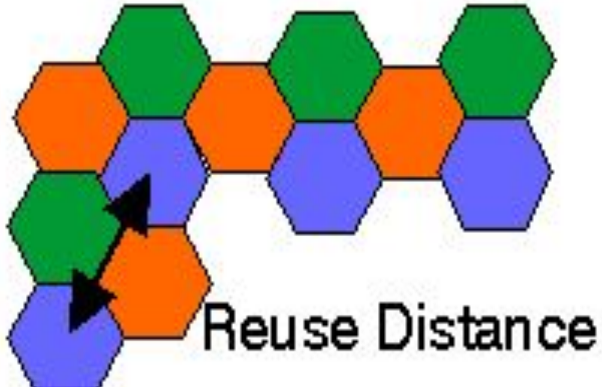




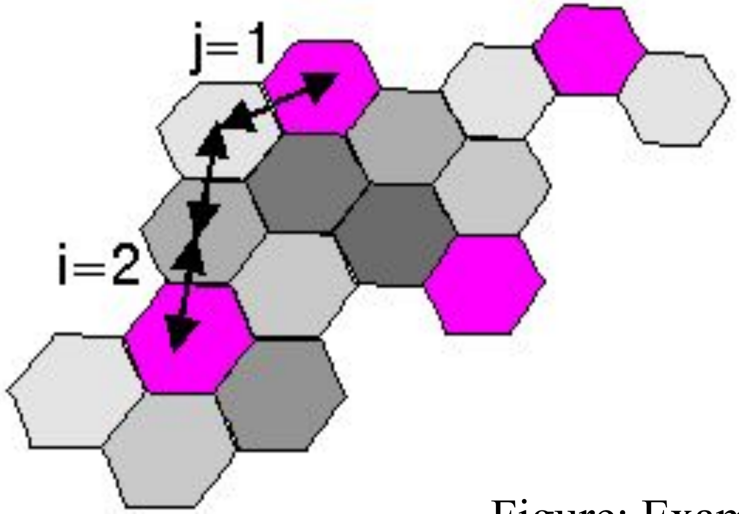
Reuse Distance (cluster design)

- The closest distance between the centres of two cells using the same frequency (in different clusters) is determined by the choice of the cluster size *C* and the lay-out of the cell cluster.
- the reuse distance r_u, normalized to the size of each

hexagon, is r_u = SQRT{3*C* }



For hexagonal cells, i.e., with 'honeycomb' cell lay-outs commonly used in mobile radio, possible cluster sizes are $C = i^2 + ij + j^2$, with integer i and j (C = 1, 3, 4, 7, 9, ...). Integers i and j determine the relative location of co-channel cells.



7-cell reuse with i = 2 and j =1.

Figure: Example of a reuse pattern i, j.

- Note that the axes of coordinates *i* and *j* have a relative angle of 60 degrees. The distance between the cell centers can be expressed by invoking Pythagoras for a triangle with one angle of 60 degrees.
- Moreover, we use that the distance between the centers of two neighboring cells is SQRT(3) times the size of an edge *R* of the hexagonal cell. This gives
- r_u = SQRT {(i^2 + 2*ij*cos(pi/3) + j^2)} SQRT{3} *R*.

Example

Problem:
If a particular FDD cellular telephone system has a total bandwidth of 33 MHz,

and if the phone system uses two 25 KHz simplex channels to provide full duplex voice and control channels...

compute the number of channels per cell if $N = 4, 7, 12$.

Solution:
Total bandwidth = 33 MHz
Channel bandwidth = 25 KHz x 2 = 50 KHz
Total available channels = 33 MHz / 50 KHz = 660

$N = 4$	Channel per cell = 660 / 4 =165 channels
$N = 7$	Channel per cell = 660 / 7 = 95 channels
$N = 12$	Channel per cell = 660 / 12 = 55 channels

Co-channel interference

Sources of interference

-another mobile in the same cell,

-a call in progress in a neighboring cell,

-other base stations operating in the same frequency band,

-or any non-cellular system which inadvertently leaks energy into the cellular frequency band.

Interference on voice channels -- cross talk—loss of quality, where the subscriber hears interference in the background due to an undesired transmission.

On control channels—dropped calls, interference leads to missed and blocked calls due to errors in the digital signaling

Interference

Major limiting factor in performance of cellular radio systems:

- **Co-channel interference**

  - Cells that use the same set of frequencies are called co-channel cells.

  - Interference between them is called co-channel interference.

- **Adjacent channel interference**

  - Interference resulting from signals which are adjacent in frequency to the desired signal.

  - Due to imperfect receiver filters that allow nearby frequencies to leak into pass band.

Increasing SNR does NOT solve co-channel interference (in fact, it can make it worse)

Reduce co-channel interference by increasing distance between co-channels

Co-channel Interference

Co-channel reuse ratio:

$$Q = \frac{D}{R}$$

R = radius of the cell

D = distance between centers of nearest co-channel cells

For hexagonal geometry,

$$Q = \frac{D}{R} = \sqrt{3N}$$

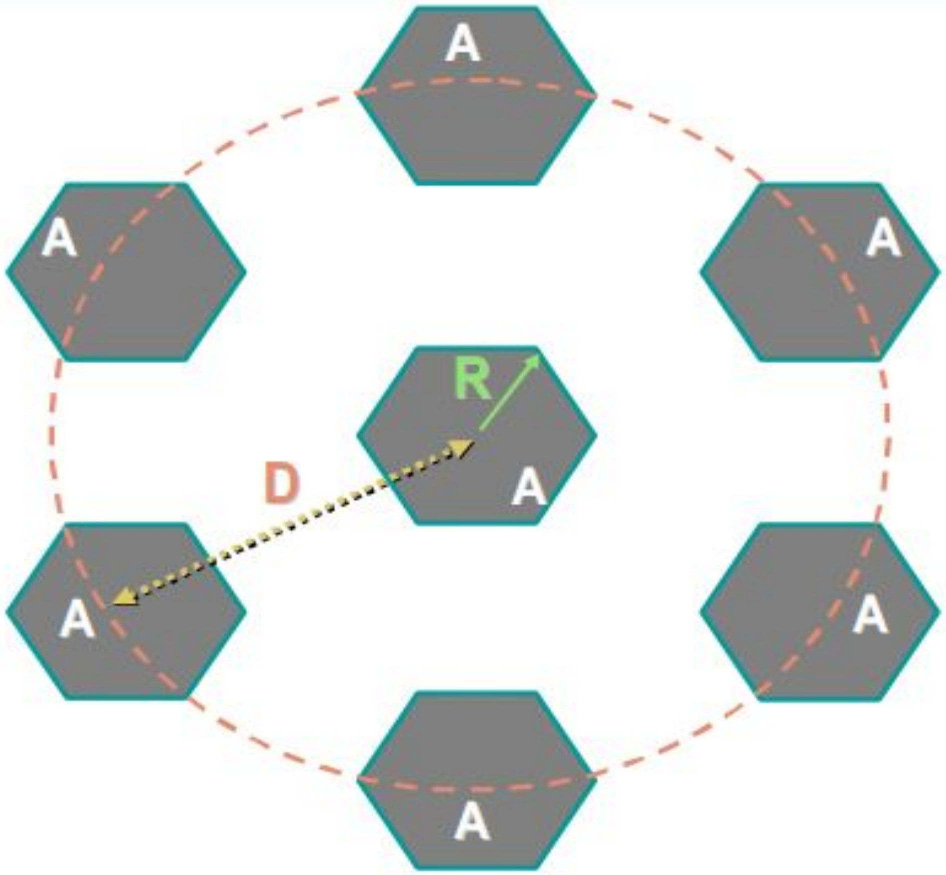


Table 3.1 Co-channel Reuse Ratio for Some Values of N

	Cluster Size (N)	Co-channel Reuse Ratio (Q)
$i = 1, j = 1$	3	3
$i = 1, j = 2$	7	4.58
$i = 2, j = 2$	12	6
$i = 1, j = 3$	13	6.24

Small Q increases system capacity (N is small)

Small Q increases co-channel interference (less distance between cells)

Co-Channel Interference

Signal to interference ratio (SIR, or S/I) for a mobile receiver is given by:

$$\frac{S}{I} = \mathrm{SIR} = \frac{S}{\sum_{i=1}^{i_0} I_i}$$

S = desired signal power from designated base station

I_i = interference power caused by the ith interfering co-channel cell base station

i_0 = number of interfering co-channel cells

- Propagation measurements in a mobile radio channel show that the average received signal strength at any point decays as a power law of the distance of separation between a transmitter and receiver. The average received power Pr at a distance d from the transmitting antenna is approximated by

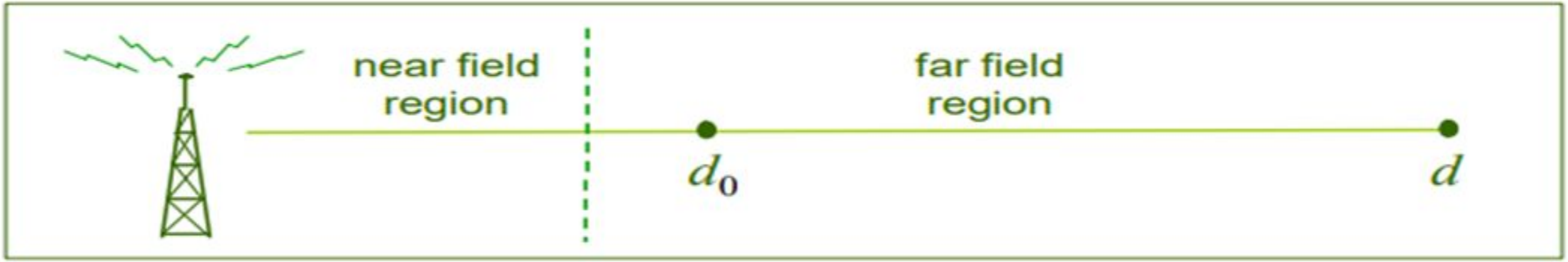
For any given antenna (base station) the power at a distance d is given by:

$$P_r(d) = P_r(d_0)\left(\frac{d}{d_0}\right)^{-n} \quad \text{or} \quad P_r(d)\,(\mathrm{dBm}) = P_r(d_0)\,(\mathrm{dBm}) - 10n\log\left(\frac{d}{d_0}\right)$$

$P_r(d_0)$: power receiver at a close-in reference point in the far field region of the antenna

d_0 : distance from the transmitting antenna to the reference point

n = path loss exponent (between 2-4 in urban cellular systems)



Co-Channel Interference

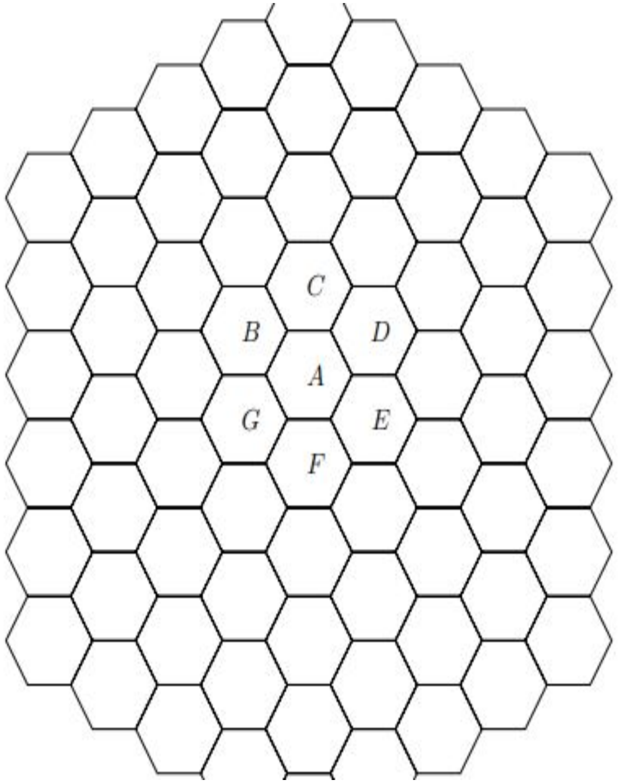
When different base stations transmit the same power, and the path loss exponent is the same throughout the coverage area, S/I for a mobile can be approximated as

$$\frac{S}{I} = \frac{R^{-n}}{\sum_{i=1}^{i_0} (D_i)^{-n}}$$

i_0 = number of first tier interfering co-channel cells

R = radius of the cell

D_i = distance of the ith interferer from the mobile



Considering only the first layer of interfering cells, if all the interfering base stations are equidistant from the desired base station and if this distance is equal to the distance D between cell centers (equidistant case), then Equation (next slide) simplifies to

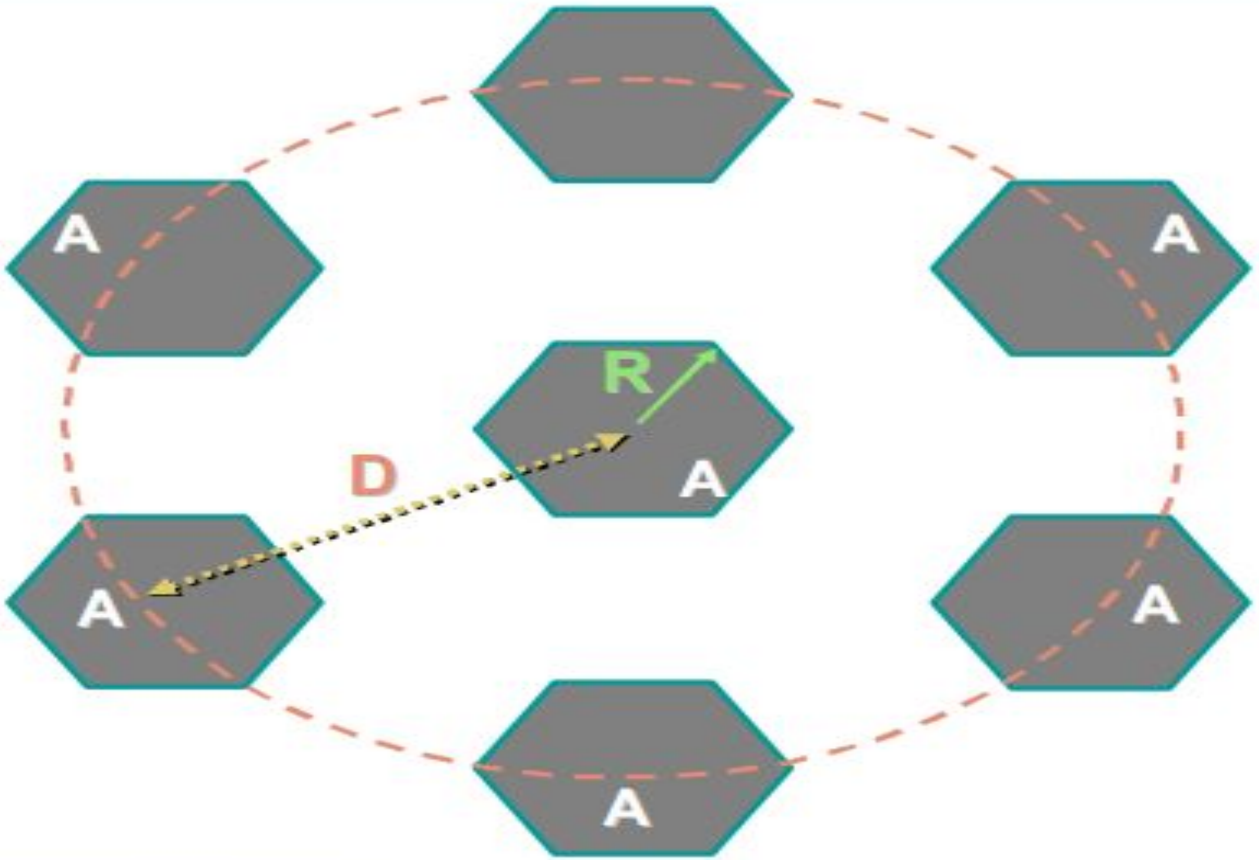
Co-Channel Interference

Equidistant case ($D_i = D$)

$$\frac{S}{I} = \frac{R^{-n}}{\sum_{i=1}^{i_0} (D)^{-n}} = \frac{(D/R)^n}{i_0} = \frac{\left(\sqrt{3N}\right)^n}{i_0}$$

To achieve 18 dB SIR (required in US AMPS), $N > 6.49$ provided $n = 4$.

That is, $N \geq 7$ should be used.



Environment	n
Free Space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban area	3 to 5
In building line of sight	1.6 to 1.8
obstructed in building	4 to 6
obstructed in factories	2 to 3

TDMA can tolerate S/I = 15 dB

Equation	Variable				
�	cluster size		N	7	(choices 4,7,12)
	path loss exponent (meas)		n	4	
3.4	co-channel reuse ratio	Q	sqrt(3N)	4.582576	
	distance between co-channels		D		meter
	radius of cells		R		meter
3.4	Ratio of distance to radius	Q	D/R	4.582576	
	number of neighboring cells	io		6	# of sides of hexagon
3.9	signal to interference ratio	S/I	(D/R)^n / io	73.5	
	convert to dB	S/I	10log(S/I)	18.66287	dB

If S/I is greater than required, it will work:� YES!

Equation	Variable				
�	cluster size		N	4	(choices 4,7,12)
	path loss exponent (meas)		n	4	
3.4	co-channel reuse ratio	Q	sqrt(3N)	3.464102	
	distance between co-channels		D		meter
	radius of cells		R		meter
3.4	Ratio of distance to radius	Q	D/R	3.464102	
	number of neighboring cells	io		6	# of sides of hexagon
3.9	signal to interference ratio	S/I	(D/R)^n / io	24	
	convert to dB	S/I	10log(S/I)	13.80211	dB

If S/I is greater than required, it will work:� NO!

Equation	Variable	�			
�	cluster size		N	7	(choices 4,7,12)
	path loss exponent (meas)		n	3	
3.4	co-channel reuse ratio	Q	sqrt(3N)	4.582576	
	distance between co-channels		D		meter
	radius of cells		R		meter
3.4	Ratio of distance to radius	Q	D/R	4.582576	
	number of neighboring cells	io		6	# of sides of hexagon
3.9	signal to interference ratio	S/I	(D/R)^n / io	16.03901	
	convert to dB	S/I	10log(S/I)	12.05178	dB

If S/I is greater than required, it will work:� NO!

Effect of sectoring:

Instead of using an omnidirectional antenna at a BS, we can use several directional antenna (e.g., three 120o sectoring antenna or six 60o sectoring antenna) to cover the same cell

FIGURE 3.10,11

120 sectoring:

Using a directional antenna with a 120 degree beamwidth.

Forward interference (primary interferers) are now 2 instead of 6 .. see figure 3.11

60 sectoring:

Using a directional antenna with a 60 degree beamwidth.

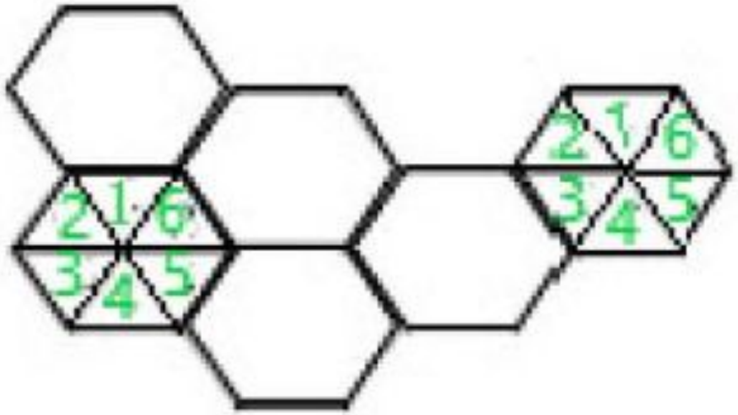
Forward interference (primary interferers) are now 1 instead of 6

The total channels assigned to the cell are split among the sectors. In this way, a BS will see less number of interfering BS because of the directiveness of the antenna.

Equation	Variable				
	cluster size		N	7 (choices 4,7,12)	
	path loss exponent (meas)		n	3	
3.4	co-channel reuse ratio	Q	sqrt(3N)	4.582576	
	distance between co-channels		D		meter
	radius of cells		R		meter
3.4	Ratio of distance to radius	Q	D/R	4.582576	
	number of neighboring cells	io		1	# of sides of hexagon
3.9	signal to interference ratio	S/I	(D/R)^n / io	96.23409	
	convert to dB	S/I	10log(S/I)	19.83329	dB

If S/I is greater than required, it will work YES!


1
2
3
1
2
3


2 1 6
3 4 5
2 1 6
3 4 5

Adjacent Channel Interference

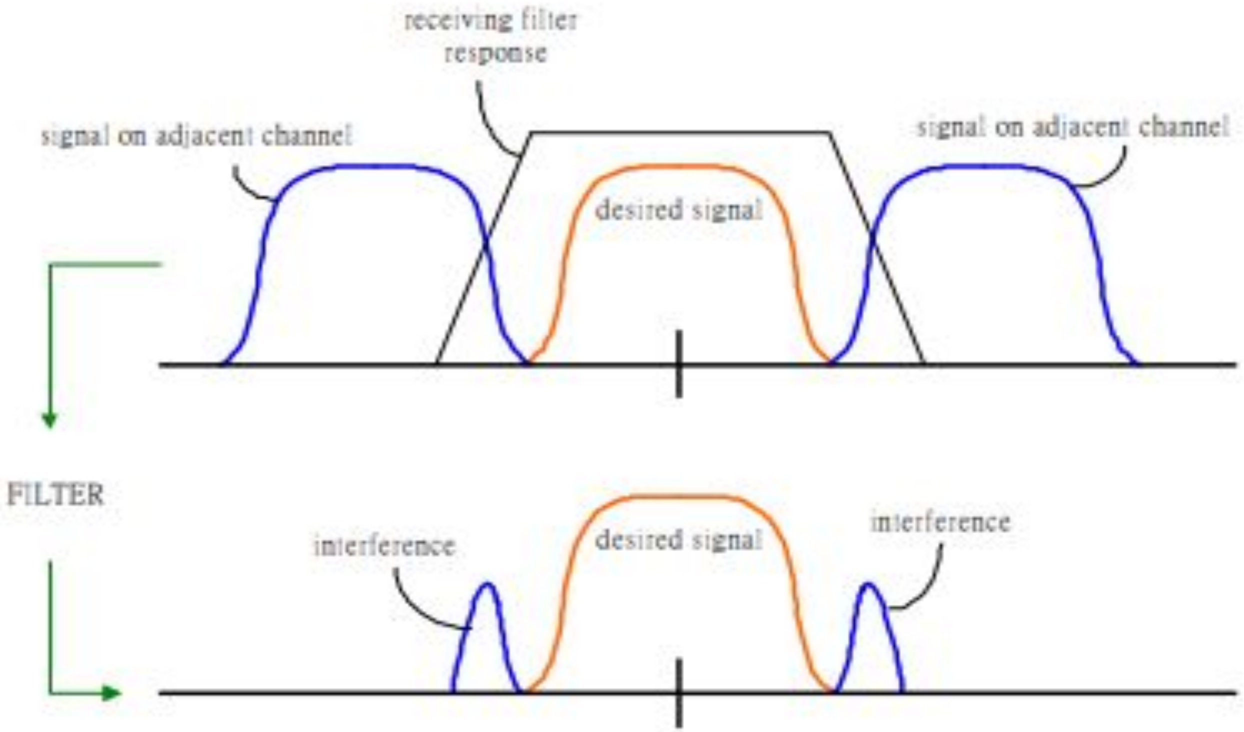
- Interference resulting from signals which are adjacent in frequency to the desired signal.

- Due to imperfect receiver filters that allow nearby frequencies to leak into pass band.

- Performance may degrade seriously due to *near-far* effect.

- Can be minimized by careful filtering and assignments; and, by keeping frequency separation between channel in a given cell as large as possible.

- A channel separation greater than six is needed to bring the adjacent channel interference to an acceptable level.



Example 3.2

If a signal-to-interference ratio of 15 dB is required for satisfactory forward channel performance of a cellular system, what is the frequency reuse factor and cluster size that should be used for maximum capacity if the path loss exponent is (a) $n = 4$, (b) $n = 3$? Assume that there are six co-channel cells in the first tier, and all of them are at the same distance from the mobile. Use suitable approximations.

Solution

(a) $n = 4$

First, let us consider a seven-cell reuse pattern.

Using Equation (3.4), the co-channel reuse ratio $D/R = 4.583$.

Using Equation (3.9), the signal-to-noise interference ratio is given by

$$S/I = (1/6) \times (4.583)^4 = 75.3 = 18.66 \text{ dB}$$

Since this is greater than the minimum required S/I, $N = 7$ can be used.

(b) $n = 3$

First, let us consider a seven-cell reuse pattern.

Using Equation (3.9), the signal-to-interference ratio is given by

$$S/I = (1/6) \times (4.583)^3 = 16.04 = 12.05 \text{ dB}$$

Since this is less than the minimum required S/I, we need to use a larger N.

Using Equation (3.3), the next possible value of N is 12, ($i = j = 2$).

The corresponding co-channel ratio is given by Equation (3.4) as

$$D/R = 6.0$$

Using Equation (3.3), the signal-to-interference ratio is given by

$$S/I = (1/6) \times (6)^3 = 36 = 15.56 \text{ dB}$$

Since this is greater than the minimum required S/I, $N = 12$ is used.

INTRODUCTION GSM

- **GSM (Global System for Mobile)** developed by **ETSI** (European Technical Standards Institute) protocols for 2G.
- GSM was developed ***to solve fragmentation problem of the 1G systems*** in Europe
- The GSM is world's 1st cellular system to specify digital modulation and network level architectures and services
- The GSM is a circuit-switched system that divides each 200kHz channel into eight 25kHz time-slots.
- GSM operates in

  890MHz to 915 MHz Reverse Link (MS to BS)

  935MHz to 960MHz Forward Link (BS to MS)
- GSM uses FDD & a combination of TDMA & FDMA technique to provide simultaneous access to multiple mobile subscriber Units.

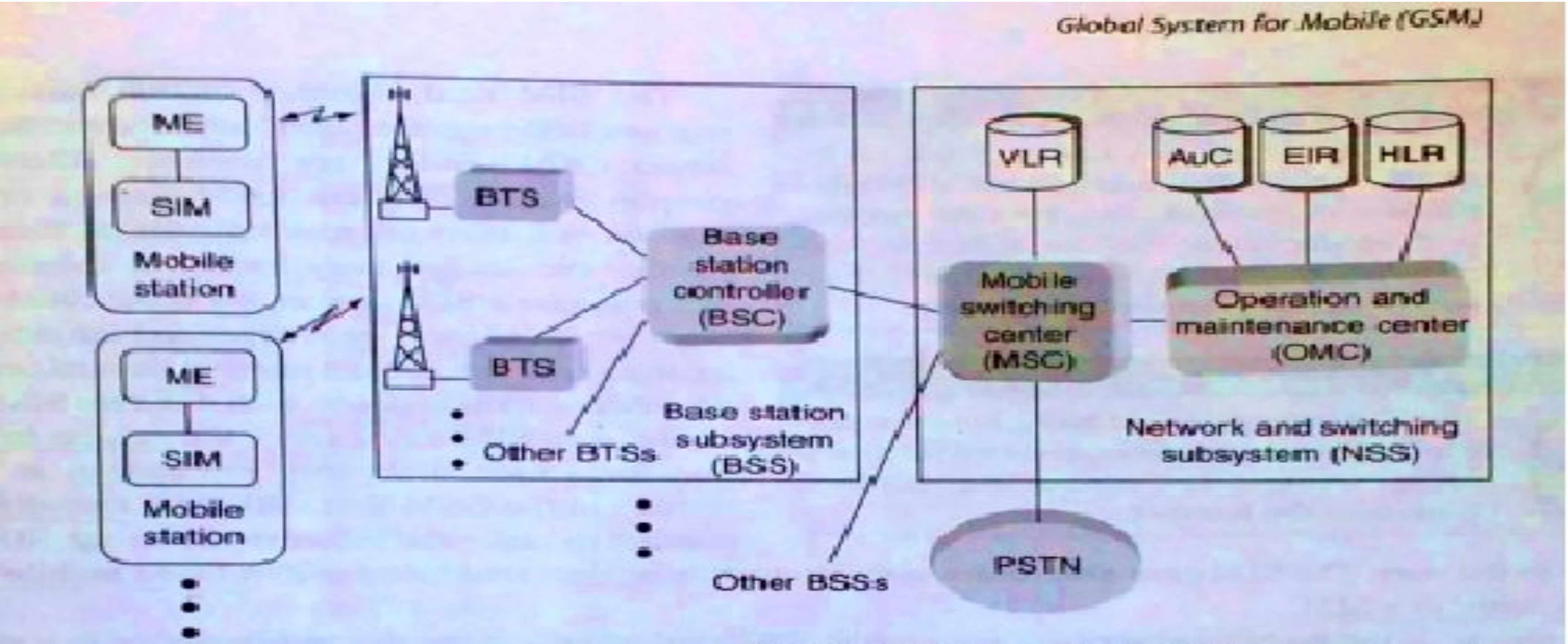
GSM is having 4 different sizes of cells are used in GSM :

- Macro : In this size of cell, Base Station antenna is installed.
- Micro : In this size of cell, antenna height is less than the average roof level.
- Pico : Small cells’ diameter of few meters.
- Umbrella : It covers the shadowed (Fill the gaps between cells) regions.

Features of GSM are :

- Supports international roaming
- Clear voice clarity
- Ability to support multiple handheld devices.
- Spectral / frequency efficiency
- Low powered handheld devices.
- Ease of accessing network
- International ISDN compatibility.

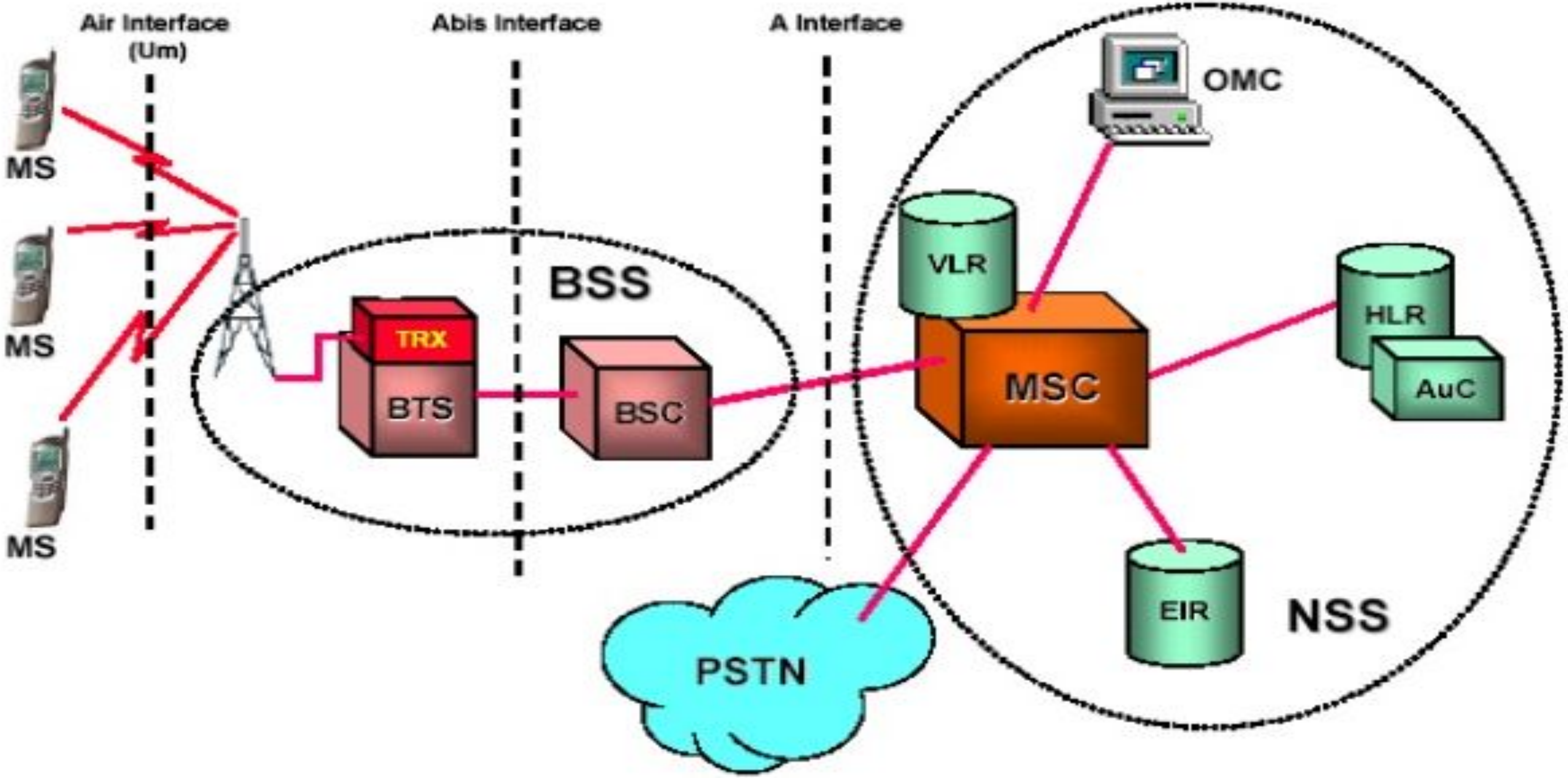
GSM ARCHITECTURE



ME	Mobile equipment
SIM	Subscriber identity module
BTS	Base transceiver station

VLR	Visitor location register
AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
PSTN	Public switched telephone network

GSM Architecture Overview



MOBILE STATION (ME & SIM)

- **ME-**

✔ physical device, consists of Transceiver, Digital Signal Processors and the antenna.

✔ uniquely identified by the **International Mobile Equipment Identity (IMEI)**.

- **SIM-**

  ✔ smart card issued at the subscription time identifying the specification of a user such as a unique number and type of the service.

  ✔ The SIM card contains the **International Mobile Subscriber Identity (IMSI)** used to identify the subscriber to the system, a secret key for authentication, service area and other information.

  ✔ The SIM card may be protected against unauthorized use by a password or personal identity number (PIN)

BASE STATION SUBSYSTEM (BSS) :(BTS & BSC)

- **BSC:**
  - ✔ is the connection between the mobile station and the Mobile service Switching Center (MSC).
  - ✔ It is a small switch inside BSS in change of frequency administration, maintains appropriate power levels of signal and handoff among the BTSs inside a BSS. This reduces burden of MSC
  - ✔ BSC Controller manages the radio resources for one upto several hundred BTSs.
- From 13kbps to 64kbps-at BSS

BASE STATION SUBSYSTEM (BSS) :(BTS & BSC)

Base Transceiver Station (BTS):

- defines a single cell (radius 100m to 35km)
- BTS components include a Tx, a Rx and signaling equipment to operate over the air interface.

✔ Interface between BTS & BSC – Abis interface- carries traffics and maintain data

✔ Interface between BSC & MSC – A interface- standardized within GSM.

✔ User's speech is converted to 13kbps digitized voice with speech coder –at MS

✔ Wired network uses 64kbps PCM digitized voice in PSTN technology.

NETWORK SUBSYSTEM

- It provides link between cellular networks and PSTN or ISDN or data network.
- The NSS **controls handoffs** between calls in different BSSs, **authenticates users & validates their accounts** & includes functions for **enabling worldwide roaming** of mobile subscriber.
- It include the main switching functions of GSM as well as data based needed for subscriber data and mobility management.
- It consists of
  - ✔ Mobile Switch Center (MSC)
  - ✔ Home Location Register (HLR)
  - ✔ Visitor Location Register (VLR)
  - ✔ Authentication Center (AuC)
  - ✔ Equipment Identity Register (EIR)
  - ✔ Interworking Function (IWF)

1. Mobile Switching Centre (MSC)

- It is a hardware part of wireless switch that can communicate with PSTN using Signaling system- 7 (SS-7) protocol.
- It also communicates other MSCs in the coverage area of the service provider.
- **Functions of MSC:**

- Call setup, supervision, release and Call routing
- Digit collection and translation
- Billing information collection
- Mobility management (registration, location updating, inter BSS and inter MSC call handoffs)
- Paging and alerting
- Management of radio resources during call.
- Echo cancellation

2. Home Location Register (HLR)

- The HLR represents **a central database software** that Handles the management of the mobile subscriber account.
- It is referenced using the SS7 signaling capabilities for every incoming call to the GSM network for determine the current location of the subscriber.
- The HLR is kept updated with the current locations of all its mobile subscribers, including those who may have roamed to other network operator within or outside the country.
- The routing information is obtained from the serving VLR on a call by call basis, so that for each incoming call the HLR queries the serving VLR for an MSRN(mobile station roaming number).
- Usually one HLR is deployed for each GSM network for administration of subscriber configuration and services.

2. Home Location Register (HLR)

- Besides the up to date information for each subscriber, which is dynamic, HLR maintains the following data on a permanent basis.
  - International Mobile Subscriber Identity (IMSI)
  - Service subscription information.
  - Service restrictions
  - Supplementary services subscribed to
  - Mobile terminal characteristics
  - Billing/ accounting information.

Supplementary services are additional **services** - include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others.

3. Visitor Location Register (VLR)

- The VLR represents a **temporary database software**
- Generally there is one VLR per MSC.
- This register contains information about the mobile subscribers who are currently in the service area covered by the MSC/ VLR.
- The VLR also contains information about locally activated features such as call forwarding on busy.
- Thus temporary subscriber information available in VLR includes:
    - Features currently activated
    - Temporary mobile station identity (TMSI)
    - Current location information about the MS.

4. AUTHENTICATION CENTER (AUC)

- It is the **database that holds different algorithms** that are used for authentication & encryption of mobile subscribers that verify the mobile user's identity
- It ensure the **confidentiality** of each call.
- AuC **protects network** cellular operators from different types of frauds and spoofing.
- It contains the security modules for the authentication keys.
  - ✔ Algorithm **A3** is used for **authentication**
  - ✔ Algorithm **A8** is used for **Cipher key generation**
  - ✔ Algorithm **A5** is used for **encryption**.

5. Equipment Identity Register (EIR)

- The EIR is **another database** that keeps the information about **identify of ME such as IMEI.**
- IMEI reveals the details about the manufacturer, country production and device type.
- This information is used to
  1. prevent calls from being misused
  2. prevent unauthorized or defective MSS
  3. report stolen mobile phones
  4. check if the mobile is operating according to the specification of its type.
- Each ME is identified by IMEI which is memorized by the manufacturer and cannot be removed.
- By the registration mechanisms the MS always sends IMEI to the network so that the EIR can memories and assign them to three different lists.

5. EQUIPMENT IDENTITY REGISTER (EIR)

- **White list:** for all known, good IMEIs- **are allowed** to enter in the network.
- **Black list:** for **bad or stolen** handsets- **are not allowed** to enter in the network
- **Grey list:** for handsets/IMEIs that are **uncertain**- are momentarily not allowed to enter in the network eg because of **software version is too old** or because they are **in repair**.
- In future there will be an interconnections between all the EIRs to avoid the situation where a mobile stolen in one country can be used in GSM network from a different country.

Equipment Identity Register – EIR

- White List
- Black List
- Grey List

IMEI is Checked In White List

If NOT found

IMEI is Checked in Black/Grey List

EIR focus on the equipment , not the subscriber!!

6. INTERWORKING FUNCTION (IWF)

- IWF-is a subsystem in the PLMN (Public Land Mobile Network)
- It **allows non speech communications** between GSM and other networks.
- The task of IWF is particularly **to adopt the transmission parameters and protocol conversion**.
- The physical manifestation of an IWF may be through a modem which is activated by MSC dependent on bearer service and destination network.

7. OSS (OPERATION & SUPPORT SYSTEM)

- The implementation of OMC is called the **operation and support system** (OSS).
- It **supports operation and maintenance of systems and allows engineers to monitor, diagnose and troubleshoot every aspect of GSM network.**
- OSS supports one or more OMC (operation maintenance center)
- Used to monitor & maintain the performance of each MS, BS, BSS and MSC within GSM system.

7. OSS (Operation & Support System)

- OSS has main 3 functions:

1. To maintain all telecommunication hardware & network operations with a particular service area
2. Manage all ME in the system
3. Manage all charging and billing procedures.

- Within each GSM system, an OMC is dedicated to each of these tasks and has a provision for adjusting all base station parameters and billing procedures .
- It provide the ability to determine their performance and integrity of each unit of ME in the system.

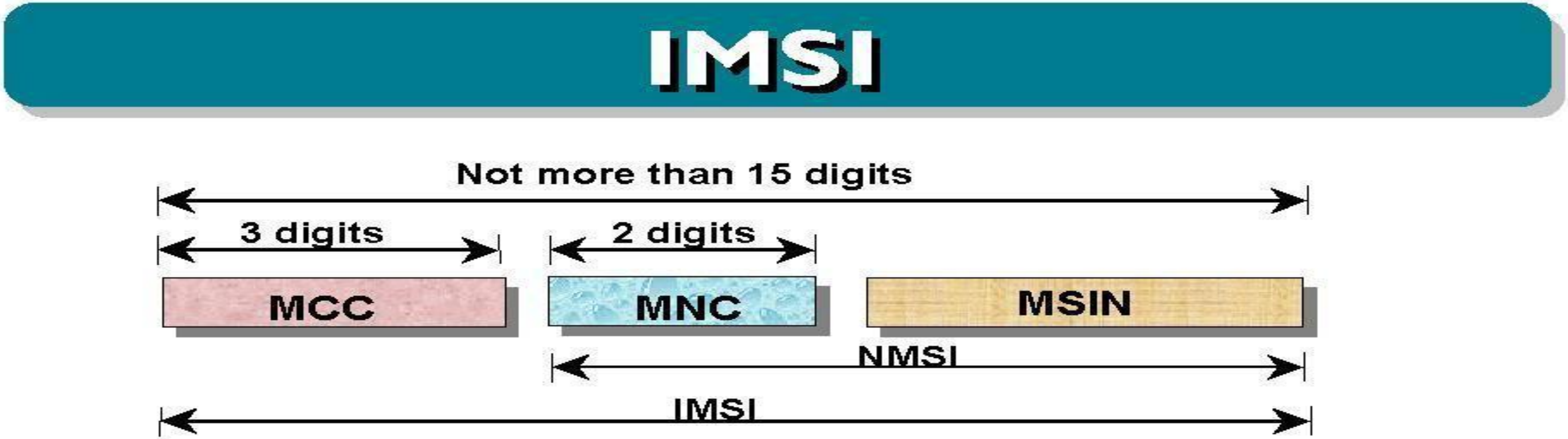
IDENTIFIERS:

1. International Mobile Subscriber Identity (IMSI):

- The IMSI is assigned to an MS at subscription time. It uniquely identifies a given MS.
- When an MS attempts a call, it needs to contact a BS. The BS can offer its service only if it identifies the MS as a valid subscriber.
- For this MS needs to store certain values uniquely defined for the MS, like country of subscription, network type, subscriber ID and so on.
- The IMSI contains 15 digits and includes
    - Mobile Country Code (MCC)—3 digits (home country)
    - Mobile Network Code (MNC)—2 digits (Network provider Code)
    - Mobile Subscriber Identification code/Number (MSIC/MSIN)
    - National Mobile Subscriber Identity (NMSI)
    - Another use of IMSI is to find information about the subscriber’s home PLMN

FORMAT OF IMSI

https://www.mcc-mnc.com/



MCC: Mobile Country Code, It consists of 3 digits .
For example: The MCC of China is "460"。

MNC: Mobile Network Code, It consists of 2 digits .
For example: The MNC of China Telecom is "00"。

MSIN: Mobile Subscriber Identification Number. H1H2H3 S ABCDEF
For example: 666-9777001

NMSI: National Mobile Subscriber Identification, MNC and MSIN form it together.

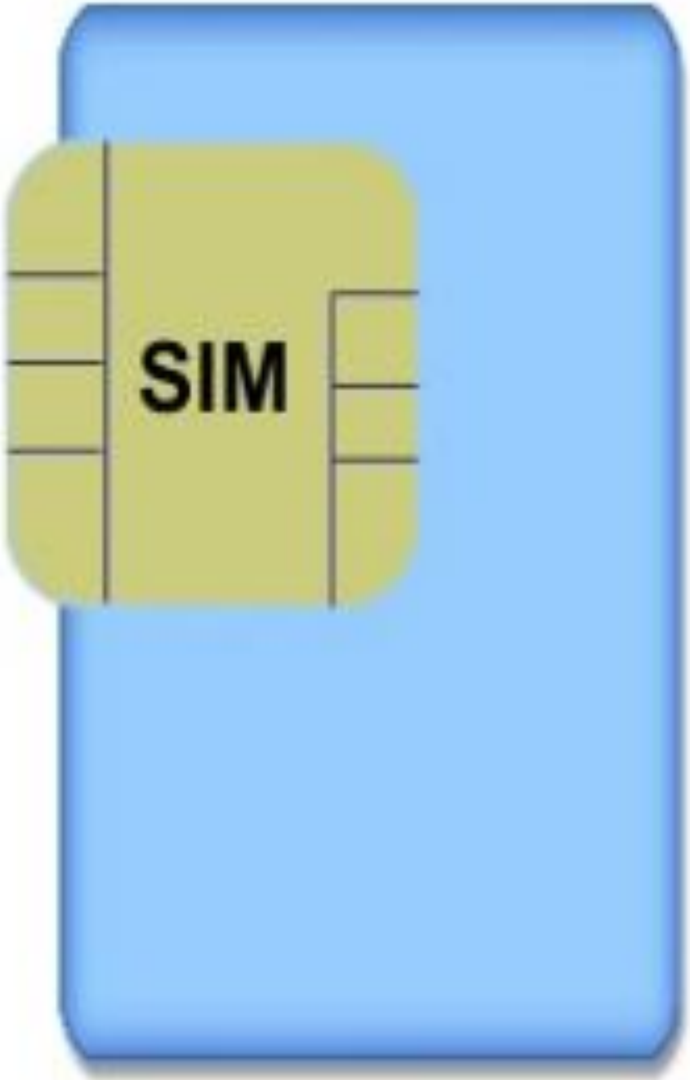
For Example of IMSI : 460-00-666-9777001

2. SIM (Subscriber Identity Module)

- Every time the MS has to communicate with a BS, it must correctly identify itself.
- An MS does this by storing the mobile phone number, personal information number for mobile station, authentication parameters and so on, in the SIM card.
- Smart SIM cards have a flash memory –to store small messages to the unit.
- Advantage- it supports roaming with or without a cell phone, also called SIM roaming.
- Carry only the SIM card alone and insert in any GSM mobile phone to make a it work as per customized MS.

Subscriber Identity Module – SIM

- International Mobile Subscriber Identity (IMSI)
- Temporary Mobile Subscriber Identity (TMSI)
- Location Area Identity (LAI)
- Subscriber Authentication Key (Ki)



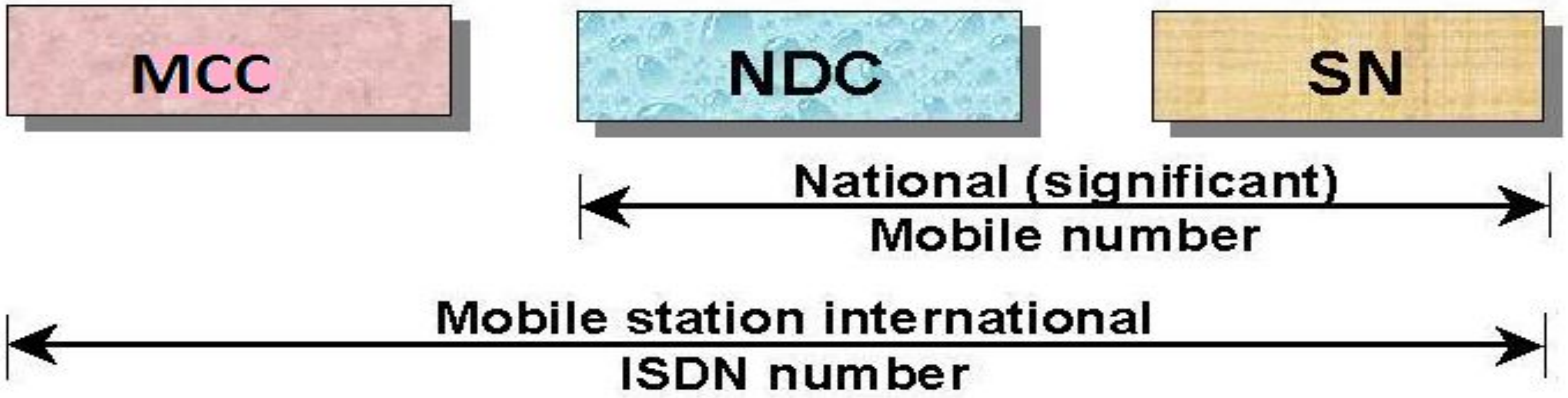
3. Mobile System ISDN (MSISDN)

- It identifies a particular MS's subscriber, with the format shown. MCC- 1 to 3 digits, NDC-variable, SN- variable
- The GSM actually does not identify a particular mobile phone, but a particular HLR.It is the responsibility of HLR to contact the mobile phone.
- https://ind.areacodebase.com/ndc_list

National Destination Code List

National Destination Code	Region Name	Carrier Name
11	**New Delhi**	**Tata** Teleservices Ltd (TTSL)
11	**New Delhi**	Videocon Telecom
11	**New Delhi**	Vodafone India Ltd
120	**Uttar Pradesh**	Aircel Ltd

3. Mobile System ISDN (MSISDN)



CC: Country Code. For example: The CC of China is "86".

NDC: National Destination Code. For example: The NDC of China Telecom is 139, 138, 137, 136, 135.

SN: Subscriber Number. Format:H0 H1 H2 H3 ABCD

Example: 86-139-0666-1234

4. Location Area Identity (LAI)

- GSM service area is usually divided into a hierarchical structures.
- Each PLMN area is divided into many MSCs.
- Each MSC typically contains a VLR to inform the system if a particular cell phone is roaming
- Each MSC is divided into many location areas (LAs).
- An LA is a group of cells and is useful when the MS is roaming in a different cell but the same LA.
- **LA identifier should contain the country code, the mobile network code and LA code.**

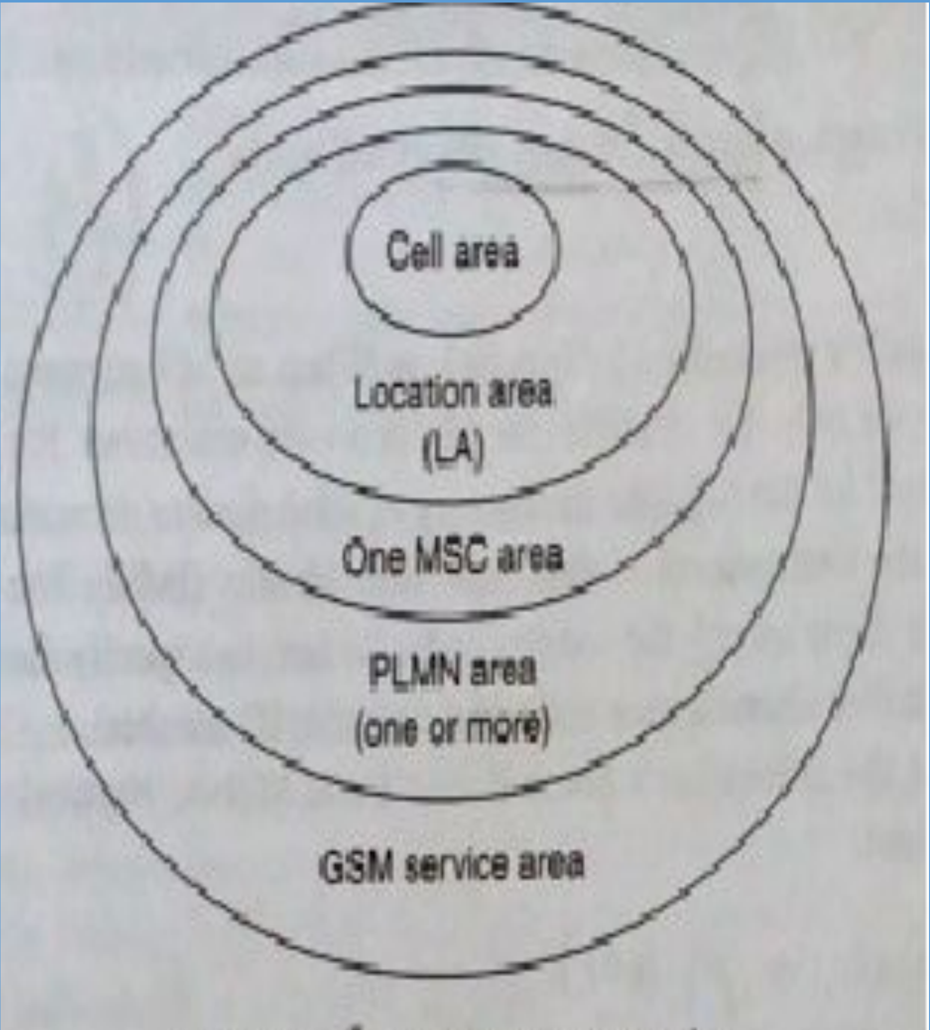


Fig. 11.7 | GSM system hierarchy

LAI

The LAI is the international code for a location area.

MCC: Mobile Country Code , It consists of 3 digits .
For example: The MCC of China is "460"

MNC: Mobile Network Code , It consists of 2 digits .
For example: The MNC of China Mobile is "00"

LAC: Location Area Code , It is a two bytes hex code.
The value 0000 and FFFF is invalid.

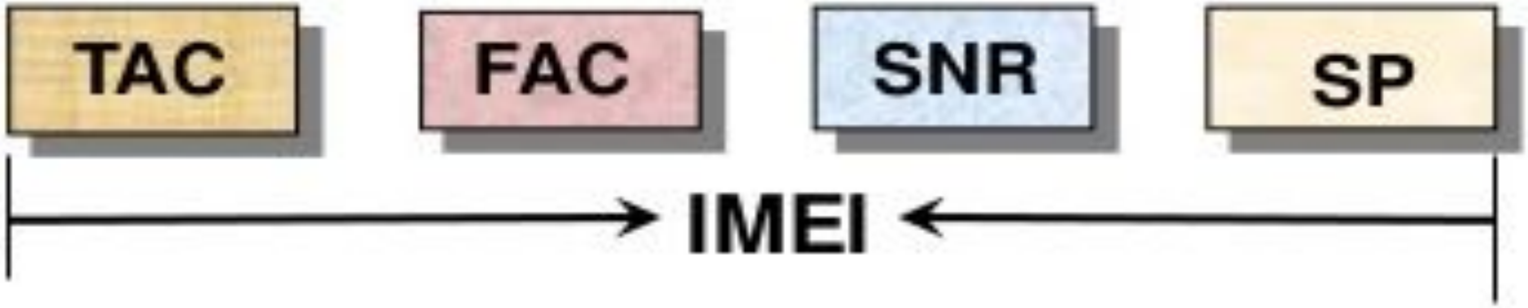
For example: 460-00-0011

5. International Mobile Station Equipment Identification (IMSEI)

- Each GSM mobile phone equipment is assigned a 15-bit long international MS equipment identity number to contain manufacturing information.
- When the mobile phone equipment passes the interoperability tests, it is assigned a type approval code.
- Since a single mobile unit may not be manufactured at the same place, a field in IMSEI, called the final assembly code, identifies the final assembly place of the mobile unit.
- To identify uniquely a unit manufactured, a Serial Number (SN) is assigned.
- A spare digit is available to allow further assignment depending on requirements.

IMEI

IMEI: International Mobile Station Equipment Identification

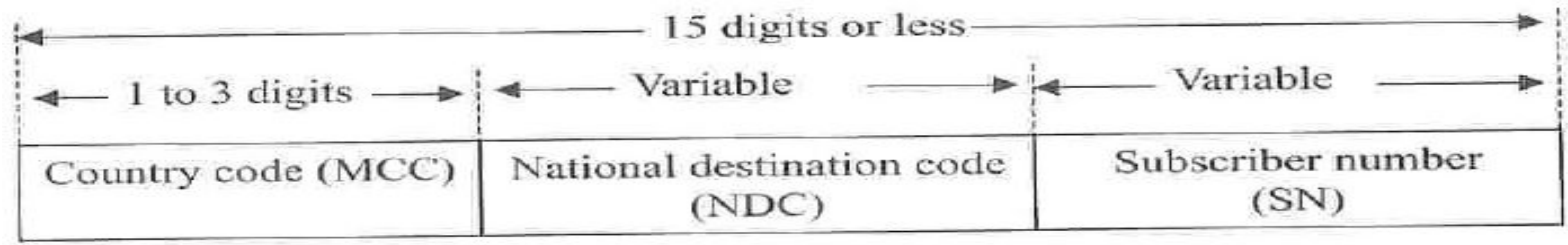


TAC: Type approval code, 6 bit, determined by the type approval center
FAC: Final assembly code, 2 bit, It is determined by the manufacturer.
SNR: Serial number, 6 bits, It is issued by the manufacturer of the MS.
SP: 1 bit , Not used.

Check the IMEI in your MS : *#06#

6. MS Roaming Number (MSRN)

- When an MS roams into another MSC, that unit has to be identified based on the numbering scheme format used in that MSC.
- Hence the MS is given a temporary roaming number called MS roaming number (MSRN)
- This MSRN is stored by the HLR and any calls coming to that MS are rerouted to cell where the MS is currently located



Format of MSRN.

7. TMSI

- As all transmission is sent through the air interface, there is a constant threat to security of information sent.
- A Temporary identity mobile subscriber identity (TMSI) is usually sent in place of IMSEI.

Self reflection week 3

Students are required to go through slide no. 50 to 61 and answer the following.

1. How do you find your IMSI number on your SIM/ handset? Give format of IMSI number and Mention your own IMSI number.
2. How do you find your SIM number on handset? Mention your SIM number?
3. Give format of MSISDN number and mention the same for your handset.
4. What is LAI. Mention LAI code for India.
5. Give format for IMEI number and mention the same for your handset.
6. Give format of MSRN and give one example for the same.

GSM AIR INTERFACE SPECIFICATIONS

Parameter	Specifications
Reverse Channel Frequency	890 - 915 MHz
Forward Channel Frequency	935 - 960 MHz
ARFCN Number	0 to 124 and 975 to 1023
Tx/Rx Frequency Spacing Tx/Rx Time Slot Spacing	45 MHz 3 Time slots
Modulation Data Rate	270.833333 kbps
Frame Period	4.615 ms
Users per Frame (Full Rate)	8
Time slot Period	576.9 μs
Bit Period	3.692 μs
Modulation	0.3 GMSK
ARFCN Channel Spacing	200 kHz
Interleaving (max. delay)	40 ms
Voice Coder Bit Rate	13.4 kbps

GSM STANDARD AIR INTERFACE SPECIFICATIONS

Sr. No.	Parameters	Specifications
1.	Frequency Band	Uplink 890MHz-915MHz Download 935MHz-960MHz
2.	Special Allocation	50MHz (25 MHz each for Uplink & Downlink)
3.	Forward & Reverse channel Frequency Spacing	45 MHz
4.	Tx/Rx time slot spacing	3 time slots
5.	RF channel BW	200 KHz (ARFCN channel spacing)
6.	ARFCN number	0 to 124 & 975 to 1023
7.	Multiple access technique	TDMA/FDMA
8.	Duplexing Technique	FDD
9.	Modulation scheme	GMSK (B* Tb = 0.3)
10.	No. of time slots per RF channel BW	8 (users per frame full rate)
11.	No of voice channels	1000

GSM STANDARD AIR INTERFACE SPECIFICATIONS

Sr. No.	Parameters	Specifications
12.	Modulation data rate	270.833 kbps
13.	Spectrum efficiency	1.35bps/Hz
14.	Frame period	4.615ms
15.	Time slot period	577 us
16.	Bit period	3.692 us
17.	Interleaving (max delay)	40 ms
18.	Speech coding	RELP-LTP @ 13.4 kbps
19.	Channel Coding	CRC with r = ½; L=5 convolution coding
20.	Type of equalizers	Adaptive
21.	Handheld mobile Tx power	1 W max; 125mW avg

GSM Radio Subsystem

As suggested by the name, the radio subsystem is comprised of all the radio specific elements, i.e.

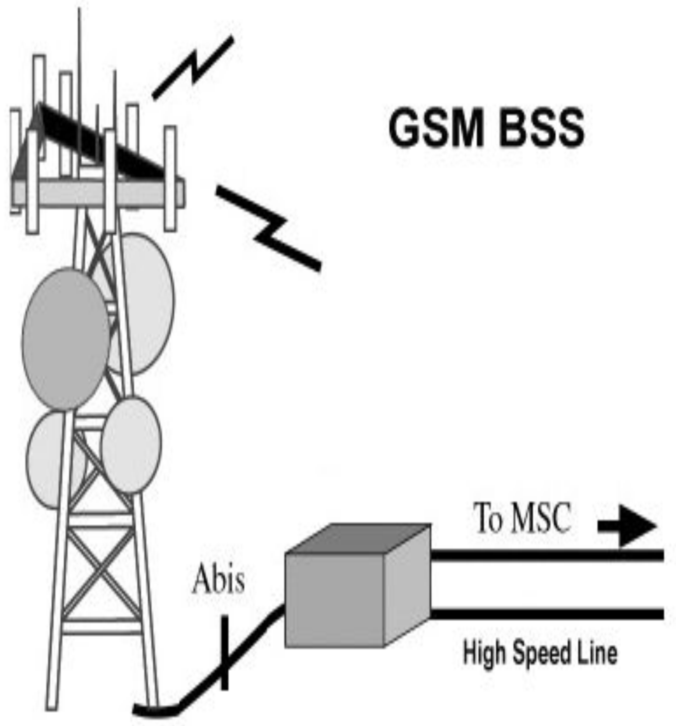
- The mobile stations (MS) and the base station subsystem (BSS).
- The connection between the RSS and the NSS via the A interface (solid lines) and
- The connection to the OSS via the O interface (dashed lines).

- The A interface is generally based on a circuit-switched PCM-30 system (2.048 Mbit/s), carrying up to 30 X 64 kbit/s connections, whereas the O interface uses the Signalling System No. 7 (SS7) based on X.25 carrying system management data to/from the RSS.

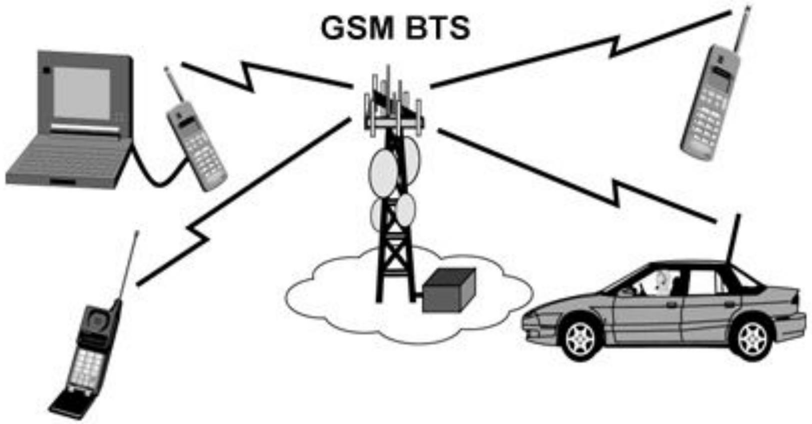
Base station subsystem(BSS)

The BSS is composed of two parts:

- The Base Transceiver Station (BTS)
- The Base Station Controller (BSC)
- The BTS and the BSC communicate across the specified Abis interface, enabling operations between components that are made by different suppliers.
- The radio components of a BSS may consist of four to seven or nine cells. A BSS may have one or more base stations.
- The BSS uses the Abis interface between the BTS and the BSC.
- A separate high-speed line (T1 or E1) is then connected from the BSS to the Mobile MSC.



The Base Transceiver Station (BTS)



The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between 1 and 16 transceivers, depending on the density of users in the cell. Each BTS serves as a single cell. It also includes the following functions:

- Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna
- Transcoding and rate adaptation
- Time and frequency synchronizing
- Voice through full- or half-rate services
- Decoding, decrypting, and equalizing received signals
- Random access detection
- Timing advances
- Uplink channel measurements

GSM CHANNELS

- Uplink Frequency = 890MHz- 915 MHz (Forward)
- Downlink Frequency = 935 MHz- 960 MHz (Reverse)
- The available 25 MHz spectrum is divided into 124 FDM channels
- Each occupy 200 KHz with 100 KHz guard band at two edges of the spectrum.
- The available Forward & reverse frequency bands are divided into 200 KHz wide channels called **ARFCN** (Absolute Radio Frequency Channel Numbers)

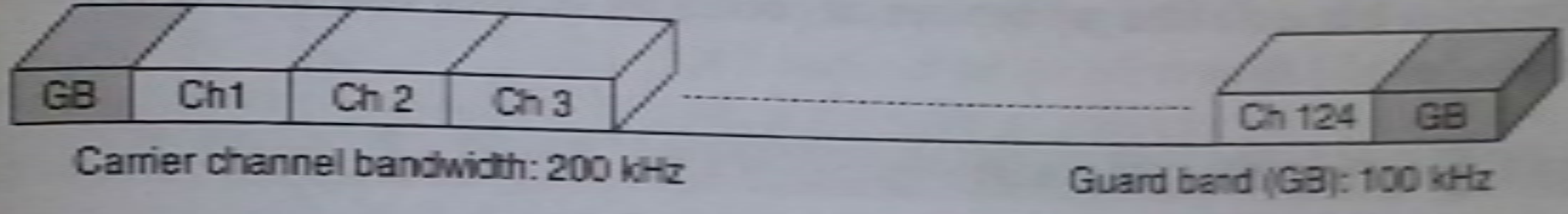
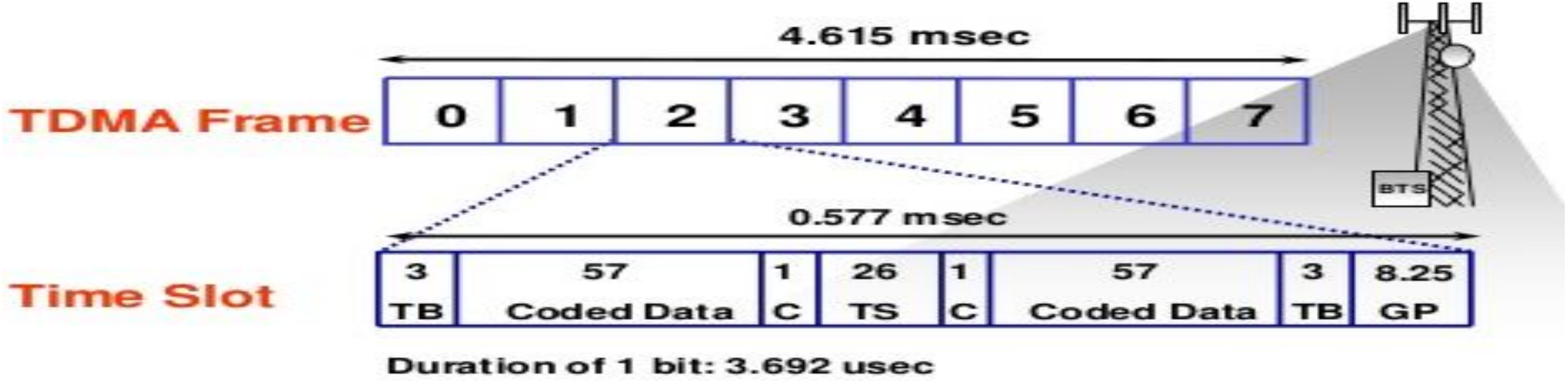


Fig. 11.10 | *Frequency channels in GSM-900*

FRAME STRUCTURE DESIGNING REQUIREMENTS:

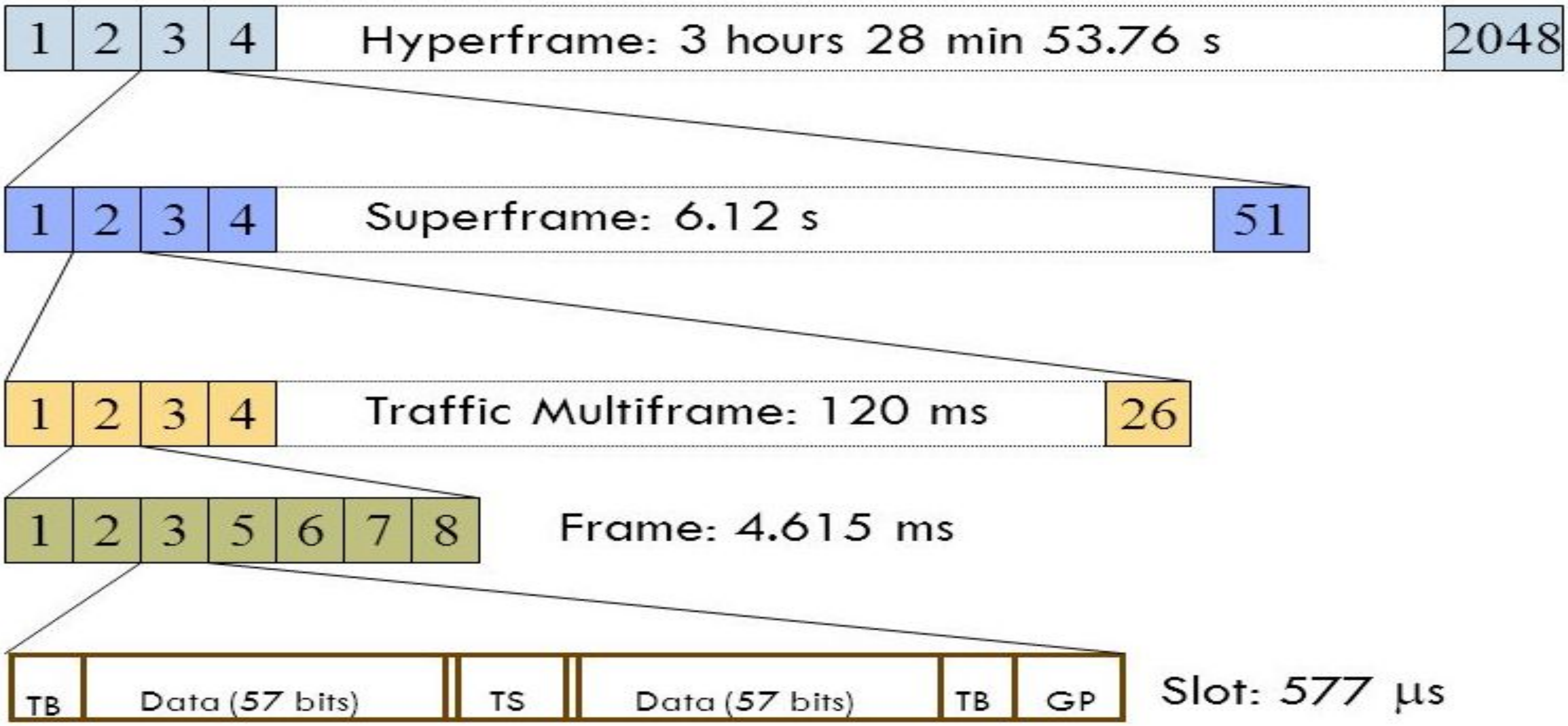
1. Frequency Band of Operation: around 900MHz
2. Number of Logical Channels or Number of Time slots in TDMA frames: 8 frames to serve 8 simultaneous users
3. Channel Bandwidth: 25 KHz . To serve 8 mobile subscribers using TDMA, Channel BW= 8*25= 200 KHz
4. Maximum Cell Radius (R): max 35km
5. Maximum Vehicle Speed (Vm): 250km/h
6. Maximum Delay Spread (Δm): 10 sec
7. Maximum Coding Delay: 20ms

GSM Basic Frame Structure



- **TB :Trail Bits**:3 bits at the start and at the end excluding Guard bits
- **Coded/Encrypted Data :** two 57 bits data fields i.e.114 cipher text bits
- **Stealing Bit :** 1 bit each at the end of two 57 bit data field. It indicate whether this block contains **data or stolen** (for urgent control signaling)
- **Training Data :** 26 bits, known bit pattern that differs for different adjacent cells. Used for **multipath equalization** to extract the desired signal from unwanted reflections.
- **Guard Bits:** 8.25 bits, used to **avoid overlapping** with other bursts due to different path delays.

GSM HYPERFRAME FORMAT



GPRS Technology

- The General Packet Radio Service (GPRS) is **non voice value added service** to the mobile users
- It is an **enhancement of GSM** system – uses packet switched data services
- Well suited for **non real time internet usage** such as retrieval of emails, Faxes & Asymmetric web browsing (where downloading is more than uploading)
- It requires some **new network elements, interfaces** and **protocols** that handles packet traffic
- It provides **short connection set up times**
- practical data rates up to **115 kbps** for each mobile data user.

Key Features of GPRS

a) **Packet switching**: information data is split into separate packets before transmission and reception.

b) **Mobile data over GPRS network :** it uses the air interface and infrastructure of GSM network that can support up to 171.2kbps

c) **Spectrum efficiency :** GPRS resources are used only when mobile users are actually sending or receiving data (instead of a dedicated channel).

This enhances the spectrum efficiency as many GPRS users can potentially share the same BW and be served together.

Key Features of GPRS

d) **Capacity Enhancement:** Because of high spectrum efficiency it may not be required to build idle capacity for use during peak hours, and allow using network resources in a dynamic and flexible way.

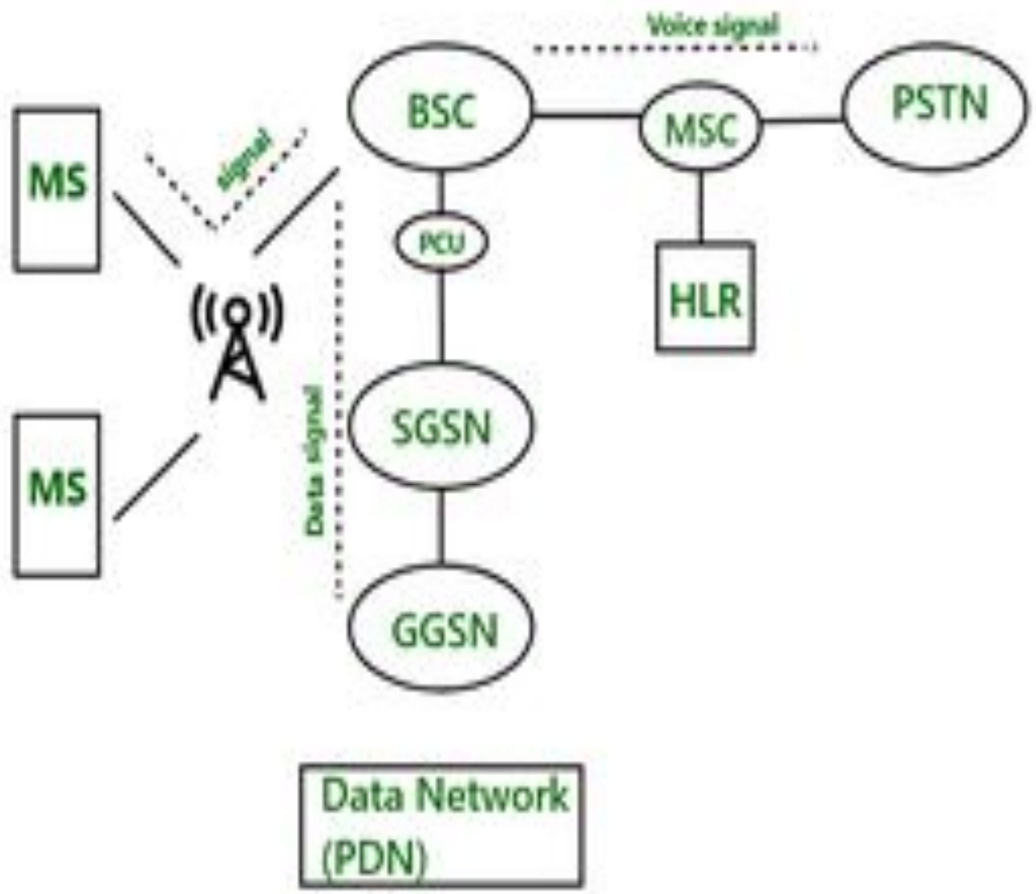
GPRS reduces SMS center and signaling channel loading by migrating some traffic using GPRS/SMS interconnect supported by the GPRS network.

e) **Reservation Protocol in GPRS:** the raw data rate (high)=171.2kbps . The same slot can be reserved for data access using slotted ALOHA reservation protocol medium access technique.

f) **Security Features:** includes key security parameters such as anonymity, authentication and confidentiality for user data and signaling. Same as GSM.

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.

GPRS Architecture



GPRS Architecture

- In GPRS there is one component is added to BSC called PCU.
- PCU stands for Packet Control Unit. If signal comes to BSC and that signal contains data, then PCU routes to the SGSN.
- Interface is used between BSC and PCU is FRI interface.
- After signal comes to SGSN, it delivers the data packet to the GGSN.
- GGSN routes the data packet to the data network (PDN- Predefined Data Network).

GPRS architecture

- New network elements:
  - ✔ GGSN(Gateway GPRS Support Node)
  - ✔ SGSN(Serving GPRS Support Node)
  - ✔ Other elements
  - ✔ GPRS backbones
- GPRS Mobile classes

GPRS Network Architecture

Technical changes to make GPRS from GSM:

1. GPRS-MS:

- new GPRS enabled mobile subscriber phones are required
- These phones are backward compatible with GSM

- Three types of GPRS Mobile phones
- **A) Class A** : support **simultaneous** GPRS services and GSM services such as voice and SMS. This support include **simultaneous** attach, activation, monitor and traffic.
- **B) Class B** : support either GSM or GPRS **at a time** (it can monitor channels of both GSM and GPRS). This support simultaneous attach, activation, monitor but **not simultaneous traffic.**
- **C) Class C:** supports only GPRS services. It supports only non-simultaneous attach.

Serving GPRS Support Node (SGSN)

- analogous to MSC (in GSM)
- deliver packets to the MSs within its service area.
- send queries to HLRs to obtain profile data of GPRS subscribers.
- detects new GPRS MSs, process its registration & keep record of their location.

Main Function :

- **to handle authentication,**
- **data compression,**
- **ciphering and**
- **mobility management .**

Gateway GPRS Support Node (GGSN)

- Mediator between GPRS backbone and external data networks.
- Saves current data for the SGSN address of the participant as well as their profile and data for authentication and invoice.
- **Main functions**
    - Interface to external data networks
    - Resembles to a data network router
    - Forwards end user data to right SGSN
    - **Routes mobile originated packets to right destination**
    - Filters end user traffic

Other elements

BG (Border Gateway): (Not defined within GPRS)

- Routes packets from SGSN/GGSN of one operator to a SGSN/GGSN of an other operator
- Provides protection against intruders from external networks

DNS (Domain Name Server)

- Translates addresses from ggsn1.oper1.fi -format to 123.45.67.89 format (i.e. as used in Internet)

Charging Gateway

- Collects charging information from SGSNs and GGSNs

PTM-SC (Point to Multipoint -Service Center)

- PTM Multicast (PTM-M): Downlink broadcast; no subscription; no ciphering

GPRS backbones

Enables communication between GPRS Support Nodes

Based on private IP network

- IPv6 is the ultimate protocol
- IPV4 can be used as an intermediate solution

Intra-PLMN backbone (The **PLMN** is the term used to describe all mobile wireless networks that use earth-based stations rather than satellites.)

- Connects GPRS Support Nodes of one operator
- Operator decides the network architecture
  - LAN, point-to-point links, ATM, ISDN, ...

Inter-PLMN backbone

- Connects GPRS operators via BGs (Border Gateways)

Mobility management

- Instead of Location Area, GPRS uses Routing Areas to group cells.
- RA is a subset of LA.
- Location management depends on **three mobile states**:

- **IDLE:** MS is **not known by the network** (SGSN) (not reachable)

- **STANDBY:** MS's location is **known in accuracy of Routing Area**

    - MS must inform its location after every Routing Area change (no need to inform if MS changes from one cell to another within same RA)

- **READY:** MS's location is **known in accuracy of cell (**the SGSN knows the cell location of the MS.)

    - MS must inform its location after every cell change

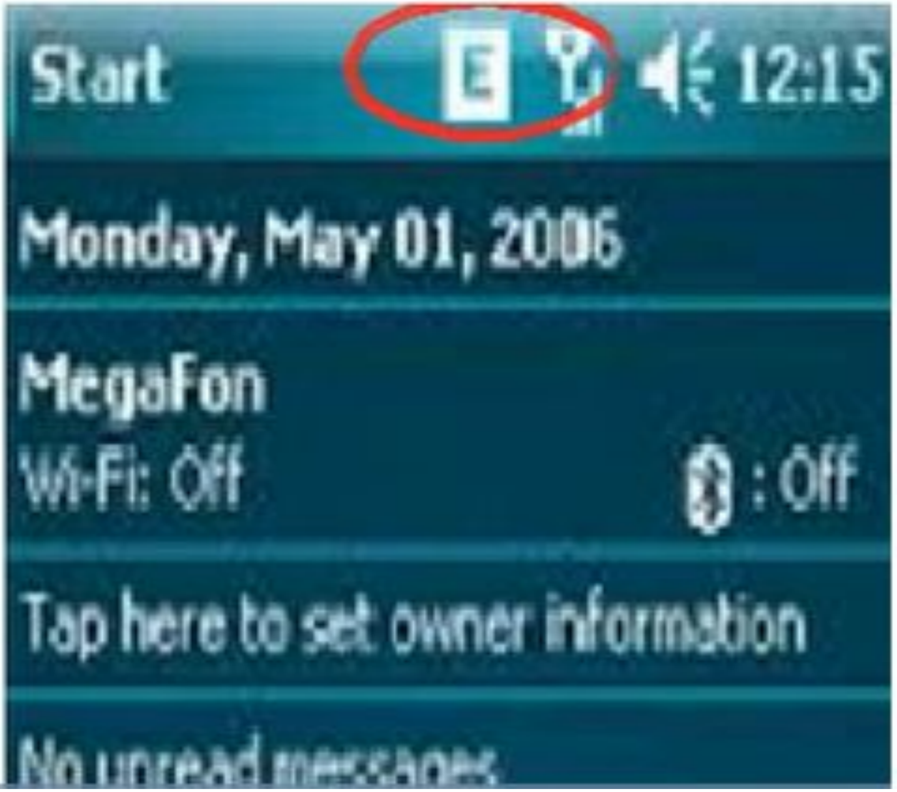
    - SGSN does not need to page the MS before data transfer

GPRS Services

- ✓ Typical GPRS applications include all **normal GSM services** but in **efficient and faster way**. It also supports services like e-mail and web browsing format language.
- ✓ It also supports new set of services such as **enhanced short messages**, **wireless imaging** with instant pictures, **video services**, document and information sharing.
- ✓ Benefits available for service providers include **efficient use of radio spectrum resources**, fast and flexible implementation with GSM coverage, low investment cost.
- ✓ The benefits offered to mobile data users include wide area coverage, **fast access time**, **higher speed**, high level security.

EDGE Technology

- It stands for Enhanced Data rates for GSM Evolution.
- EDGE is extended version of GPRS i.e. EGPRS.
- First launched in the United States in 2003 by Cingular, which is now AT&T.

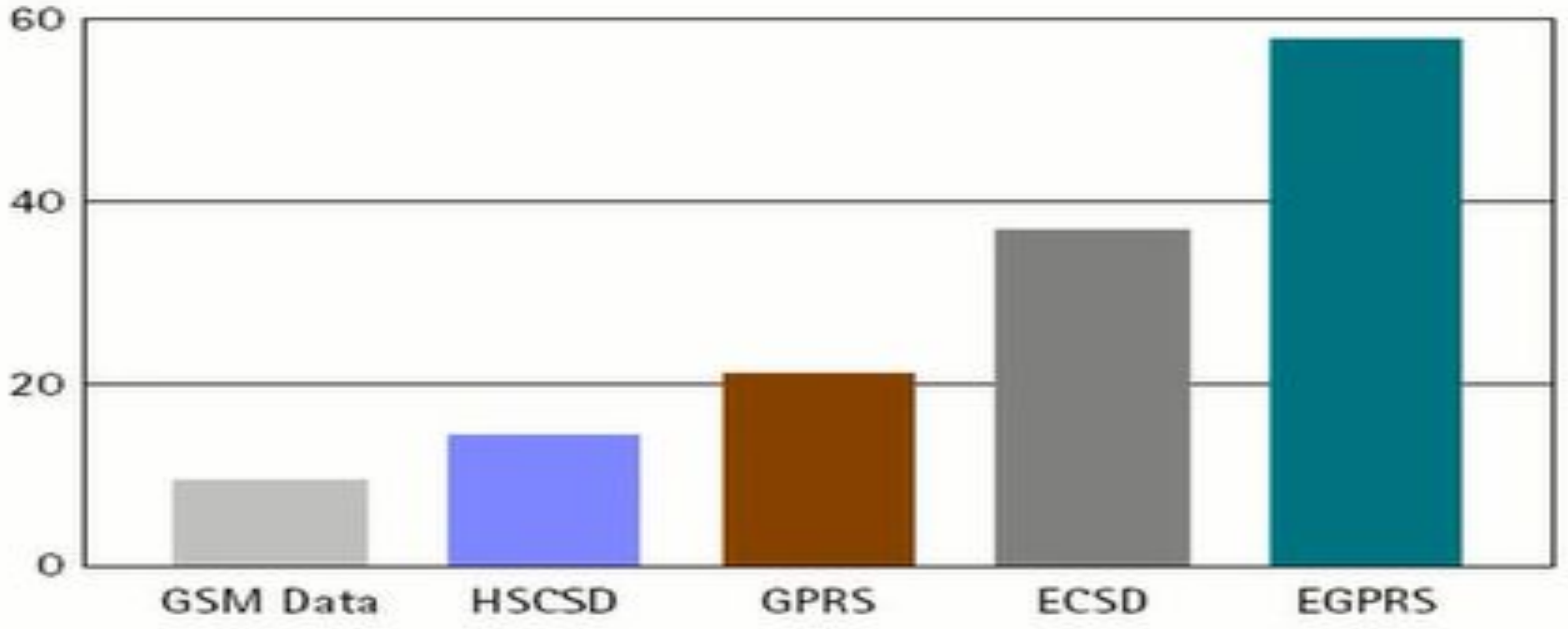


- EDGE is a new set of GSM-bearer services that provides packet mode transmission within the GSM network & interconnects with external packet data networks.
- Designed to deliver multimedia applications such as streaming television, audio and video to mobile phones at speeds up to 384 Kbps, theoretically up to 473.8 kbps.

Salient Features of EDGE

- Compliment to 3G.
- Standardized by ETSI.
- EDGE is deployed over GPRS network.
- Provides Data Packet delivery service.
- Support for leading internet communication protocols.
- Billing based on volume of data transferred.
- Utilizes existing GSM/GPRS authentication and privacy procedures.

Evolution of EDGE/EGPRS



Data rate evolution, throughput in kbit/s per single radio timeslot

GSM:
- 9.6-14.4 Kbps
- launched 1991 in Finland
- 900 m subs by 2003

GPRS (2001):
- 115 Kbps (1 user)
- 20-30 Kbps (avg)
- GMSK modulation
- >280m subs by 05

EDGE/EGPRS (2003):
- 384 Kbps (1 user)
- 100-130 Kbps (avg)
- 8PSK modulation
- >36m subs by 2005

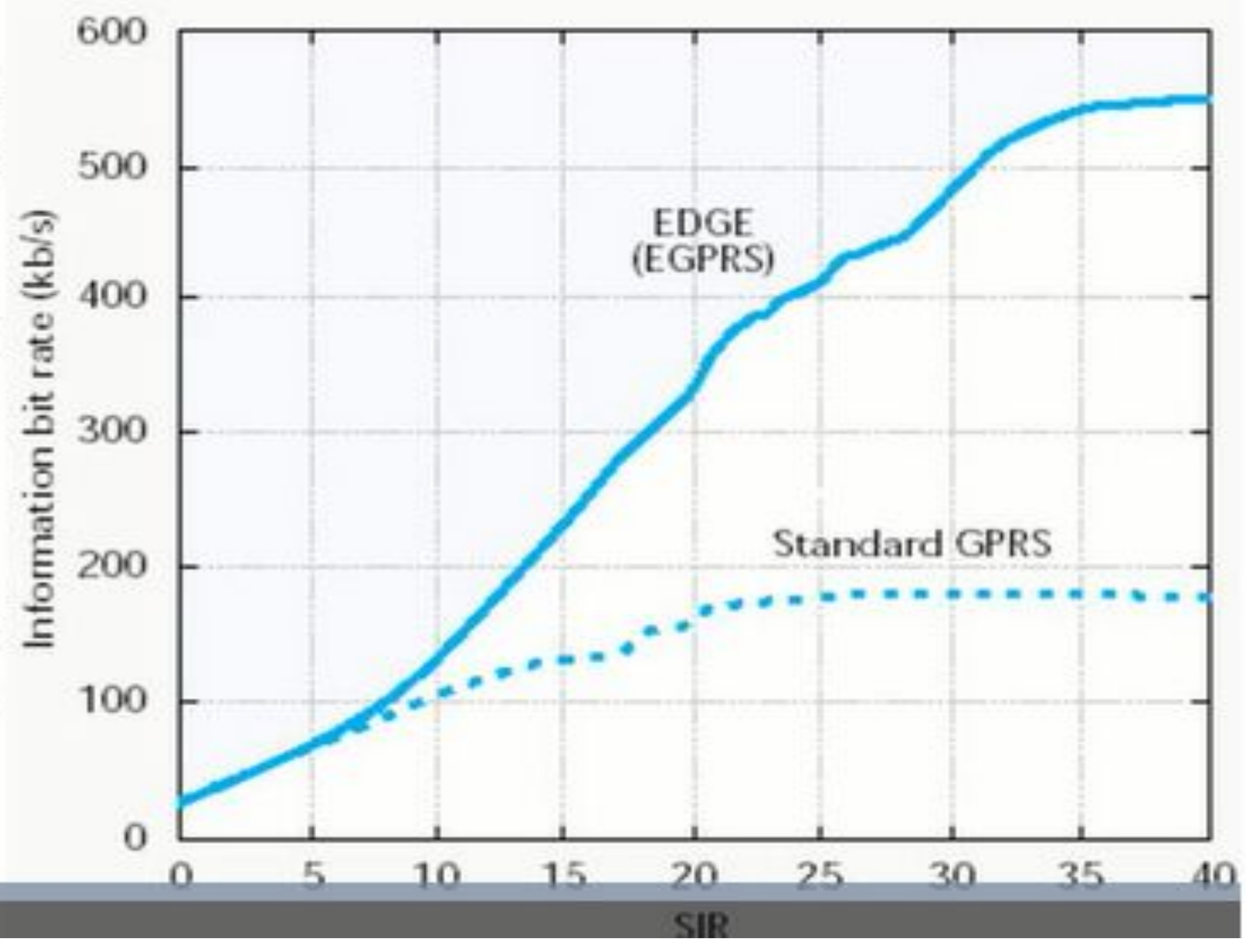
GPRS vs EDGE

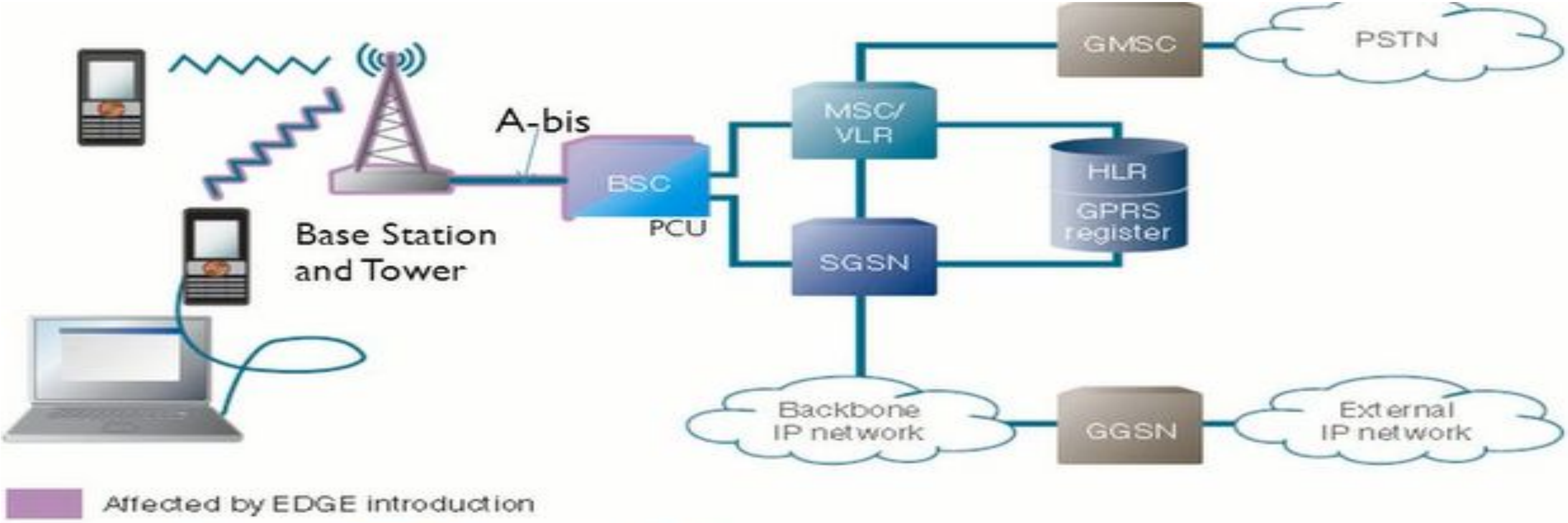
- EDGE only introduces a new modulation technique and new channel coding that can be used to transmit both packet-switched and circuit-switched voice and data services.
- EDGE is an add-on to GPRS and cannot work alone. And is therefore much easier to introduce than GPRS. GPRS has a greater impact on the GSM system than EDGE has.
- EDGE offers significantly higher throughput and capacity.
- EDGE can transmit three times as many bits as GPRS during the same period of time.
- GPRS can transfer data at rates of 115 kbps theoretically and up to 60 kbps on physical layer,
  whereas EDGE/EGRPS can transfer up to 473.6 kbps and 384 kbps respectively.

- With EDGE, the same time slot can support more users.
- GPRS and EDGE have different protocols and different behaviour on the base station system side.

•On the core network side, GPRS and EDGE share the same packet-handling protocols and, therefore, behave in the same way.

•GPRS and EDGE share the same symbol rate, but the modulation bit rate differs.





SGSN – Serving GPRS Support Node- takes care of routing, handover and IP address assignment and Performs security functions and access control.
GGSN – Gateway GPRS Support Node- gateway/anchor to external networks.
HLR – Home Location Register- database that contains subscriber information.
VLR – Visitor Location Register- mobile station's profiles are preserved in it.
PSTN – Public Switched Telephone Network
BSC – Base Station Controller
GMSC – Gateway Mobile Switching Centre
PCU – Packet Control Unit- Distinguishes data and voice

Modulation and Coding Schemes(MCS)

Modulation and Coding Scheme	Modulation	Bits per symbol	User Data Rate per Timeslot (kbps)	Coding Rate
MCS-1	GMSK	1	8.8	0.53
MCS-2	GMSK	1	11.2	0.66
MCS-3	GMSK	1	14.8	0.85
MCS-4	GMSK	1	17.6	1.00
MCS-5	8PSK	3	22.4	0.37
MCS-6	8PSK	3	29.6	0.49
MCS-7	8PSK	3	44.8	0.76
MCS-8	8PSK	3	54.4	0.92
MCS-9	8PSK	3	59.2	1.00

EDGE Technology

- **Base station:** Apart from the upgrade to incorporate the **8PSK** modulation capability, other small changes are required to the base station. These are normally **relatively small** and can often be accomplished by **software upgrades**.

- **Mobile stations:** It is necessary to have a GSM EDGE handset that is **EDGE compatible**. As it is **not possible to upgrade handsets**, this means that the user needs to buy **a new GSM EDGE handset**.

EDGE Technology

- **Upgrade to network architecture:** GSM EDGE provides the capability for IP based data transfer. As a result, additional network elements are required.
  - Gateway GPRS Service Node (GGSN)
  - Serving GPRS Service Node (SGSN)
  - Packet Control Unit (PCU)

EDGE Technology

GSM EDGE network architecture upgrades

- **Gateway GPRS Service Node (GGSN)** : The GGSN connects to packet-switched networks such as the Internet and other GPRS networks. It forms the gateway to the outside world.

- **Serving GPRS Service Node (SGSN):** The SGSN provides the packet-switched link to mobile stations. This forms a gateway to the services within the network.

- **Packet Control Unit(PCU):** which differentiates whether data is to be routed to the packet switched or circuit switched networks

EDGE Technology

SGSN (Serving GPRS Service Node): It provides a variety of services to the mobiles:

- Packet routing and transfer
- Mobility management
- Authentication
- Attach/detach
- Logical link management
- Charging data

There is a location register within the SGSN and this stores location information (e.g., current cell, current VLR). It also stores the user profiles (e.g., IMSI, packet addresses used) for all the GPRS users registered with the particular SGSN.

EDGE Technology

GGSN (Gateway GPRS Service Node)

 The GGSN organizes the inter-working between the GPRS / EDGE network and external packet switched networks to which the mobiles may be connected. These may include both Internet and X.25 networks.

 The GGSN can be considered to be a combination of a **gateway, router and firewall** as it hides the internal network to the outside.

 When the GGSN receives data addressed to a specific user, it checks if the user is active, then forwarding the data. In the opposite direction, packet data from the mobile is routed to the right destination network by the GGSN.

EDGE Technology

PCU (Packet Control Unit)

- It is a **hardware router** that is added to the BSC.

- It **differentiates data destined for** the standard **GSM** network (circuit switched data) and data destined for the **EDGE** network (Packet Switched Data).

- The PCU itself may be a separate physical entity, or more often these days it is incorporated into the base station controller, BSC, thereby saving additional hardware costs.

What EDGE Would Mean to Subscribers

- Streaming applications
- Very high speed downloads
- Corporate intranet connections
- Quicker MMS
- Video phone
- Vertical corporate applications - Video conference, Remote presentations.

GSM EDGE evolution specification overview

Parameter	Details
Multiple Access Technology	FDMA / TDMA
Duplex Technique	FDD
Channel Spacing	200 kHz
Modulation	GMSK, 8PSK
Slots per channel	8
Frame duration	4.615 ms
Latency	Below 100 ms
Overall symbol rate	270 k symbols / s
Overall modulation bit rate	810 kbps
Radio data rate per time slot	69.2 kbps
Max user data rate per time slot	59.2 kbps (MCS-9)
Max user data rate when using 8 time slots	473.6 kbps **

1G TO 5G

Comparison of 1G to 5G Technologies

Technology	1G	2G	3G	4G	5G
Deployment	1970/ 1984	1980/1999	1990/2002	2000/2010	2014/2015
Bandwidth	2kbps	14-64kbps	2mbps	200 mbps	>1 gbps
Technology	Analog cellular	Digital cellular	Broad Bandwidth / CDMA / ip technology	Unified IP & seamless combo of LAN/ WAN/ WLAN/ PAN	4G+ WWW
Service	Mobile telephony	Digital voice, short messaging	Integrated high-quality audio, video & data	Dynamic information access, variable devices	Dynamic information access, variable devices with AI capabilities
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit / circuit for access network & air interface	Packet except for air interface	All packet	All packet
Core network	PSTN	PSTN	Packet network	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal & vertical	Horizontal & vertical

Universal Mobile Terrestrial Telecommunication Systems (UMTS)

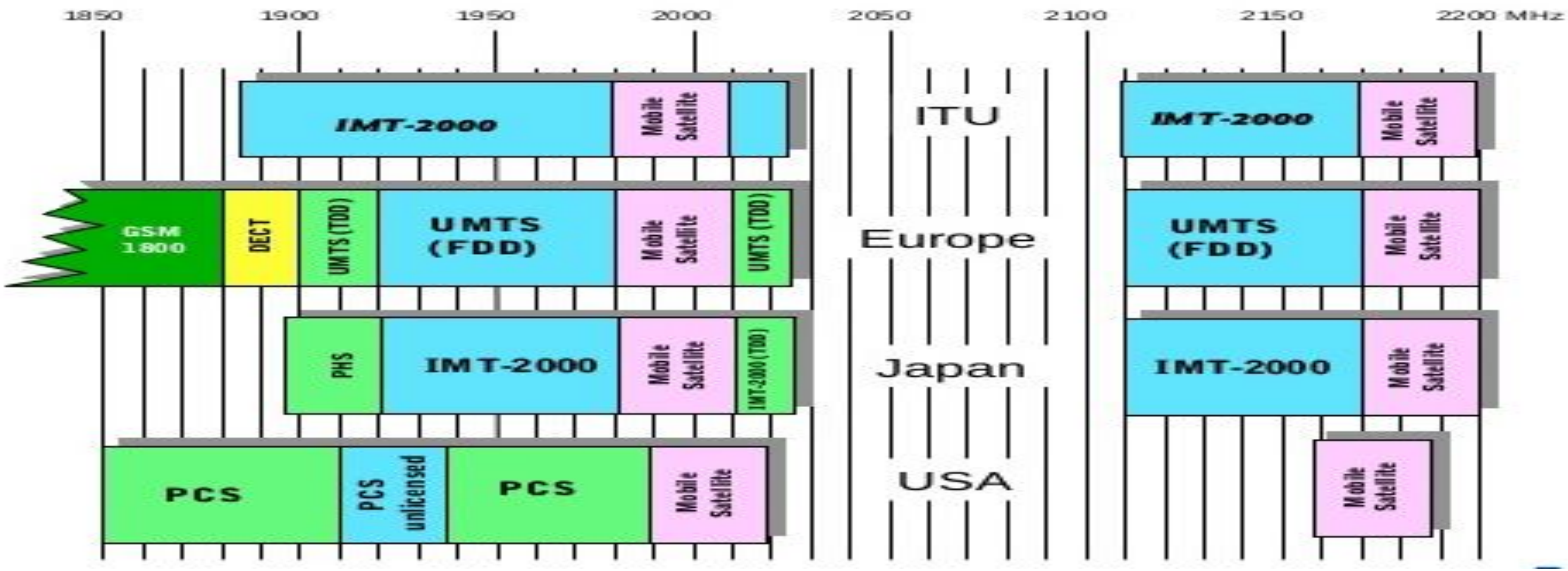
- Is the standard for delivering 3G services based on GSM.
- Global Wireless standard
- UMTS includes all aspects of the system, including
  - ✔ Physical layer
  - ✔ Network planning
  - ✔ Architecture & protocols
  - ✔ Services & applications

  - Objectives: to integrate all forms of mobile communication
- It provides up to **2Mbps** in local area &
  less than **1Mbps** in wide area access with full mobility

GSM/GPRS → UMTS

	Summary of Changes
New	WCDMA Air Interface (UE–Node B) RAN Interfaces Iub (Node B – RNC), Iur (RNC – RNC) CN Interface – Iu (MSC–RNC & SGSN–RNC)
Modification	MSC and SGSN for Iu Interface
No Changes	Circuit Core Network (HLR/AuC) Packet Core Network (GGSN)

Frequency Allocations for UMTS

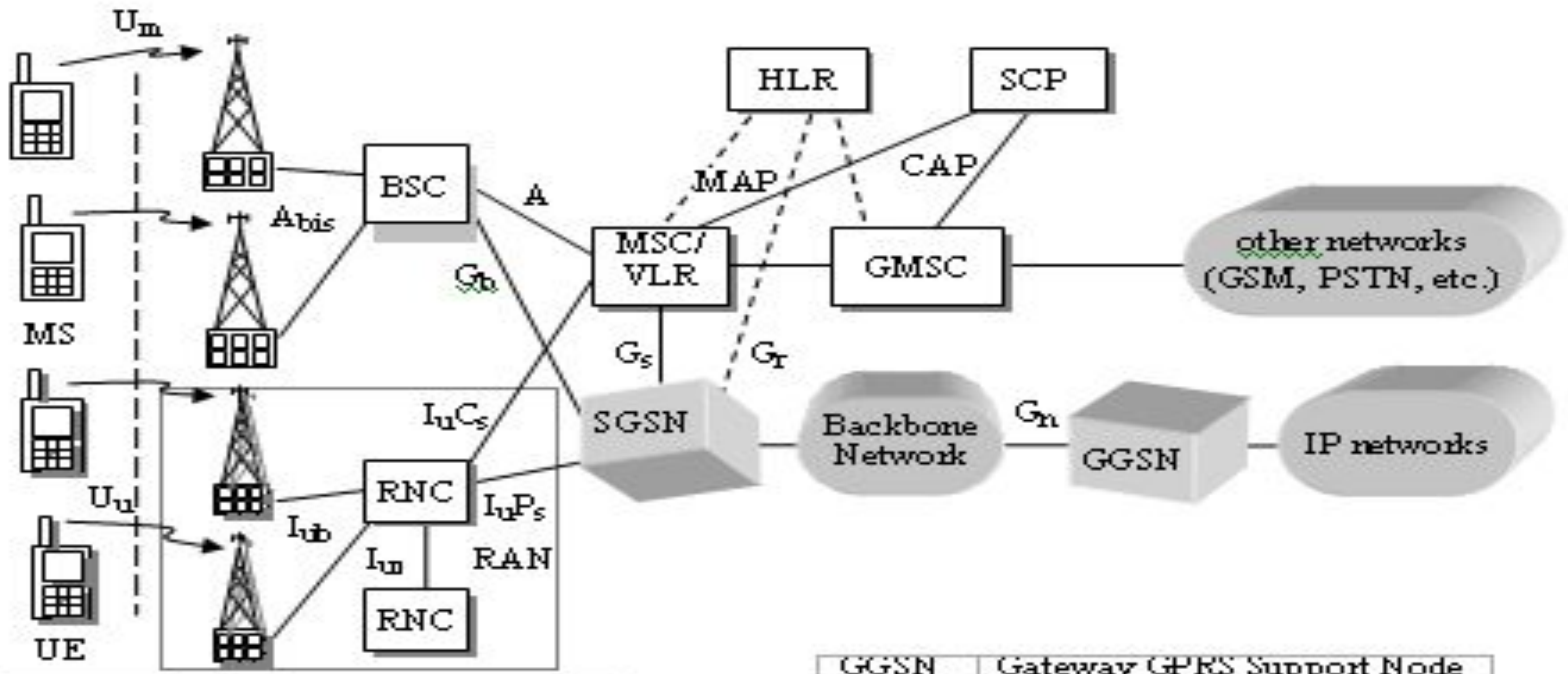


Frequency Bands Uplink: 1885 MHz-2035MHz &

Downlink : 2110 MHz-2200MHz

High frequency spectrum efficiency.

UMTS Network Architecture



MS/UE	2G/3G Mobile Station
RAN	Radio Access Network
CAP	CAMEL Application Part
GMSC	Gateway MSC

GGSN	Gateway GPRS Support Node
SGSN	Serving GPRS Support Node
BS/NB	2G/3G Base Station
RNC	Radio Network Controller
MAP	Mobile Application Part

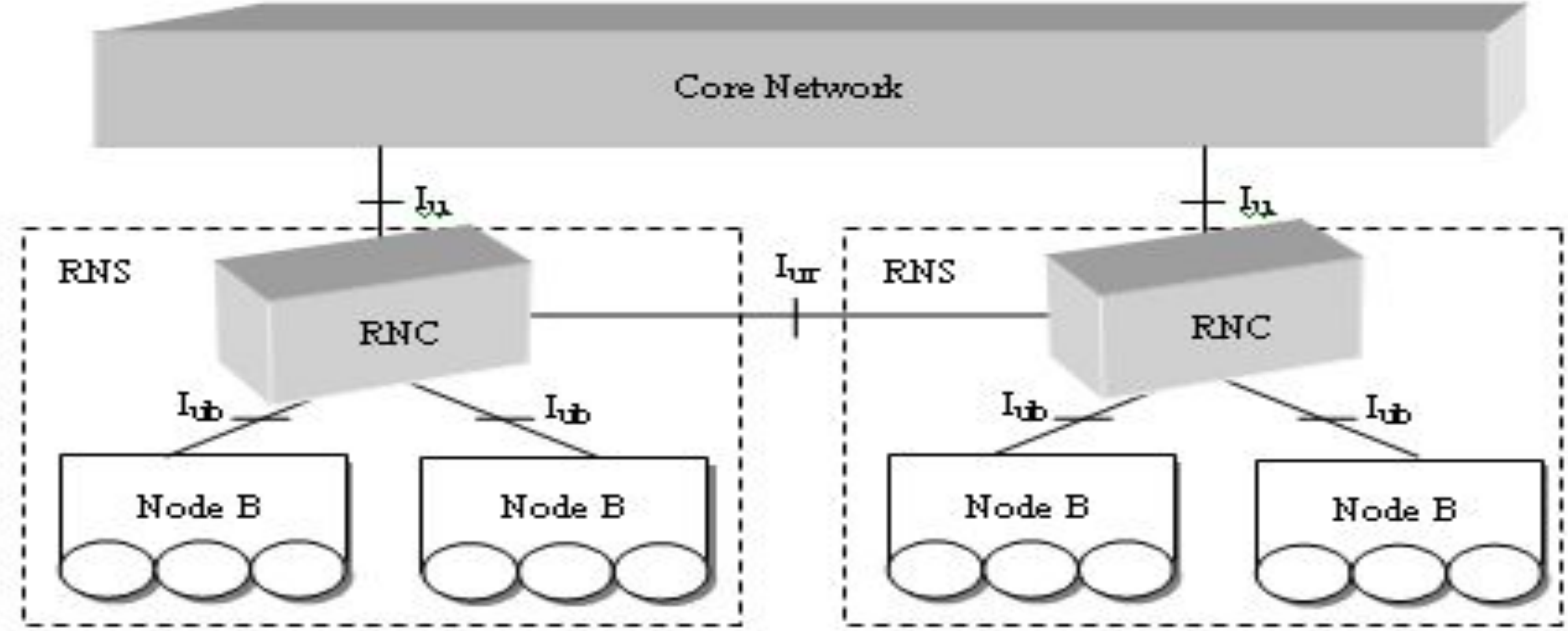
UMTS Network Architecture

- Partly based on 2G with some new components
- The MS of GSM=User Equipment (UE) in UMTS-additional functionality
- MSC has same function in GSM and UMTS
- **SGSN**: supports up to 2Mbps
- **Iu interface**: connects the core network element to radio network similar to 'A-interface' in GSM

- **Major changes:**

1. Radio Access Network (**RAN**) also called UMTS terrestrial RAN (UTRAN)
2. **Iur interface** : connects 2 neighboring Radio Network Controllers (RNCs)
3. **Iub interface** : connects BSs to RNC

UTRAN Architecture



RNS : Radio Network Subsystems , is responsible for Radio resources and transmission/reception in a set of cells.
Iub = RNC to BSs , Node B= BTS

UTRAN Architecture

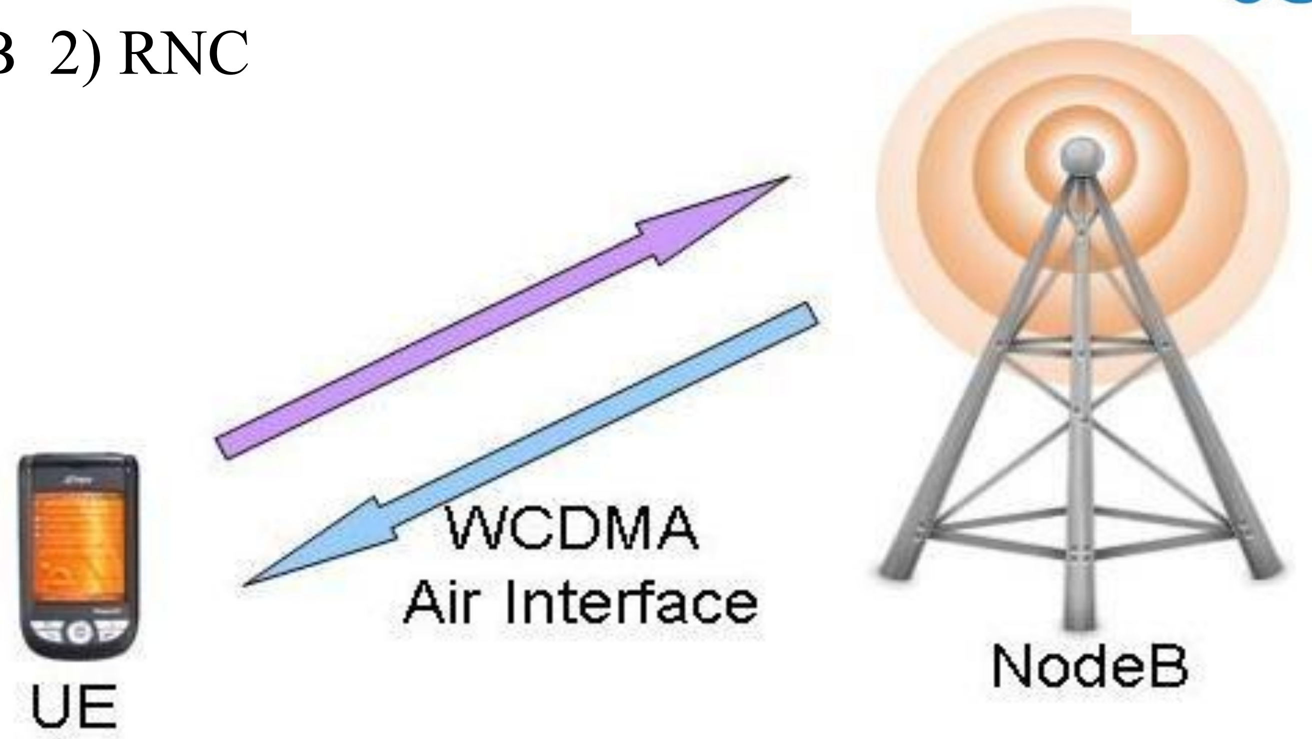
- RNS has main two elements : 1) Node B 2) RNC

1. Radio Network Controller (RNC):

Functions:

- Radio resource management
- Serving RNS relocation
- Frame synchronization
- Macro diversity combining
- Intra-UTRAN handoff
- Splitting of the I_{ub} data streams
- Outer loop power control
- RLC sublayers function execution

- Functions equivalent to BSC in GSM
- RNCs can manage handovers without using MSC and SGSN



2. Node B

- equivalent to BTS
- physically co-located with GSM BTS to reduce the cost

UMTS interfaces

1.Uu –between UE and network, air interface ‘*Um*’ In GSM

2. **Iu**-*CS*-circuit switched connection for carrying voice traffic and signaling between the UTRAN and core network

‘A’ interface in GSM

3. **Iub**- used by RNC to control multiple Node Bs

‘A-bis’ interface in GSM/GPRS

4. **Iu**-PS packet switched connection for data traffic and signaling between the UTRAN and core data GPRS network,

Gb inteface in GSM/GPRS

5. **Iur**-*to* support inter MSC mobility.

When a mobile user moves between areas served by diff RNCs mobile subscriber data is transferred to new RNC via Iur.

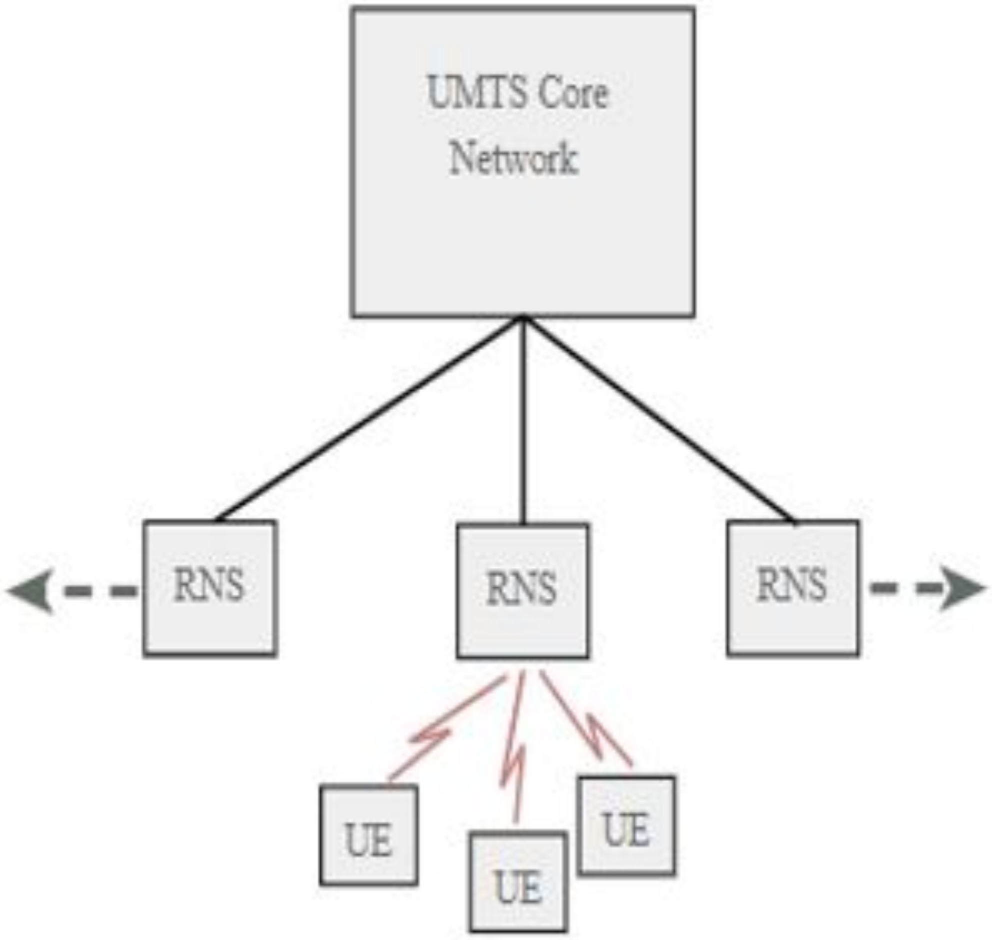
original RNC-serving RNC new RNC-drift RNC

UMTS Air Interface Specifications

S. No.	Parameter	Specification
1.	Frequency Spectrum	Uplink: 1920 MHz – 1980 MHz; Downlink: 2110 MHz – 2170 MHz
2.	Channel Bandwidth	5 MHz
3.	Chip Rate	3.84 Mcps
4.	Duplexing Technique	FDD and TDD modes
5.	Modulation Scheme	Direct Sequence CDMA with QPSK
5.	Frame Length	10 ms frame with 15 time slots
6.	Coding Technique	Orthogonal Variable Spreading Factor (OVSF)
7.	Service Type	Multi-rate and multi-service

WCDMA – is radio interface technology in UMTS network, **CH BW**-5 MHz
The UMTS air interface is based on **DS-CDMA** (direct sequence CDMA)
Spreading Factor – ration of chip rate to data rate

UMTS



The main UMTS network blocks

- User Equipment: new name - considerably greater functionality that the UE could have. It could also be anything between a mobile phone to a data terminal attached to a computer with no voice capability.

UE RF circuitry, Baseband processing, Battery, USIM

- 3G UMTS Radio Network Subsystem- UMTS Radio access network-UTRAN: interfaces to both the UE and the core network.

- 3G UMTS Core Network: Additional functionality –split in to two different areas: 1) circuit switched elements and 2) packet switched elements

Circuit switched elements:

primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.

- It is used to provide voice and CS data services.
- It contains Mobile Switching Center (MSC) and Gateway MSC(GMSC) as functional entities.

Packet switched elements:

to carry packet data.

 It is used to provide packet based services.

It contains Serving GPRS support node (SGSN),

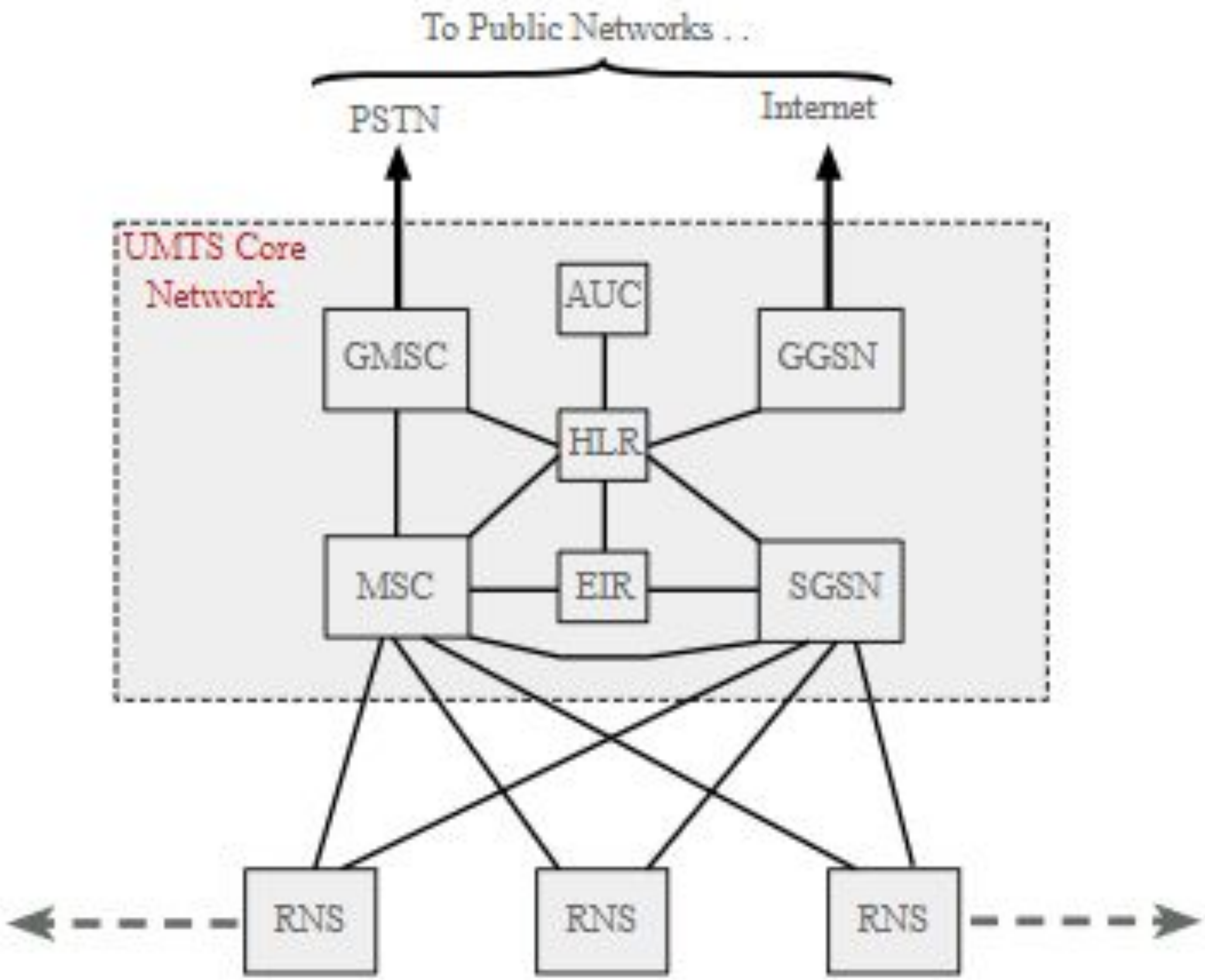
- Gateway GPRS support node (GGSN),
- Domain Name Server (DNS),
- Dynamic Host Configuration Protocol (DHCP) server,
- packet charging gateway, and firewalls.

The core network can be split into the following different functional areas:

- Functional entities needed to support PS services (e.g.3G-SGSN, 3G- GGSN)
- Functional entities needed to support CS services (e.g. 3G-MSC/VLR)
- Functional entities common to both types of services (e.g. 3G-HLR)

Other areas that can be considered part of the core network include:

- Network management systems (billing and provisioning, service management, element management, etc.)
- IN system (service control point (SCP), service signaling point (SSP), etc.)
- ATM/SDH/IP switch/transport infrastructure.
- Some network elements: associated with registration are shared by both domains and operate in the same way that they did with GSM.



UMTS Network Architecture Overview

Circuit switched elements

Mobile switching centre (MSC): This was essentially the same as that within GSM, and it managed the circuit switched calls under way.

Gateway MSC (GMSC): This was effectively the interface to the external networks.

Packet switched elements

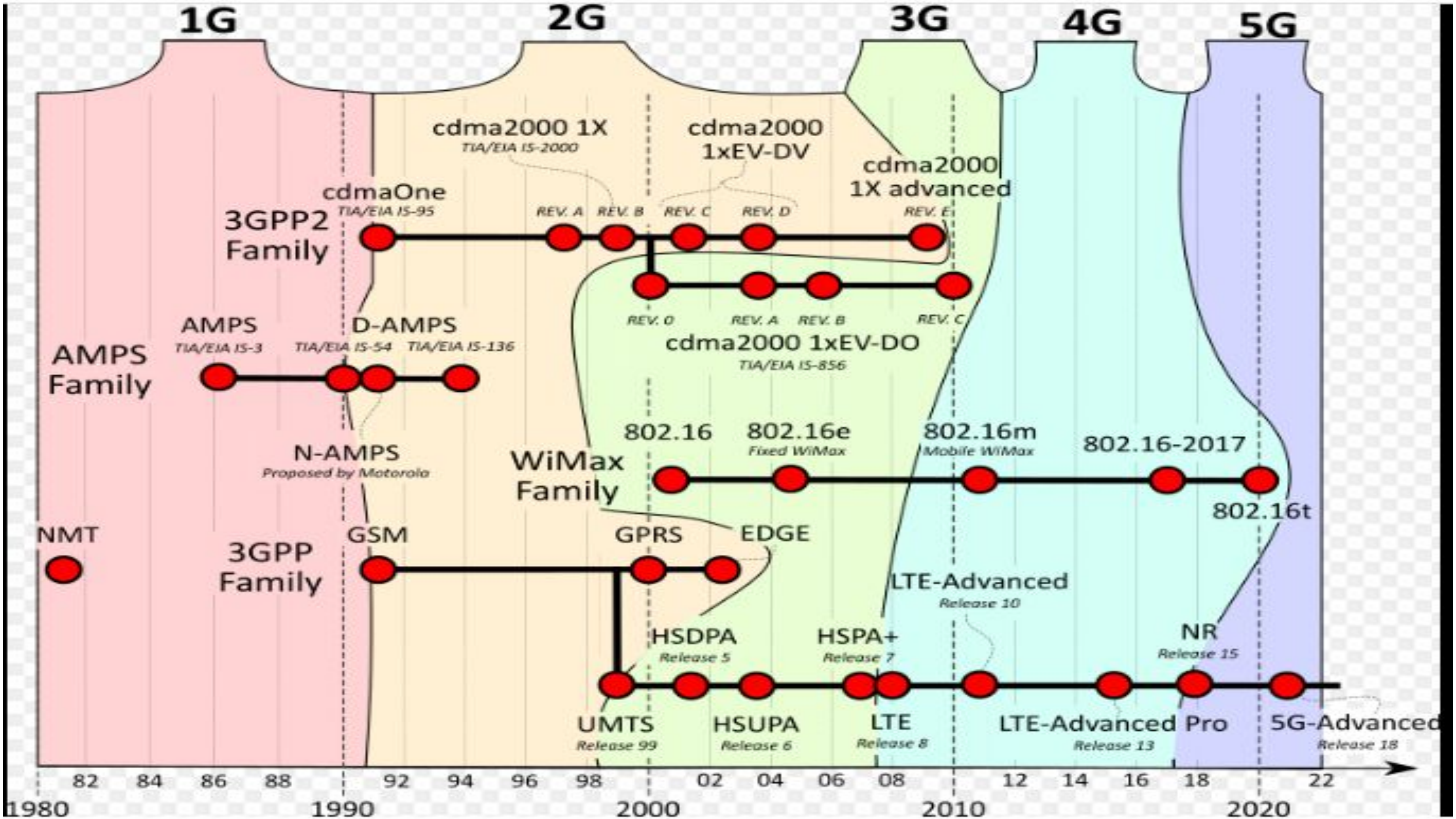
- ***Serving GPRS Support Node (SGSN):***
- The SGSN provided a number of functions within the UMTS network architecture.
  - Mobility management When a UE attached to the Packet Switched domain of the UMTS Core Network, the SGSN generates MM information based on the mobile's current location.
  - Session management: The SGSN managed the data sessions providing the required quality of service and it also managed what were termed the PDP (Packet data Protocol) contexts, i.e. the pipes over which the data was sent.
  - Interaction with other areas of the network: The SGSN was able to manage its elements within the network only by communicating with other areas of the network, e.g. MSC and other circuit switched areas.
  - Billing: The SGSN was also responsible billing. It achieved this by monitoring the flow of user data across the GPRS network. CDRs (Call Detail Records) were generated by the SGSN before being transferred to the charging entities (Charging Gateway Function, CGF).

- ***Gateway GPRS Support Node (GGSN):***

GGSN was the central element within the UMTS packet switched network.

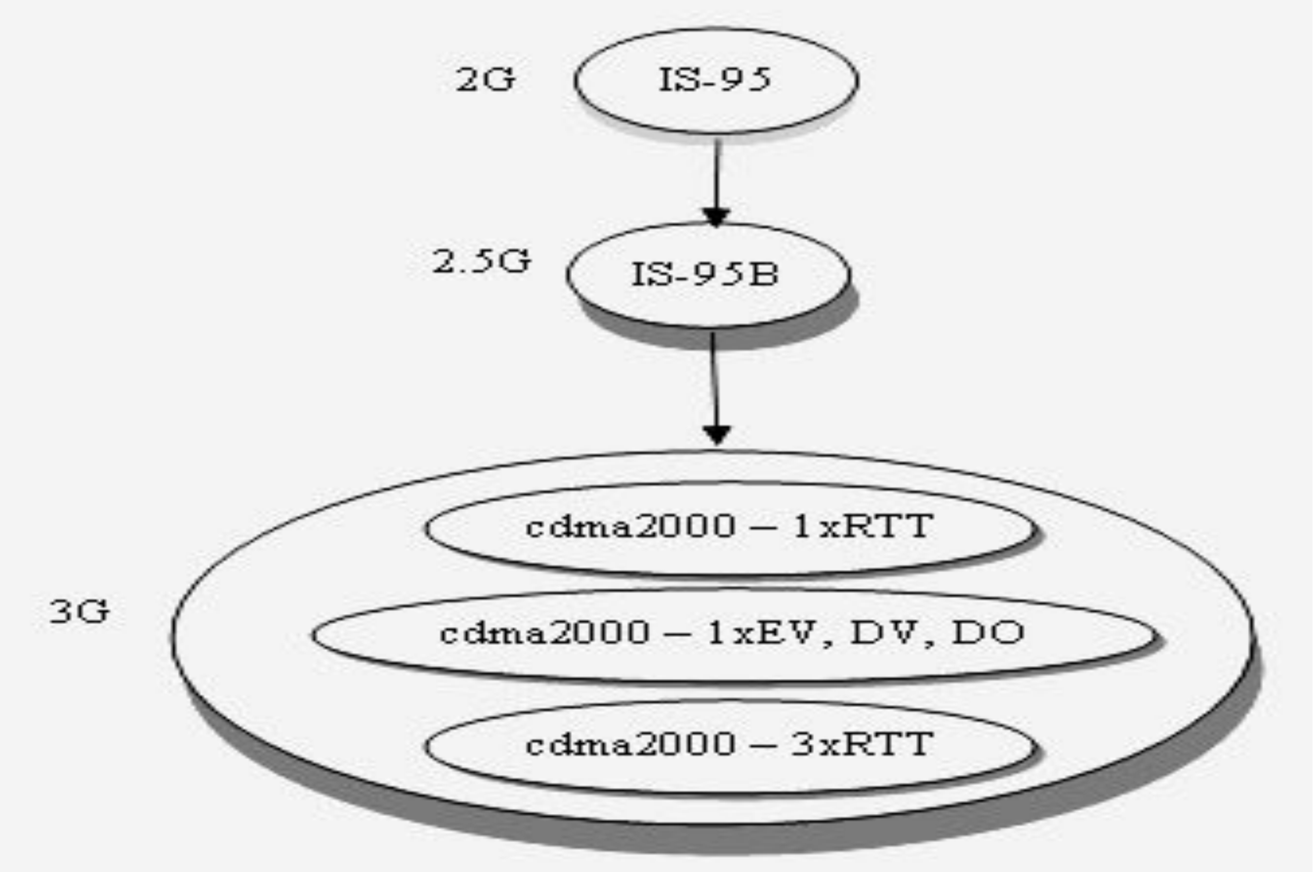
It handled inter-working between the UMTS packet switched network and external packet switched networks, and could be considered as a very sophisticated router.

In operation, when the GGSN received data addressed to a specific user, it checked if the user was active and then forwarded the data to the SGSN serving the particular UE.



1G
2G
3G
4G
5G
cdma2000 1X
TIA/EIA IS-2000
cdma2000
1xEV-DV
cdma2000
1X advanced
cdmaOne
TIA/EIA IS-95
REV. A
REV. B
REV. C
REV. D
REV. E
3GPP2
Family
REV. 0
REV. A
REV. B
REV. C
cdma2000 1xEV-DO
TIA/EIA IS-856
AMPS
TIA/EIA IS-3
D-AMPS
TIA/EIA IS-54
TIA/EIA IS-136
AMPS
Family
N-AMPS
Proposed by Motorola
802.16
802.16e
Fixed WiMax
802.16m
Mobile WiMax
802.16-2017
802.16t
WiMax
Family
NMT
GSM
3GPP
Family
GPRS
EDGE
LTE-Advanced
Release 10
HSDPA
Release 5
HSPA+
Release 7
NR
Release 15
UMTS
Release 99
HSUPA
Release 6
LTE
Release 8
LTE-Advanced Pro
Release 13
5G-Advanced
Release 18
82
84
86
88
92
94
96
98
02
04
06
08
12
14
16
18
22
1980
1990
2000
2010
2020

CDMA2000 Cellular Technology



Cdma 2000-1xMC (Multi-carrier)

3G CDMA Evolution Path

RTT: Radio transmission Technology

EV: Evolutionary advancement, DV: data & voice DO: Data only

INTERIM STANDARD 95 (IS-95)

- **Interim Standard 95 (IS-95)** was the first ever CDMA-based digital cellular technology. It was developed by Qualcomm and later adopted as a standard TIA/EIA/IS-95 release published in 1995.
- Also known as IS-95A.The proprietary name for IS-95 is **cdmaOne**.
- It is a 2G mobile telecommunications standard that uses CDMA.
- In 1999, IS-95B added a 64 Kbps packet capability, enabling data to be transmitted to a CDMA cell phone.

IS-95 → cdma2000

	Summary of Changes
New	Packet Core Network (PDSN, AAA, HA/FA) New Interface (R-P) – BS - PDSN
Modification	Air Interface (MS – BS) Network Interface (BS – MSC)
No Changes	Core Network Nodes (HLR, AC)

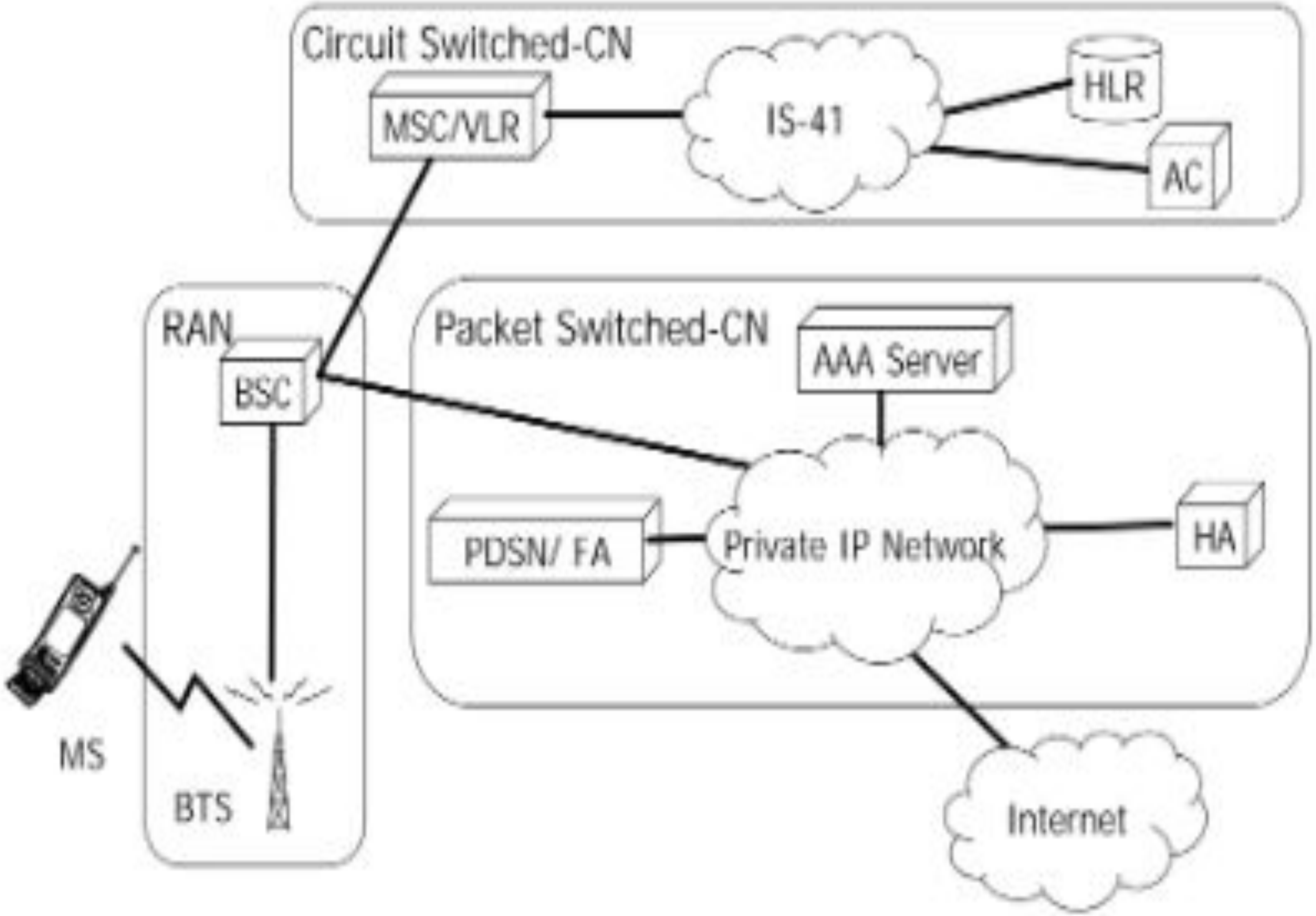
Cdma2000 Technical Specifications

Frequency band	Any existing band
Minimum frequency band required	1X: 2 x 1.25MHz; 3X: 2 x 3.75 MHz
Chip rate	1X: 1.2288 Mcps; 3X: 3.6864 Mcps
Maximum user data rate	1X: 144 kbps - 307 kbps;
	1X EV-DO: 384 kbps - 2.4 Mbps;
	1X EV-DV: 4.8 Mbps
Frame length	5ms, 10ms or 20ms
Power control rate	800 Hz
Spreading factors	4 ... 256 Uplink

Key Features of CDMA2000

- ❖ Leading performance in terms of data-speeds, voice capacity and latencies
- ❖ Efficient use of spectrum
- ❖ Support for advanced mobile services
- ❖ Compatible with IP
- ❖ Broadest selection of mobile devices
- ❖ Seamless evolution path
- ❖ Flexibility

cdma2000 Network Architecture



- AAA: Authentication, Authorization and Accounting
- FA: Foreign Agent
- GR: Gateway Router
- HA: Home Agent
- PDSN: Packet Data Serving Node

AAA Services cdma2000 networks

- AAA Services of Cdma2000 Networks
  - Migrate from a "one size fits all" model to personalized services
  - Package premium services for both residential and corporate users
  - Collect detailed usage information for flexible billing options
  - Track resource usage in real time for guaranteed access and access control.

- AAA consists of three key functions:
  - Authentication – recognize the user
  - Authorization – enforce access controls and deliver services
  - Accounting – track users' usage of network resources

Air Interface Parameters (1)

	UMTS	cdma2000
Spreading rate	3.84 Mcps	1.2288 Mcps
Bandwidth	5 MHz	1.25 MHz
Synchronization between cell sites	Asynchronous	Synchronous
Configuration	Direct spread configuration	Direct spread (1x) Multi-carrier (3x forward link)
Channel coding	Convolutional Turbo (Parameters flexible)	Convolutional Turbo (Parameters fixed in the standard)

Air Interface Parameters (2)

	UMTS	cdma2000
Modulation	QPSK in both directions	QPSK in forward BPSK in reverse
Frame size	10 msec for physical layer 10,20,40 and 80 msec for transport layer	5 (for signaling), 20, 40 and 80 msec physical layer frames
Modes	FDD and TDD Mode	Only FDD Mode
Transmit Diversity schemes	Time Switched Transmit Diversity Space Time Block Coded Transmit Diversity	Orthogonal Transmit Diversity Space Time Spreading

CDMA TECHNOLOGY

cdmaOne

Advantages of CDMA Cellular System

- **Frequency diversity** -frequency dependent transmission impairments have less effect on signal
- **Multipath resistance** -chipping codes used for CDMA exhibit low cross correlation and low autocorrelation
- **Privacy** -privacy is inherent since spread spectrum is obtained by use of noise-like signals
- **Gradual degradation** -system only gradually degrades as more users access the system
- CDMA uses larger bandwidth but utilizing resulting processing gain to enhance capacity.
- Efficient practical utilization of the fixed frequency spectrum
- Flexible allocation of resources-larger numbers of phones can be served by smaller numbers of cell-sites
- CDMA superior over TDMA in terms of capacity ,cost and speech quality.

CDMA TECHNOLOGY

Drawbacks of CDMA Cellular

- **Self-jamming** – arriving transmissions from multiple users not aligned on chip boundaries unless users are perfectly synchronized
- **Near-far problem** – signals closer to the receiver are received with less attenuation than signals farther away
- **Soft handoff** – requires that the mobile acquires the new cell before it relinquishes the old; this is more complex than hard handoff used in FDMA and TDMA schemes
- Air-interface is the most complex
- Not symmetrical (unlike TDMA):Forward and reverse channels are different. Forward channel uses orthogonal spreading codes. Reverse channel transmissions are not synchronized

3GPP LONG TERM EVOLUTION(LTE)

Introduction

- In Nov. 2004, 3GPP (3rd Generation Partnership Project) began a project to define the Long-Term Evolution (LTE) of Universal Mobile Telecommunications System (UMTS) cellular technology.
- LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standards.
- The goal of LTE was to **increase the capacity and speed** of wireless data networks using new DSP (digital signal processing) techniques and modulations.
- A further goal was the **redesign and simplification of the network architecture to an IP-based system with significantly reduced transfer latency** compared to the 3G architecture.

Why cellular industry wants to move to new standard ?

(i) **Need for improved data rates and spectral efficiency** in particular in dense urban environments,

(ii) For some operators, the possibility to **“leapfrog” from 2G directly to 4G technology,**

(iii) The competition from **WiMAX**

(iv) The possibility of **acquiring new spectrum** in the name of getting it for a new system.

Goals of LTE

Category	Goal	communication
Peak Data Rate	100 Mbit/s	downlink
	50 Mbit/s	Uplink
spectrum allocation	20-MHz	Downlink
	20-MHz	Uplink
spectral efficiency	5 bit/s/Hz	downlink
	2.5 bit/s/Hz	Uplink

Goals of LTE

LTE defines a number of **different types of Mobile Stations** (MSs) that present a tradeoff between complexity and performance

Table 27.1 Performance requirements for different MS classes

Category	1	2	3	4	5
Peak data rate DL (Mbit/s)	10	50	100	150	300
Max DL modulation	64 QAM	64 QAM	64 QAM	64 QAM	64 QAM
Peak data rate UL (Mbit/s)	5	25	50	50	75
Max UL modulation	16 QAM	16 QAM	16 QAM	16 QAM	64 QAM
Max number of layers for DL MIMO	1	2	2	2	4

Goals of LTE

For latency, the goals distinguish between

1. **Control-plane latency** is defined as the time for a handset to transition from various nonactive states to active states, which are **between 50 and 100 ms**, depending on the state in which the MS originally was. At least 400 active MSs per cell should be supported.

2. **User-plane latency** is defined as the time it takes to transmit a small Internet Protocol (IP) packet to the edge node of the Radio Access Network, RAN, which **should not exceed 5ms** in a network with a single MS (i.e., no congestion problems).

Goals of LTE

Generally, **user throughput** should improve 2–4 times compared to previous technology.

The system is intended to be optimized for:

- ✔ **Low speeds (0–15 km/h),** since the **main usage**, especially for data services.
- ✔ **Slight performance degeneration** is allowed for **speeds up to 120 km/h**,
- ✔ Truly **high-speed applications (up to 500 km/h),** only **basic connectivity** needs to be retained.

Goals of LTE

- The **transition from WCDMA/HSPA**(High Speed Packet Access) (including legacy Global System for Mobile communication (GSM) systems) **to LTE** should be made as **seamless** as possible.
- Transitions from one system to another will be frequently required, especially during the initial rollout of LTE, when only parts of the country will be covered by LTE Base Stations (BSs).
- **Transition times for real-time applications should be less than 300 ms, and for non real-time applications should be 500 ms**

Frequency Bands and Spectrum Flexibility

- LTE can be operated in a **variety of frequency bands**
- This spectrum can be used for any member of the IMT-2000 and IMT-Advanced family.

Bands	Frequencies/application	Used by country
3, 8	Migration from GSM to LTE	Europe
2, 4, 10	PCS frequencies	USA
5	Lower frequency operation	USA
6. 9	Traditional Japanese operator	Japan
12, 13, 14, 17	Auctioned off	USA

Table 27.2 Bands for FDD operation of LTE

Operating band	UL (MHz)	DL (MHz)	Bandwidth 1.4	3	5	10	15	20	
1	1920–1980	2110–2170			✓	✓	✓	✓	Europe, Asia
2	1850–1910	1930–1990	✓	✓	✓	✓	✓	✓	America
3	1710–1785	1805–1880	✓	✓	✓	✓	✓	✓	Europe, Asia
4	1710–1755	2110–2155	✓	✓	✓	✓	✓	✓	America
5	824–849	869–894	✓	✓	✓	✓			America
6	830–840	875–885			✓	✓			Japan
7	2500–2570	2620–2690			✓	✓	✓	✓	Europe, Asia
8	880–915	925–960	✓	✓	✓	✓			Europe, Asia
9	1750–1785	1845–1880			✓	✓	✓	✓	Japan
10	1710–1770	2110–2170			✓	✓	✓	✓	Americas
11	1428–1453	1476–1501			✓	✓	✓	✓	Japan
12	698–716	728–746	✓	✓	✓	✓			Americas
13	777–787	746–756	✓	✓	✓	✓			Americas
14	788–798	758–768	✓	✓	✓	✓			Americas
17	704–716	734–746	✓	✓	✓	✓			Americas

Table 27.3 Bands for TDD operation of LTE

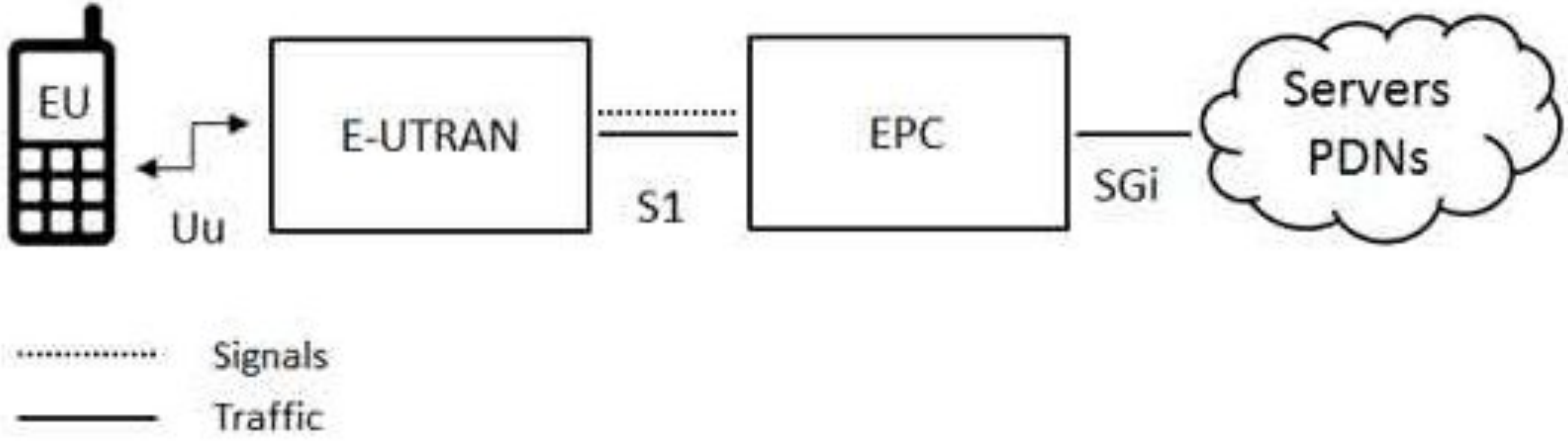
Operating band	Band	Bandwidth						
		1.4	3	5	10	15	20	
33	1900–1920			✓	✓	✓	✓	Europe, Asia
34	2010–2025			✓	✓	✓		Europe, Asia
35	1850–1910	✓	✓	✓	✓	✓	✓	
36	1930–1990	✓	✓	✓	✓	✓	✓	
37	1910–1930			✓	✓	✓	✓	
38	2570–2620			✓	✓			Europe
39	1880–1920			✓	✓	✓	✓	China
40	2300–2400				✓	✓	✓	Europe, Asia

LTE Architecture

The high-level network architecture of LTE is comprised of following three main components:

- The User Equipment (UE).
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
- The Evolved Packet Core (EPC).

The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below:



The User Equipment (UE)

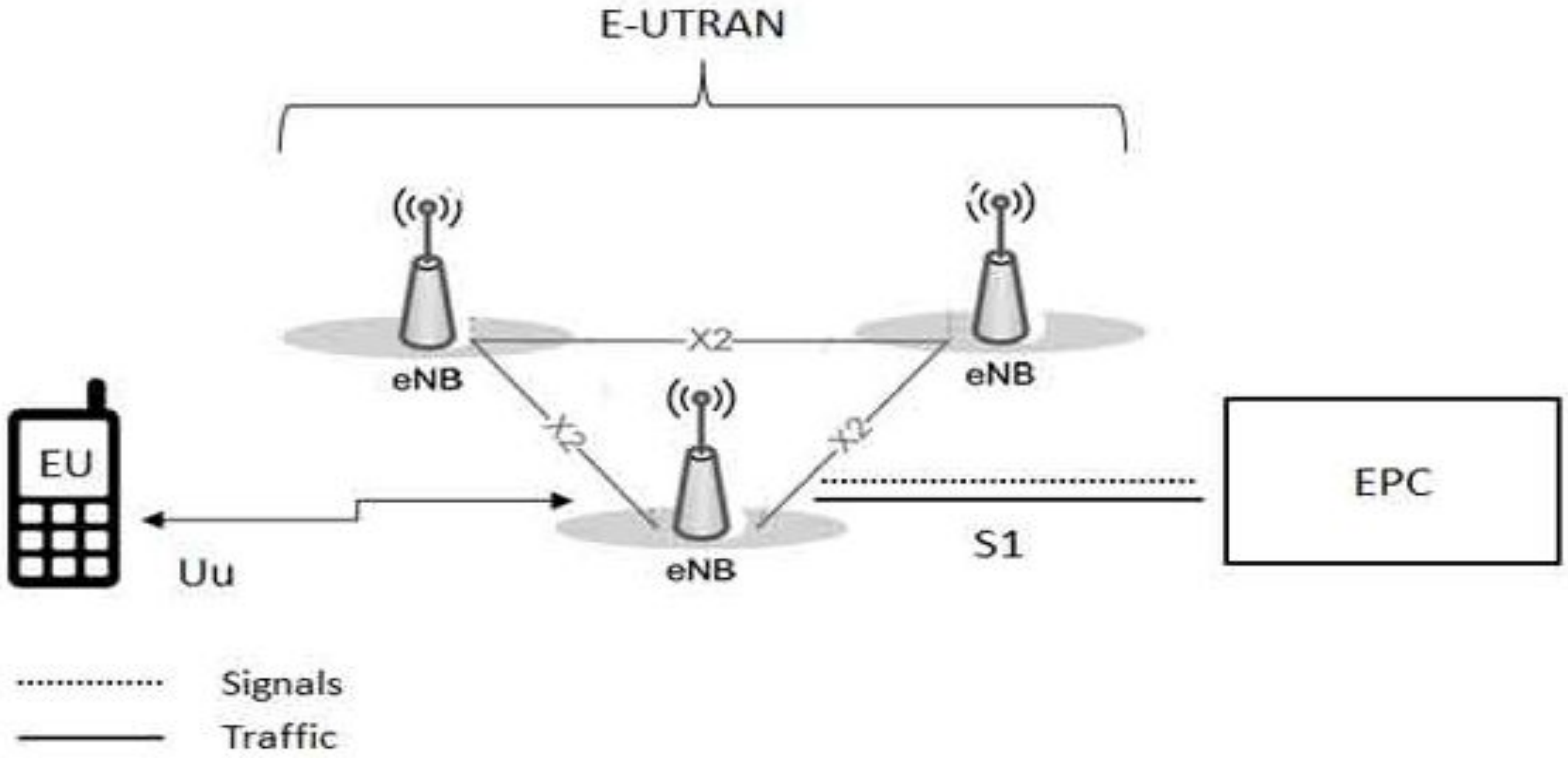
The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment (ME). The mobile equipment comprised of the following important modules:

- **Mobile Termination (MT)** : This handles all the communication functions.
- **Terminal Equipment (TE)** : This terminates the data streams.
- **Universal Integrated Circuit Card (UICC)** : This is also known as the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module (USIM).

A **USIM** stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

The E-UTRAN (The access network)

The architecture of evolved UMTS Terrestrial Radio Access Network (E-UTRAN) has been illustrated below.



The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called **eNodeB** or **eNB**. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

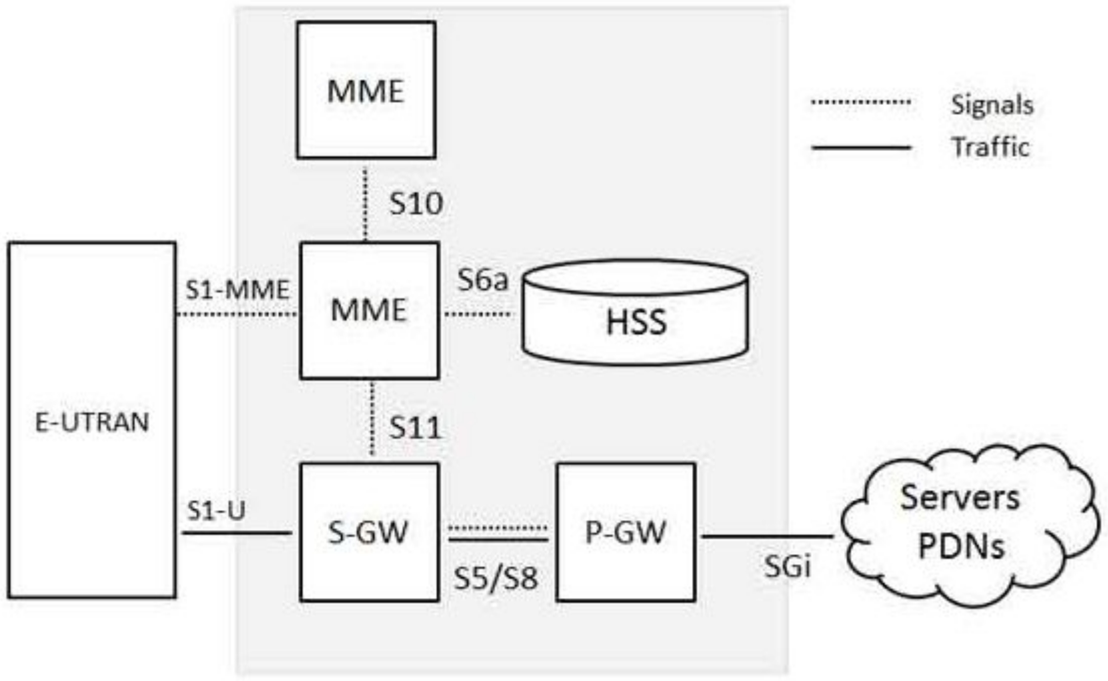
LTE Mobile communicates with just one base station and one cell at a time and there are following two main functions supported by eNB:

- The eBN sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
- The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

- Each eBN connects with the EPC by means of the S1 interface and it can also be connected to nearby base stations by the X2 interface, which is mainly used for signalling and packet forwarding during handover.
- A home eNB (HeNB) is a base station that has been purchased by a user to provide femtocell coverage within the home.
- A home eNB belongs to a closed subscriber group (CSG) and can only be accessed by mobiles with a USIM that also belongs to the closed subscriber group.

The Evolved Packet Core (EPC) (The core network)

- There are few more components which have not been shown in the diagram to keep it simple. These components are like the Earthquake and Tsunami Warning System (ETWS), the Equipment Identity Register (EIR) and Policy Control and Charging Rules Function (PCRF).



2G/3G Versus LTE

Following table compares various important Network Elements & Signaling protocols used in 2G/3G abd LTE.

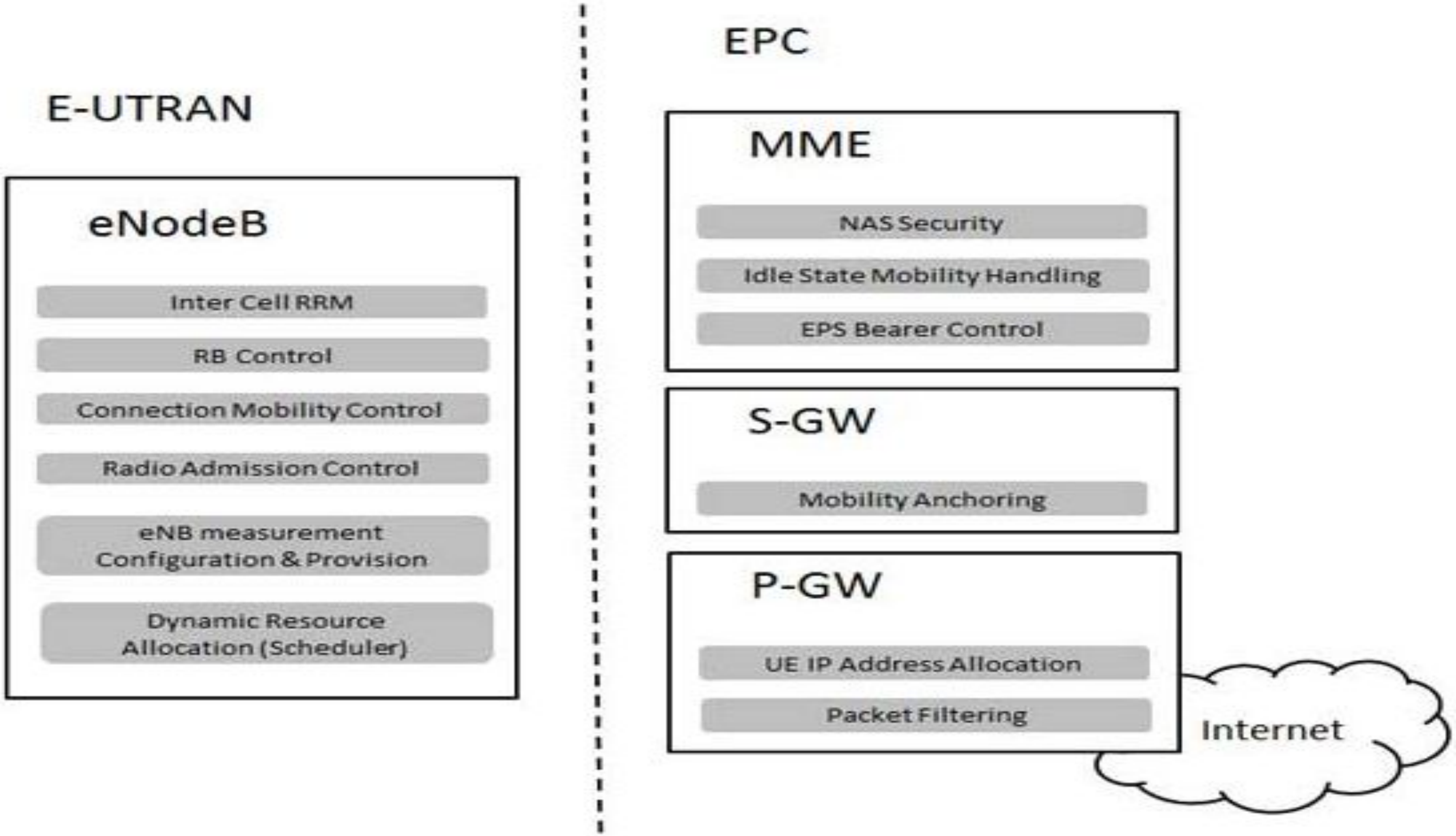
2G/3G	LTE
GERAN and UTRAN	E-UTRAN
SGSN/PDSN-FA	S-GW
GGSN/PDSN-HA	PDN-GW
HLR/AAA	HSS
VLR	MME
SS7-MAP/ANSI-41/RADIUS	Diameter
DiameterGTPc-v0 and v1	GTPc-v2
MIP	PMIP

- The Home Subscriber Server (HSS) component has been carried forward from UMTS and GSM and is a central database that contains information about all the network operator's subscribers.
- The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world ie. packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN). The PDN gateway has the same role as the GPRS support node (GGSN) and the serving GPRS support node (SGSN) with UMTS and GSM.

- The serving gateway (S-GW) acts as a router, and forwards data between the base station and the PDN gateway.
- The mobility management entity (MME) controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server (HSS).
- The Policy Control and Charging Rules Function (PCRF) is a component which is not shown in the above diagram but it is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW.

- The interface between the serving and PDN gateways is known as S5/S8. This has two slightly different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.

Functional split between the E-UTRAN and the EPC



Overview of LoRa & LoRaWAN

- Communication is one of the most important parts of any IoT project. The ability of a thing to communicate with other “things” (a device cloud/server) is what gives the “thing” the right to attach the “internet” to its name. While tons of communication protocols exist, each of them lacks one thing or the other which made them “not totally suitable” for IoT applications. The Major problems being power consumption, range/coverage and bandwidth.
- Most communication radios like Zigbee, BLE, WiFi among others are of short range and others like, 3G and LTE, are power hungry and the span of their coverage areas cannot be guaranteed especially in developing countries. While these protocols and communication modes work for certain projects, it brings an extensive limitation like; difficulties in deploying IoT solutions in areas without cellular (GPRS, EDGE, 3G, LTE/4G) coverage and gross reduction in battery life of devices. Thus, envisaging the future of IoT and the connection of all kind of “things”, located in all kind of places, there was a need for a communication medium tailor-made for IoT which supports it’s requirements of specifically low power, significantly long range, cheap, secure, and easy to deploy. This is where **LoRa** comes in.

- **LoRa** (which stands for **Long Range**) is a patented wireless communication technology which combines **ultra-low power consumption with an effective long range**.

- While range highly depends on the environment and possible obstructions (LOS or N-LOS), **LoRa** typically has a **range between 13- 15Km**, which means a single **LoRa gateway** can provide coverage for an entire city, and with a couple more, a whole country.

- The technology was developed by Cycleo in France and came to fore when the company was acquired by Semtech in 2012. We used **LoRa module**

with Arduino and **with Raspberry Pi** and they worked as expected.

Features of LoRa

- A LoRa radio comprise of a few features which help it achieve long-range effective power and Low cost.

Some of these features include;

- Modulation Technique
- Frequency
- Adaptive Data Rates
- Adaptive Power Levels

Modulation

- Lora radios use the chirp spread spectrum modulation technique to achieve a significantly high communication range while maintaining low power characteristics that are similar to the FSK modulation physical layer based radios.

- While chirp spread spectrum modulation has been around for a while with applications in military and space communications, LoRa presents the first, low-cost commercial application of the modulation technique.

Frequency

- While the LoRa technology is frequency agnostic, Communication between LoRa radios happen via the use of unlicensed sub-GHz radio frequency bands that are available around the world.
- These frequencies vary from region to region and often also differ between countries.
- For instance the 868MHz is commonly used for LoRa communications in Europe, while the 915MHz is used in North America.
- Irrespective of the frequency, LoRa can be used without any major variation in the technology.
- (Using Lower frequencies than those of the communication modules like WiFi based on the 2.4 or 5.8GHz ISM bands enable a much larger coverage area especially for NLOS situations.
- It is important to note that permissions are still required in some countries before the unlicensed bands can be used

Frequency Bands for LoRa in Different Countries

	Europe	North America	China	Korea	Japan	India
Frequency band	867-869MHz	902-928MHz	470-510MHz	920-925MHz	920-925MHz	865-867MHz
Channels	10	64 + 8 +8	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee
Channel BW Up	125/250kHz	125/500kHz				
Channel BW Dn	125kHz	500kHz				
TX Power Up	+14dBm	+20dBm typ (+30dBm allowed)				
TX Power Dn	+14dBm	+27dBm				
SF Up	7-12	7-10				
Data rate	250bps- 50kbps	980bps-21.9kpbs				
Link Budget Up	155dB	154dB				
Link Budget Dn	155dB	157dB				

.

Adaptive Data Rate

LoRa uses a combination of variable bandwidth and spreading factors (SF7-SF12) to adapt the data rate in a trade-off with the range of the transmission. Higher spreading factor allows longer range at the expense of lower data rate, and vice versa.

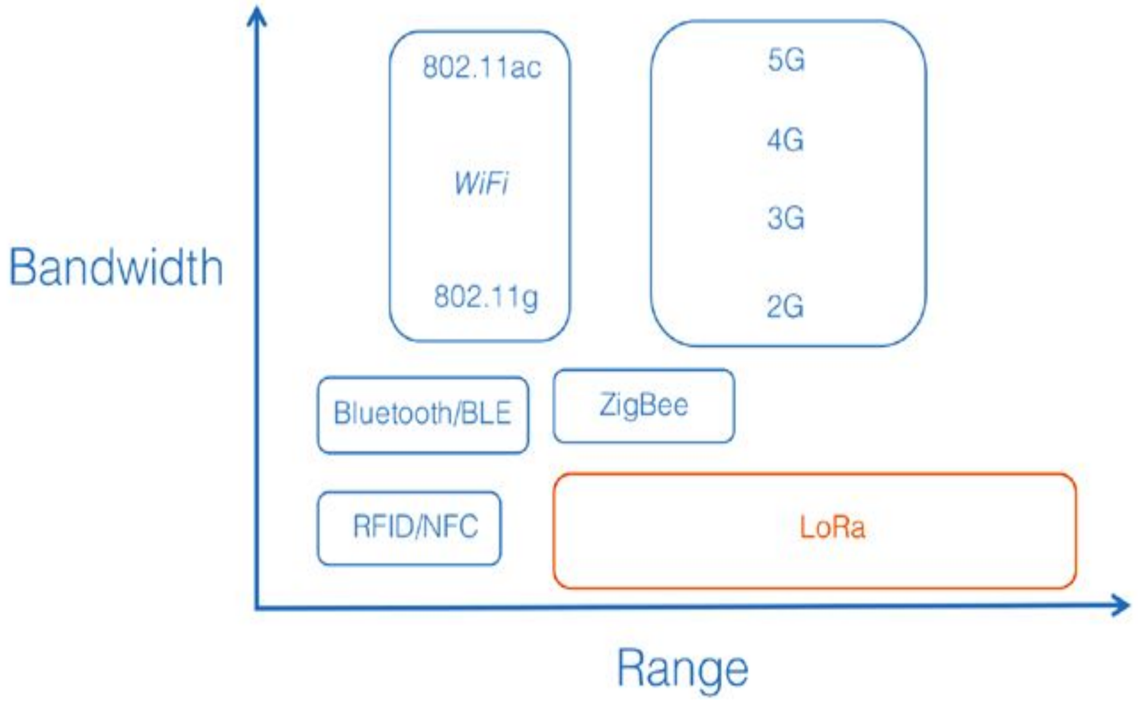
The combination depend on the link conditions and the level of data to be transmitted. Thus, a higher spreading factor improves transmission performance and sensitivity for a given bandwidth, but it also increases transmission time as a result of lower data rates.

LoRa Spreading Factors (125kHz bw)

Spreading Factor	Chips/symbol	SNR limit	Time-on-air (10 byte packet)	Bitrate
7	128	-7.5	56 ms	5469 bps
8	256	-10	103 ms	3125 bps
9	512	-12.5	205 ms	1758 bps
10	1024	-15	371 ms	977 bps
11	2048	-17.5	741 ms	537 bps
12	4096	-20	1483 ms	293 bps

Adaptive Power Level

- The power level used by LoRa radios is adaptive.
- It is dependent on factors like the data rate and link conditions among others.
- When a fast transmission is required, the transmitted power is pushed closer to the maximum and vice versa.
- Thus, battery life is maximized and network capacity maintained.
- Power consumption also depends on the class of devices among several other factors.



Advantages of LoRa

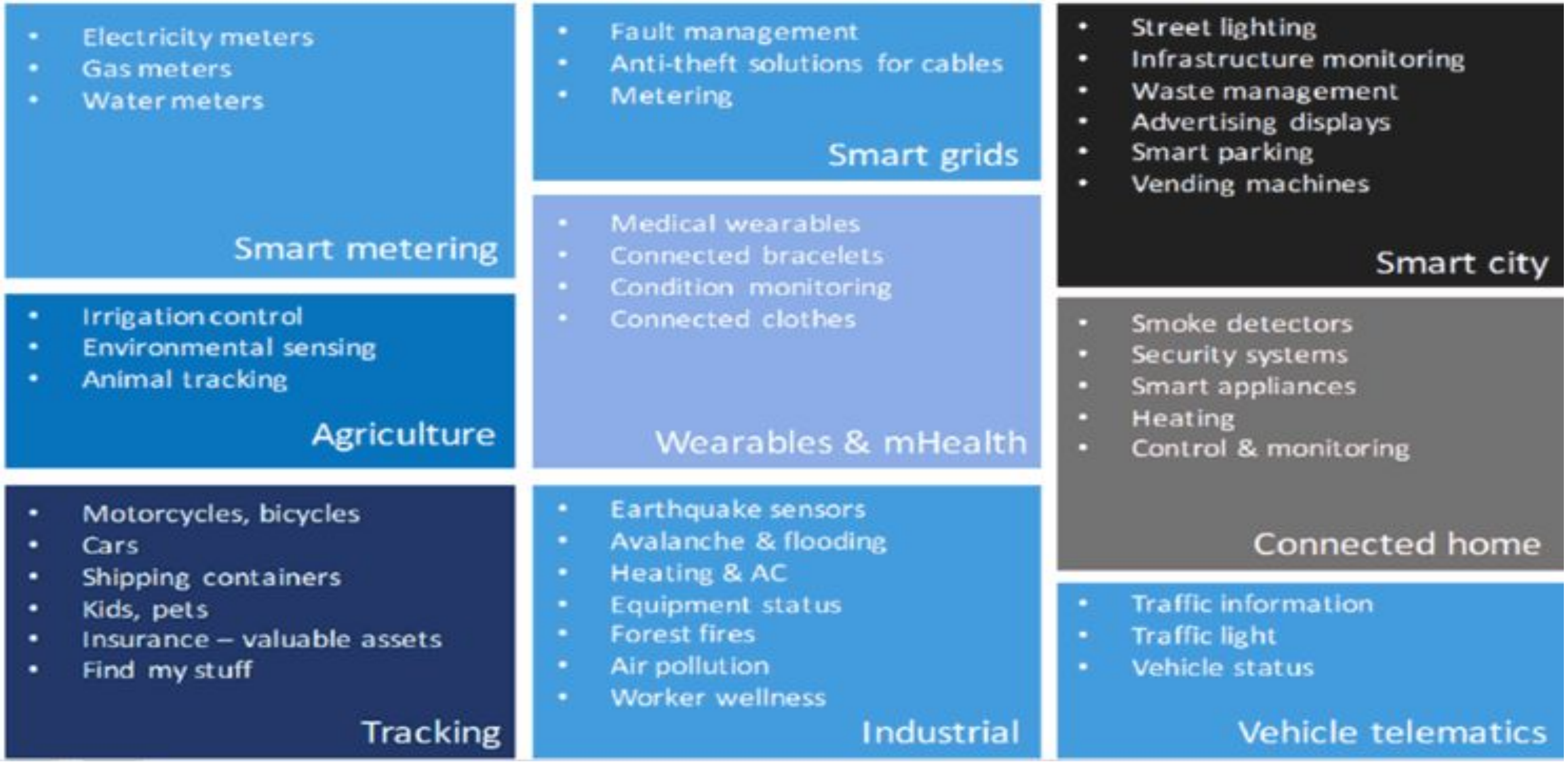
Below are some of the advantages associated with LoRa;

- **1. Long Range and Coverage:** With up to 15km LOS Range, its range can't be compared with that of any other Communication protocol.
- **2. Low Power:** LoRa offers hyper low power radios which makes them Ideal for devices that are required last for 10 years or more on a single battery charge.
- **3. Low cost hardware:** Infrastructures for LoRaWAN are extremely low cost compared to other networks and cost of radios for end-devices are equally Low. More so, several open source versions of infrastructures like gateways are being developed which helps to further reduce costs.
- **4. High Capacity:** Thousands of end devices could be connected to a single LoRa gateway

Disadvantages of LoRa

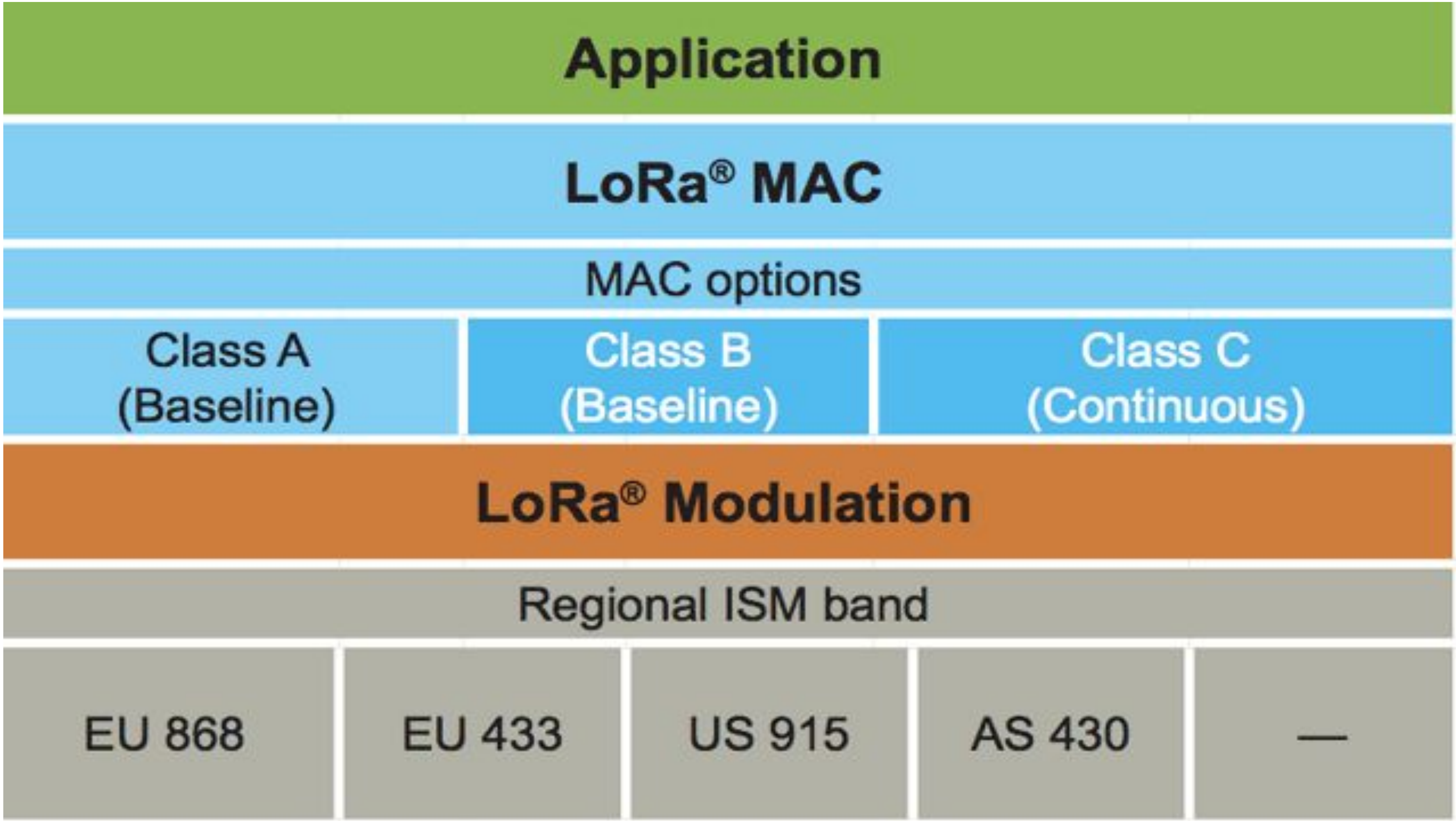
- With a maximum data rate of around 50kb/s, **LoRa has the lowest of data rates** when compared with most of the other technology which makes it not ideal for certain applications where high data rates are required.

Applications of LoRa

- The applications of LoRa are only Limited by imagination. It has been one of the major drivers of smart city in countries around the world with full-scale city wide LoRa Network already deployed in several cities. Applications of LoRaWAN cuts across all sorts of IoT Solution. A few are listed in the image below.
- 

LoRaWAN

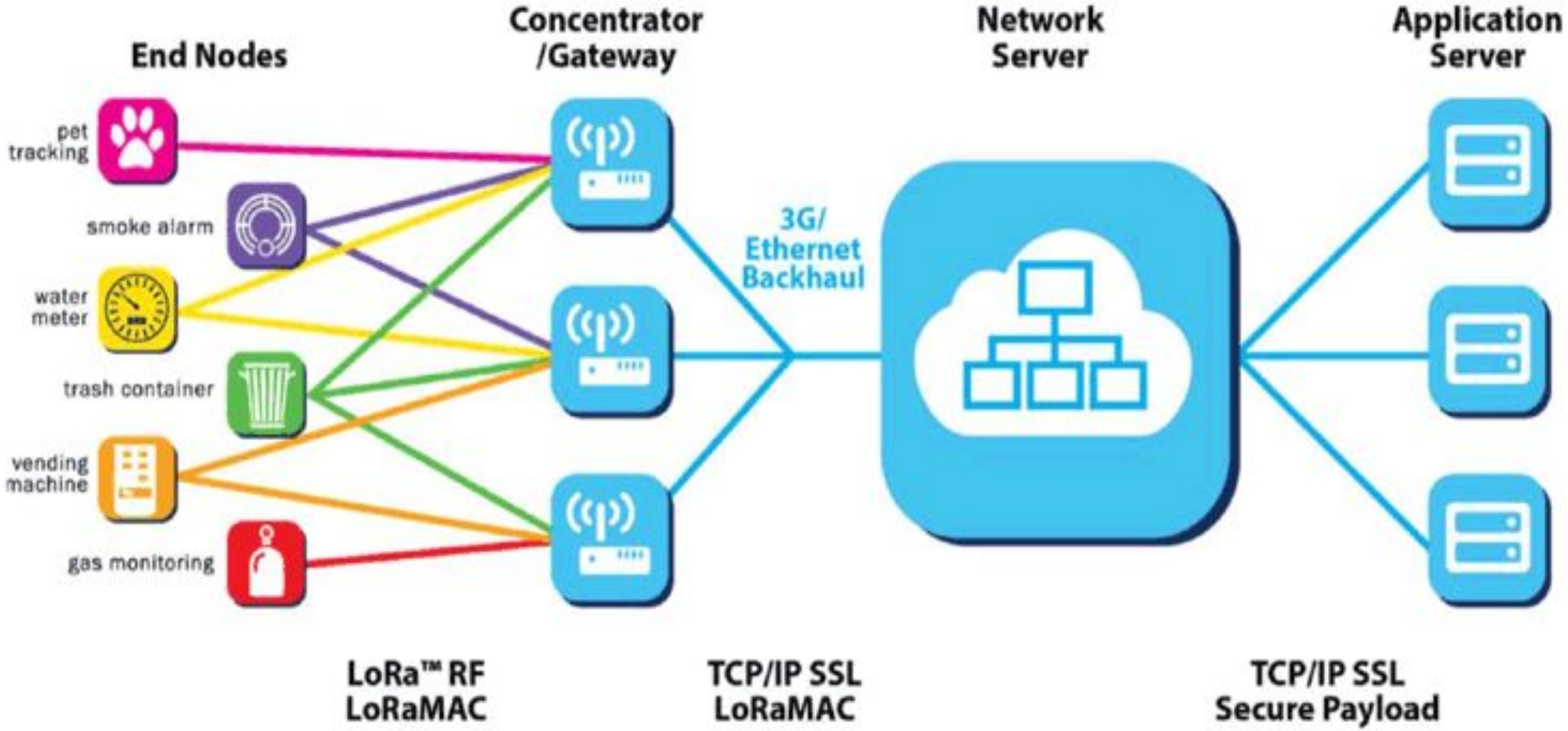
- **LoRaWAN is a high capacity, Long Range, open, Low Power Wide Area Network** (LPWAN) standard designed for **LoRa Powered IoT Solutions** by the **LoRa Alliance**.
- It is a bi-directional protocol which takes full advantage of all the features of the LoRa technology to deliver services including reliable message delivery, end to end security, location and multicast capabilities.
- The standard ensures the interoperability of the various LoRaWAN networks world-wide.
- There is usually a mix up when people try to **define LoRa and LoRaWAN** which is probably best solved by examining the OSI reference stack Model.


Application
LoRa® MAC
MAC options
Class A (Baseline)
Class B (Baseline)
Class C (Continuous)
LoRa® Modulation
Regional ISM band
EU 868
EU 433
US 915
AS 430
—

- Simply put, based on the OSI stack Model, **LoRaWAN corresponds to Media Access protocol** for the communication network while **LoRa corresponds to the Physical layer**.
- Thus LoRaWAN defines the communication protocol and system architecture for the network, while LoRa architecture enables the long-range communication link.
- The two of them merged together to provide the functionality that determines battery life of a node, the network capacity, the quality of service, the security and other applications served by the network.
- While LoRaWAN is the most popular MAC layer for LoRa other proprietary layers which are also built on the LoRa technology exists.
- A good example is Symphony link by Link Labs which is specially developed for industrial applications.

The LoRaWAN Network Architecture

- Opposed to the mesh network topology adopted by most networks, LoRaWAN uses the star network architecture, thus, rather than have each end-device in an almost always on state, repeating transmission from other devices to increase range, end-devices in the LoRaWAN network communicate directly with gateways and are only on when they need to communicate with the gateway since range is not a problem.
- This is a contributing factor to the Low power features and High battery life obtained in the LoRa end devices

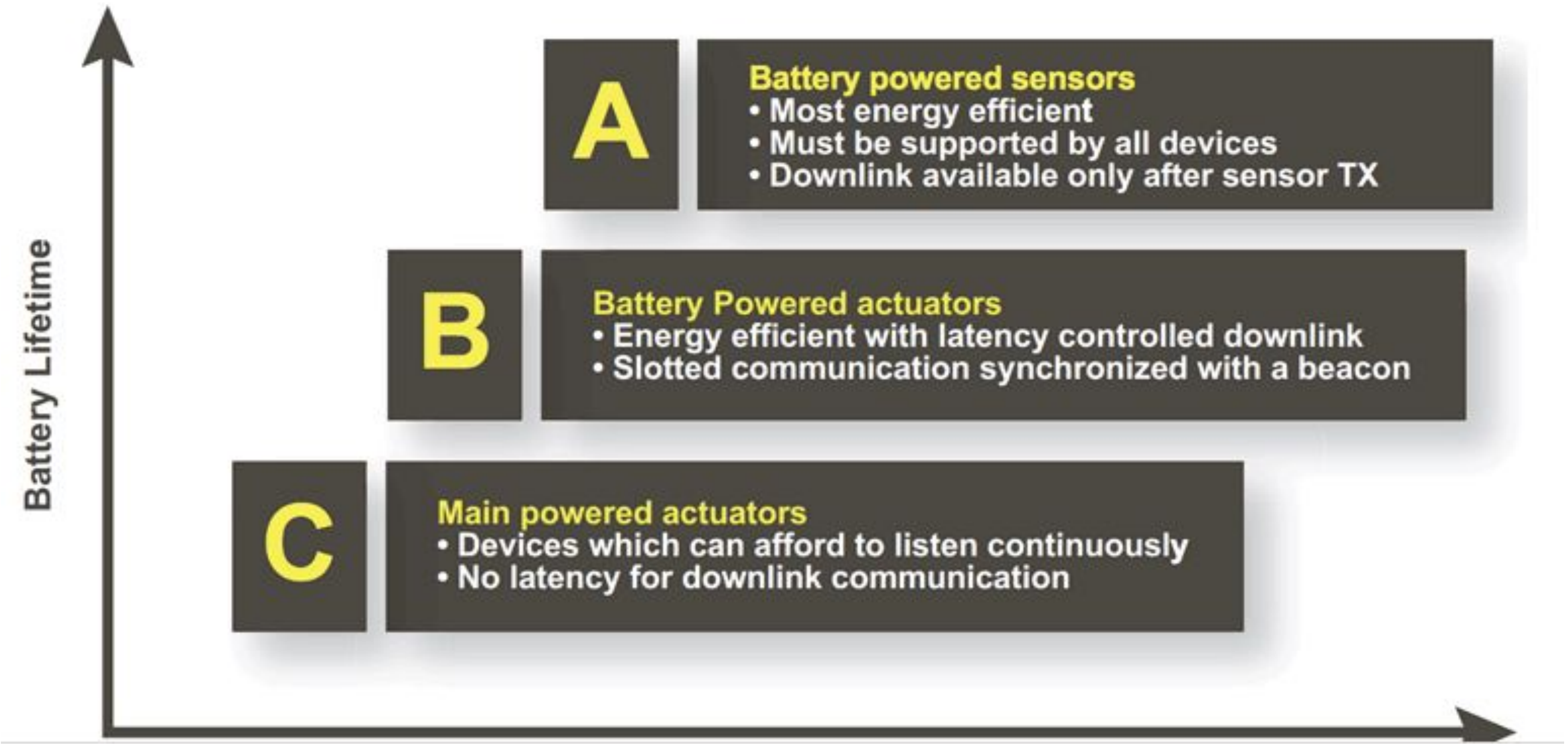

End Nodes
Concentrator
/Gateway
Network
Server
Application
Server
pet
tracking
smoke alarm
water
meter
trash container
vending
machine
gas monitoring
3G/
Ethernet
Backhaul
LoRa™ RF
LoRaMAC
TCP/IP SSL
LoRaMAC
TCP/IP SSL
Secure Payload

The LoRa Network Architecture comprises of four major parts;

- 1. End Devices
- 2. Gateways
- 3. Network server
- 4. Application Server

1. End Devices

- These are sensors or actuators at the network edge. End-devices serve different applications and have different requirements. In order to optimize a variety of end application profiles, LoRaWAN™ utilizes three different device classes to which end-devices can be configured as. The classes feature trade offs between downlink communication latency and battery life of the device.
- The three major classes are;
- 1. Bi-Directional end-devices (Class A)
- 2. Bi-directional end-devices with scheduled receive slots (Class B)
- 3. Bi-directional end-devices with maximal receive slots (Class C)


Battery Lifetime
A
Battery powered sensors
• Most energy efficient
• Must be supported by all devices
• Downlink available only after sensor TX
B
Battery Powered actuators
• Energy efficient with latency controlled downlink
• Slotted communication synchronized with a beacon
C
Main powered actuators
• Devices which can afford to listen continuously
• No latency for downlink communication

- **2. Gateways**
- Gateways (concentrators) are devices connected to the network server via standard IP connections that relay messages between the central network server backend and end-devices using single-hop wireless communication protocol. They are designed to support bi-directional communication and are equipped with multicast enabling the software to send mass distribution messages like over-the-air updates.
- At the heart of every LoRa gateway is a multi-channel LoRa demodulator able to decode all LoRa modulation variants on several frequencies in parallel.
- LoRa spreads communication between end-devices and gateways across multiple frequency channels and data rates. The spread spectrum technology uses data rates ranging from 0.3 kbps to 50 kbps to prevent communications from interfering with each other and creates a set of "virtual" channels that increase the capacity of the gateway.
- To maximize both the battery life of the end-devices and the overall network capacity, the LoRa network server manages the data rate and RF output for each end-device individually through an adaptive data rate (ADR) scheme.

3. Network Server

- Lora Network server is the interface between the Application server and the Gateways. It relays commands from the Application server to the gateway while ferrying data from the gateways to the application server. It perform functions including ensuring there are no duplicate packets, Scheduling acknowledgements and managing the data rate and RF output for each end-device individually using a adaptive data rate (ADR) scheme.

4. Application Server

- The application server determines what the data from the end devices are used for. Data Visualization etc are probably done here.