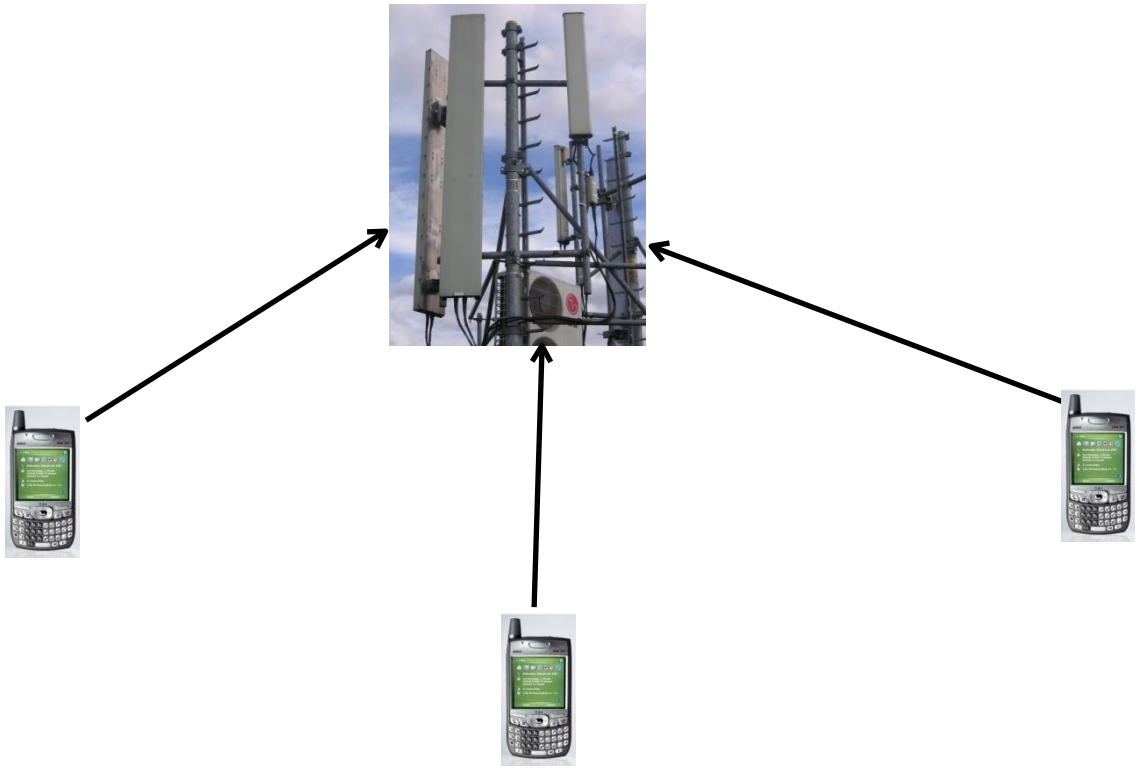
Mechatronics & Robotics

Global System for Mobile (GSM) Communication Protocol

Wireless Communications

- Channel is the air medium.
- Multiple users can simultaneously transmit over the air medium

- For instance, different cell phone users in a cell are trying to transmit to the Base Station.



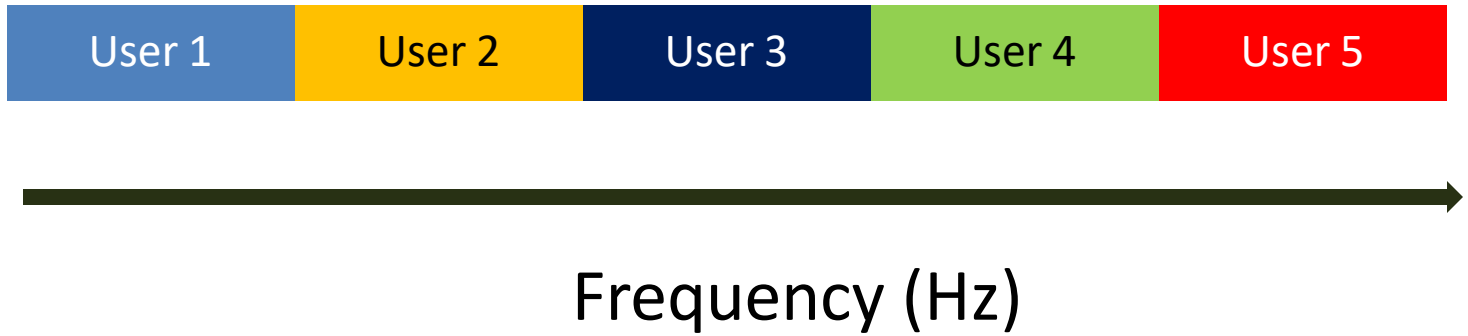
Wireless Communications

How to allocate the medium to a certain user?

The answer is **Multiple Access** (MA) technology!

Multiple Access Technologies

- FDMA – “Frequency Division for Multiple Access”
- Each user is allocated a different frequency band.
  - Forms the 1st Generation or 1G Mobile Technology



An FDMA Phone

Multiple Access Technologies

- TDMA – Time Division for Multiple Access.
- Each user is allocated a certain time “slot” for information transmission.

GSM uses TDMA!

Introduction to GSM

- GSM (*Global System for Mobile Communication*)is an ETSI (European Telecommunication Standards Institute) standard

- GSM went beyond the air-interface and defined a system that complied with ISDN (*Integrated Services Digital Network*) like services.
  - ISDN provides data services over traditional telephone network or PSTN (*Public Switched Telephone Network*)

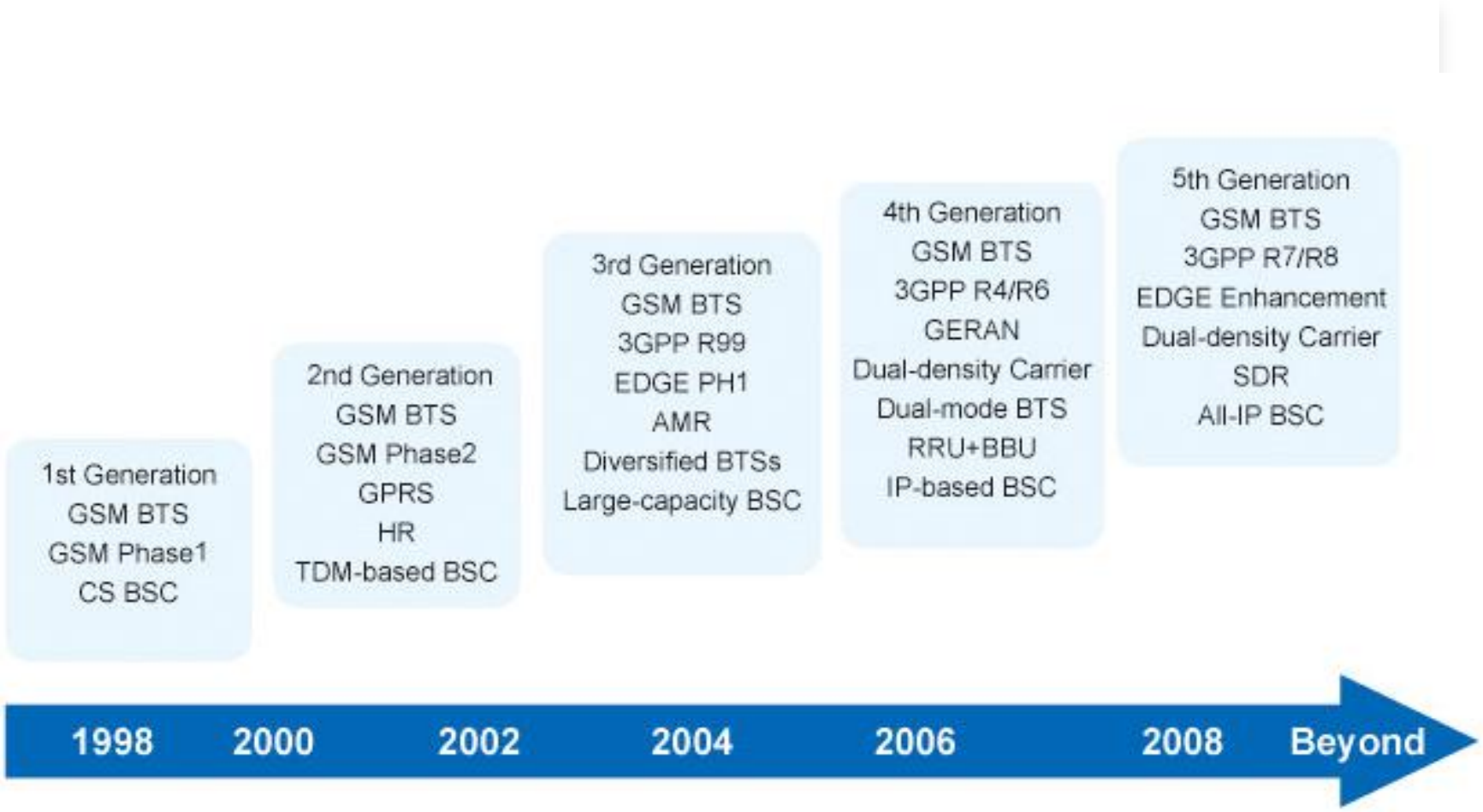
Introduction to GSM

- One of the leading digital cellular systems
- GSM was first introduced in 1991 and as of the end of 1997; GSM service was available in more than 100 countries and has become the de standard in Europe and Asia
- GSM uses narrowband TDMA, which allows eight simultaneous calls on the same radio frequency.

Timeline – Brief History of GSM

1982	**Frequency bands allocated for Pan-European PLMN (Public Land Mobile Network).**
1986	GSM Task Force formed
1987	Memorandum of understanding signed.
1989	ETSI officially included GSM in its domain. Name of the group was changed to Special Mobile Group (SMG). Hence, the resulting standard was named GSM (**Groupe Spécial Mobile**).
1991	Specification completed.
1992	First deployment
1993	32 Operators in 22 countries.
2001	Deployed in close to 150 countries.

Evolution of GSM



Features of GSM

- Compatibility: can use the same mobile to make calls in several countries.
- Noise Robust such that digital GSM is better than analog because it suffers from noise therefore using digital will reduce the noise interference
- Flexibility and increased capacity as the equipment is smaller in size
- Security and confidentiality
- Flexible handovers in using GSM than by using analog systems.
- Enhanced range services such that the services available are speech services including Telephony and emergency calls, Data services including Short Message Service (SMS), cell Broadcast and supplementary services which charge extra including number identification, call Baring, call forwarding and call completion.

GSM Services

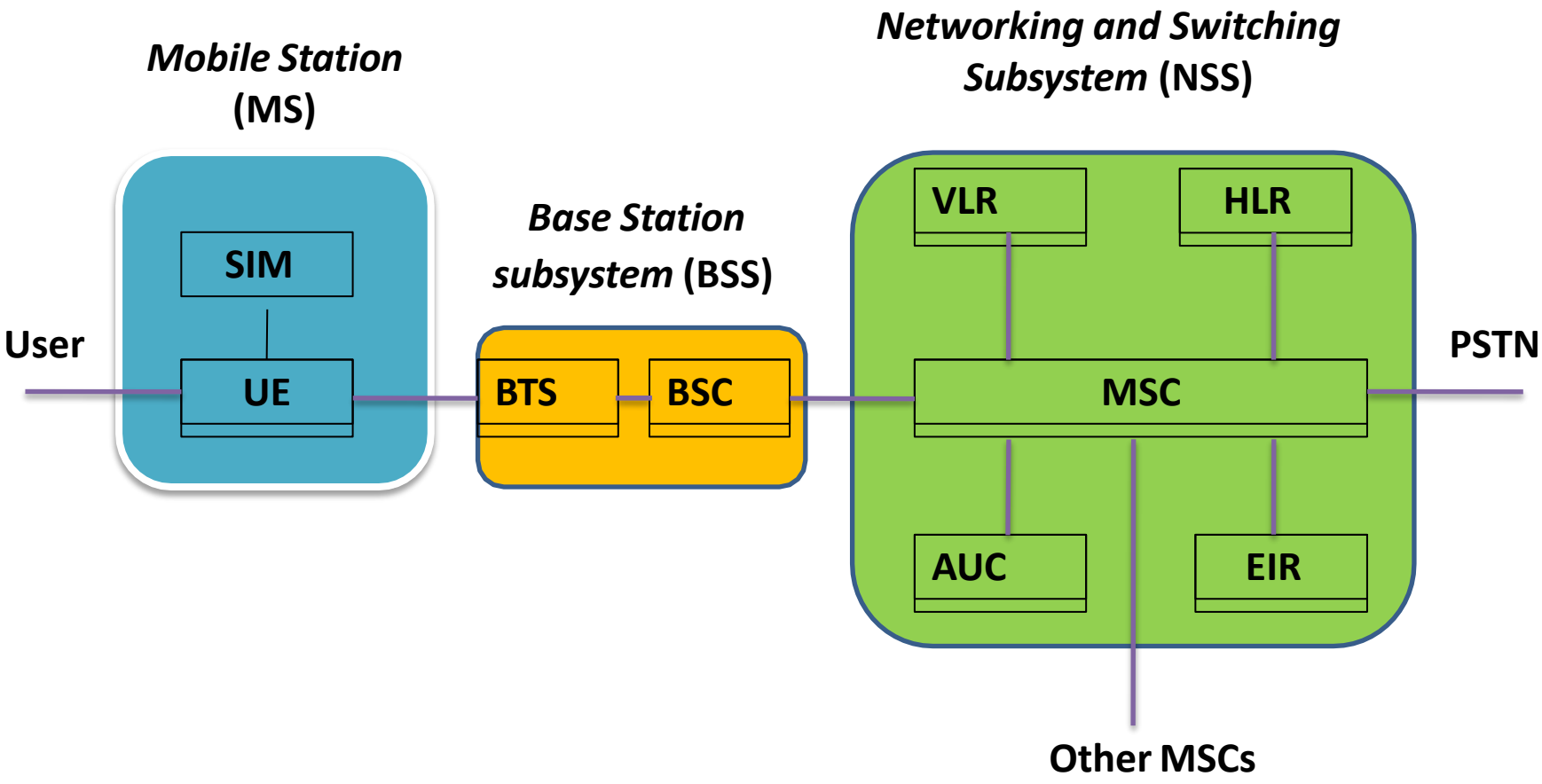
- Analog cellular systems were designed for the sole purpose of voice traffic similar to PSTN.

- GSM is an integrated voice-data service that provides several services beyond voice.

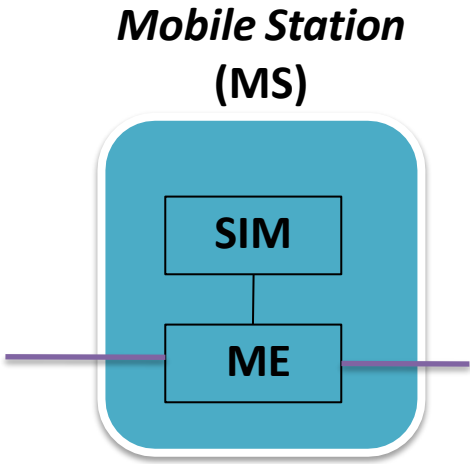
GSM Reference Architecture

- GSM is organized into three major segments.
  - Mobile station (MS).
  - Base station subsystem (BSS).
  - Network and switching subsystem (NSS).

GSM Reference Architecture

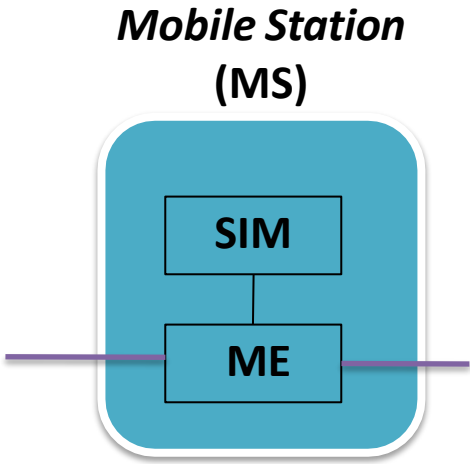


Mobile Station (MS)



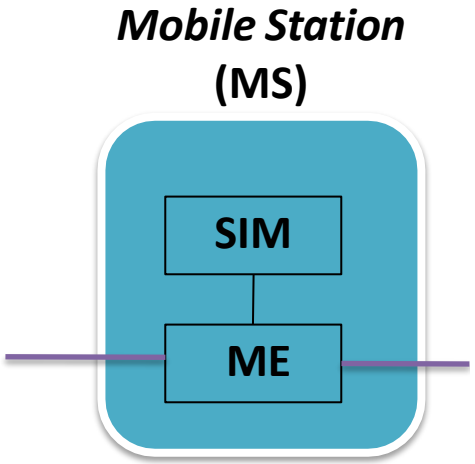
- Functionality
  - Communicates information with user.
  - Demodulates radio signals, extracts digital voice
  - Modifies user info for transmission over the air-interface to communicate with the BS.
- MS has two elements
  - Mobile Equipment (ME)
    - Purchased from equipment vendor.
    - Components include speaker/microphone and the *radio modem* (modulation-demodulation).

Mobile Station (MS)



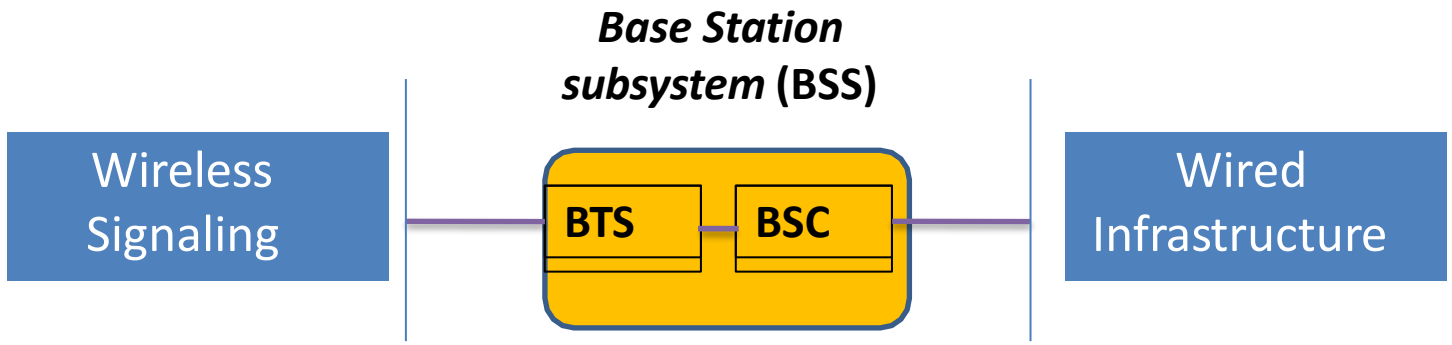
– Subscriber Identity Module (SIM)
  - Smart card issued at the subscription time identifying the user specs such as operator, service type.
    – Identity of user in the mobile network
  - Calls in GSM are directed to the SIM rather than the terminal
  - SMS (Short Message Service) messages are also stored in the SIM.

Mobile Station (MS)



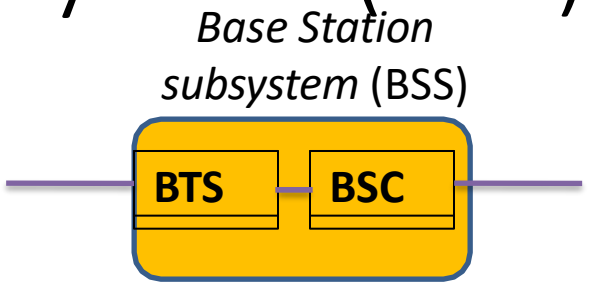
- SIM has a significant impact on the way that a user transacts with the service provider.
  - For instance, determines charging, roaming etc.
- SIM carries the user personal information, which enables a number of useful applications.
- SIM is identified with an IMSI (*International Mobile Subscriber Identity*) for the internal network.

Base Station Subsystem (BSS)



- BSS communicates with the user through the wireless air-interface (through ME).
- Communicates with the wired infrastructure through a different set of wired protocols.
- Separates packet data from PSTN traffic.
  - To implement packet data services such as GPRS.

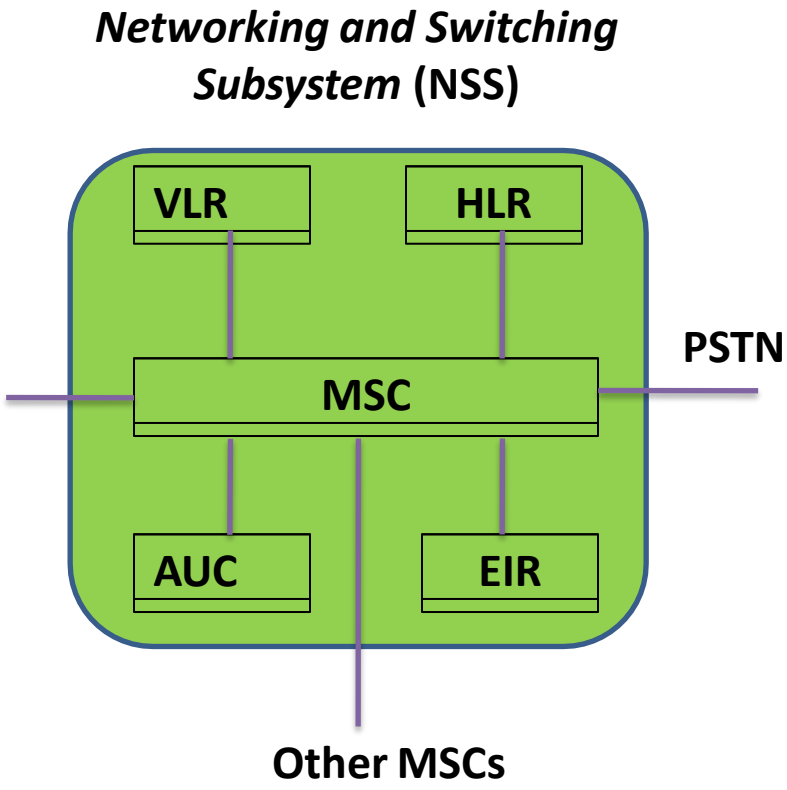
Base Station Subsystem (BSS)



- BSS has two architectural elements
  - Base Transceiver Station (BTS)
    - Counterpart of MS for physical communication.
    - Includes Tx, Rx and signaling equipment for Demod
    - One BSS may have several BTSs in its domain.
  - Base Station Controller (BSC)
    - Small switch inside the BSS that is in charge of frequency administration.
    - Also in charge of handover among the BTSs inside a BSS.

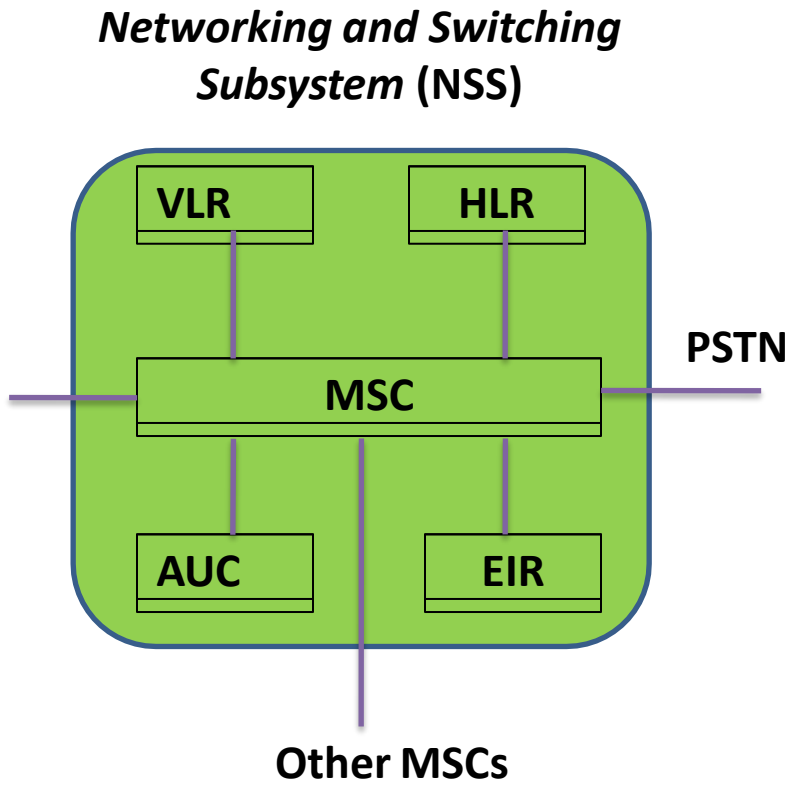
Network and Switching Subsystem

- NSS is master system responsible for network operation.
- It is responsible for
  - Communication with other wired and wireless networks.
  - Also support for registration and maintenance of the connection with the MSs.
- Connects to the PSTN (Public Switched Telephone Network) through ISDN protocols.
- It has one H/W element i.e. MSC and four S/W elements – VLR, HLR, EIR and AUC.



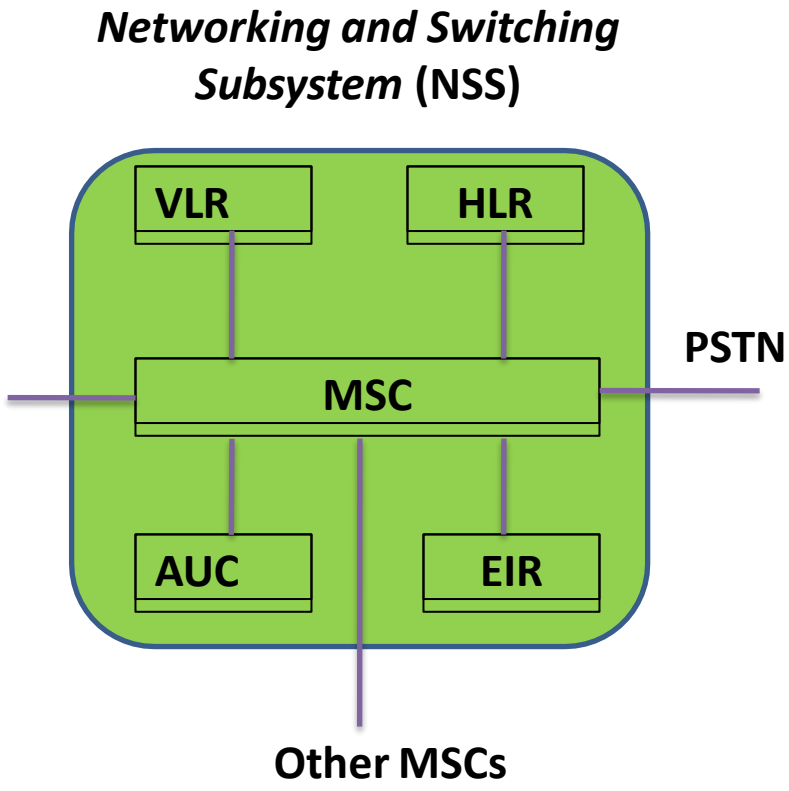
NSS Architectural Elements

- Mobile Station Controller (MSC)
  - The H/W part of the NSS.
  - Communicates with other MSCs in the coverage area of the service provider.
  - Also communicates with the PSTN switches.
    - This is the Gateway MSC (GMSC)
- Home Location Register (HLR)
  - Database S/W that handles management of the mobile subscriber account.
  - Stores the subscriber's address, service type, current location, forwarding address etc.



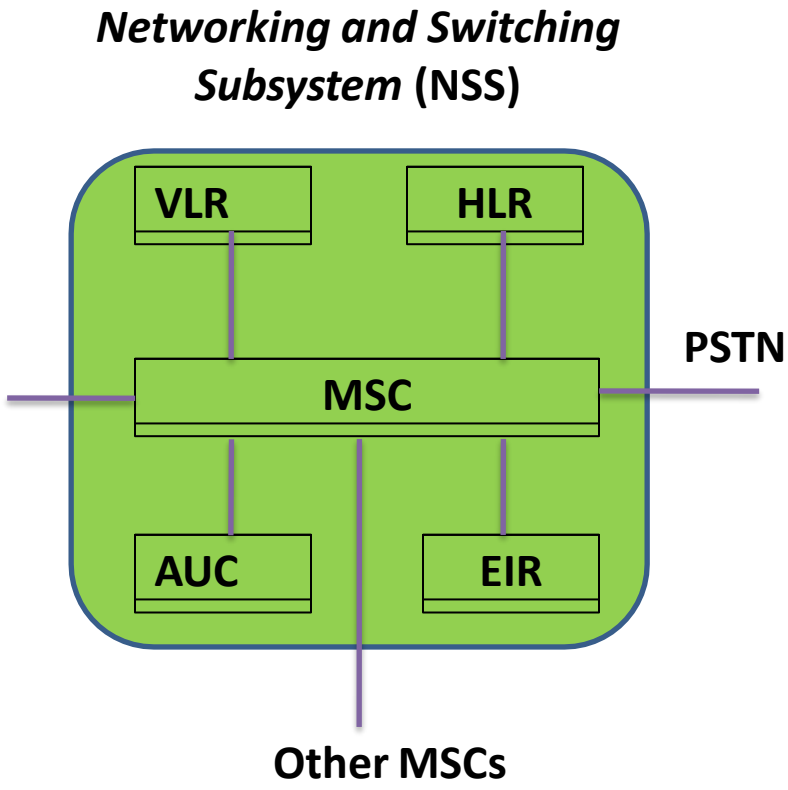
NSS Architectural Elements

- Visitor Location Register (VLR)
  - Temporary database S/W in *Visiting Cell*, similar to the HLR.
  - Identifies the subscribers *visiting* inside the coverage area of the MSC.
  - Thus, calls from Home MSC can be forwarded to visiting MSC.



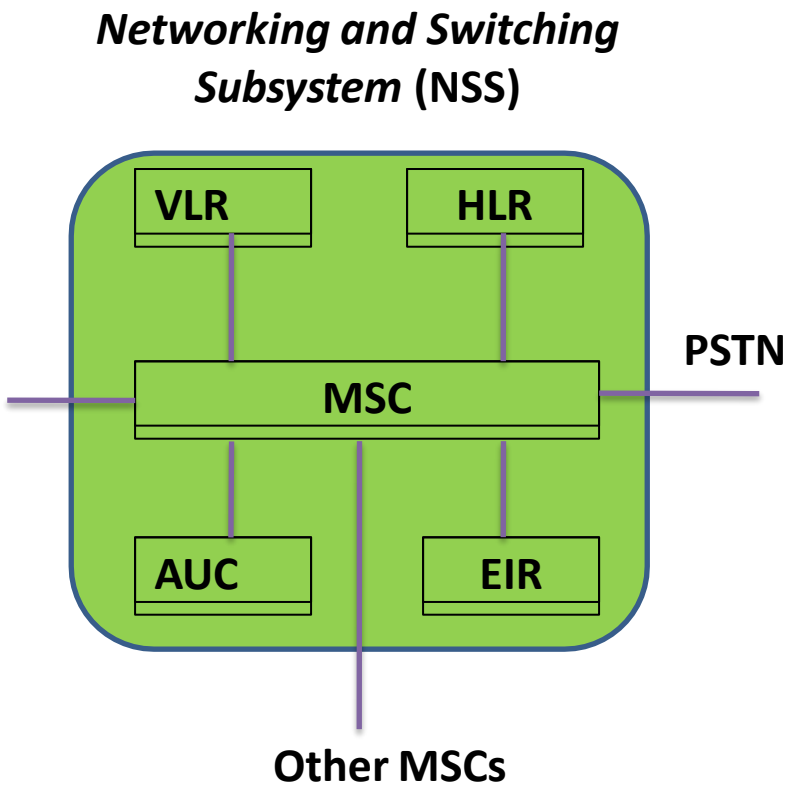
NSS Architectural Elements

- Authentication Center (AUC)
  - Holds different algorithms that are used for authentication and encryption of subscribers.
  - Different SIM cards have different algorithms and the AUC collects all of these algorithms.



NSS Architectural Elements

- Equipment Identification Register (EIR)
- Keeps the IMEI (International Mobile Equipment Identity) that reveals the manufacturer, country of production, terminal type.
  - Used to report stolen phones and to check if the phone is operating according to the service type.



GSM Services

- Tele-services
- Bearer or Data Services
- Supplementary services

Tele-services

- Telecommunication services that enable voice communication via mobile phones.

- Offered services
  - Mobile telephony
  - Emergency calling

Bearer Services

- Include various data services for information transfer between GSM and other networks like PSTN, ISDN etc at rates from 300 to 9600 bps
- Short Message Service (SMS)
  - up to 160 character alphanumeric data transmission to/from the mobile terminal
- Unified Messaging Services(UMS)
- Group 3 fax
- Voice mailbox
- Electronic mail

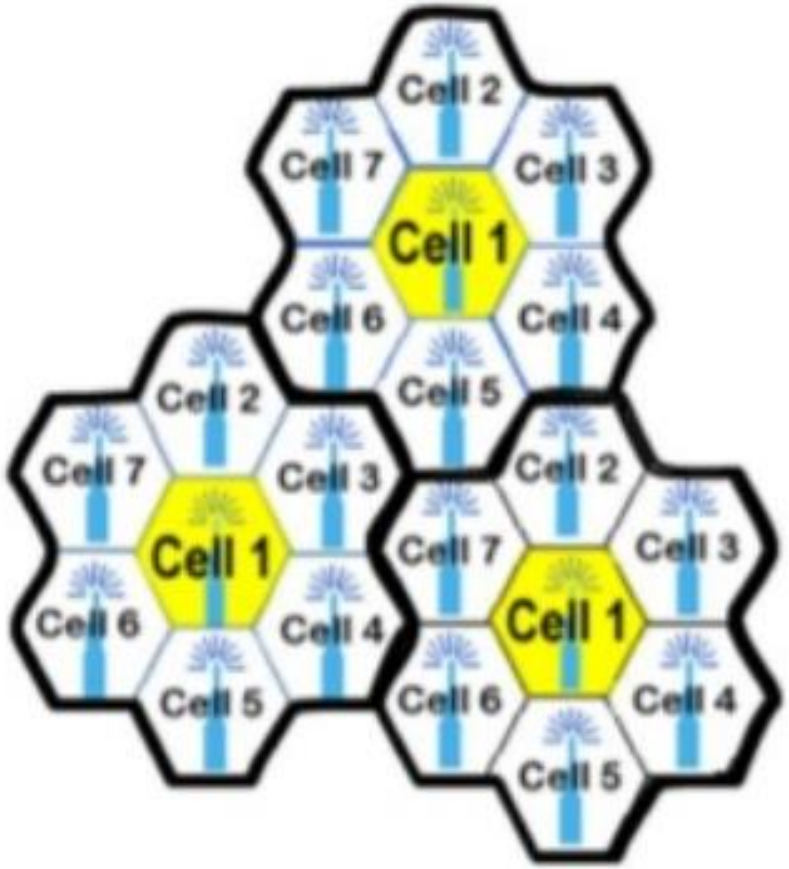
Supplementary Services

Call related services :

- Call Waiting
  - Notification of an incoming call while on the handset
- Call Hold
  - Put a caller on hold to take another call
- Call Barring
  - All calls, outgoing calls, or incoming calls
- Call Forwarding
  - Calls can be sent to various numbers defined by the user
- Multi Party Call Conferencing
  - Link multiple calls together

GSM Cell Structure

Macro-cells(3 to 35 km)
Micro-cells(0,1 to 1 km)



What happens in a GSM phone?

- GSM (Global System for Mobile) uses TDMA, i.e., Time Division for Multiple Access technology.
- Each user is allocated a time “slot” on a frame of data bits.
- The raw data rate of GSM is 270 Kbps.
- Each user transmits for 577 micro seconds
  - This corresponds roughly to 156 bits of information.
- 8 users use the same frequency band
  - Which implies that a frame size is 8 x 577 micro - secs or 4.615 ms.

Handoff (Handover) in GSM

- Transfer from one BTS/BSS to another
- Two types of handover
  - Internal
    - Between two BTSs of the same BSS.
  - External
    - Between two BSSs controlled by same MSC.

Handoff (Handover) in GSM

- Handover is initiated for different reasons.
  - Most common is signal strength deterioration.
  - Traffic balancing, to ease traffic congestion by moving calls to a lightly loaded cell.

Outgoing Call in GSM

1, MS sends dialed number to BSS

2, BSS sends dialed number to MSC

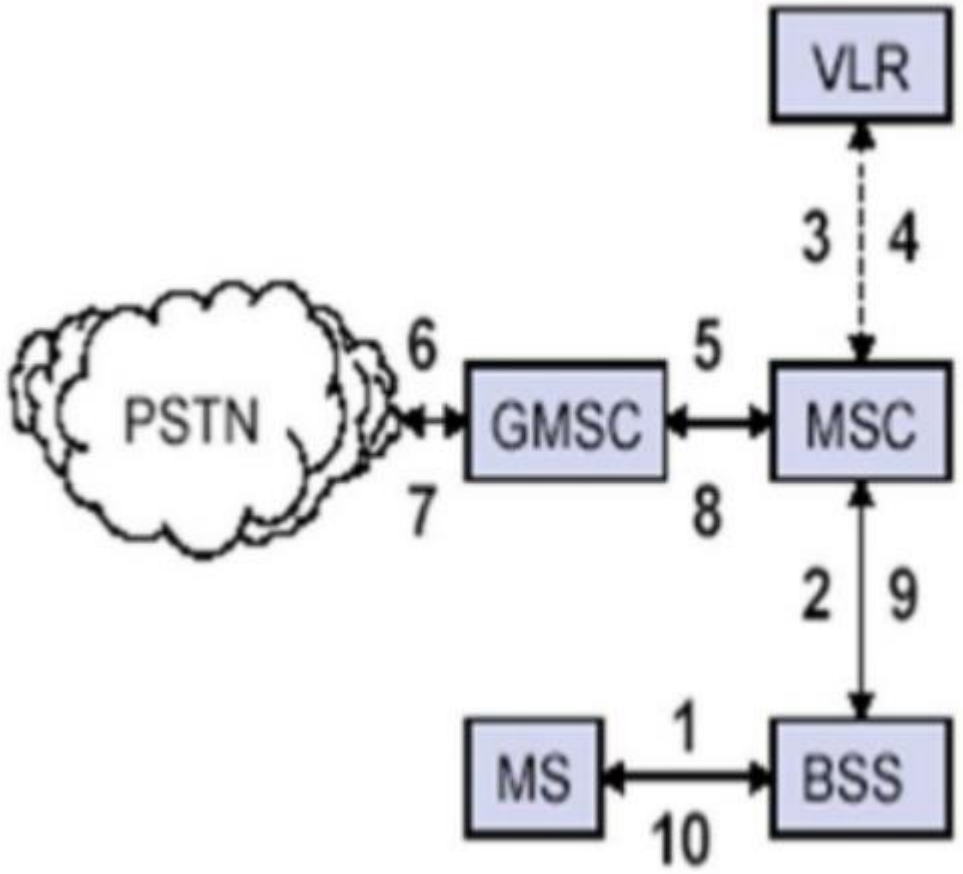
3,4 MSC checks VLR if MS is allov the requested service. If so, MSC ask BSS to allocate resources for call.

4, MSC routes the call to GMSC

6, GMSC routes the call to local exchange of called user

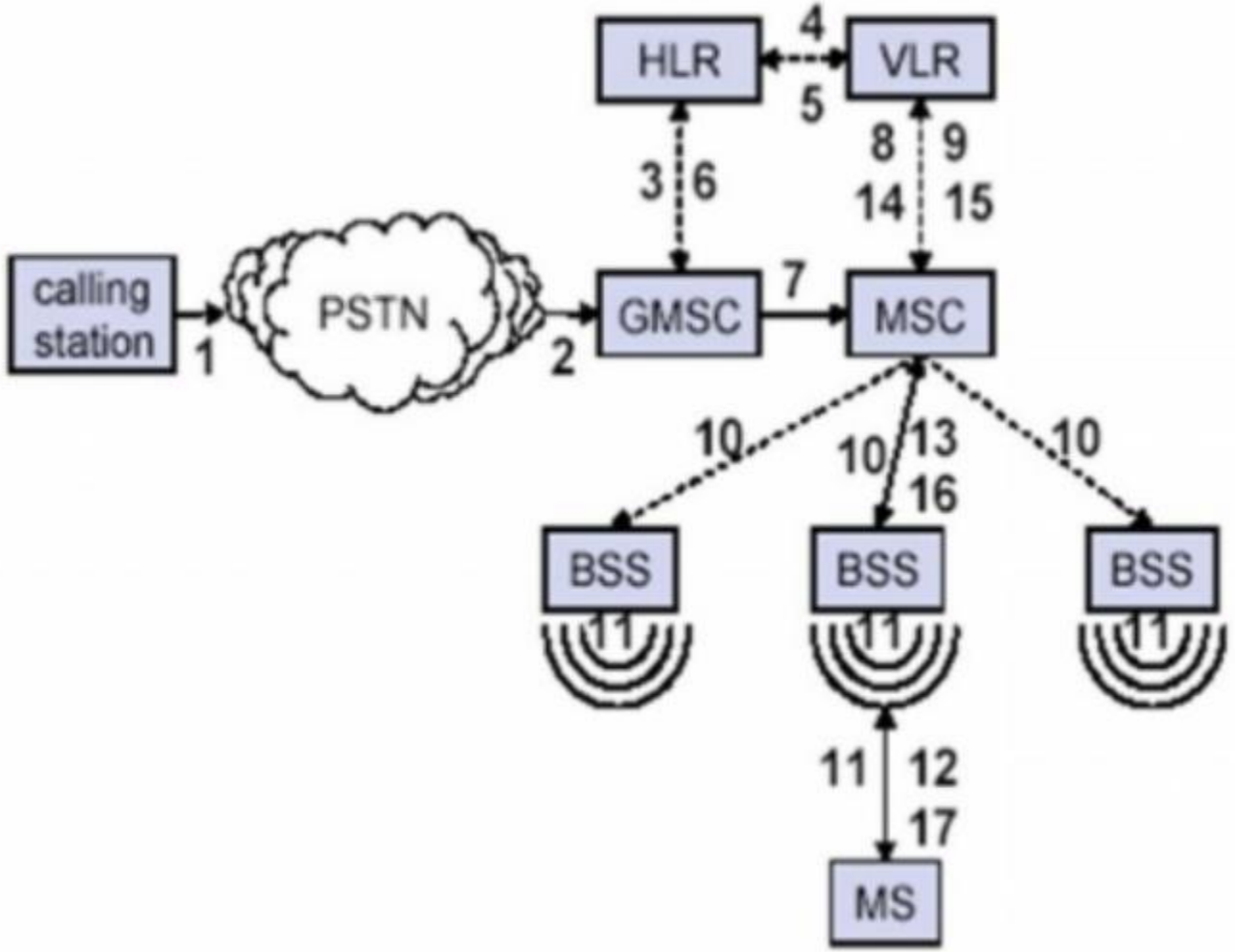
7,8 Answer back

9,10 Answer back(ring back) tone i routed from called user to MS via GMSC,MSC,BSS



Incoming Call in GSM

1. Calling a GSM subscribers
2. Forwarding call to GSMC
3. Signal Setup to HLR
4. 5. Request MSRN from VLR
6. Forward responsible MSC to GMSC
7. Forward Call to current MSC
8. 9. Get current status of MS
10. 11. Paging of MS
12. 13. MS answers
14. 15. Security checks
16. 17. Set up connection



Data Rate Evolution

- **2G**
  - GSM: Data rate: 9.6 Kbps
- **2.5G**
  - GPRS (General Packet Radio service): Data rate: 14.4 - 115.2 Kbps
- **2.75G**
  - EDGE (Enhanced data rate for GSM Evolution): Data rate: 547.2 Kbps
- **3G**
  - WCDMA(Wide band CDMA)
    - RSS: Data rate : 0.348 – 2.0 Mbps
    - HSPA: Data rate: 7.2 Mbps
- **3.5G (3G+)**
  - HSPA+: Data rate: 21 – 42 Mbps
- **4G**
  - LTE (Long Term Evaluation): Data rate: 100 Mbps

Applications of GSM

- Mobile telephony
- GSM-R
- Telemetry System
  - Fleet management
  - Automatic meter reading
  - Toll Collection
  - Remote control and fault reporting of DG sets
- Value Added Services

GSM Module

- Any GSM module is using the normal GSM network
- GSM modules can be communicated to PIC-microcontroller using normal serial USART protocol
- Communication is being done using regular GSM modem AT Commands.

AT Commands

Call control	
Command	Description
ATA	Answer command
ATD	Dial command
ATH	Hang up call
ATL	Monitor speaker loudness
ATM	Monitor speaker mode
ATO	Go on-line
ATP	Set pulse dial as default
ATT	Set tone dial as default
AT+CSTA	Select type of address
AT+CRC	Cellular result codes

http://www.expertcore.org/viewtopic.php?f=18&t=3549

AT Commands

MS Text mode	
Command	Description
AT+CSMS	Select message service
AT+CPMS	Preferred message storage
AT+CMGF	Message format
AT+CSCA	Service centre address
AT+CSMP	Set text mode parameters
AT+CSDH	Show text mode parameters
AT+CSCB	Select cell broadcast message types
AT+CSAS	Save settings
AT+CRES	Restore settings
AT+CNMI	New message indications to TE
AT+CMGL	List messages
AT+CMGR	Read message
AT+CMGS	Send message
AT+CMSS	Send message from storage
AT+CMGW	Write message to memory
AT+CMGD	Delete message

AT Commands, Calls

Command **CHECK COM**	Positive Response
AT<CR><LV>	OK

Command **DIAL**	Positive Response
ATD<number><CR><LV>	OK

Command **ANSWER**	Positive Response
ATA<CR><LV>	After RING, OK

Command **end**	Positive Response
ATH<CR><LV>	OK

Parameters
<CR> = ASCII character 13
<LV> = ASCII character 10

AT Commands, SMS

Command **SET**	Positive Response
AT+CMGF=<mode><CR><LV>	<mode>: **0 = PDU Mode**, 1 = Text Mode OK

Command **DELETE**	Positive Response
AT+CMGD=<index><CR><LV>	<index>: Index number of the message , OK

Command **SEND**	Response
AT+CMGS=<number><CR><LV><message><CTRL-Z>	+CMGS:<mr> OK

Parameters
<CR> = ASCII character 13
<LV> = ASCII character 10
<CTRL-Z> = ASCII character 26
<mr> = Message Reference

- Reference Video Links:
- Working of GSM Protocol:

https://www.youtube.com/watch?v=1JZG9x_VOwA