Review of GSM Technology

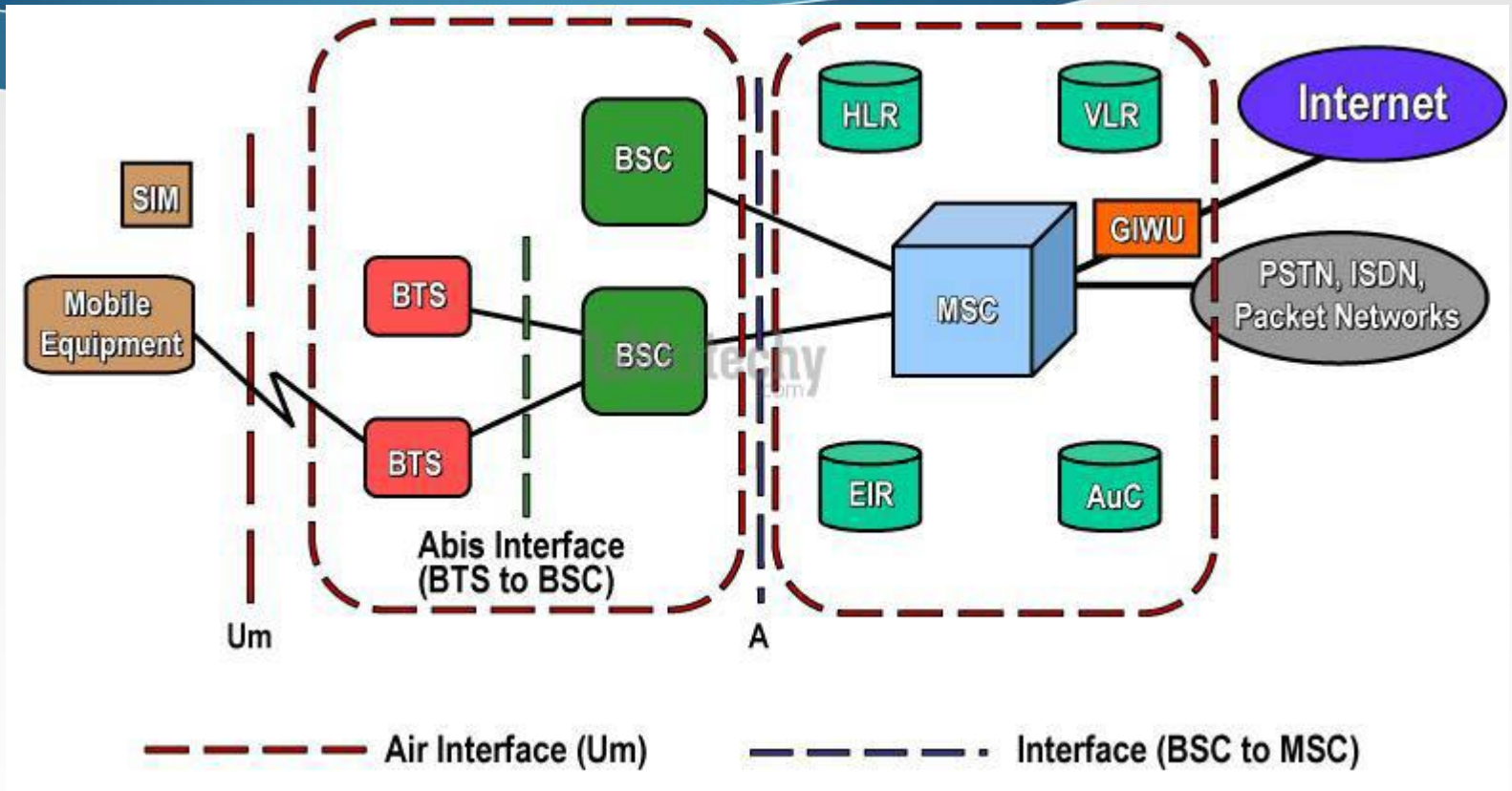
Basics:

- GSM: Global Systems for Mobile
- TDMA + FDMA + FDD
- ETSI Standard for 2G pan-European digital cellular with international roaming
- Frequency bands: 890 – 915 MHz and 935 – 960 MHz
- 1991: Standards were completed and 1992 first deployment started
- Now more than 200 countries using GSM

GSM Services:

- Integrated voice-data service that provides a number of services beyond cellular telephone
- Teleservices: Telephony, Emergency call, SMS, Fax etc.
- Bearer Services: Data/packet data etc
- Supplementary Services: Call forwarding, Call barring, calling line identification etc

GSM Network:



MS: Mobile Station
SIM: Subscriber Identity Module
BTS: Base Transceiver Station
BSC: Base Station Controller
HLR: Home Location Register
VLR: Visitor Location Register
AuC: Authentication Centre
IN: Interrogating Node

Mobile Station:

- MS is the physical equipment used by a GSM subscriber (their 'mobile handset')
- It comprises two parts:
  - a Subscriber Identity Module (SIM) and
  - the Mobile Equipment (ME)
- Mobile station has three identities
  - International Mobile Subscriber Identity (IMSI)
  - International Mobile Equipment Identity (IMEI)
  - Temporary Mobile Subscriber Identity (TMSI)

Mobile Equipment (ME):

- Mobile Station Power Classes:
  - Vehicular & portable units can be either class I or class II
  - Handheld units can be class III, IV, & V

Class	Max. RF Power (W)
I	20
II	8
III	5
IV	2
V	0.8

Home Location Register (HLR):

- HLR is an intelligent database and service control function responsible for:
  - management of each subscriber's records and control of certain services (primarily those associated with incoming calls)
- It stores:
  - subscribers address, and service type
  - IMSI number
  - current location and forwarding address (i.e. the MSC/VLR currently serving the MS)
  - Authentication/ciphering keys
  - billing information

Visitor Location Register:

- VLR is an temporary, intelligent database and service control function
- Identifies subscribers inside the coverage of MSC
- It assigns temporary mobile subscriber identity (TMSI), which is used for communication (also to avoid use of IMSI on the air)

Visitor Location Register:

- Responsibilities of the VLR include:
  - executing supplementary service programs (outgoing calls barred)
  - initiating authentication and ciphering
  - initiating paging
  - mapping of various identities (MSISDN, IMSI, TMSI)
  - passing location information to HLR

Authentication Centre (AUC):

- AuC is an intelligent database concerned with the regulation of access to the network ensuring that services can be used only by those who are entitled to do so and that the access is achieved in a secure way.
- The principle is that the AuC and the SIM have a unique key for every subscriber which is used as the basis for generating a response
- Only the true SIM will be able to generate the correct response and thus gain access to the network.

AUC/EIR

- The AuC is generally integrated with the HLR and also EIR.
- Equipment Identity Register - another database that holds a list of ‘allowed’ equipment identities, i.e. ME numbers: white / grey / black lists

Mobile Station Identities:

- Mobile station has three identities
  - International Mobile Subscriber Identity (IMSI)
  - International Mobile Equipment Identity (IMEI)
  - Temporary Mobile Subscriber Identity (TMSI)

International Mobile Subscriber Identity (IMSI):

- IMSI is assigned to an MS at subscription time
- It uniquely identifies a given MS
- It contains 15 digits:
  - Mobile Country Code (MCC): 3 digits (home country)
  - Mobile Network Code (MNC): 2 digits (home GSM PLMN)
  - Mobile Subscriber Identification(MSIN) and National Mobile Subscriber Identity(NMSI):
    - Mobile Subscriber Identification Number (MSIC)
- 262 02 454 275 1010
- MCC = Germany, NMC = private operator

International Mobile Equipment Identity (*#06#)

- IMEI uniquely identifies the MS equipment
- Assigned by the equipment manufacturer
- It contains 15 digits
  - Type Approval Code (ATC) (6 digits)
  - Final Assembly Code (FAC) (2 digits)
  - Serial Number (SNR) (6 digits)
  - Spare (SP): 1 digit

Temporary Mobile Subscriber Identity (TMSI):

- TMSI is assigned to MS by the Visitor Location Register (VLR)
- TMSI uniquely identifies an MS within the area controlled by a given VLR
  - A maximum of 32 bits can be used for TMSI

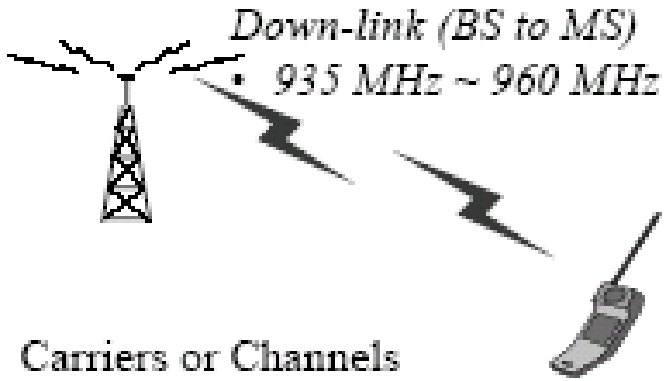
GSM Band and Time Slots:

- TDMA + FDMA + FDD
- 124 radio carriers, inter carrier spacing 200 KHz
- 890 to 915 MHz MS to BTS (UPLINK)
- 935 to 960 MHz BTS to MS (DOWNLINK)
- 8 channels/carrier

GSM 900 Frequency bands and Bandwidth:

- Frequency Bands and Bandwidth

GSM 900



Down-link (BS to MS)

- *935 MHz ~ 960 MHz (25 MHz Bandwidth)*

Up-link (MS to BS)

- *890 MHz ~ 915 MHz (25 MHz Bandwidth)*

Carriers or Channels

- Each up-link or down-link has 124 Carriers with a bandwidth of 200 KHz, excluding 2×100 KHz edges of the band
- The use of carrier 1 and 124 are optional for operators.

$$F_u = 890 .2 + 0.2 \times (N - 1)\ MHz$$

$$F_d = 935 .2 + 0.2 \times (N - 1)\ MHz \qquad N = 1, 2, \cdots, 124$$

FDMA/TDMA Structure:

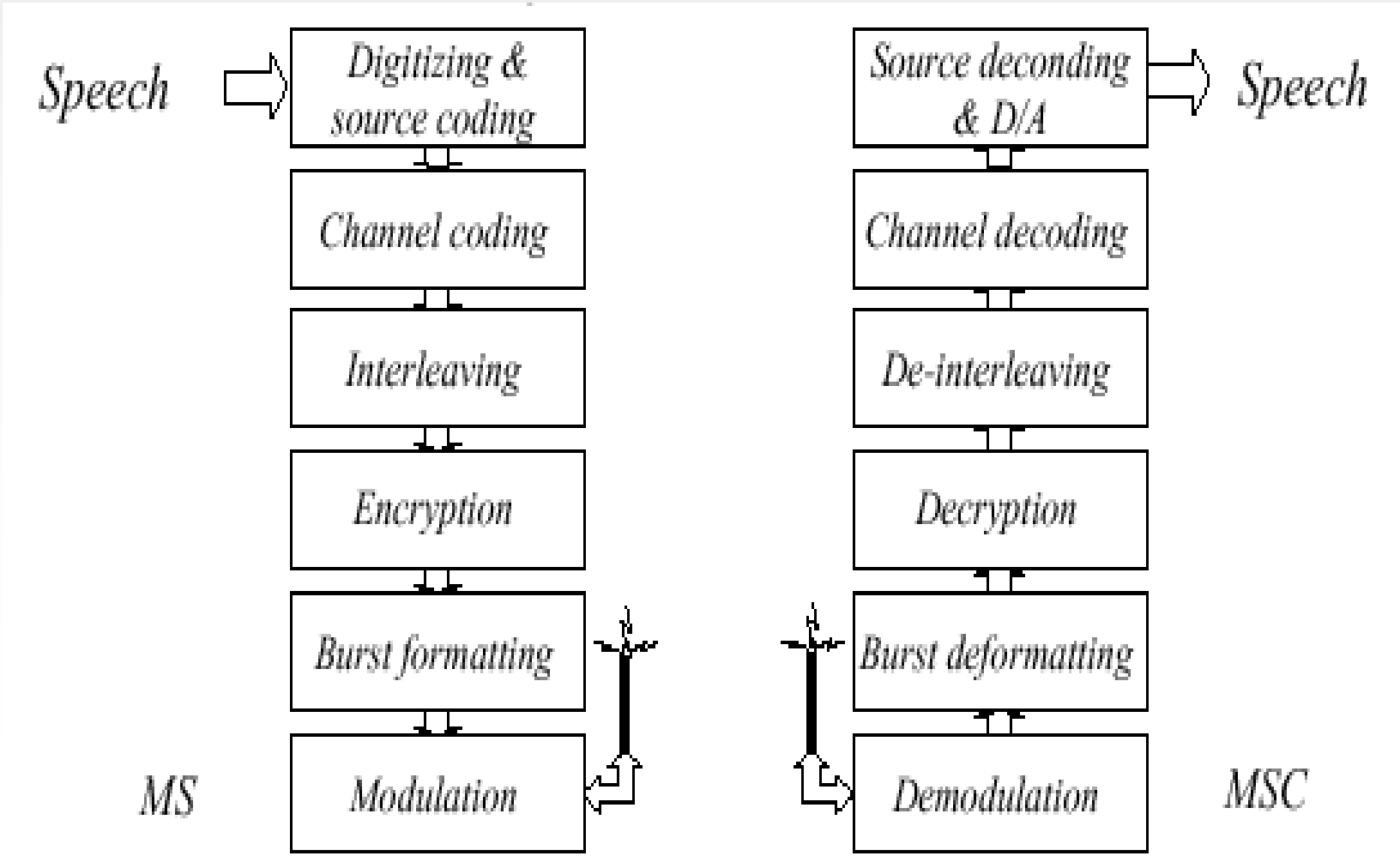
- FDMA/TDMA Structure
  - The total bandwidth is divided into 124×200 kHz bands (FDMA)
  - Each 200 kHz band can support maximum 8 users (TDMA)
  - The GSM can support up to 992 (124×8) simultaneous users with the full-rate speech coder.

	TS0	*TS1*	*TS2*	*TS3*	*TS4*	*TS5*	*TS6*	*TS7*
Freq. #1	Channel #1	Channel #2	Channel #3	Channel #4	Channel #5	Channel #6	Channel #7	Channel #8
Freq. #2	Channel #1	Channel #2	Channel #3	Channel #4	Channel #5	Channel #6	Channel #7	Channel #8
Freq. #124	Channel #1	Channel #2	Channel #3	Channel #4	Channel #5	Channel #6	Channel #7	Channel #8

GSM Handoffs

- Three types of handoffs
  - Intra-BSS: if old and new BTSs are attached to same base switching station
    - MSC is not involved
  - Intra-MSC: if old and new BTSs are attached to different base switching stations but within same MSC
  - Inter-MSC: if MSCs are changed

GSM System Block Diagram:



GSM Protocol Stack: