PART 3
Introduction to GSM

Lecture 3.0
History

History of wireless communication

- **1896: Marconi**
  - first demonstration of wireless telegraphy
  - tx of radio waves to a ship at sea 29 km away
  - long wave transmission, high power req. (200 kW and +)
- **1901: Marconi**
  - Telegraph across the atlantic ocean
  - Close to 3000 Km hop!
- **1907 Commercial transatlantic connections**
  - huge ground stations (30 by100m antennas)
- **1915: Wireless telephony established**
  - NY – S. Francisco
  - Virginia and Paris
- **1920 Marconi:**
  - Discovery of short waves (< 100m)
  - reflection at the ionosphere
  - (cheaper) smaller sender and receiver, possible due to the invention of the vacuum tube (1906, Lee DeForest and Robert von Lieben)

History of wireless communication

- ➔ **1920's: Radio broadcasting became popular**
- ➔ **1928: many TV broadcast trials**
- ➔ **1930's: TV broadcasting deployment**
- ➔ **1946: First public mobile telephone service in US**
  - ⇨ St. Louis, Missouri
  - ⇨ Single cell system
- ➔ **1960's: Bell Labs developed cellular concept**
  - ⇨ brought mobile telephony to masses
- ➔ **1960's: Communications satellites launched**
- ➔ **Late 1970's: technology advances enable affordable cellular telephony**
  - ⇨ entering the modern cellular era
- ➔ **1974-1978: First field Trial for Cellular System**
  - ⇨ AMPS, Chicago

Giuseppe Bianchi

1st generation mobile systems early deployment

- ➔ **First system:**
  - ⇨ NMT-450 (Nordic Mobile Telephone)
    - →Scandinavian standard; adopted in most of Europe
    - →450 MHZ band
    - →First european system (Sweden, october 1981)
- ➔ **Italian history:**
  - ⇨ 1966: first experiments (CSELT) at 160 MHZ
    - →RTMI (Radio Telefono Mobile Italiano)
    - →Market: 1973
  - ⇨ First italian cellular system: 1985
    - →RTMS (Radio Telefono Mobile di Seconda Generazione)
    - →450 MHZ
  - ⇨ Evolution: 1990, TACS
    - →Total Access Communication System
    - →900 MHZ

Giuseppe Bianchi

1st generation mobile systems

- **First generation: 1980's**
- **Several competing standards in different countries**
  - NMT (Nordic Mobile Telephone)
    - Scandinavian standard; adopted in most of Europe
    - First european system (Sweden, 1981)
  - TACS (Total Access Communication Systems), starts in 1985
    - UK standard; A few of Europe, Asia, Japan
  - AMPS (Advanced Mobile Phone Service)
    - US standard
  - C-Netz (Only in Germany)
  - Radiocom 2000 (Only in France)
- **Analog transmission**
  - Frequency modulation
- **Various bands:**
  - NMT:
    - 450 MHz first
    - 900 MHz later
  - TACS
    - 900 MHz
    - 1230 bidirectional channels (25KHz)
  - AMPS
    - 800 MHz
- **Today still in use in low-technology countries**
  - And not yet completely dismissed in high-tech countries

2nd generation mobile systems

- **4 systems**
  - Global System for Mobile (GSM)
  - Digital AMPS (D-AMPS), US
  - Code Division Multiple Access (IS-95) – Qualcomm,US
  - Personal Digital Cellular (PDC),Japan
- **GSM by far the dominant one**
  - Originally pan-european
  - Deployed worldwide
    - (slow only in US)
- **Basic bands:**
  - 900 MHz
  - 1800 MHz
    - (Digital Cellular System: DCS-1800)
  - 1900 MHz
    - (Personal Communication System:PCS-1900,US only)
- **Specifications for**
  - GSM-400 (large areas)
  - GSM-800 (north america)

Timing

- ➔ **1982: Start of GSM-specification in Europe (1982-1990)**
- ➔ **1983: Start of American AMPS widespread deployment**
- ➔ **1984 CT-1 standard (Europe) for cordless telephones**
- ➔ **1991 Specification of DECT**
  - ⇨ Digital European Cordless Telephone (today: Digital Enhanced Cordless Telecommunications)
  - ~100-500m range, 120 duplex channels, 1.2Mbit/s data transmission, voice encryption, authentication
- ➔ **1992: Start of GSM operation Europe-wide**
- ➔ **1994: DCS-1800**

2 ½ generation mobile systems

GSM incremental extension

- ➔ **High speed circuit switched data (HSCSD)**
  - ➔ Circuit switched data communication
  - ➔ Uses up to 4 slots (1 slot = 9.6 or 14.4 Kbps)
- ➔ **General Packet Radio Service (GPRS)**
  - ➔ Packet data (use spectrum only when needed!)
  - ➔ Up to 115 Kbps (8 slots)
- ➔ **Enhanced Data-rates for Global Evolution (EDGE)**
  - ➔ Higher data rate available on radio interface (3x)
    - » Up to 384 Kbps (8 slots)
    - » Thanks to new modulation scheme (8PSK)
    - » May coexist with old GMSK

3rd generation mobile systems

- **UMTS (Universal Mobile TelecommunicationSystem)**
  - ITU standard: IMT-2000 (International Mobile Telecommunication – 2000)
  - UMTS forum created in 1996
  - Later on 3GPP forum (bears most of standardization activities)
- Wideband CDMA radio interface
  - But several other proposals accepted as "compatible"
- Radio spectrum: 1885-2025 & 2110-2200 MHz
- Already deployed in Japan
- Time to market in Italy: 2004?

Facts about wireless communication

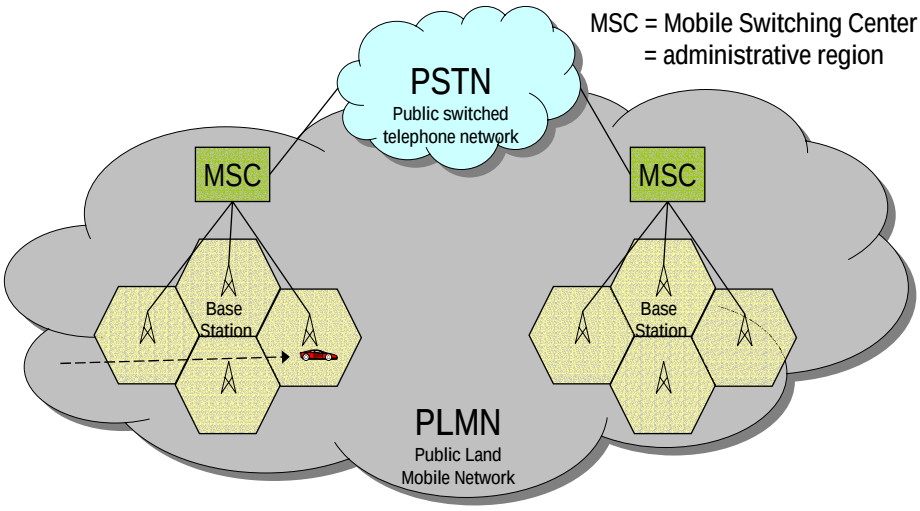
- **Who has a cellular phone?**
  - USA: Over 50% of US households
  - Italy: from 2001, more wireless lines than wired
  - World: from march 2002, 1 billion wireless cellular users
    - Much faster than projections!
    - August 2000: 372 GSM networks, 362M customers
- **Revenues:**
  - global revenue from wireless portals predicted to grow from $700M to $42 billion by 2005
  - WLAN revenues predicted at $785M by 2004
  - Forecasting a 59 percent growth rate for wireless usage in rural areas between 2000 and 2003

PART 3
Introduction to GSM

Lecture 3.1
Architecture and components

Giuseppe Bianchi

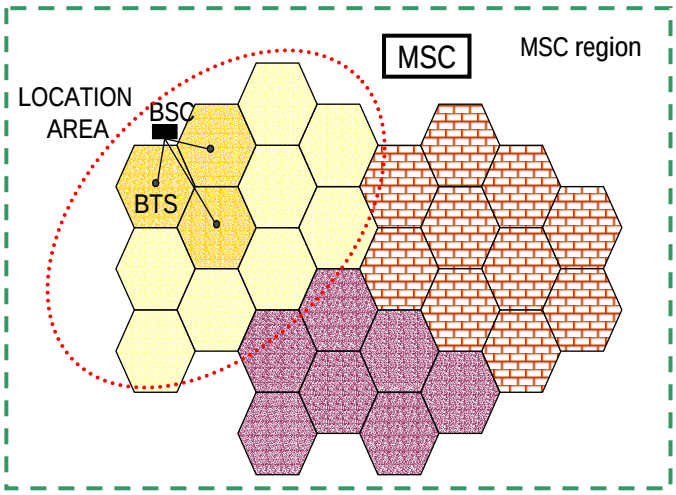
GSM Network
high-level view



MSC role: telephone switching central with special mobility management capabilities

Giuseppe Bianchi

GSM system hierarchy

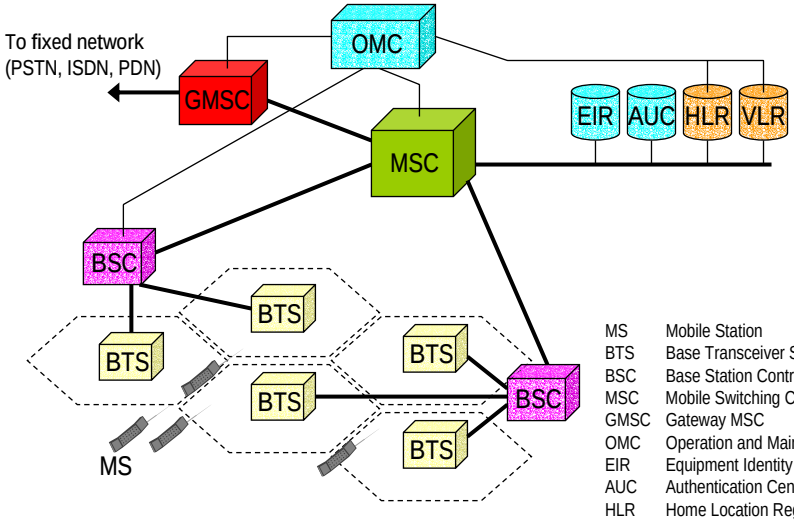


MSC: Mobile Switching Center
LA: Location Area
BSC: Base Station Controller
BTS: Base Transceiver Station

Hierarchy: MSC region → n x Location Areas → m x BSC → k x BTS

Giuseppe Bianchi

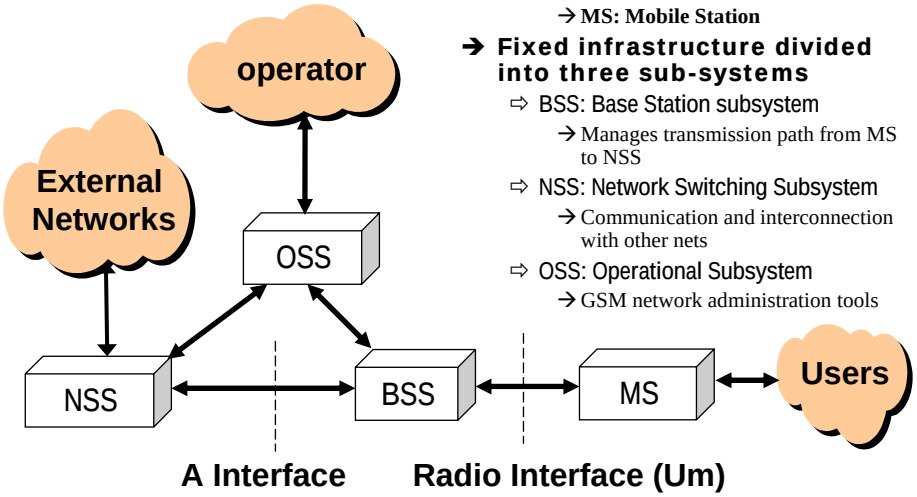
GSM essential components



MS	Mobile Station
BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
GMSC	Gateway MSC
OMC	Operation and Maintenance Center
EIR	Equipment Identity Register
AUC	Authentication Center
HLR	Home Location Register
VLR	Visitor Location Register

Giuseppe Bianchi

GSM Sub-Systems



- **Two components:**
  - *Fixed installed infrastructure*
    - The network in the proper sense
  - *Mobile subscribers*
    - **MS: Mobile Station**
- **Fixed infrastructure divided into three sub-systems**
  - BSS: Base Station subsystem
    - Manages transmission path from MS to NSS
  - NSS: Network Switching Subsystem
    - Communication and interconnection with other nets
  - OSS: Operational Subsystem
    - GSM network administration tools

Giuseppe Bianchi

PART 3
Introduction to GSM

Lecture 3.2
Mobile Station and addresses

Giuseppe Bianchi

Mobile Station (MS)

GSM separates user mobility from equipment mobility, by defining two distinct components

➔ **Mobile Equipment**

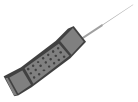
- ➔The cellular telephone itself (or the vehicular telephone)
- ⇨Address / identifier:
  - ➔IMEI (International Mobile Equipment Identity)

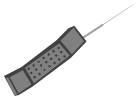
➔ **Subscriber Identity Module (SIM)**

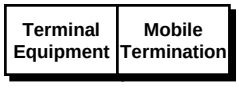
- ➔Fixed installed chip (plug-in SIM) or
- ➔exchangeable card (SIM card)
- ⇨Addresses / identifiers:
  - ➔IMSI (International Mobile Subscriber Identity)
  - ➔MSISDN (Mobile Subscriber ISDN number)
    - » the telephone number!

Giuseppe Bianchi

Mobile Equipment structure



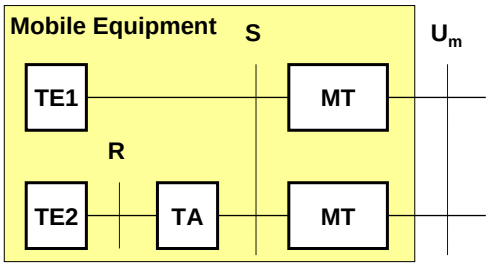




➔ **Mobile Termination** functions
- ⇨ tRadio interface (tx, rx, signalling)

➔ **Terminal Equipment** functions
- ⇨ User interface (microphone, keyboard, speakers, etc);
- ⇨ Functions specific of services (telephony, fax, messaging, etc), independent of GSM

➔ **Terminal Adaptor** functions
- ⇨ Interfaces MT with different types of terminals (PCs, Fax, etc.)



Giuseppe Bianchi

Mobile Equipment Max Power

5 power classes

CLASS	max power (watt)	Type of terminal
I	20	vehicular
II	8	vehicular
III	5	portable
IV	2	portable
V	0.8	portable

Normally used

This was for 900 MHz – for 1800 MHz only two classes: 1W, and 0.25 W

IMEI

International Mobile Equipment Identity

- **Uniquely identifies the mobile equipment**
- **15 digits hierarchical address**
- **assigned to ME during manifacturing and "type approval" testing**
  - ⇨ Type approval procedure: guarantees that the MS meets a minimum standard, regardless of the manifacturer
- **IMEI structure:**

TAC – 6 digits (Type Approval Code)	FAC – 2 digits (Final Assembly Code)	SNR – 6 digits (Serial Number)	SP – 1 digit (Spare Digit)
centrally assigned upon type approval	assigned by manufacturer Identifies place where ME was assembled or manufactured	assigned by manufacturer Unique for given TAC+FAC combination	Additional digit available

IMEI management

- **Protection against stolen and malfunctioning terminals**
- **Equipment Identity Register (EIR): 1 DataBase for each operator; keeps:**
  - WHITE LIST:
    - valid IMEIs
    - Corresponding MEs may be used in the GSM network
  - BLACK LIST:
    - IMEIs of all MEs that must be barred from using the GSM network
    - Exception: emergency calls (to a set of emergency numbers)
    - Black list periodically exchanged among different operators
  - GRAY LIST:
    - IMEIs that correspond to MEs that can be used, but that, for some reason (malfunctioning, obsolete SW, evaluation terminals, etc), need to be tracked by the operator
    - A call from a "gray" IMEI is reported to the operator personnel

Giuseppe Bianchi

SIM card

Subscriber Identity Module

- **Uniquely associated to a user**
  - Not to an equipment, as in first generation cellular networks
- **Stores user addresses**
  - IMSI
  - MSISDN
  - Temporary addresses for location, roaming, etc
- **authentication and encryption features**
  - All security features of GSM are stored in the SIM for maximum protection
    - subscriber's secret authentication key (*Ki)*
    - Authentication algorithm ("secret" algorithm - A3 – not unique)
    - Cipher key generation algorithm (A8)
- **Personalization**
  - SIM stores user profile (subscribed services)
  - RAM available for SMS, short numbers, user's directory, etc
  - Protection codes
    - PIN (Personal Identification Number, 4-8 digits)
    - PUK (PIN Unblocking Key, 8 digits)

Giuseppe Bianchi

IMSI

International Mobile Subscriber Identity

- ➔ **Uniquely identifies the user (SIM card)**
- ➔ **GSM-specific address**
  - ⇨ unlike MSISDN - normal phone number
- ➔ **15 digits hierarchical address**
- ➔ **assigned by operator to SIM card upon subscription**
- ➔ **IMSI structure:**

MCC – 3 digits (Mobile Country Code)	MNC – 2 digits (Mobile Network Code)	MSIN – max 10 digits (Mobile Subscriber Identification Number)
Internationally standardized; identifies operator country Italy: 222	Identifies operator network (PLMN) within country TIM=01 OMNI=10 WIND=88 BLU=98	Uniquely identifies subscriber in the operator network

Giuseppe Bianchi

MSISDN

Mobile Subscriber ISDN Number

- ➔ **MSISDN: the "usual" telephone number**
  - ⇨ Follows international ISDN numbering plan (ITU-T E.164 recommendations)
  - ⇨ Structure:

CC – up to 3 digits (Country Code)	NDC – 3 digits (for PLMN) (National Destination Code)	SN – max 10 digits (Subscriber Number)

- ➔ **GSM is the first network to distinguish**
  - ⇨ The user identity (i.e. IMSI)
  - ⇨ From the number to dial (i.e. MSISDN)
- ➔ **Separation IMSI-MSISDN protects confidentiality**
  - ⇨ IMSI is the real user address: never public!
  - ⇨ Faking false identity: need signal IMSI to the network; but IMSI hard to obtain!
- ➔ **Separation IMSI-MSISDN allows**
  - ⇨ Easy modification of numbering and routing plans
- ➔ **single IMSI may be associated to several MSISDN numbers**
  - ⇨ E.g. different services (fax, voice, data, etc) may be associated with different MSISDN numbers

Giuseppe Bianchi

Temporary addresses

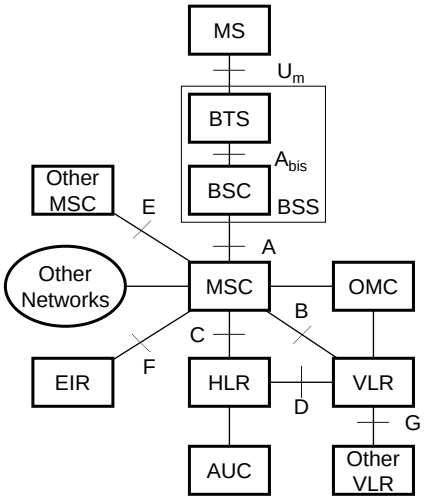
➔ **TMSI - Temporary Mobile Subscriber Identity**
- ⇨ 32 bits
- ⇨ assigned by VLR within an administrative area
  - →has significance only in this area
- ⇨ transmitted on the radio interface instead of IMSI
  - → reduces problem of "eavesdropping"

➔ **MSRN - Mobile Station Roaming Number**
- ⇨ An MSISDN number
  - →CC, NDC of the visited network
  - →SN assigned by VLR
- ⇨ Used to route calls to a roaming MS
  - →Subscriber Number (SN) assigned to provide routing information towards actually responsible MSC

PART 3
Introduction to GSM

Lecture 3.3
Fixed Infrastructure

Components and interfaces



Components

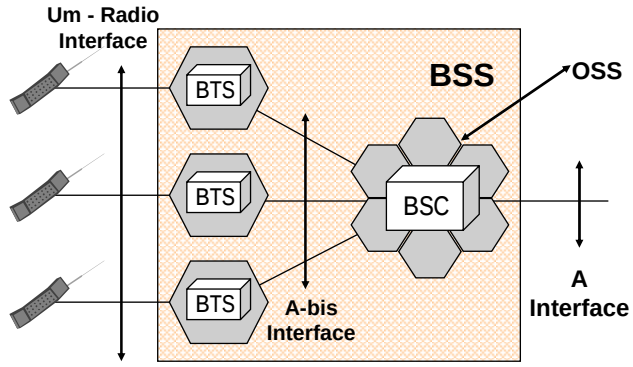
MS	Mobile Station
BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
OMC	Operation and Maintenance Center
EIR	Equipment Identity Register
AUC	Authentication Center
HLR	Home Location Register
VLR	Visitor Location Register

Interfaces

Um	Radio Interface
Abis	BTS-BSC
A	BSS-MSC
B	MSC-VLR
C	MSC-VLR
D	HLR-VLR
E	MSC-MSC
F	MSC-EIR
G	VLR-VLR

Giuseppe Bianchi

Base Station Sub-System



⇨Base Transceiver Station (BTS)

→Transmitter and receiver devices, voice coding & decoding, rate adaptation for data

→Provides signaling channels on the radio interface

→Limited signal and protocol processing (error protection coding, link layer LAPDm)

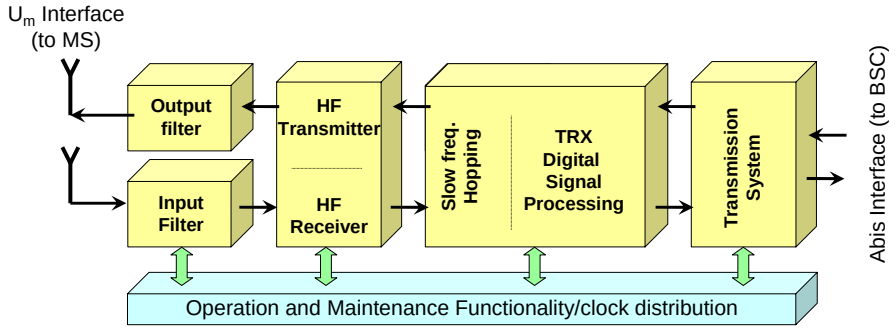
⇨Base Station Controller (BSC)

→performs most important radio interface management functions:

→Radio channels allocation and deallocation; handover management; …

Giuseppe Bianchi

Base Transceiver Station - BTS



TRX radio interface functions:
- GMSK modulation-demodulation
- channel coding
- encryption/decryption
- burst formatting, interleaving
- signal strength measurements
- interference measurements

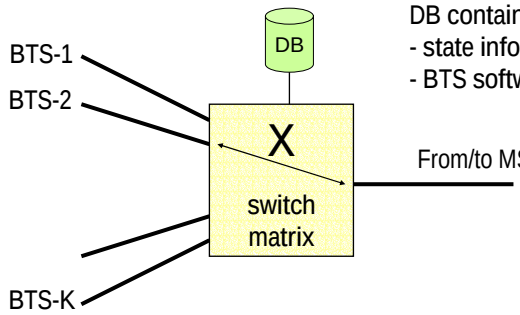
In essence, BTS is a complex modem!

BTS – maximum power

➔ **GSM 900**
- ⇨ 320 W
- ⇨ 160 W
- ⇨ 80 W
- ⇨ 40 W
- ⇨ 20 W
- ⇨ 10 W
- ⇨ 5 W
- ⇨ 2.5 W
- ⇨ 0.25 W (micro-BTS)
- ⇨ 0.08 W (micro-BTS)
- ⇨ 0.03 W (micro-BTS)

➔ **DCS 1800**
- ⇨ 20 W
- ⇨ 10 W
- ⇨ 5 W
- ⇨ 2.5 W
- ⇨ 1.6 W (micro-BTS)
- ⇨ 0.5 W (micro-BTS)
- ⇨ 0.16 W (micro-BTS)

Base Station Controller - BSC



DB contains
- state information for all BSS
- BTS software

From/to MSC

FUNCTIONS:

- ➔ **switch calls from MSC to correct BTS**
  - ⇨ and conversely
- ➔ **Protocol and coding conversion**
  - ⇨ for traffic (voice) & signaling (GSM-specific to ISDN-specific)
- ➔ **Manage MS mobility**
- ➔ **Enforce power control**

1 BSC may control
up to 40 BTS

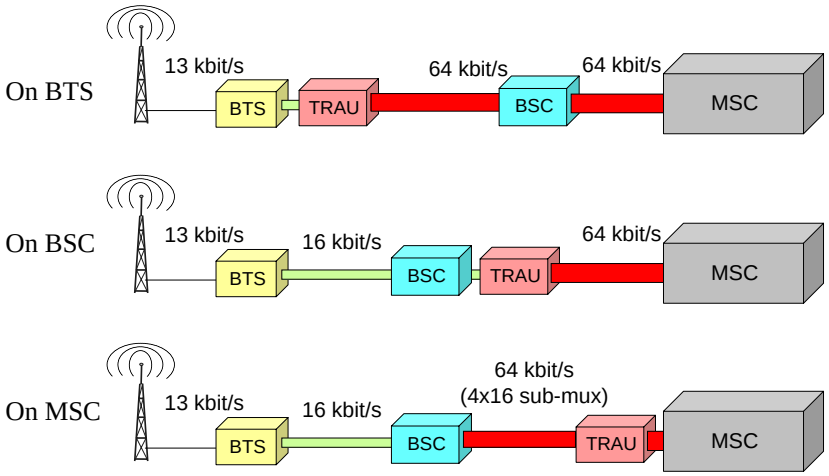
Transcoding and Rate Adaptation

BTS:
-collects speech traffic
-Deciphers and removes error protection
-Result:
-13 kbps air-interface GSM speech-coded signal
MSC:
-A modified ISDN switch
-Needs to receive ISDN-coded speech
-64 kbps PCM format (A-law)

⇨ Transcoding and Rate Adaptation Unit (TRAU) needed!

Rationale: re-use existing ISDN switches & protocols

TRAU possible placements



Why 16 kbps instead of 13? Inband signalling needed for BTS control of TRAU (TRAU needs to receive synchro & decoding information from BTS)

Giuseppe Bianchi

Network Switching Sub-System

➔ **Elements:**
- ⇨ Mobile Switching Center (MSC) / Gateway MSC (GMSC)
- ⇨ Home Location Register (HLR) / Authentication Center (AuC)
- ⇨ Visitor Location Register (VLR)
- ⇨ Equipment Identity Register (EIR)

➔ **Functions:**
- ⇨ Call control
- ⇨ User management

➔ **Inter-component communication**
- ⇨ Via SS7 signalling network
- ⇨ With suitable extensions (e.g. MAP – Mobile Application Part)

Giuseppe Bianchi

Mobile Switching Center - MSC

- ➔ **An ISDN switch (64 kbps channels)**
- ➔ **Performs all the switching and routing functions of a fixed network switching node**
- ➔ **PLUS specific mobility-related functions:**
  - ⇨ Allocation and administration of radio resources
  - ⇨ Management of mobile users
    - →registration, authentication
    - →handover execution and control
    - →paging
- ➔ **A PLMN (operator network) has, in general, many MSC**
  - ⇨ Each MSC is responsible of a set of BSS
    - →(note: a BSS refers to just 1 MSC, not many)

Giuseppe Bianchi

Home Location Register - HLR

- ➔ **1 database per operator (PLMN)**
  - ⇨ In principle; in practice may be
    - →N-plicated for reliability reasons
    - →In large operator networks, there may be 2+ HLR with distinct information, although MSISDN-HLR association needs to be introduced (e.g. first two digits of the Subscriber Number)
- ➔ **HLR entries:**
  - ⇨ Every user / MSISDN that has subscribed to the operator
- ➔ **Stores:**

➔ **Permanent information associated to the user**
- ⇨ IMSI, MSISDN
- ⇨ Services subscribed
- ⇨ Service restrictions (e.g. roaming restrictions)
- ⇨ Parameters for additional services
- ⇨ info about user equipment (IMEI)
- ⇨ Authentication data

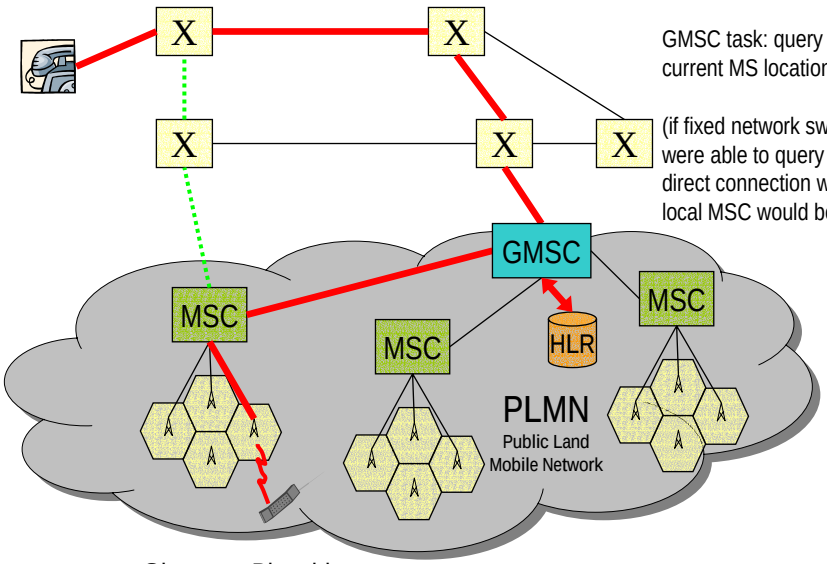
➔ **Temporary information associated to the user**
- ⇨ Link to current location of the user:
  - →Current VLR address (if avail)
  - →Current MSC address (if avail)
  - →MSRN (if user outside PLMN)

Giuseppe Bianchi

Authentication Center - AUC

- **Associated to HLR**
  - Eventually integrated with HLR
- **Search key: IMSI**
- **Responsible of storing security-relevant subscriber data**
  - Subscriber's secret key Ki (for authentication)
  - Encryption key user on the radio channel (Kc)
  - Algorithms to compute volatile keys used during authentication process

Gateway MSC – GMSC



Needed, as fixed network switches are not mobile capable!!

GMSC task: query HLR for current MS location

(if fixed network switches were able to query HLR, direct connection with local MSC would be available)

Visitor Location Register - VLR

➔ **At most 1 database per MSC**
- ⇨ Generally, joint MSC-VLR implementation
  - →No need to carry heavy MSC-VRL signalling load on network links
- ⇨ but 1 VLR may serve many MSCs

➔ **VLR entries:**
- ⇨ Every user / MSISDN actually staying in the administrative area of the associated MSC
  - →Entry created when an MS enters the MSC area (registration)
- ⇨ NOTE: may store data for roaming users (subscribed to different operators)

➔ **Stores:**

➔ **Subscriber and subscription data**
- ⇨ IMSI, MSISDN
- ⇨ Parameters for additional services
- ⇨ info about user equipment (IMEI)
- ⇨ Authentication data

➔ **Tracking and routing information**
- ⇨ Mobile Station Roaming Number (MSRN)
- ⇨ Temporary Mobile Station Identity (TMSI)
- ⇨ Location Area Identity (LAI) where MS has registered
  - →Used for paging and call setup

Operation & Maintenance Sub-system (OSS)

➔ **Network measurement and control functions**

➔ **Monitored and initiated from the OMC (Operation and Maintenance Center)**

➔ **Basic functions**
- ⇨ Network Administration
  - →configuration, operation, performance management, statistics collection and analysis, network maintenance
- ⇨ Commercial operation & charging
  - →Accounting & billing
- ⇨ Security Management
  - →E.g. Equipment Identity Register (EIR) management

O&M functions based on ITU-T TMN standards (Telecommunication Network Management) – complex topic out of the scopes of this course