Wireless Networks

Lecture 24:
Cellular: 1G, 2G, and 3G

Peter Steenkiste
CS and ECE, Carnegie Mellon University

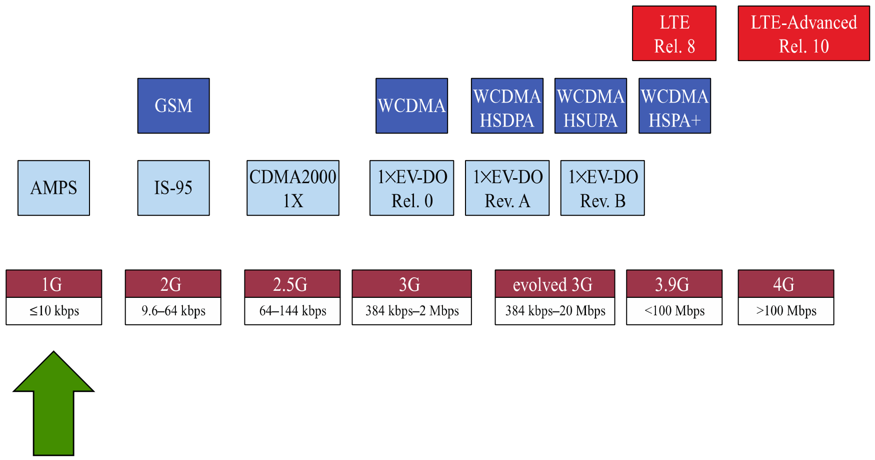
Peking University, Summer 2016

Outline

- 1G: AMPS
- 2G: GSM
- 2.5G: EDGE, CDMA
- 3G: WCDMA

Some slides based on material from
“Wireless Communication Networks and Systems”
© 2016 Pearson Higher Education, Inc.

Evolution of Cellular Wireless Systems



LTE Rel. 8

LTE-Advanced Rel. 10

GSM

WCDMA

WCDMA HSDPA

WCDMA HSUPA

WCDMA HSPA+

AMPS

IS-95

CDMA2000 1X

1×EV-DO Rel. 0

1×EV-DO Rev. A

1×EV-DO Rev. B

1G	2G	2.5G	3G	evolved 3G	3.9G	4G
≤10 kbps	9.6–64 kbps	64–144 kbps	384 kbps–2 Mbps	384 kbps–20 Mbps	<100 Mbps	>100 Mbps

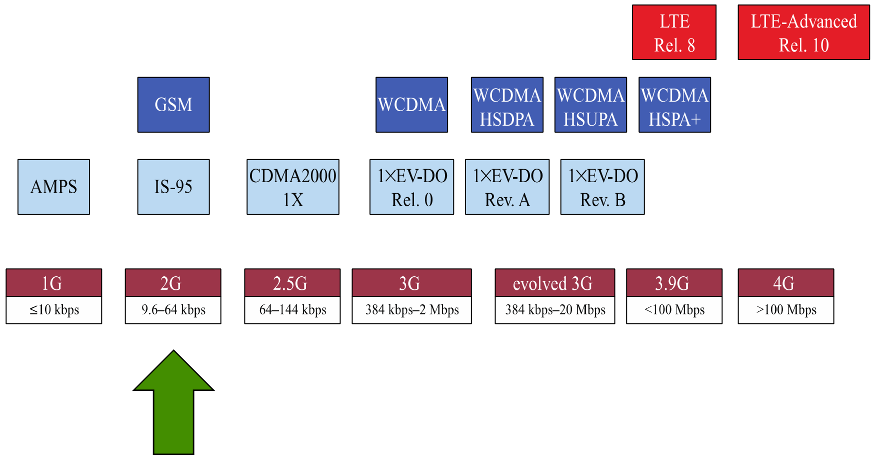
Advanced Mobile Phone Service (AMPS)

- In North America, two 25-MHz bands were allocated (DL: 869-894 MHz, UP: 824-849 MHz)
  - » Deployed since early 80's by two providers
- Channels are spaced by 30 KHz, allowing for 416 channels (21 control, 395 for voice calls)
  - » Control channels are full duplex data channels at 10 Kbps
  - » Includes preamble, word sync, and Digital Color Code identifying the base station
  - » Can send urgent control in data channels
- Conversations carried in analog using frequency modulation
  - » Effectively extends analog telephone over wireless
- Cell size = 2-20Km, frequency reuse is exploited

AMPS Operation

- When unit wakes up, it sends telephone and serial number to the Mobile Telephone Switching Office (MTSO) over control channel
  - » Both stored in read-only memory
  - » Used for billing purposes and to detect stolen phones
- Steps in placing a call:
  1. User dials in a number – sent to the MTSO
  2. MTSO verifies validity of service request
  3. MTSO notifies user of channels to use for up/down link
  4. MTSO sends ring signal to the called party
  5. MTSO completes circuit when party picks up
  6. When either party hangs up, MTSO releases circuit and wireless channels, and completes billing

Evolution of Cellular Wireless Systems



LTE Rel. 8

LTE-Advanced Rel. 10

GSM

WCDMA

WCDMA HSDPA

WCDMA HSUPA

WCDMA HSPA+

AMPS

IS-95

CDMA2000 1X

1×EV-DO Rel. 0

1×EV-DO Rev. A

1×EV-DO Rev. B

1G ≤10 kbps

2G 9.6–64 kbps

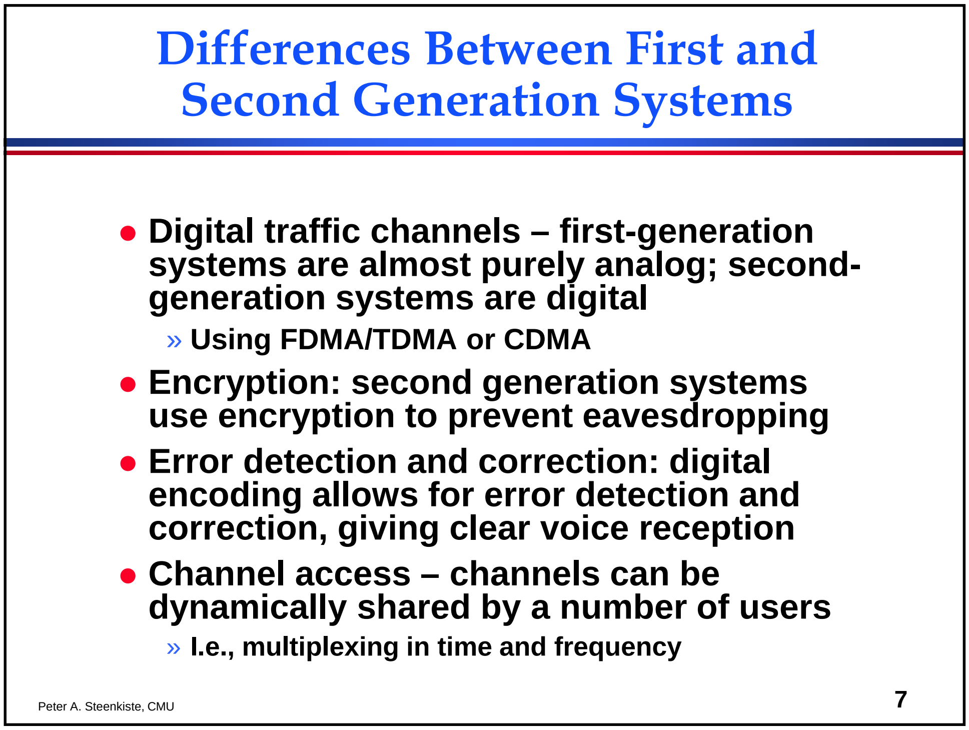
2.5G 64–144 kbps

3G 384 kbps–2 Mbps

evolved 3G 384 kbps–20 Mbps

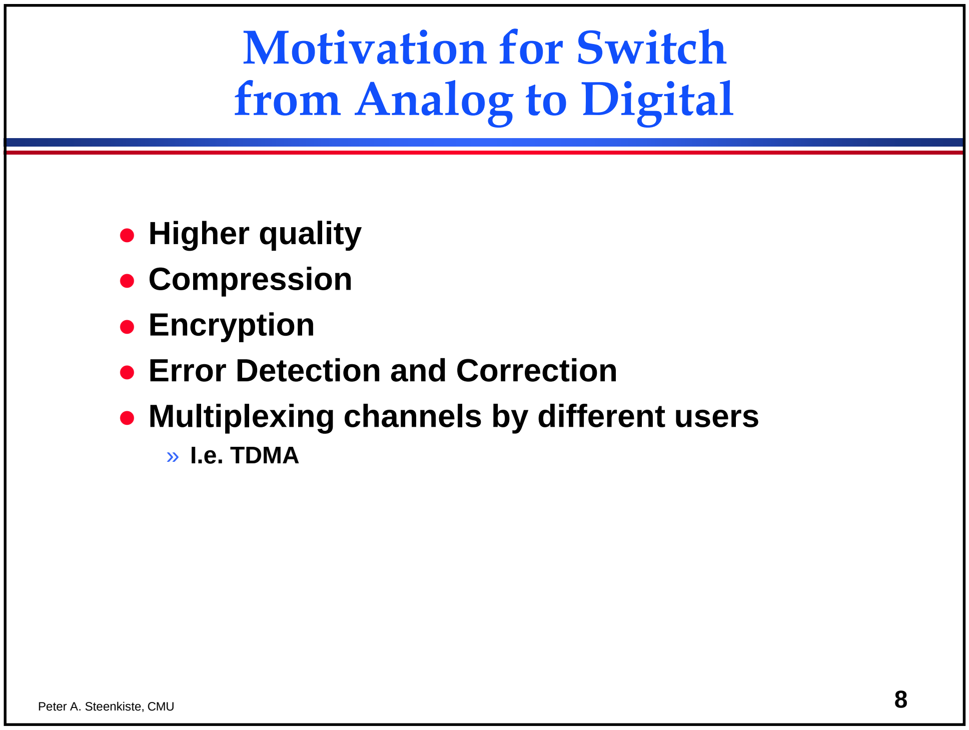
3.9G <100 Mbps

4G >100 Mbps



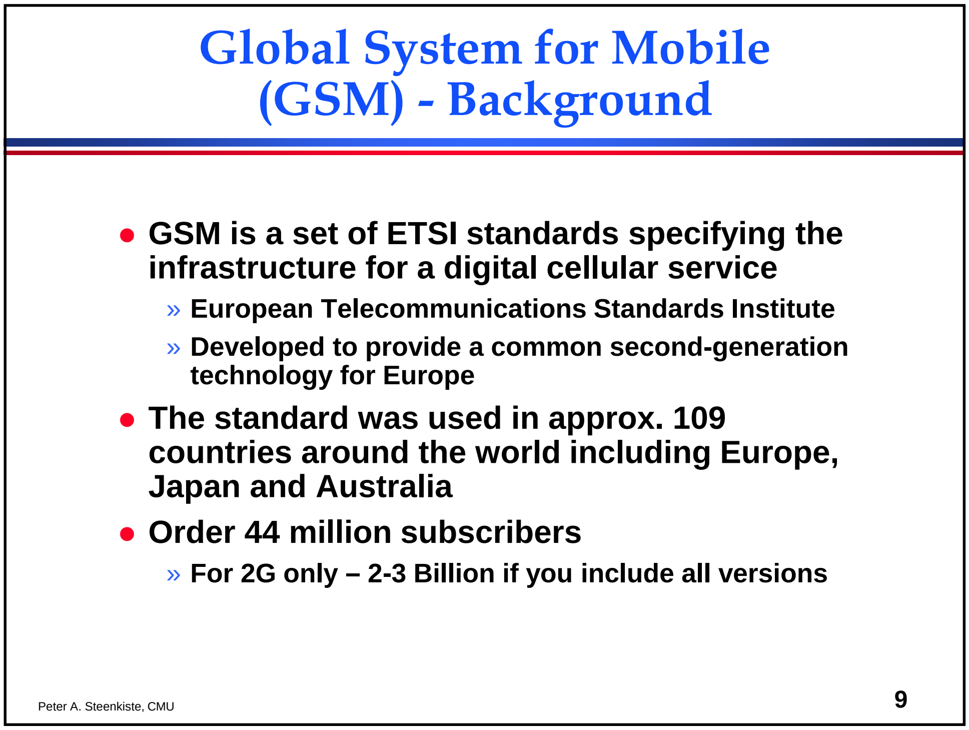
Differences Between First and Second Generation Systems

- Digital traffic channels – first-generation systems are almost purely analog; second-generation systems are digital
    - » Using FDMA/TDMA or CDMA
- Encryption: second generation systems use encryption to prevent eavesdropping
- Error detection and correction: digital encoding allows for error detection and correction, giving clear voice reception
- Channel access – channels can be dynamically shared by a number of users
    - » I.e., multiplexing in time and frequency



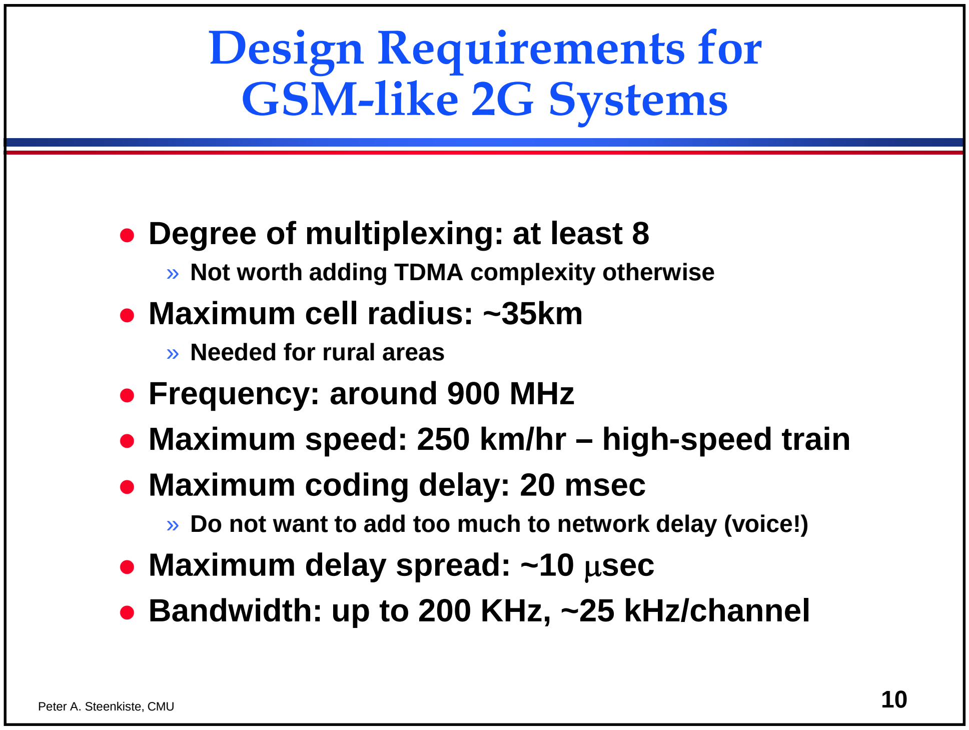
Motivation for Switch from Analog to Digital

- Higher quality
- Compression
- Encryption
- Error Detection and Correction
- Multiplexing channels by different users
    - » I.e. TDMA



Global System for Mobile (GSM) - Background

- GSM is a set of ETSI standards specifying the infrastructure for a digital cellular service
  - » European Telecommunications Standards Institute
  - » Developed to provide a common second-generation technology for Europe
- The standard was used in approx. 109 countries around the world including Europe, Japan and Australia
- Order 44 million subscribers
  - » For 2G only – 2-3 Billion if you include all versions



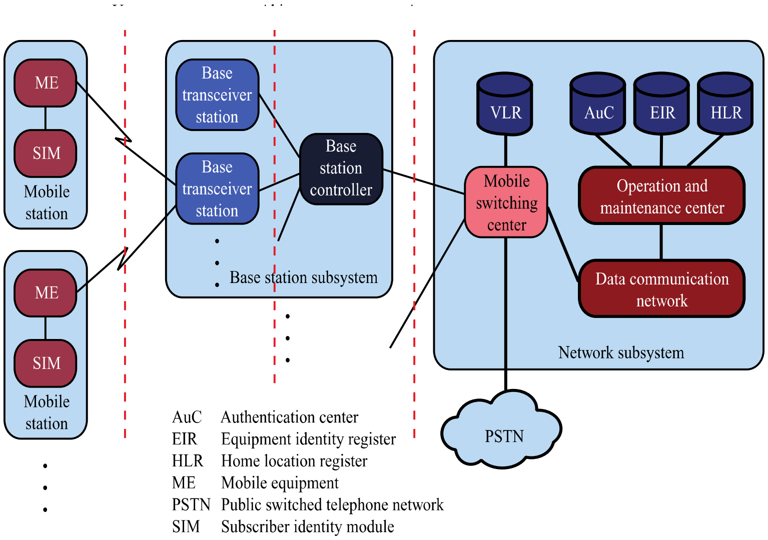
Design Requirements for GSM-like 2G Systems

- Degree of multiplexing: at least 8
  - » Not worth adding TDMA complexity otherwise
- Maximum cell radius: ~35km
  - » Needed for rural areas
- Frequency: around 900 MHz
- Maximum speed: 250 km/hr – high-speed train
- Maximum coding delay: 20 msec
  - » Do not want to add too much to network delay (voice!)
- Maximum delay spread: ~10 μsec
- Bandwidth: up to 200 KHz, ~25 kHz/channel

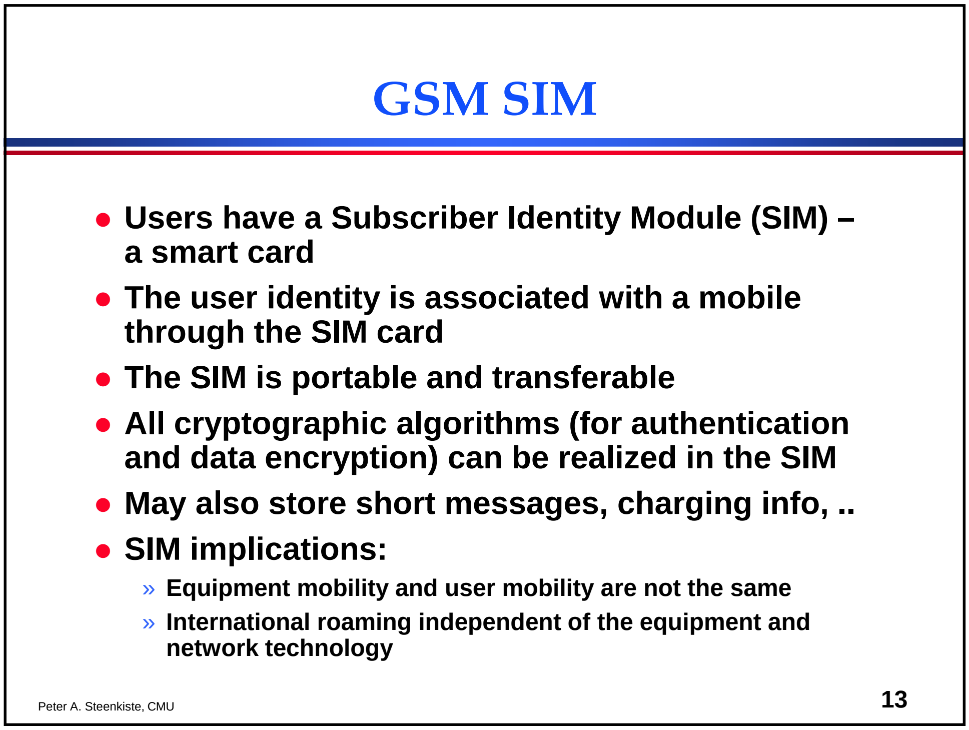
GSM Features

- Hybrid FDMA/TDMA approach
- Mobile station communicates across the air interface with base station in the same cell as mobile unit
- Mobile equipment (ME) – physical terminal, such as a telephone or PCS
  - » ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)
- GSM subscriber units are generic until a SIM is inserted
  - » SIMs roam since they are based on single standard
  - » Not necessarily the case for subscriber devices – may use different versions of the protocol

Global GSM System

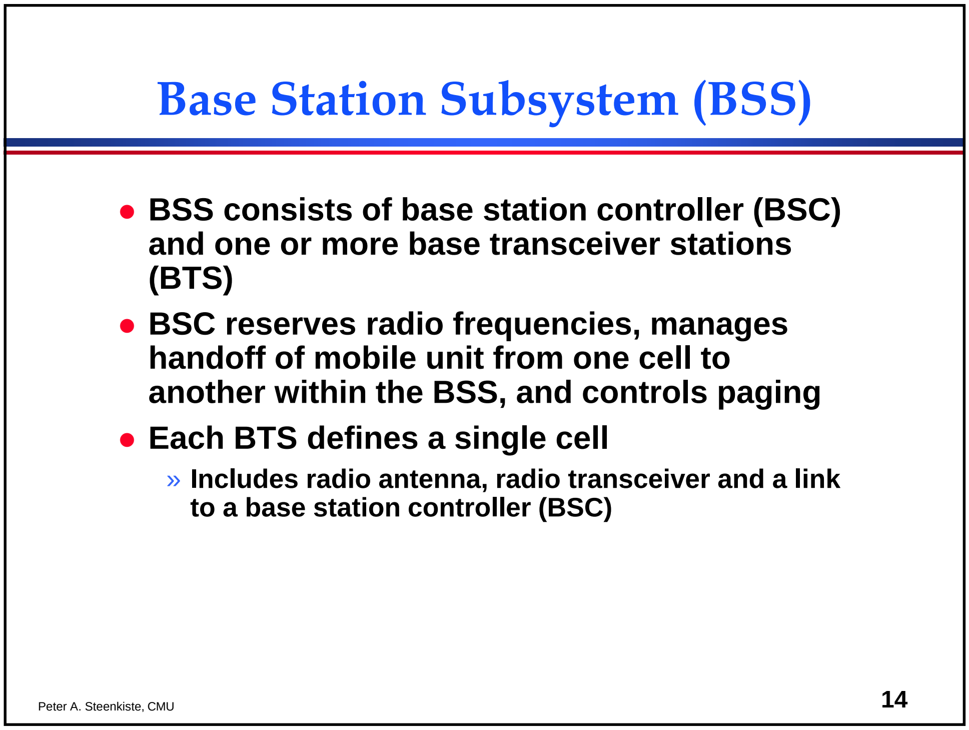


AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
ME	Mobile equipment
PSTN	Public switched telephone network
SIM	Subscriber identity module
VLR	Visitor location register



GSM SIM

- Users have a Subscriber Identity Module (SIM) – a smart card
- The user identity is associated with a mobile through the SIM card
- The SIM is portable and transferable
- All cryptographic algorithms (for authentication and data encryption) can be realized in the SIM
- May also store short messages, charging info, ..
- SIM implications:
  - » Equipment mobility and user mobility are not the same
  - » International roaming independent of the equipment and network technology

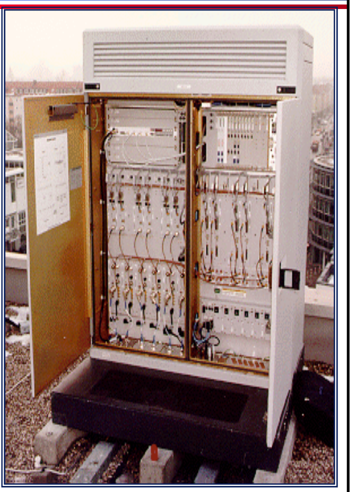


Base Station Subsystem (BSS)

- BSS consists of base station controller (BSC) and one or more base transceiver stations (BTS)
- BSC reserves radio frequencies, manages handoff of mobile unit from one cell to another within the BSS, and controls paging
- Each BTS defines a single cell
  - » Includes radio antenna, radio transceiver and a link to a base station controller (BSC)

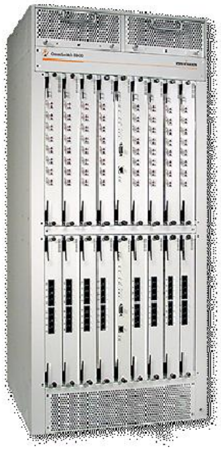
Base Transceiver Station

- Radio transmission/reception management (modulation/demodulation, equalisation, interleaving ...)
- Physical layer management (TDMA transmission, SFH, coding, ciphering ...)
- Link layer management
- Received signal quality and power measurement



Base Station Controller

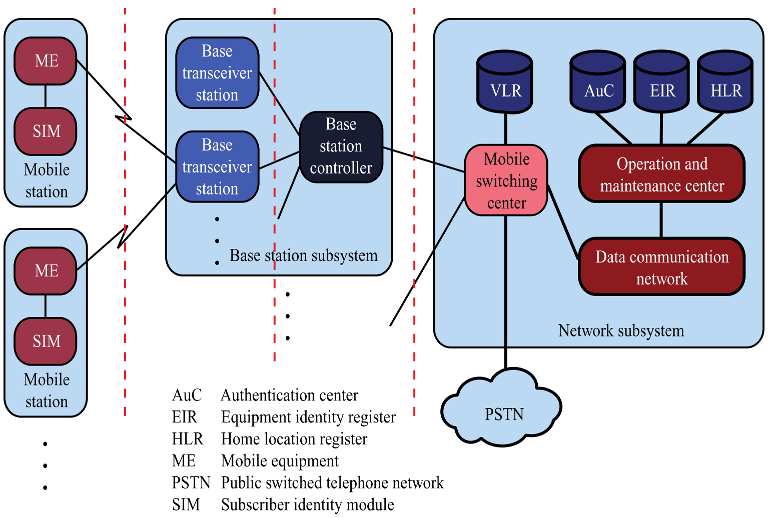
- Interface between MSC and BTSs
  - Forwarding of traffic
  - Coordination of and with BTSs
- Radio resource management for the Base Station Subsystem
  - Channel allocation
  - BTS measures processing
  - BTS and MS power control
  - Handover
  - ...



Network Subsystem (NS)

- NS provides link between cellular network and public switched telecommunications networks (PSTN)
  - » Controls handoffs between cells in different Base Station Subsystems
  - » Authenticates users and validates accounts
  - » Enables worldwide roaming of mobile users
- Central element of NS is the Mobile Switching Center (MSC)

Global GSM System



AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
ME	Mobile equipment
PSTN	Public switched telephone network
SIM	Subscriber identity module
VLR	Visitor location register

Mobile Switching Center

- Management of the communication between mobiles and the fixed network
  - The Gateway Mobile Switching Controller forms the gateway for calls to and from external networks
- MSC is also responsible for mobility management
  - Handover between Base Station Subsystems
  - Roaming across networks

Handover

- Executed by BSC (channels) and by MSC (routing)
- Initiated by base station:
  - » BS monitors the signal coming from the MT
  - » Low signal => HO! Need to do handover
- Mobile-terminal aided
  - » BS transmit beacon
  - » MT, hearing better beacon, request join
    - – Sends the identity of the old BS to the new BS
  - » BS accepts the MT, calls are then forwarded
- Inter-system system handover is managed MSC
  - » With extra connections to the HLR/VLR

Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to this MSC
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

Home Location Register

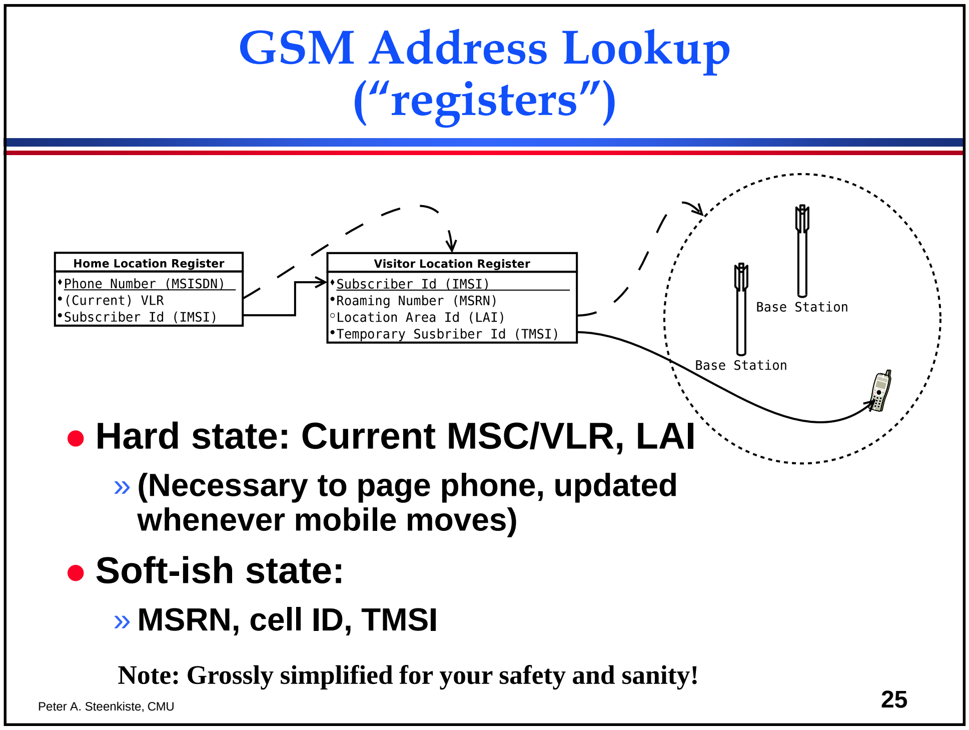
- One per “Public Land Mobile Network”
  - Basically an operator
- Contains entries for every subscriber and every mobile ISDN number that is homed in the respective network
- Permanent subscriber data and relevant temporary information
- Current location of the mobile station
- All administrative activities of the subscriber happen here!

Visitor Location Register

- One per MSC
- Stores data on all mobile stations which are currently in the administrative area of the respective MSC
- 1 VLR could be responsible for more than 1 MSC
- A roaming MS may be registered in a VLR of its home network or the foreign network depending on its location
- MS registers upon entering a LA. The MSC passes the identity of the MS and LAI to VLR

GSM Addressing Hierarchy

- Device
  - » IMEI (International Mobile Equipment Identifier)
- User
  - » IMSI (International Mobile Subscriber Identifier)
  - » MSISDN (Mobile Subscriber IDSN Number)
    - – “Real phone number”
  - » MSRN (Mobile Station Roaming Number)
  - » TMSI (Temporary Mobile Subscriber Identity
  - » LMSI (Local Mobile Subscriber Identity)
- Other
  - » LAI (Location Area Identity)
  - » CI (Cell Identity)



GSM Address Lookup (“registers”)

Home Location Register
- Phone Number (MSISDN)
- (Current) VLR
- Subscriber Id (IMSI)

Visitor Location Register
- Subscriber Id (IMSI)
- Roaming Number (MSRN)
- Location Area Id (LAI)
- Temporary Susbriber Id (TMSI)

Base Station
Base Station

- **Hard state: Current MSC/VLR, LAI**
  - » **(Necessary to page phone, updated whenever mobile moves)**
- **Soft-ish state:**
  - » **MSRN, cell ID, TMSI**

Note: Grossly simplified for your safety and sanity!