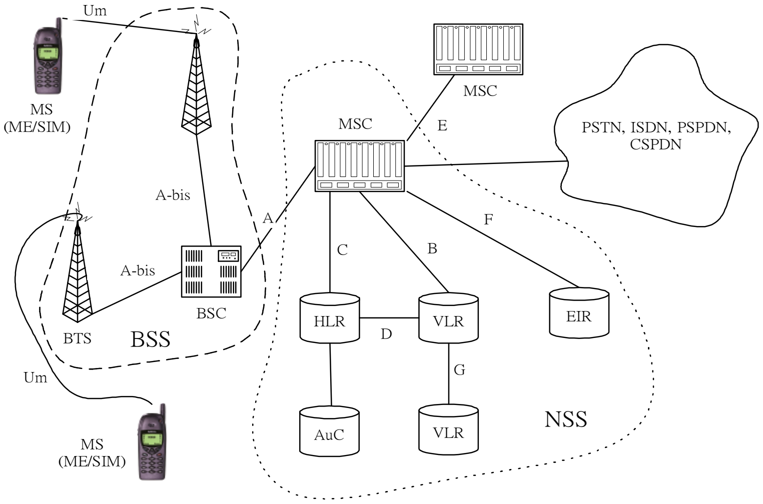
Global System for Mobile Communication (GSM)

Li-Hsing Yen

National University of Kaohsiung

GSM System Architecture



Nomenclature

- MS (Mobile Station) =
  MT (Mobile Terminal) +
  TE (Terminal Equipment)
- BSS (Base Station Subsystem) =
  BTS (Base Transceiver Station) +
  BSC (Base Station Controller)
- NSS (Network Switching Subsystem)
- MSC (Mobile Switching Center): telephony switching function and authentication of user

HLR and VLR

- HLR (Home Location Register)
  - a database to store and management **permanent** data of subscribers
- VLR (Visitor Location Register)
  - a database to store **temporary** information about subscribers
  - needed by MSC in order to service visiting subscribers

AuC and EIR

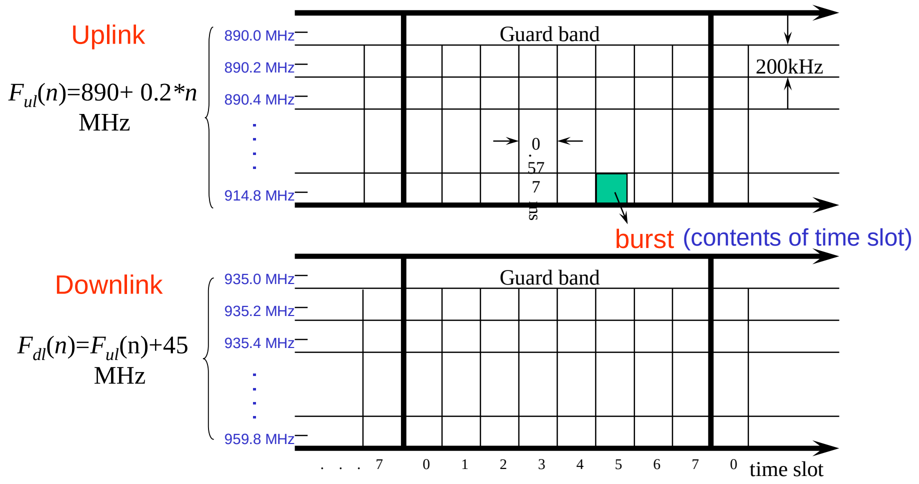
- Authentication Center (AuC)
  - used in the security data management for the authentication of subscribers.
- Equipment Identity Register (EIR)
  - used to maintain a list of legitimate, fraudulent, or faulty MSs.
  - optional in GSM network, and is not used generally.

GSM Interfaces

- U_m
  - Radio interface between MS and BTS
  - each physical channel supports a number of logical channels
- A_{bis}
  - between BTS and BSC (vender specific)
  - primary functions: traffic channel transmission, terrestrial channel management, and radio channel management

Frequency Division Duplex

n: Absolute Radio Frequency Channel Number (ARFCN). $1 \le n \le 124$



Uplink

$F_{ul}(n)$=890+ 0.2**n* MHz

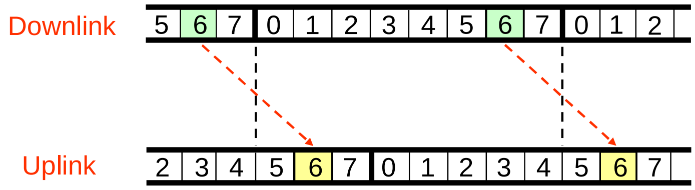
Downlink

$F_{dl}(n)=F_{ul}(\mathrm{n})+45$ MHz

burst (contents of time slot)

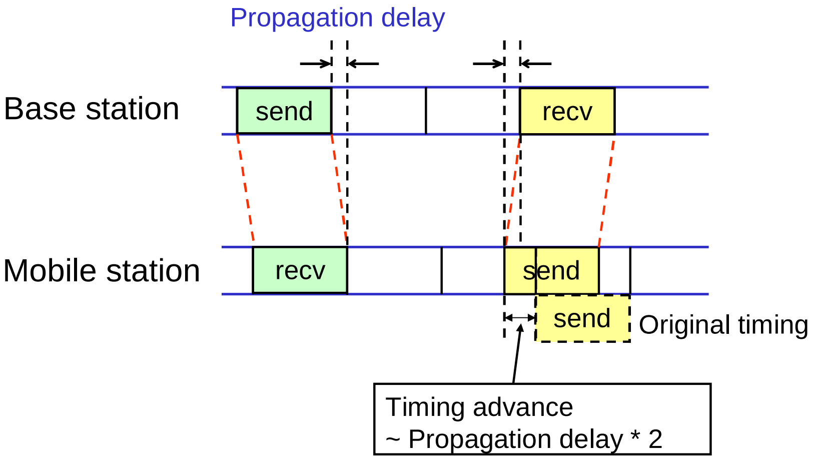
Time Division Duplex

MS and BTS do not transmit simultaneously
(MS transmits 3 time slots after the BTS)



Timing advance: MS transmits its data a little earlier as demanded by the “three time slots delay rule”.

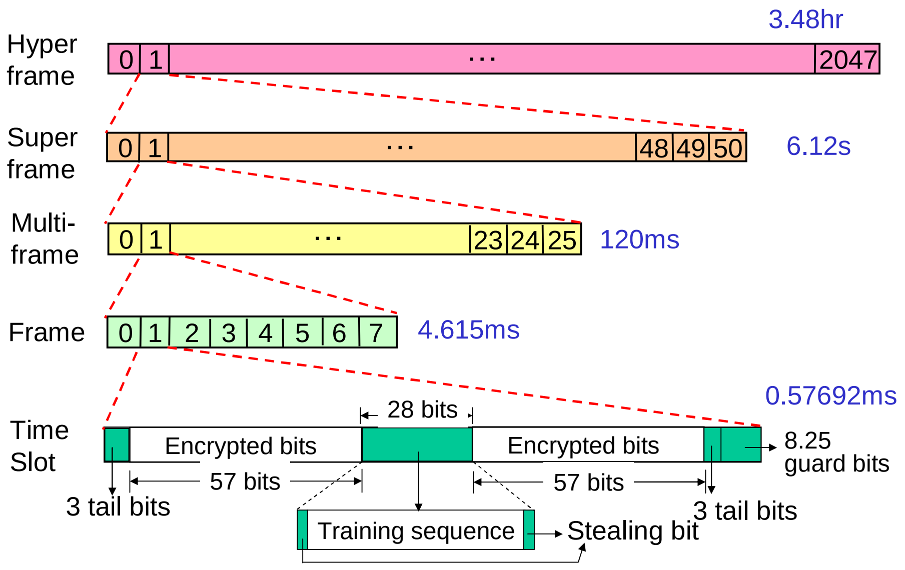
Timing Advance



GSM Frame Structure

- 1 hyperframe = 2048 superframes (~3.5hr)
- For speech
  - 1 superframe = 51 multiframes = 6.12s
  - 1 multiframe = 26 frames = 120ms
- For Signaling
  - 1 superframe = 26 multiframes
  - 1 multiframe = 51 frames
- 1 frame = 8 time slots = 4.615 ms
- 1 time slot = 156.25 bit duration = 0.577ms

GSM Frame Hierarchy



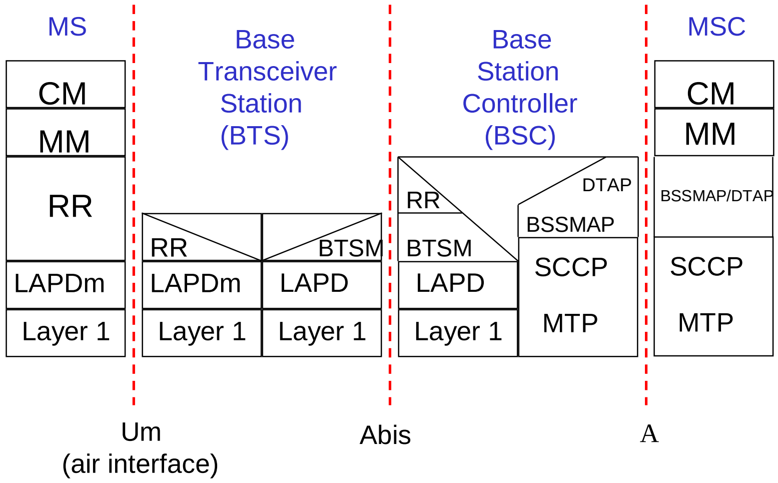
Normal Burst Format

- Trail bits
  - always (0,0,0); provide start and stop bit pattern
- encrypted bits
  - data is encrypted
- stealing bits
  - indicate whether the burst was stolen for urgent control signaling (FACCH signaling)
- Guard bits
  - avoid overlapping with other bursts due to different path delay

Training Sequence

- A known bit pattern that differs for different adjacent cells
- to adapt the parameters of the receiver to the current path propagation characteristics
- to select the strongest signal in case of multipath propagation
- for multipath equalization
  - extract the desired signal from unwanted reflections

GSM Protocol Stack



MS

Base Transceiver Station (BTS)

Base Station Controller (BSC)

MSC

CM

MM

RR

LAPDm

Layer 1

RR

BTSM

LAPDm

LAPD

Layer 1

Layer 1

RR

DTAP

BSSMAP

BTSM

LAPD

SCCP

MTP

Layer 1

CM

MM

BSSMAP/DTAP

SCCP

MTP

Um
(air interface)

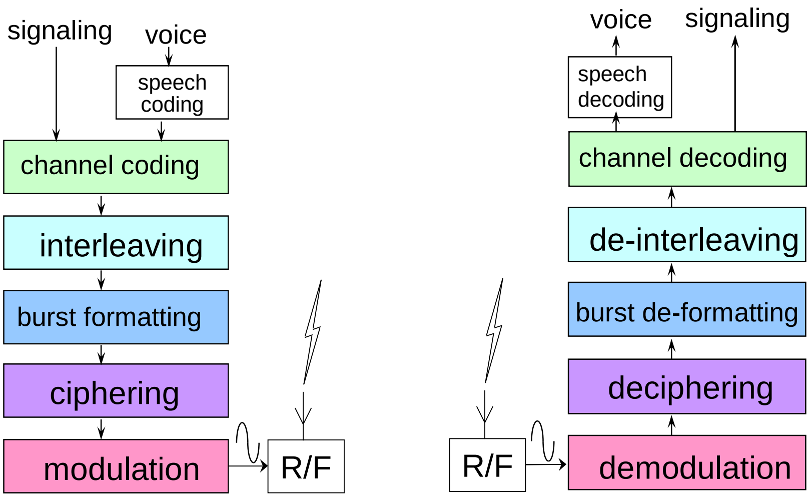
Abis

A

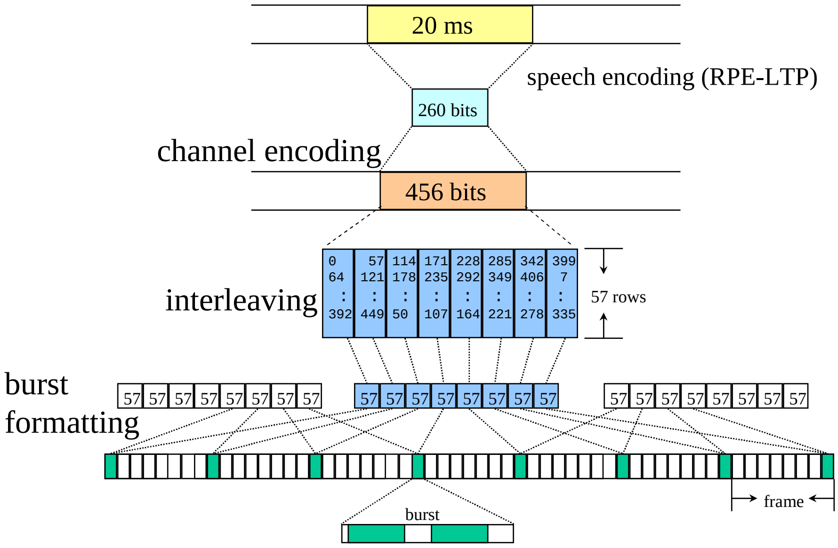
Layer 1 - Physical Layer

- Modulation
- Equalization
- Channel coding
  - block code
  - convolutional code
- Interleaving
  - to distribute burst error

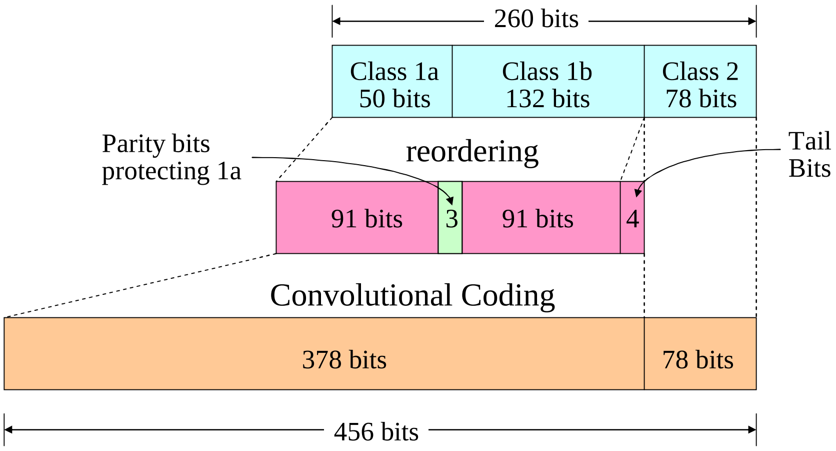
GSM Physical Layer (MS Side)



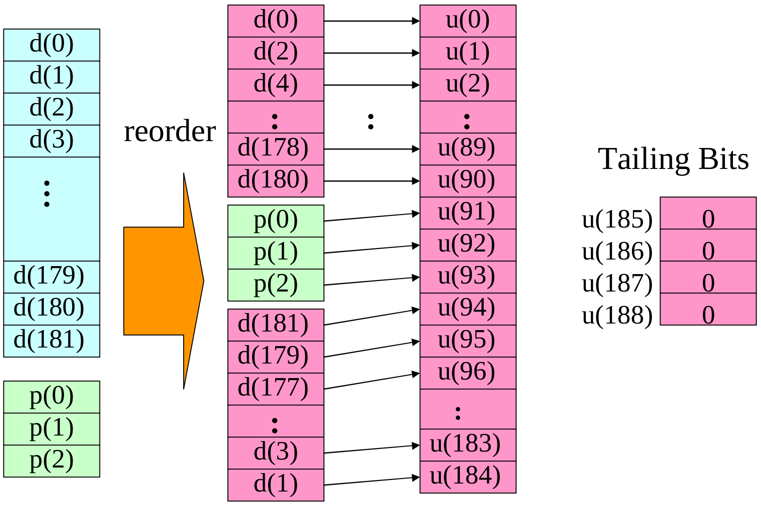
GSM Speech Transmission



GSM Speech Channel Coding



Tailing Bits and Reordering



d(0)
d(1)
d(2)
d(3)
⋮
d(179)
d(180)
d(181)

p(0)
p(1)
p(2)

reorder

d(0) → u(0)
d(2) → u(1)
d(4) → u(2)
: : :
d(178) → u(89)
d(180) → u(90)
p(0) → u(91)
p(1) → u(92)
p(2) → u(93)
d(181) → u(94)
d(179) → u(95)
d(177) → u(96)
: :
d(3) → u(183)
d(1) → u(184)

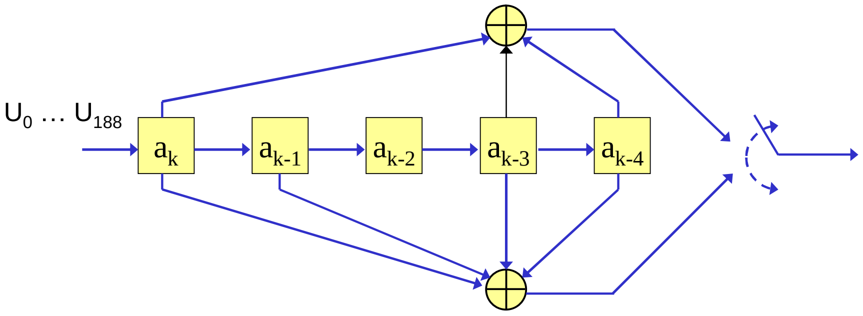
Tailing Bits

u(185)	0
u(186)	0
u(187)	0
u(188)	0

Parity Bits

- The first 50 bits are protected by 3 parity bits p(0), p(1), p(2)
- generator polynomial $g(D)=D^3+D+1$
- the remainder of $d(0)D^{52}+d(1)D^{51}+\ldots+d(49)D^3+p(0)D^2+p(1)D+p(2)$ divided by $g(D)$ should be $1+D+D^2$

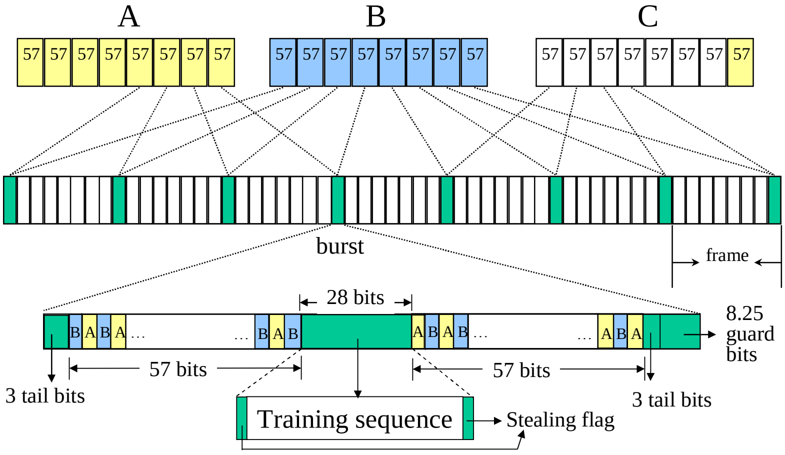
Convolutional Encoder for GSM Speech (Rate=1/2, K=5)



Interleaving

0	57	114	171	228	285	342	399
64	121	178	235	292	349	406	7
128	185	242	299	356	413	14	71
192	249	306	363	420	21	78	135
256	313	370	427	28	85	142	199
320	377	434	35	92	149	206	263
384	441	42	99	156	213	270	327
448	49	106	163	220	277	334	391
56	113	170	227	284	341	398	455
120	177	234	291	348	405	6	63
184	241	298	355	412	13	70	127
248	305	362	419	20	77	134	191
312	369	426	27	84	141	198	255
:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:
392	449	50	107	164	221	278	335

GSM Normal Burst Formatting



Physical Vs. Logical Channels

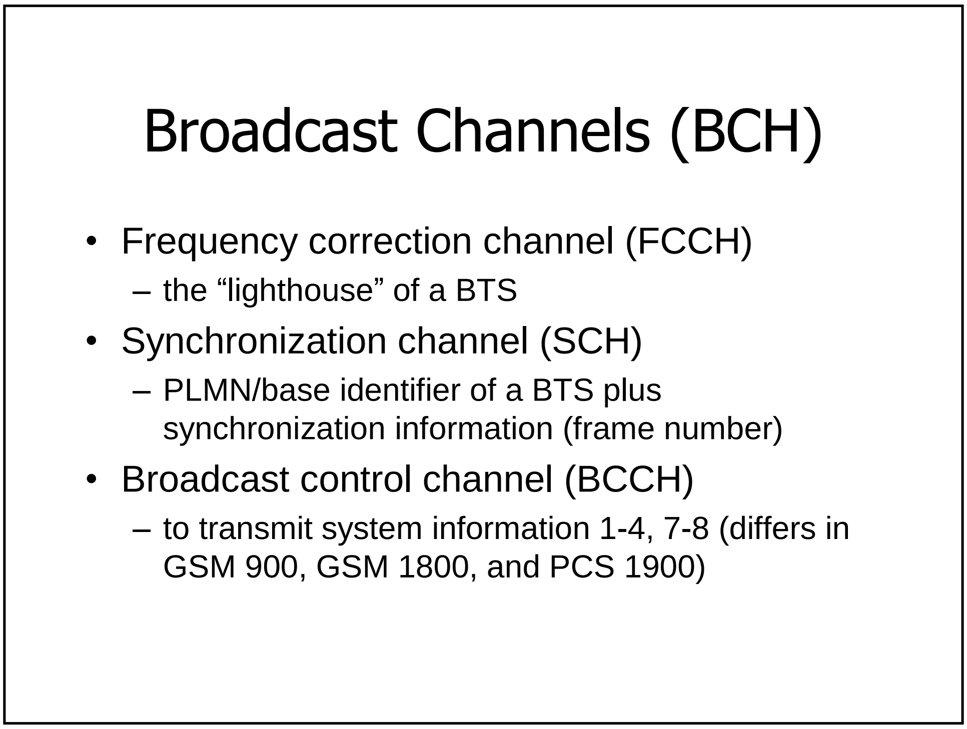
- Physical channels are all the available time slots of a BTS
  - a BTS with 6 carriers has 48 physical channels
- Logical channels are piggybacked on the physical channels
  - logical channels are laid over the grid of physical channels
  - each logical channel performs a specific task

GSM Logical Channels (I)

- Speech traffic channels (TCH)
  - Full-rate TCH (TCH/F)
  - Half-rate TCH (TCH/H)
- Broadcast channels (BCH)
  - Frequency correction channel (FCCH)
  - Synchronization channel (SCH)
  - Broadcast control channel (BCCH)
- Cell broadcast channel (CBCH)

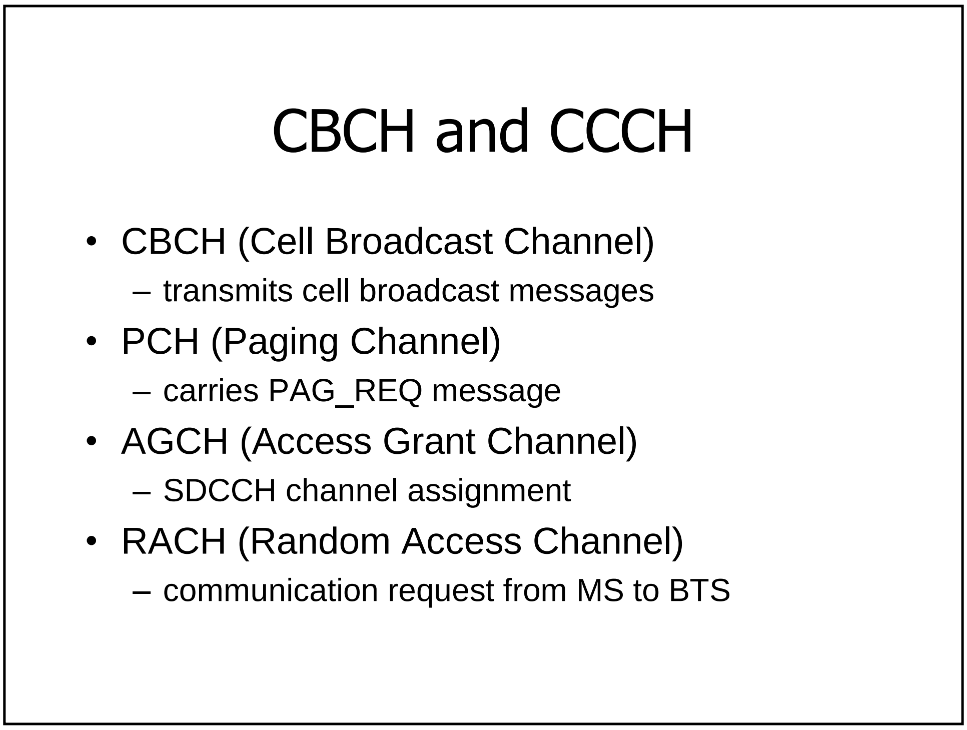
GSM Logical Channels (II)

- Common control channels (CCCH)
  - Paging channel (PCH)
  - Access grant channel (AGCH)
  - Random access channel (RACH)
- Dedicated control channel (DCCH)
  - Slow associated control channel (SACCH)
  - Stand-alone dedicated control channel (SDCCH)
  - Fast associated control channel (FACCH)



Broadcast Channels (BCH)

- Frequency correction channel (FCCH)
  - the “lighthouse” of a BTS
- Synchronization channel (SCH)
  - PLMN/base identifier of a BTS plus synchronization information (frame number)
- Broadcast control channel (BCCH)
  - to transmit system information 1-4, 7-8 (differs in GSM 900, GSM 1800, and PCS 1900)



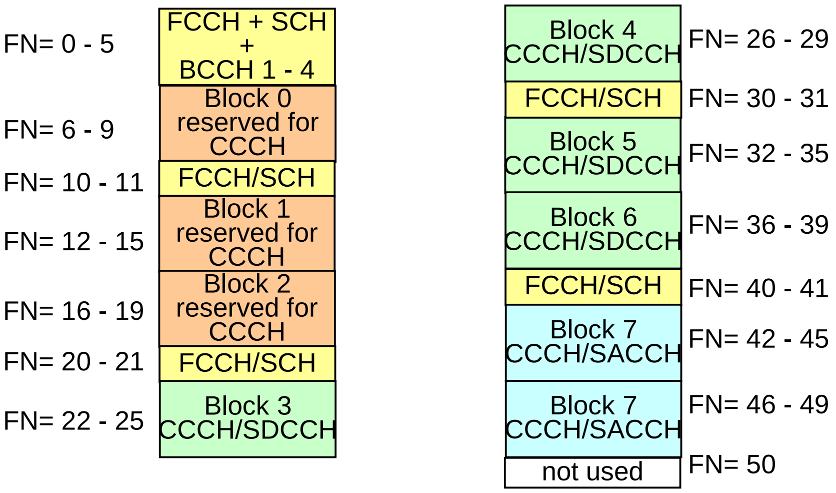
CBCH and CCCH

- CBCH (Cell Broadcast Channel)
  - transmits cell broadcast messages
- PCH (Paging Channel)
  - carries PAG_REQ message
- AGCH (Access Grant Channel)
  - SDCCH channel assignment
- RACH (Random Access Channel)
  - communication request from MS to BTS

Mapping of Logical Channels

- Each BTS has a particular frequency carrier called BCCH-TRX to transmit BCCH info
- The following channel structure can be found on time slot 0 of carrier BCCH-TRX
  - FCCH
  - SCH
  - BCCH information 1-4
  - Four SDCCH subchannels (optional)
  - CBCH (optional)

Example Mapping of Logical Channels on Time Slot 0 (Downlink)



FN= 0 - 5 FCCH + SCH + BCCH 1 - 4

FN= 6 - 9 Block 0 reserved for CCCH

FN= 10 - 11 FCCH/SCH

FN= 12 - 15 Block 1 reserved for CCCH

FN= 16 - 19 Block 2 reserved for CCCH

FN= 20 - 21 FCCH/SCH

FN= 22 - 25 Block 3 CCCH/SDCCH

FN= 26 - 29 Block 4 CCCH/SDCCH

FN= 30 - 31 FCCH/SCH

FN= 32 - 35 Block 5 CCCH/SDCCH

FN= 36 - 39 Block 6 CCCH/SDCCH

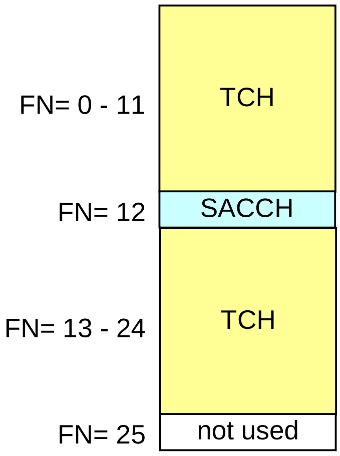
FN= 40 - 41 FCCH/SCH

FN= 42 - 45 Block 7 CCCH/SACCH

FN= 46 - 49 Block 7 CCCH/SACCH

FN= 50 not used

Example Mapping of Logical Channels on Time Slot 2 (Downlink)



FN= 0 - 11 TCH

FN= 12 SACCH

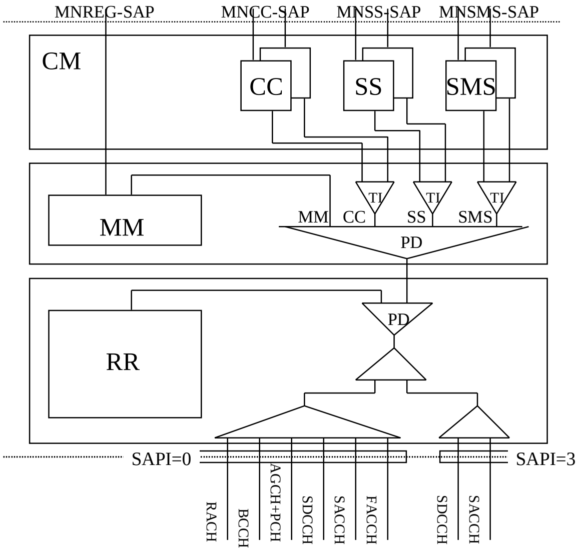
FN= 13 - 24 TCH

FN= 25 not used

GSM Layer 2: LAPDm

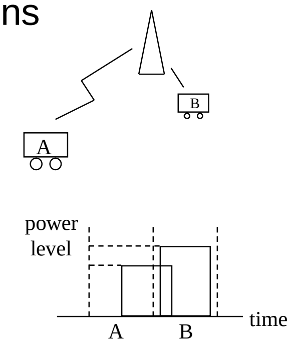
- Functions
  - organization of Layer 3 information into frames
  - peer-to-peer transmission of signaling data in defined frame formats
  - recognition of frame formats
  - establishment, maintenance, and termination of one or more (parallel) data links on signaling channels

Layer 3 Protocol Architecture: Mobile Station Side

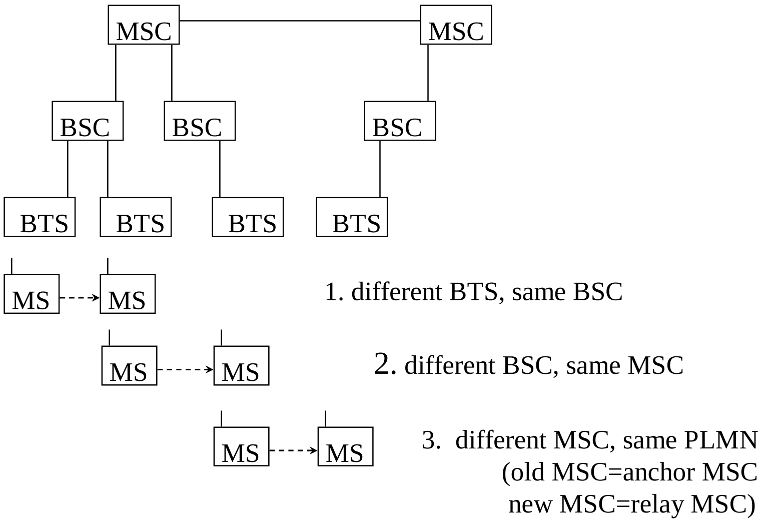


Layer 3 - RR Sublayer

- The RR sublayer handles all the procedures necessary to establish, maintain, and release dedicated radio connections
  - – channel allocation
  - – handover
  - – timing advance
  - – power control
  - – frequency hopping



Three Cases of Hand-over



1. different BTS, same BSC

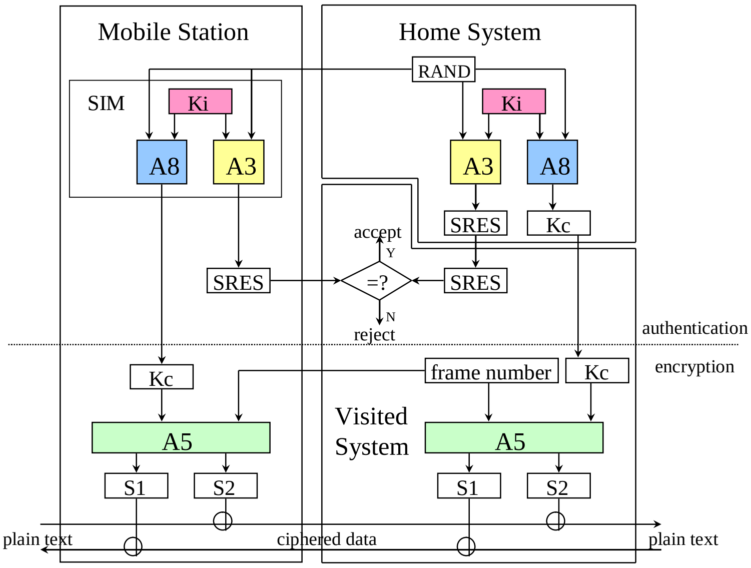
2. different BSC, same MSC

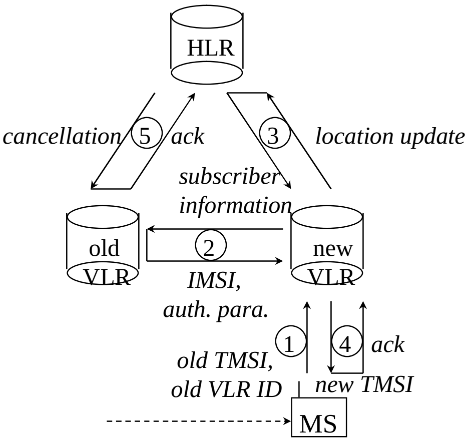
3. different MSC, same PLMN
(old MSC=anchor MSC
new MSC=relay MSC)

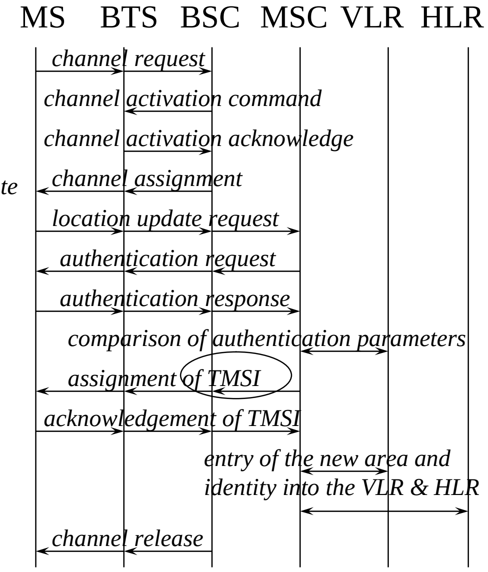
Layer 3 - MM Sublayer

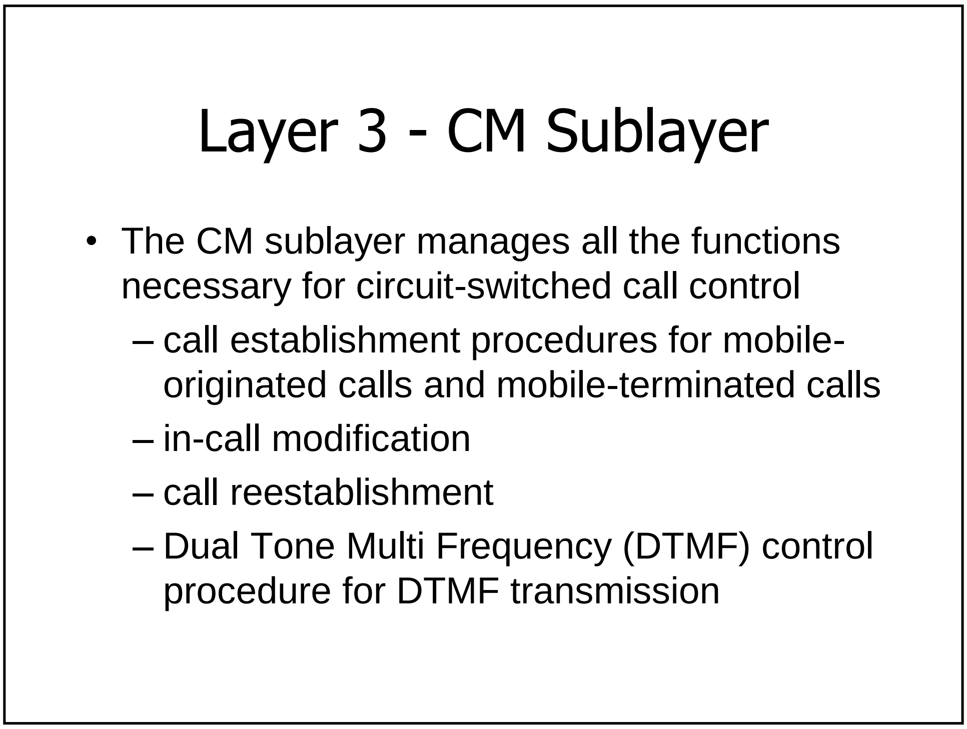
- The MM sublayer copes with all the effects of handling a mobile user that are not directly related to radio functions
  - location area
  - location registration & call delivery
  - location update & paging

Authentication & Encryption/Decryption in GSM



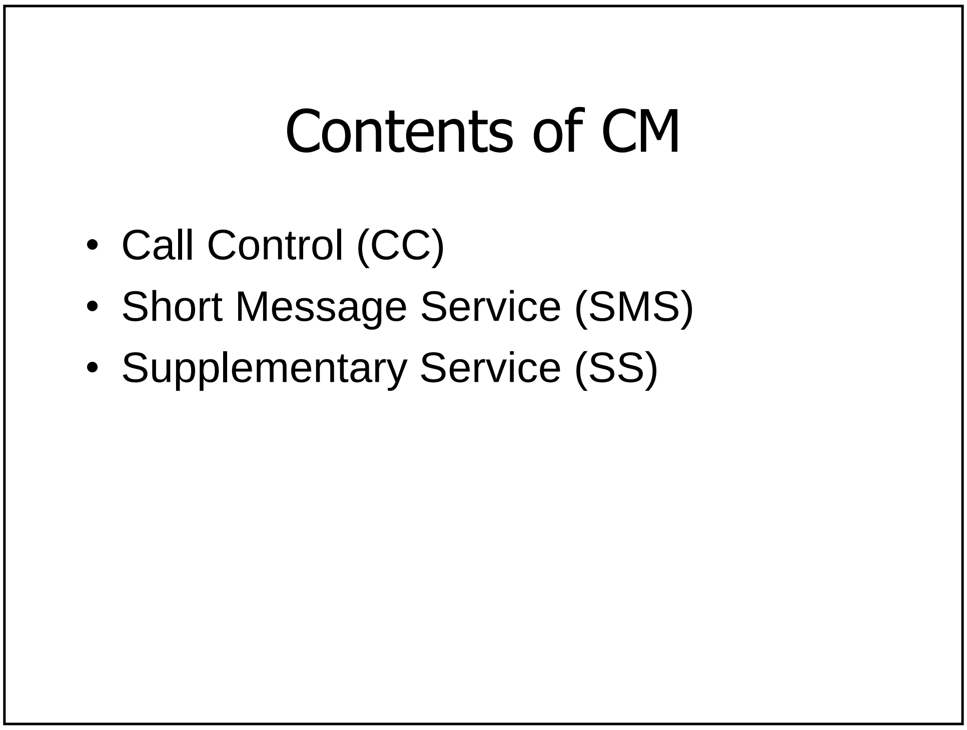






Layer 3 - CM Sublayer

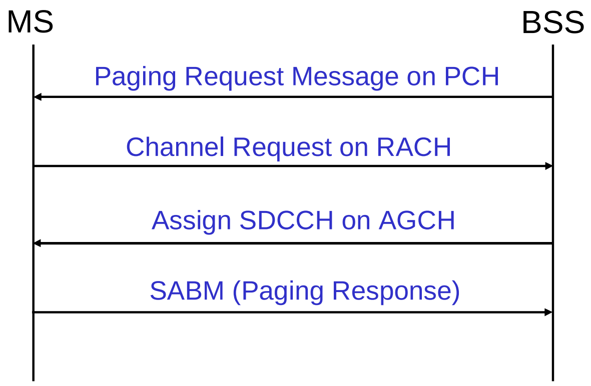
- The CM sublayer manages all the functions necessary for circuit-switched call control
  - call establishment procedures for mobile-originated calls and mobile-terminated calls
  - in-call modification
  - call reestablishment
  - Dual Tone Multi Frequency (DTMF) control procedure for DTMF transmission



Contents of CM

- Call Control (CC)
- Short Message Service (SMS)
- Supplementary Service (SS)

Paging Procedure



MS

BSS

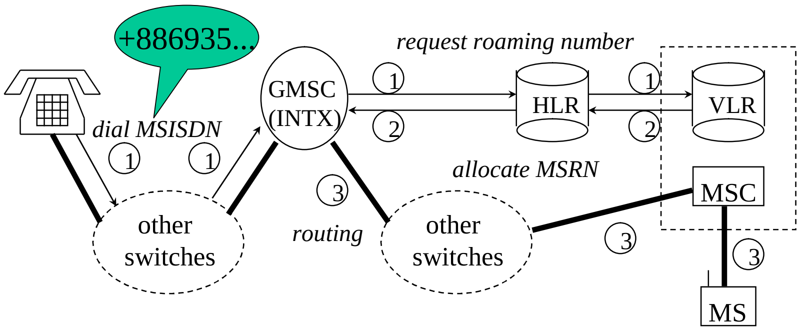
Paging Request Message on PCH

Channel Request on RACH

Assign SDCCH on AGCH

SABM (Paging Response)

Call Setup Procedure: Mobile Terminated Call



+886935...

dial MSISDN

GMSC (INTX)

request roaming number

HLR

VLR

allocate MSRN

MSC

other switches

routing

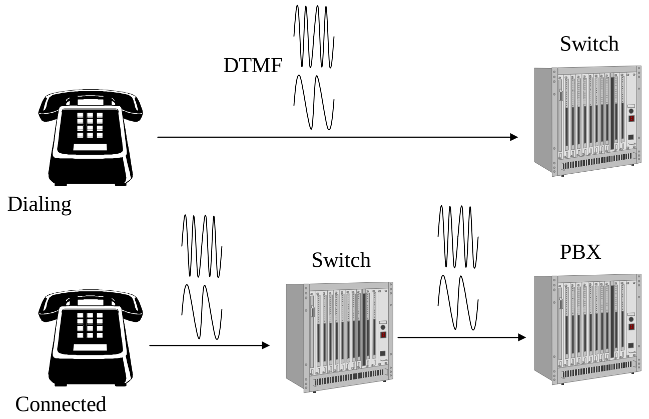
other switches

MS

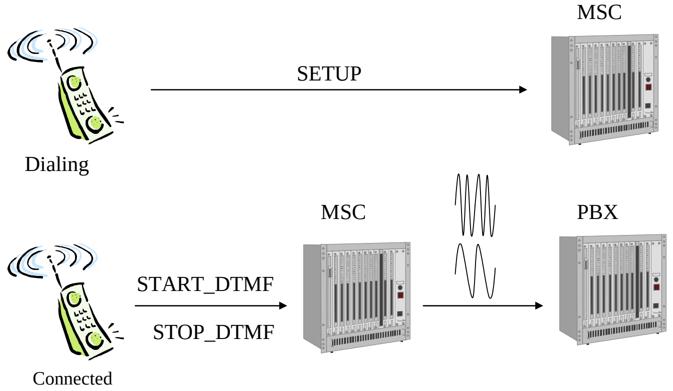
1 1 1 1 2 2 3 3 3

INTerrogating eXchange (INTX)
Mobile Station ISDN Number (MSISDN) (Country Code, see E.164)
Mobile Station Roaming Number (MSRN) (Mobile Country Code, see E.212)

Dual Tone Multiple Frequency (DTMF) in PSTN



DTMF in GSM


MSC
SETUP
Dialing
MSC
PBX
START_DTMF
STOP_DTMF
Connected