G 364: Mobile and Wireless Networking

CLASS 21, Mon. Mar. 29 2004

Stefano Basagni

Spring 2004

M-W, 11:40am-1:20pm, 109 Rob

Global System for Mobile Communications (GSM)

- Digital wireless network standard designed in Europe
- Provide a common set of compatible services and capabilities
- User throughout Europe and more
- Several millions of customers worldwide

Basic Requirements

- Services
- Quality of Service (QoS) and security
- Radio frequency utilization
- Network
- Cost

Services

- Service portability: MSs can be used in all participating countries
- Services like in the wireline network, as well as mobile-specific services
- Service is provided to vehicle-mounted MSs, as well as to those used by pedestrian or on a ship

QoS and Security

- GSM quality of voice services has to be as least as good as the one of previous analog systems
- Information encryption is provided to those who require it
- Cost is kept low enough not to affect users that do not require it

Radio Frequency Utilization

- High level of spectrum efficiency and state-of-the-art subscriber facilities
- Operating in the entire allocated frequency band
- Coexist with earlier systems in the same frequency

Network and Cost

- Identification and numbering plan based on ITU recommendations
- Standard signaling system for switching and mobility management
- Public network should not be significantly affected
- Design to limit the cost of the complete system, in particular the MSs

GSM Architecture

- Mobile Station (MS), communicate with
- Base Station System (BSS), via the
- Radio Interface
- BSS is connected to the Network and Switching Subsystem (NSS) via a
- Mobile Switching Center (MSC) using
- A interface

Mobile Station

- Consist of two parts
  - Subscriber Identity Module (SIM)
  - Mobile Equipment (ME)
- Broader definition
  - Terminal Equipment (TE): PDA or PC connected to the ME
  - The SIM + ME are called the Mobile Terminal

SIM, 1

- A SIM can be
  - A smart card, usually the size of a credit card
  - A smaller sized “plug-in SIM”
  - A smart card that can be “perforated,” which contains a plug-in SIM to be broken out of it

SIM, 2

- A SIM is protected by a Personal Identity Number (PIN), between 4 to 8 digits in length
- PIN is loaded on the SIM by the network operator at subscription time
- Can be activated or changed by the user
- Protected by the PIN Unblocking Key (PUK)

SIM, 3

- A SIM contains subscriber-related information (+ PIN + PUK)
- Include: Short list of abbreviated and customized short dialing numbers
- Short messages received when the user is not present
- Name of preferred networks to provide service
- RS232 modifiable (or via MS keypad)
- “SIM toolkit”

Mobile Equipment (ME), 1

- The ME contains non-customer related hardware and software specific to the radio interface
- It cannot be used to reach the service without SIM, except for emergency calls
- A SIM can fit several MEs

ME, 2

- At every connection, SIM sends to the network the classmark of its current ME
- This SIM-ME design enhances portability and security
- The ME is property of the user
- The SIM is loaned to the subscriber, but it is owned by the service provider

ME 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

Base Station System (BSS)

- Connects the MSs to the Network Switching Subsystem (NSS)
- Consist of two parts:
  - The Base Transceiver Station (BTS)
  - The Base Station Controller (BSC)

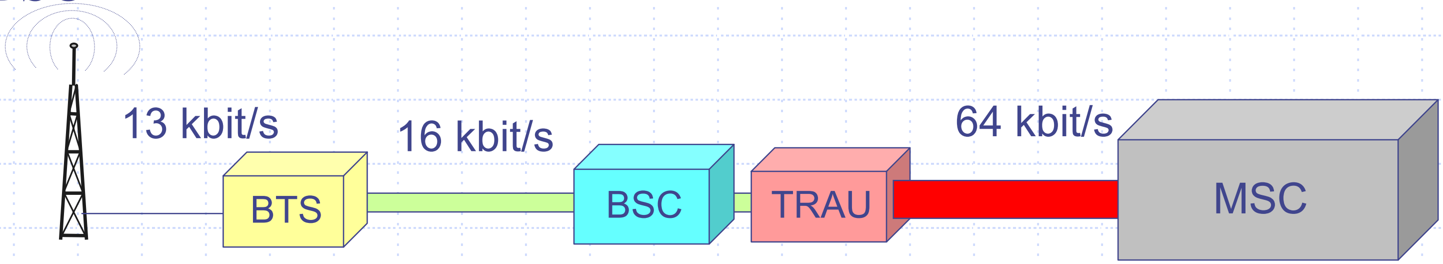
Base Transceiver Station

- The BTS contains
  - Transmitter
  - Receiver
  - Signaling equipment specific to the radio interface
  - Transcoder/Rate Adapter Unit (TRAU): Implements GSM-specific encoding-decoding and rate adaptation in data transmission

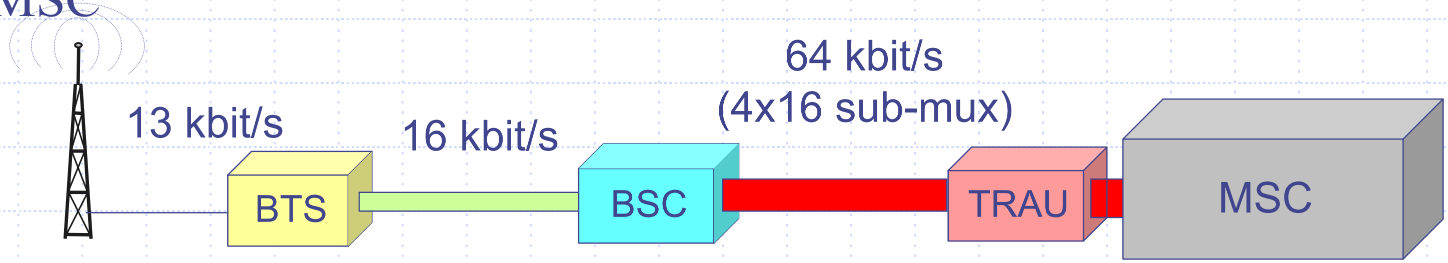
TRAU possible placements

On BTS

On BSC



On MSC



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

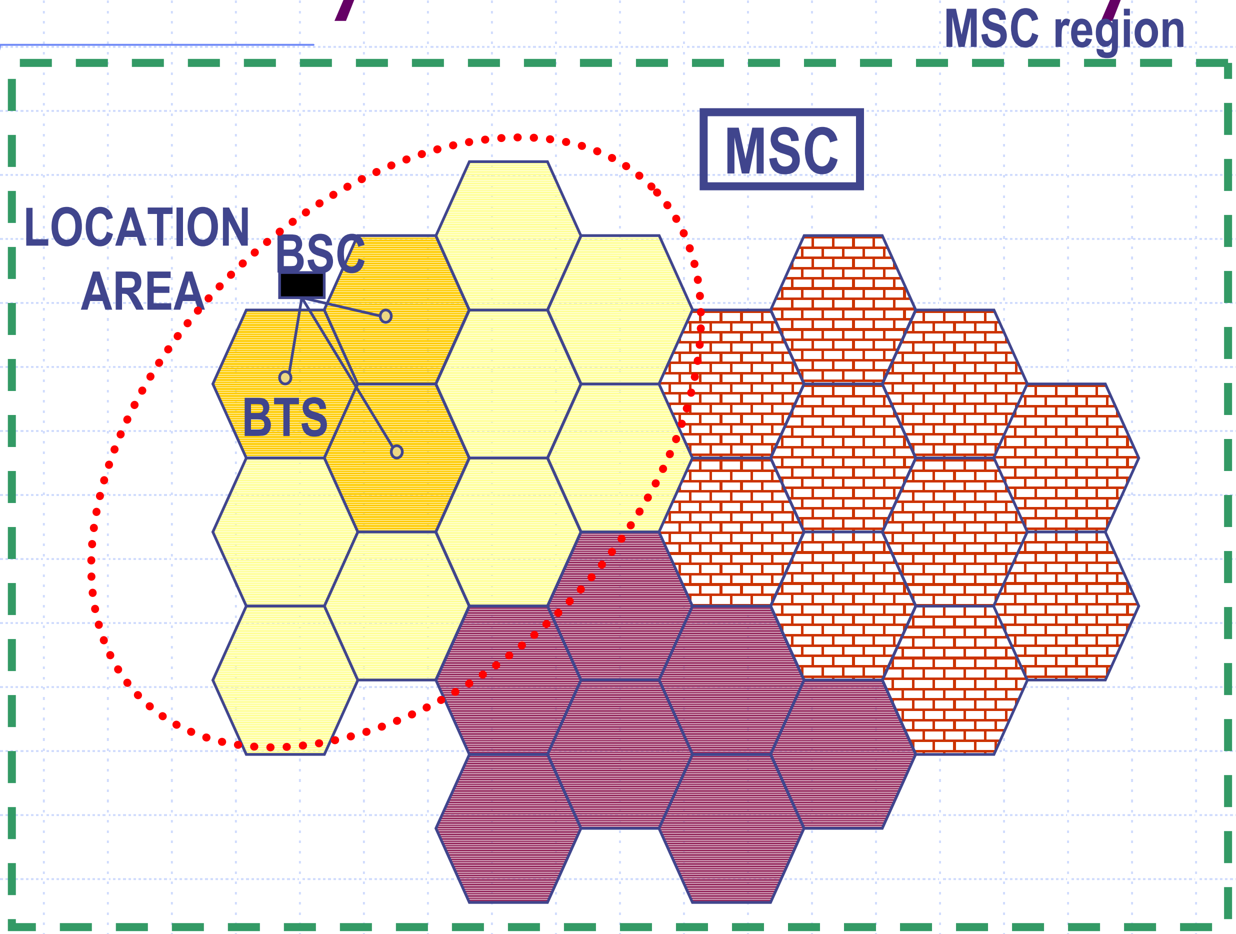
Base Station Controller

- The BSC:
  - Support radio channel allocation/release
  - Handoff management
- May connect to several BTSs (not in GSM) and maintain their cell configuration data
- Communicated to the BTS via ISDN protocols using the A-bis interface
- In GSM BTS and BSC are usually co-located and integrated (do not need the A-bis interface)

BSC, Capacity Planning

- Busy hours processor load allocation:
  - Call activities: 20/25%
  - Paging and SMSs: 10/15%
  - Mobility management (handoff and location update): 20/25%
  - Hardware checking/Network-triggered events: 15/20%
- Overload rejects: 1) location update, 2) MS originating calls, 3) handoffs

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

Network and Switching Subsystems, NSS

- NSS supports
  - Switching functions
  - Subscriber profiles
  - Mobility management
- Switching is performed by MSCs
  - Follows a protocol used in the telephone network
  - MSC communicates also with extra-GSM entities (using the same protocol)

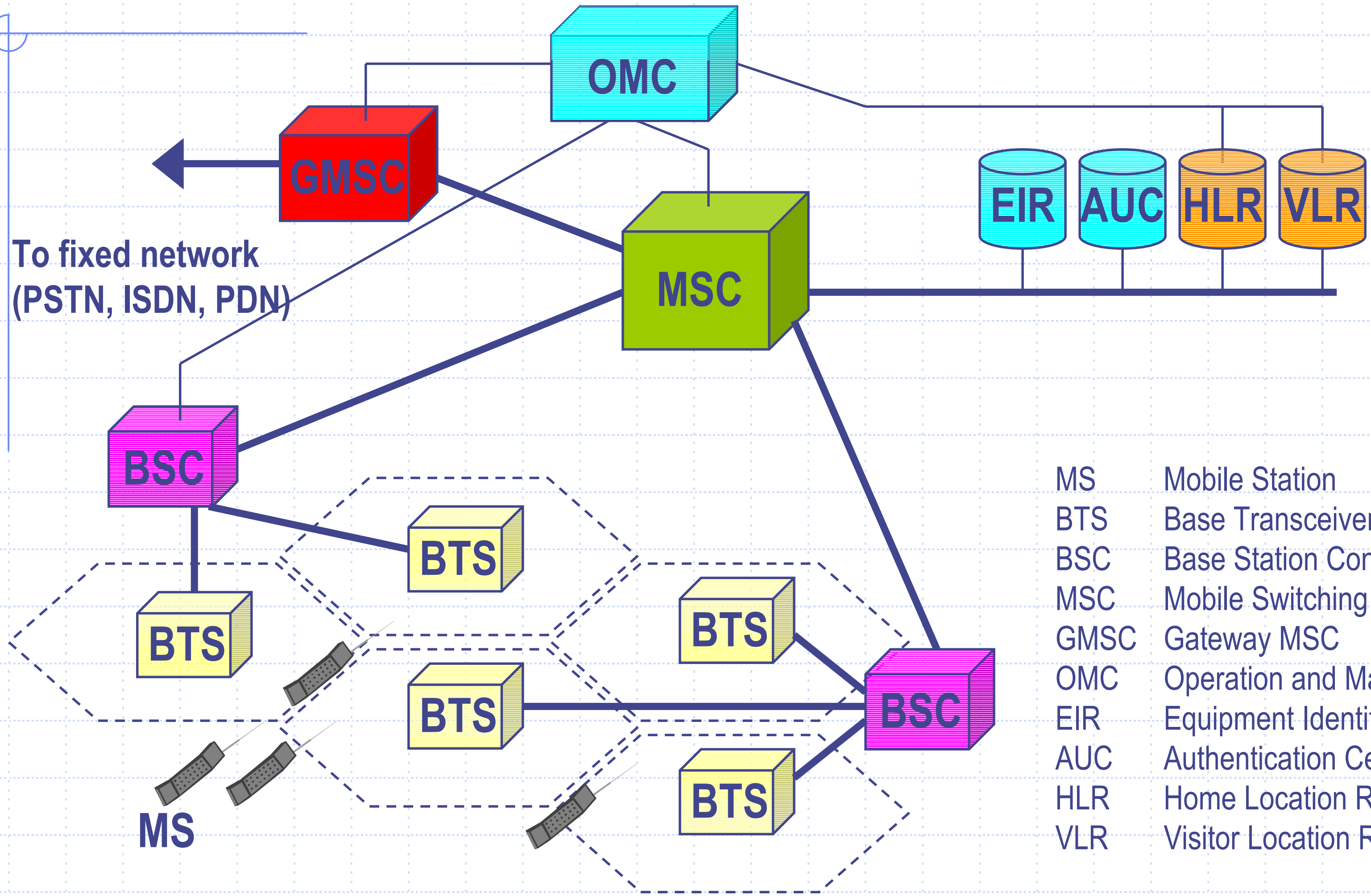
NSS, 2

- MS current location is maintained by HLR and VLR
- Roaming operations are aided by the Authentication Center (AuC)
  - Security data management for the authentication of subscribers
  - Usually co-located with the HLR

NSS, 3

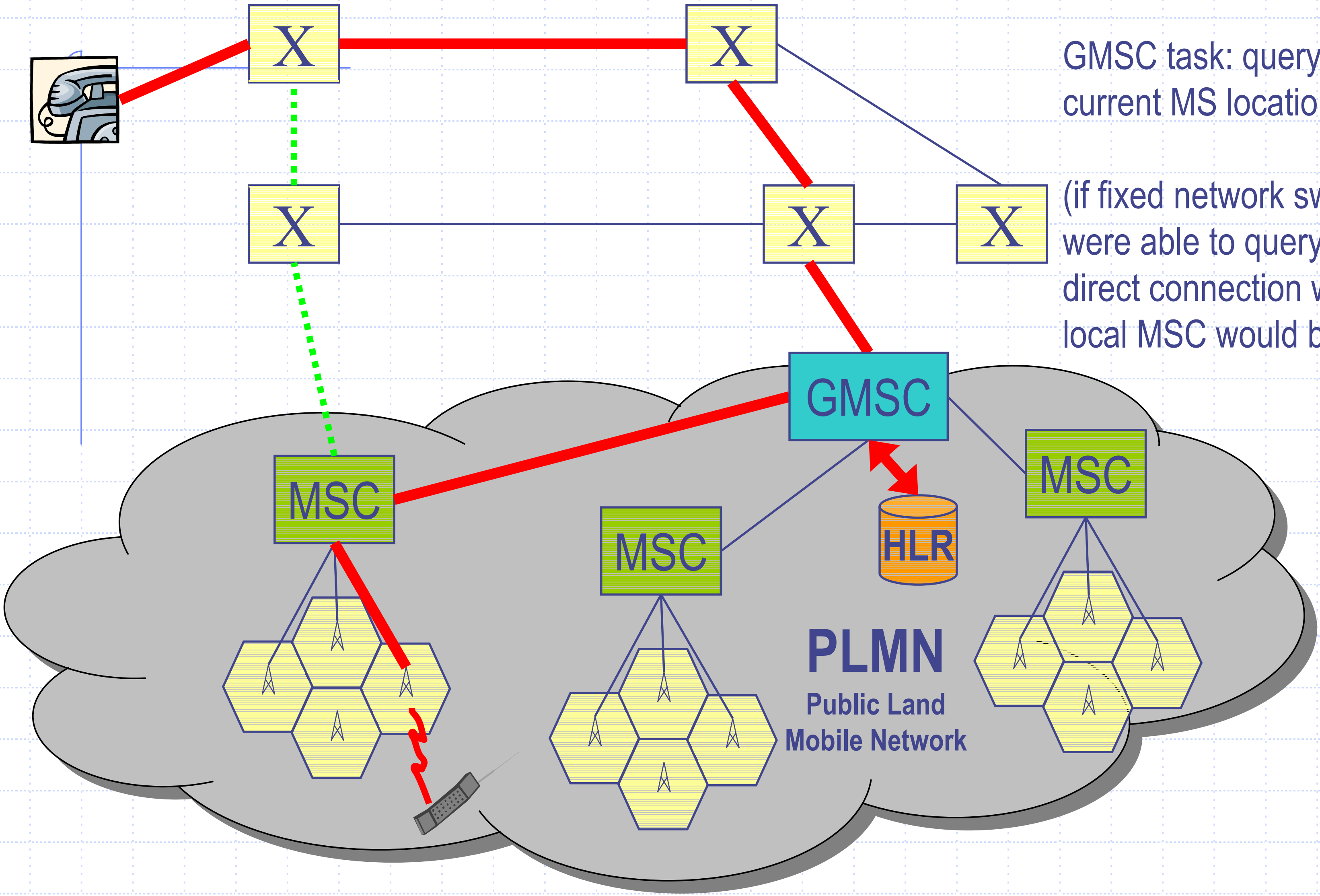
- Incoming calls are routed to MSC, called the Gateway MSC (GSMC)
- An MSC can function as GSMC by
  - Adding appropriate software
  - HLR interrogation functions
  - Provisioning interface and signaling link to HLR

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

Gateway MSC–GMSC

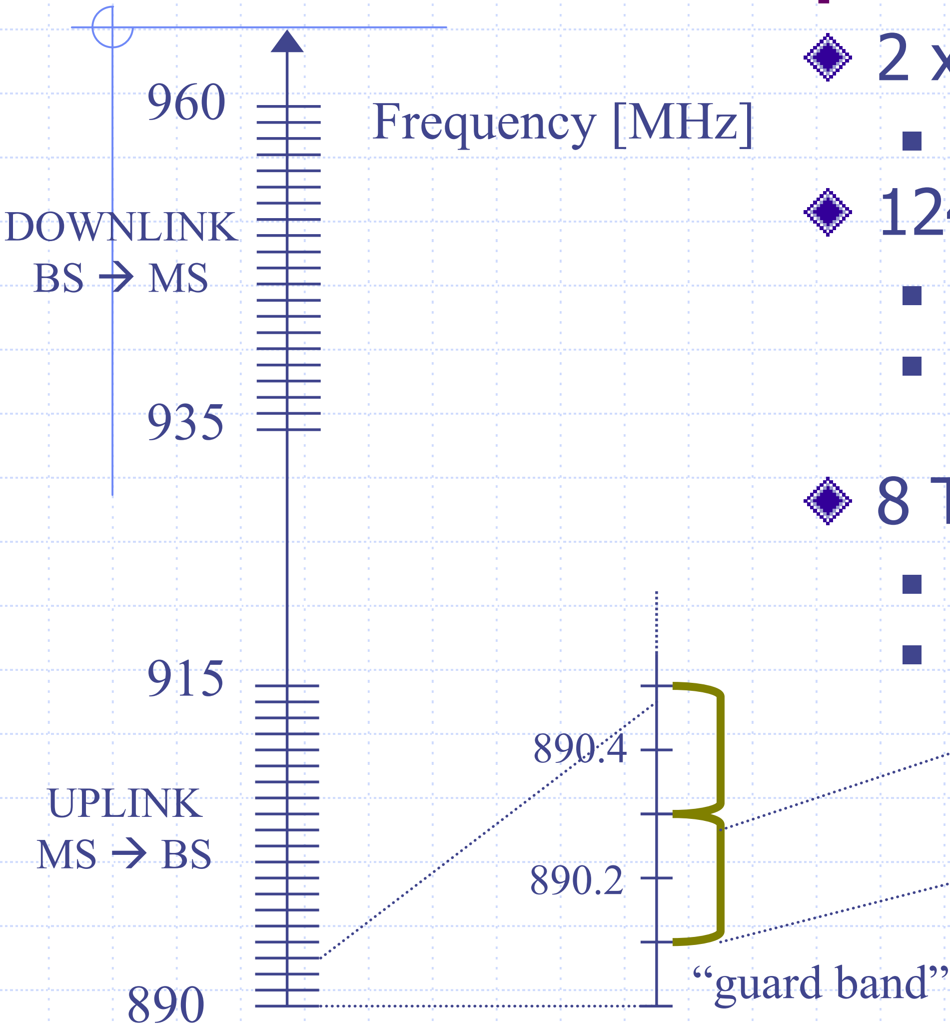


Needed, as fixed network switches are not mobile capable!!

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)

GSM Radio Spectrum



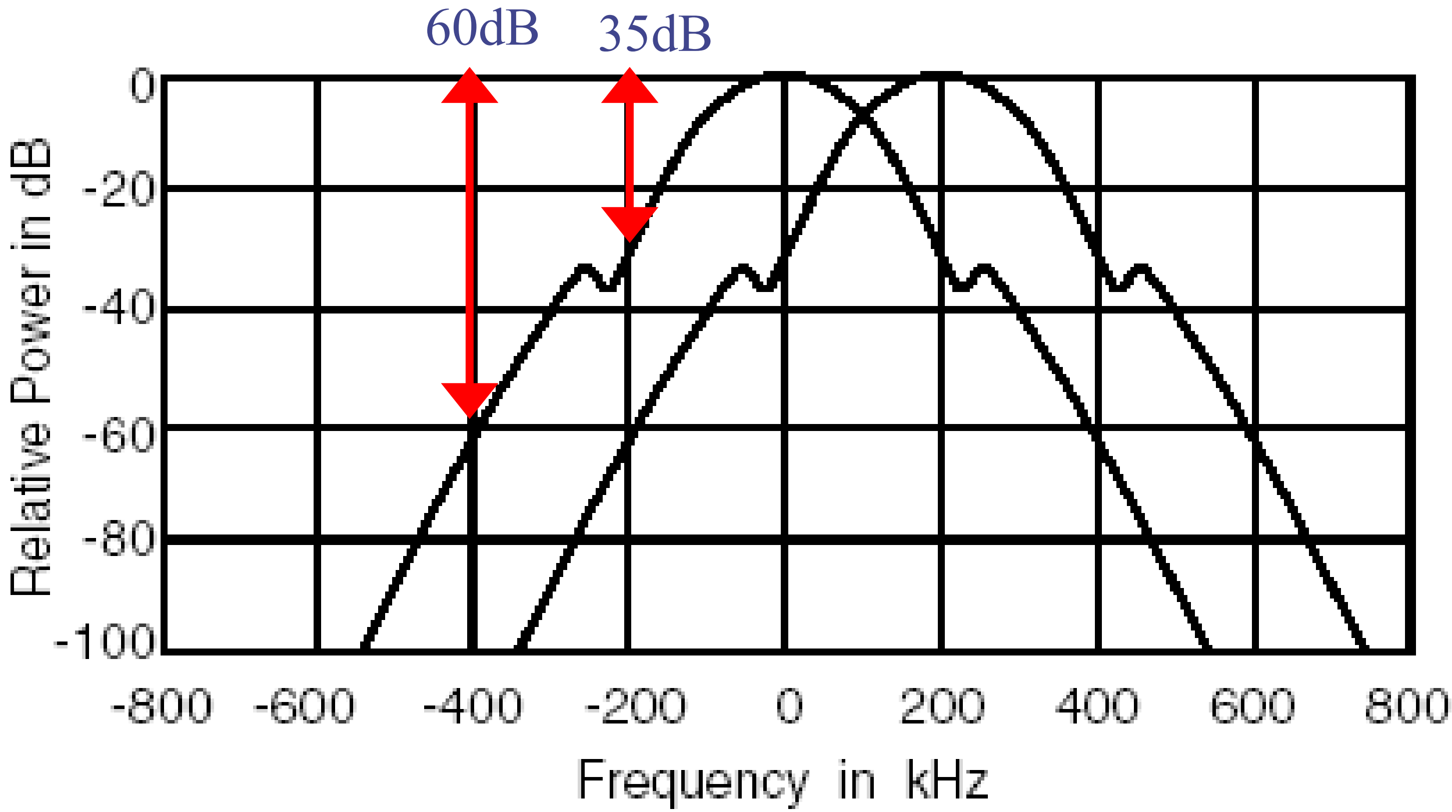
- 2 x 25 Mhz band
  - Duplex spacing: 45 MHz
- 124 carriers x band
  - 200 KHz channels
  - Suggested use: only 122
    - Use top & bottom as additional guard
- 8 TDMA slots x carrier
  - full rate calls – 13 Kbps
  - If half-rate used, 16 calls at 6.5 kbps

1	2	3	4	5	6	7	8

$$F_{uplink}(n) = [890.2 + 0.2(n-1)]\,\text{MHz}$$

$$F_{dwlink}(n) = [935.2 + 0.2(n-1)]\,\text{MHz}$$

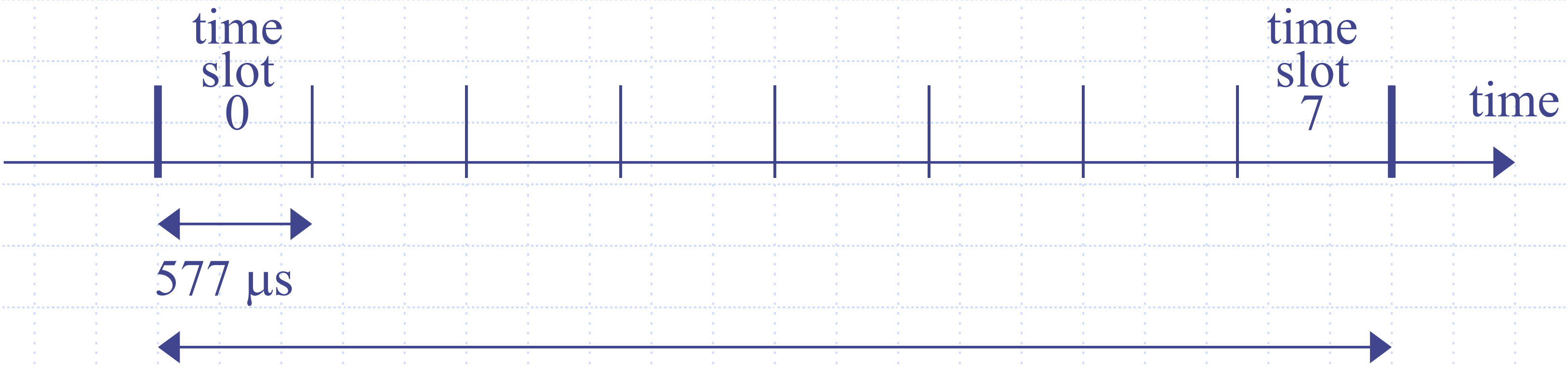
Adjacent Channels
(due to GMSK)



Specification: 9dB
In practice, due to power control and shadowing, adjacent channels
Cannot be used within the same cell…

Physical Channel

- 200 KHz bandwidth + GMSK modulation
  - 1625/6 kbps gross channel rate (270.8333 kbps)
- 1 time slot = 625/4 bits
  - 156.25 bits
  - 15/26 ms = 576.9 μs

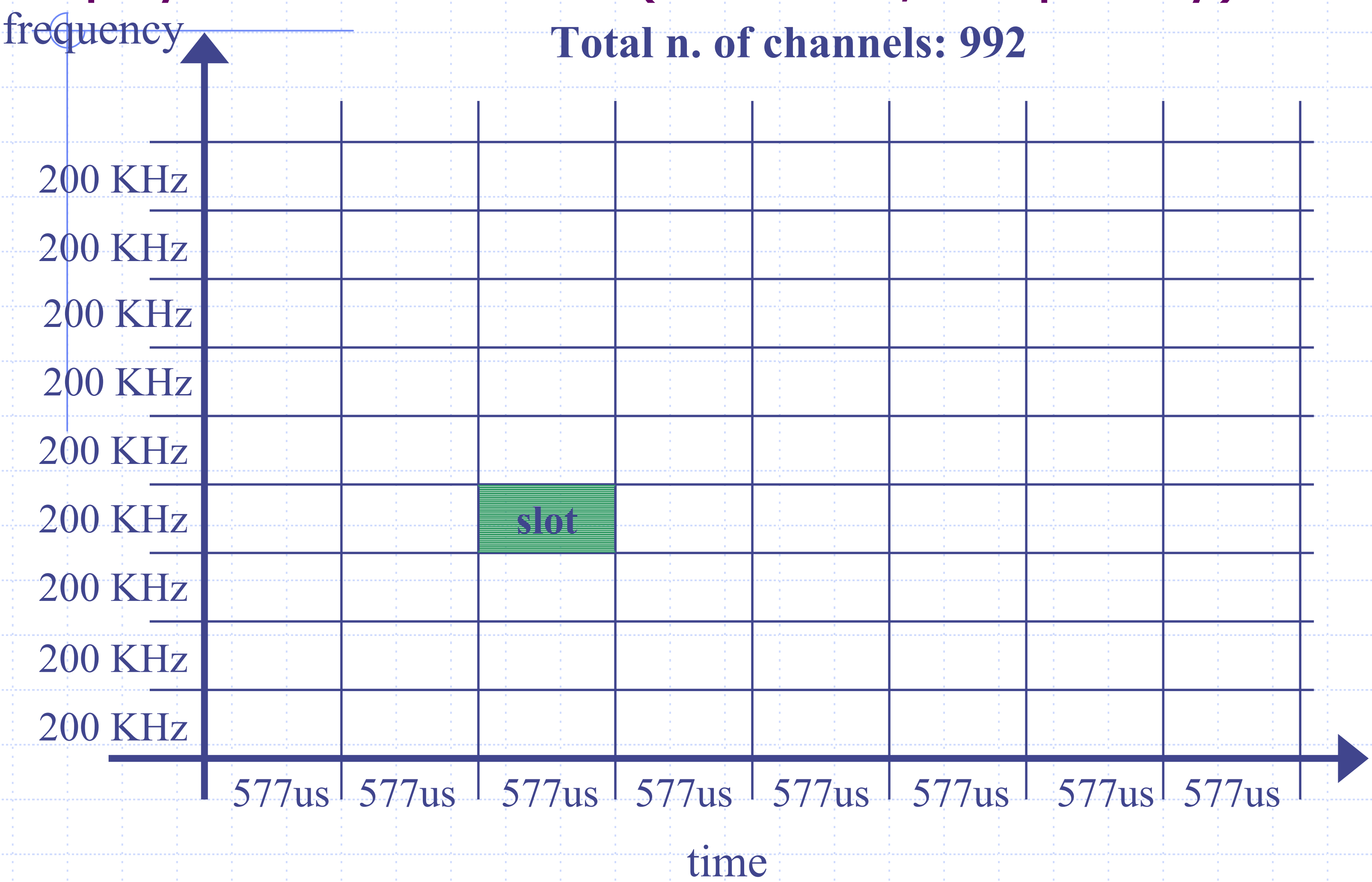


1 frame = 60/13 ms = 4.615 ms

26 frames = 120 ms (*this is the key number*)

Hybrid FDMA-TDMA

physical channel = (time slot, frequency)



DCS 1800 radio spectrum

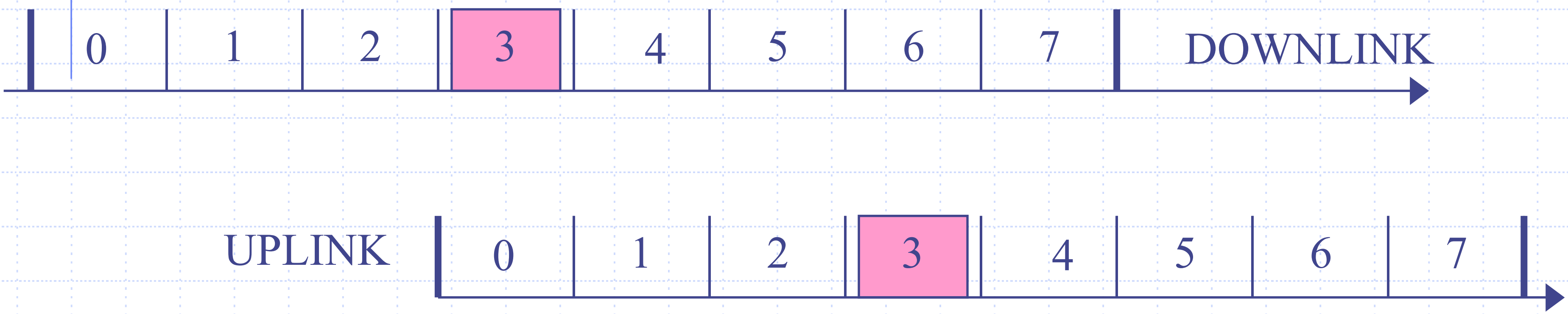
- Greater bandwidth available
  - EUROPE: 75 MHz band
    - 1710-1785 MHz uplink; 1805-1880 MHz downlink
  - ITALY: 45 MHz band from 2005
    - 1740-1785 MHz uplink; 1835-1880 MHz downlink
- Same GSM specification
  - 200 KHz carriers
    - A total of 374 carriers (versus124 in GSM)
- DCS 1800 operators
  - Common rule in most of the countries:
    - First and second operators @ 900 MHz; Third etc @1800 MHz
    - DCS 1800 deployment (1996+):
      - 15 MHz (=75 carriers) to Wind; 7.5 (=37 carriers) to first and second operator (plus existing 27 GSM 900 carriers)

Other GSM Bands

- Extended GSM (E-GSM) band
  - Uplink: 880-915 MHz
  - Downlink: 925-960 MHz
- Other bands:
  - 450 MHz → (450.4-457.6 up; 460.4-467.6 down)
  - 480 MHz → (478.8-486 up; 488.8-496 down)
  - 1900 MHz → (1850-1910 up; 1930-1990 MHz)

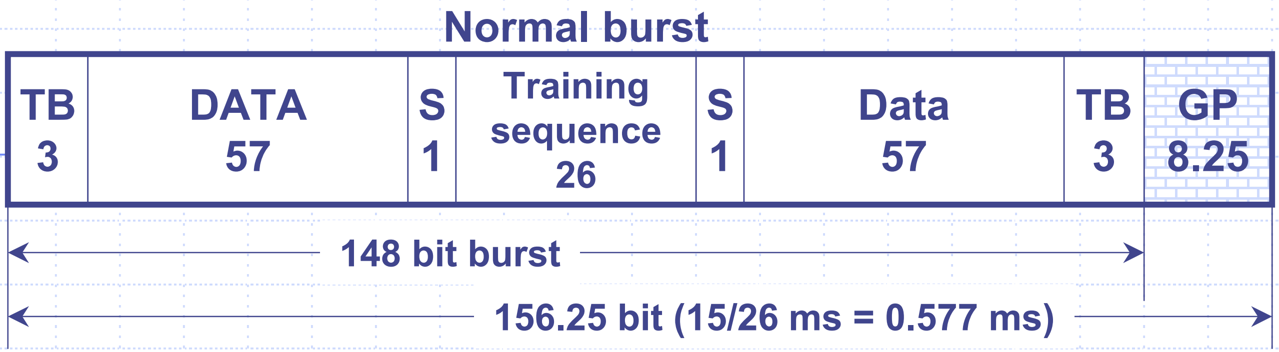
Duplexing

- **MS uses SAME slot number on uplink and downlink**
- **Uplink and downlink carriers always have a 45 MHz separation**
    - *I.e. if uplink carrier is 894.2 → downlink is 919.2*
- **3 slot delay shift!!**



MS: no need to transmit and receive at the same time on two different frequencies!

Structure of a TDMA Slot



- Symmetric structure
- DATA: 2 x 57 data bits
  - 114 data bits per burst
  - "gross" bits (error-protected; channel coded)
  - "gross" rate: 24 traffic burst every 26 frames (120 ms)
    - 22.8 kbps gross rate
    - 13 kbps net rate!
- S: 2 x 1 stealing bit
  - Also called stealing flags, toggle bits
  - Needed to grab slot for FACCH (other signalling possible)

Tail & Training Bits

- 2 x TB = 3 tail bits set to 000
  - At start and end of frame
  - Leave time available for transmission power ramp-up/down
  - Assures that Viterbi decoding starts and ends at known state
- 26 bit training sequence
  - Known bit pattern (8 Training Sequence Code available)
  - for channel estimation and synchronization
  - Why in the middle?
    - Because channel estimate reliable ONLY when the radio channel "sounding" is taken!
    - Multipath fading rapidly changes the channel impulse response...

Training Sequences

Training sequence code (TSC)	Training sequence bits (b61, b62, ..., b86)
0	(0,0,1,0,0,1,0,1,1,1,0,0,0,0,1,0,0,0,1,0,0,1,0,1,1,1)
1	(0,0,1,0,1,1,0,1,1,1,0,1,1,1,1,0,0,0,1,0,1,1,0,1,1,1)
2	(0,1,0,0,0,0,1,1,1,0,1,1,0,1,0,0,0,1,0,0,0,1,1,1,1,0)
3	(0,1,0,0,0,1,1,1,1,0,1,1,0,1,0,0,0,1,0,0,0,1,1,1,1,0)
4	(0,0,0,1,1,0,1,0,1,1,1,0,0,1,0,0,0,0,0,1,1,0,1,0,1,1)
5	(0,1,0,0,1,1,1,0,1,0,1,1,0,0,0,0,0,1,0,0,1,1,1,0,1,0)
6	(1,0,1,0,0,1,1,1,1,1,0,1,1,0,0,0,1,0,1,0,0,1,1,1,1,1)
7	(1,1,1,0,1,1,1,1,0,0,0,1,0,0,1,0,1,1,1,0,1,1,1,1,0,0)

Different codes used in adjacent cells! Avoids training sequence disruption because of co-channel interference

Logical vs. Physical Channels

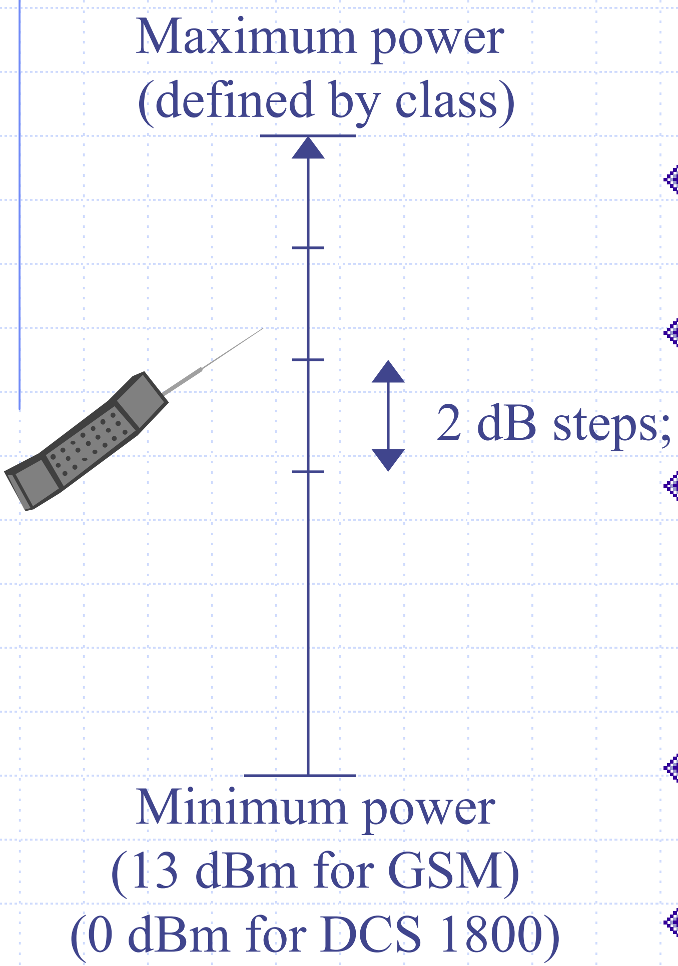
Logical channels (traffic channels, signaling (=control) channels)
Physical channels (FDMA/TDMA)

- Physical channels
  - Time slots @ given frequencies
  - Issues: modulation, slot synchronization, multiple access techniques, duplexing, frequency hopping, etc
- Logical channels
  - Built on top of phy channels
  - Issue: which information is exchanged between MS and BSS

GSM Logical Channels

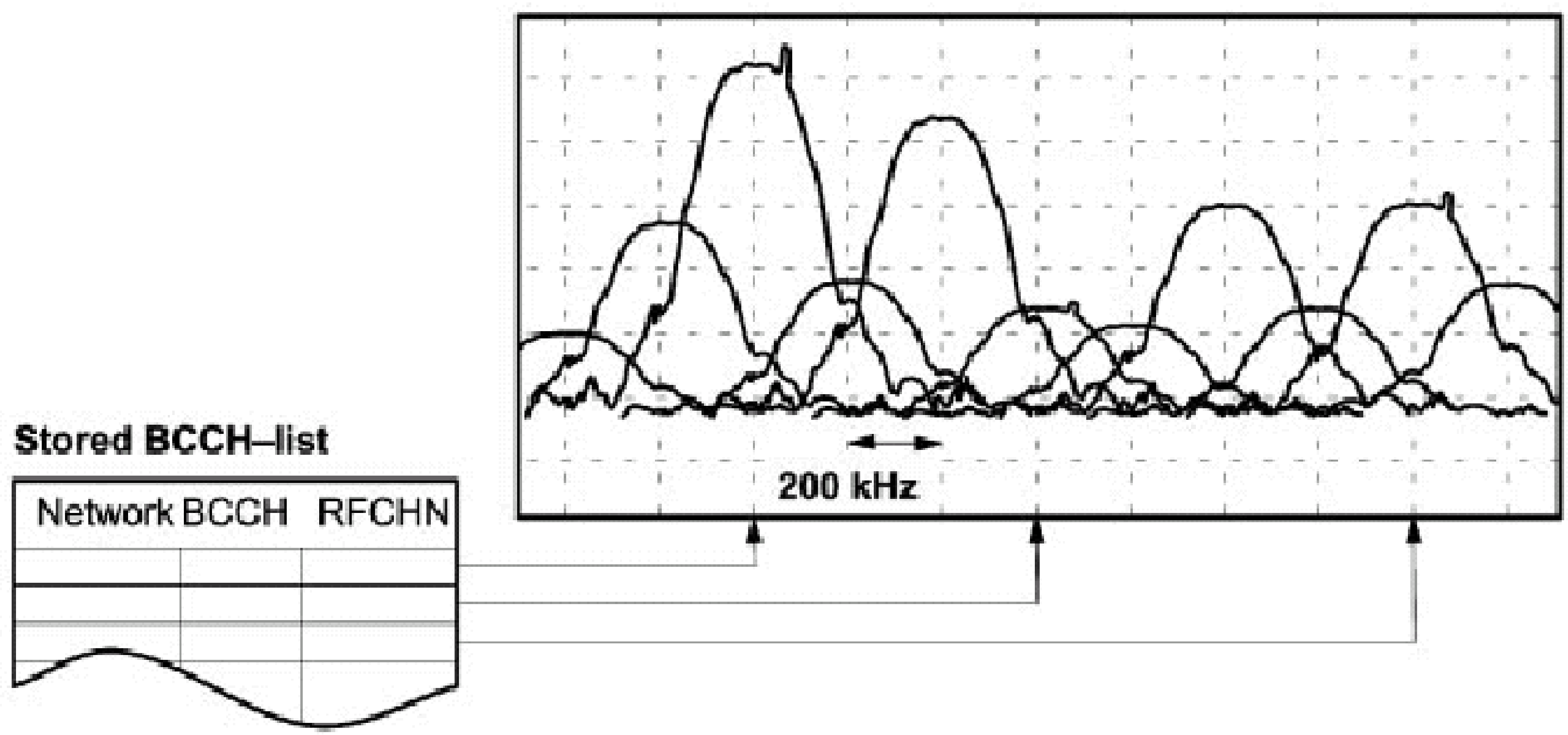
Traffic channel (TCH)	TCH/F	**TCH full rate**	**MS←→BSS**
	TCH/H	**TCH half Rate**	**MS←→BSS**
Broadcast channel	BCCH	**Broadcast control**	**BSS→MS**
(same information to all MS in a cell)	FCCH	**Frequency Correction**	**BSS→MS**
	SCH	**Synchronization**	**BSS→MS**
Common Control channel (CCCH)	RACH	**Random Access**	**MS→BSS**
(point to multipoint channels)	AGCH	**Access Grant**	**BSS→MS**
(used for access management)	PCH	**Paging**	**BSS→MS**
Dedicated Control channel (DCCH)	SDCCH	**Stand-alone Dedicated control**	**MS←→BSS**
(point-to-point signalling channels)	SACCH	**Slow associated control**	**MS←→BSS**
(dedicated to a specific MS)	FACCH	**Fast associated control**	**MS←→BSS**

Power Control



- MS has ability to reduce/increase power
  - Up to its power class maximum
- Maximum one 2 dB step every 60 ms
- Uplink power measures taken by BTS
- Notified back to MS
  - Power level values: 0-15
    - 0 = 43 dBm (20 W)
    - 15 = 13 dBm (20 mW)
- algorithm: manifacturer specific
  - runs on BSC
- Also on downlink

MS Powering Up



First operation when MS turned ON: spectrum analysis

(either on list of up to 32 Radio Frequency Channel Numbers of current network)

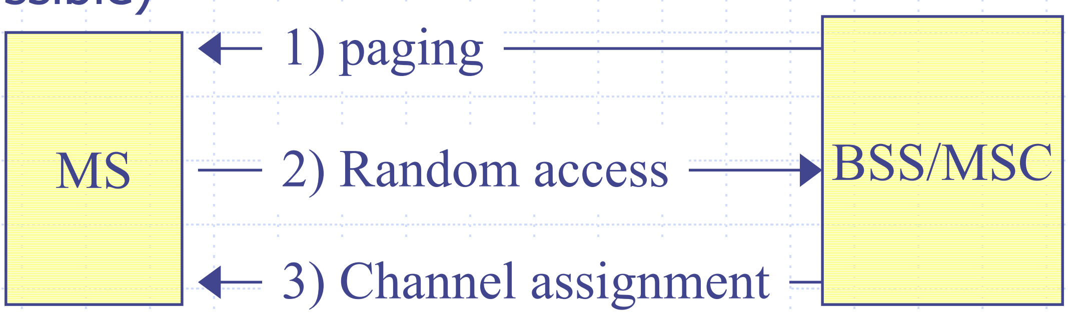
(or on whole 124 carriers spectrum)

Tuning

- MS listens on strongest beacon for a pure sine wave (FCCH)
  - Coarse bit synchronization
  - Fine tuning of oscillator
- Immediately follows SCH burst
  - Fine tuning of synchronization (64 bits training sequence)
  - Read burst content for synchronization data
- Finally, MS can read BCCH

Paging, 1

- Channel assignment:
  - only upon explicit request from MS
- Paging
  - needed to “wake-up” MS from IDLE state when incoming call arrives to MS
- MS accesses on RACH to ask for a channel
  - Generally SDCCH (but immediate TCH assignment is possible)



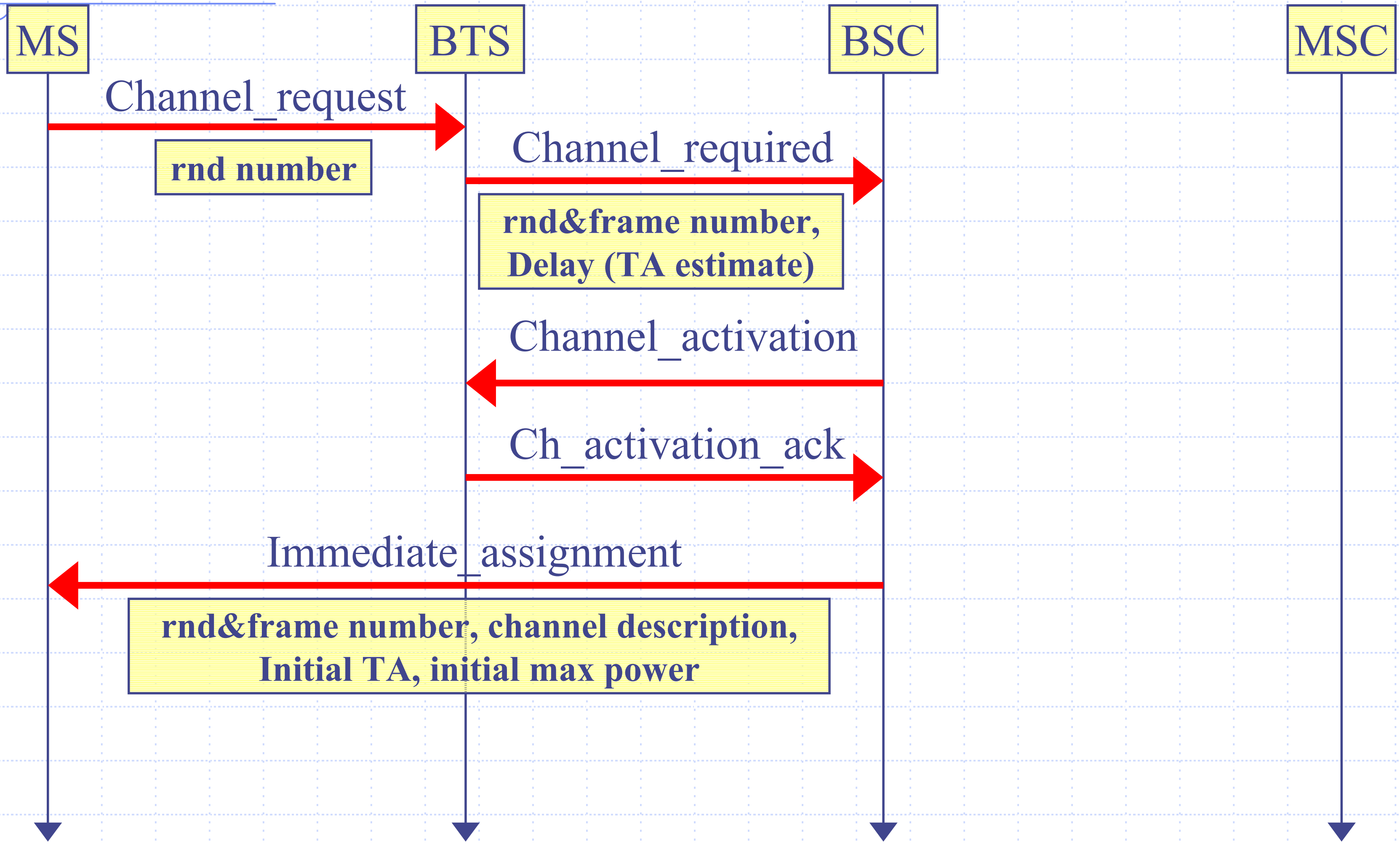
Paging channel: PCH
Access Grant Channel: AGCH
Random Access Channel: RACH

PCH and AGCH = PAGCH; PCH, AGCH and RACH = CCCH (Common Control CHannel)

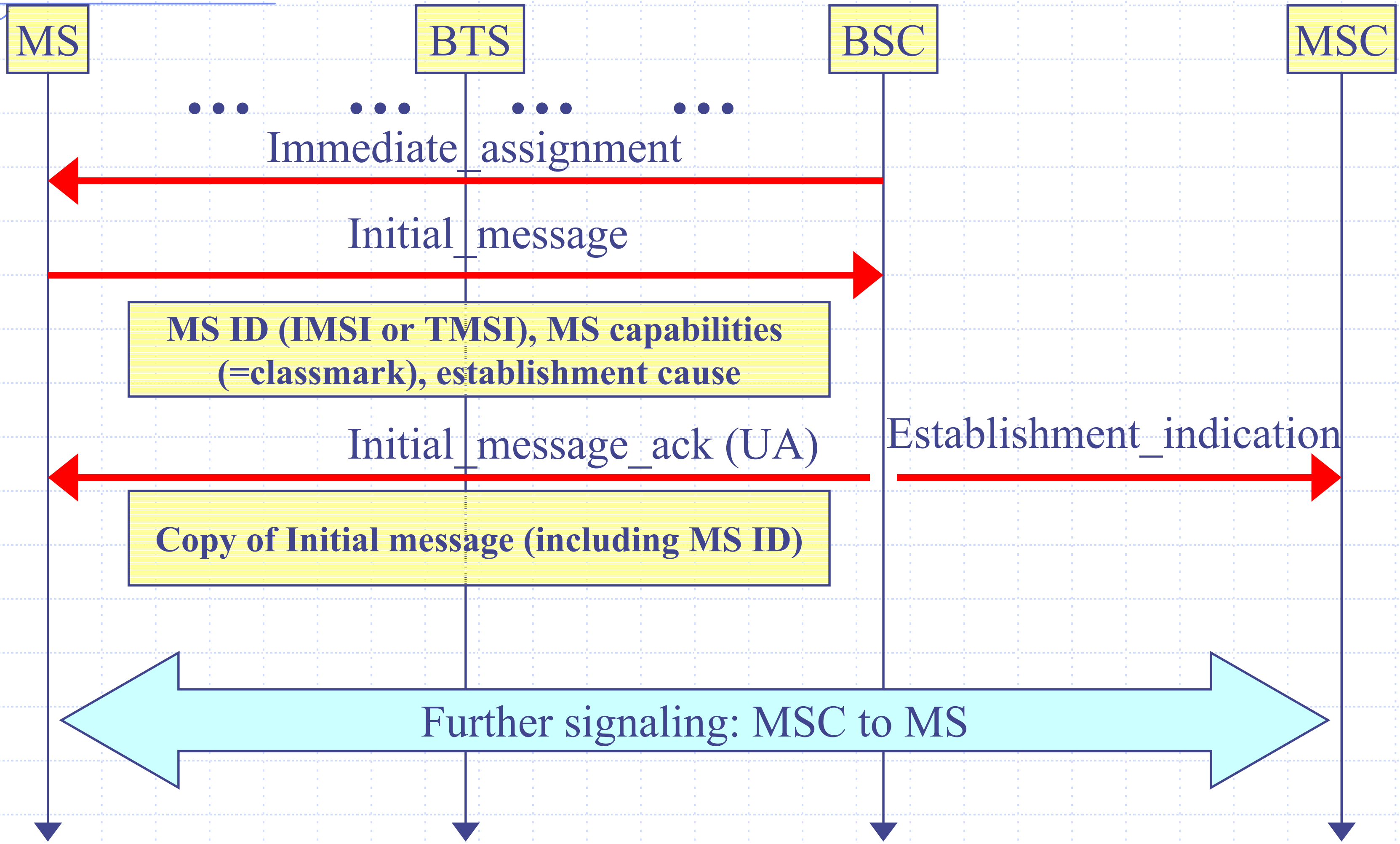
Paging, 2

- Paging message generated by MSC (receives incoming call)
- Transferred to subset of BSC
  - Paging limited to user's location area
  - Paging message contains:
    - List of cells where paging should be performed
    - Identity of paged user
- Paging message coded in 4 consecutive bursts over the air interface
- Paging for more MSs may be joined in one unique paging message

Access Signaling, 1



Access Signaling, 2



Assignments

- Read Chapter 9 of the textbook
- Updated information on the class web page:

  www.ece.neu.edu/courses/eceg364/2004sp