

EFREI M1

Mobile Networks

GSM Networks

Paul Simmons

Tamum Consulting February 2013

GSM Networks-1

- The GSM radio interface:
 - Radio interface basics
 - Structure of the GSM radio interface

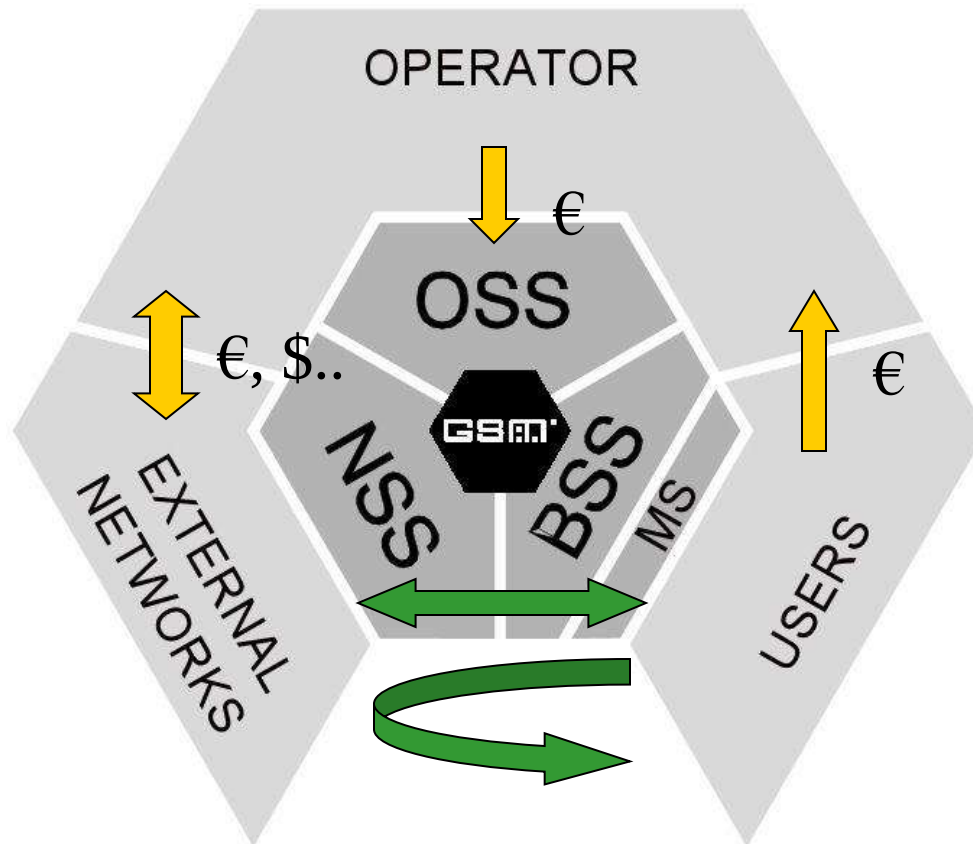
GSM Networks-2

- GSM Architecture
 - Call routing
 - Location Updating and Cell Selection
 - Dedicated Channel Assignment
 - GSM Protocol Structure

Engineering Problem 4: GSM Architecture and Function

- Problem statement: How to create information flows necessary to establish efficient and quality communication between mobile users and their correspondants?
- And how to pay for it?

GSM Architecture-Basic



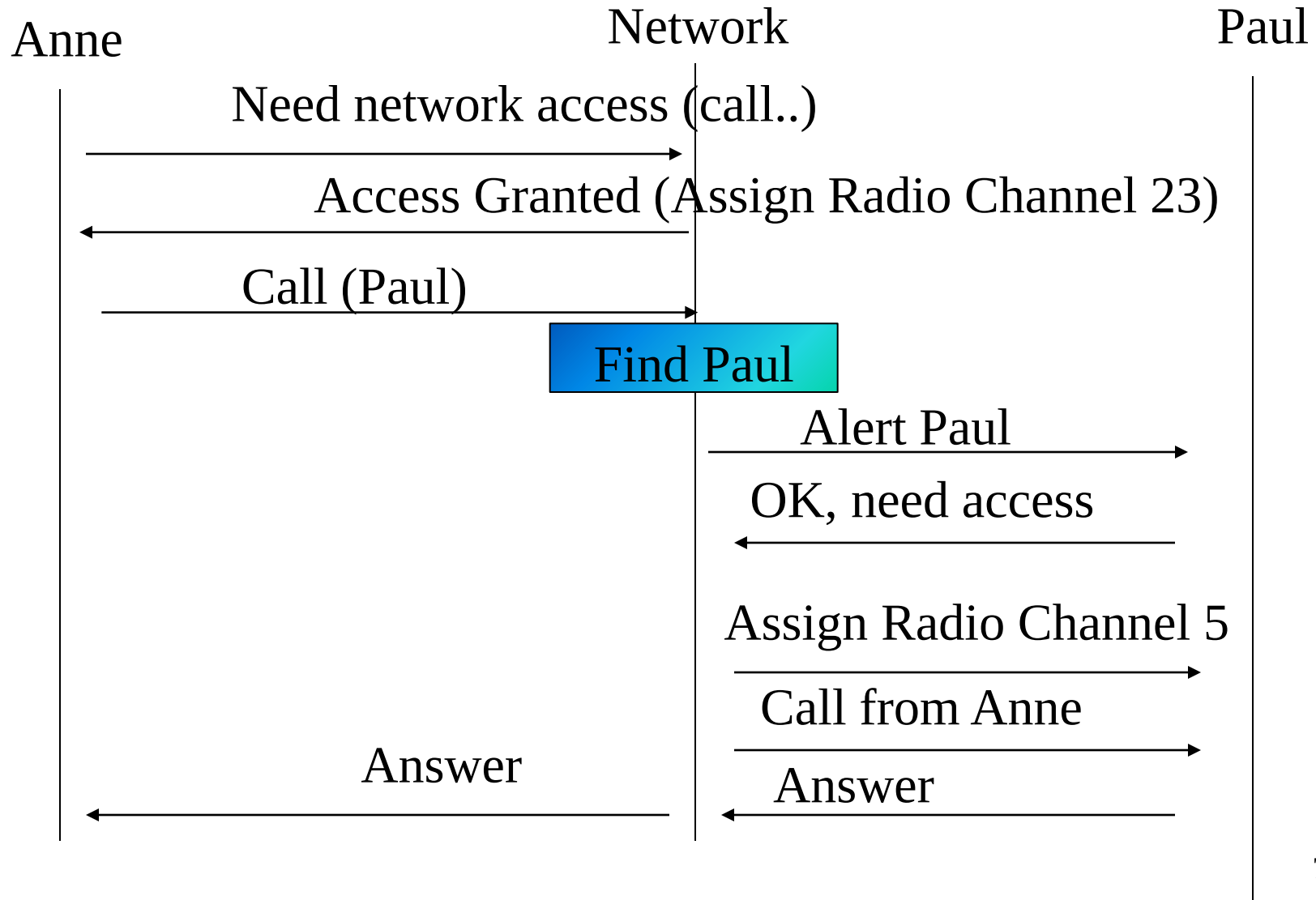
Source: Mouly & Pautot



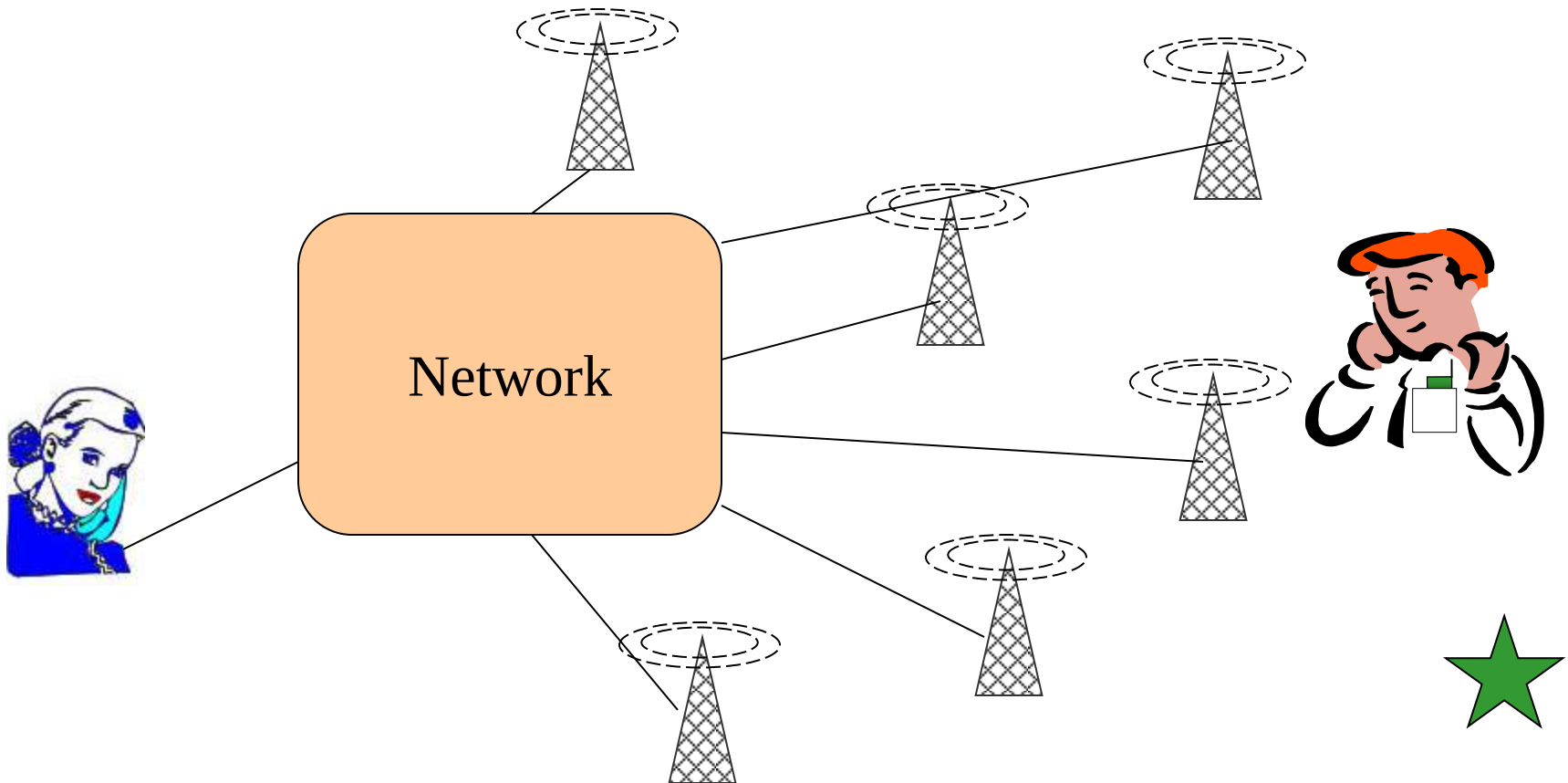
EP4.1 Call routing

- Problem: How to route a call to a user who is mobile?
- Method:
 - Analyse alternatives:
 - Paging
 - Home Location Register

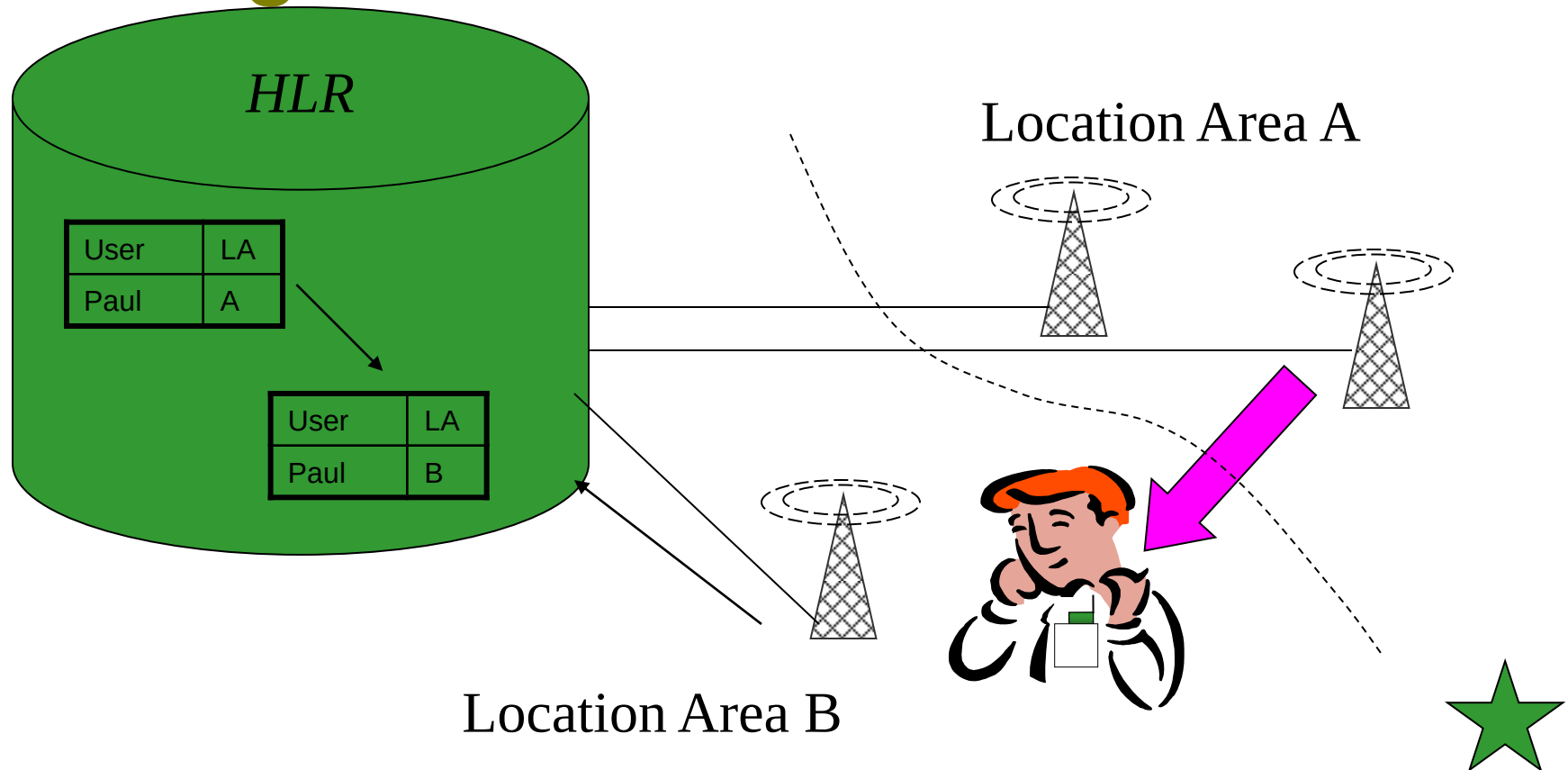
Simplified radio protocol for call setup



Finding by Paging



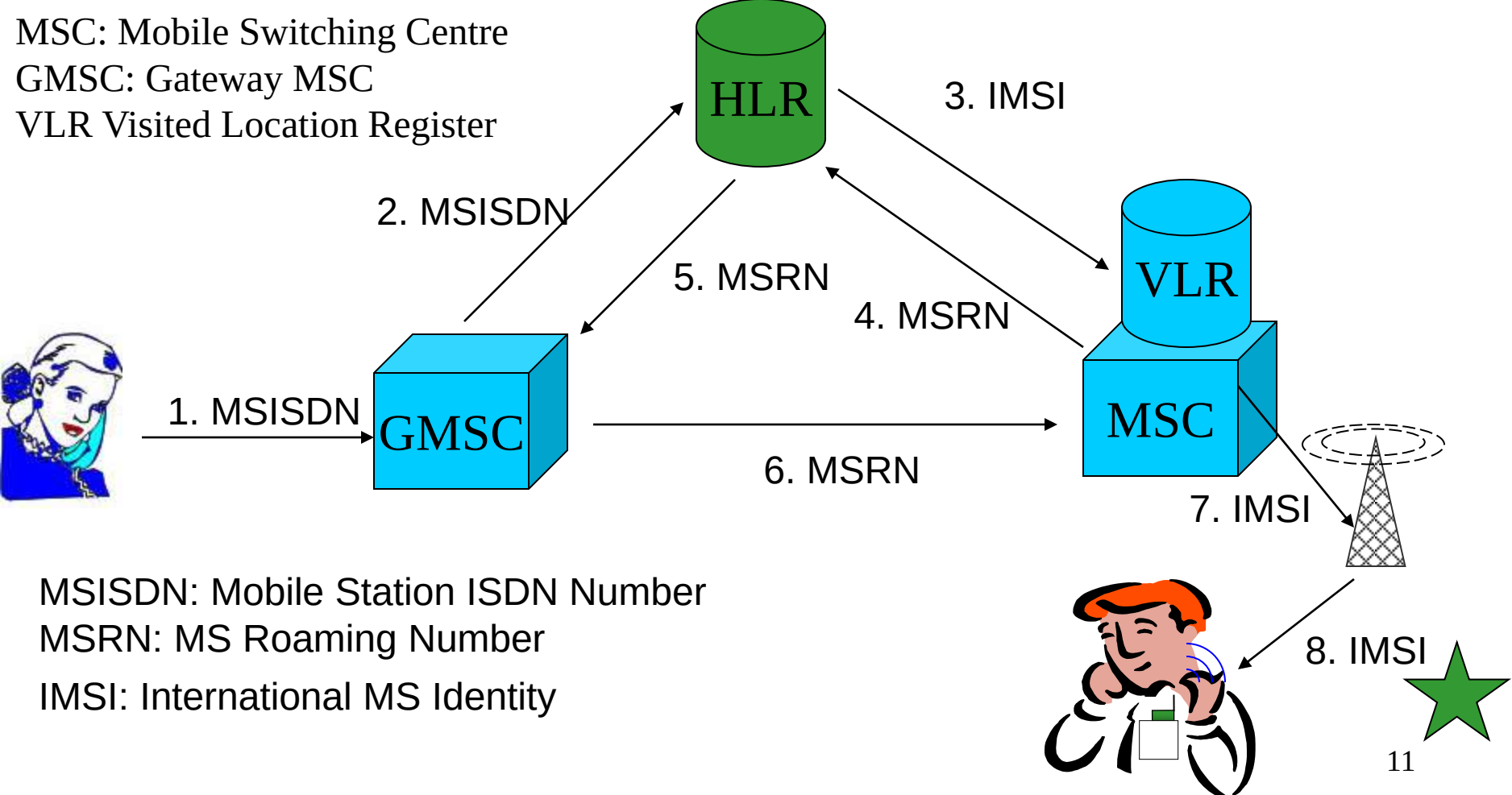
Finding by Home Location Register and Location Area



Use of Visited Location Register (VLR)

- In practice, to prevent too frequent updating of the HLR, GSM HLRs store just the addresses of a location register responsible for the location areas of the mobile: the VLR (Visited Location Register), and it's local MSC
- The VLR stores the more precise location area of the mobile (area where it should be paged). On request from the HLR the VLR provides a Mobile Station Roaming Number (MSRN) for routing of calls.

Routing by Location Register (after Location Updating)



EP4.1 Call routing: Solution

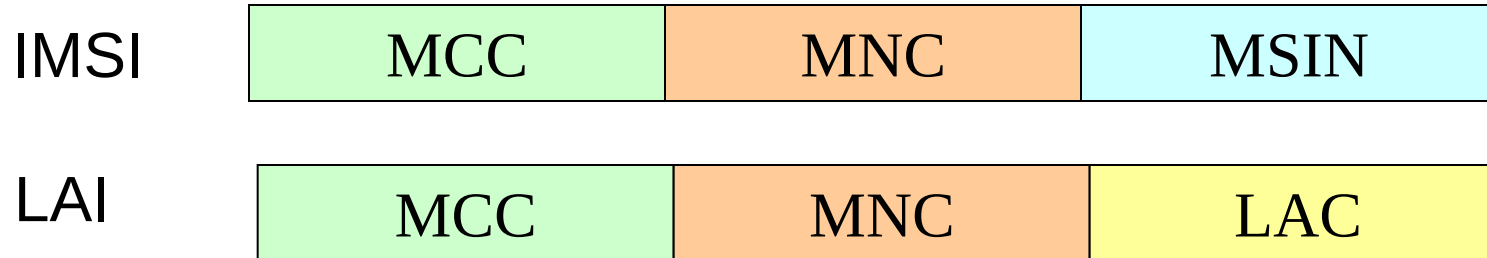
- Problem: How to route a call to a user who is mobile?
- Solution:
 - Paging alone is too expensive
 - Location Registers (HLR + VLR) store user broad location information
 - Location registers with paging provide an effective solution



EP4.2 Location Updating and Cell Selection

- Problem: How to choose the best cell for a mobile station, network and the subscriber?
- Issues:
 - Radio parameter and subscription matter
 - Occurs at switch on and during mobility (idle mode)
 - During call, handover procedure takes precedence

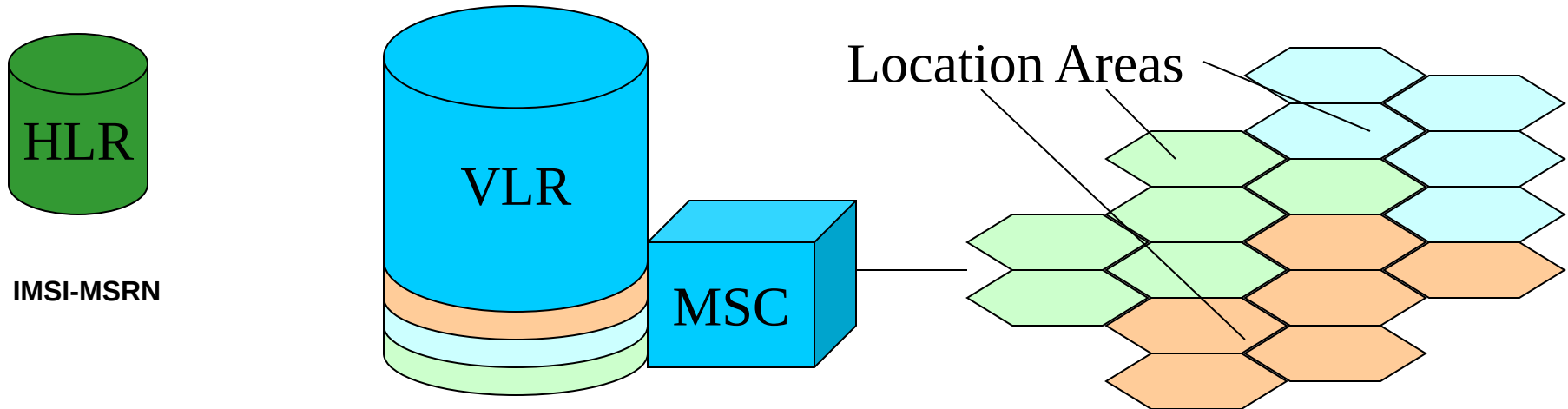
IMSI and LAI



- IMSI: International Mobile Subscriber Identity: Uniquely identifies the mobile subscriber
- LAI: Location Area Identification
- MCC: Mobile Country Code: identifies the country of the mobile subscriber;
- MNC: Mobile Network Code: identifies the home PLMN of the mobile subscriber
- MSIN: Mobile Subscriber Identification Number identifies the mobile subscriber within a PLMN
- LAC: Location Area Code : identifies a location area within a PLMN



Cell Selection, Reselection and Location Updating



- PLMN: Public Land Mobile Network, Identified by MCC and MNC. Operates mobile network within a country. Functionally one HLR
- Available PLMN: One that has at least one unbarred cell.
- Suitable cell: part of the selected PLMN, is unbarred, path loss criterion $C1 > 0$.
- Normal Location Updating: when LAI received on the BCCH of the selected cell $\neq$ the LAI stored (when MS is switched on or moves to a new LA).



Cell Selection and Reselection

- The MS is camped on a cell (selects it) when the cell is suitable and it stays tuned to the BCCH + CCCH of that cell --> BCCH data, Paging msgs and Radio Access and are obtained from that cell.
- The list of all BCCH carriers in use by a given PLMN, in a given area is included in the System Information message BCCH (BCCH Allocation List = BA).
- Note: BA(BCCH) may or may not be identical to BA(SACCH) sent in System Information message on the SACCH which indicates to the MS those BCCH carriers to be monitored during the Handover process.

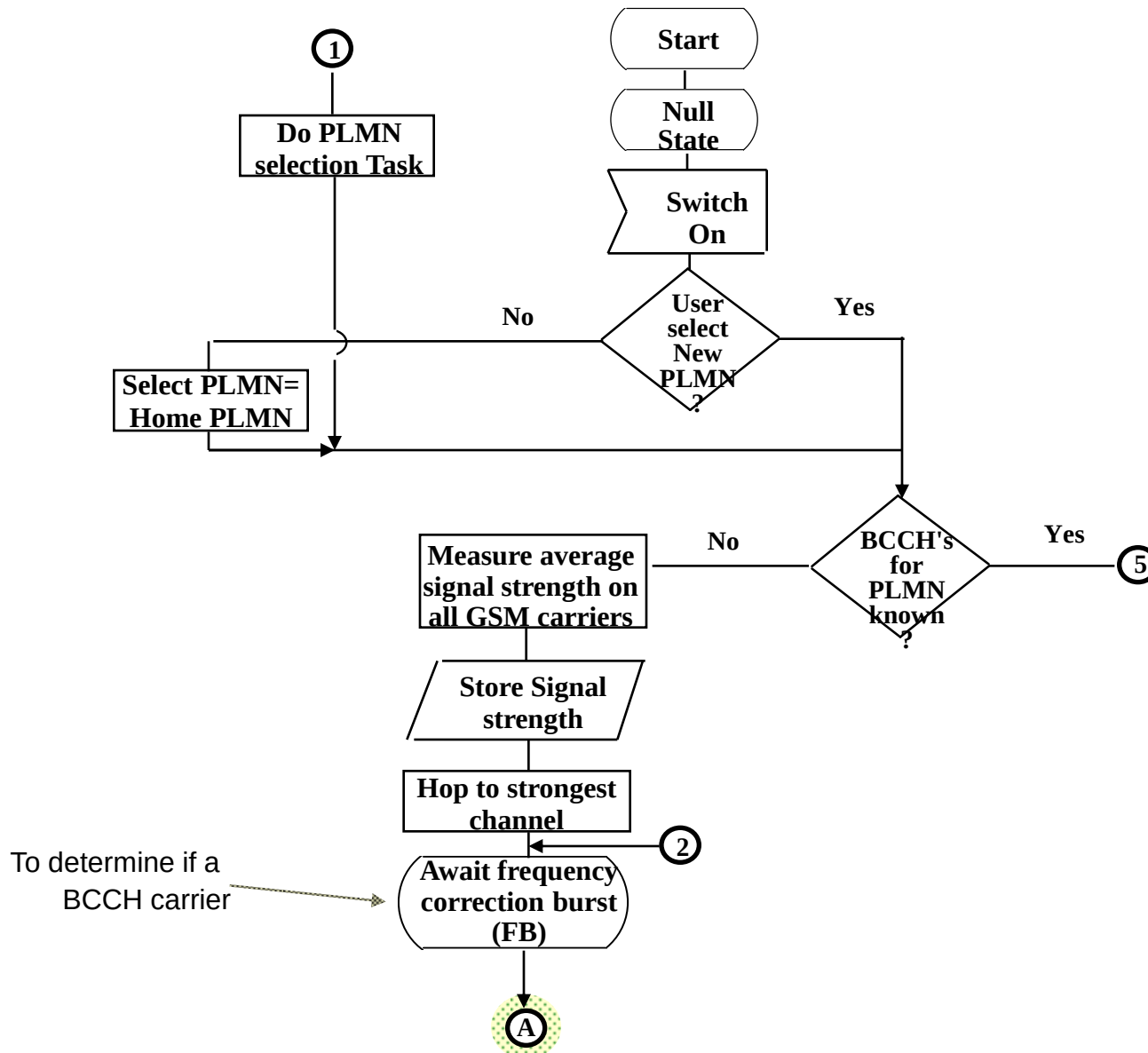
To execute the process of cell selection and reselection the MS maintains an average of RXLEVEL for all monitored frequencies.



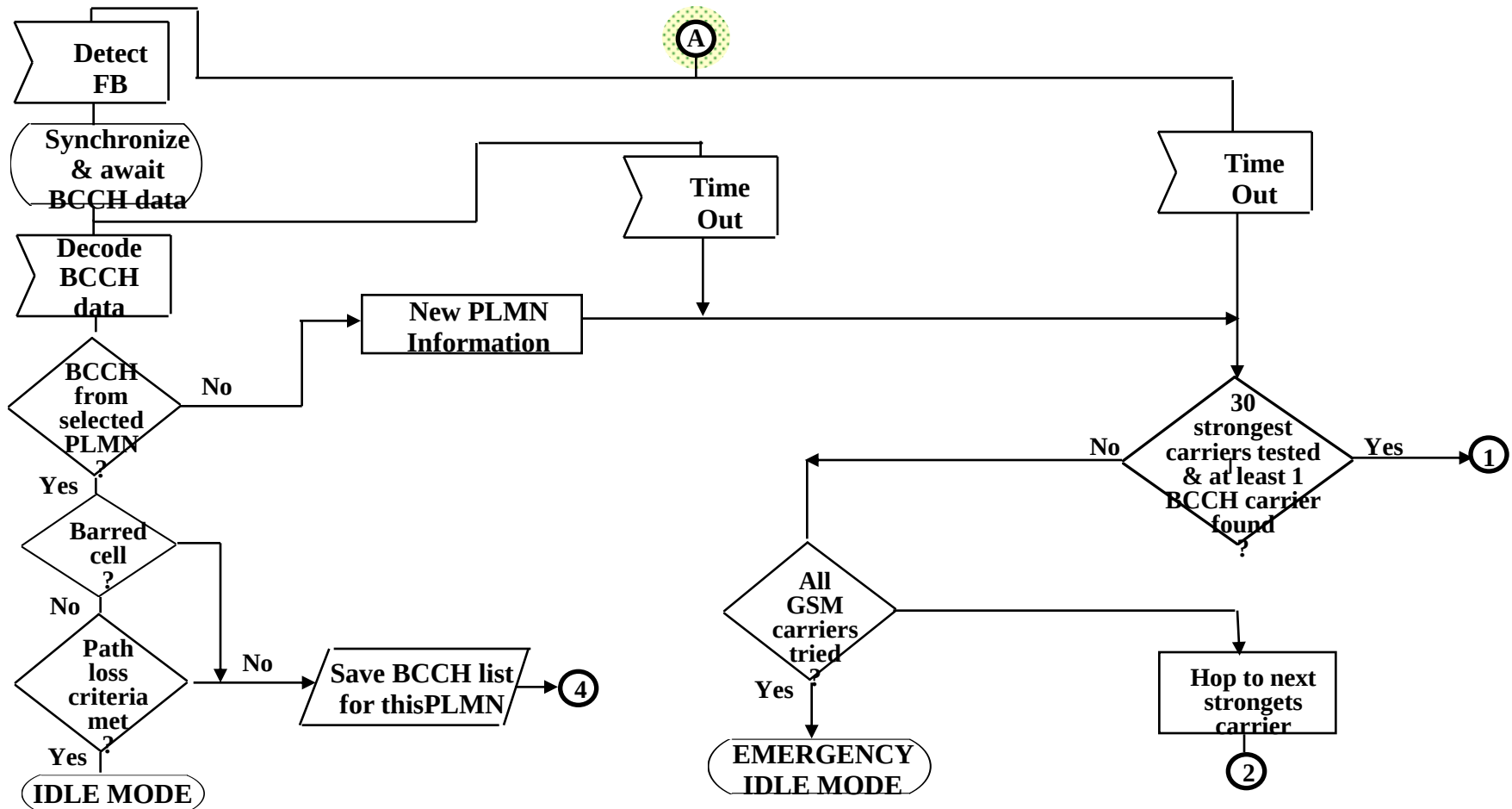
System Information on BCCH and SACCH

- Type 1 (on BCCH): RACH control and cell allocation.
- Type 2 (on BCCH) :RACH control and BCCH allocation in neighboring cells.
- Type 3 (on BCCH): RACH control , LAI, Cell Identity, and other cell information.
- Type 4 (on BCCH): RACH control, LAI, Cell Identity, CBCH description, and other cell info.
- Type 5 (on SACCH): BCCH allocation in the neighbor cells for H/O purposes.
- Type 6 (on SACCH): LAI, Cell Identity, and other information.

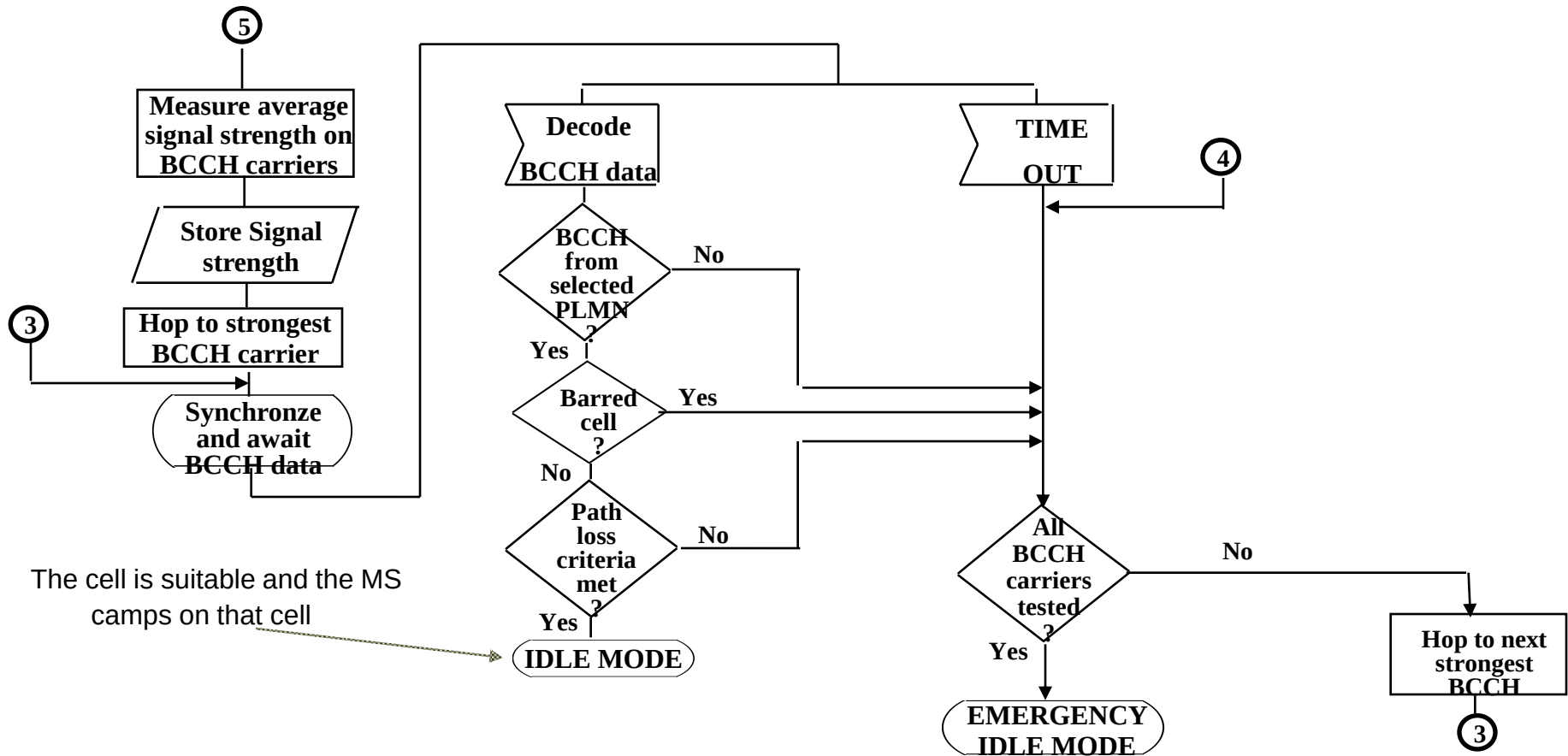
Cell Selection at Switch On.



Cell Selection at Switch On (cont.)

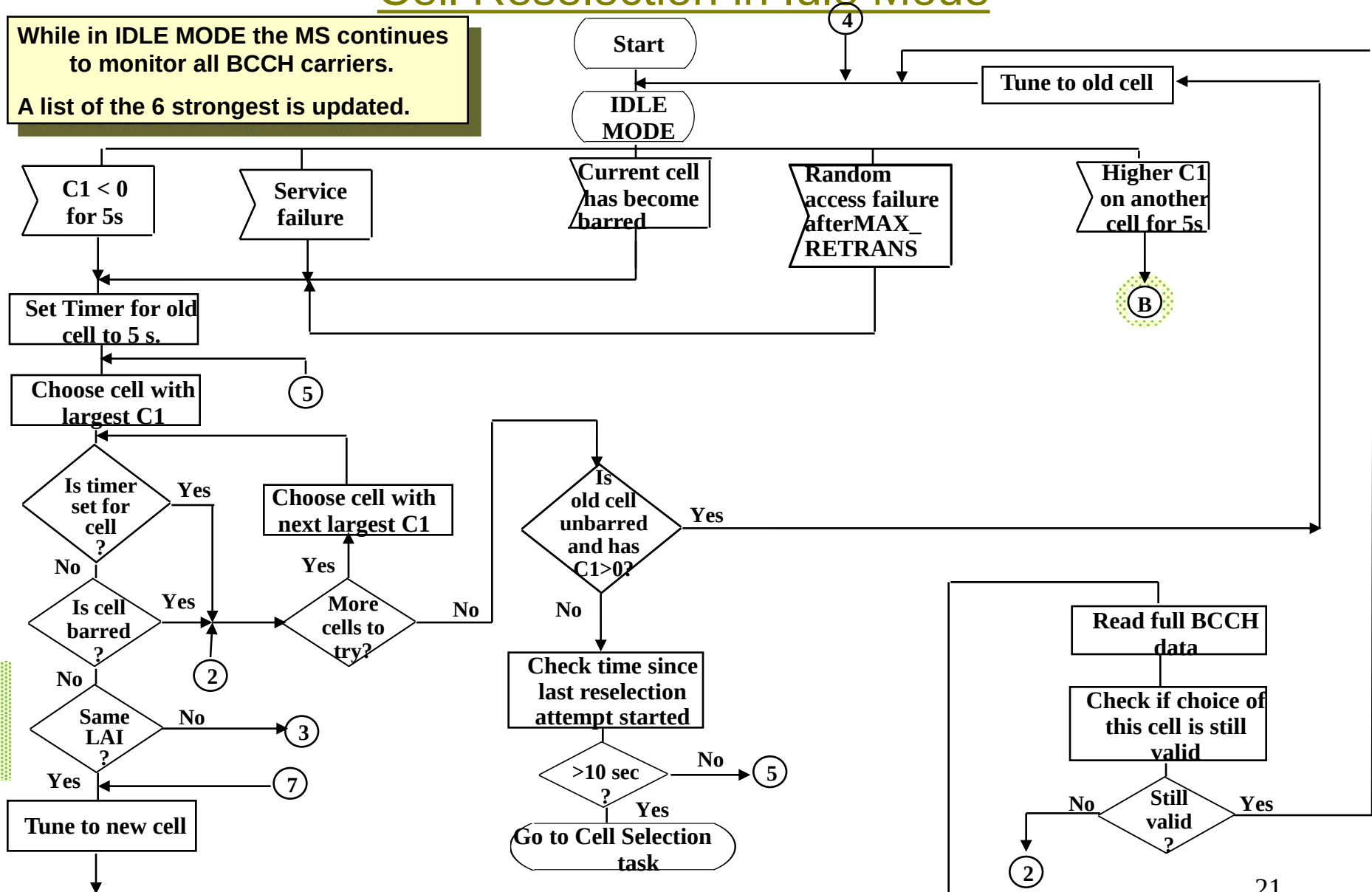


Cell Selection at Switch On (cont.)

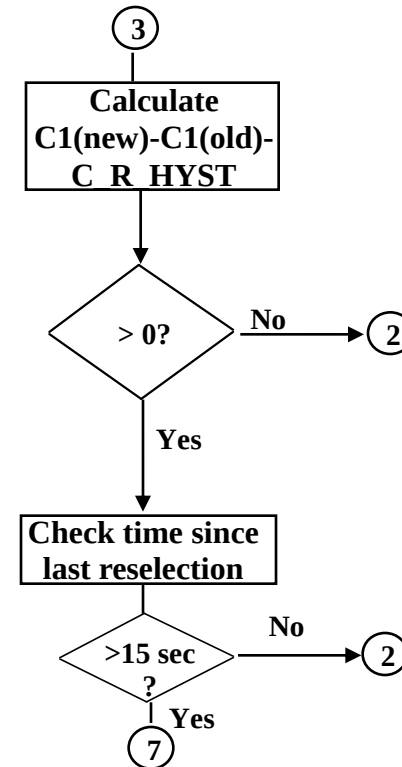
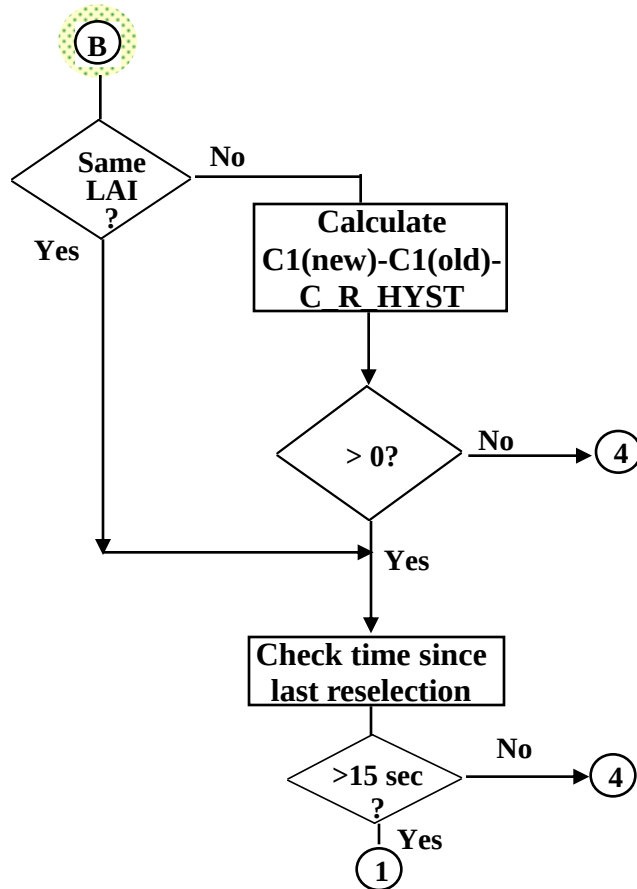


Cell Reselection in Idle Mode

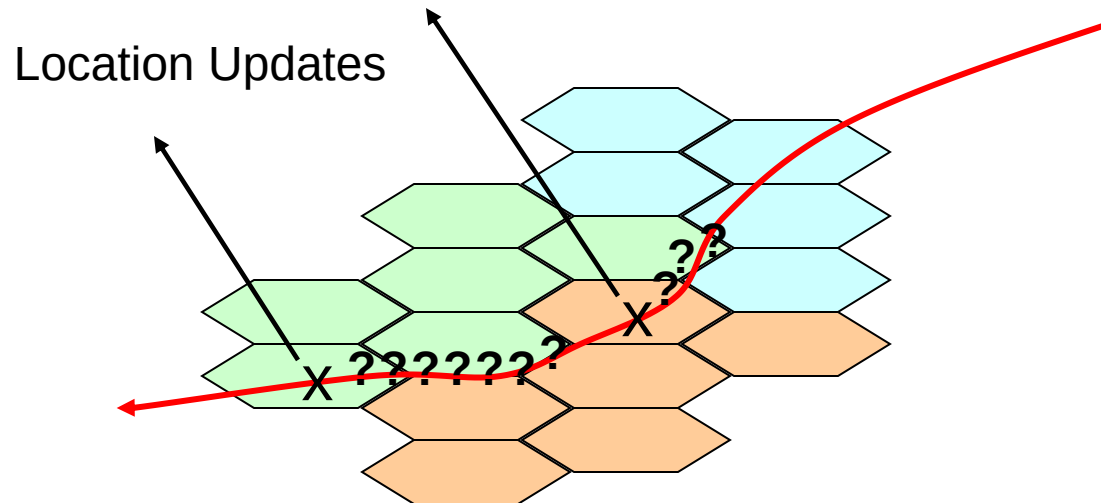
While in IDLE MODE the MS continues to monitor all BCCH carriers.
A list of the 6 strongest is updated.



Cell Reselection in Idle Mode (cont.)



Cell re-selection hysteresis



- Cell hysteresis added to criteria for cells on border of location areas
- Reduced sensitivity of re-selection reduces location update load

Roaming

- Within his home country, a mobile subscriber will normally stay within coverage of his Home PLMN
 - I.e. $(\text{MCC}+\text{MNC})_{\text{IMSI}} = (\text{MCC}+\text{MNC})_{\text{LAI}}$
- When changing country, or changing network coverage within a foreign country, or when local agreements allow, a mobile station may move onto the coverage of a different PLMN. Receiving service from this Visited PLMN is known as roaming.
- Permission to roam is subject to agreements between the Home PLMN and Visited PLMN.



EP4.2 Solution: Location Updating and Cell Selection

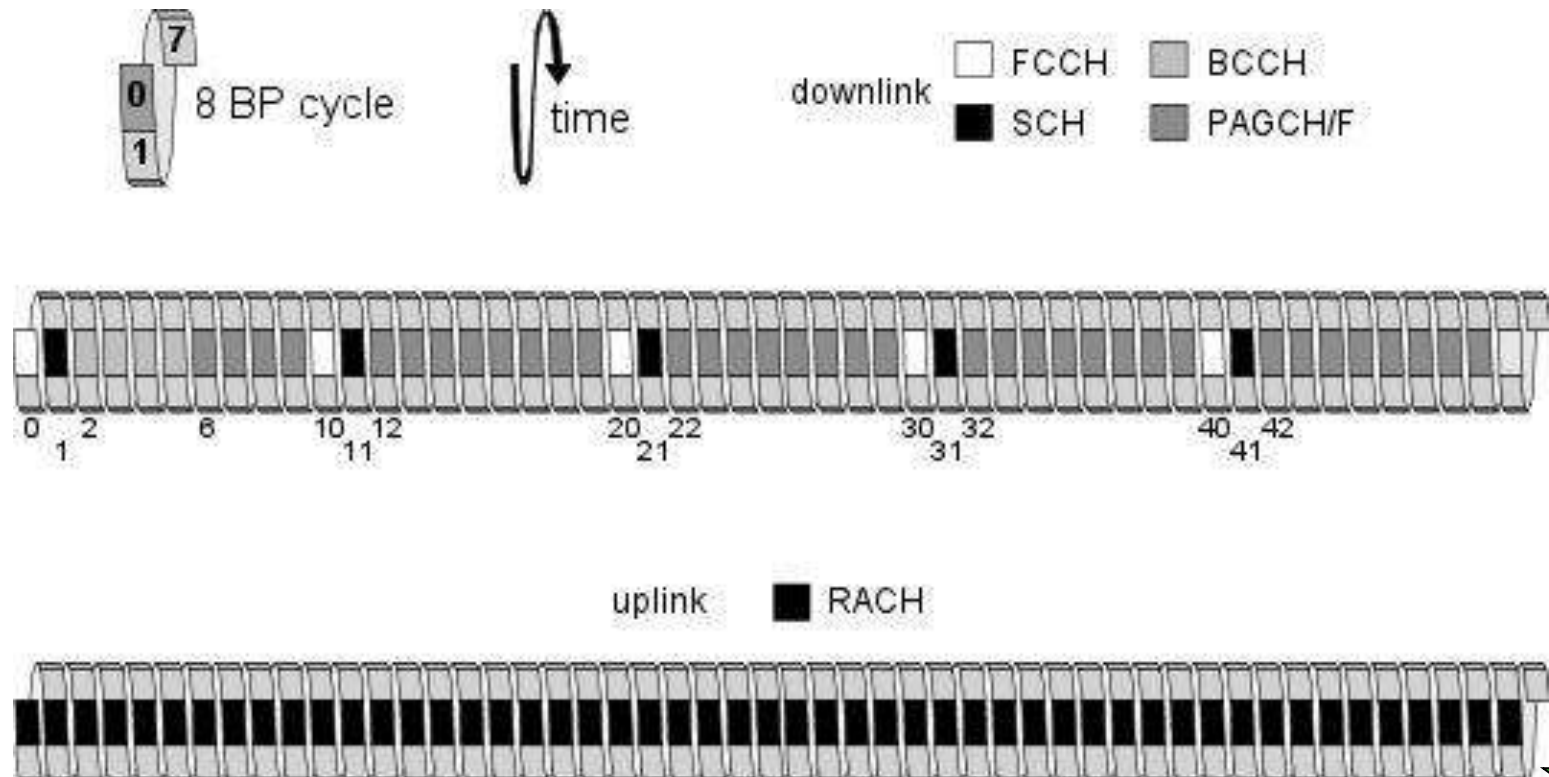
- Problem: How to choose the best cell for a mobile station, network and the subscriber?
- Solution:
 - Mobile station at switch on and in idle mode scans radio environment
 - Uses radio and network broadcast parameters to determine best cell
 - If location area changes, perform location update
 - Provide hysteresis to control location update load



EP 4.3 Dedicated Channel Assignment

- Problem:
 - After cell selection, before a call can be established or even a message (e.g.. Location update) sent, the mobile must receive a dedicated channel
 - How to request a communication channel without an assigned communication channel?

Common Channel Organisation



Typical only; allocations vary according to traffic needs
 Note: PAGCH= PCH+AGCH; /F= full rate traffic



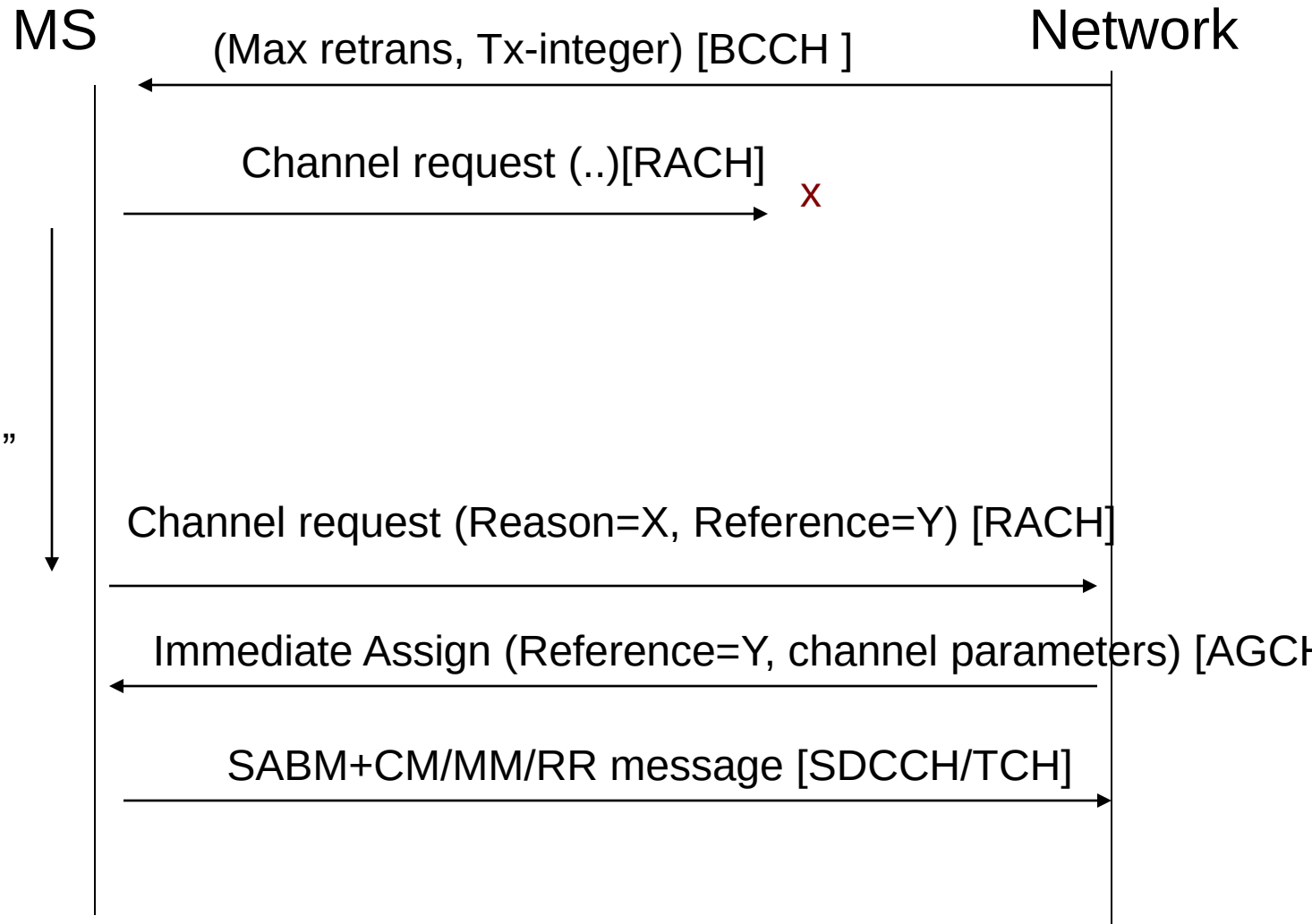
Dedicated channel assignment

- Each cell contains a carrier where the Timeslot Number $TN=0$ of each TDMA frame in the downlink contains the SCH, FCH, BCCH, and PAGCH.
- The $TN=0$ on the uplink is used for random access: the RACH channel*
- The RACH channel, shared by all mobiles in a cell, is used for sending channel requests by randomly spaced (slotted) Aloha attempts
- The random spacing and number of retries is controlled by the cell BCCH



* Typically; $TN=0$ may also be shared with TCH

Initial Assignment



EP 4.3 Solution: Dedicated Channel Assignment

- Problem:
 - How to request a communication channel without an assigned communication channel?
- Solution:
 - Use a slotted Aloha protocol on the RACH, controlled by the BCCH and acknowledged by the AGCH



EP 4.4 GSM Protocol Structure

- Problem:
 - GSM Information Flows are complex, heirarchical on access and many-to-many in network
 - Bandwidth and time (especially on radio interface) are limited
 - Changes might be needed! New requirements will arise
 - How to structure protocols?

GSM Network Entities-I

- MS - Mobile Station
- BSS - Base Station System
- NSS - Network & Switching Subsystem
- OSS - Operation SubSystem
- PSTN - Public Switched Telephone Network
- SIM - Subscriber Identification Module
- ME - Mobile Equipment.
- BTS - Base Transceiver System
- BSC - Base Station Controller

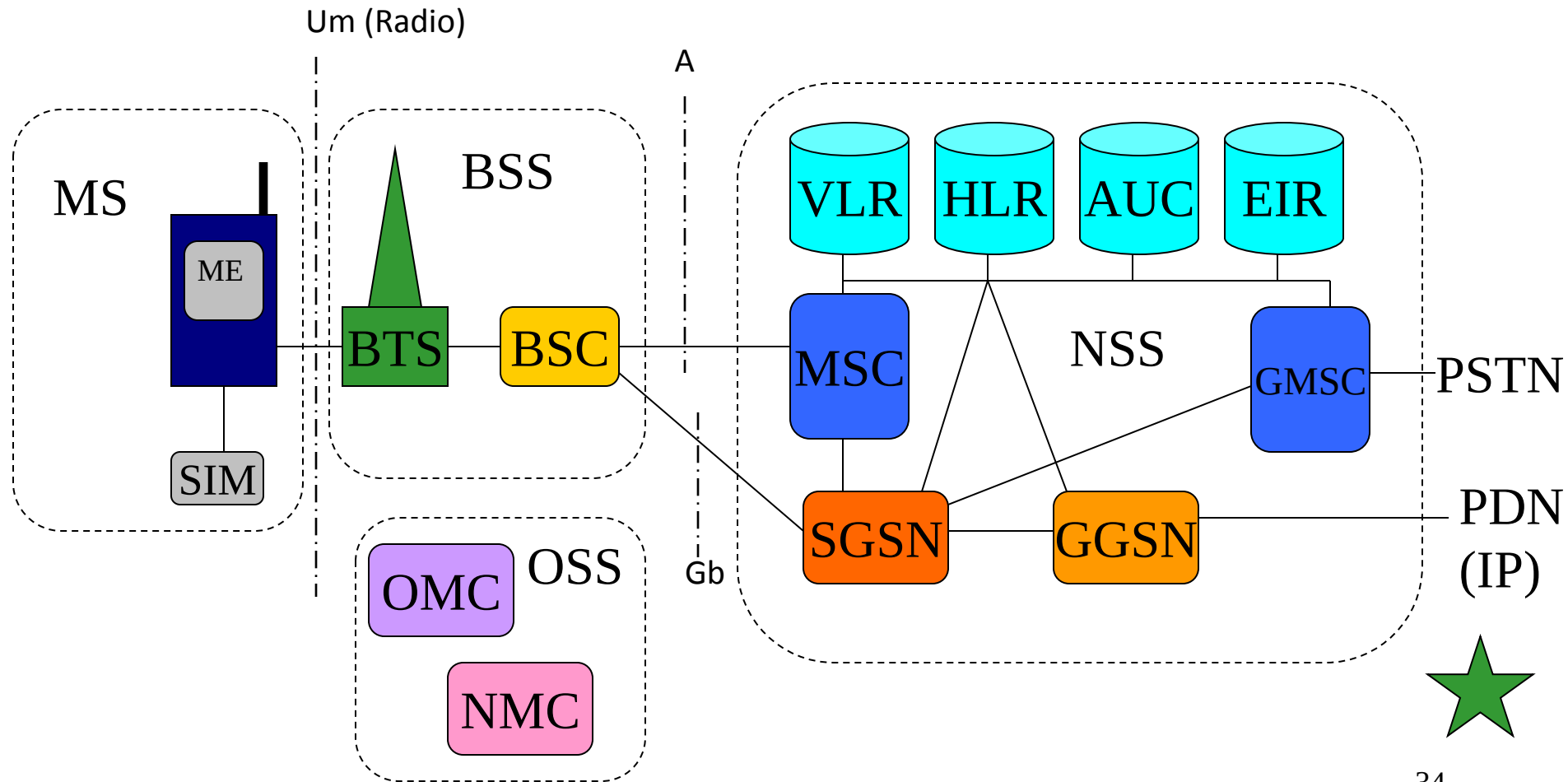


GSM Network Entities-II

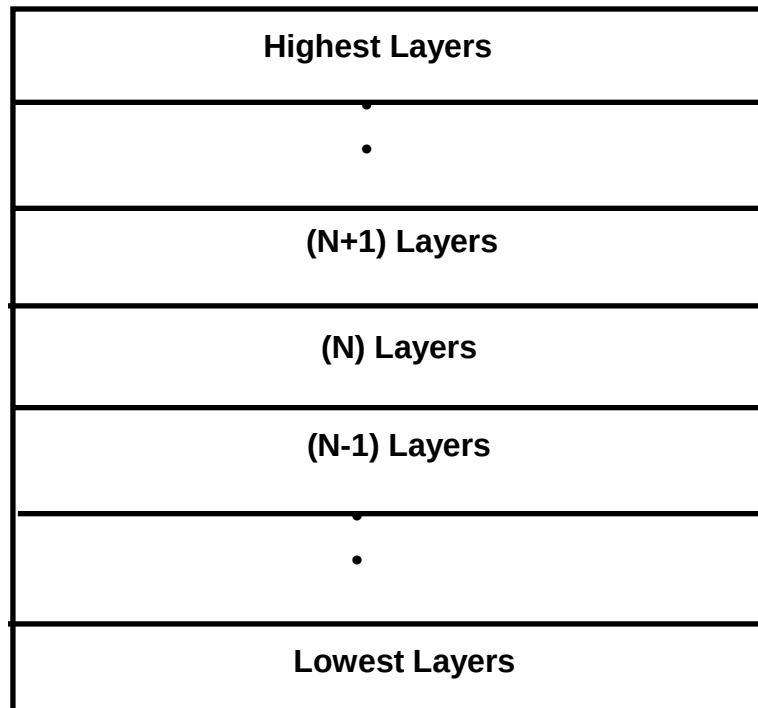
- MSC - Mobile services Switching Center
- HLR - Home Location Register
- VLR -Visited Location Register
- EIR - Equipment Identity Register
- AuC - Authentication Centre
- OMC - Operations and Maintenance Centre
- NMC - Network Management Centre
- SGSN - Serving GPRS Support Node
- GGSN - Gateway GPRS Support Node



GSM Network Architecture



OSI protocol layer model

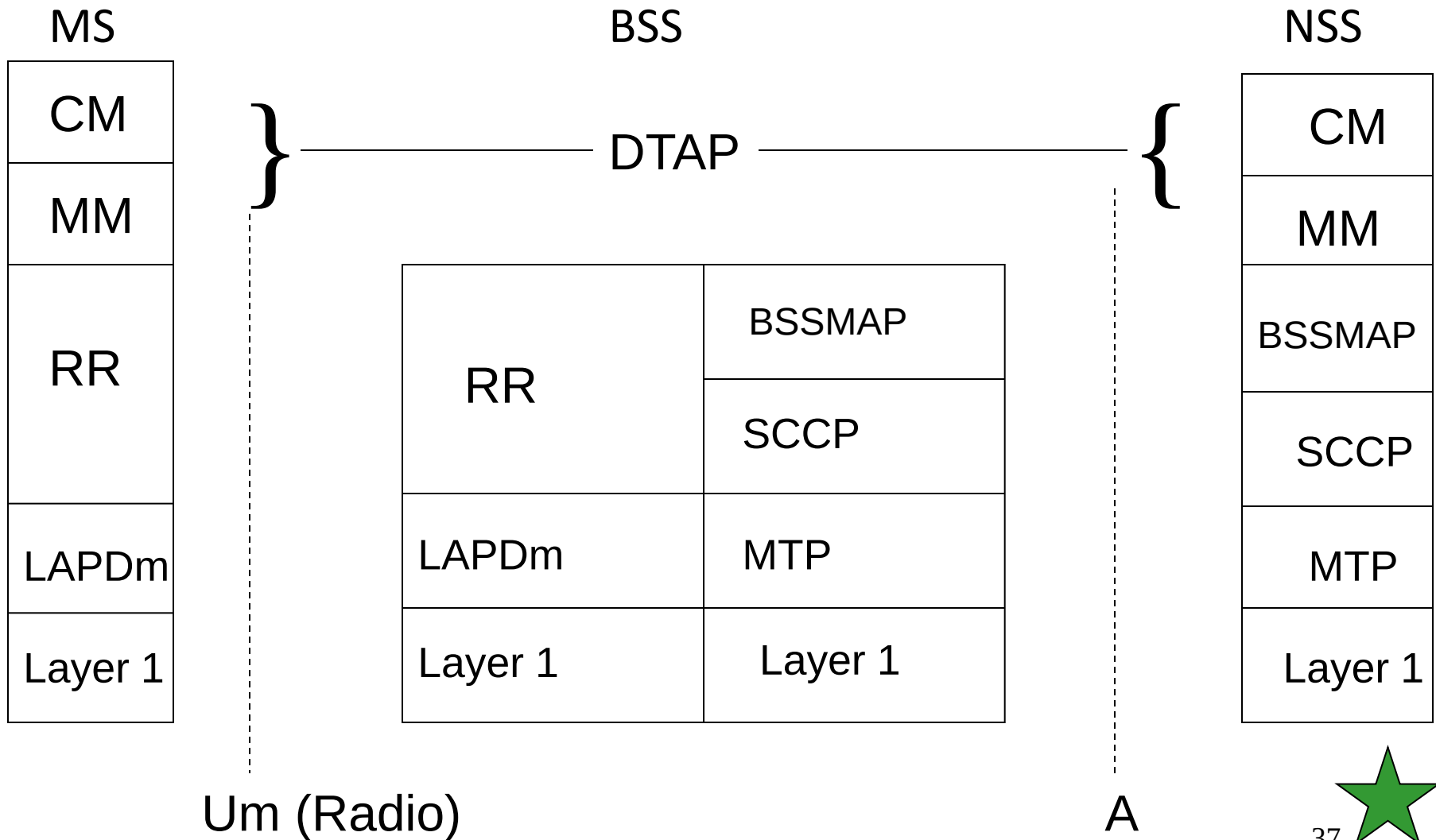


GSM Radio Access signalling protocols (Um Interface)

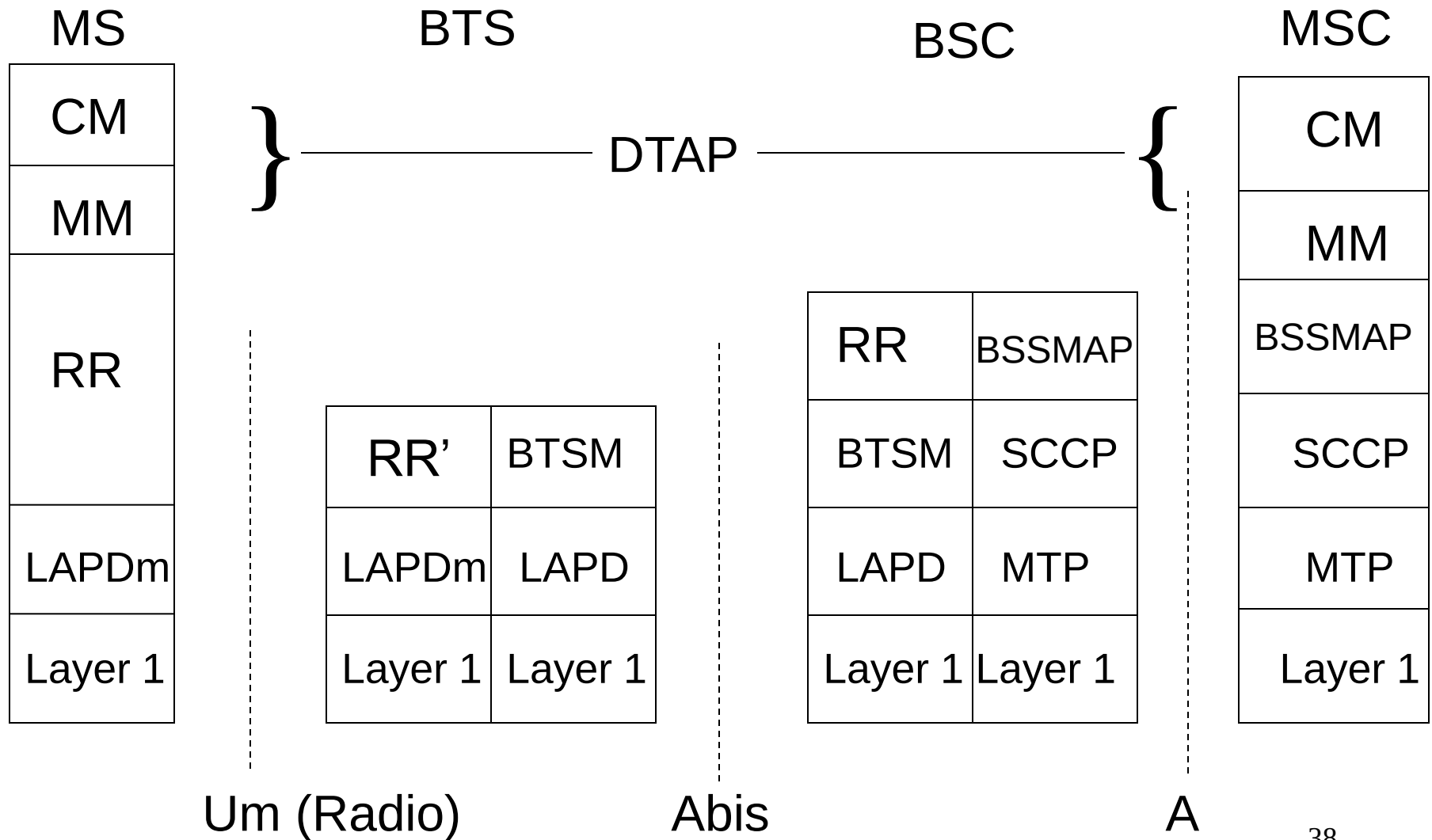
- One Layer 2 Protocol:
 - LAPDm (Mobile Link Access protocol)
 - multiplexed by SAP;
 - SAPI=0 for signalling
 - SAPI=3 for SMS
- Multiple “Layer 3” protocols, identified by a protocol discriminator (PD).
 - The 3 basic (non-GPRS) L3 sub-layers are:
 - Connection Management (CM)
 - Mobility Management (MM)
 - CM+MM=Direct Transfer Application Part (in network)
 - Radio Resource management (RR)



GSM Access protocols-I



GSM Access protocols-II



Error Detection and Correction

- Transmission of information is susceptible to errors
- Errors can be detected and corrected by transmitting related “redundant” information, for example repeating. This “redundancy” can be applied in several ways to improve detection and correction
- There are two main types of correction used:
 - Forward Error Correction (FEC): correction is by redundancy contained within the information
 - Automatic ReQuest for retransmission (ARQ): correction is by repetition of information containing detected errors

Forward Error Correction

- There are two main types of FEC:
 - Block codes
 - Convolutional codes
- All error correcting codes add redundancy to detect and correct errors
- Block Codes add several redundant bits related to a block of data bits
- Convolution codes add redundancy by adding a time-shifted function of the original data bits

Block Code for Error detection- Parity

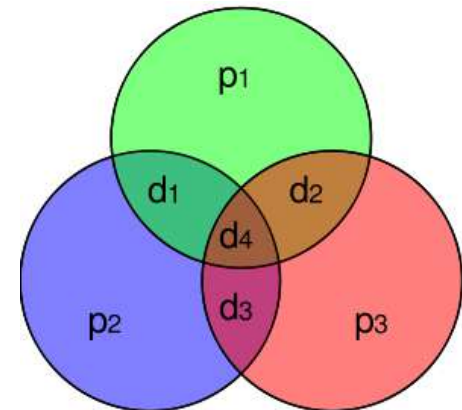
- Two variants, even and odd
- Even parity set to make the total sum even
- Odd parity is set make the total sum odd
- Example: 3 data bits, even parity

d1	d2	d3	even parity
0	0	0	0
0	1	0	1
1	1	0	0
1	1	1	1

- If the total sum is not even, we have an error!
- Only single errors detected
- No correction

Error correcting block codes

- To prevent computer crashes resulting from night-time relay failures, in 1950 Richard Hamming invented some automatic correcting codes
- Example: Hamming (7,4)
 - 4 data bits + 3 parity
 - Parity bit p_1 protects data bits d_1 , d_2 , d_4 (see diagram)
 - The different coverage allows an erroneous bit (including parity) to be pinpointed- hence corrected
 - Only corrects single errors

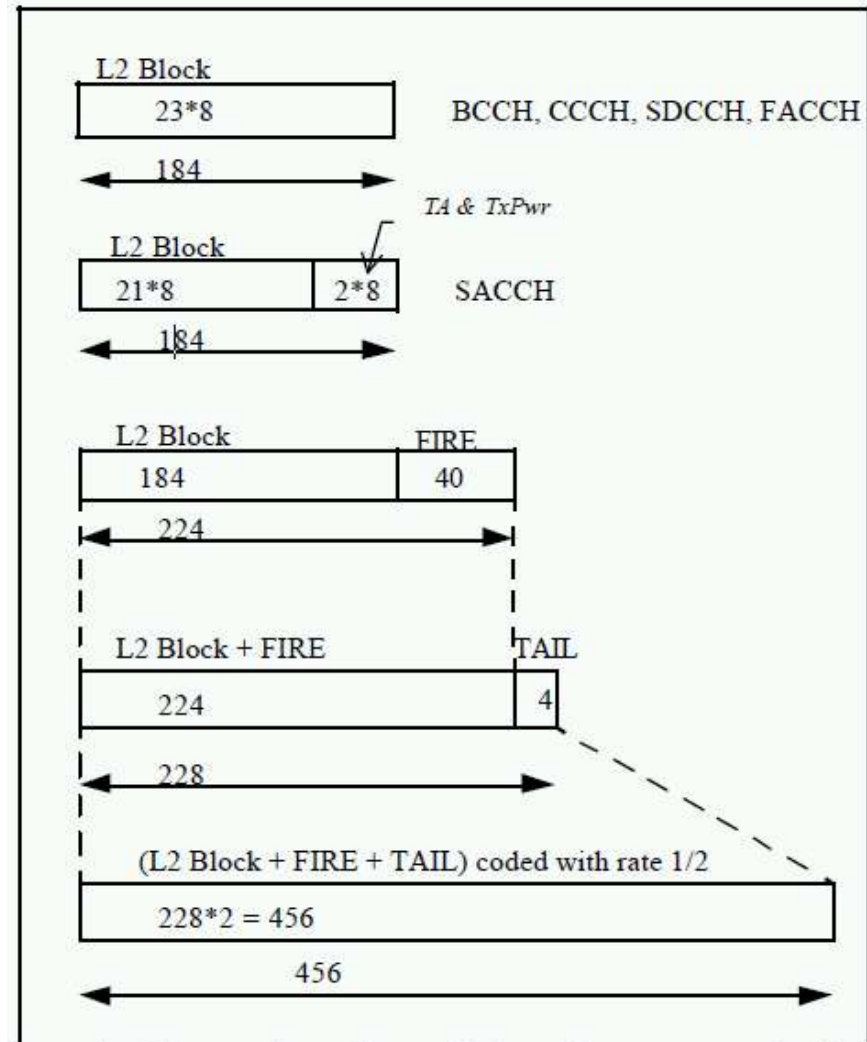


Fire Block Codes

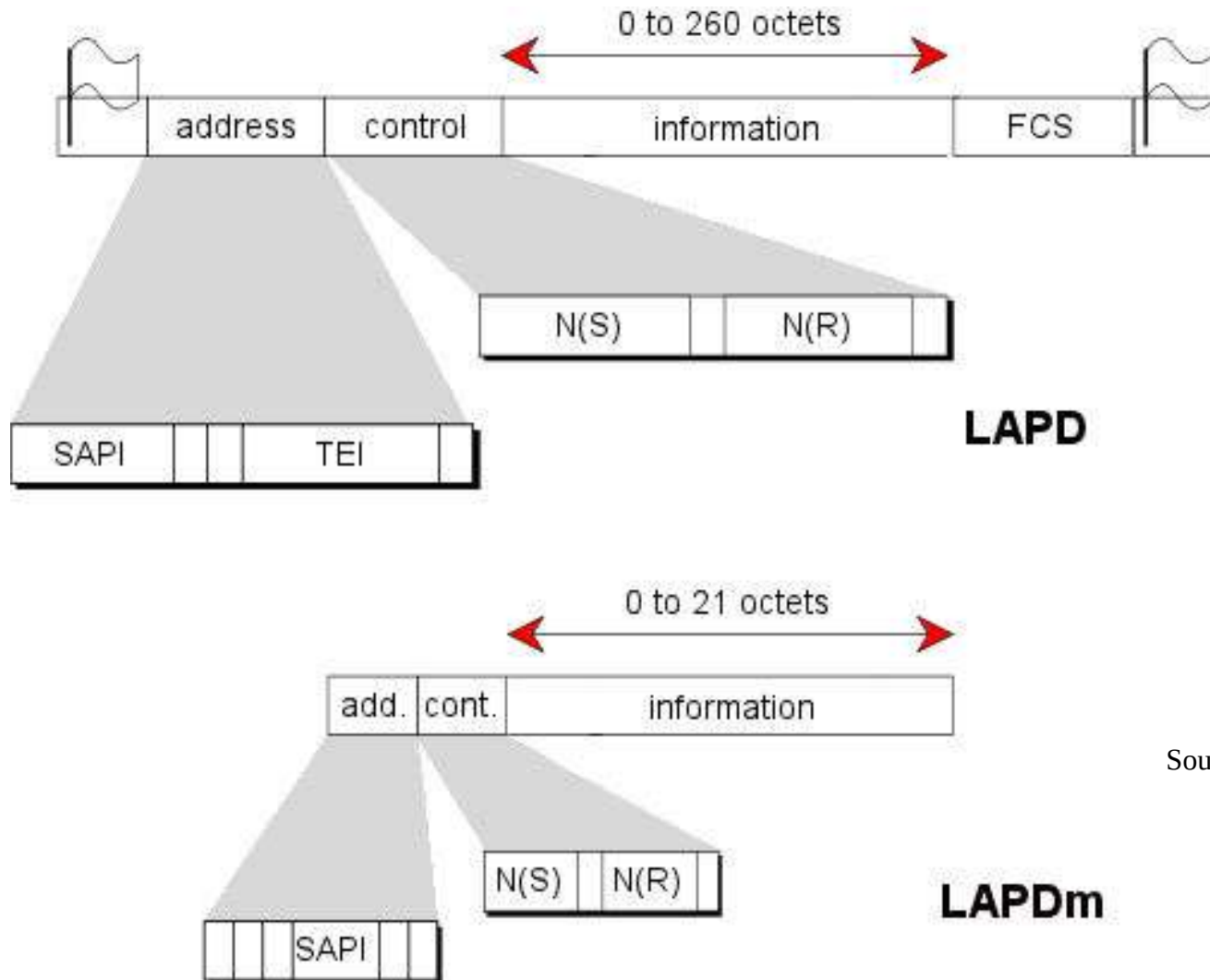
- The Fire code used in GSM is a more sophisticated block code which generates a signature sequence which can correct/detect multiple errors in a block
- 40 bits of redundancy are added to 184 data bits which can correct up to 11 errors
- Good for correcting the groups of errors which are residual from the convolutional code

L1 signalling protection

- Signalling messages are protected at layer 1 by Forward Error Correction (FEC): a block (Fire) code for error detection, and all information bits are convolutional coded.



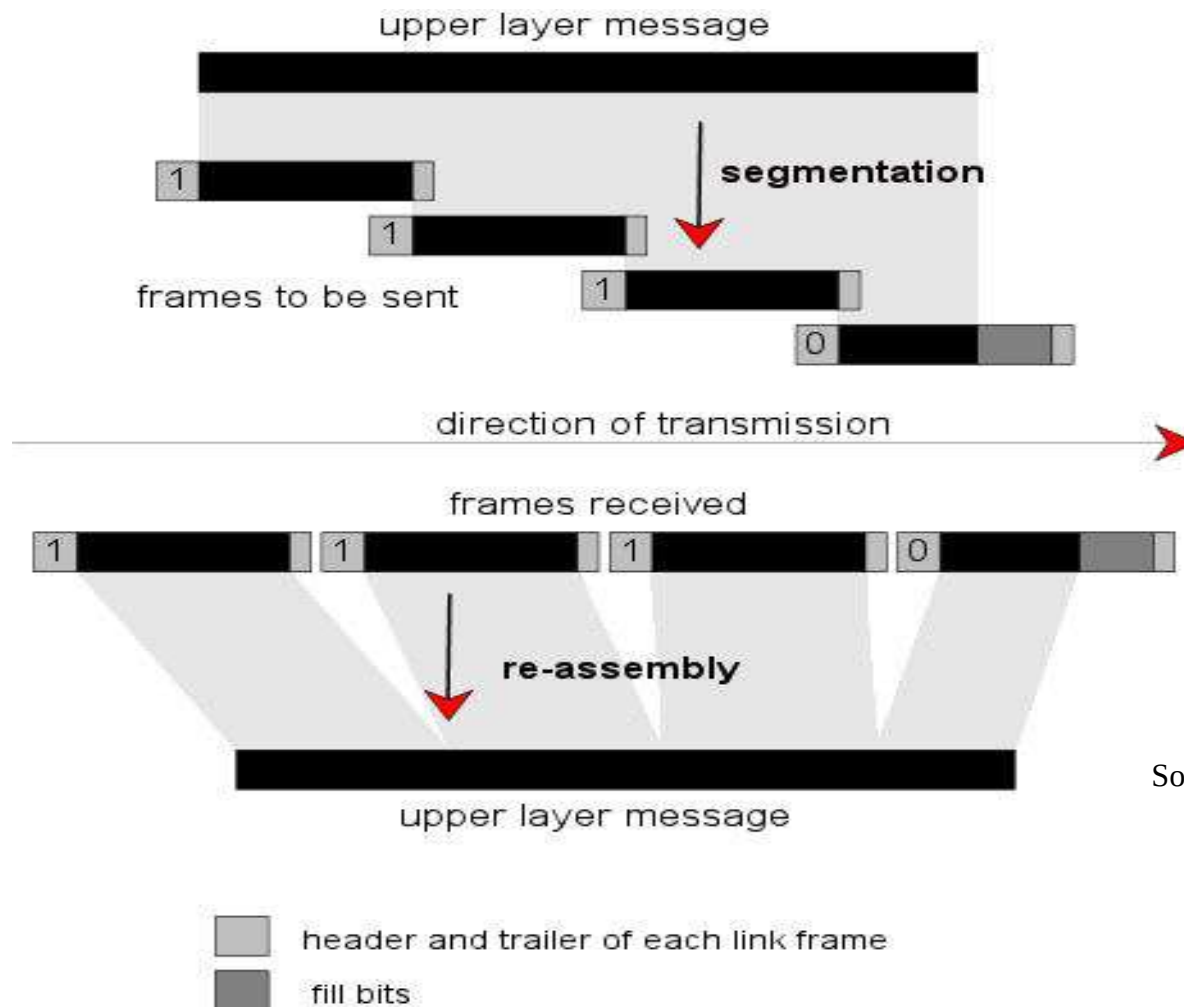
LAPDm: frame structure



Source: Mouly & Pautot



LAPDm: frame segmentation



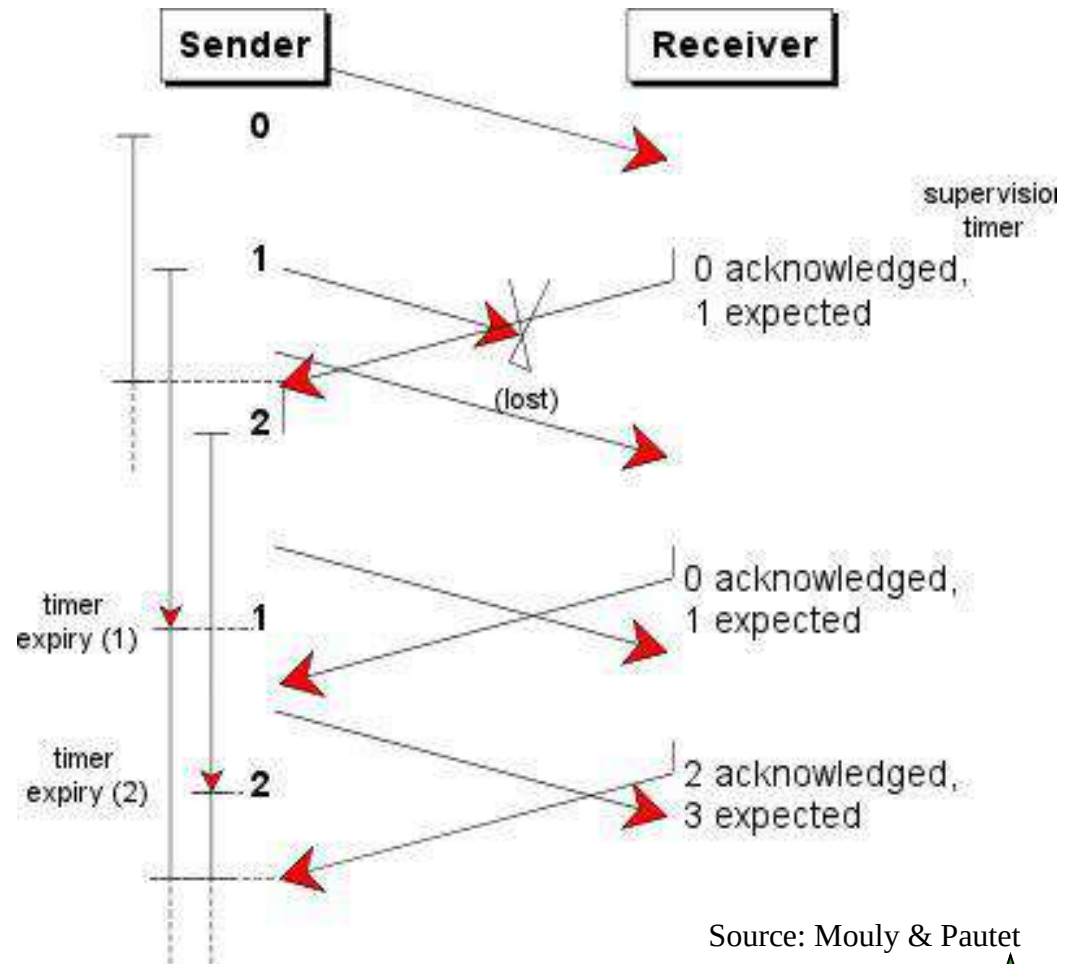
Source: Mouly & Pautet



Repetition mechanism

Sender repeats when:

- It receives an acknowledgment for a frame which was not the last one sent
- It does not receive an acknowledgment after a timeout



Source: Mouly & Pautet

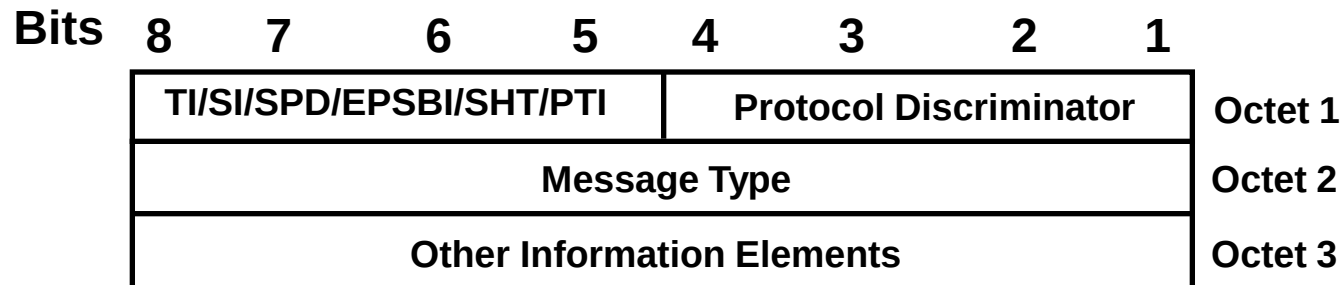


Layer 3 Access Protocol structure

- “Future-proofing” GSM for future enhancement was an early requirement of the protocol architecture:
 - all changes must be backward compatible, especially with mobiles.
 - Mobile Response to errors/unexepected events is described
- At the same time, radio capacity is at a premium, so coding is steeply layered, with implicit dependencies
- Structure is described in TS 24.007



Message Format



- In the message transmission bit 1 is transmitted before 2 and so forth. Also, octet 1 is transmitted before octet 2 and so forth.
- Thus the first element sent is the Protocol Discriminator (PD)
- The second nibble (bits 5-8) use depends on PD

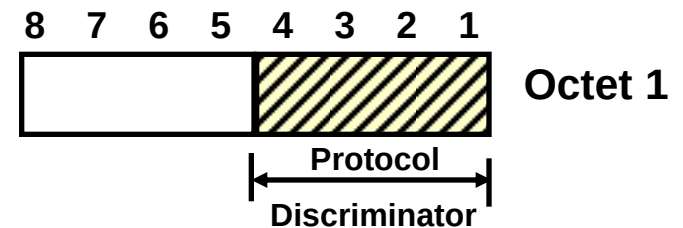


Protocol Discriminator

Purpose to distinguish the protocol of the message: e.g. Call control, Mobility

Management (MM) Radio Resource Management (RR), GPRS...

First part of every message occupies 1st four bits of 1st octet



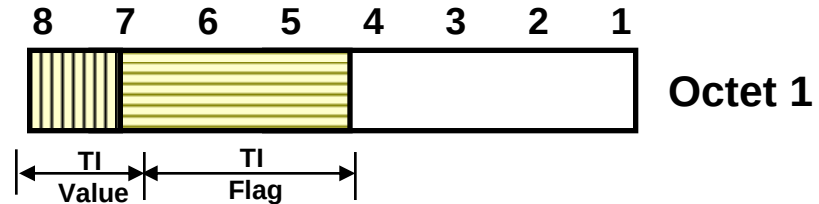
<u>Bits</u>				<u>Mapping</u>
4	3	2	1	
0	0	1	1	Call Control; call related SS messages
0	1	0	1	Mobility Management Messages
1	0	0	1	SMS messages
1	0	1	1	Non Call Related SS Messages
1	1	1	1	Reserved for Test Procedures



Other values used by GPRS, Location services, etc. See TS 24.007

Transaction Identifier(TI)

- Used by some protocols e.g. Call Control. Purpose is to distinguish multiple parallel transactions / activities within one mobile
- It is the second part of these messages



TI Value: assigned by the side initiating the transaction. Remains the same for the life of transaction. Two TI values (identical) could exist at the same MS. But pertaining to transactions originated at different ends (side).

TI Flag: Used to identify which end of the radio (A) Interface originated a transaction

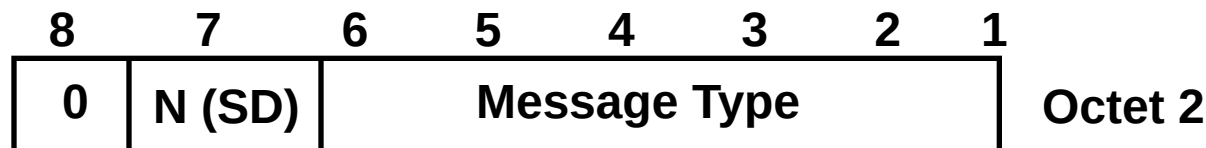
Originating side: 0

Destination side: 1

<u>TI Flag</u>		<u>TI Value</u>				
Bit 8	(Octet 1)	Bits	7	6	5	(Octet 1)
0	The message is sent from the side that originates transaction		0	0	0	TI Value 0
			0	0	1	TI Value 1
			0	1	0	TI Value 2
			0	1	1	TI Value 3
1	The message is sent to the side that originated the transaction		1	0	0	TI Value 4
			1	0	1	TI Value 5
			1	1	0	TI Value 6
			1	1	1	Reserved

Message type

- Purpose is to identify the function of the message being sent
- It is the third part of every message, one octet long
- Bit 8 reserved for future extension;
- Bit 7 for send sequence number in some protocols (e.g. CC & MM)
- Messages with different Protocol Discriminators can have same message types



Message Type-II

Examples:

Handover messages:

8 7 6 5 4 3 2 1

0	0	1	0	1	0	1	1	HANDOVER	COMMAND
0	0	1	0	1	1	0	0	HANDOVER	COMPLETE
0	0	1	0	1	0	0	0	HANDOVER	FAILURE
0	0	1	0	1	1	0	1	PHYSICAL	INFORMATION
... etc									

See TS 44.018, 24.008

<http://www.3gpp.org/ftp/Specs/html-info/44018.htm>

Information Elements

- Purpose: to carry information needed for the relevant messages
- IE can be:
 - (i) Optional for the message - identified by IEI
 - (ii) Mandatory for the message -no IEI sent

Since IE length can be fixed or variable, length indicators may be added.

The formats possible are:

Format	Meaning	IEI present	LI present	Value part present
T	Type only	yes	no	no
V	Value only	no	no	yes
TV	Type and Value	yes	no	yes
LV	Length and Value	no	yes	yes
TLV	Type, Length and Value	yes	yes	yes

Note:

- IEs may have different formats in different message types

Some Mobility Management Messages

Registration Messages	Security Messages
IMSI Detach Indication	Authentication Request
Location Updating Request	Identify Request
Location Updating Accept	Identify Response
Location Updating Reject	TMSI Reallocation Command

Some Call Control messages

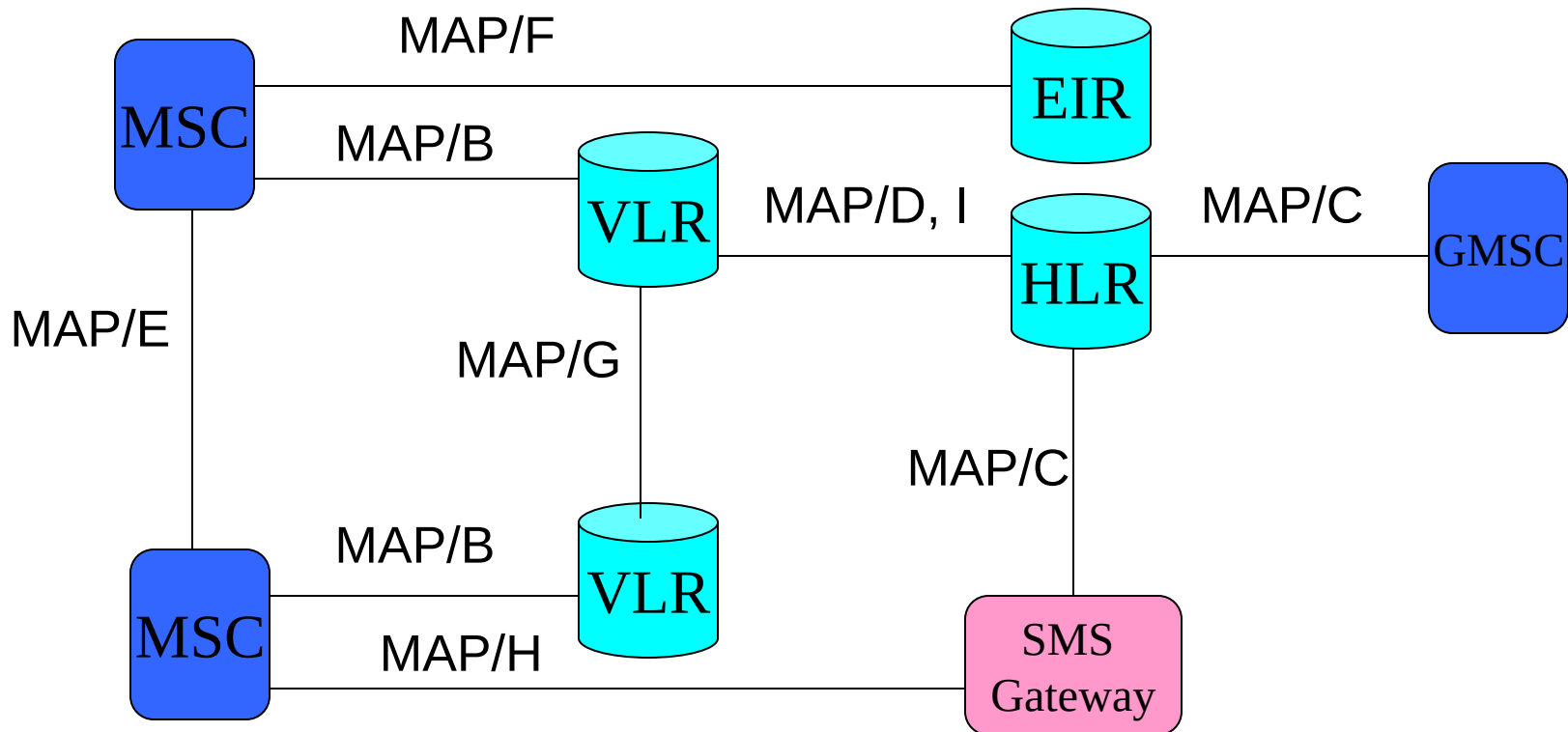
- Call Establishment
 - Alerting
 - Call Confirmed
 - Call Proceeding
 - Connect
 - Connect Acknowledge
 - Emergency Setup
 - Progress
 - Setup
- Call Info. Phase
 - Modify
 - Modify Complete
 - Modify Reject
- Call Clearing
 - Disconnect
 - Release
 - Release Complete
- Misc. Messages
 - Notify
 - Status Inquiry
 - Start DTMF
 - Stop DTMF

Core Network (NSS) Protocols

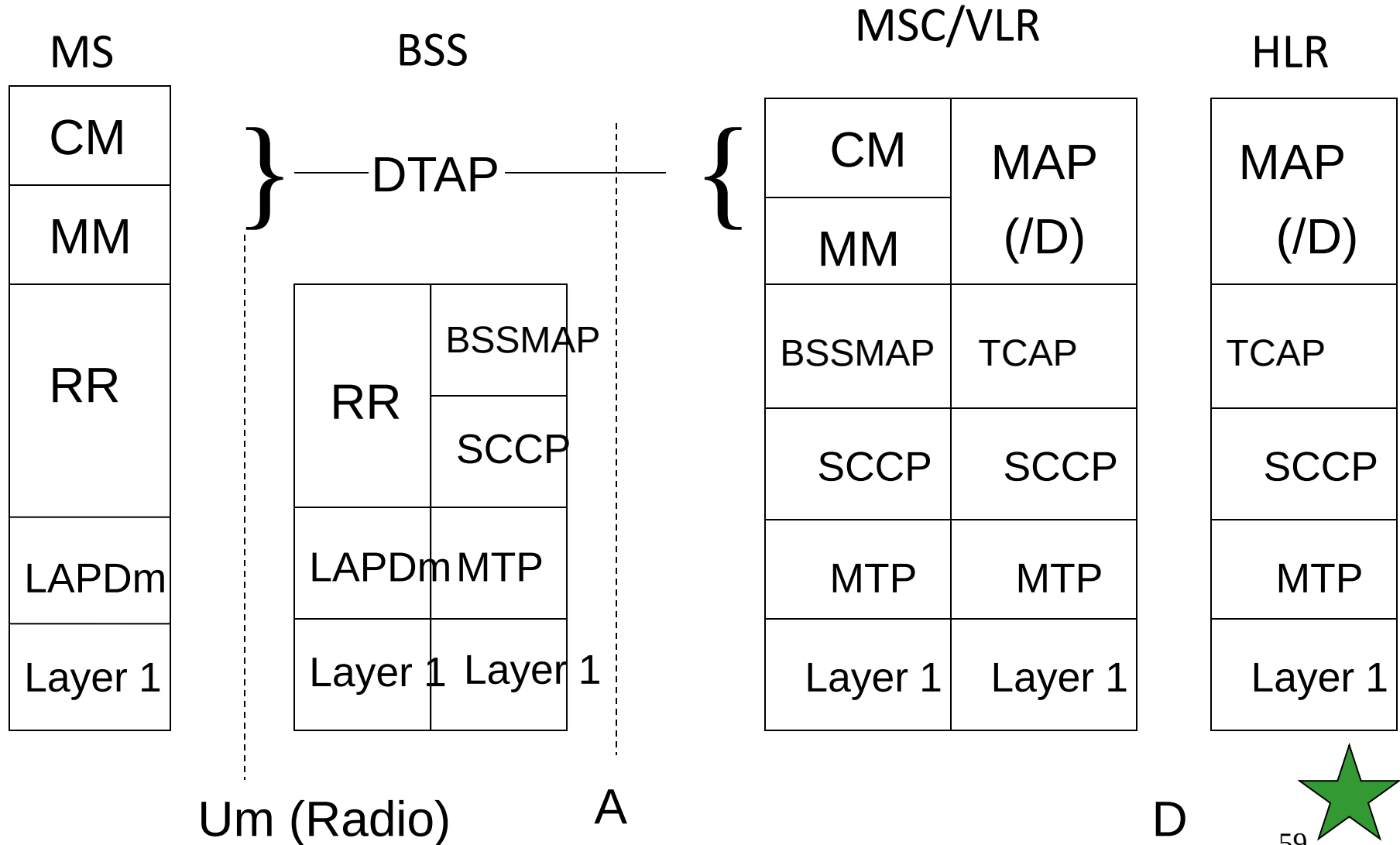
- The basic GSM core network uses circuit switched CCITT signalling system 7. This has international connectivity and acceptance
- A special application part was developed: the Mobile Application Part (MAP)
- MAP variants/message sets were developed for each interface requiring signalling and information flows



GSM MAP Network Architecture



Access-NSS protocol interworking



EP 4.4 Solution: GSM Protocol Structure

- Problem:
 - GSM information flows are complex many-to-many
 - Bandwidth and time (especially on radio interface) are limited.
 - Changes might be needed!
 - How to structure protocols?
- Solution:
 - Use Layered Structure, segmentation etc.
 - Provide backward compatibility mechanisms
 - Use efficient bit coding on radio (Compress if needed)



EFREI M1

Mobile Networks

GSM Networks

Paul Simmons

Tamum Consulting February 2013