

PART 5

GSM – Switching & Mobility

Lecture 5.1

Protocol architecture overview

===== Giuseppe Bianchi =====

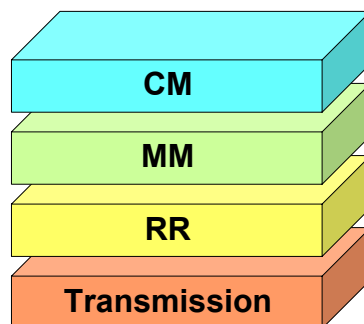
The GSM network layer

→ Divided in three sub-layers

- ⇒ Radio Resource Management (RR)
 - Provides a communication link between MS and MSC;
- ⇒ Mobility Management (MM)
 - Manages DB for MS location
- ⇒ Communication Management (CM)
 - Controls user connection

→ Underlying base:

- ⇒ Transmission level



===== Giuseppe Bianchi =====

RR

→ Manages administration of frequencies and channels

⇒ Mostly deals with air interface

→ Several RR functions considered in previous part

→ Guarantees stable link upon handover

→ Surprise! handover is part of RR, not MM!

→ Function summary:

⇒ Monitoring BCCH, PCH

⇒ RACH administration

⇒ Request/assignment of channels

⇒ MS power control & synchronization

⇒ Handover

→ Where is RR:

⇒ MS, BTS, BSC, MSC

===== Giuseppe Bianchi =====

MM

→ Manages user location and tasks resulting from mobility

→ Function summary:

⇒ TMSI assignment

⇒ MS localization

⇒ Location updating

⇒ MS authentication

⇒ MS identification, attach/detach

→ Where is MM:

⇒ MS, MSC

===== Giuseppe Bianchi =====

CM

→ Controls calls, supplementary services, and SMS

→ Function summary:

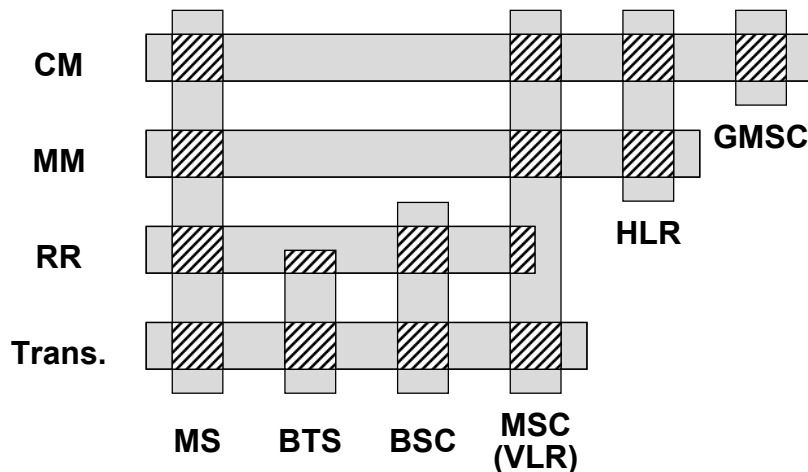
- ⇒ Call establishment (from MS, to MS)
- ⇒ Emergency call management
- ⇒ Call termination
- ⇒ DTMF signaling (Dual Tone MultiFrequency)
- ⇒ In-call modification

→ Where is CM:

- ⇒ MS, MSC, GMSC

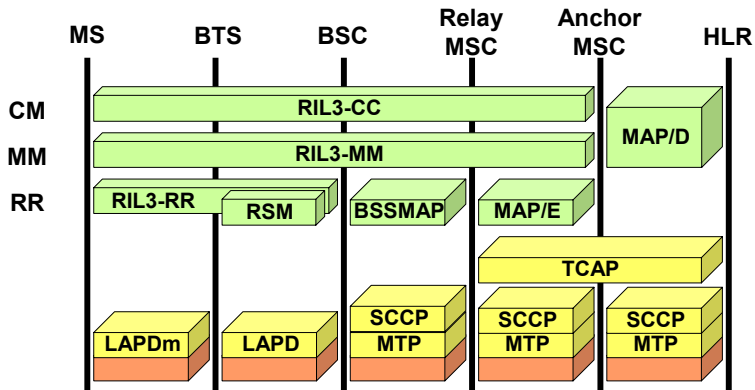
==== Giuseppe Bianchi =====

Protocol placement



==== Giuseppe Bianchi =====

Protocol outline



RIL3: Radio Interface Layer 3

RSM: Radio Subsystem Management

BSSMAP: BSS Management Application Part

MAP: Mobile Application Part

TCAP: Transaction Capabilities Application Part

SCCP: Signaling Connection Control Part

MTP: Message Transfer Part

LAPD: Link access Protocol on D channel

LAPDm: Link access Protocol on Dm channel

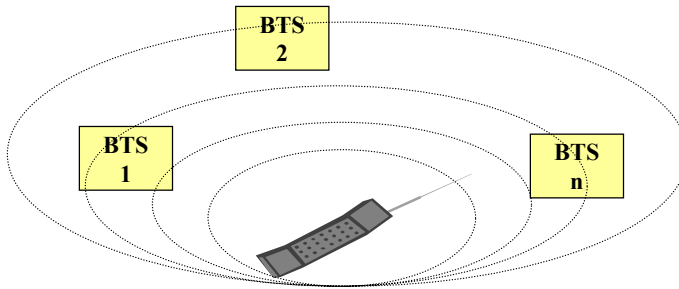
Giuseppe Bianchi

PART 5 GSM – Switching & Mobility

Lecture 5.2 handover (physical mobility)

Giuseppe Bianchi

Neighbor cells



→ A station must:

- ⇒ monitor beacon power level of neighbor cells
- ⇒ Keep detailed track of best 6 neighbor cells
- ⇒ DECODE their BCCH (i.e. read FCCH, SCH) to get parameters
 - At least once every 5 minutes
 - BSIC (from SCH) refreshed every at most 30s

===== Giuseppe Bianchi =====

Camping cell selection

path loss criterion C1

Select cell with greatest $c1(n) > 0$:

$$C1(n) = RXLEV(n) - \\ - RXLEV_ACCESS_MIN - \\ - \max[0, (MS_TXPWR_MAX_CCH - P)]$$

- RXLEV(n): received power from BTS(n)
- RXLEV_ACCESS_MIN: minimum received power level required for registration in the cell
 - (parameter transmitted on BCCH; typically -98 to -106 dB)
- MS_TXPWR_MAX_CCH: maximum allowed transmitted power on RACH
 - (parameter transmitted on BCCH; typically 31-39 dBm)
- P: maximum MS power (from MT class)

When cell parameters are the same, simply select cell with higher RXLEV!

===== Giuseppe Bianchi =====

Cell reselection criterion (C2)

→ Reselect cell with greatest $C2 > 0$:

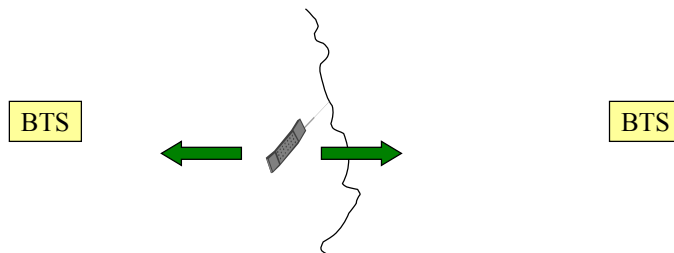
$$C2(n) = C1(n) + \text{CELL_RESELECT_OFFSET} - \\ - \text{TEMPORARY_OFFSET} \times H(\text{PENALTY_TIME} - T)$$

$$\text{where } H(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases}$$

- T: amount of consecutive time since considered cell became with $C1 > 0$
- PENALTY_TIME, CELL_RESELECT_OFFSET, TEMPORARY_OFFSET: BCCH parameters
- If all parameters = 0, reselect cell with better path loss performance (no time hysteresis included)

==== Giuseppe Bianchi =====

Consequences of cell reselection



→ **None, when MS idle!**

→ No need to inform BTS at all!

→ **Exception:**

⇒ When cell reselection implies a Location Area Update

→ Need to inform the network!

→ **Additional restriction:**

⇒ $C2 > \text{CELL_RESELECT_HYSTERESIS}$

==== Giuseppe Bianchi =====

handover

→ Procedure in which an MS releases a connection with a BTS, and establishes a connection with a new BTS, while ensuring that the ongoing call is maintained

⇒ The MS remains in dedicated state (unlike cell reselection, where MS is in idle state)

→ **Handoff: synonymous of handover**

→ **Needs two mechanisms**

⇒ Handover preparation: detection of cell-border crossing

→ Based on radio link quality measurements

⇒ Handover execution: setup of a new channel in a cell, and tear-down of a previous channel

→ **Improved handover mechanisms:**

⇒ Seamless handover: when active call performance is not impaired

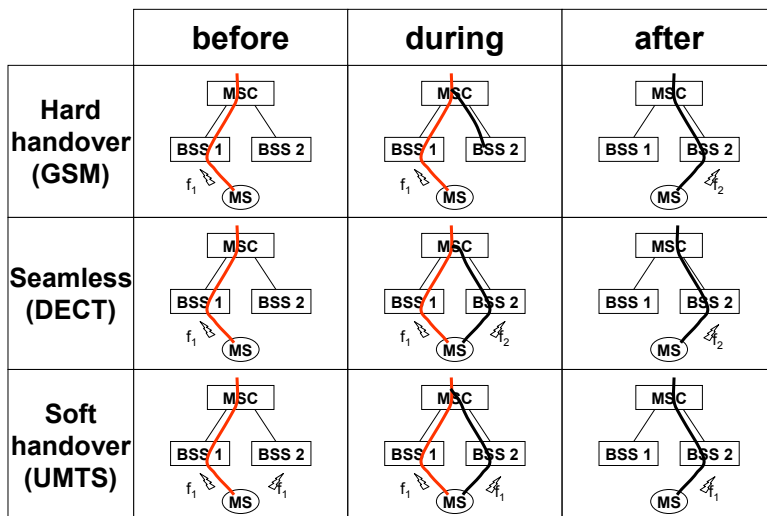
→ Not possible in GSM: for about 100-200ms, communication is interrupted

⇒ Soft Handover: when two channels are simultaneously set-up (old and new)

→ Not possible in GSM; possible in UMTS

===== Giuseppe Bianchi =====

Hard, Seamless, Soft handover



===== Giuseppe Bianchi =====

Handover classification

Classification by motivation

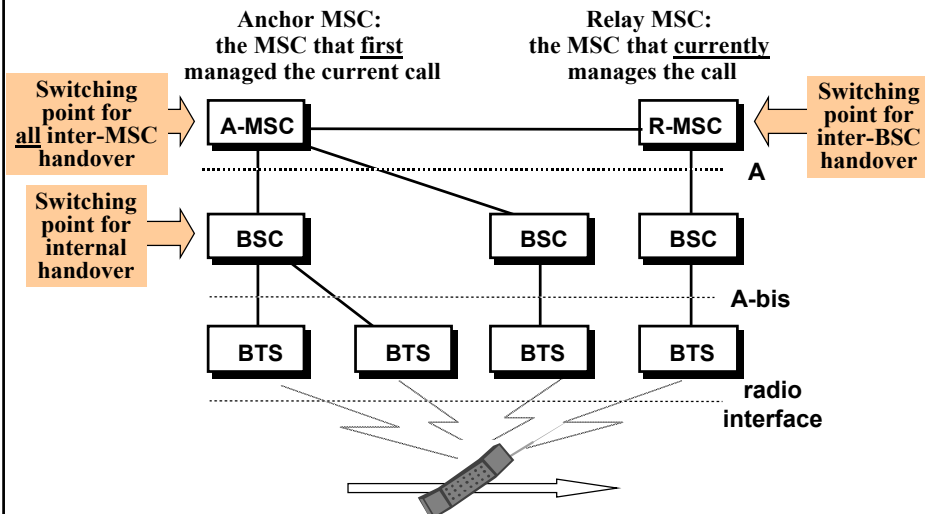
- **Rescue handover (mandatory handover)**
 - ⇒ Driven by radio channel quality degradation
- **Confinement handover (network-directed handover)**
 - ⇒ Target: minimize radio interference
 - ⇒ Assign new channel when old channel results critical for total interference
- **Traffic handover (network-directed handover)**
 - ⇒ Driven by traffic congestion conditions
 - ⇒ Also called load-balancing

Classification by typology

- **Internal handover**
 - ⇒ Intra-BTS
 - New radio channel in the same cell
 - Not termed as “handover” but as “subsequent assignment”
 - ⇒ Inter-BTS (Intra-BSC)
 - Under control of same BSC
- **External handover**
 - ⇒ Inter-BSC (Intra-MS-C)
 - Change reference BSC; may imply a location area update
 - ⇒ Inter-MS-C
 - Most complex: need to change MS-C

Giuseppe Bianchi

Types of handover



Giuseppe Bianchi

Handover taxonomy

→ BCHO: Base station Controlled Handover

- ⇒ Handover detection: BS
- ⇒ Handover Execution: BS

→ MCHO: Mobile Controlled Handover

- ⇒ Handover detection: MS
- ⇒ Handover Execution: MS

→ MAHO: Mobile Assisted Handover

- ⇒ Handover detection: MS
- ⇒ Handover Execution: BS

→ GSM: somehow a BCHO with a flavor of MAHO

- ⇒ Handover decision always taken by BSC
- ⇒ Based on measures taken at both BTS and MS
- ⇒ New channel selection decision taken at BSC or R-MSC or A-MSC (depending on handover type) based on traffic consideration

===== Giuseppe Bianchi =====

Handover preparation

→ Measurements performed at BTS

- ⇒ Up-link signal level received from MS lower than threshold
→ $RXLEV_{UL} < L_{RXLEV_{UL_H}}$
- ⇒ Up-link signal quality (BER) received from MS
→ $RXQUAL_{UL} < L_{RXQUAL_{UL_H}}$
- ⇒ Distance between MS and BTS
→ adaptive timing advance parameter $> MAX_{MS_RANGE}$
- ⇒ Interference level in unallocated time slots.

→ Measurements performed at MS.

- ⇒ Down-link signal level received from serving cell
→ $RXLEV_{DL} < L_{RXLEV_{DL_H}}$
- ⇒ Down-link signal quality (BER) received from serving cell
→ $RXQUAL_{DL} < L_{RXQUAL_{DL_H}}$
- ⇒ Down-link signal level received from n -th neighbor cell
→ $RXLEV_{NCELL(n)} > RXLEV_{MIN(n)}$

RX signal level	From (dBm)	To (dBm)
RXLEV_0	-	-110
RXLEV_1	-110	-109
RXLEV_2	-109	-108
RXLEV_3	-108	-107
...
...
RXLEV_62	-49	-48
RXLEV_63	-48	-

Bit error Ratio	From (%)	To (%)
RXQUAL_0	-	0.2
RXQUAL_1	0.2	0.4
RXQUAL_2	0.4	0.8
RXQUAL_3	0.8	1.6
RXQUAL_4	1.6	3.2
RXQUAL_5	3.2	6.4
RXQUAL_6	6.4	12.8
RXQUAL_7	12.8	-

===== Giuseppe Bianchi =====

A note on MS distance

→ Distance can be measured based on TA

→ TA = advance bits

⇒ Ideally, TA should be set as

$$TA[\text{bits}] \cdot t_{\text{bit}} = \frac{2d}{c} \Rightarrow d = \frac{TA}{2} \cdot c \cdot t_{\text{bit}}$$

⇒ Hence, the TA resolution, in mt, is:

$$d(TA) = TA \frac{c \cdot t_{\text{bit}}}{2} = TA \frac{300000[\text{mt/ms}] \cdot \frac{1}{270.833}[\text{ms}]}{2} \approx TA \cdot 554\text{mt}$$

⇒ INSUFFICIENT for microcells!

⇒ Sufficient only to understand we are going out of the cell

===== Giuseppe Bianchi =====

Handover preparation – additional metrics

→ **Transmission power**

- ⇒ Maximum MS transmission power
- ⇒ Maximum serving BTS transmission power
- ⇒ Maximum neighboring BTSs transmission power

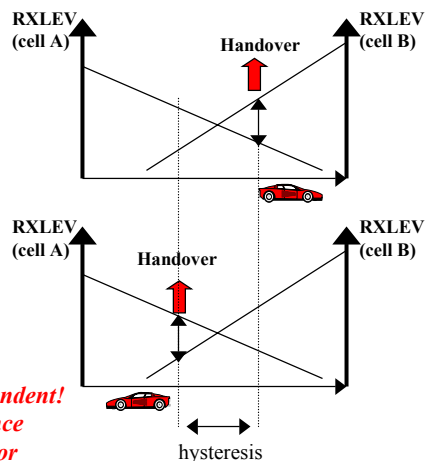
→ **congestion status**

- ⇒ of serving BTS
- ⇒ of neighboring BTSs
- provided they can support the MS.

→ **Handover Margin**

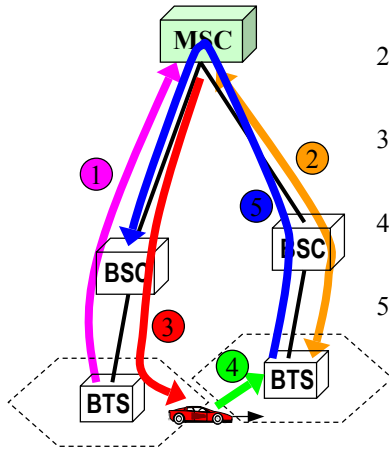
- ⇒ To avoid ping-pong handover effect
- ⇒ 5-10 dB in normal operation; up to 30dB in urban operation (to fight shadowing)

HANDOVER ALGORITHM: operator-dependent!
GSM standard SUGGESTS a simple reference algorithm, but implementation left to operator



===== Giuseppe Bianchi =====

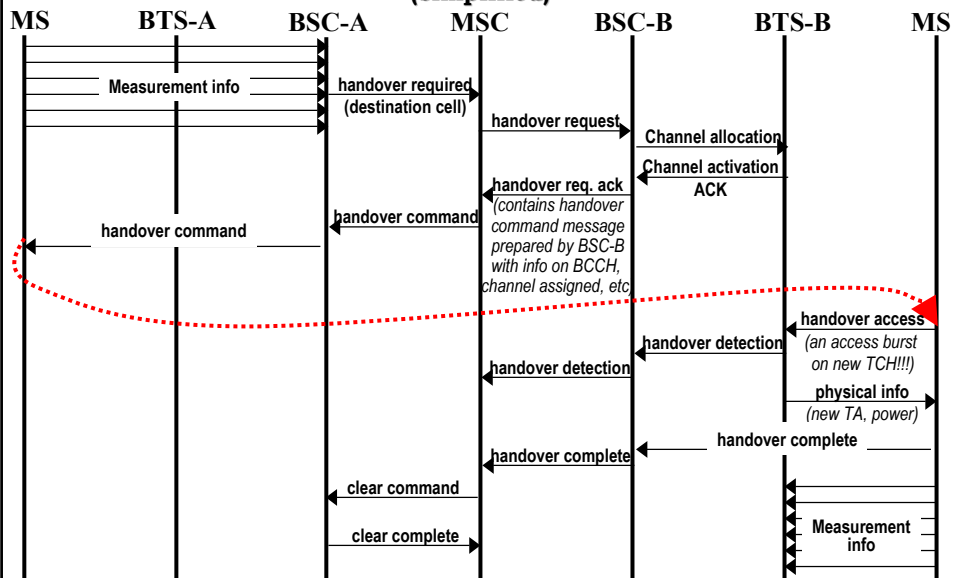
handover procedure skeleton



- 1) Handover request goes up to switching point
- 2) Switching point prepares new path on fixed net
- 3) Switching point sends HO command to MS
- 4) MS accesses new channel
- 5) Old channel/path torn down

Giuseppe Bianchi

Signaling for intra-MS handover (simplified)



Giuseppe Bianchi

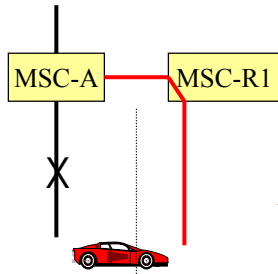
Inter-MSC handover

→ More complex, as an ISDN circuit must be set between MSCs

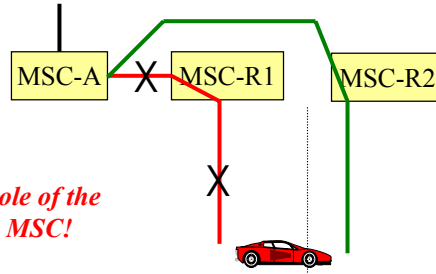
⇒ We'll not enter into details (just the basic ideas)

→ Two cases

First MSC change
(basic handover)



Second MSC change
(subsequent handover)



*Note the role of the
Anchor MSC!*

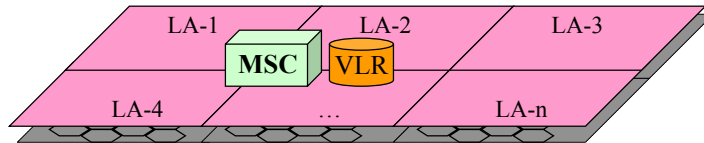
==== Giuseppe Bianchi =====

PART 5 GSM – Switching & Mobility

Lecture 5.3 location registration/update Authentication & Ciphering

==== Giuseppe Bianchi =====

Location Area vs MSC service area



==== Giuseppe Bianchi =====

Registration vs update

→ Very similar procedures, with goals:

- ⇒ Determine where the user is
- ⇒ Authenticate user

→ Differences:

- ⇒ Location Registration
 - User first access to PLMN
 - » Needs to send IMSI and receive TMSI
- ⇒ Location Update
 - Subsequent accesses to PLMN (either in old or new MSC/VLS)
 - » Also after MS shut-down!
 - » TMSI-based identification

→ Registered user:

- ⇒ The PLMN knows the LA where the user is (or is supposed to be)

==== Giuseppe Bianchi =====

Procedure start-up

→MS switches on

→Detects BCCH carrier

⇒Tune and synchronize

→Listens to BCCH

→Obtains Location Area Identifier

⇒LAI: [CC,MNC,LAC]

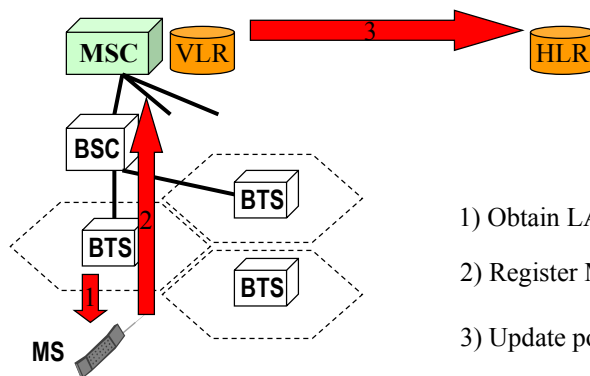
→Country Code (CC): 3 digits

→Mobile Network Code: 2 digits

→Location Area Code: max 5 digits

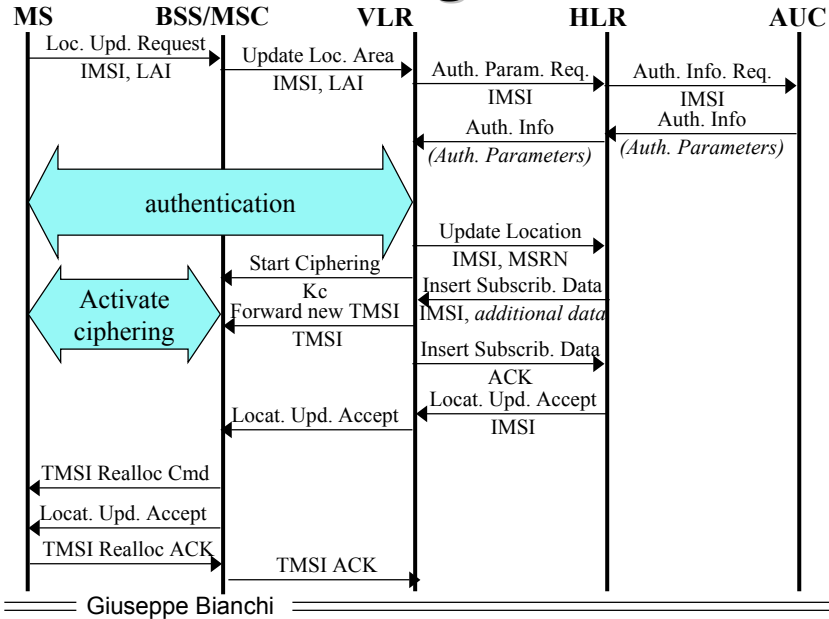
Giuseppe Bianchi

LR/LU (very) basic idea

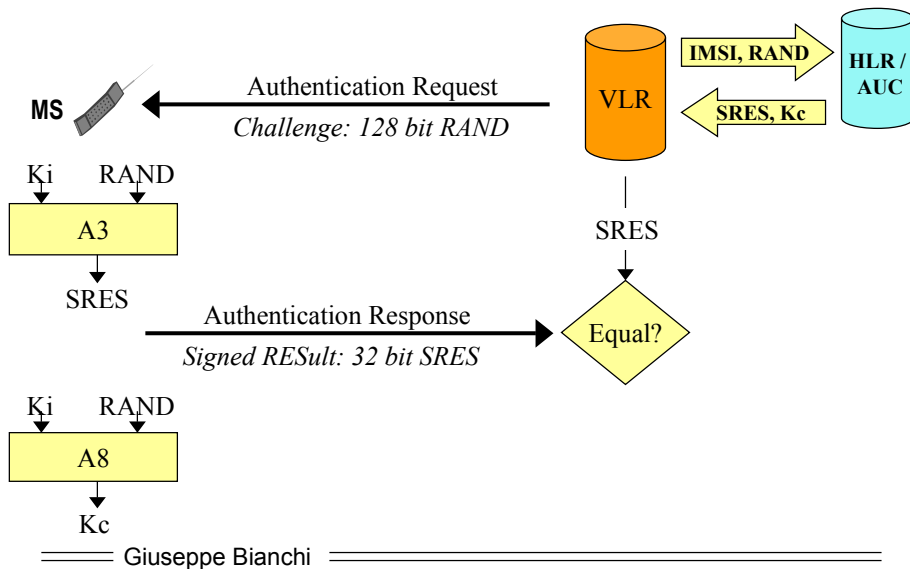


Giuseppe Bianchi

Location Registration



Authentication (managed by VLR)



Authentication (details)

→ **Side effect of authentication:**

⇒ Generate encryption key Kc via A8 algorithm

→ **Secret A3, A8 algorithms (one-way hash functions)**

⇒ Stored into the SIM

→ Along with secret key Ki

⇒ Note that roaming operator DOES NOT need to know them!

→ Since A3, A8 run ONLY in the AUC at the home HLR

→ Ki is NEVER transmitted away from AUC or MS!

→ **Generally implemented together**

⇒ $[SRES, Kc] = A38[Ki, RAND]$

→ **To reduce signaling, real implementation slightly different:**

⇒ VLR sends IMSI

⇒ Receives back several tuples of (RAND, SRES, Kc) to be used for the considered MS also in subsequent accesses

===== Giuseppe Bianchi =====

ciphering

→ **A5 algorithm is known (to allow roaming)**

→ **Generates two ciphering sequences**

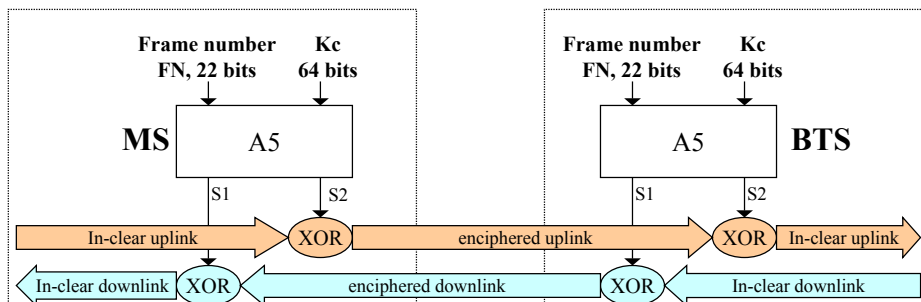
⇒ one for uplink, one for downlink

⇒ Sequence periodic with period $26 \times 51 \times 2048 = 2,715,648$

→ $2^{21} = 2,097,152 < 2,715,648 < 2^{22} = 4,194,304$

→ **114 bits per frame, depending on frame number**

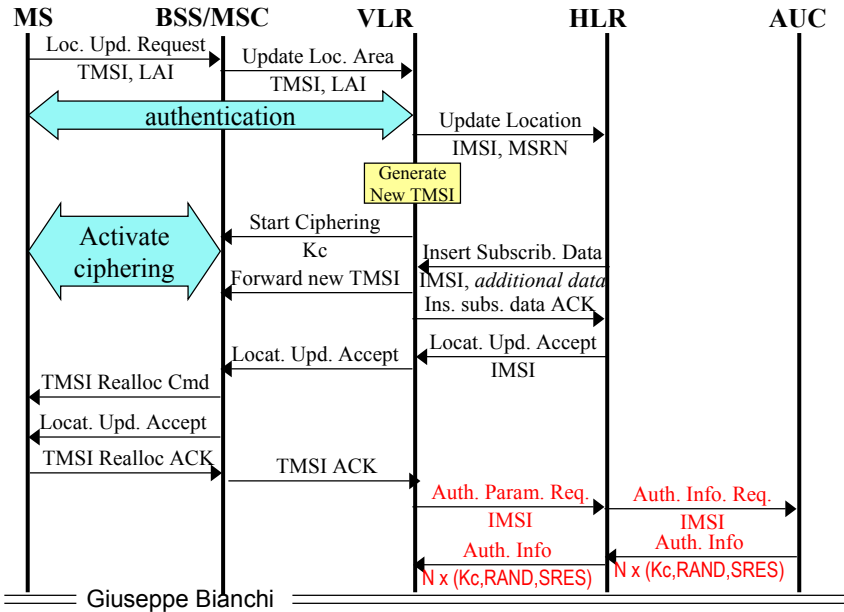
→ **XOR-ed with burst data field**



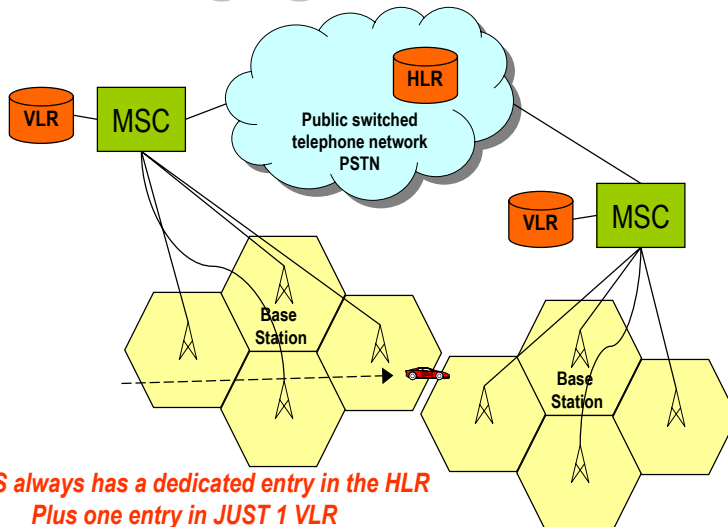
===== Giuseppe Bianchi =====

Location Update in same VLR

(same as location registration, but with TMSI)



Changing MSC/VLR



**An MS always has a dedicated entry in the HLR
Plus one entry in JUST 1 VLR
(related to the MSC the user is connected to)**

Giuseppe Bianchi

TMSI

→ TMSI = Temporary Mobile Subscriber Identity

⇒ 4 octets (32 bits)

- ⇒ Renewed periodically; at every LU / IMSI_attach
 - Via TMSI_Reallocation_Command/TMSI_Reallocation_Complete
 - RATIONALE: renew TMSI when transmitted in clear!
(TMSI reallocation occurs in ciphering mode)

Operator may set a 6min up to 24hrs periodicity for LU (value transmitted on BCCH)

IMSI_attach = a special LU in a same Location Area;

IMSI_attach follows an IMSI_detach (power-down of MS)

→ Meaningful only in a given VLR

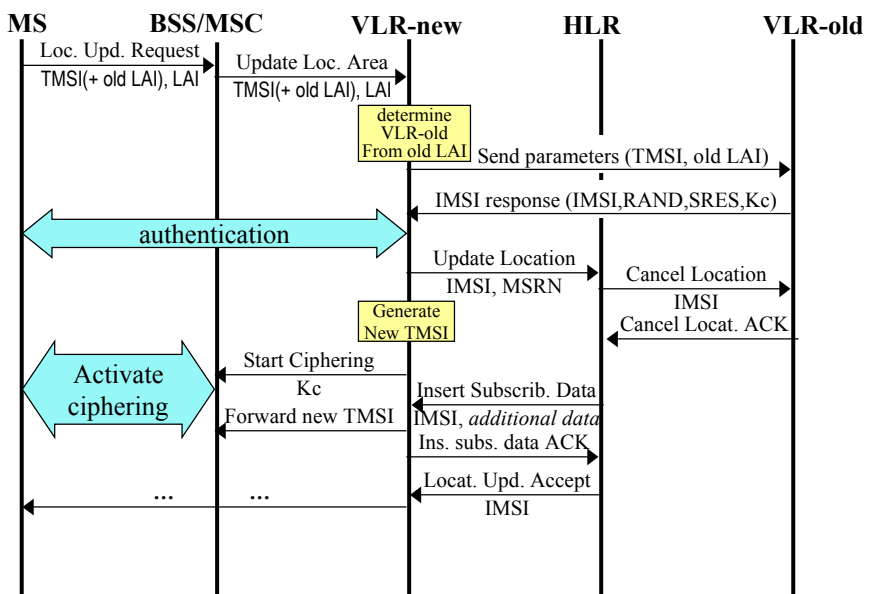
- ⇒ Specifically, only for a given Location Area!!
 - Some author (Mouly-Pautet) uses the term
 - » TIC (Temporary Identity Code) = 4 bytes
 - » TMSI = TIC+LAI = unambiguous user identification

→ While entering a new Location Area:

- ⇒ user must identify itself with TMSI+LAI pair.

Giuseppe Bianchi

Location Update: different VLR

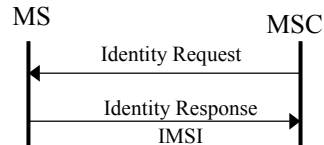


Giuseppe Bianchi

Special cases

1. New VLR not capable of determining old VLR from old LAI
2. Old VLR does not recognize TMSI

⇒ Identification procedure
→ IMSI transmitted in clear



PAGING:

- Normally based on TMSI
- But when no valid TMSI information available (e.g. after a DB restore after crash), based on IMSI

==== Giuseppe Bianchi =====

PART 5 GSM – Switching & Mobility

Lecture 5.4 Call Management & routing

==== Giuseppe Bianchi =====

Notation

→ A call involves two "Parties"

→ Calling Party (caller)

⇒ user generating the call

→ Called Party (callee)

⇒ user receiving the call

→ Mobile Originating Call (MOC)

⇒ Call originated by an MS

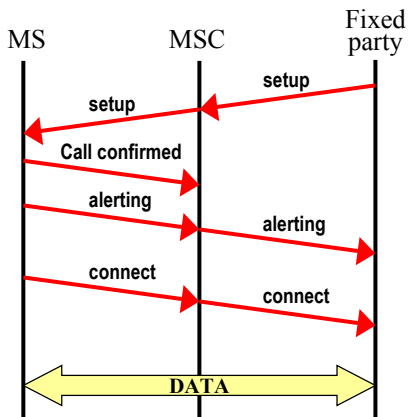
→ Mobile Terminating Call (MTC)

⇒ Call directed to an MS

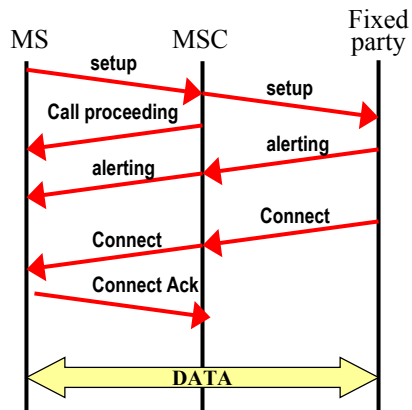
==== Giuseppe Bianchi =====

Call establishment basics

Mobile Terminated Call



Mobile Originated Call



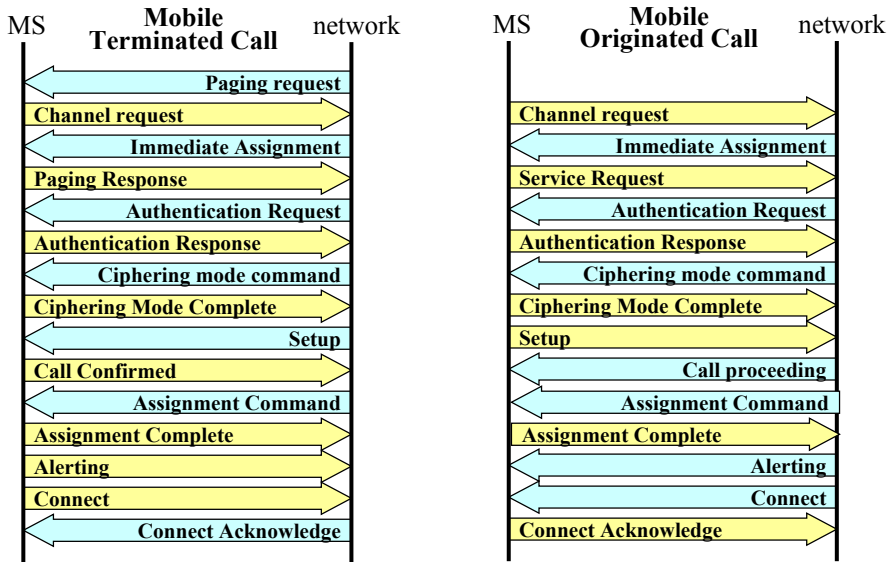
In ISDN ISUP:

- setup = IAM
- Alerting = ACM
- Connect = ANS

(Initial Address Message);
(Address Complete Message);
(Answer)

==== Giuseppe Bianchi =====

Call establishment steps



Giuseppe Bianchi

Radio Resource allocation

three standardized solutions

→ Non-Off Air Call Set-Up (Non-OACSU)

⇒ Normally used (previous description)

→ Off Air Call Set-Up (OACSU)

⇒ TCH assigned only when the called party actually responds!

→ Best utilization of radio resource (avoids allocation if callee not available)

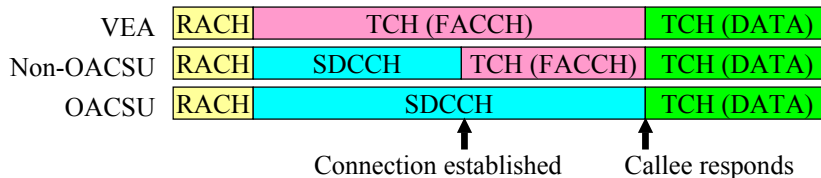
→ Call drop if no TCH is available at this point

→ Very Early Assignment (VEA)

⇒ Immediate assignment of TCH

→ Fastest signalling process

→ Waste of resources



Giuseppe Bianchi

DTMF signaling

→ Dual-Tone Multi-Frequency

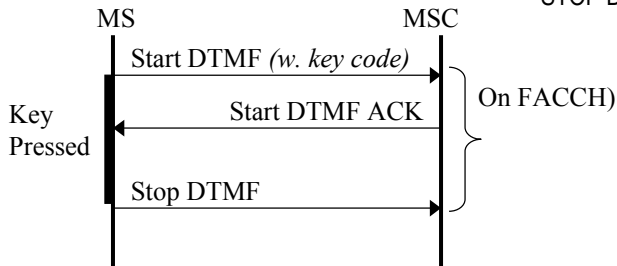
- ⇒ Digital tones associated to terminal keys
→ '0'...'9'...'#'...

→ Inband signalling

- ⇒ transmitted in the traffic channels!
- ⇒ Not in the signalling network

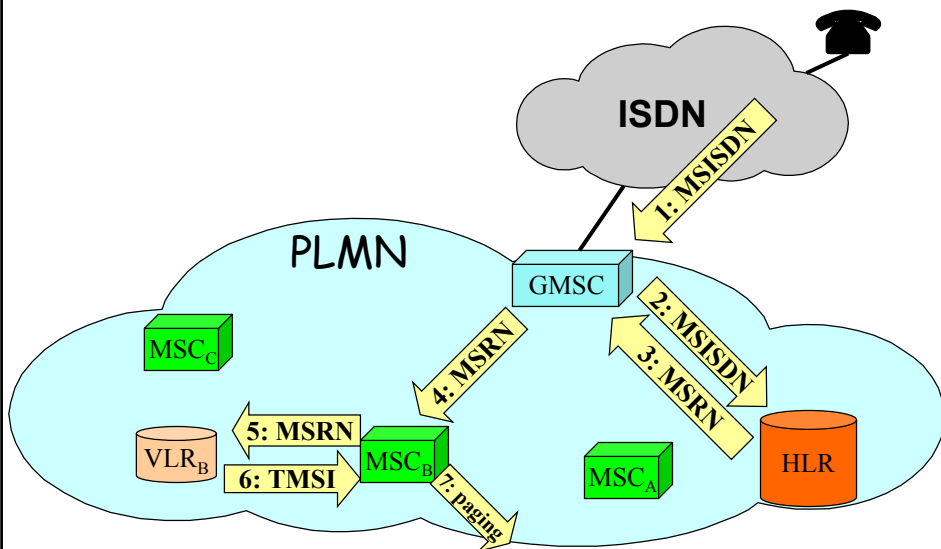
On air interface:

- ⇒ Signal transmitted on FACCH as signalling data (code of pressed key)
- ⇒ Otherwise coded compression would distort DTMF tones
- ⇒ Tone generated at MSC when STOP DTMF message received



Giuseppe Bianchi

Routing an MTC



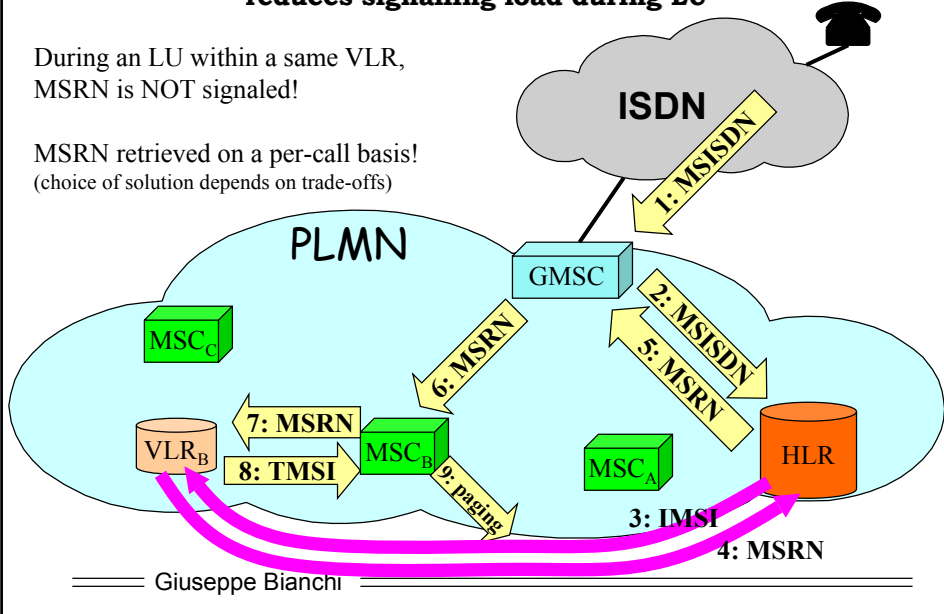
Giuseppe Bianchi

Routing an MTC (alternative)

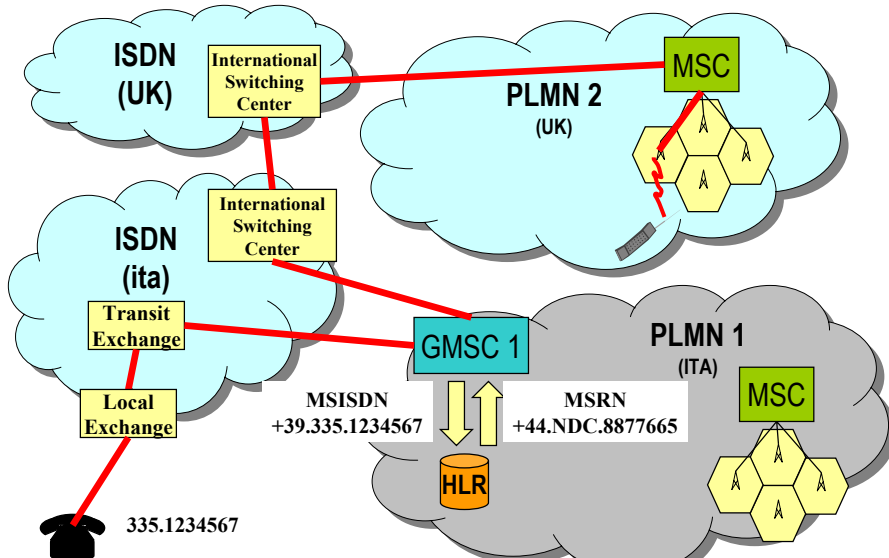
reduces signalling load during LU

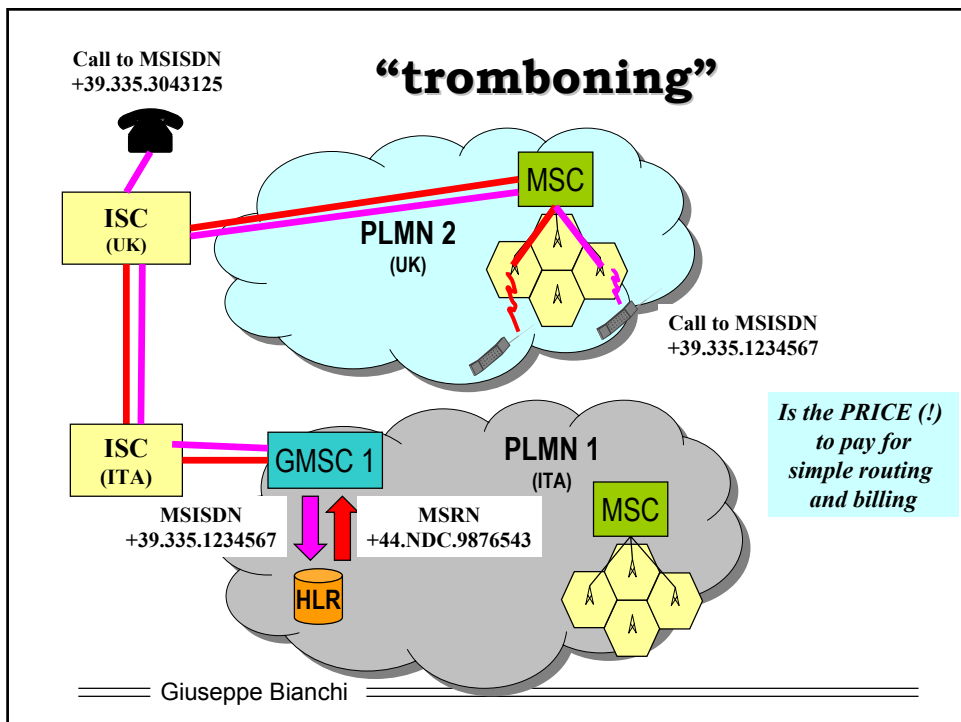
During an LU within a same VLR, MSRN is NOT signaled!

MSRN retrieved on a per-call basis!
(choice of solution depends on trade-offs)



Routing calls to Roaming MS





Tromboning technical solutions

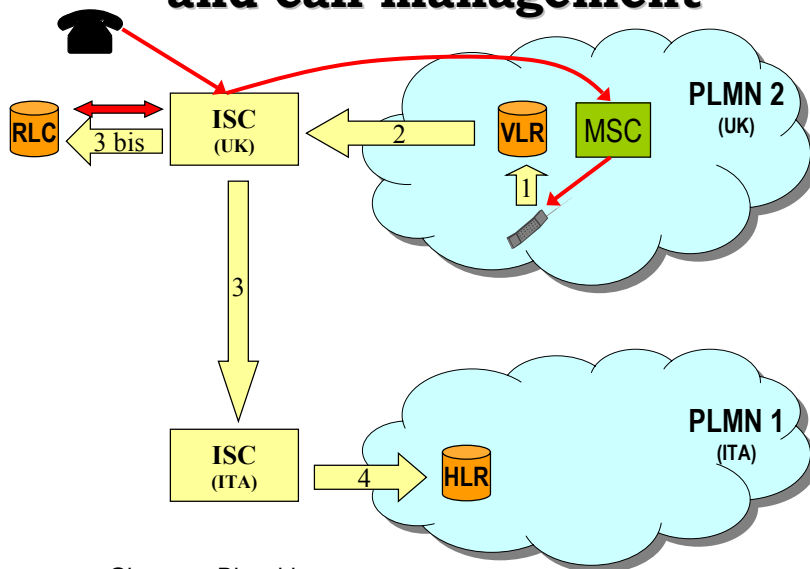
→ First alternative: national-wise

- ⇒ Add a new database - Roamer Location Cache (RLC)
 - Consulted by ISCs (which MUST support GSM-MAP!)

→ Second alternative: PLMN specific

- ⇒ RLC within the PLMN + associated switch
- ⇒ Caller must dial special NDC number (the switch!)
 - I.e. must know the MS is roaming in the PLMN...
- ⇒ Additional devices and protocol modifications required
 - » Extensions to VLR or to GMSC
 - » Details in “Lin-Chlamtac”

RLC at ISC - Location Registration and call management



Giuseppe Bianchi

Short Message Service

→ SMS:

- ⇒ messages up to 160 bytes
- ⇒ Message concatenation allowed

→ Transmitted on air interface over:

- ⇒ SACCH (when user in conversation)
- ⇒ SDCCH (when user in idle state)

→ Two transmission modes in a cell:

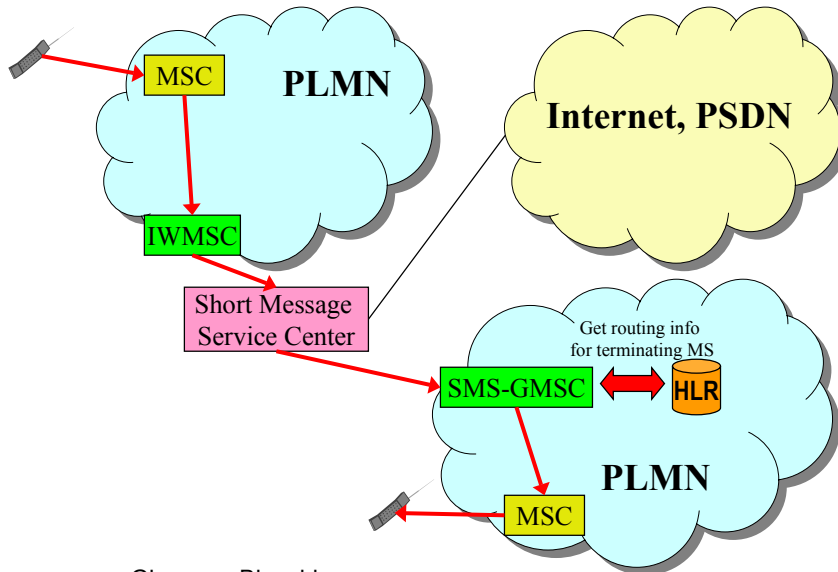
- ⇒ Point-to-point
- ⇒ cell broadcast

→ Connectionless service

- ⇒ message switching (store&forward)
- ⇒ Implemented through the Short Message Service Center

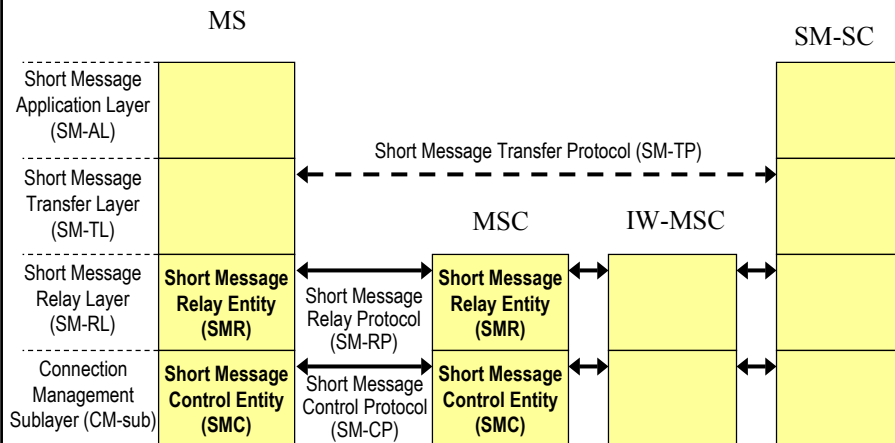
Giuseppe Bianchi

SMS routing management



Giuseppe Bianchi

Protocol hierarchy



Quite complex signalling involved (see specific texts)

Giuseppe Bianchi

Number portability

→ **Subscriber may switch operator without changing his number**

→ **First implemented in fixed network**

⇒ Recently (may 2002) extended to mobile networks

→ **Essential for fair competition among network operators**

⇒ UK survey: 42% of corporate subscribers were willing to change mobile operator; but 96% were, if number could be ported

→ **Resistance from leading operators**

⇒ Number portability helps newer operators to compete with traditional ones

==== Giuseppe Bianchi =====

Notation

→ **Donor switch**

⇒ The switch corresponding to a “ported” telephone number

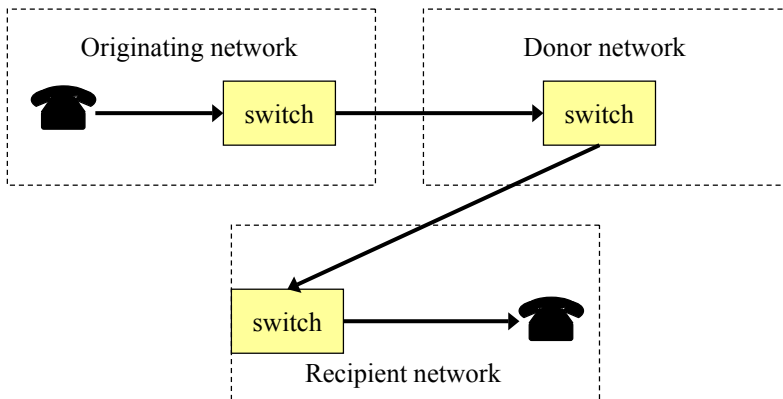
→ **Recipient switch**

⇒ The switch to which the ported number is attached

==== Giuseppe Bianchi =====

Technical solutions

a) call forwarding



Originating switch sets-up trunk to donor switch

Donor switch sets-up trunk to recipient switch

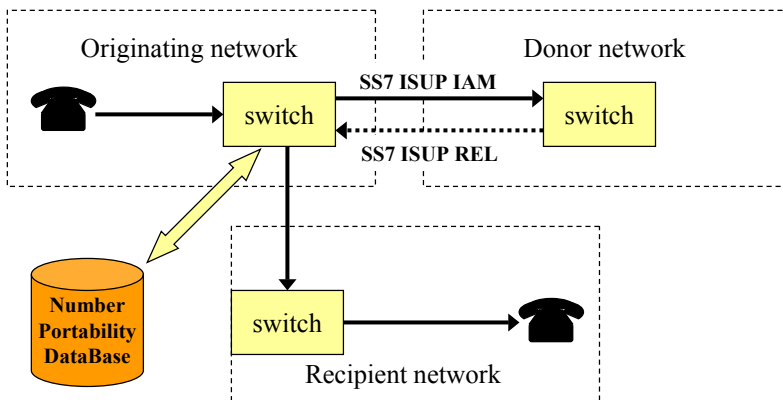
Simplest solution, as call forwarding is a feature available in virtually all switches

But extremely inefficient routing and trunking resource consumption!

Giuseppe Bianchi

Technical solutions

b) query on release



Donor switch “blocks” incoming call with a release message (REL)

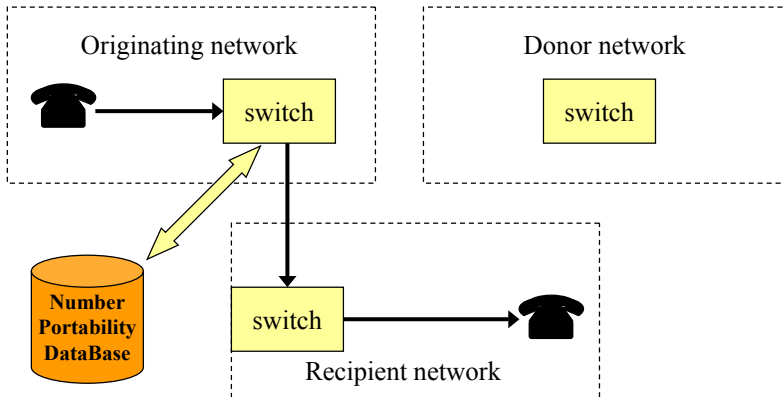
REL carries a QoR cause value, stating that called party number is ported

Originating switch then queries Number Portability database

Giuseppe Bianchi

Technical solutions

c) all-call query



Originating switch queries Number Portability database for every call!!

- best solution if majority of numbers are ported (no interaction with donor)
- but very high DB load, as EVERY number must be looked-up!

===== Giuseppe Bianchi =====

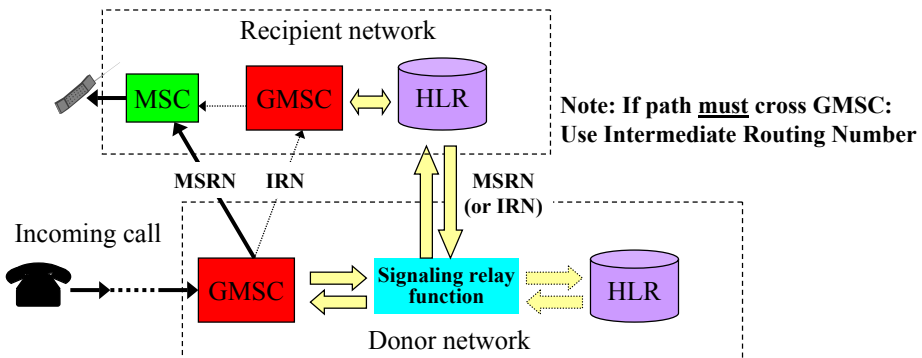
Mobile Number Portability

→ Same ideas as fixed number portability

⇒ The donor switch is the GMSC of the donor network

→ Donor GMSC Call forwarding (if more efficient fixed number portability not supported)

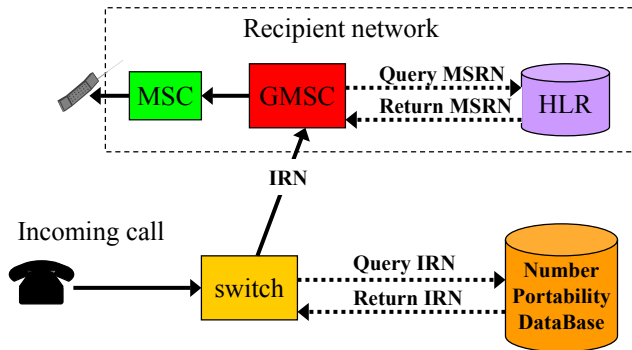
⇒ While porting number, may also get MSRN!



Clearly, still suffers of tromboning!

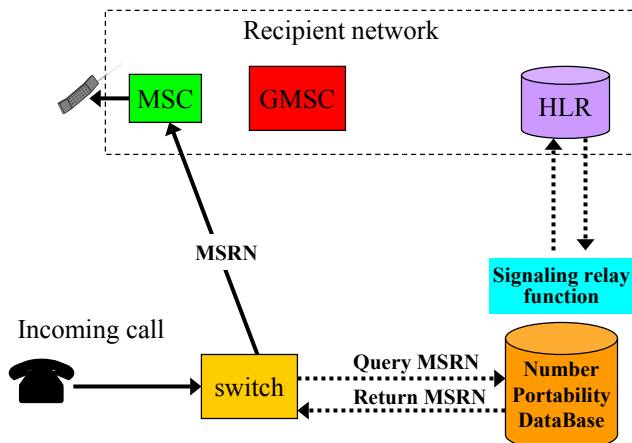
===== Giuseppe Bianchi =====

Mobile Number Portability (with all call query approach)



Giuseppe Bianchi

Mobile Number Portability improved – (with all call query approach)



Giuseppe Bianchi