



**Cellular telecommunications: GSM case study**

**Lecture 4**

**Course website:**

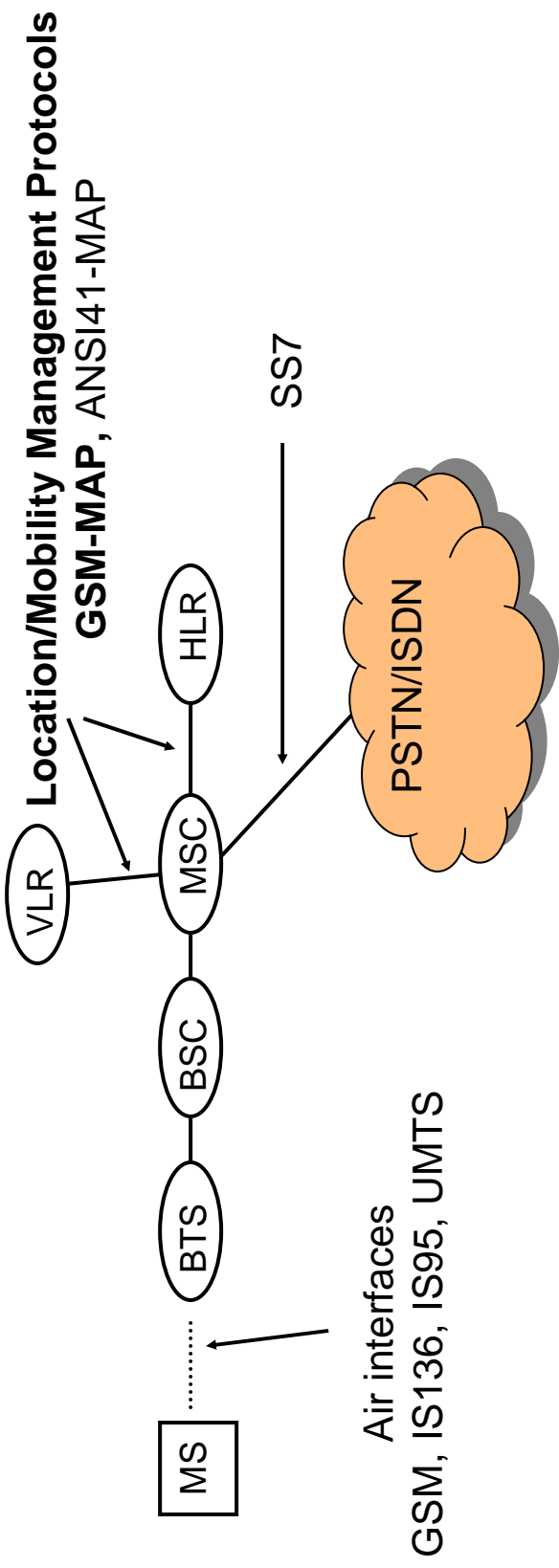
**<http://www.ee.columbia.edu/~ramjee/ee6950.html>**

## Homework 1



- **Due today**
- **Will be reviewed in the next lecture**

# Protocols examined today



## Readings

- Chapter 4, Goodman (covers IS-41)
- Chapter 10.9/10.10, Rappaport (covers SS7)

## **Mobility Management in Cellular Telecommunication Networks**

---

- **Issues and Architecture**
- **MAP**
- **Simple mobility model and performance**
- **Optimizations**
- **Security**
- **Messaging**

# Cellular Telecommunication Mobility Management

---

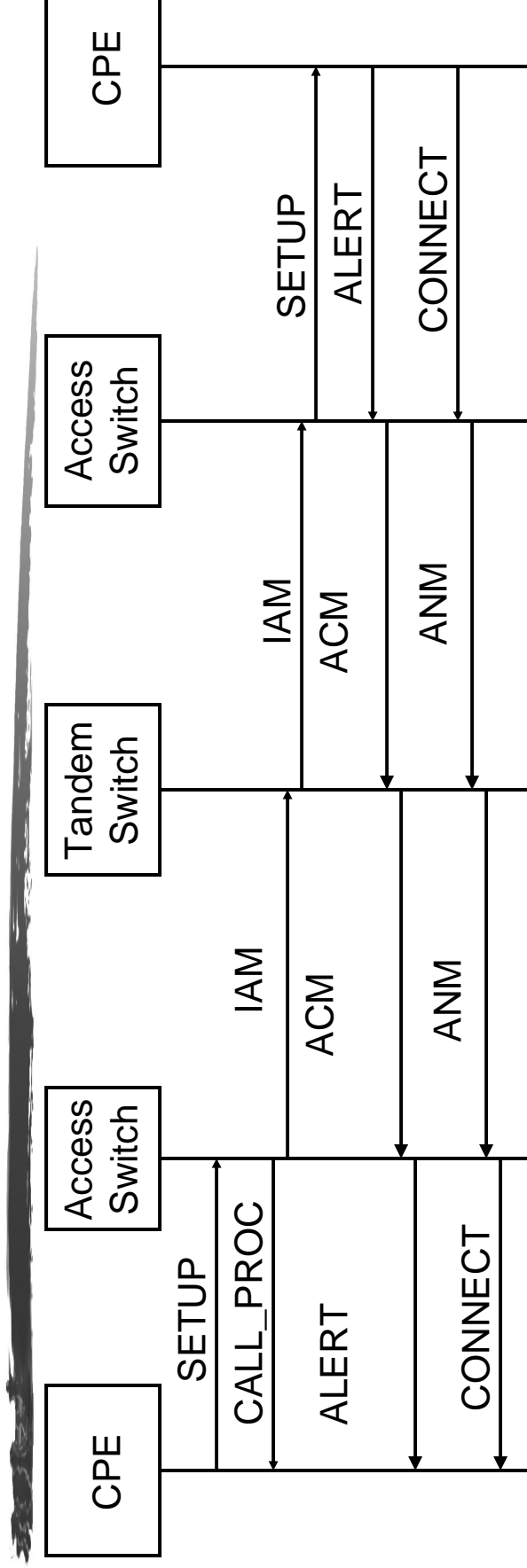
- **Routing**
  - tracking mobile while idle
  - mobile location during connection establishment
- **Services**
  - telecommunication switches provide intelligence
  - access switches manage service profiles
- **Handoffs**
  - state (context) issues
    - connection information
    - services information

# Cellular Telecommunication Systems: Performance Issues

---

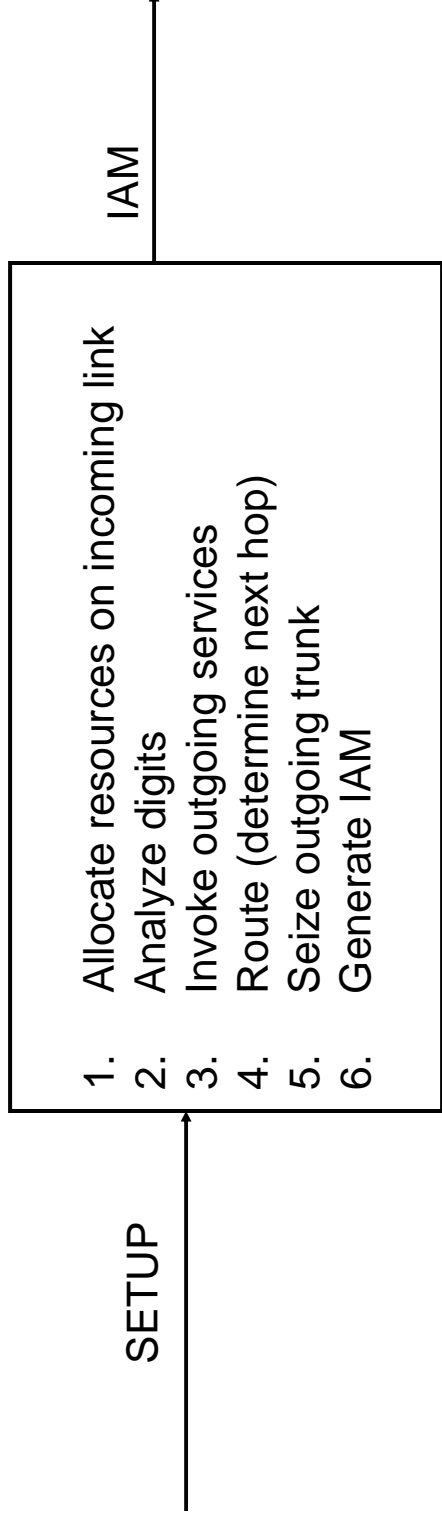
- **Signaling load**
  - network signaling due to movement of idle users
  - air interface signaling load
  - processing load on databases
- **Call establishment delay**
  - mobile location
  - data management for services

# ISDN Call Establishment



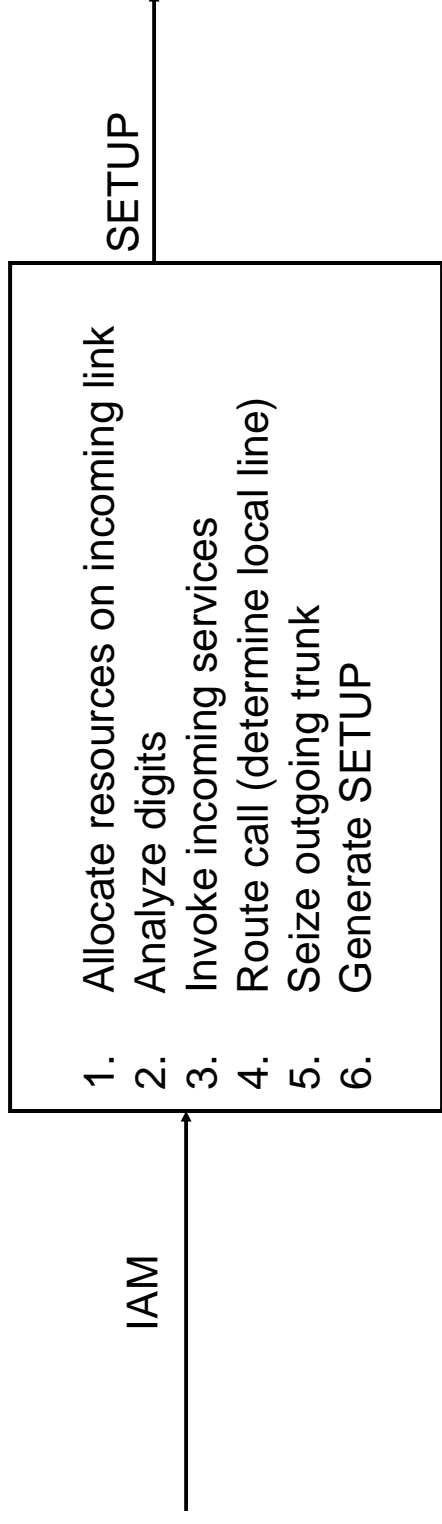
- **SETUP** – requests a call for a network/indicates an arriving call
- **ALERT** – phone is ringing
- **CONNECT** – call is answered/connection is established
- **IAM (Initial Address Message)** – seizes a trunk in the network
- **ACM (Address Complete Message)** – call has been routed and delivered
- **ANM (Answer Message)** – call has been answered

# Call Establishment Procedure



- **Access switch executes Basic Call State Model**
  - triggers services based on calling party's profile (service triggers)
  - service logic may be resident on off-switch processors
- **Access switch routes call based on called party number**
  - telephone numbers are hierarchical
    - Area code
    - Exchange
    - line

# Call Establishment Procedure



- **Egress switch executes Basic Call State Model**
  - triggers services based on called party's profile (service triggers)
  - service logic may be resident on off-switch processors
- **Egress switch routes call based on called party number**
  - telephone numbers are hierarchical
    - Area code
    - Exchange
    - line

## Impact of mobility on call establishment

---

- **Routing**

- dialed number no longer indicates a location to the access switch (or tandem switches)
- in general, telephone number is only a logical identifier
- how do we know it refers to a mobile number?

- **Services**

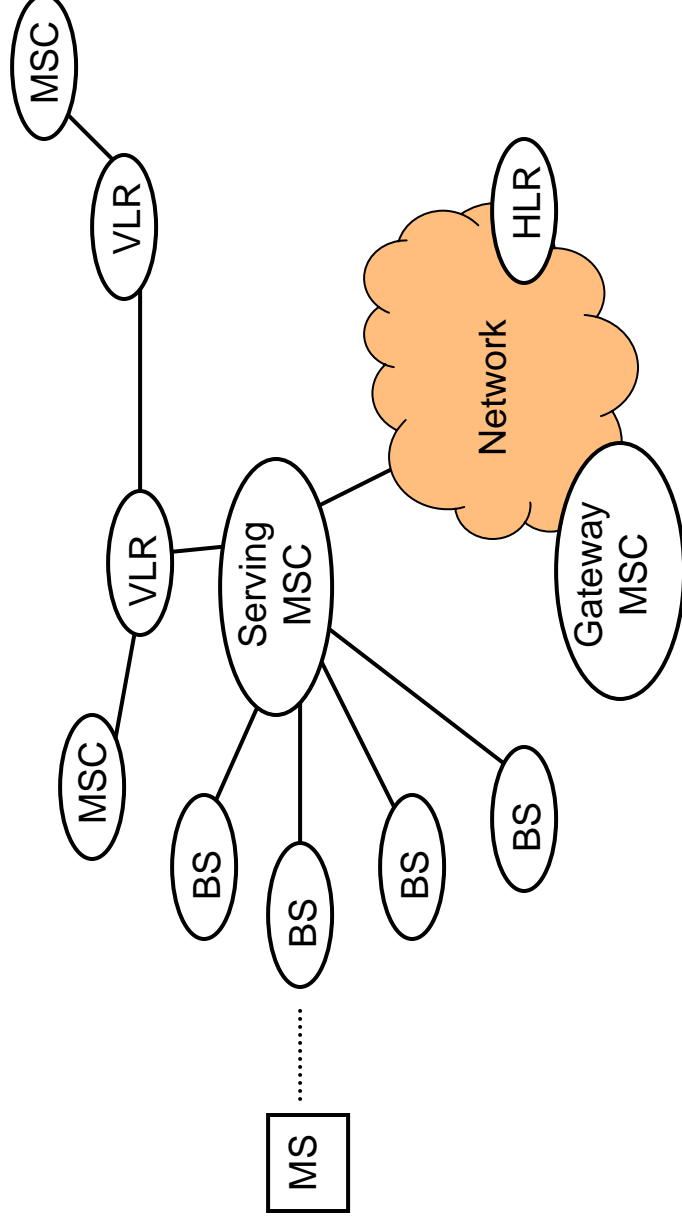
- users are no longer associated with a switch
- how do we access service profiles?

## **Impact of mobility on on-going calls**

---

- **Handoffs and connections**
  - connection state must be changed
- **Handoffs and services**
  - service state must be maintained

# Basic Network Architecture



- Gateway MSC receives incoming calls for mobiles
  - if using a home MSC, it is permanently assigned
- Serving MSC: assigned based on location of MS
- HLR: permanent registry for service profiles, pointer to VLR
- VLR: temporary repository for profile information, pointer to serving MSC

## **Basic step: before a call arrives**

---

- **User is registered with a serving MSC**
  - this MSC will page to find the BS when an incoming call arrives
- **User is registered with a VLR**
  - the VLR points to the current serving MSC
  - has temporary copy of user profile
- **User is registered with its HLR**
  - points to the VLR

**Basic steps: when a call arrives**

---

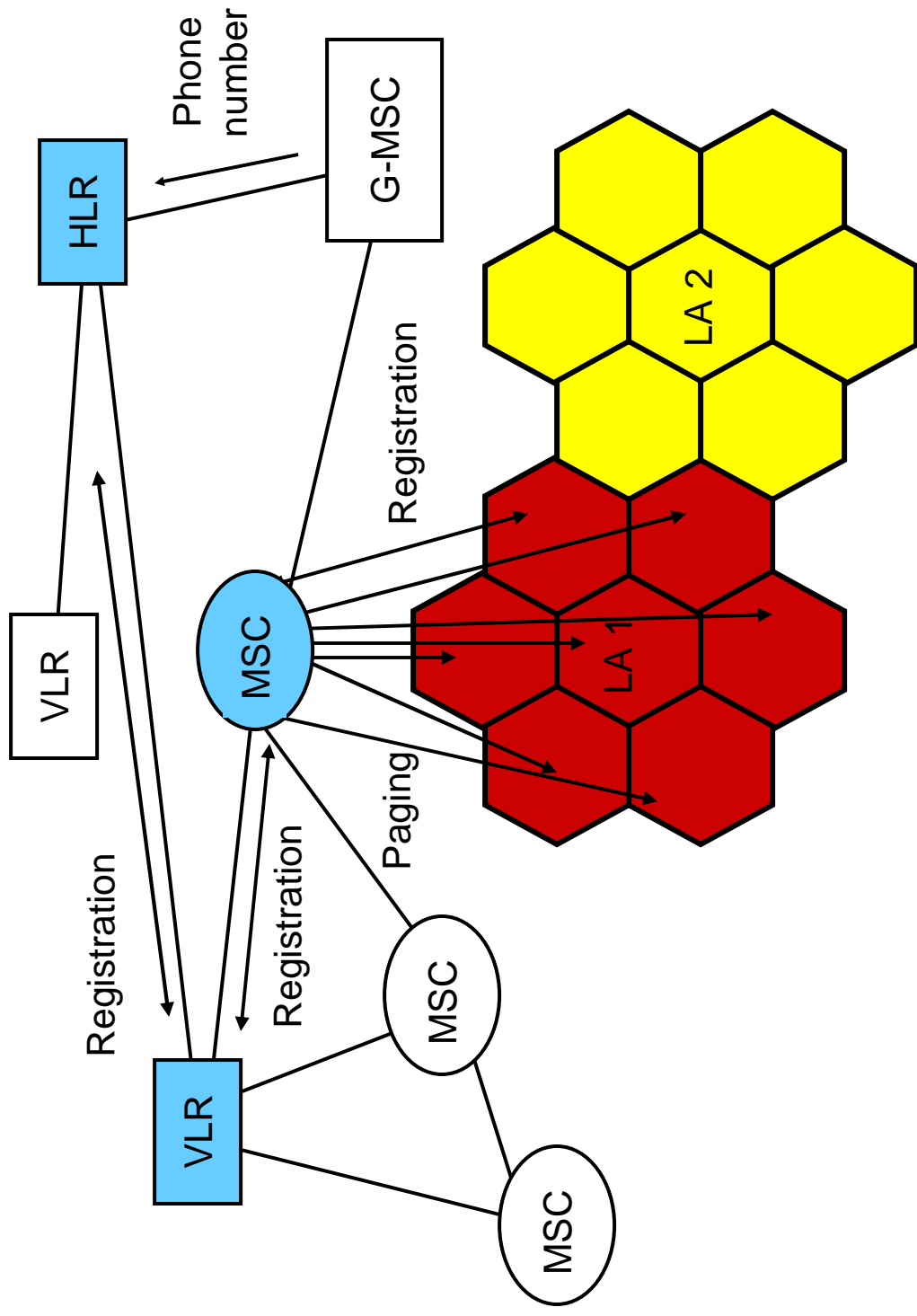
- **Call is routed to a gateway MSC based on the MS-ISDN (phone number)**
- **Gateway MSC queries HLR (known by MS-ISDN)**
- **HLR queries VLR (known by registration)**
- **Results returned to home MSC which completes the call**
- **Serving MSC pages user**

## Paging vs Registration

---

- **MSC typically manages hundreds of cells**
  - **Paging over 100s of cells can increase paging load substantially**
  - **Therefore, cells under the MSC are further split into Location Areas (LA) or Paging Areas**
  - **Whenever a mobile device crosses a Location Area, the device sends a registration informing the MSC of its current LA**
  - **Thus, the MSC pages only the cells of a particular Location Area – however, this increases the registration rate**
- Cellular planning also involves careful partitioning of cells under the MSC into Location Areas in order to balance paging and registration rate**

# Hierarchy of Location Information



**Basic steps: when a user moves**

---

- **User registers with the serving MSC**
- **If the serving MSC is new**
  - New serving MSC updates its VLR
  - If this is a new VLR
    - VLR updates the HLR
    - VLR obtains copy of user service profile
    - Old VLR entry is cancelled

## Managing Signaling Load: updates to HLR

- **Introduce hierarchy: allow VLRs to manage multiple MSCs**
  - movement between MSCs is shielded from HLR
  - localizes signaling traffic
  - reduces load for movement of idle users
  - increases load to find users (VLR to MSC) messages
- **Drawbacks**
  - can increase call setup time
  - MSC must retrieve service profiles during setup
  - VLR must signal to MSCs during setup to locate the mobile

## Managing establishment time

---

- **Reduce hierarchy: co-locate MSCs and VLRs**

- fewer database lookups to setup a call
- no service profile transfer during setup

- **Drawbacks**

- increases signaling load

## → Opposing Solutions!

- **Current solution**

- co-locate VLRs and MSCs

## Mobile Application Part

---

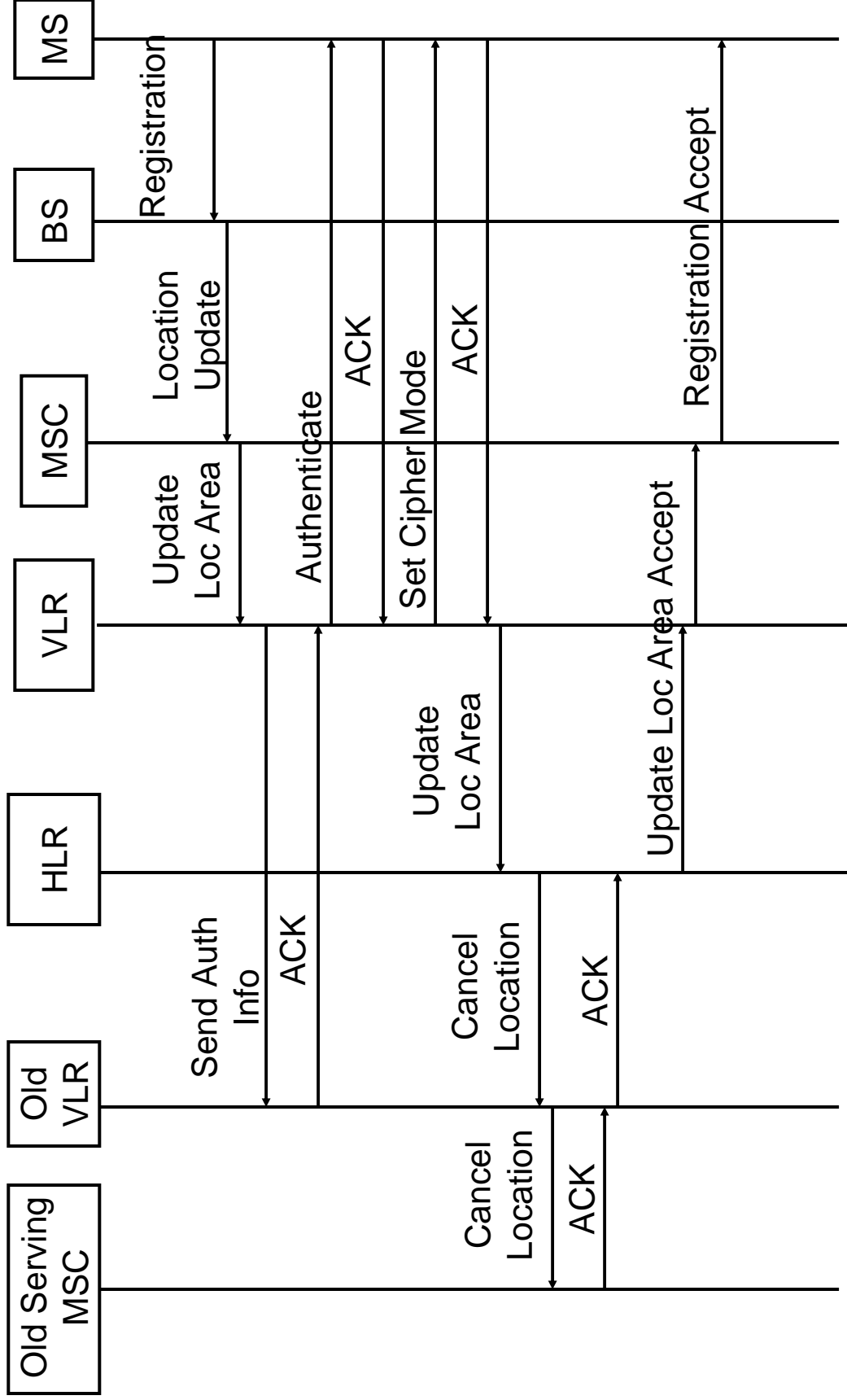
- **Mobile Tracking**
  - track idle mobile users
- **Mobile location**
  - locates mobile users to deliver a call
- **Profile downloads**
  - enables mobile users to receive services
- **Security**
  - authentication

## MAP Stack (part of SS7)

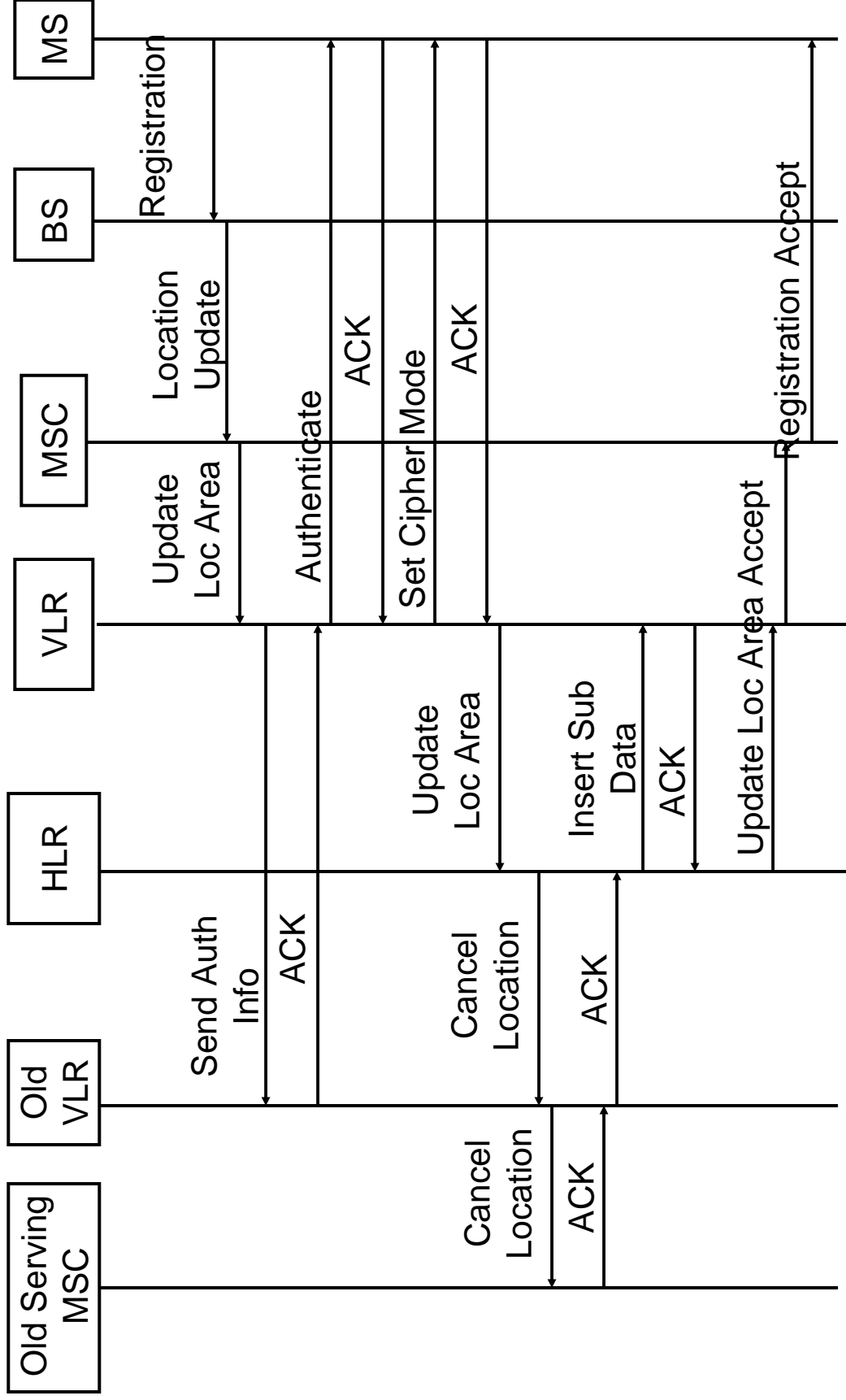
MAP (Mobile Application Part)
TCAP (Transactions Capability Application Part)
SCCP (Signaling Connection Control Part)
MTP L3 (Message Transfer Part)
Lower Layers

- **Message Transfer Part Layer 3**
  - message routing, network management
- **Signaling Connection Control Part**
  - expanded addressing
- **Transaction Capability Application Part**
  - provides transaction support
- **MAP**
  - operation definitions and parameters

# GSM Location Area Registration without Profile download



# GSM Location Area Registration with Profile download

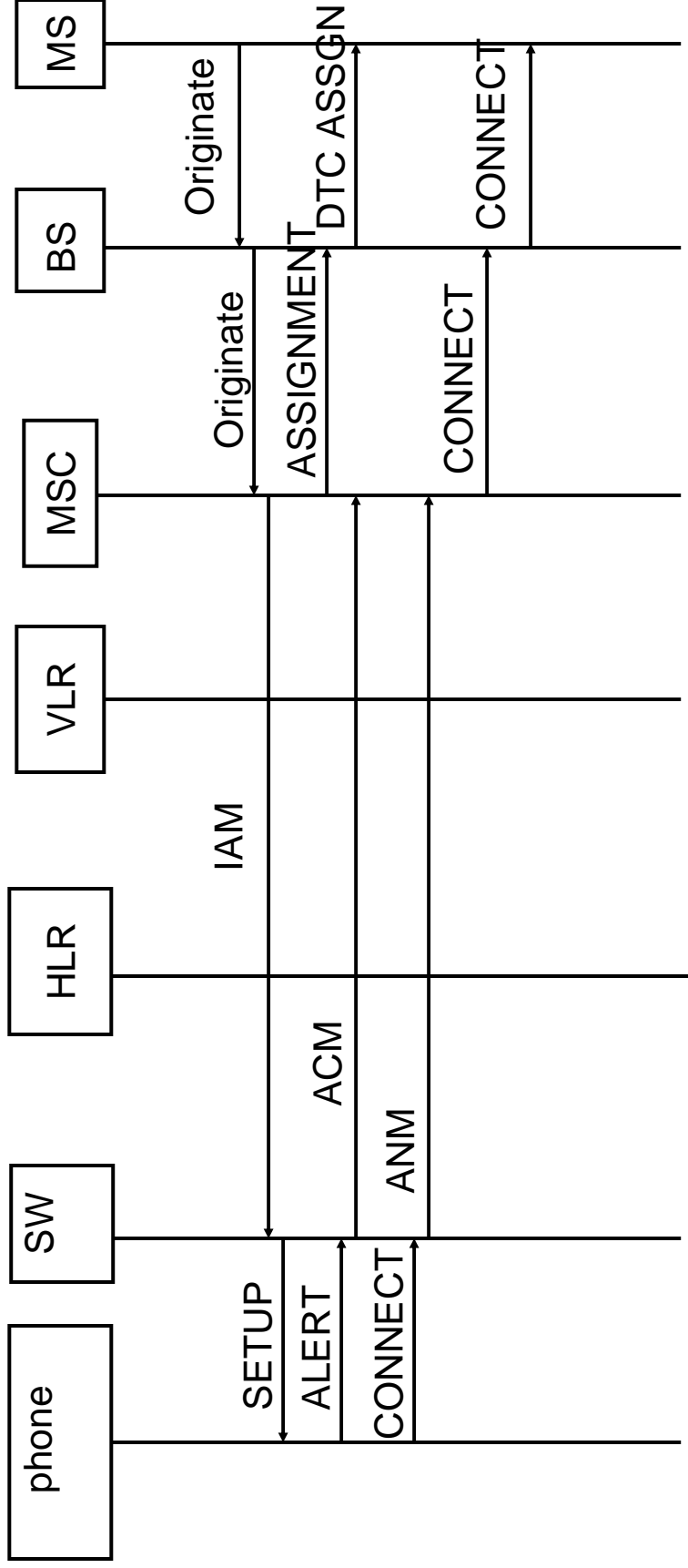


## Registration messages

---

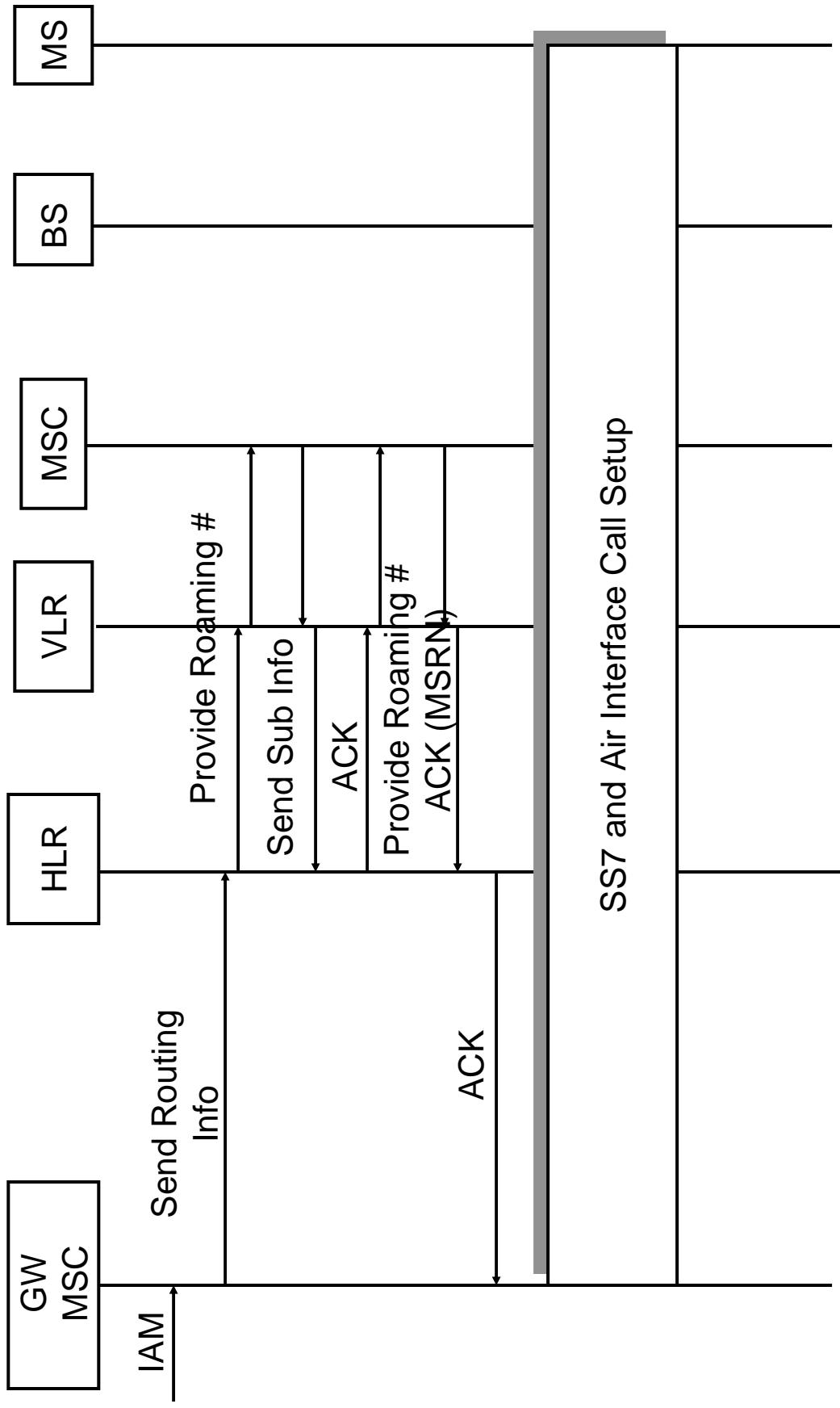
- **Update Location Area**
  - IMSI, TMSI, Previous LA, CKSN (Cipher Key Sequence Number), Target LA
- **Cancel**
  - cancels registration in old VLR
  - IMSI
- **Send Auth Info**
  - VLR gets IMSI
- **Authenticate**
  - RAND, CKSN
  - get back SRES
- **Set cipher mode**
  - on/off
- **Insert subscriber data**
  - list of services and parameters

# GSM Basic Call Origination



- For basic call
  - No interaction with databases
  - We will see interaction for advanced calls later

# GSM Call Termination with profile download



## Messages

---

- **Send routing info**
  - used to get preferred routing information
  - gateway MSC returned Mobile Station Routing Number (MSRN)
- **Provide Roaming #**
  - used to get location information from the VLR
  - IMSI, MSISDN, GMSC
  - returns MSRN
- **Send subscriber info**
  - list of services and parameters

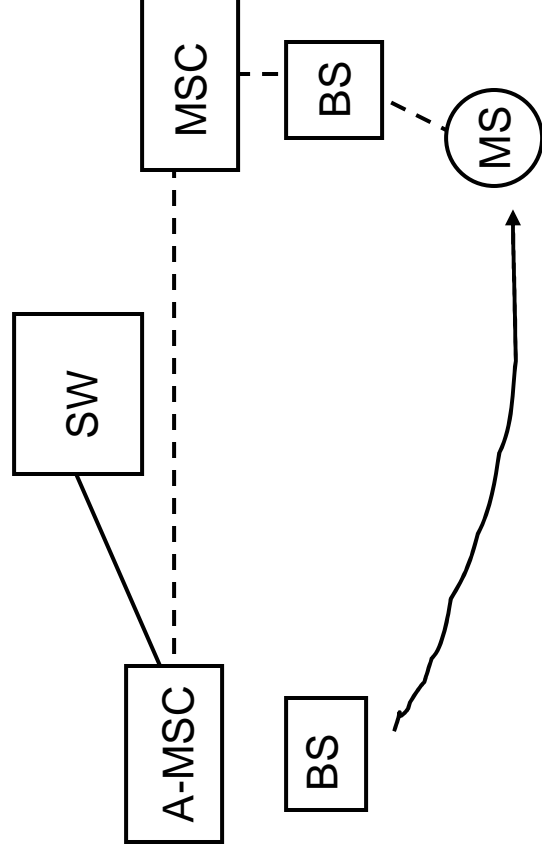
## Handoff problems

---

- **Service triggers and state**
  - should they be moved during the call?
- **Routing information**
  - should it be updated during a call?

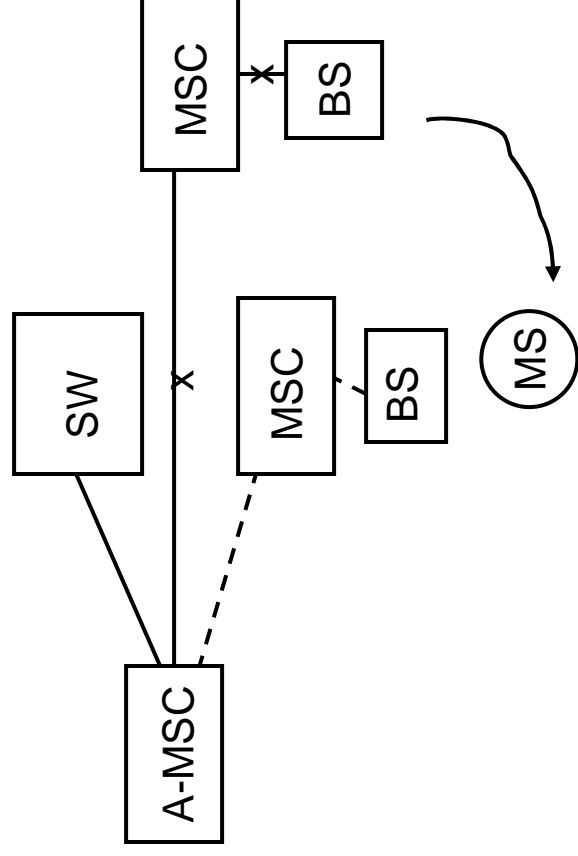
## Basic handoff solution

- **Forward connections**
  - creates an anchor MSC
  - maintains call state
  - isolates routing information changes
- **May waste resources**
  - inefficient routes

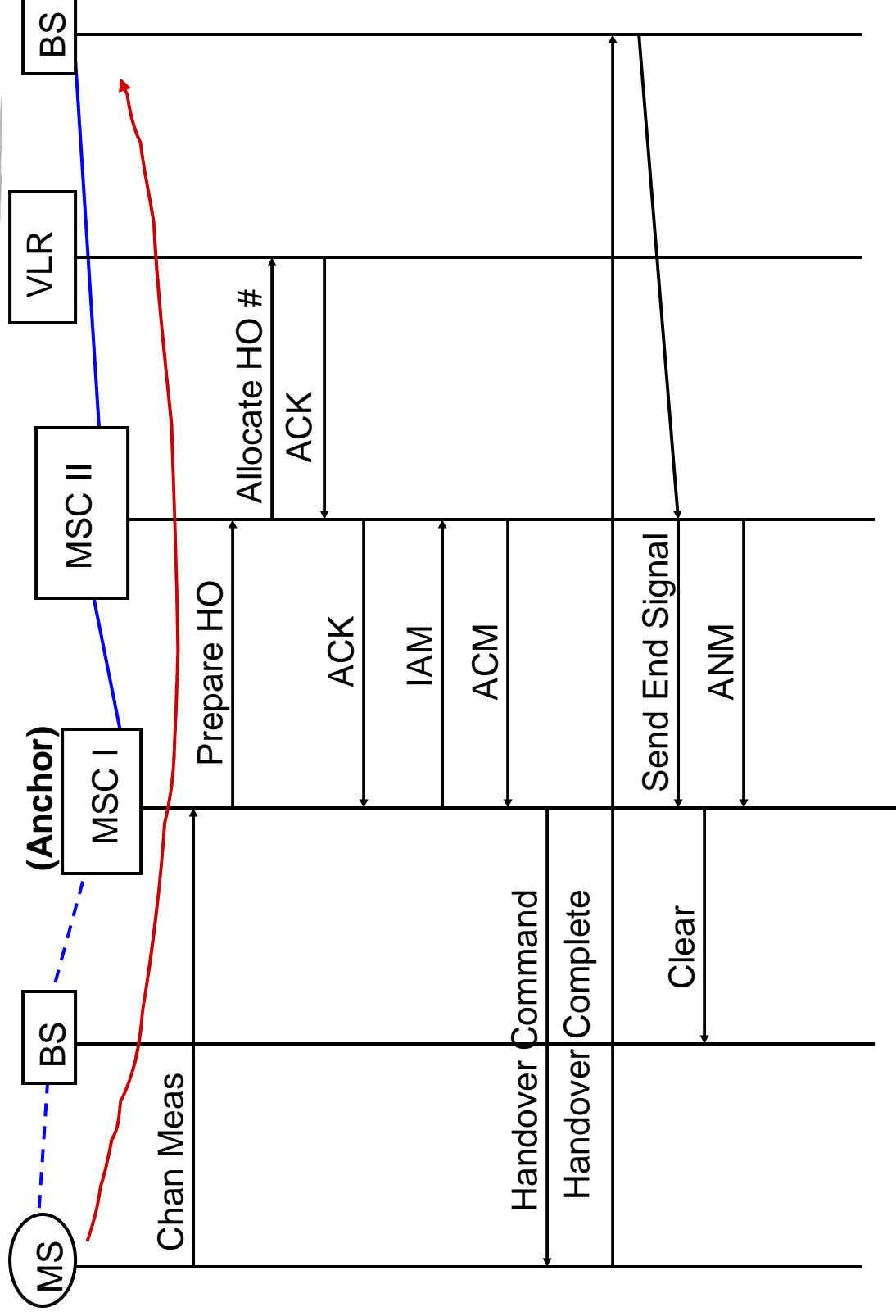


## Advanced handoff solutions

- **Subsequent**
  - maintains anchor, but eliminates hops

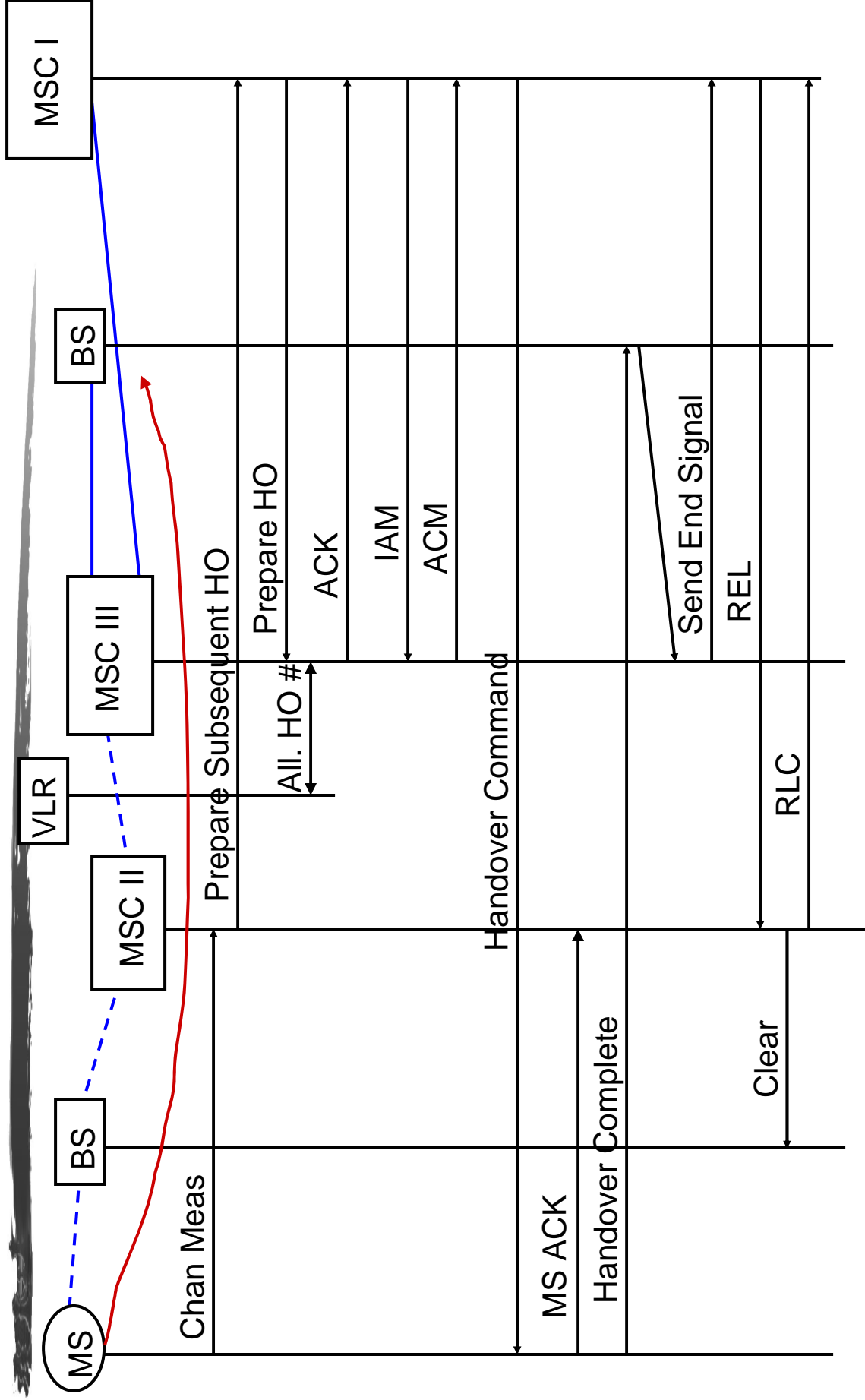


# GSM Handoff: Basic



# GSM Handoff: Subsequent

ANCHOR

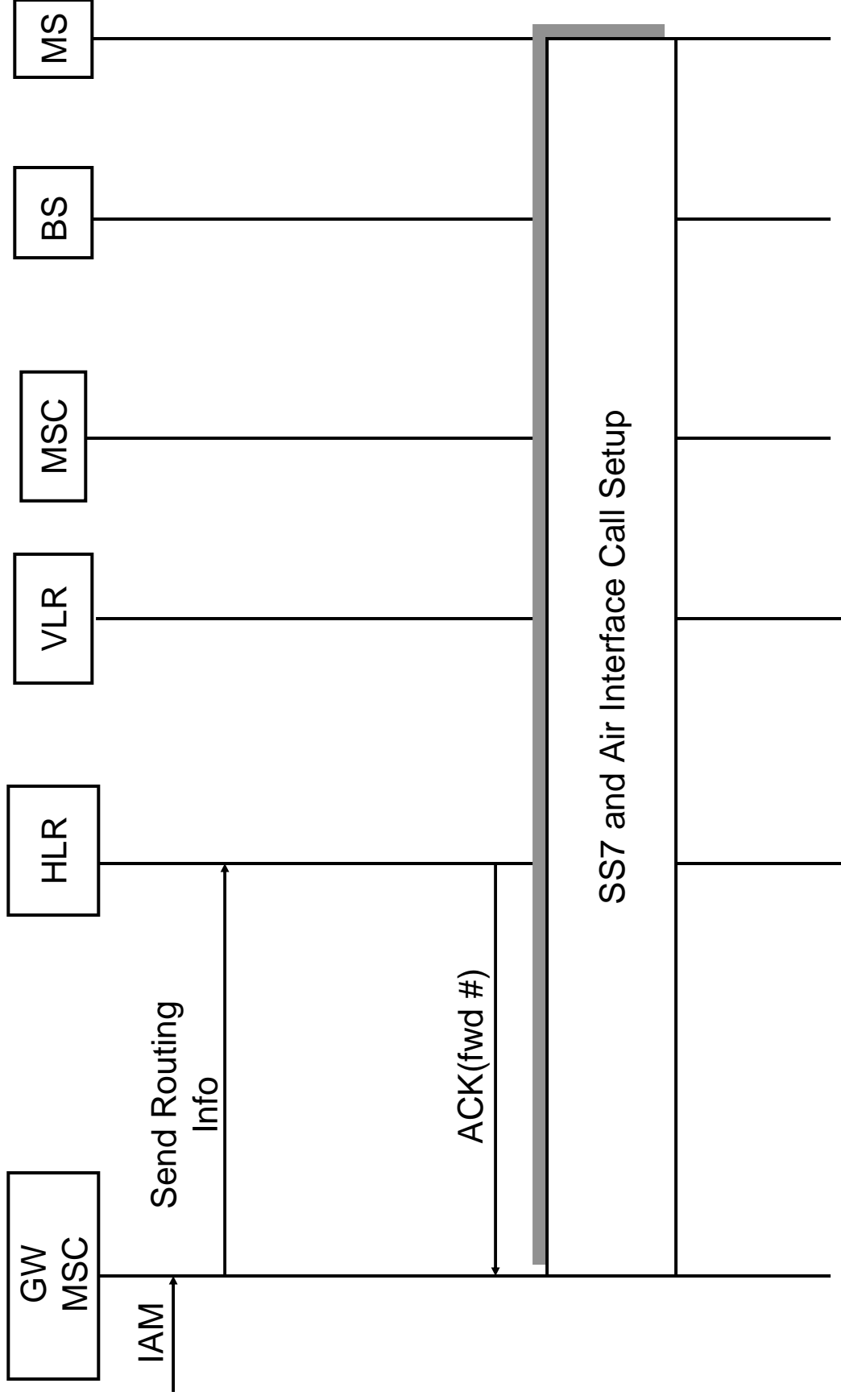


## Results of handoff

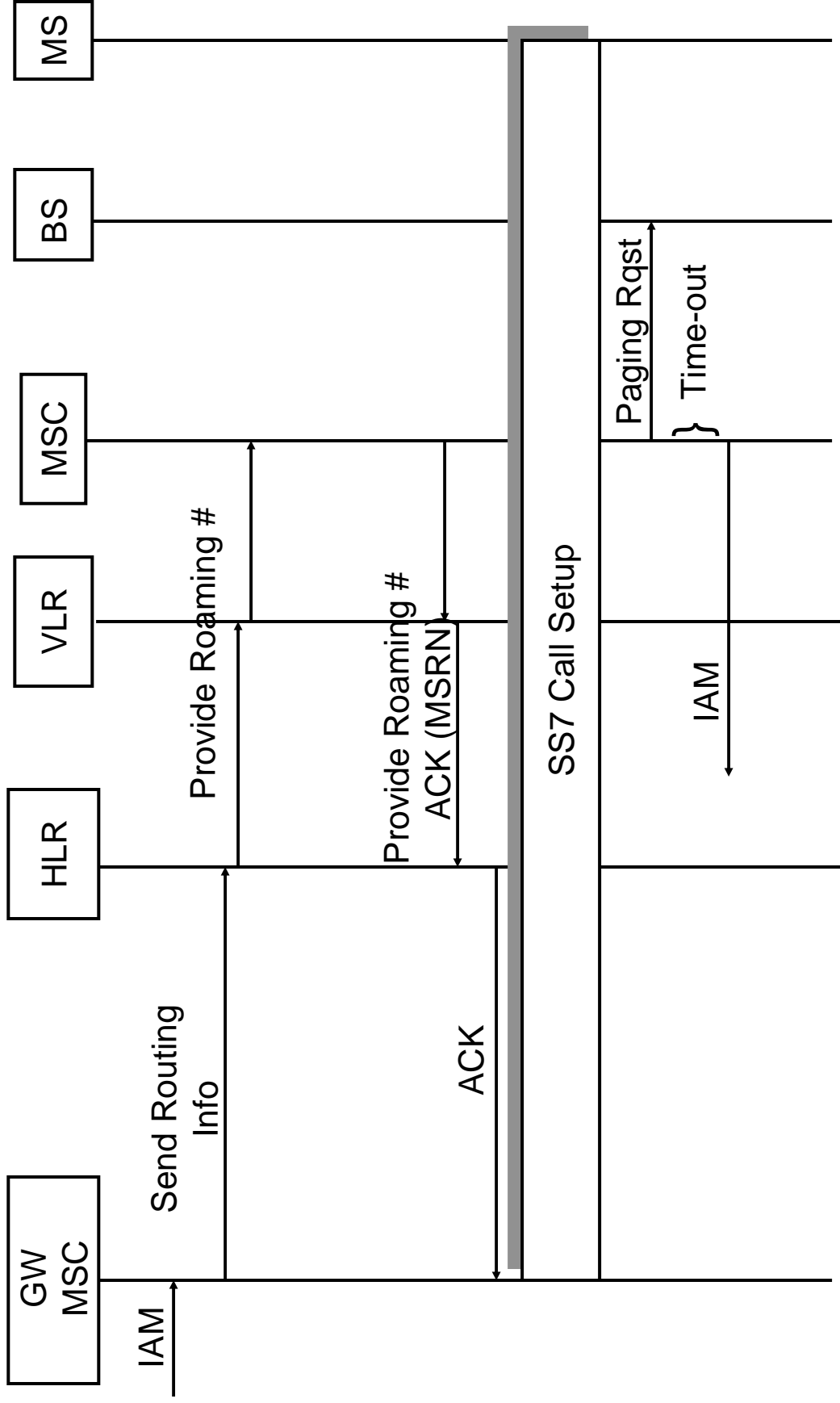
---

- **Anchor switch**
  - retains call state and services information
  - points to next switch
- **Successive switches**
  - points to any other switches

# GSM Basic Service Example: Immediate Call Forwarding

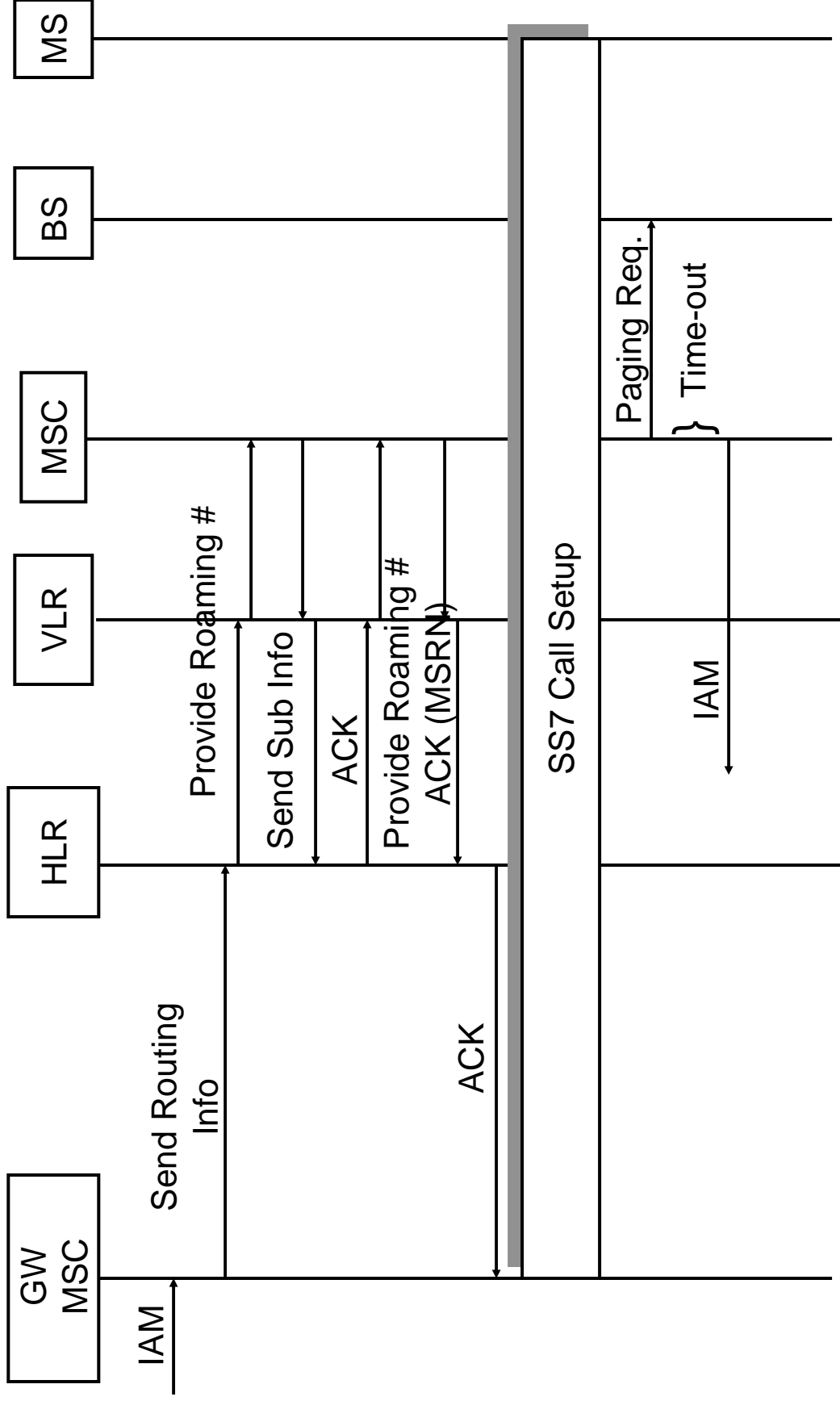


# GSM Service Example: CF on No Response to Page



Profile downloaded during registration

# GSM Service Example: CF on No Response to Page



Profile downloaded during call setup

## Service Observations

---

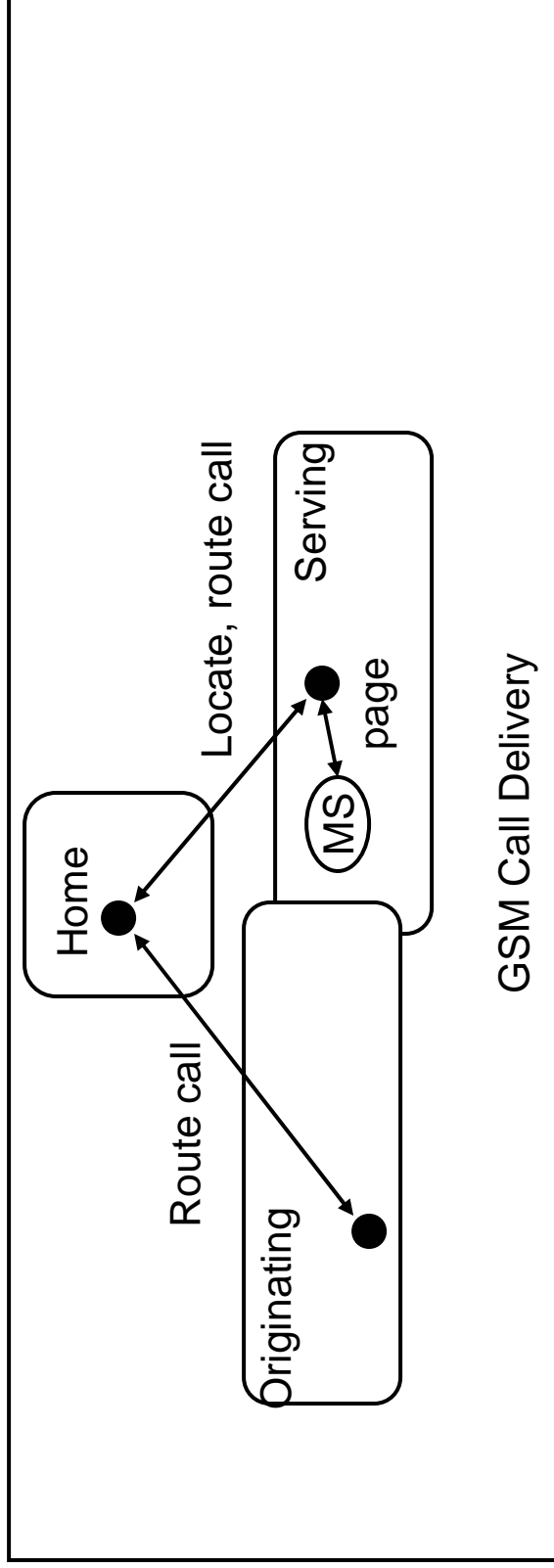
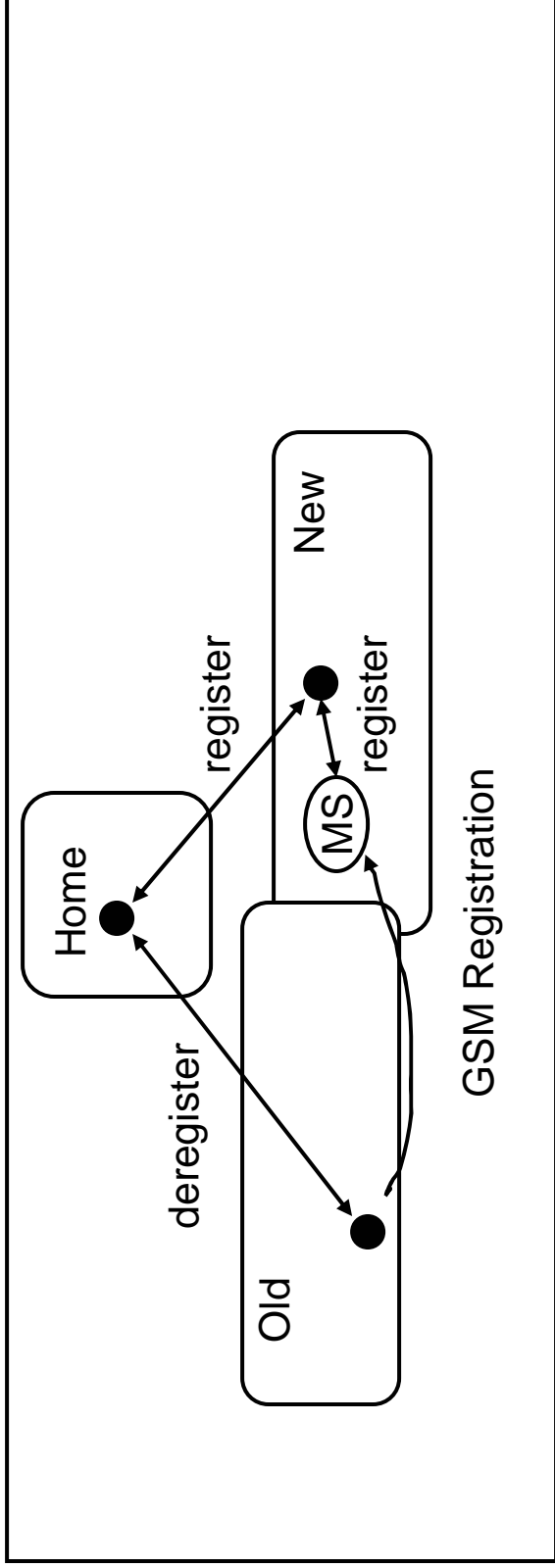
- **VLRs/Serving MSCs**
  - profiles are downloaded with service triggers during registration or call establishment
  - serving MSC can detect if a feature is active
- **HLRs**
  - store triggers and service data
  - triggers are downloaded to MSCs/VLRs during registration or call establishment
  - HLRs can directly offer some services for incoming calls

## Impact of Service Observations

---

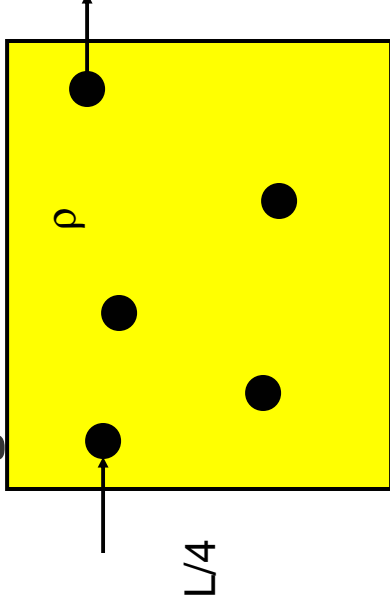
- **Trigger downloads upon registration**
  - reduce call establishment time for calls with services
  - do not have to access databases in real-time
- **Trigger downloads upon call establishment**
  - reduces signaling load if services are not activated
  - increases call establishment time for many services when they are activated

# Review of GSM Cellular



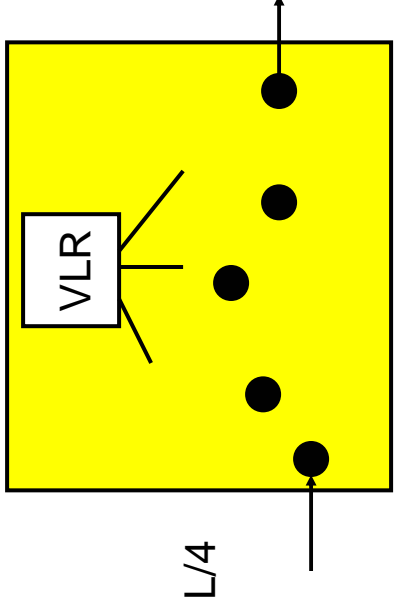
## Simple Mobility Model

- Based on conservation of flow
- Measure boundary crossings



- Assumes users move in a random direction at a constant velocity
- Rate of boundary crossings =  $\rho vL/\pi$ 
  - $\rho$  is the density of users
  - $v$  is the velocity
  - $L$  is a area boundary length (perimeter)

## Example: Load at VLR



- Calculate the boundary crossings
- Each entering mobile creates an Update LA
- Each exiting mobile creates a Cancel
- Assume
  - $L = 70$  miles
  - $\rho = 150$  users/sq. mile
  - $v = 50$  miles/hour

**Example: VLR Load (subscriber info downloaded during reg.)**

- **Boundary crossing rate =  $150 \times 50 \times 70/\pi$** 
  - 46 crossings/second
- **Load on VLR due to mobility is 138 operations/second**
  - updates (3): Update LA, Reg. Canc., Insert Sub Data

## Example, continued

- **Assume  $\lambda = 3$  calls/user/hour, equal amount in and out**
  - for each incoming call there is one database query (Provide Roaming #)
- **$\rho = 150$  users/sq. mile,  $L = 70$  miles square**
  - each area contains  $150 \times (70/4)^2 = 46,000$  users
  - Rate of queries =  $1.5 * 46000 / 3600 = 19$  queries /second
- **Total load**
  - 19 queries/second (call related)
  - 138 updates/second (mobility related)
- **Conclusion**
  - in this case, mobility dominates the database load

# Optimizations in Cellular Mobility Management

---

- **Problem**

- high signaling load due to mobility
- most signaling traffic is to track idle users
- load vs. setup time

- **Possible Solutions**

- introduce more hierarchy
- distribute processing

## Two strategies for modifying MAP procedures

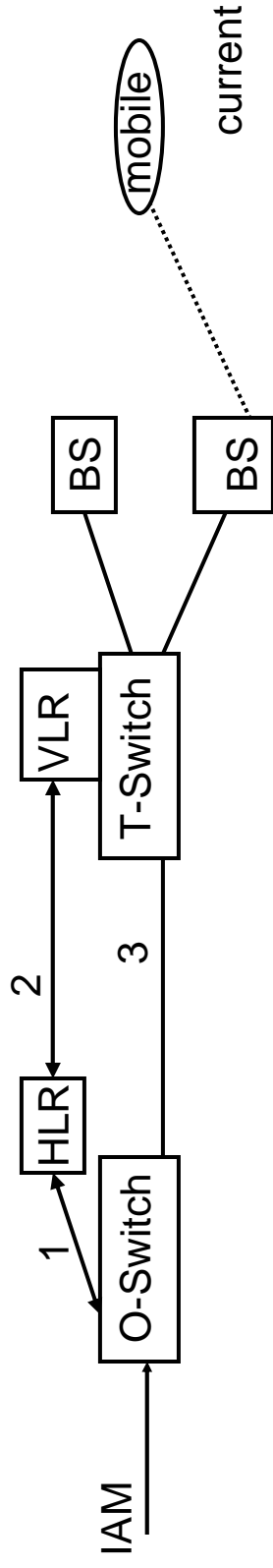
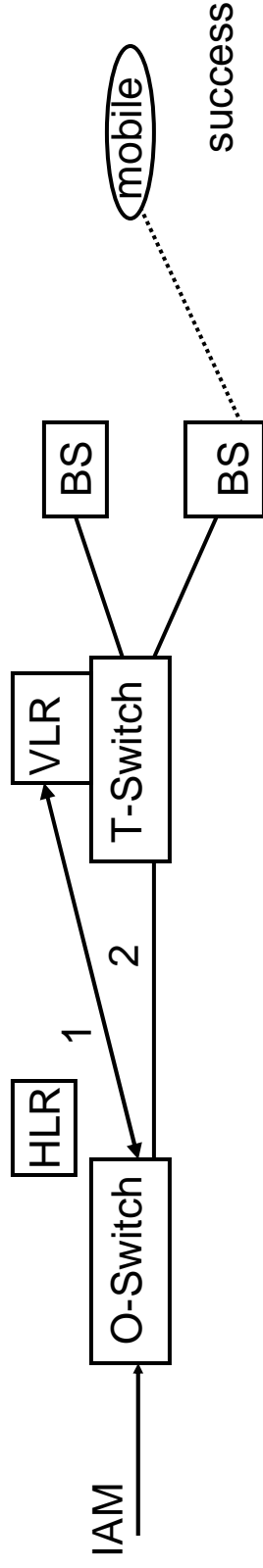
---

- **Caching**
  - works well for low mobility users
  - may reduce setup time and signaling load
  - depends on originating switch
- **Forwarding**
  - works well for high mobility users
  - decreases signaling load at the expense of setup time

# Caching

R. Jain, et al, "A Caching Strategy to Reduce Network Impacts of PCS, *IEEE JSAC*, 10/94

- Location (pointer to VLR) is cached at originating switch
- For calls to a mobile, originating switch checks cache
  - if hit, query VLR directly
  - if miss, follow standard procedures
  - saves one query (to HLR) if VLR query is successful
  - cost one query if VLR query is unsuccessful



## Caching: Results

---

- **Depends on Local Call-Mobility Ratio**
  - (LCMR = # calls from an originating switch to a user/registration area movements of that user)
  - can define a threshold to decide if one should attempt caching
- **Good for high LCMR (>5)**
  - can reduce both load and setup time
- **Depends on originating switch**

## Simple Example: Load on VLRs/HLRs

- For every successful cache, VLR has 1 query, HLR has 0 queries
- For every miss, VLR has 2 queries, HLR has 1 query
- Assume success rate of 30%
- HLR query load reduced by 30%
  - $0.7 \times 1 + 0.3 \times 0 = 0.7$  queries/call
- VLR query load increased by 70%
  - $0.7 \times 2 + 0.3 \times 1 = 1.7$  queries/call
- Total query load increased by 20%
  - $0.7 + 1.7 = 2.4$  queries/call
  - signifies increased call setup time

## Simple example: Load on VLRs/HLRs

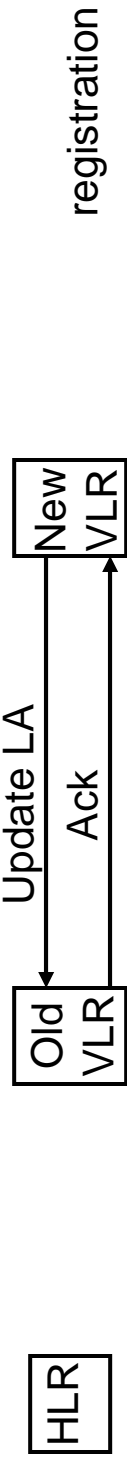
---

- **Assume success rate of 85%**
- **HLR query load reduced by 85%**
  - $0.15 \times 1 + 0.85 \times 0 = 0.15$  queries/call
- **VLR query load increased by 15%**
  - $0.15 \times 2 + 0.85 \times 1 = 1.15$  queries/call
- **Total query load decreased by 35%**
  - $0.15 \times 3 + 0.85 \times 1 = 1.3$  queries/call
  - signifies decreased call setup time

# Forwarding

R. Jain, et al, "An Auxiliary User Location Strategy Employing Forwarding Pointers to Reduce Network Impacts of PCS," IEEE ICC'95.

- **When chaining LAs, new VLR updates old VLR**
  - cuts down load to HLR
- **To find mobile, HLR queries last known VLR which forwards request (chaining)**
  - increases call setup time



## Forwarding

---

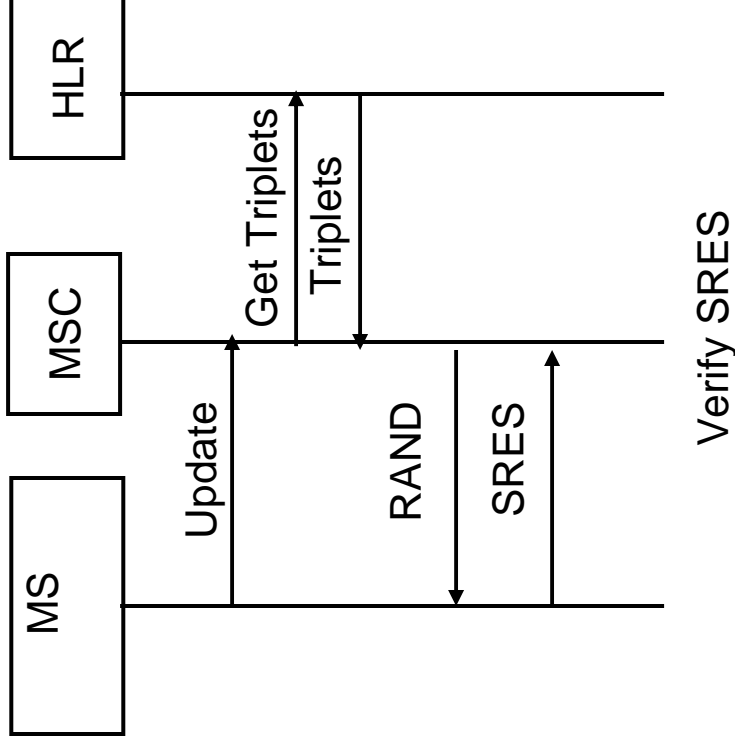
- **Tradeoff between load and setup time**
  - define a maximum number of forwarding VLRs,  $K$
- **Results depend on  $K$  and CMR**
  - good for low CMRs ( $< 1$ )

# Security

---

- **Shared secret between SIM and HLR**
  - Ki, 128-bit key
- **Three main secret algorithms A3, A8, and A5**
  - A3 used for authentication
  - A8 used for generating key for encryption (Kc)
  - A5 used for ciphering
- **Encryption key, kc**
- **When MS first signs up, HLR provides MSC with five triplets**
  - RAND (random challenge), SRES (32-bit signed response) and Kc

# Security Signaling



- **MS generates session key, Kc, using Ki, RAND, and A8**
- **BTS receives Kc from the triplet sent by the HLR**
- **Over-the-air traffic is encrypted using A5 algorithm and Kc**

## A3 authentication algorithm

---

- A3 takes the 128bit Ki, 128bit RAND, and generates 32-bit SRES
- A3 is supposed to be a secret but it was found that COMP128 algorithm was primarily being used
- COMP128 generates 128bits and uses first 32bits as SRES
- COMP128 can be broken by chosen challenge attack
- Provide the SIM appropriate RANDs and discover the secret key
  - 8 hours physical access to the SIM can reveal Ki
  - Masquerade as base station and discover Ki

## A8 session key generation algorithm

---

- A8 takes the 128bit  $K_i$ , 128bit RAND, and generates 64-bit  $K_c$
- COMP128 algorithm is also used here
- COMP128 generates 128bits and uses last 54bits+10zeros as  $K_c$
- The COMP128 can be broken as before

## A5 ciphering algorithm

---

- A5 takes the 64bit Kc and 22 bit Frame number and generates 114-bit keystream
- This keystream is XORed with the plain text to produce ciphered text
- A5/1 is the original algorithm (time-complexity of  $2^{54}$ )
- Weaker versions such as A5/2 defined for export
- Brute-force attack is feasible given modern processors but may not be possible in real-time
- Other ways to reduce the complexity of attack exist
- Also note that only the wireless link is encrypted – communication from base station towards MSC is in the clear (this could be a fixed wireless link!)

## Cloning



- **Once Ki is known, the SIM can be cloned**
- **If both original subscriber and clone subscriber are powered-on at the same time, the network (HLR) can detect that cloning has occurred and can shut-down both phones**
- **However, the clone can still unobtrusively listen to all conversations of the original phone**

## Security: lessons learned



- **Using well publicized algorithms that are battle tested is better than using secret algorithms that are not well scrutinized**
- **Mutual authentication of subscriber AND network essential**
- **Longer bits for the ciphering algorithm will help prevent brute-force attacks**
- **Ciphering should extend to other network elements rather than just the base station**

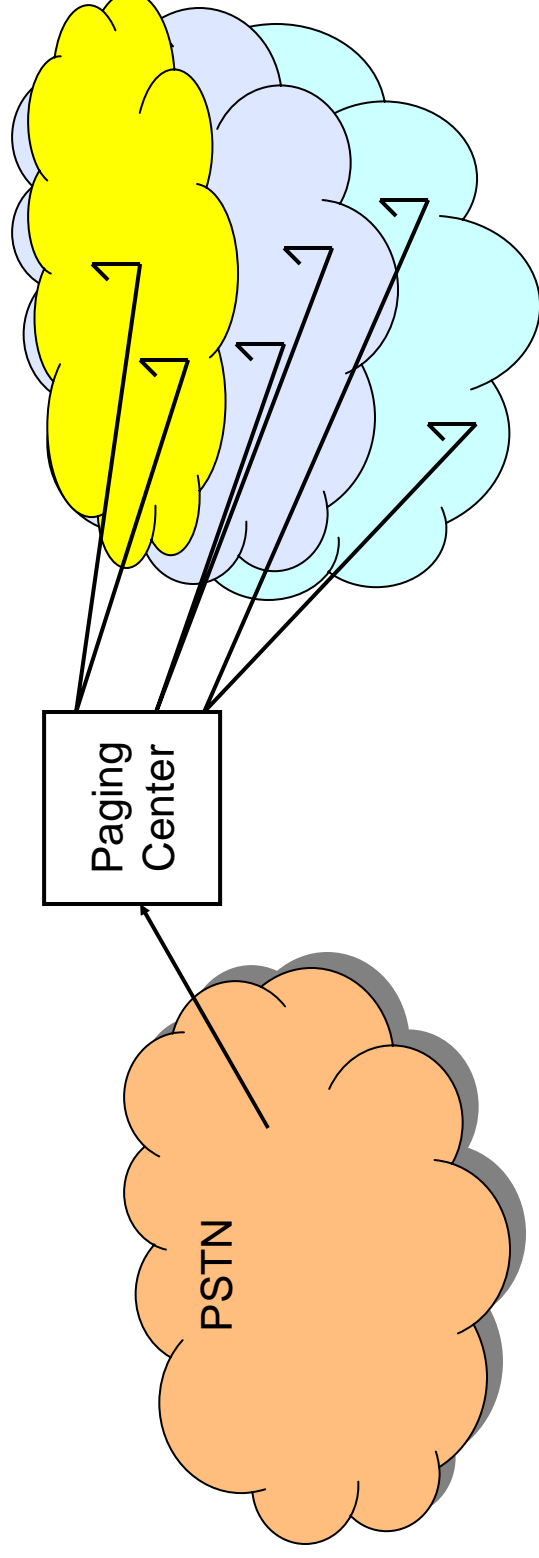
## Application: Cellular Messaging

---

- **Two-way paging**
  - adds a reverse channel to paging systems
- **Benefits of reverse channel**
  - reliable paging
  - replies to pages
  - pager initiated messages
- **Other services**
  - multicast
  - delayed delivery
  - robust operation despite disconnectivity
- **Requirement**
  - small, long lasting device

# Paging Systems

- **One way channel (down-link)**
  - unreliable
  - no location information available
- **Page delivery**
  - based on flooding
  - creates bottlenecks
- **Service available (and paid for) by coverage area**

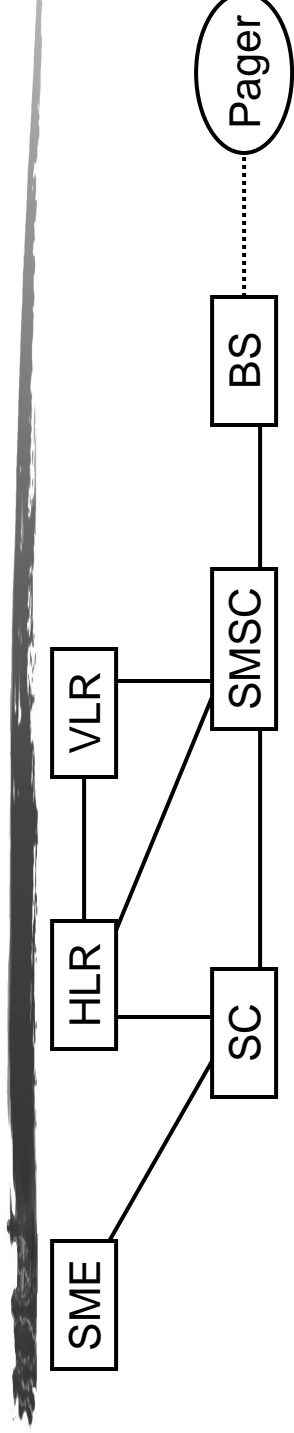


## Solutions using the reverse link

---

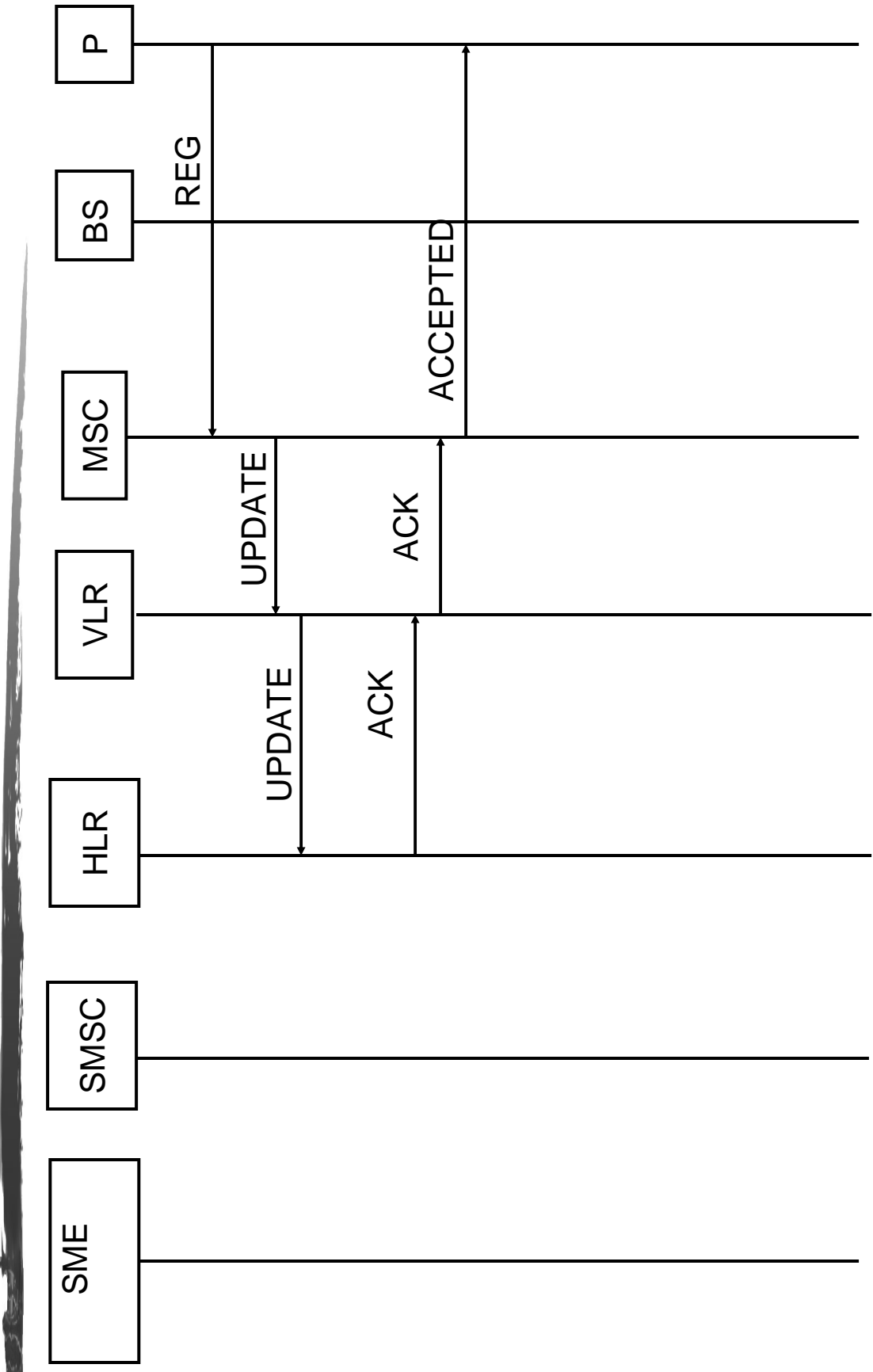
- **Reliability**
  - send automatic acknowledgements from paging unit
- **No Flooding**
  - obtain location information from pagers
- **Trade-offs**
  - registrations = power consumption
  - registrations = lower paging load

## Cellular Messaging Architecture



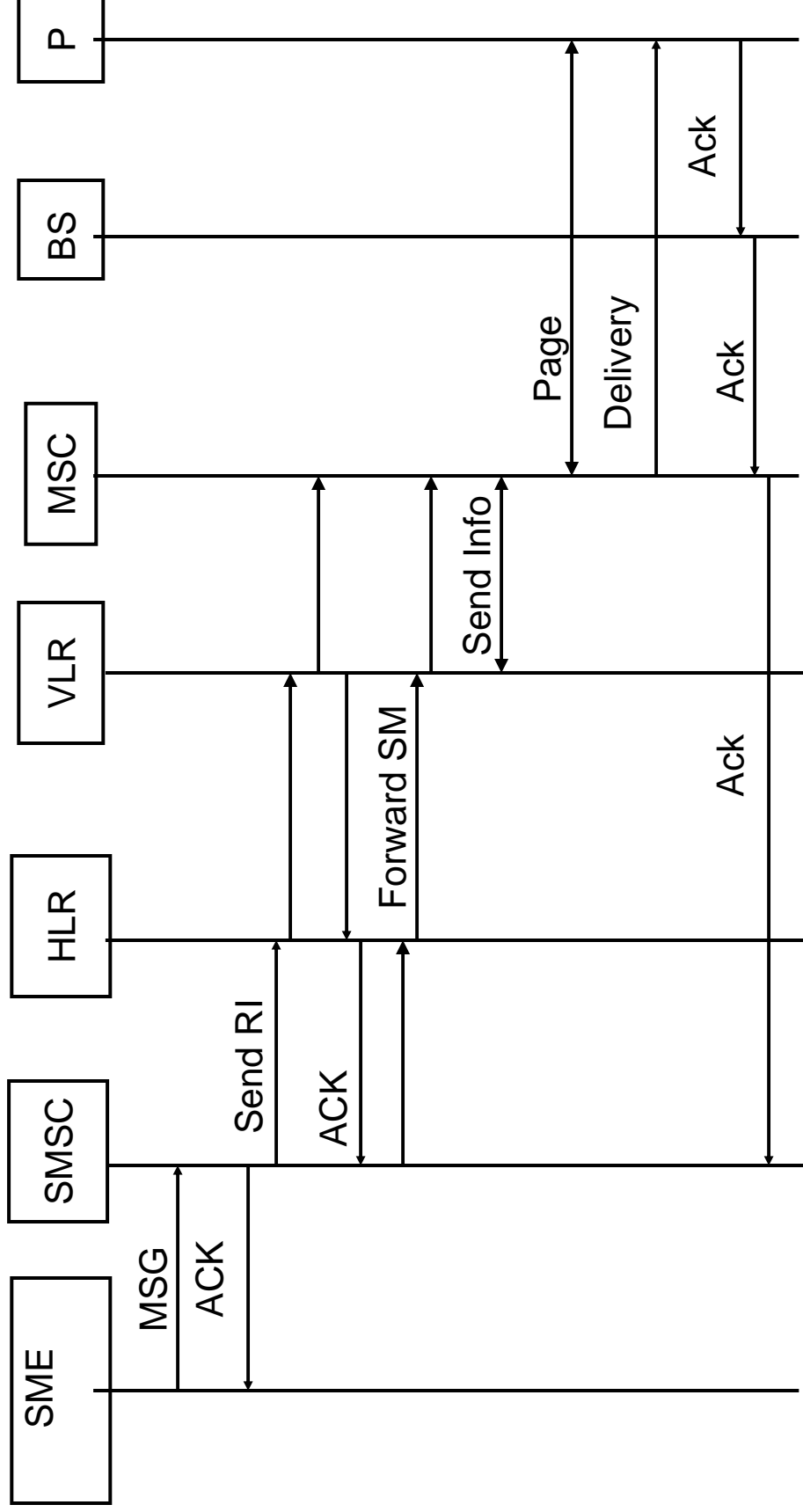
- **Short Messaging Agent (SME) – a fixed messaging endpoint**
- **Service Center (SC) – coordinates messaging activity**
- **MSC, HLR, VLR, BS – similar roles as in cellular**
- **Primary difference**
  - messages are sent as signaling messages, i.e., no connections are established

# Delivery to a pager: registration



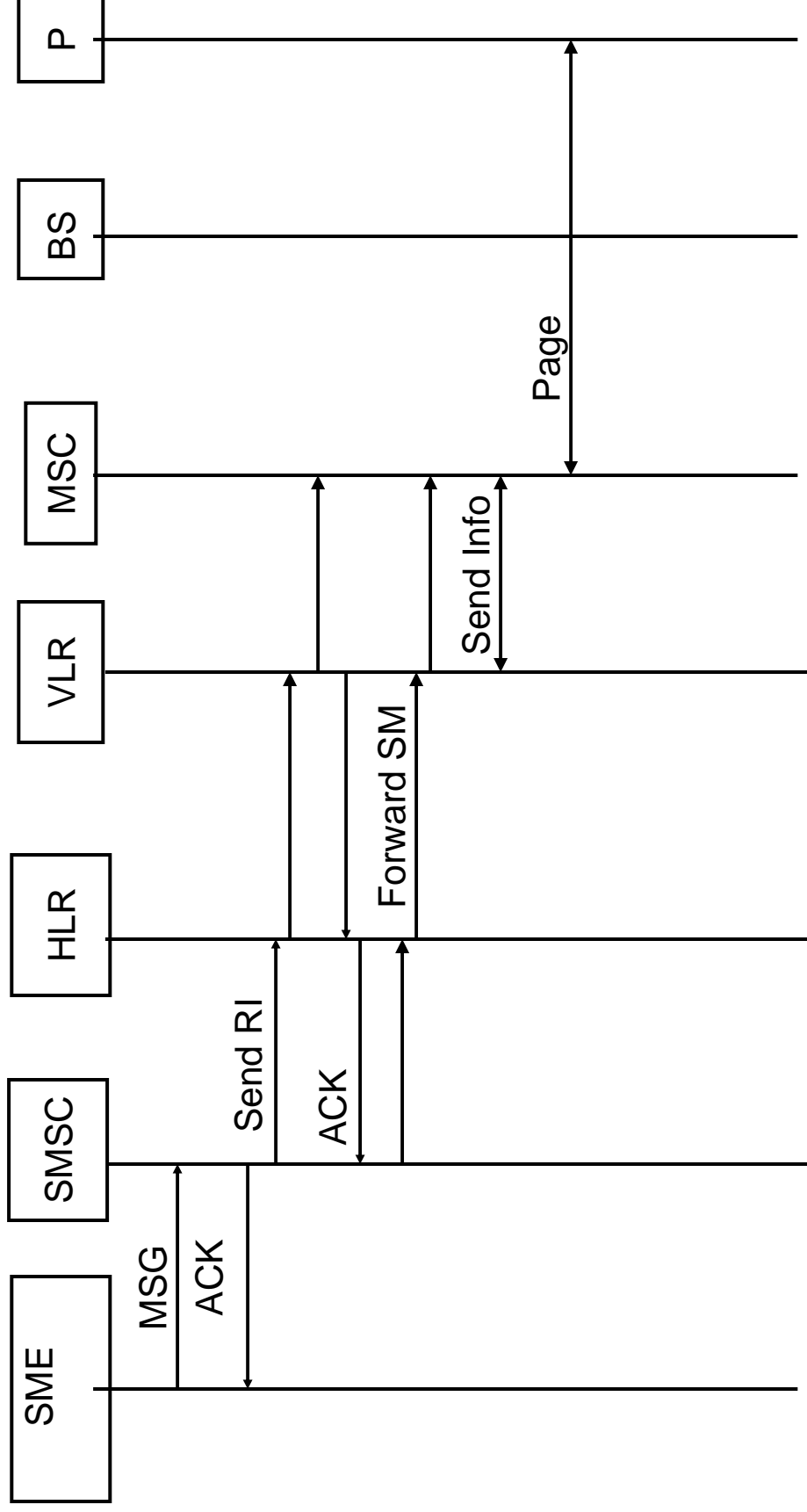
VLRs/HLRs act as in a cellular network

# Delivery to a pager: message delivery



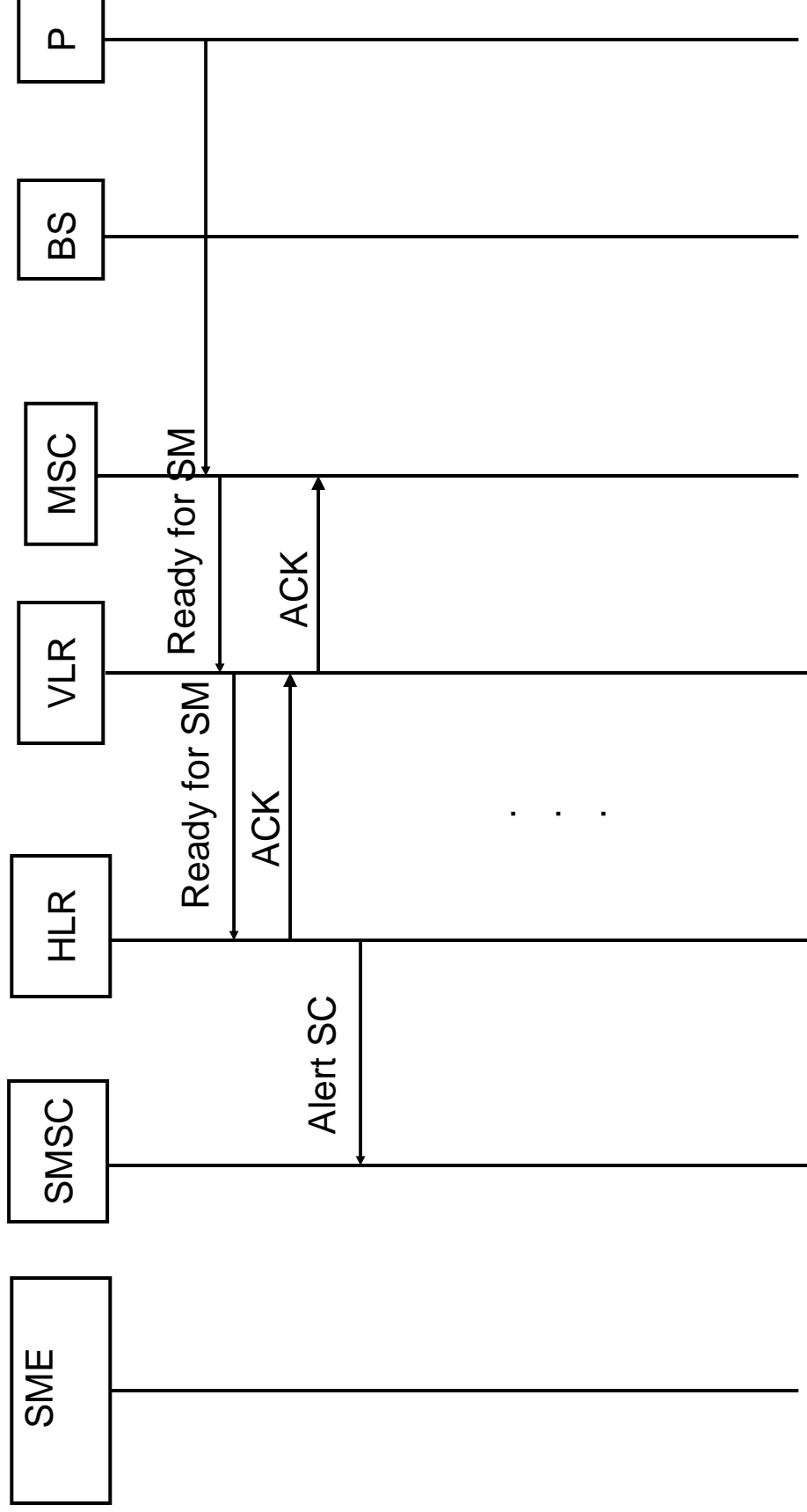
- **Send Routing Info for SM**
  - like regular cellular telephony
- **MT Forward SM**
  - contains message
- **Send info for MT SMS**
  - Where to page

# Delivery to a pager: time-out



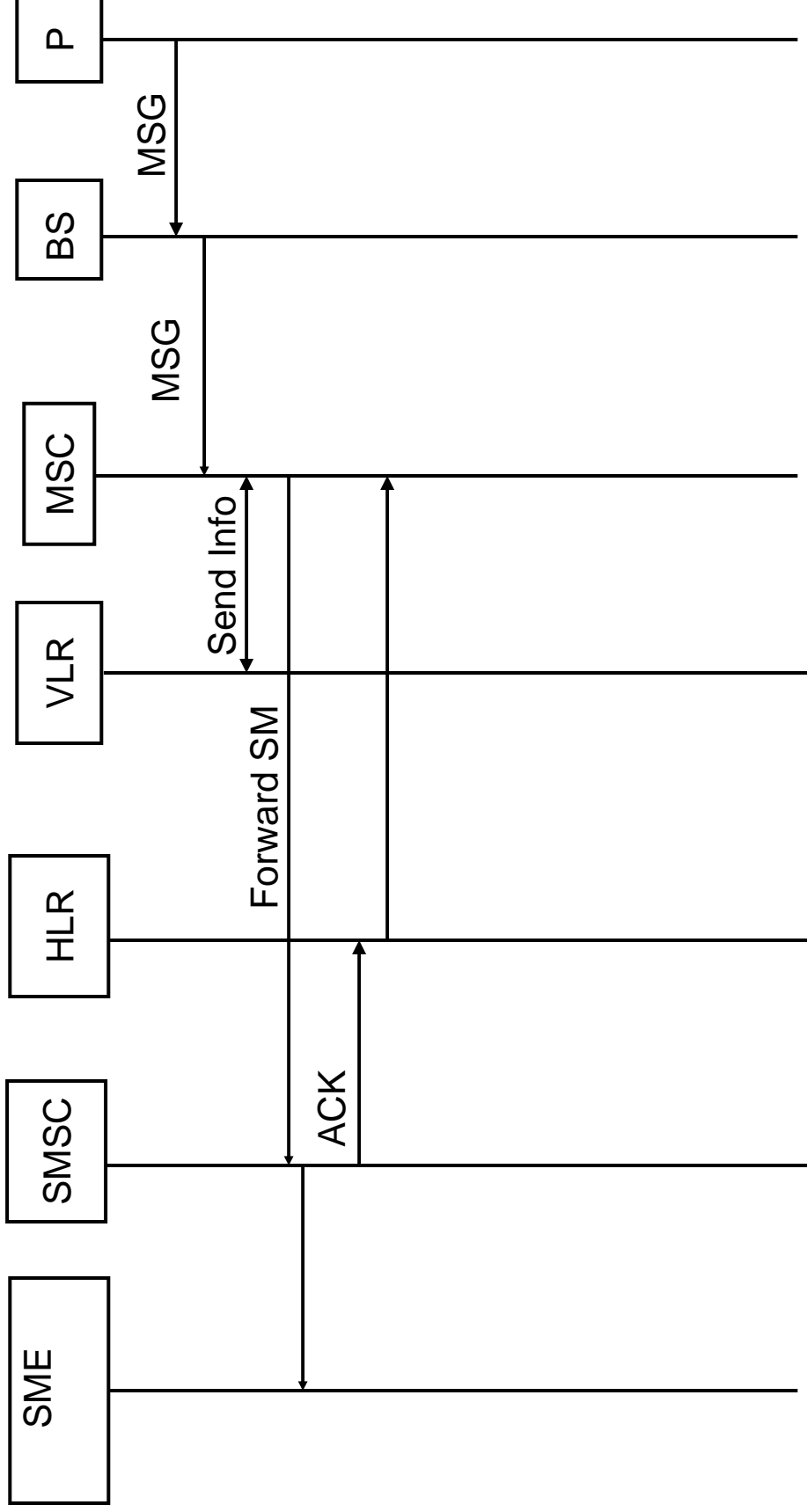
- SMSC sets a flag

# Delivery to a pager: time-out



- Alert SC  
- tells SMSC of change in status

# Delivery from a pager



- **Send Info**  
- which SMSC
- **Forward SM**  
- contains message