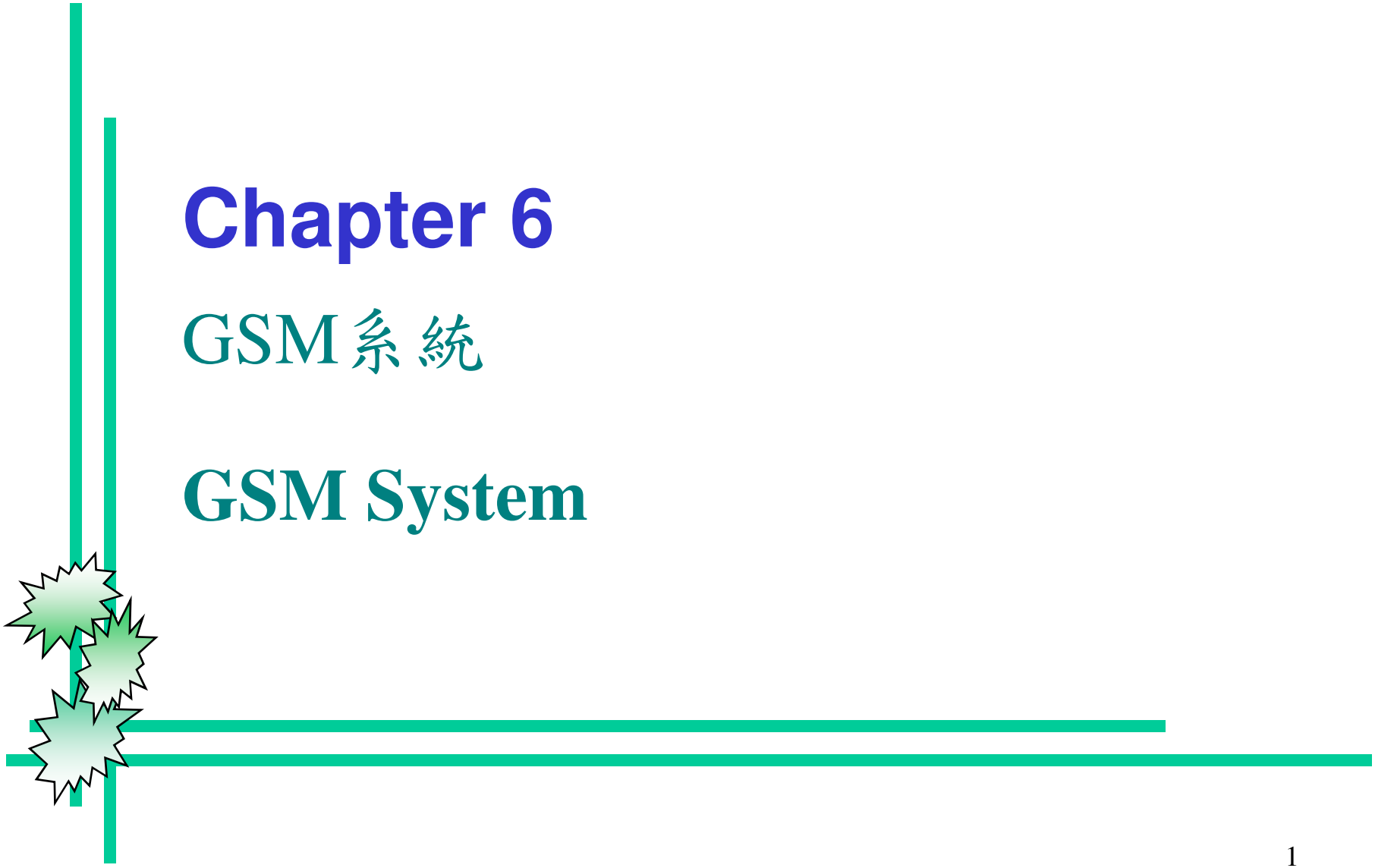


Chapter 6

GSM系統

GSM System

課程目標

- GSM全名為Global System for Mobile Communication，原稱為Group Special Mobile，在台灣被稱為泛歐式數位行動電話系統，是全球佔有率最大的第二代蜂巢式行動通訊系統。在這一章中將說明GSM系統的架構與運作方式，包括GSM的無線電介面，建立電話與交遞的流程，認證與加解密等基本議題。了解GSM的架構，才比較容易進入GPRS、UMTS等先進系統的領域。

章節目錄

- GSM現況介紹
- GSM系統架構
- GSM無線電介面
- GSM行動管理
- 安全性考量
- GSM功能性平面
- 簡訊系統
- 結語
- 作業

Section 6.1

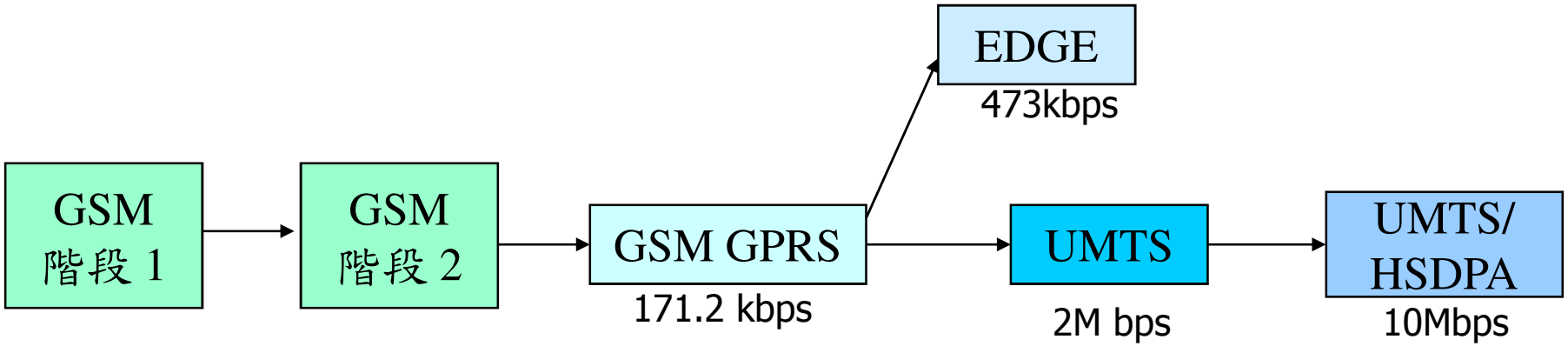
GSM 現況介紹

GSM Overview

GSM

- Global System for Mobile Communication
- 原稱為Group Special Mobile
- 在台灣被稱為泛歐式數位行動電話系統
- 由歐洲電信標準協會（European Telecommunications Standard Institute，ETSI）所制定，是一個全歐洲共同的通訊系統結構，解決歐洲各類比系統間不相容的問題。
- 1999年後改由3GPP（the 3rd Generation Partnership Project）負責後續維護與制定
- 廣泛用於全世界

圖 6-1 GSM 演進


GSM
階段 1
GSM
階段 2
GSM GPRS
171.2 kbps
EDGE
473kbps
UMTS
2M bps
UMTS/
HSDPA
10Mbps

GSM 的各個階段 (1/2)

- GSM 階段1：提供電路式交換的傳輸（circuit-switched transmission）
- GSM 階段2：增加簡訊服務（Short Message Service，SMS）和承載服務（bearer service）
- GSM+
  - 高速電路交換數據（High Speed Circuit Switched Data，HSCSD）：使用電路式交換的方式傳送數據資料，最高可達115.2kbps。
  - 一般封包式無線電服務（General Packet Radio Service，GPRS）：採用分封交換傳輸（packet-switched transmission）方式，最大171.2kbps。

GSM 的各個階段 (2/2)

- GSM++：EDGE（Enhanced Data rates for GSM Evolution）
  - 利用調變技術與編碼方式來提高傳輸速率，最高傳送速度可達384kbps。
- 3G：通用行動通訊系統（Universal Mobile Telecommunications System，UMTS）
  - 使用WCDMA（Wideband CDMA）技術
  - 提供品質保證（Quality of Service，QoS）
  - 高速下行封包存取（High Speed Downlink Packet Access，HSDPA）
    - ✓增加UMTS下載封包的傳輸速度

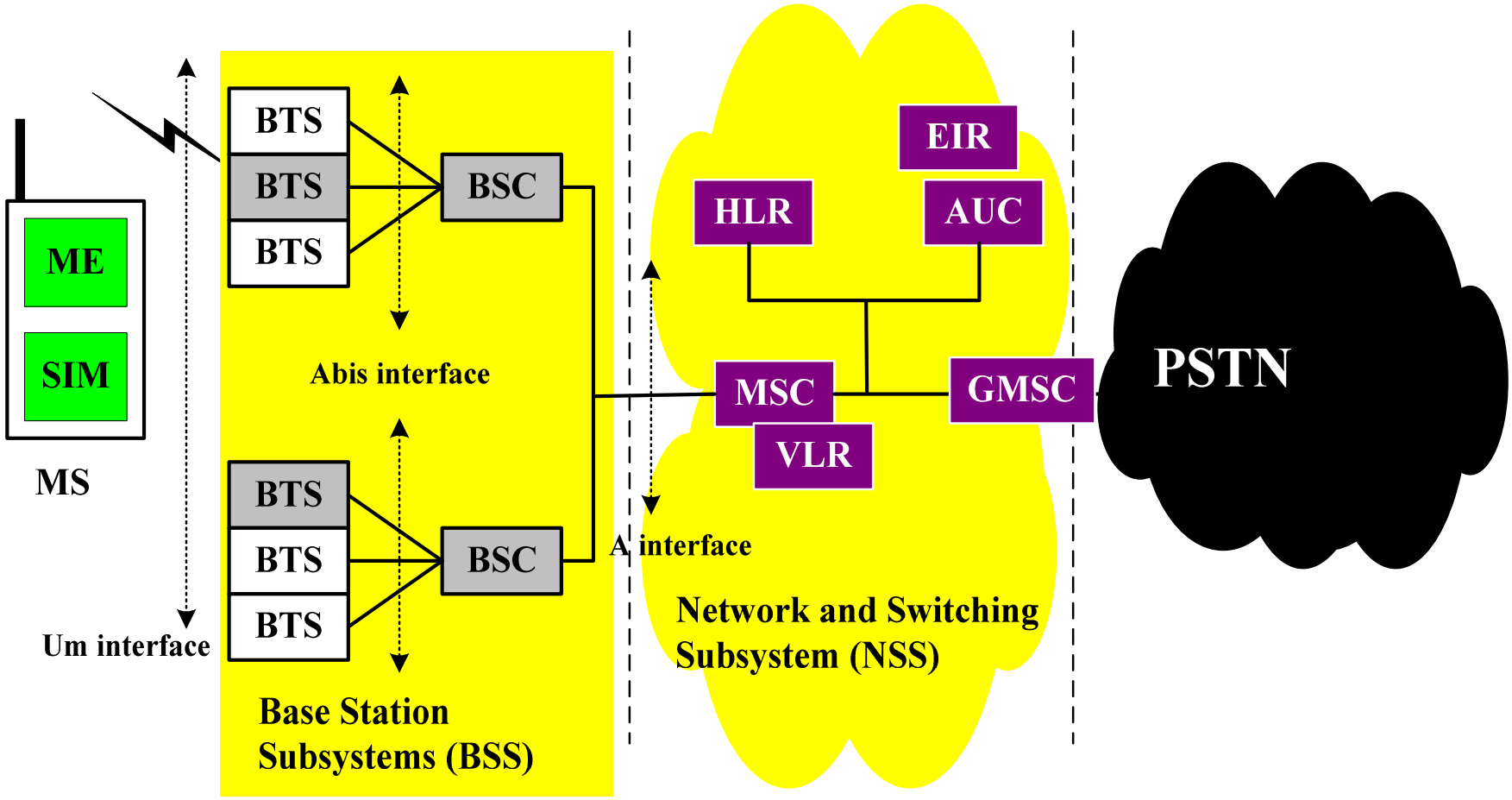
Section 6.2

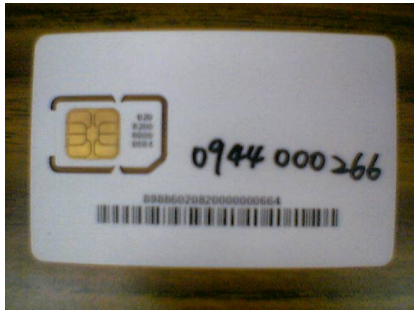
GSM 系統架構
GSM Architecture

GSM 網路的組成

- 手機（Mobile Station，MS）
- 基地台子系統（Base Station Subsystem，BSS）
- 網路及交換子系統（Network and Switch Subsystem，NSS）
- 網路營運子系統（Operation Subsystem，OSS）
  - 負責監控整體網路的運作
- 溝通介面（interface）的制定，做為資料傳遞或控制信令傳達的準則。

圖 6-2 GSM 系統架構圖





手機

- 用戶識別模組（Subscriber Identity Module，SIM）
  - 含有記憶體晶片的智慧卡
  - 認證加密所需的安全程序演算法與相關的參數
  - 儲存用戶基本資料、服務提供者的資料、手機位置、電話號碼、簡訊
- 手機通訊模組（Mobile Equipment，ME）
  - 包括與基地台通訊所需之無線軟硬體，例如控制模組與無線電模組。

基地台子系統

- 基地收發台（Base Transceiver Station，BTS）
  - BTS透過無線電介面與MS進行資料的傳送與接收。
  - 包括發射機、接收機、與無線介面相關之訊號處理的設備。
  - 在通話過程中執行信號強度測量（signal strength measurement），BTS會將自己與MS的信號測量數據轉交給BSC。
- 基地台控制器（Base Station Controller，BSC）
  - 負責無線電通道的分配（channel assignment），決定交遞（handover）程序。

網路及交換子系統 (1/2)

- 也稱為交換系統（switching system），通常稱這裡為GSM的核心網路（core network）。
- 提供電話線路交換、客戶資料儲存及手機漫遊管理（roaming management）的功能。
- 使用SS7傳送信令。
- GSM MAP（Mobile Application Part）用於建立通話或進行註冊或認證程序。
- NSS包含以下這些元件：
  - 行動交換中心（Mobile Switching Center，MSC）執行基本的線路交換功能，負責計費的工作。

網路及交換子系統 (2/2)

- NSS包含以下這些元件：
  - GMSC（Gateway MSC）是特殊的MSC，是PCS網路與PSTN等其他網路連接的閘道。
  - 本籍註冊資料庫（Home Location Register，HLR）專門儲存訂購本系統用戶的資料。
  - 客籍註冊資料庫（Visitor Location Register，VLR）儲存移動到其負責特定區域內的用戶相關資訊。
  - 設備認證資料庫（Equipment Identity Register，EIR）紀錄手機的型態與出廠的序號。
  - 認證中心（Authentication Center，AuC）用來認證用戶SIM卡之真偽。

營運子系統

- 負責網路管理與設備的維護。
  - 監控系統的負荷、電話的阻塞率（blocking rate）、兩個細胞間交遞的次數
  - 設備要能自我測試，以及自動備份（redundancy）的功能。
- 用戶管理（subscriber management）
  - 管理用戶的資料與電話計費（call charging），轉成真正的帳單。

Section 6.3

GSM 無線電介面
GSM Radio Interface

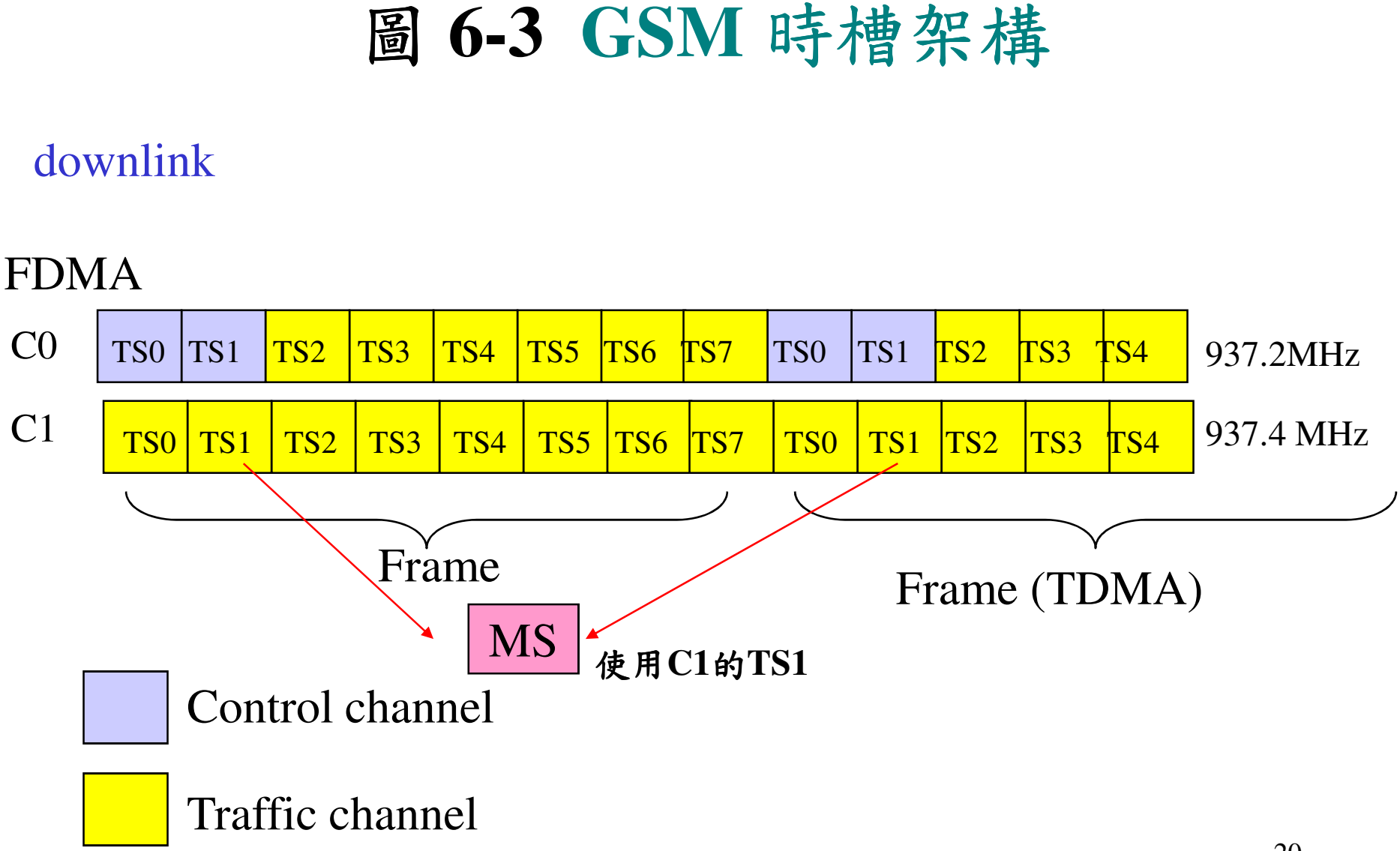
無線電介面 (1/2)

- 採用GMSK（ GPRS/GSM coding Gaussian Modular Shift Keymodulation）、13kbps RPE-LTP full-rate和5.6kbps VSELP的編碼方式。
- 分頻多工（Frequency Division Duplex，FDD）
  - 上行或上鏈路（uplink）： 890-915 MHz
  - 下行或下鏈路（downlink）： 935-960 MHz
- 相臨的頻道間距為200 KHz
- 共分成124對的頻道

無線電介面 (2/2)

- 分頻多重存取（Time Division Multiple Access，TDMA）的技術。
  - 先切成每個4.615msec的訊框（frame），每一個GSM訊框都會有一個編號，稱為訊框號碼（frame number）。
  - 訊框再切成長為0.577msec的8個時槽（timeslot），做為獨立傳送資料的基本單位。
  - 週期性出現的時槽，就稱為一個通道（channel）。

圖 6-3 GSM 時槽架構


downlink
FDMA
C0
TS0 TS1 TS2 TS3 TS4 TS5 TS6 TS7 TS0 TS1 TS2 TS3 TS4
937.2MHz
C1
TS0 TS1 TS2 TS3 TS4 TS5 TS6 TS7 TS0 TS1 TS2 TS3 TS4
937.4 MHz
Frame
Frame (TDMA)
MS
使用C1的TS1
Control channel
Traffic channel

DCS 1800

- 以GSM標準架構為基礎
- 使用1710-1785 MHz（uplink）與1805-1880 MHz（downlink）頻段的標準，稱為DCS 1800（Digital Cellular Standard 1800）或GSM1800。
- 美國使用1900MHz頻段的GSM系統，就被稱為DCS1900或GSM1900。
- 整合GSM與DCS1800可形成微細胞/巨細胞（microcell/macrocell）的架構。

GSM 的資料結構

- 透過GSM傳送的資料都是以burst的型式加以封裝，再將資料放入時槽中傳送。
- 時槽內容包括burst與guard time。
- Burst的種類：
  - Normal burst用於傳送使用者語音或數據資料。
  - F burst放置基地台廣播的信號，讓MS校正頻率，以維持與基地台頻率上的同步。
  - S burst放置基地台廣播的信號，讓MS校正時間，以維持與基地台時間上的同步。
  - A burst是當手機想要打電話時，上傳A burst告知基地台欲使用無線電資源。

圖 6-4 Normal Burst

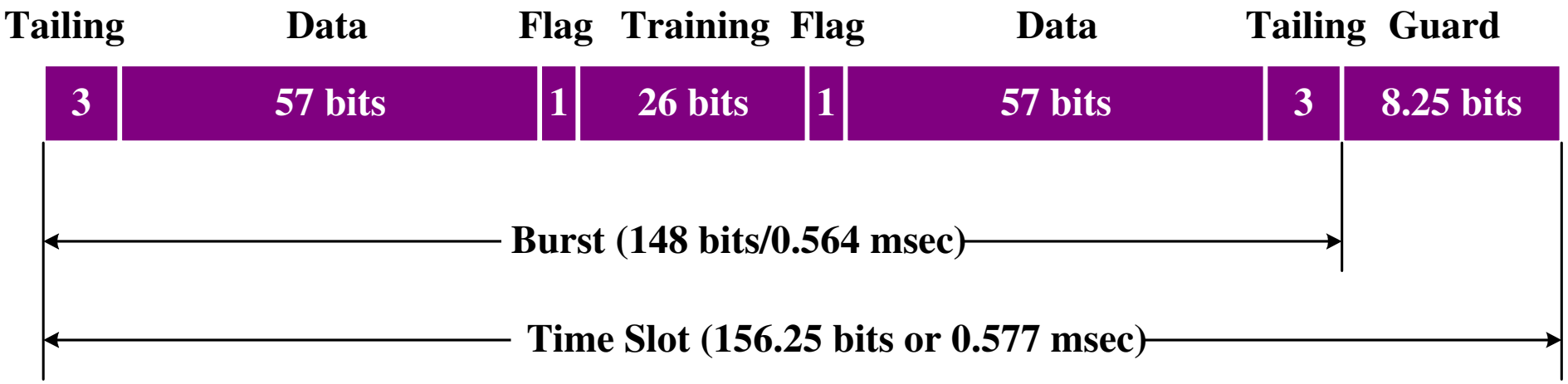
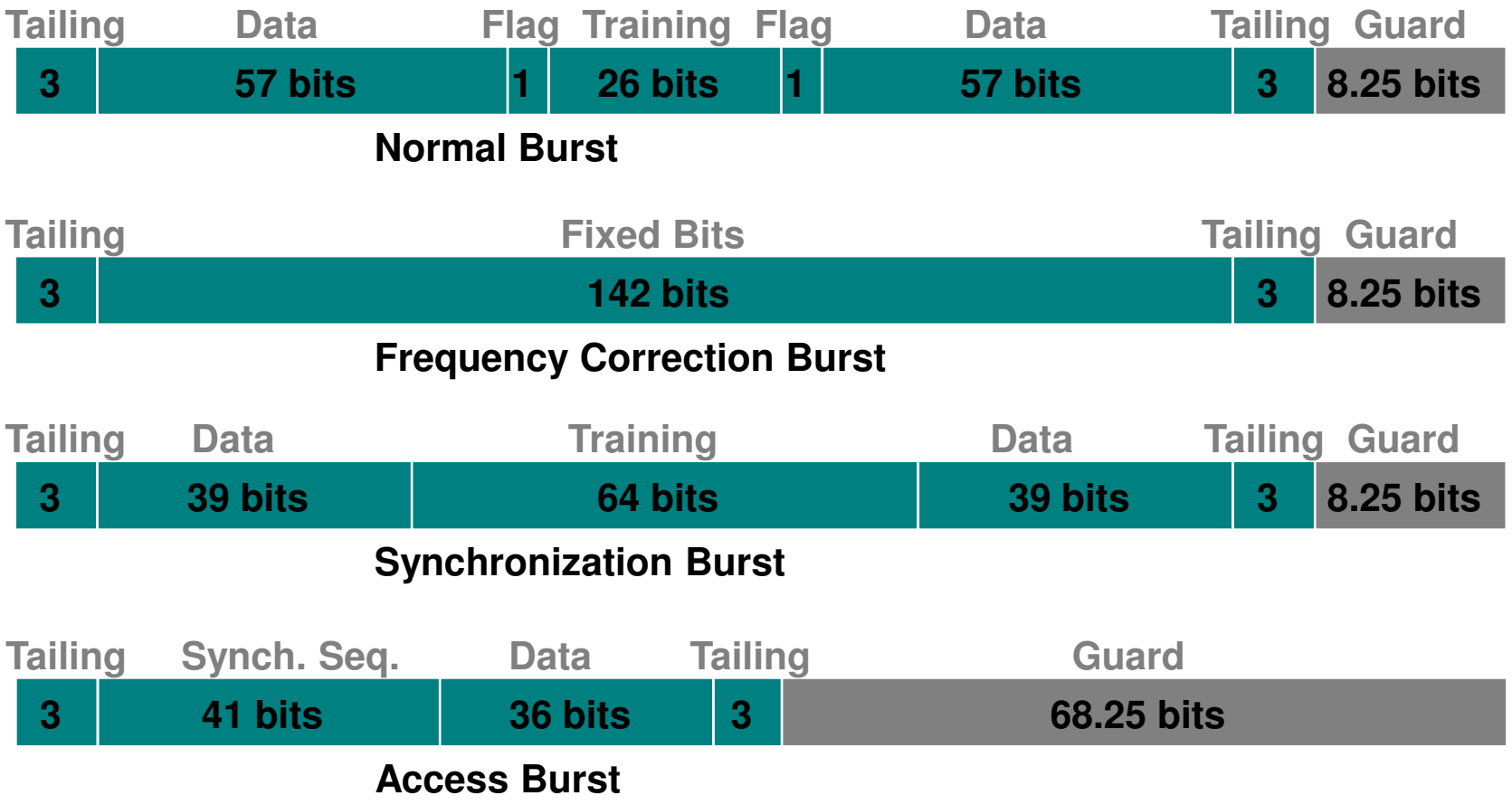


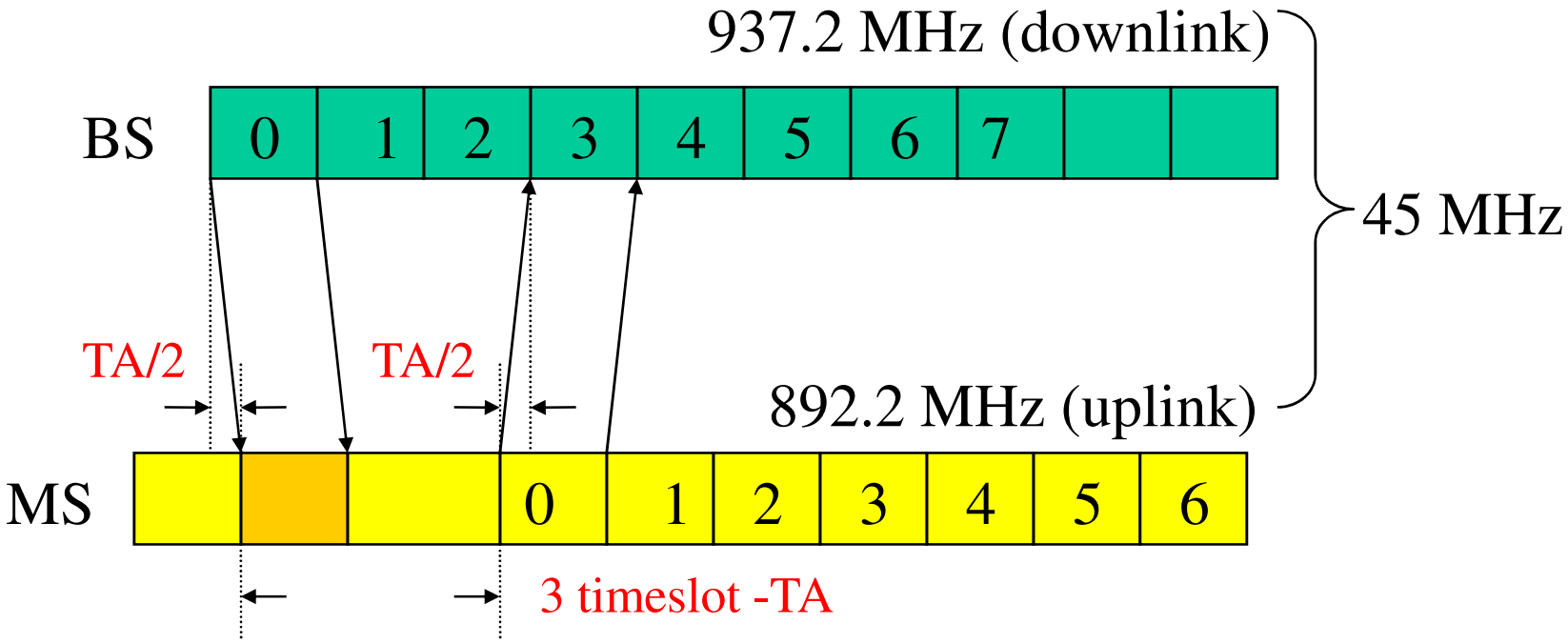
圖 6-5 GSM Bursts



提前時序（Time Advance，TA)

- 若BTS下傳給MS使用第一個時槽，則BTS會在第三個時槽收到MS送出上傳的burst。
- 訊號傳遞會發生延遲
  - BTS發送的訊號傳到MS所需要的時間，加上MS發送訊號讓BTS接收的時間，稱為往返傳播延遲（round-trip propagation delay）。
- MS的發送時刻要提前一段round trip propagation delay的時間，所以稱為Time Advance，縮寫為TA。

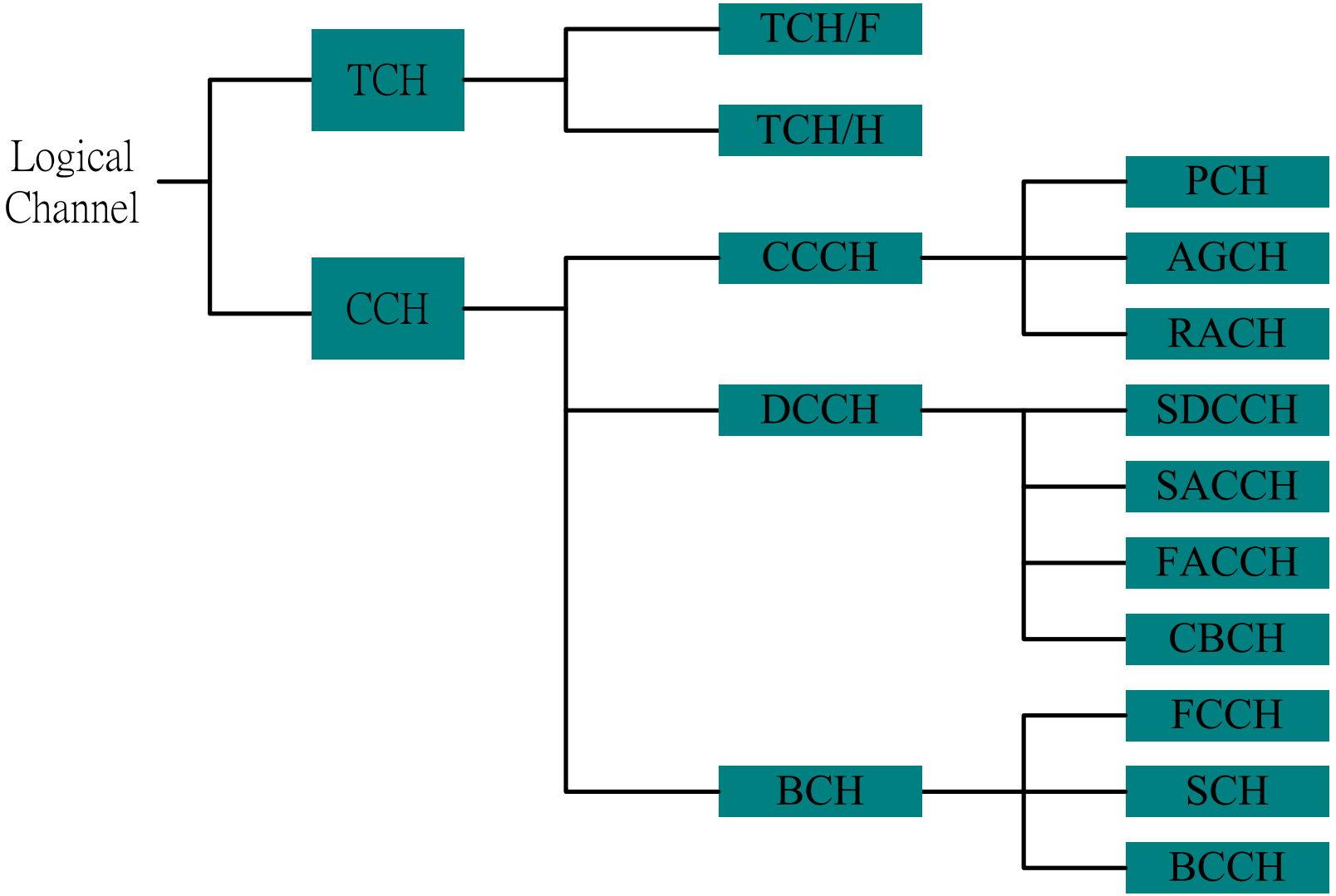
圖 6-6 Time Advance



實體通道與邏輯通道

- 實體通道（physical channel）：BTS與MS間用來傳送資訊的無線電通道
- 邏輯通道（logical channel）：依據所傳送的控制訊號的用途，或是依據使用者資料來分類將傳送的通道命名。
  - 邏輯通道與其使用的實體通道的對應關係有一定的規則。
  - 分成訊務通道（Traffic CHannel，**TCH**）與控制通道（Control CHannel，**CCH**）兩大類。
  - 參考圖 6-7。

圖 6-7 GSM 邏輯通道


Logical Channel
TCH
TCH/F
TCH/H
CCH
CCCH
PCH
AGCH
RACH
DCCH
SDCCH
SACCH
FACCH
CBCH
BCH
FCCH
SCH
BCCH

訊務通道（**Traffic CHannel，TCH**）

- 全速率訊務通道（Full rate TCH，**TCH/F**）
  - 傳送13kbps之語音或12、6、3.6kbps的數據資料。
  - 使用整個Normal Burst來傳送。
- 1/2速率訊務通道（Half rate TCH，**TCH/H**）
  - 提供7kbps語音傳輸，6或3.6kbps數位資料傳輸。
  - 只使用Normal burst中一個Data欄位來傳送資料。

控制通道（Control channel，CCH）

- 區分為三類：
  - 廣播通道（Broadcast CHannel，**BCH**）
    - ✓基地台廣播系統資訊給各手機的下行邏輯通道。
  - 共用控制通道（Common Control CHannel，**CCCH**）
    - ✓用於BTS對一群手機間信令的通訊，但是所有手機共用這些控制頻道，所以被稱為共用控制通道。
  - 專屬控制通道（Dedicated Control CHannel，**DCCH**）
    - ✓BTS分配給手機的專屬邏輯通道。

廣播通道（**Broadcast CHannel，BCH**）

- 頻率校正通道（Frequency Correction CHannel，**FCCH**）
  - 傳送F burst，提供頻率校正的資訊。
- 同步通道（Synchronization CHannel，**SCH**）：
  - 傳送S burst，讓MS取得與BTS訊框架構的同步。
- 廣播控制通道（Broadcast Control CHannel，**BCCH**）
  - 提供手機有關基地台的資料。

共用控制通道（Common Control CHannel，CCCH）

- 傳呼通道（Paging CHannel，**PCH**）
  - 當有電話打該手機時，BTS透過**PCH**呼叫手機。
- 隨機接取通道（Random Access CHannel，**RACH**）
  - 手機主動打電話時，手機在**RACH**上傳送A burst，告知基地台欲使用無線電資源。
- 接取允諾通道（Access Grant CHannel，**AGCH**）
  - 基地台透過**AGCH**告知手機可以使用的無線電通道。

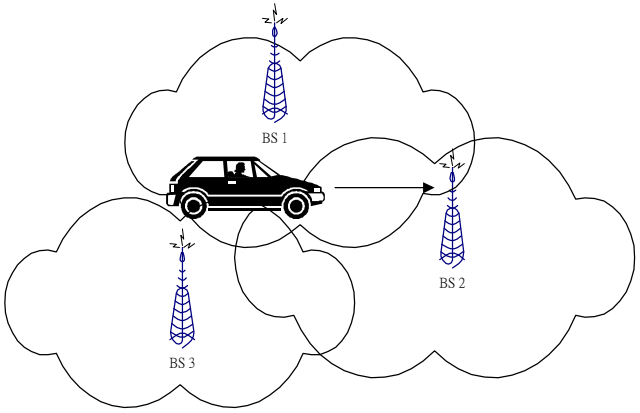
專屬控制通道（DCCH）(1/2)

- 獨立專屬控制通道（Stand along Dedicated Control CHannel，**SDCCH**）
  - 傳送建立電話的控制訊號，或使用者之簡訊。
- 慢速相關控制通道（Slow Associated Control CHannel，**SACCH**）
  - 非緊急的維運資訊，例如功率控制（power control）及時差校正（time alignment）等控制資訊，以及無線電線路訊號測量結果(measurement report)。

專屬控制通道（DCCH）(2/2)

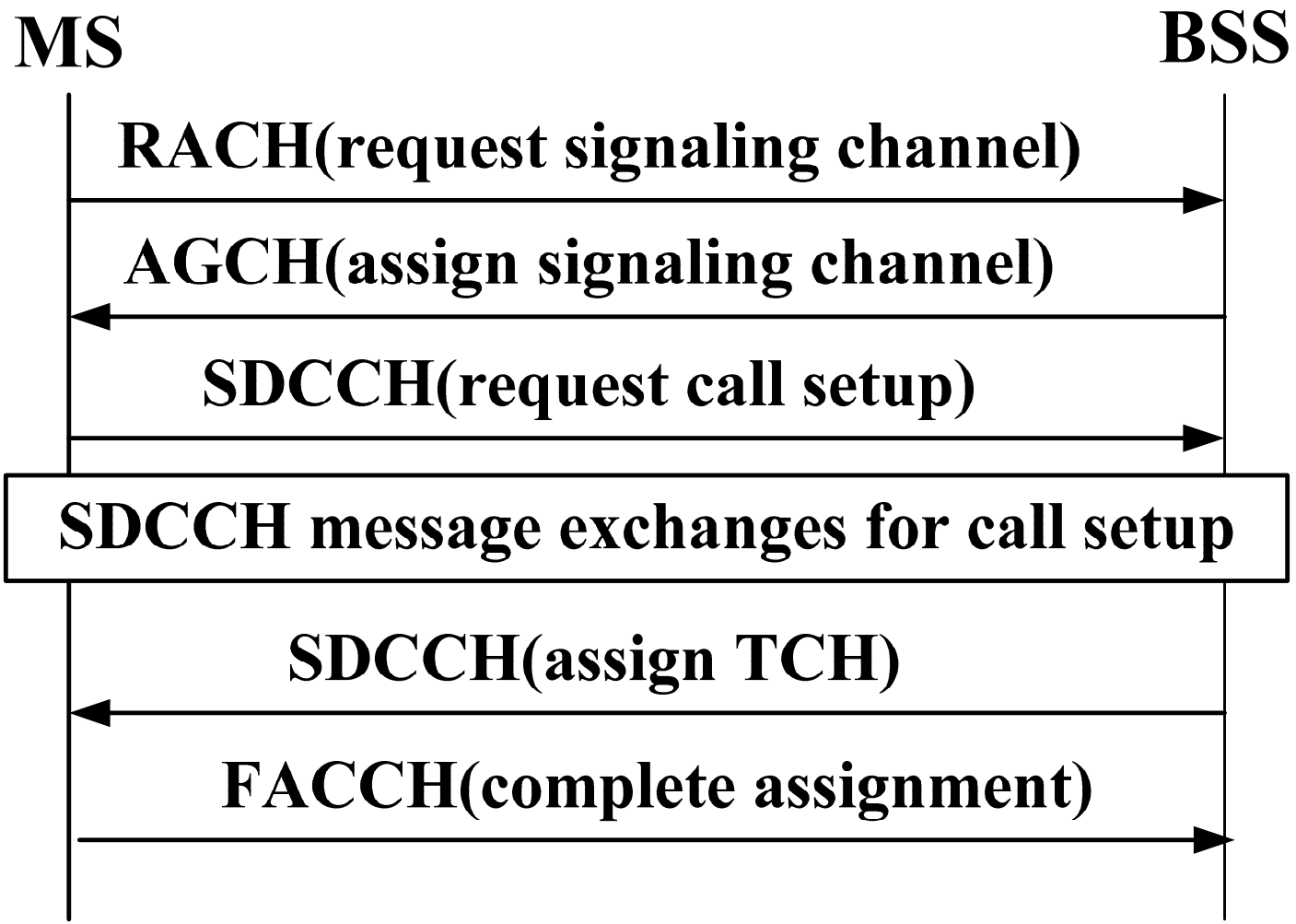
- 快速相關控制通道（Fast Associated Control CHannel，**FACCH**）
  - 傳送緊急控制信令（time-critical signaling），包括電話線路的設定、手機認證（authentication）以及交遞（handover）的信號。
  - **FACCH**佔用訊務通道的時槽。
- 細胞廣播通道（Cell Broadcast CHannel，**CBCH**）
  - 提供簡訊的廣播服務（short message service cell broadcast messages）。

手機註冊

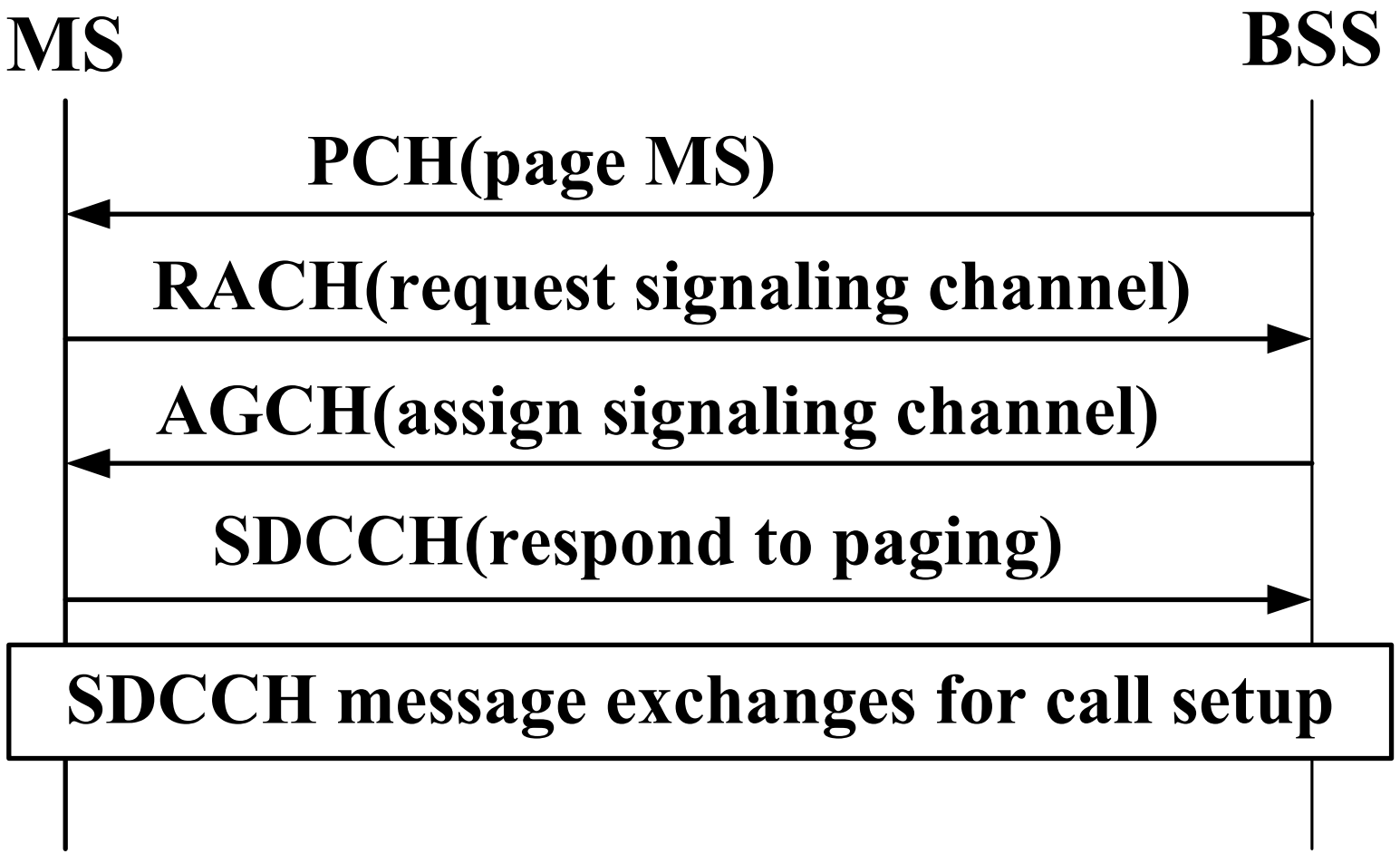


- 當MS開機後，會掃瞄屬於GSM的全部頻道。
- MS會找出訊號最強的頻道，判斷是否為承載 **BCCH** 的控制頻道。
- MS會利用 **FCCH** 校正自己的頻率以便與BTS的頻率同步。
- 由 **SCH** 可得到基地台的編號（BSIC）。
- 從 **BCCH** 則可得到細胞的編號，判斷是否是為所屬的 PLMN 的細胞。若不是則再繼續搜尋，直到找到可用的細胞為止。
- 接下來MS向MSC註冊。

手機主撥電話


MS
BSS
RACH(request signaling channel)
AGCH(assign signaling channel)
SDCCH(request call setup)
SDCCH message exchanges for call setup
SDCCH(assign TCH)
FACCH(complete assignment)

呼叫手機接電話


MS
BSS
PCH(page MS)
RACH(request signaling channel)
AGCH(assign signaling channel)
SDCCH(respond to paging)
SDCCH message exchanges for call setup

Section 6.4
GSM 行動管理
GSM Mobility Management

GSM 行動管理

- 這節要說明
  - 位置區域
  - 識別號碼
  - 兩層式的資料庫
  - 手機的位置追蹤
  - 電話設定的流程
    - ✓發話程序（Call Origination Procedure）：手機主動打電話
    - ✓受話程序（Call Termination Procedure）：手機被動被呼
  - 交遞程序

識別號碼

- GSM系統中和手機相關的識別號碼：
  - Mobile system ISDN (MSISDN)
  - Mobile Station Roaming Number (MSRN)
  - International Mobile Subscriber Identity (IMSI)
  - Temporary Mobile Subscriber Identity (TMSI)
  - International Mobile station Equipment Identity (IMEI)

MSISDN

- Mobile System ISDN
  - MSISDN uses the same format as the ISDN address (based on ITU-T Recommendation E.164).
  - HLR uses MSISDN to provide routing instructions to other components in order to reach the subscriber.

Total up to 15 digits

Country code (CC)	National destination code (NDC)	Subscriber number (SN)

MSRN

- Mobile Station Roaming Number
- The routing address to route the call to the MS through the visited MSC.
  - MSRN=CC+NDC+SN

IMSI

- International Mobile Subscriber Identity
  - Each mobile unit is identified uniquely with an IMSI.
  - IMSI includes the country, mobile network, mobile subscriber.
  - Total up to 15 digits

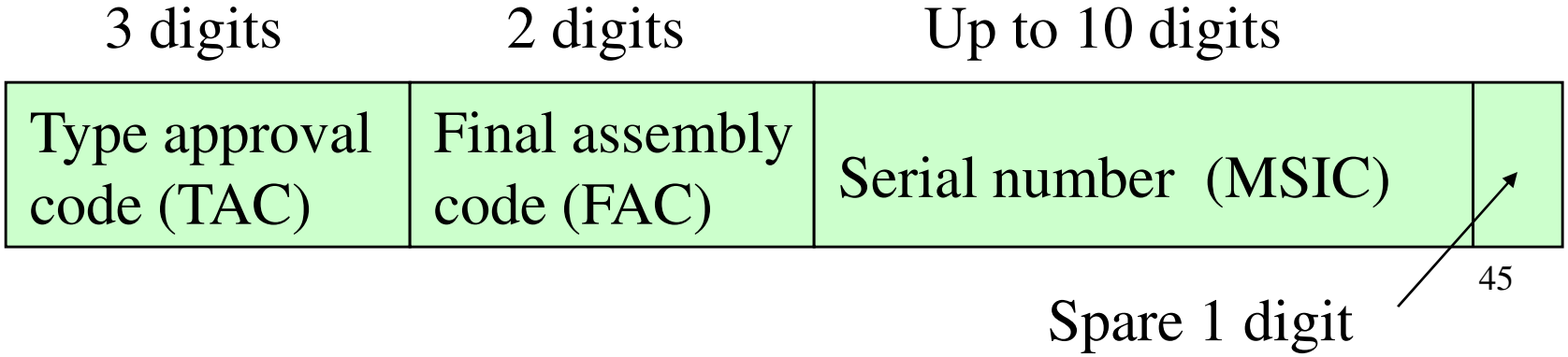
3 digits	1- 2 digits	Up to 10 digits
Mobile country code (MCC)	Mobile network code (MNC)	Mobile subscriber identification code (MSIC)

TMSI

- Temporary Mobile Subscriber Identify
  - TMSI is an alias used in place of the IMSI.
  - This value is sent over the air interface in place of the IMSI for purposes of security.

IMEI

- International Mobile Station Equipment Identity
  - IMEI is assigned to the GSM at the factory.
  - When a GSM component passes conformance and interoperability tests, it is given a TAC.
  - Up to 15 digits



LAI

- Location Area Identity
  - LAI identifies a location area (LA).
  - When an MS roams into another cell, if it is in the same LAI, no information is exchanged.
  - Total up to 15 digits

3 digits	1-2 digits	Up to 10 digits
Mobile country code (MCC)	Mobile network code (MNC)	Location area code (LAC)

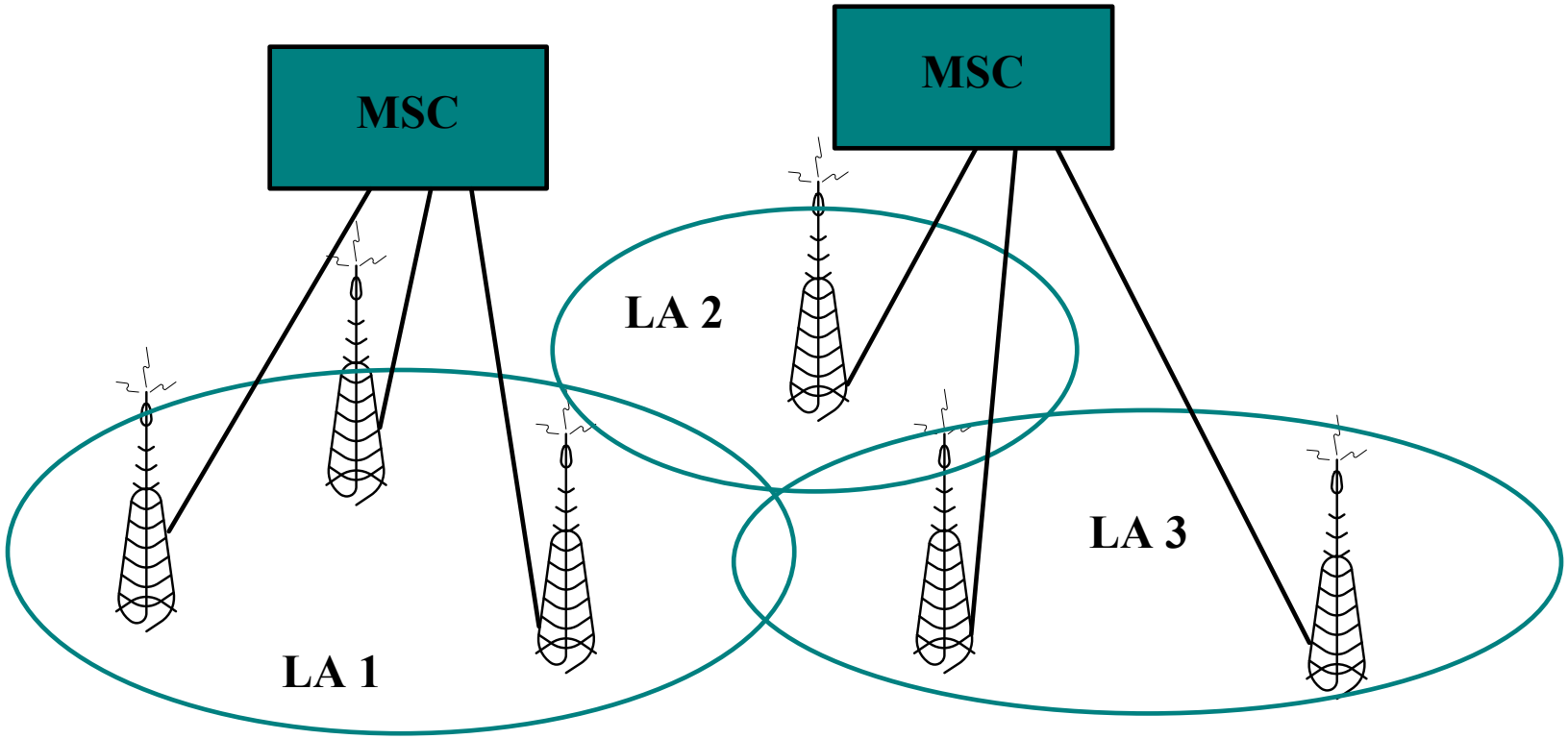
CGI

- Cell Global Identity
- CGI = LAI + CI

  = MCC + MNC + LAC + CI

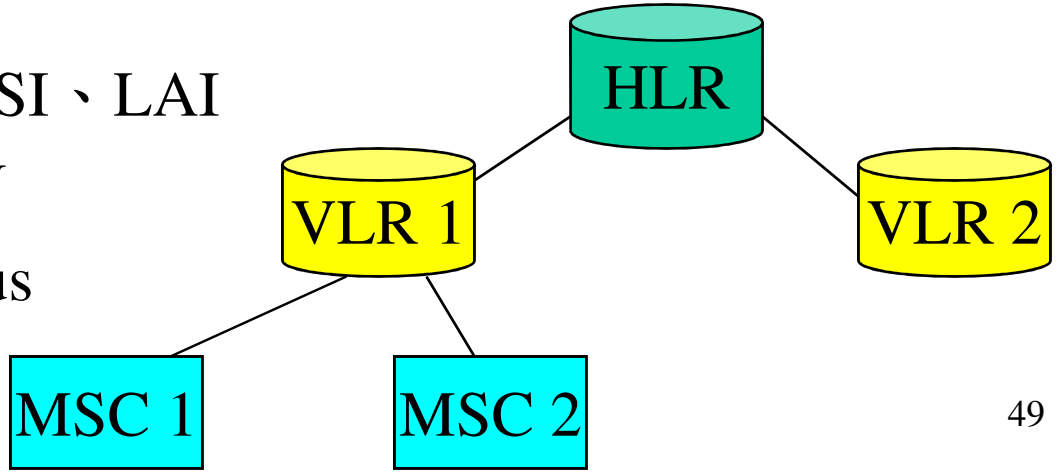
  - CI : Cell Identity

圖 6-8 位置區域示意圖



兩層式的資料庫

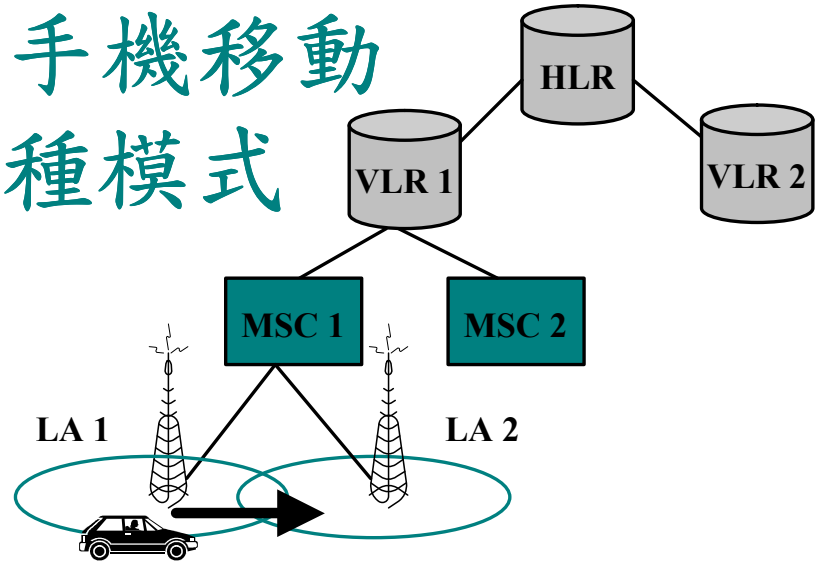
- 本籍註冊資料庫（Home Location Register，HLR）
  - MSISDN、IMSI、VLR ISDN、MSC ISDN與subscriber status
- 客籍註冊資料庫（Visitor Location Register，VLR）
  - MSISDN、IMSI、LAI
  - TMSI、MSRN
  - subscriber status



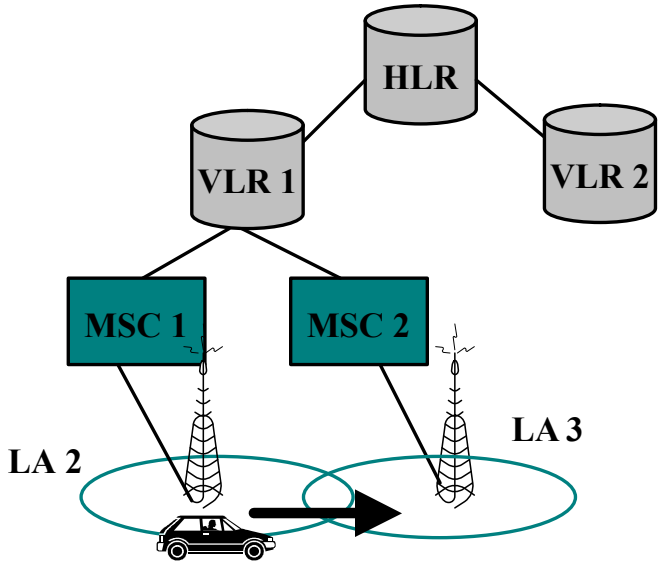
註冊程序

- 當MS在待機狀況且四處漫遊時，若發現鄰近BTS之訊號強度較佳時：
  - 新的BTS與舊的BTS有相同的LAI，不會做任何註冊的動作，只要保持與新BTS的**BCH**的同步。
  - 新的BTS與舊的BTS有不同的LAI，MS通知VLR進行註冊的動作。

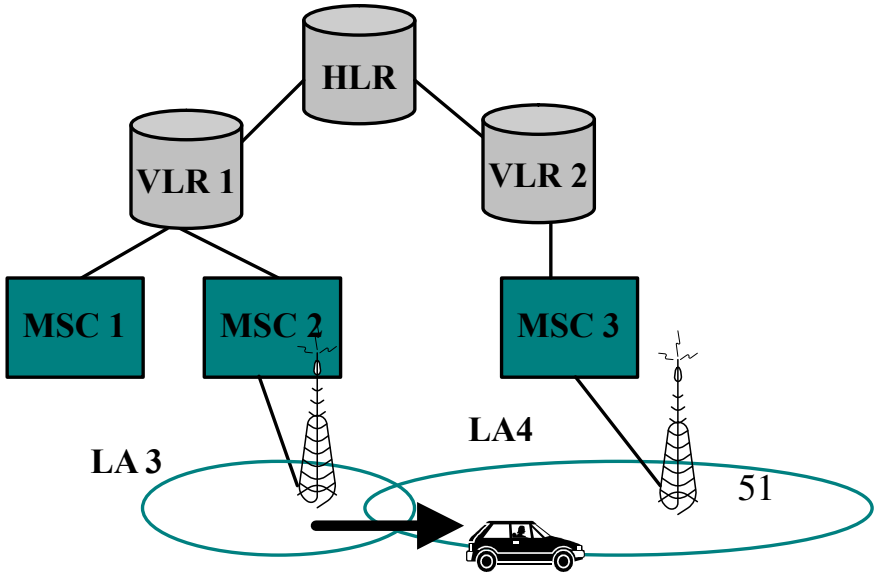
圖 6-9 手機移動的三種模式



(a) Inter-LA movement



(b) Inter-MSC movement



(c) Inter-VLR movement

圖 6-10 Inter-LA 的註冊流程

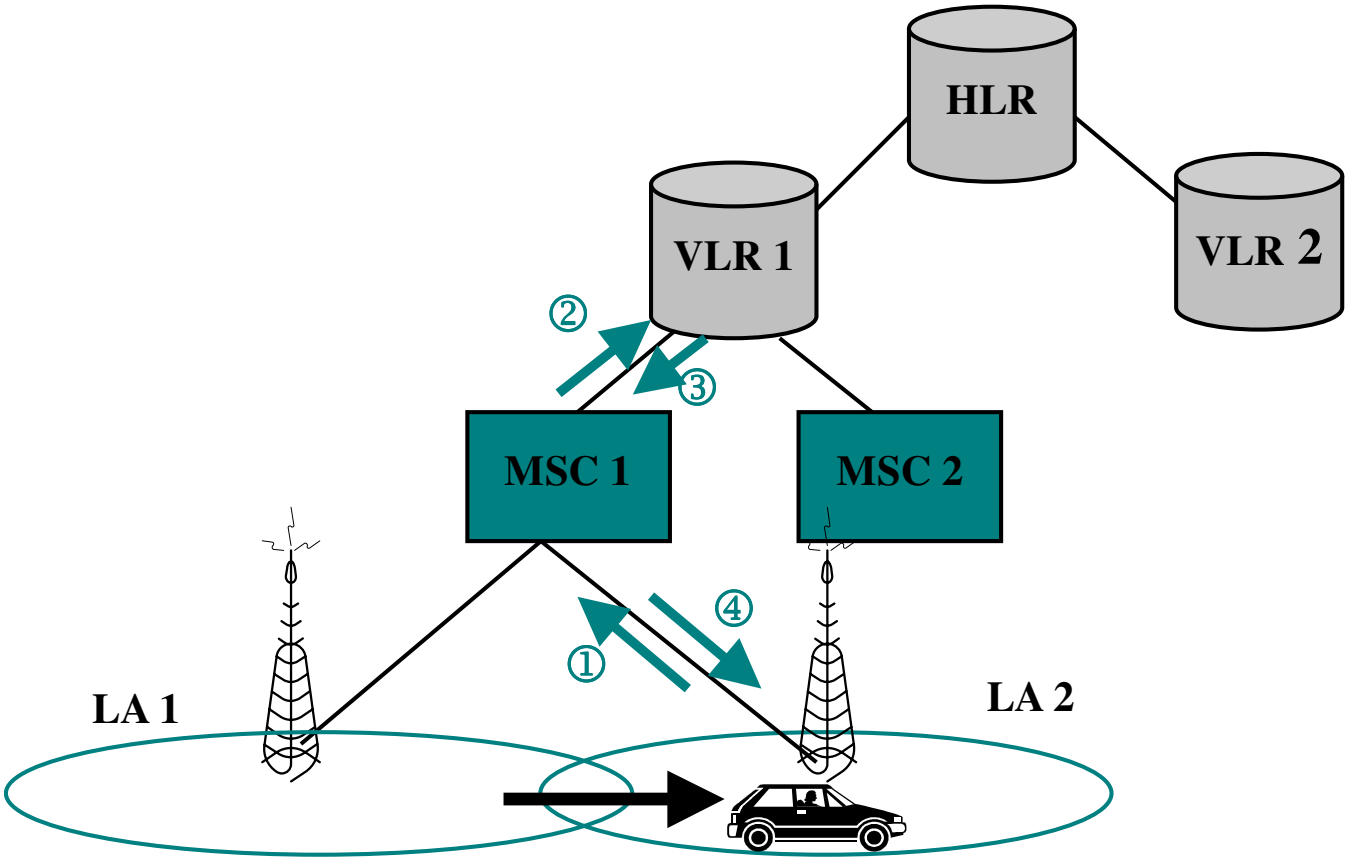
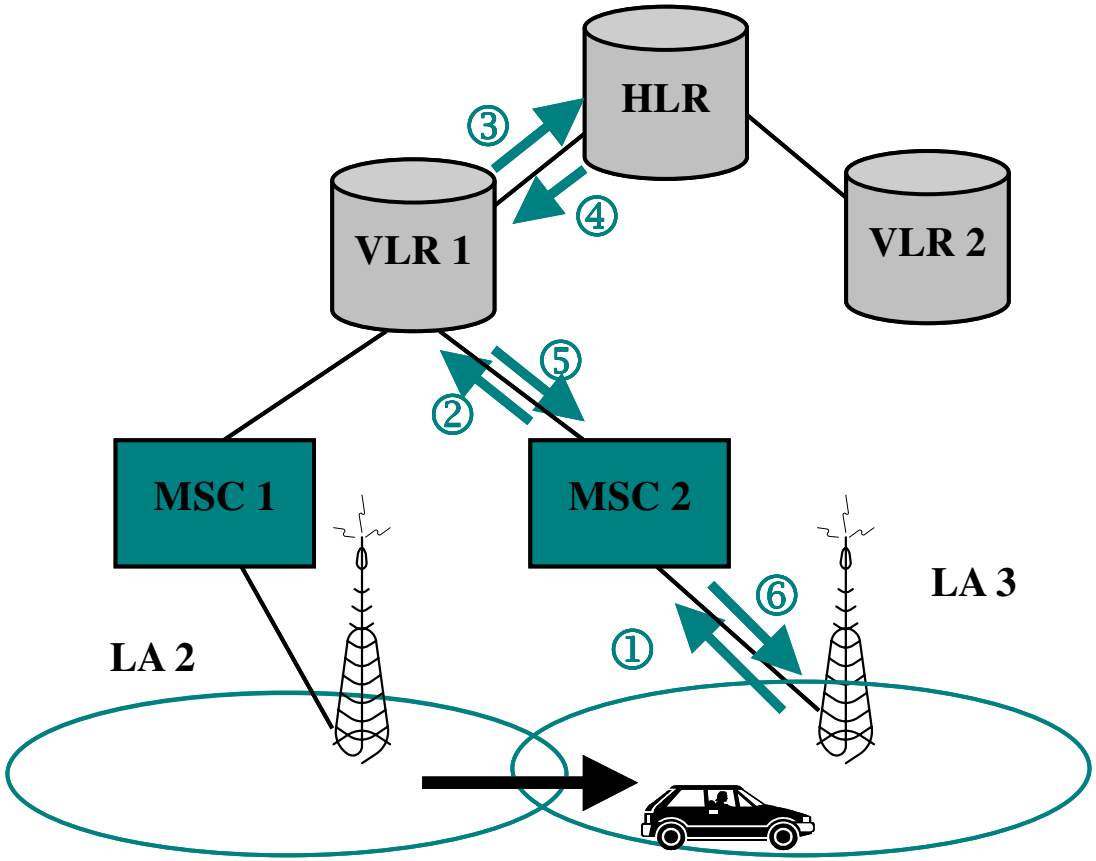
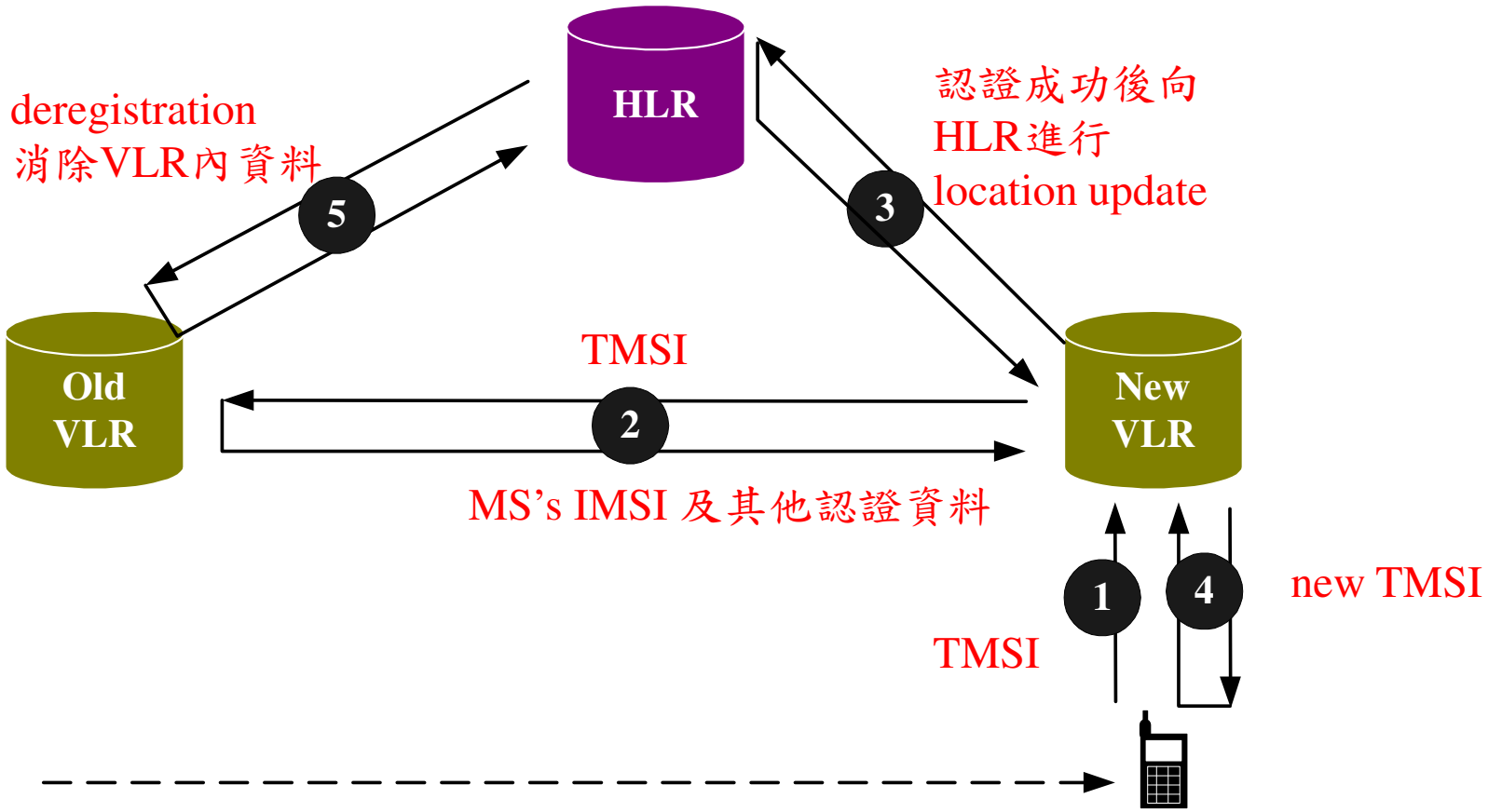


圖 6-11 Inter-MSC 的註冊流程



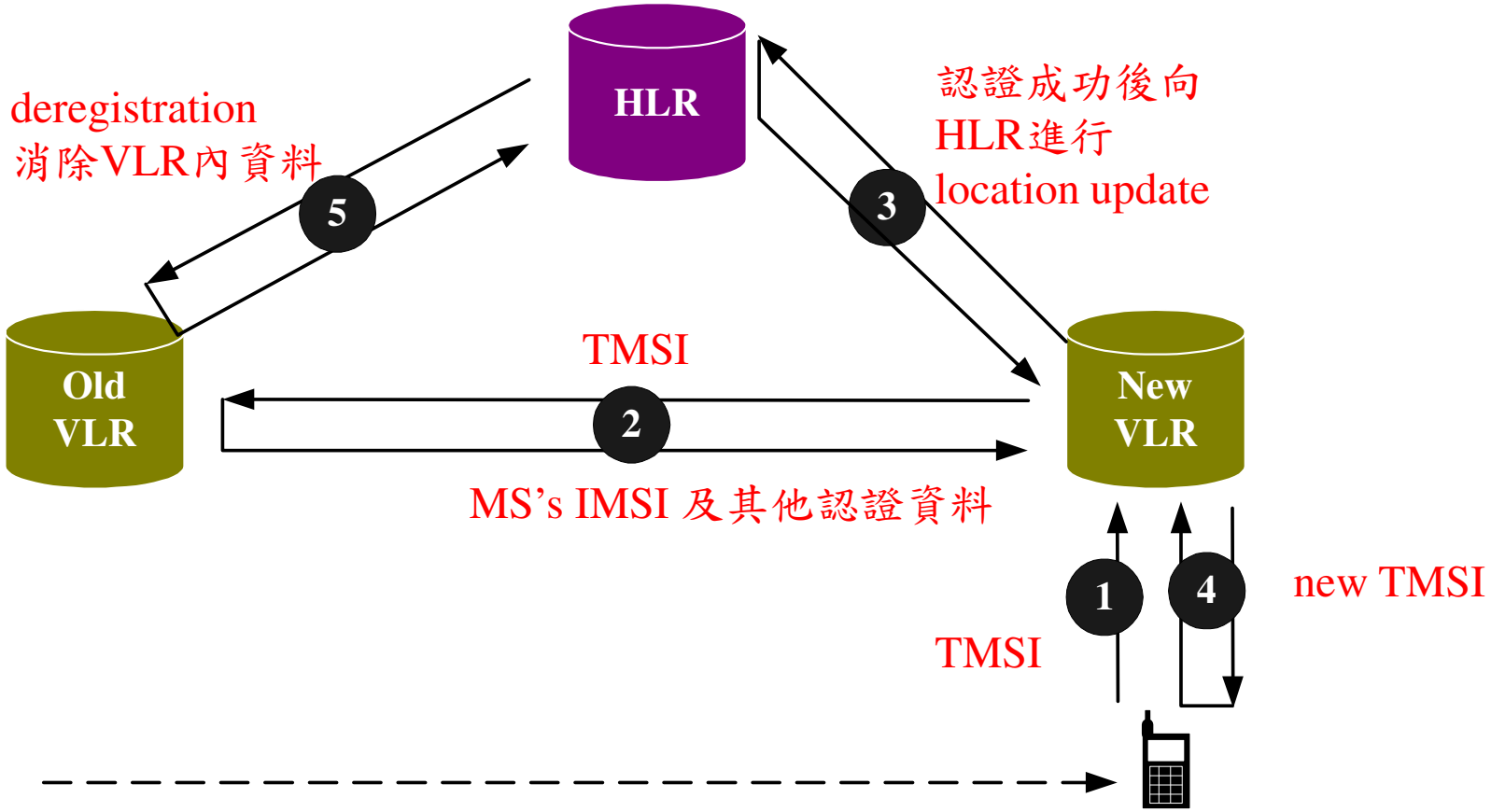


Step 1:

當手機移動至一個新的基地台的範圍，它可經由基地台的廣播控制通道（BCCH）的廣播資料(LAC, Location code)獲知是否已移動至一個新的位置區域。

若手機偵測到其位置已改變，則透過 SDCCH 通知 new VLR ，進行註冊的動作。

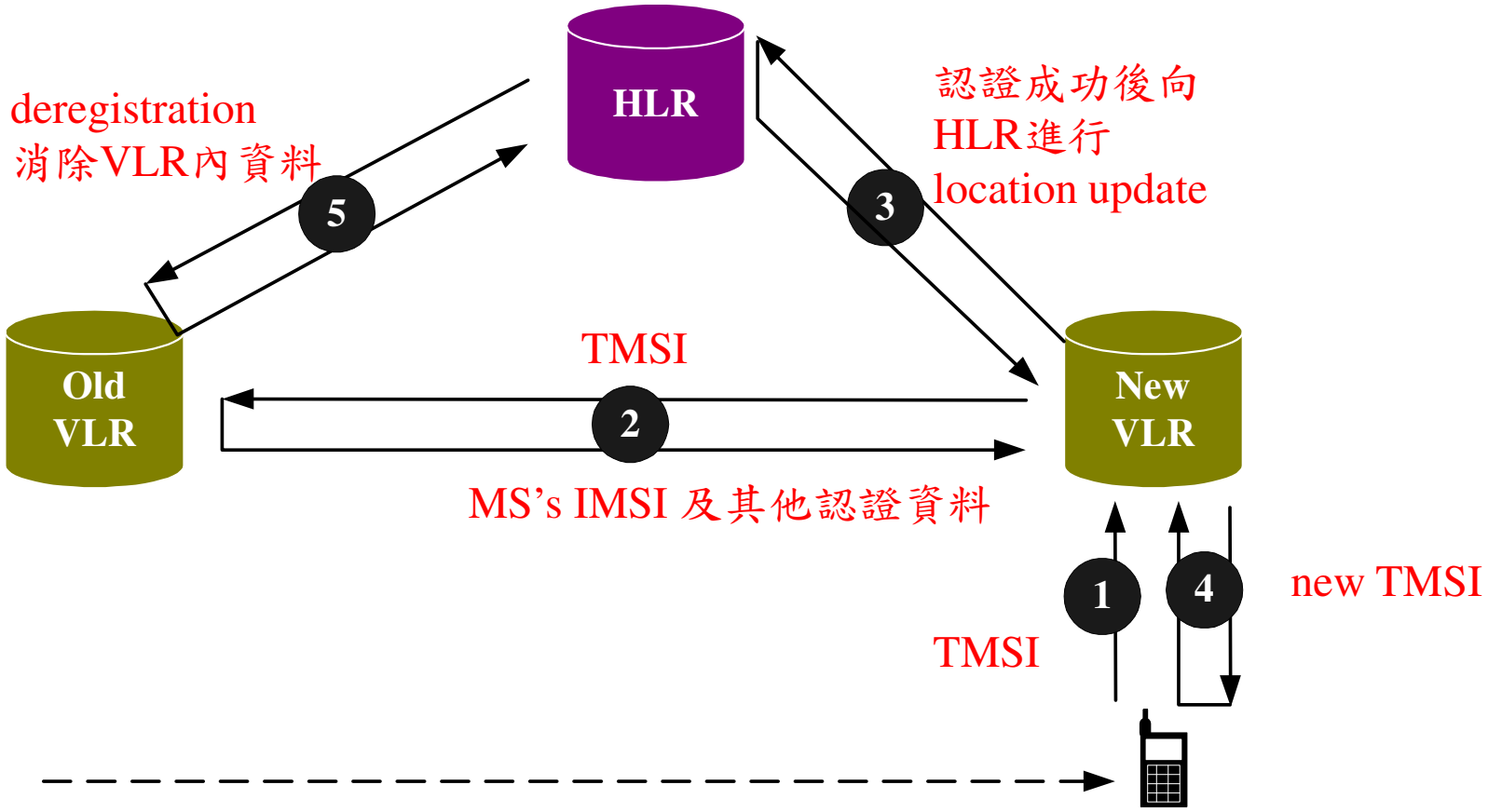
MS 將 Temporary Mobile Subscriber Identity (TMSI）及舊的VLR 住址傳送給新的VLR，進行註冊的動作。每個註冊 MS 送給 VLR 的資料都會有: MSC位址, TMSI, old LAI, target LAI 和其他相關資訊.



Step 2:

IMSI 在舊的 VLR 記錄中，因此新的 VLR 根據手機所送資料，利用公共電話網路將 TMSI 碼送至舊的 VLR ，以索取 IMSI。

新的 VLR 進行認證（authentication）的程序，此程序將在後面詳細解釋。 利用 TMSI 方式，手機的 IMSI 只在有線公共電話網路傳送，而不會在“空中”被盜取。

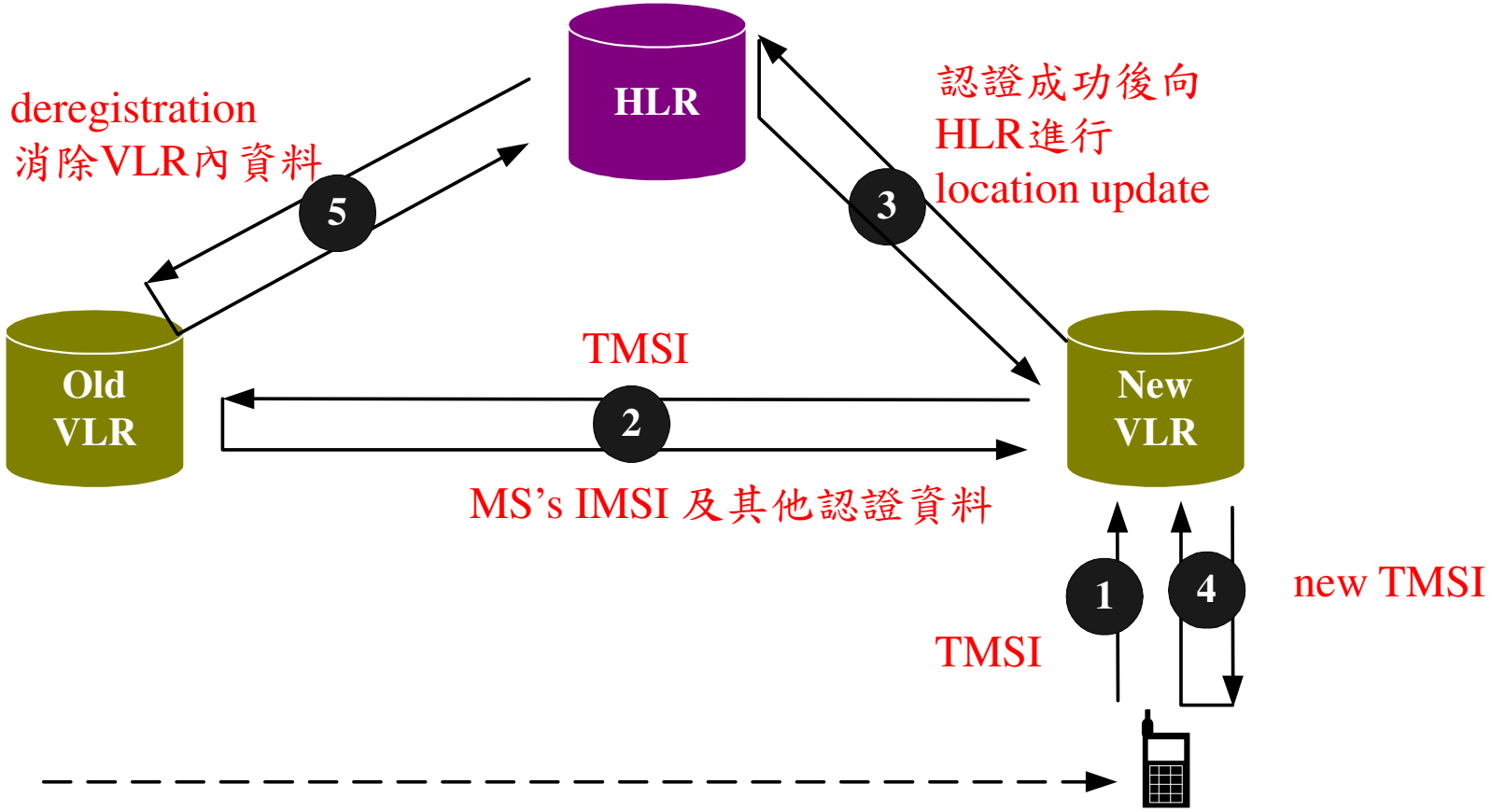


Step 3**:**

在認證完成後，新的 VLR 將手機的新位置告知 HLR 進行註冊的動作 。
VLR 是利用 IMSI 可找到 MS 的 PLMN, i.e., HLR 位址。
HLR 則將手機相關資料送回給新的VLR。

Step 4:

新的 VLR 產生一個新的 TMSI 給手機，通知手機註冊程序完成。



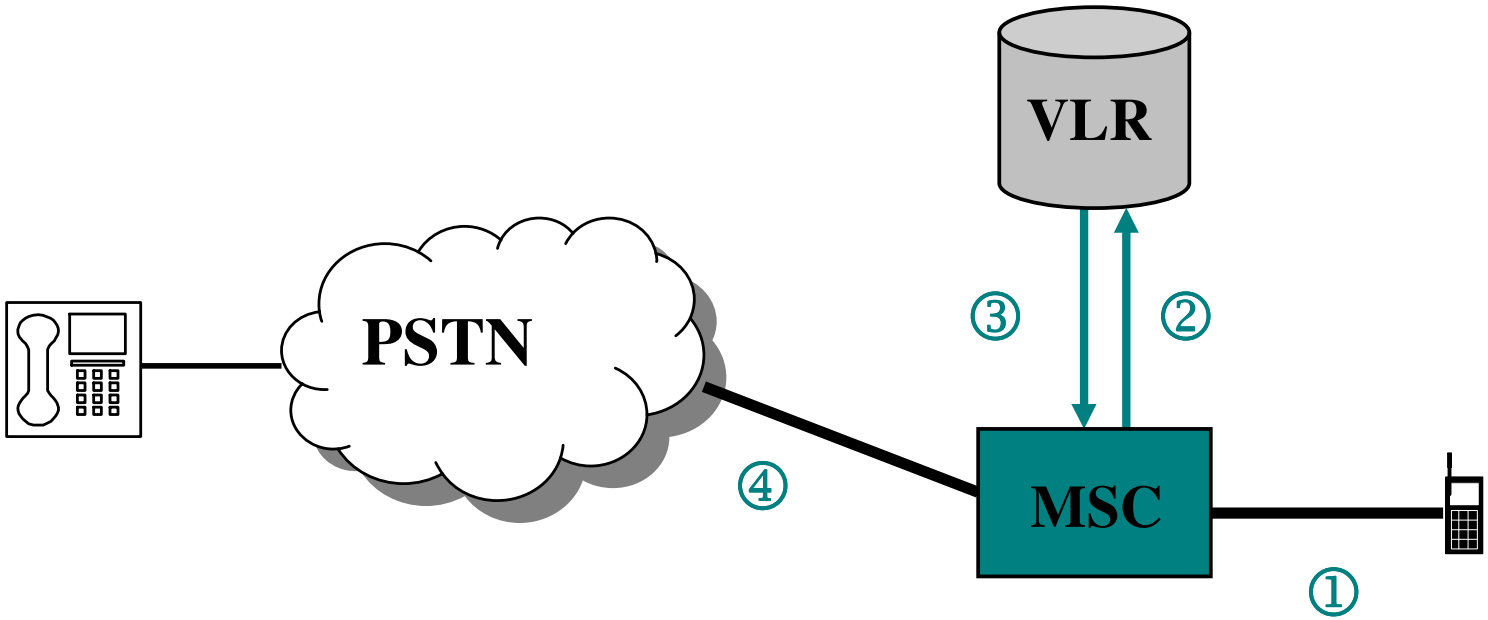
Step 5:

在步驟3後，HLR 會送一訊號至舊的VLR，要求將手機的記錄消除。
舊的 VLR 將手機的記錄消除後，則回覆執行完畢的訊息。

定期註冊（**Periodical Registration**）

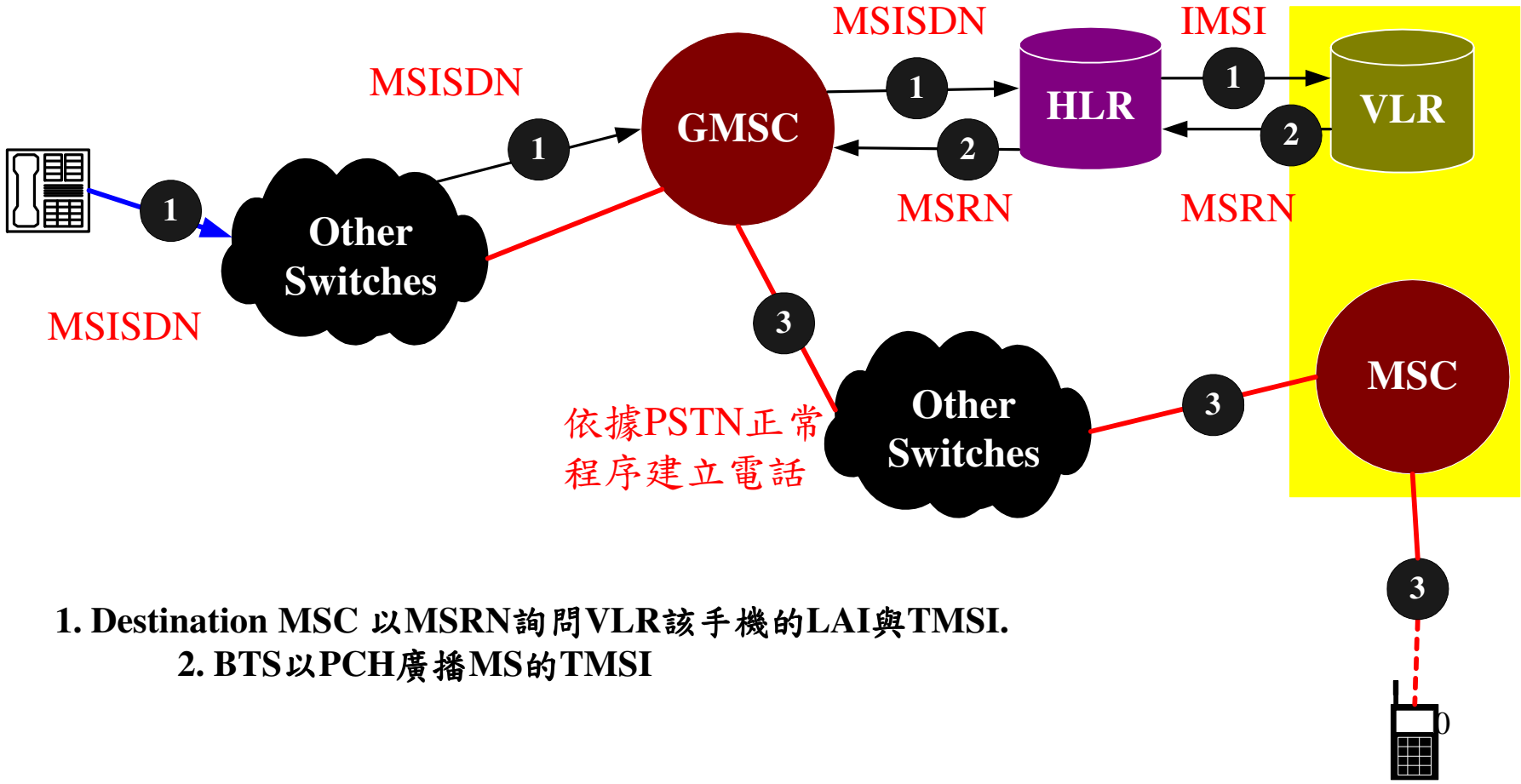
- MS 在 roaming 時，藉由註冊程序，HLR 隨時可知道手機的正確位置。
- 但 GSM 亦要求手機定期向網路再註冊（re-registration）。
- 系統會告訴 MS periodically registration 的 period，時間到時則以一般 registration 的方式做註冊的動作，其週期範圍為6分鐘至24小時。
- Detection of potential fraudulent usage

發話程序（Call Origination Procedure）



1. **Logical channel usage**
   Authentication between VLR and MS
   SS7 ISUP signaling between MSC and PSTN CO

受話程序（Call Termination Procedure）



1. Destination MSC 以MSRN詢問VLR該手機的LAI與TMSI.
2. BTS以PCH廣播MS的TMSI

交遞

- 手機輔助交遞（Mobile-Assisted Handoff，MAHO）
- 由網路端主控且下決定進行交遞
- MS測量附近的BTS的訊號強度。
- 服務手機的BTS也會將MS語音上傳的訊號強度回報給網路端。

交遞的種類

- Intra-BSS handover
  - 新舊BTS屬於同一個BSC的管轄範圍。
- Intra-MSC handover
  - 新舊BTS屬於不同BSC的管轄範圍，但仍在同一個MSC的管轄範圍之中。
  - 又稱為inter-BSS handover
  - 圖6-15
- Inter-MSC handover
  - 新舊BTS屬於不同MSC的管轄範圍。
  - 圖6-16

圖 6-15 Intra-MSC Handover

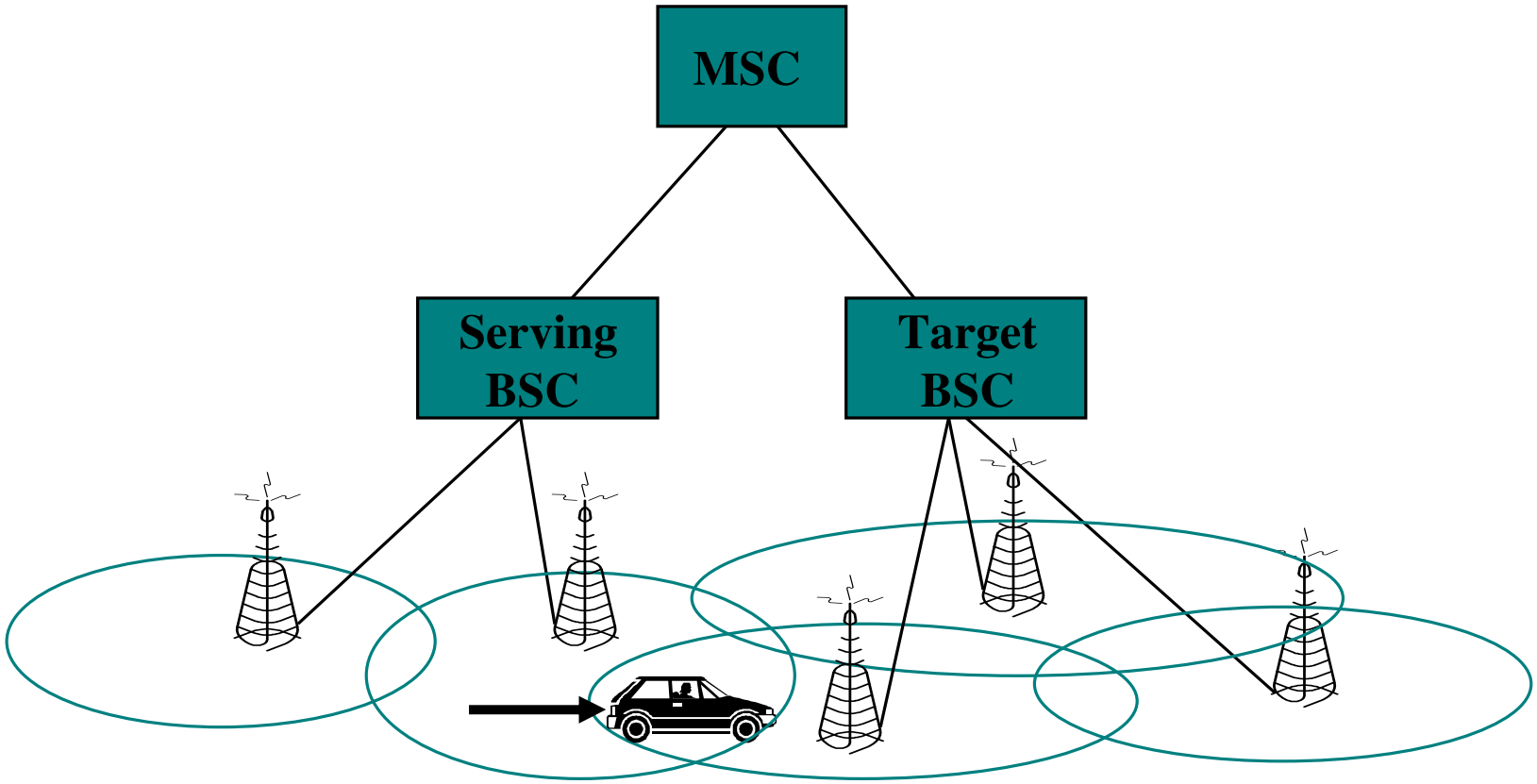
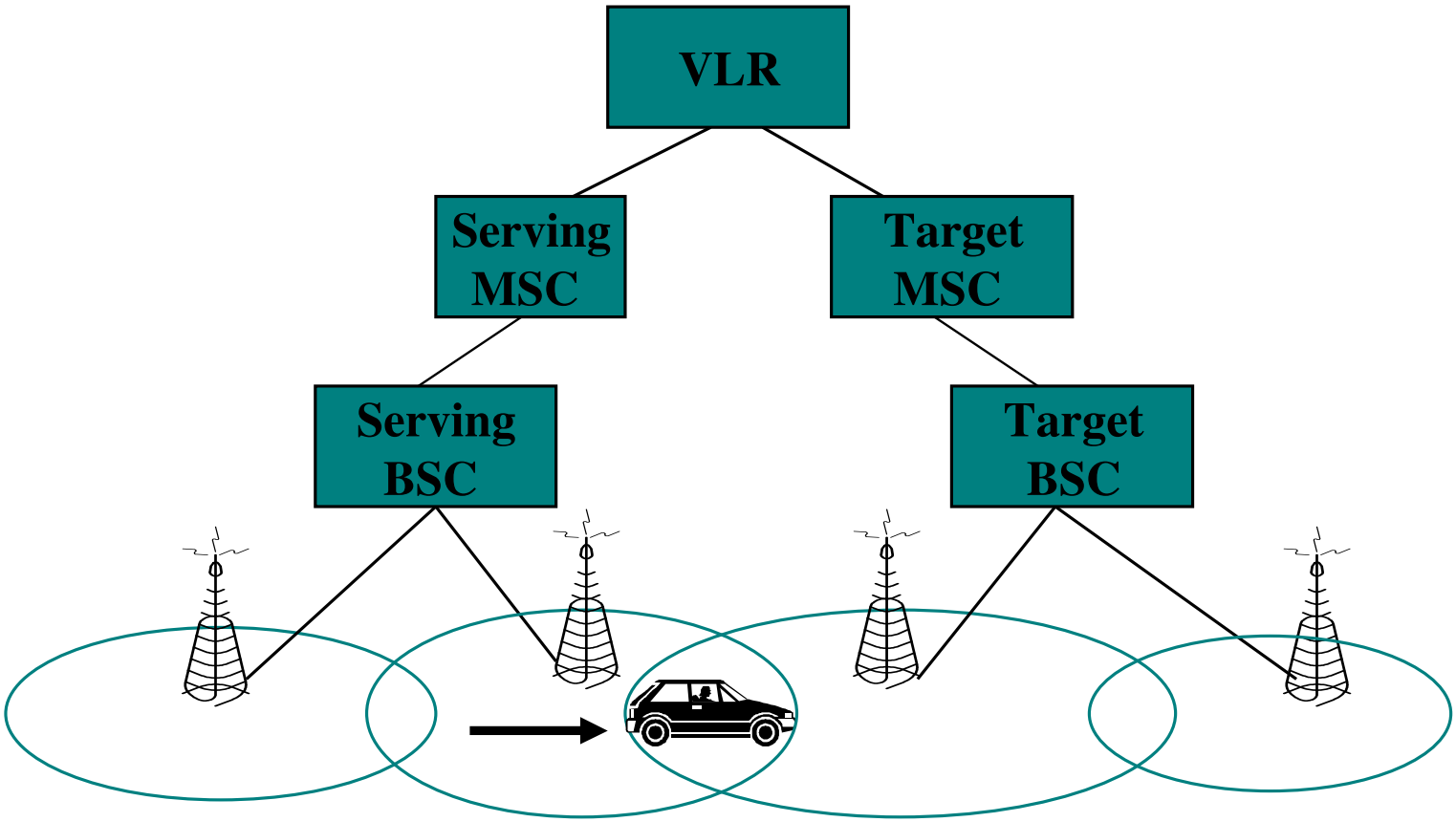


圖 6-16 Inter-MSC Handover



Section 6.5

安全性考量

Security Issue

安全性考量

- GSM的安全措施有兩個方向：
  - 手機認證（authentication）
    - ✓認證係用以防止他人假冒合法手機以盜用GSM的服務。
    - ✓時機: 註冊, 手機位置更新, 通話建立等
  - 訊號加密（encryption）
    - ✓加密則是避免他人竊聽無線電鏈結的通話。

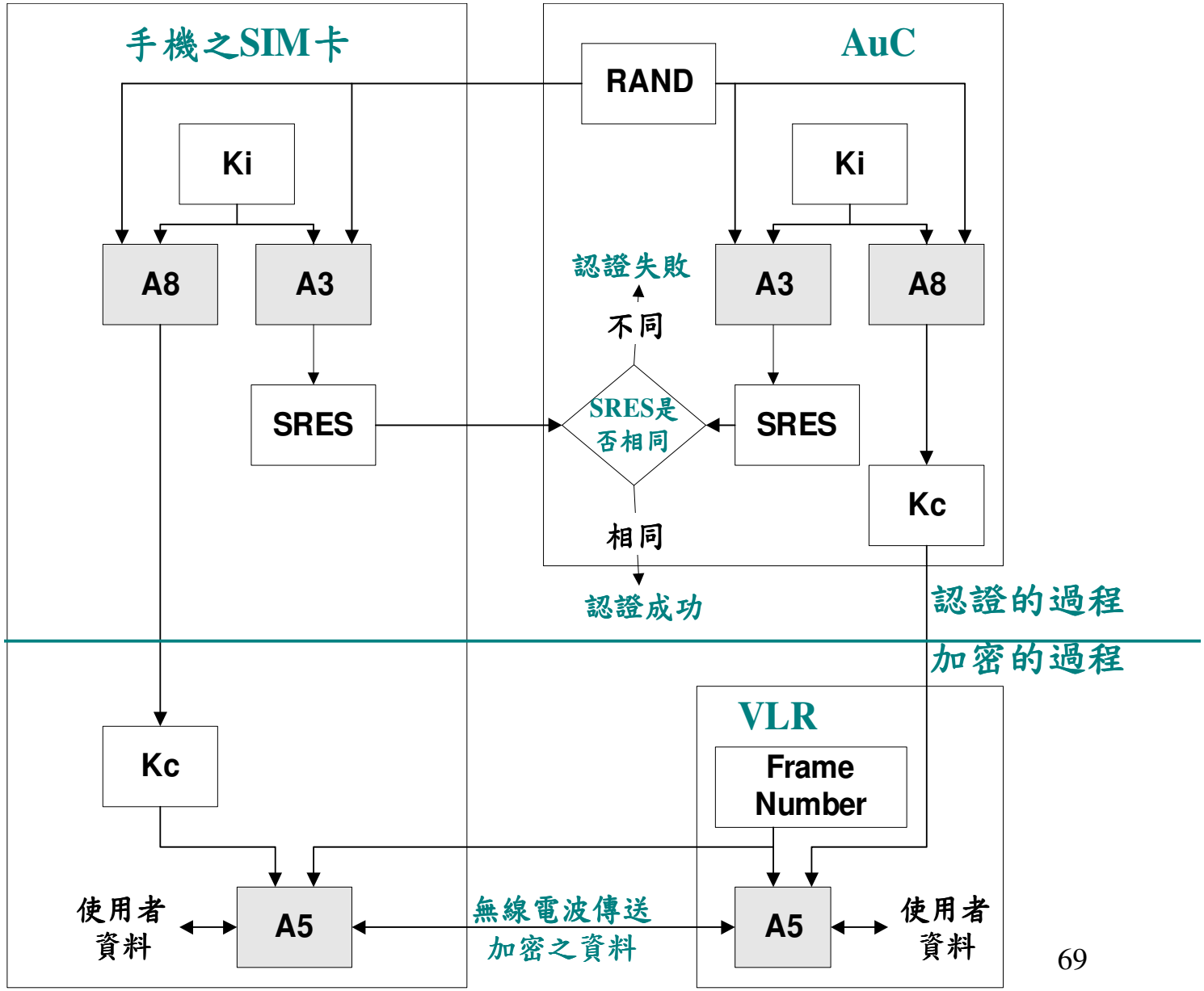
演算法

- 認證演算法
  - **A3.**
    - ✓用於認證的函數。
    - ✓只存於 AuC 和 SIM 卡中，用戶無法取得。
    - ✓漫遊到新的GSM系統, 此新系統不會知道手機的A3演算法
- 加密演算法
  - **A8.**
    - ✓用於產生加密鑰匙 (encryption key)。
    - ✓只存於 AuC 和 SIM 卡中，用戶無法取得。
  - **A5.**
    - ✓存於手機與所有的 visited system (如 BSS, VLR)。
    - ✓用於資料的加密 (ciphering) 與解密 (deciphering)。

相關參數

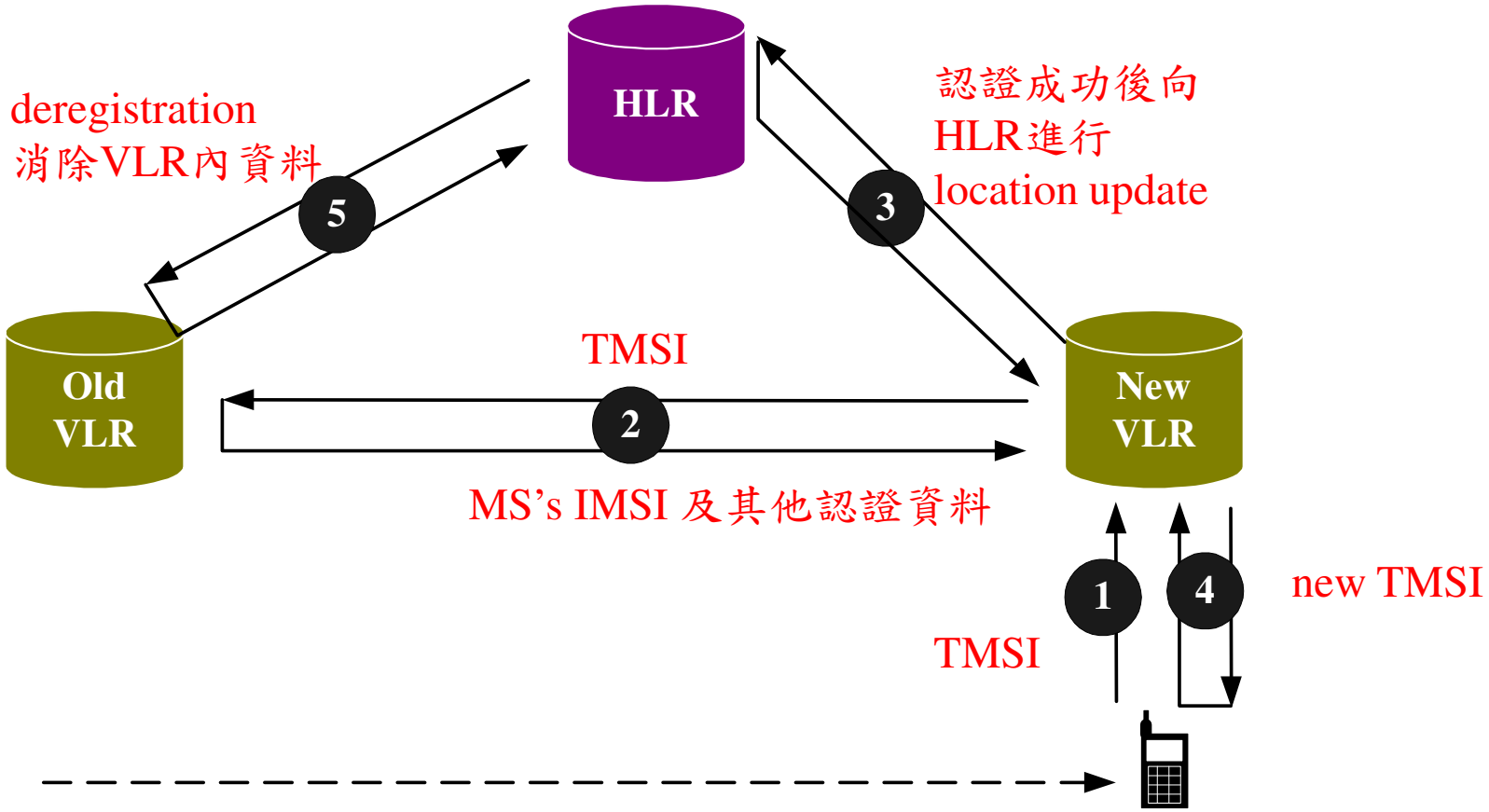
- **Ki** 用於認證
  - 只存於 AuC 和 SIM 卡中，用戶無法取得。
- **RAND** 在 AuC 產生的 128-bit 的亂數
- **SRES**
  - 由演算法 A3 產生的結果，比對 AuC 與 SIM 產生之 SRES，可以認證 MS 的合法性。
- **Kc** 由演算法 A8 產生的結果，用於加密。
- **Frame Number.**
  - TDMA 訊框號碼，用於加密。

圖 6-17 GSM 的認證與加密



使用 Triplets 認證

- Ki 只存於 AuC，會造成 AuC 的負擔太重。
- 當 MS 移動到一個新的 VLR，便會向 AuC 要多個認證碼組（triplet）。
  - Triplet 包含3項資料：RAND 、SRES與Kc。
  - HLR 任意產生 RAND，計算 SRES 與 Kc，合稱為一個 triplet。
- 認證時，VLR 可以直接送 RAND 給 MS，用 triplet 中的 SRES 與 MS 送回之 SRES 比對。
- 認證成功，VLR 送 Kc 給 BTS，而手機可自行產生Kc。

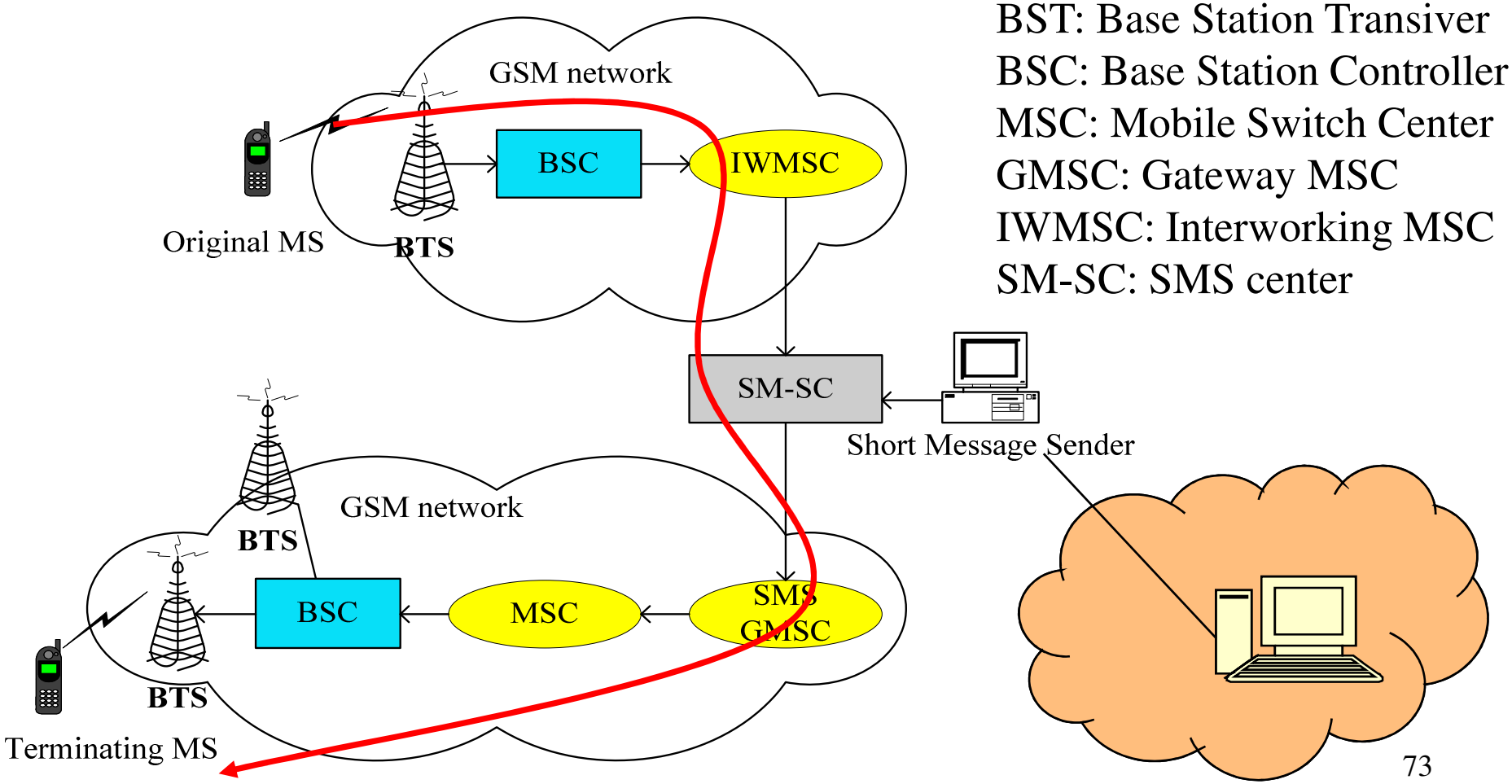

HLR
deregistration
消除VLR內資料
5
認證成功後向
HLR進行
location update
3
Old
VLR
TMSI
2
New
VLR
MS's IMSI 及其他認證資料
1
4
new TMSI
TMSI

Section 6.7

簡訊系統

Short Message Service，SMS

圖 6-20 SMS 的架構

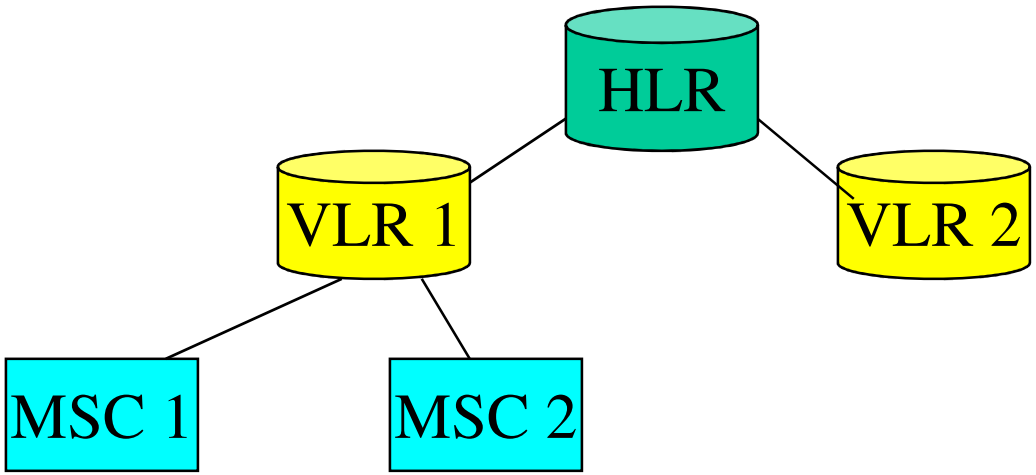


BST: Base Station Transiver
BSC: Base Station Controller
MSC: Mobile Switch Center
GMSC: Gateway MSC
IWMSC: Interworking MSC
SM-SC: SMS center

Mobility Databases

Mobility Databases

- The hierarchical databases used in GSM.
  - The home location register (HLR) is a database used for MS information management.
  - The visitor location register (VLR) is the database of the service area visited by an MS.



Home Location Register (HLR)

- An HLR record consists of 3 types of information:
  - Mobile station information
    - ✓ IMSI (used by the MS to access the network)
    - ✓ MSISDN (the ISDN number—"Phone Number" of the MS)
  - Location information
    - ✓ ISDN number of the VLR (where the MS resides)
    - ✓ ISDN number of the MSC (where the MS resides)
  - Service information
    - ✓ service subscription
    - ✓ service restrictions
    - ✓ supplementary services

Visitor Location Register (VLR)

- The VLR information consists of three parts:
  - Mobile Station Information
    - ✓ IMSI
    - ✓ MSISDN
    - ✓ TMSI
  - Location Information
    - ✓ MSC Number
    - ✓ Location Area ID (LAI)
  - Service Information
    - ✓ A subset of the service Information stored in HLR

Two Issues of GSM Mobility Databases

- **Fault Tolerance.**
  - If the databases fail, the loss or corruption of location information will seriously degrade the service.
- **Database Overflow.**
  - VLR may overflow if too many users move into the VLR-controlled area in a short period.
  - If VLR is full, a new arrival user fails to register in VLR and thus cannot receive service.
  - This phenomenon is called VLR overflow.

VLR Failure Restoration

VLR Failure Restoration (1/2)

- After a VLR failure, VLR's information:
  - **Mobile Station Information**
    - ✓ Recovered either by the first contact with HLR or MS.
  - **Location Information**
    - ✓ Recovered by the first radio contact with MS.
  - **Service Information**
    - ✓ Recovered by the first contact with HLR of the corresponding MS.

VLR Failure Restoration (2/2)

- After a VLR failure, the VLR record restoration is initiated by one of the following three events:
  - MS registration
  - MS call origination
  - MS call termination

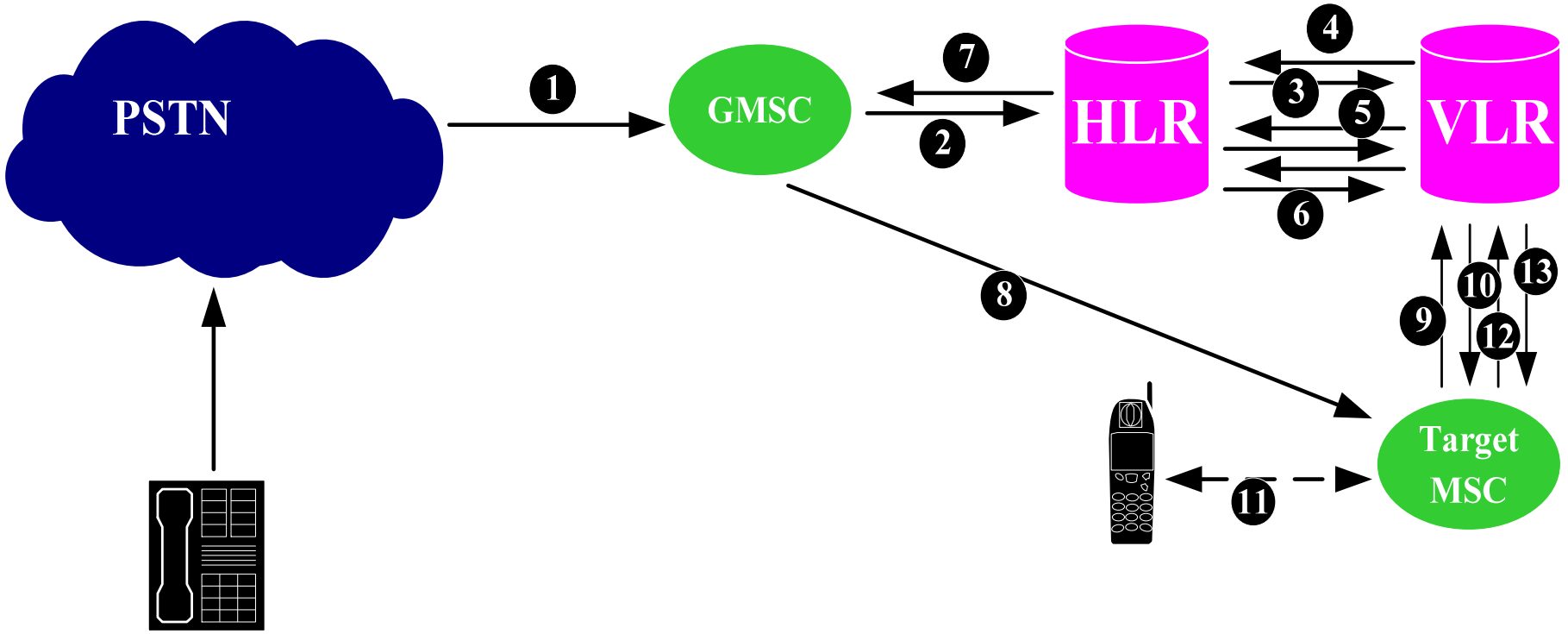
Restoration—MS Registration

- After a VLR failure:
  - No record of MS in VLR
  - VLR considers the registration as an inter-VLR movement.
  - VLR ask MS to follow the normal registration procedure defined in inter-VLR movement.
  - The TMSI sent from the MS to the VLR cannot be recognized
  - VLR asks MS to send IMSI over the air.

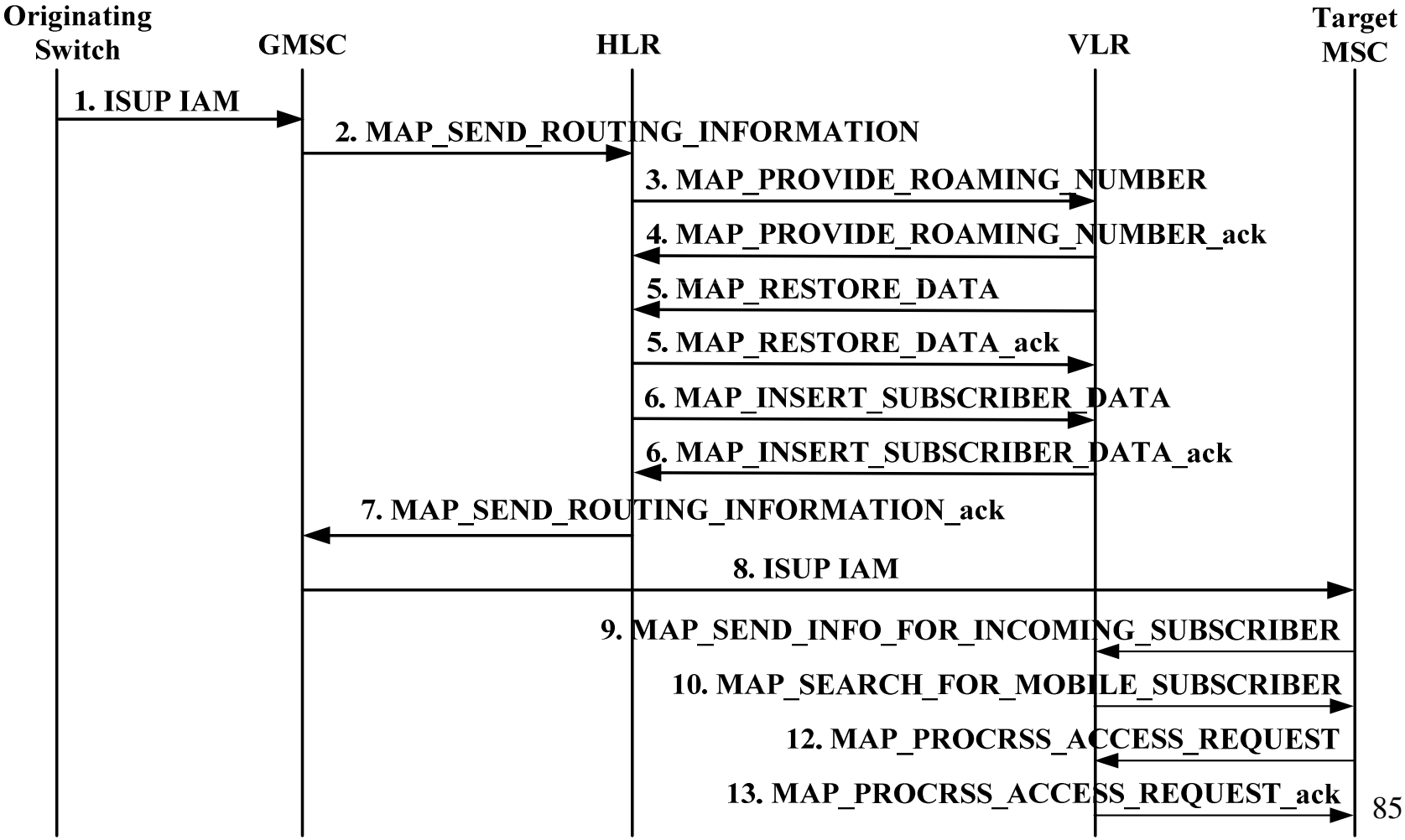
Restoration – MS Call Origination

- After a VLR failure:
  - VLR receives the call origination request **MAP_SEND_INFO_OUTGOING_CALL** from the MSC (and MS).
  - No record of MS in VLR
  - VLR considers it as a system error: "**unidentified subscriber**" and rejects the request.
  - VLR asks MS to initiate the registration procedure of inter-VLR movement.
  - After the registration procedure, the VLR record is recovered.

Restoration – Call Termination Message (1/2)



Restoration – Call Termination Message (2/2)

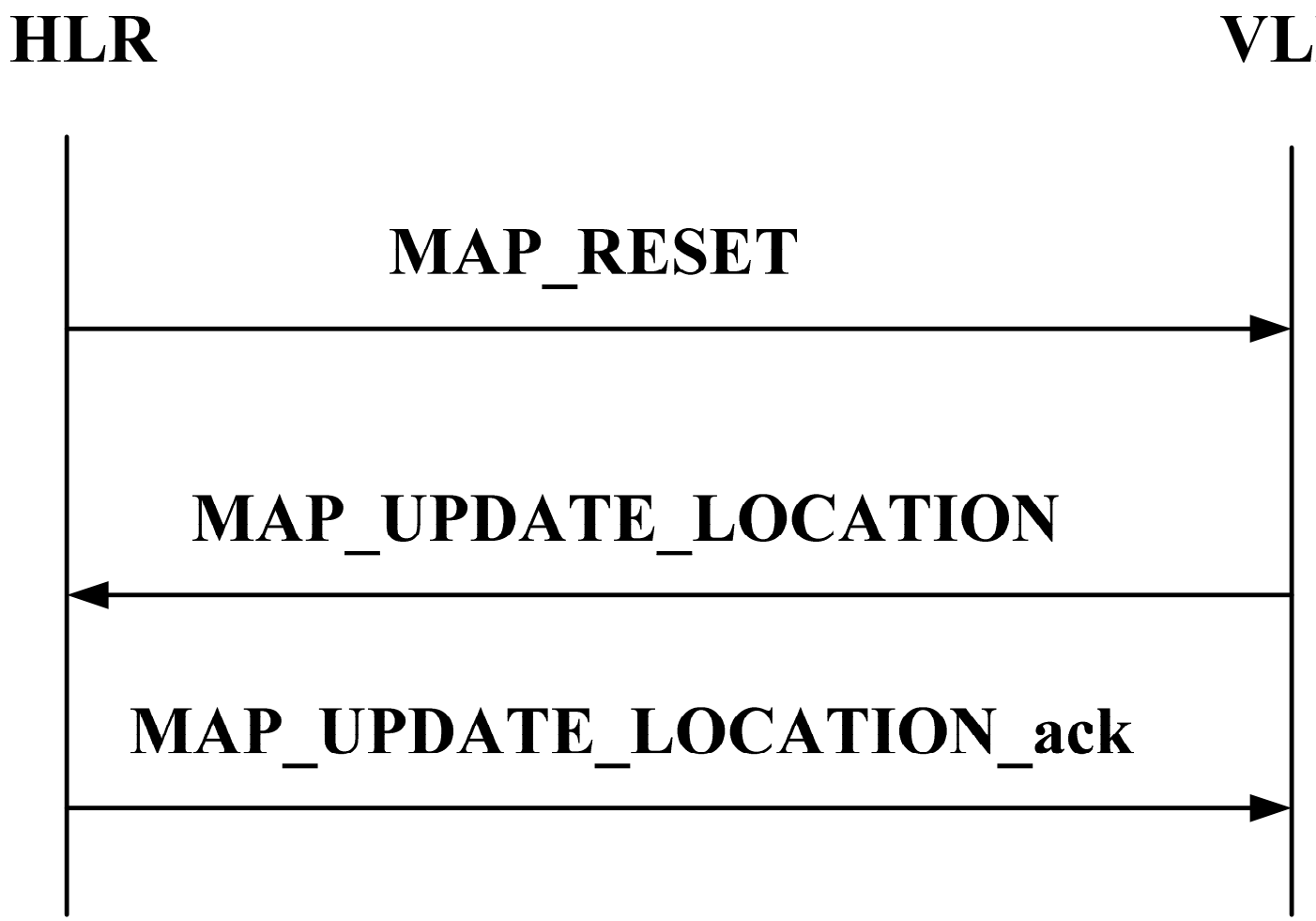


HLR Failure Restoration

HLR Failure Restoration

- In HLR, it is mandatory to save the updates into backup storage.
- The **service information** is immediately transferred from the HLR into the backup.
- The **location information** is periodically transferred from the HLR into the backup.
- After an HLR failure, the data in the backup are reloaded into the HLR.

HLR Restoration Procedure Message Flow



Questions in HLR Restoration Procedure

- The HLR restoration procedure is not robust.
  - An MS moves into a VLR during the uncovered period.
  - HLR does not know this VLR at checkpoint.
  - HLR will not ask the VLR to send location information.
- VLR Identification Algorithm is to solve the problem.

VLR Identification Algorithm (VIA)

VLR Identification Algorithm

- VIA identifies the exact VLRs to be contacted by the HLR after an HLR failure.
- Extra data structures are needed.
- Extra procedures are needed:
  - Check-point procedure
  - Registration procedure
  - Restoration procedure

Data Structure in VLR Identification Algorithm (VIA) (1/2)

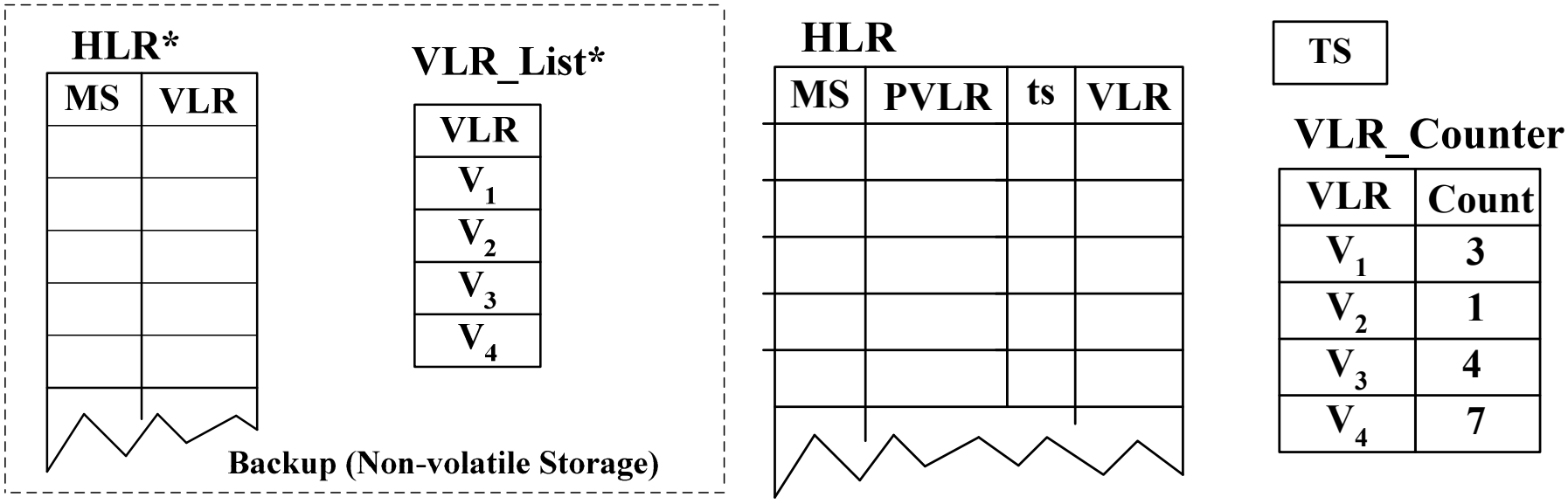
- To simply the description, we assume that every VLR covers exactly one MSC.
- An extra data structure **VLR_List*** is a set of VLRs that have been contacted with HLR during the uncovered period.
- After an HLR failure, the HLR only needs to send the **MAP_RESET** messages to VLRs listed in **VLR_List***.

Data Structure in VLR Identification Algorithm (VIA) (2/2)

- In HLR, every record includes two extra fields.
  - ts = the last time of location update
  - PVLR = the address of VLR where the resided at the lat check-pointing time. Thus, for any MS p, we have

    HLR*[p].VLR = HLR[p].PVLR
- Two extra data structures in the HLR
  - TS = the last check-pointing or backup time
  - VLR_Counter = {(*VLR1*,*Count 1*), (*VLR2*,*Count 2*), …, (*VLRn*,*Count n*)} where Count n represents the "effective number" of MSs entering the *VLRn* during the uncovered period.
  - Note that the VLRs recorded in VLR_Counter are the VLRs in VLR_List*.

VIA Data Structure



VIA Procedure 1: Check-Pointing

- In VIA, information of the HLR is periodically saved into the backup by this procedure.
- **Step 1.** For every entry p in HLR* do:

  HLR[p]*.VLR ← HLR[p].VLR
- **Step 2.** TS ← current time;
- **Step 3.** For every location entry p in HLR do:

  HLR[p].ts ← TS

  HLR[p].PVLR ← HLR[p].VLR
- **Step 4.** VLR_Counter ← NULL; VLR_List* ← NULL;

VIA Procedure 2: Registration (1/3)

- **Step 1.** Update HLR:
  - Vold ← HLR[p].VLR;
  - Send message, MAP_CANCEL_LOCATION, to cancel the VLR entry of p at Vold;
  - HLR[p].VLR ← Vnew;
  - told ← HLR[p].ts;
  - HLR[p].ts ← t;

VIA Procedure 2: Registration (2/3)

- **Step 2.** Update the V_{new} Count field in VLR_Counter:

```
If (HLR[p].VLR <> HLR[p].PVLR){
   If (VLR_Counter[Vnew] exists){
     VLR_Counter[Vnew].Count <-
   VLR_Counter[Vnew].Count+1;
   }else{
     create VLR_Counter[Vnew] and VLR_List*[Vnew];
     VLR_Counter[Vnew].Count <- 1;
   }
}
```

VIA Procedure 2: Registration (3/3)

- **Step 3.** Update the V_{old} counter entry:

```
If (told > TS and Vold <> HLR[p].PVLR){
    VLR_Counter[Vold].Count <-
    VLR_Counter[Vold].Count – 1;
    If (VLR_Counter[Vold].Count = 0){
      Delete VLR_Counter[Vold] and VLR_List*[Vold];
    }
}
```

VIA Procedure 3: Restore

- **Step 1.** TS <- current time;
- **Step 2.**

```
for (every location entry p in HLR){
    HLR[p].PLVR = HLR[p].VLR <- HLR[p]*.VLR;
    HLR[p].ts <- TS;
}
```

- **Step 3.**

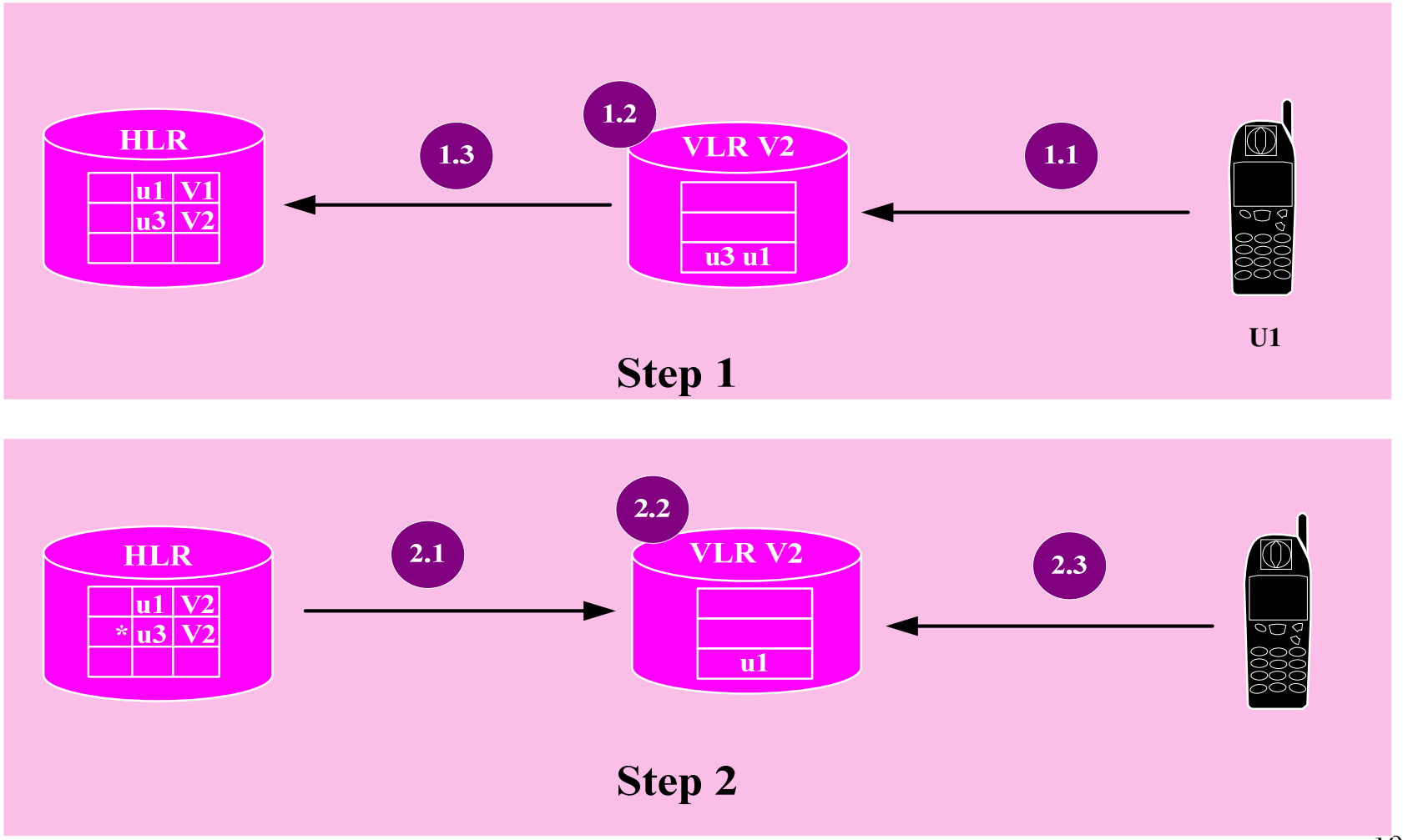
```
for (every VLR entry V in VLR_List*){
    send an SS7 TCAP MAP_RESET message to V;
}
```

VLR Overflow Control

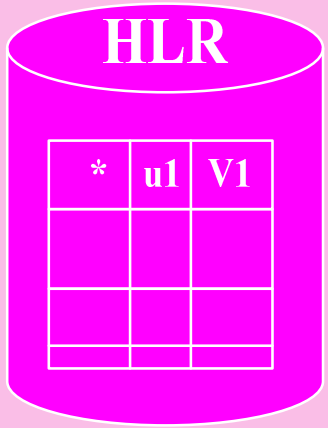
VLR Overflow Control

- VLR may overflow if too many mobile users move into the LA in a short period.
- When a VLR is full, a new arrival user can not register and get service.
- If we want to let the new arrival user can get service, all of the following procedures need to be modified:
  - registration, cancellation, call origination, call termination

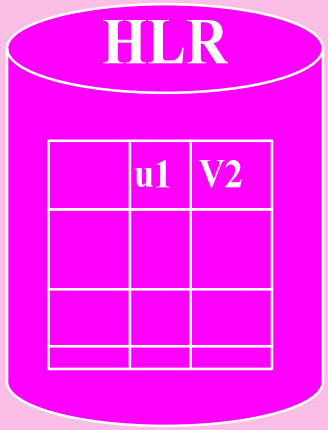
Overflow Registration Operation



Cancellation Operation with Overflow VLR

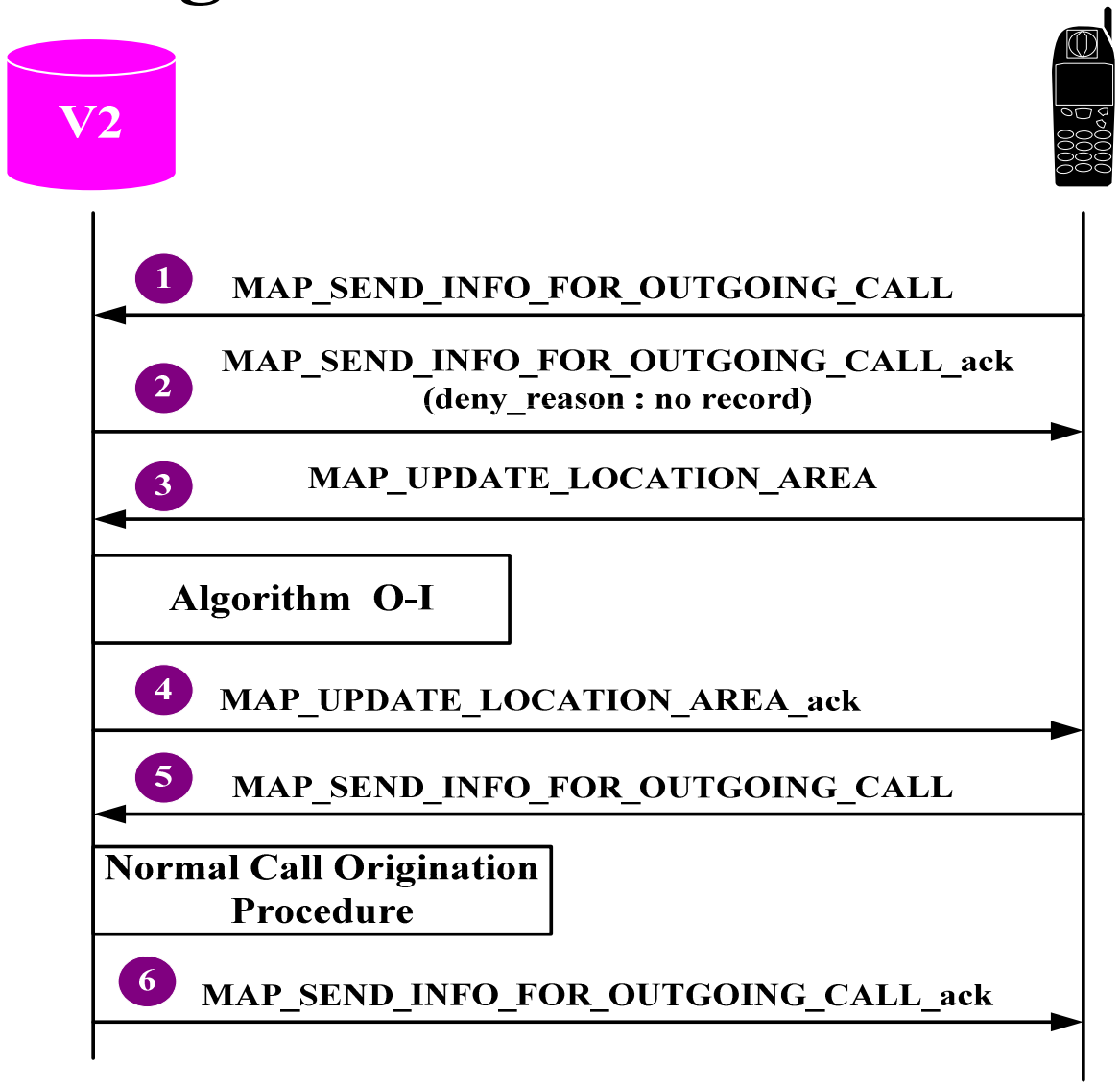


Before the registration operation

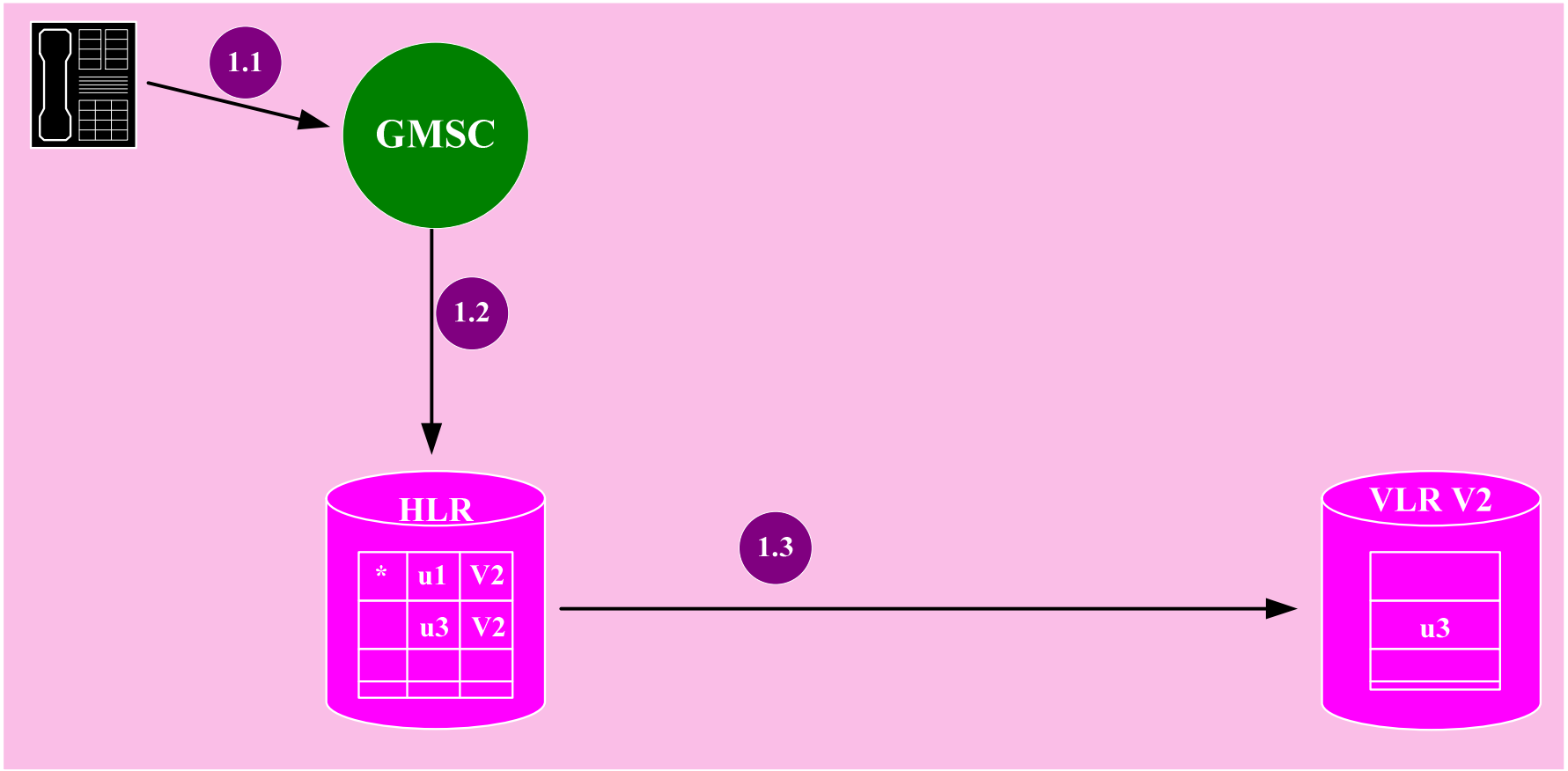


After the registration operation (V1 may not be accessed for de-registration)

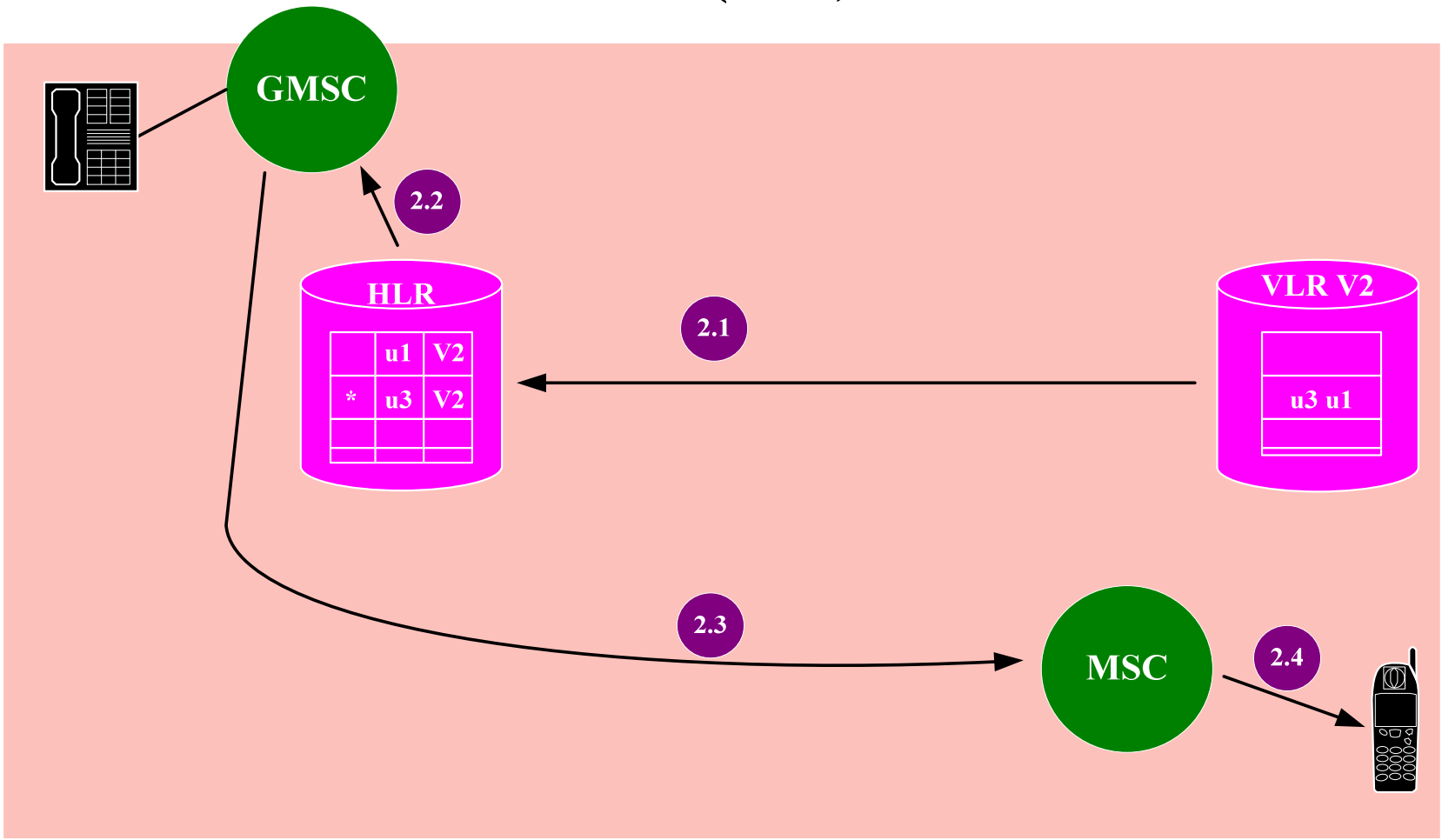
Call Origination with Overflow VLR



Call Termination with Overflow VLR (1/2)



Call Termination with Overflow VLR (2/2)



Section 6.8

結語

Summary

Summary

- GSM雖然使用許多已成熟的傳統技術，但系統業者經過多年的經營，不斷地調整系統參數與相關設定，使整個GSM系統效能達到最好的狀態。而且GSM開始時便以結合歐洲各國行動電話系統做為設計的方針，採用開放的架構，與良好的行動管理設計，只要使用自己的SIM卡就可漫遊到各國的GSM系統，真正達到anytime、anywhere的目標。

Homework