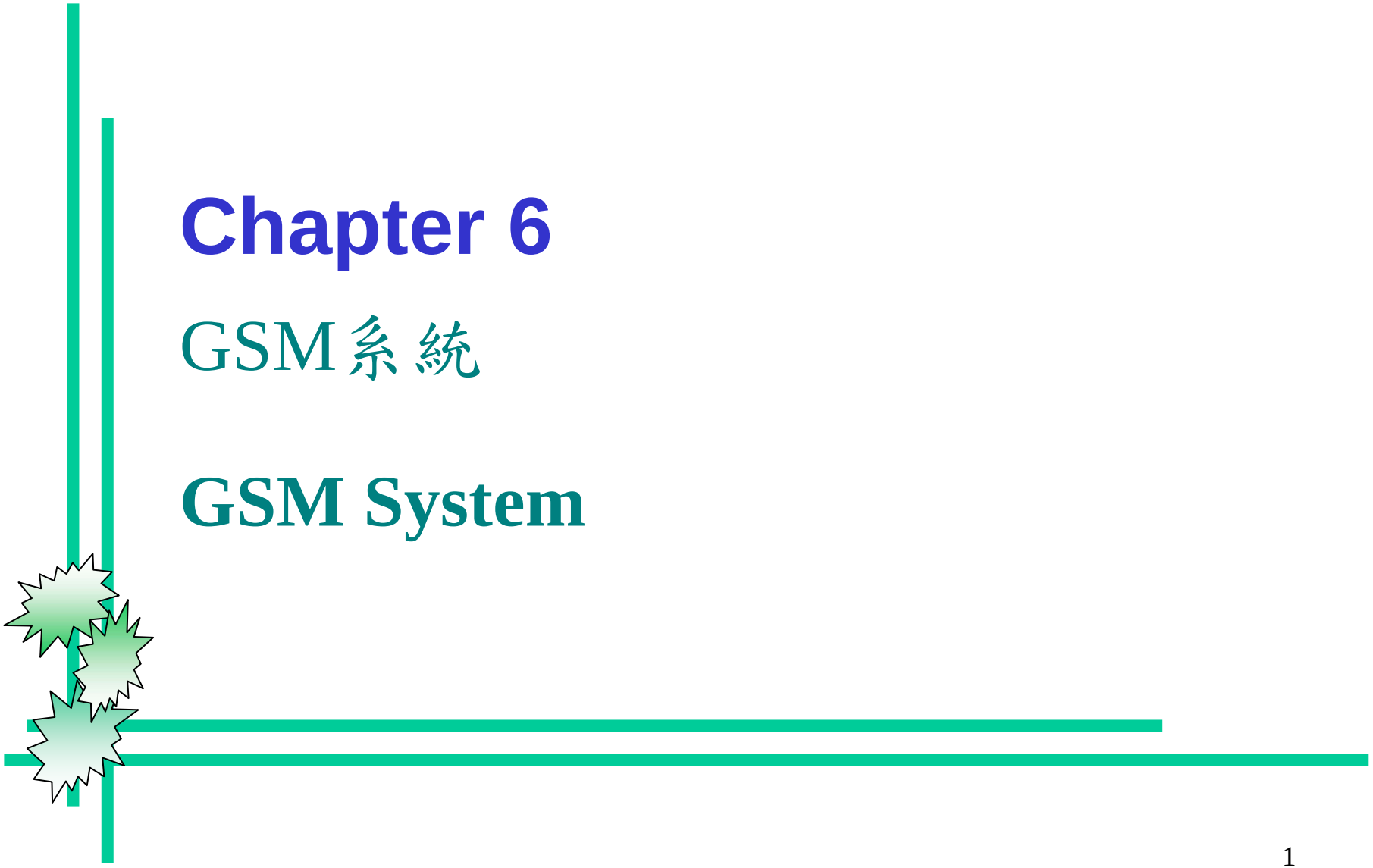


Chapter 6

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

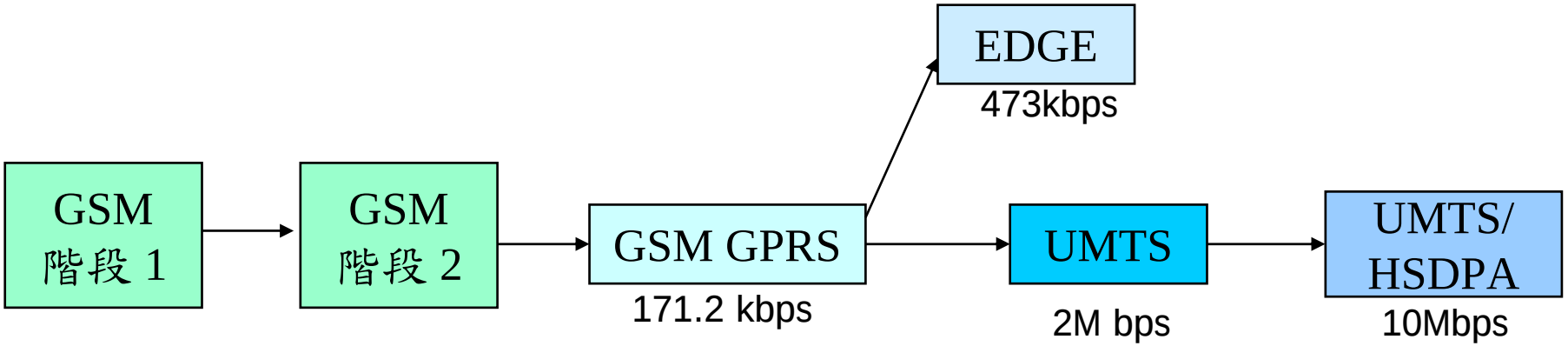
GSM 現況介紹

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

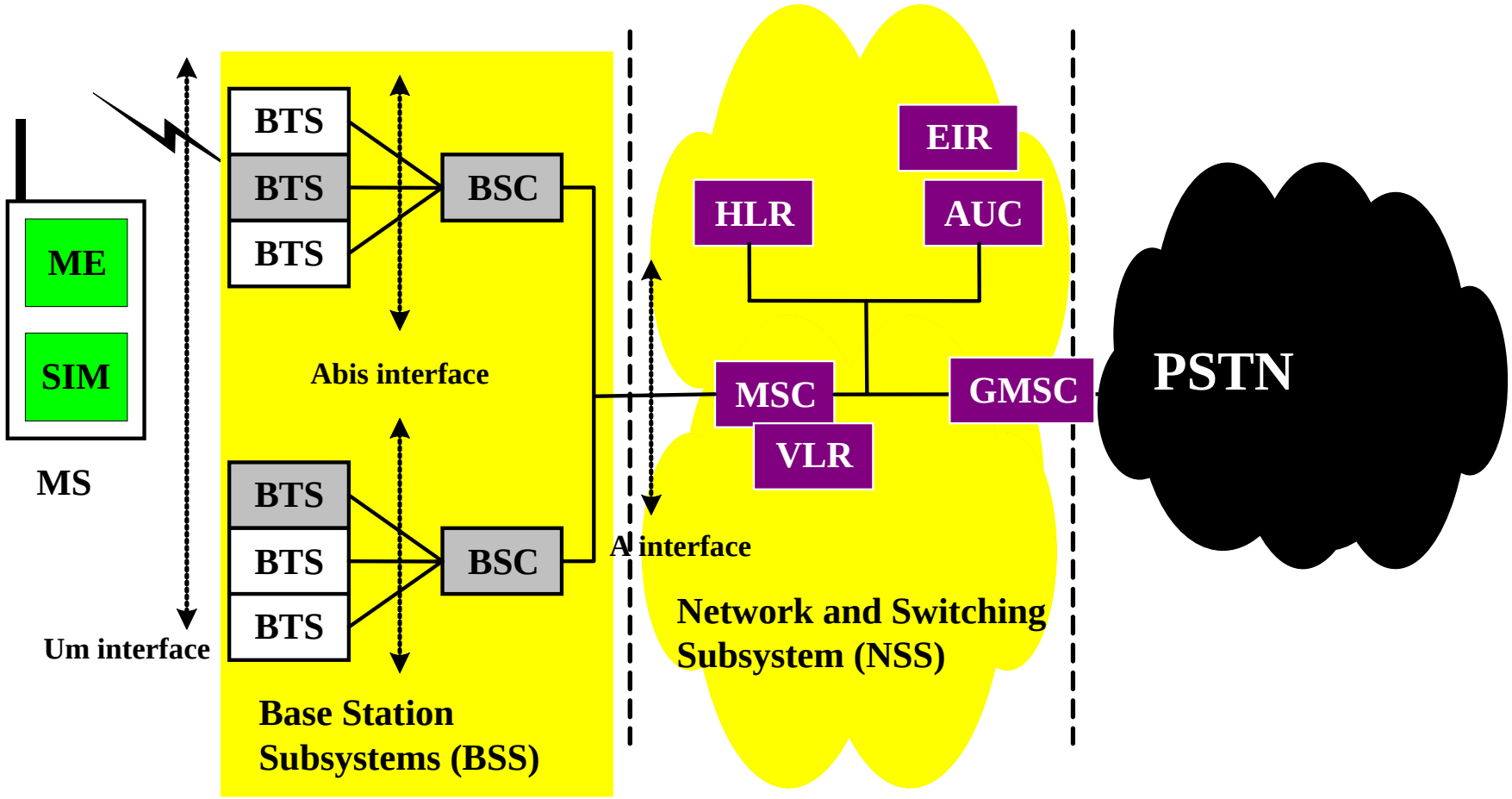
Section 6.2

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。

傳輸編碼器與速率轉接器單元

- 傳輸編碼器與速率轉接器單元（Transcoder/Rate Adapter Unit，TRAU）
- BSS與GSM網路間必須進行語音資訊的轉換
  - 無線電介面採用13kbps的GSM編碼方式
  - 核心網路採用64kbps的PCM（Pulse–Code Modulation）
  - 轉換語音編碼與解碼及調整傳輸速率
- 在GSM規格書中，TRAU是BTC的一部份，但許多時候TRAU是置於MSC與BTS間，以減少BSC與BTS間的資料傳送。

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 (1/2)

- 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

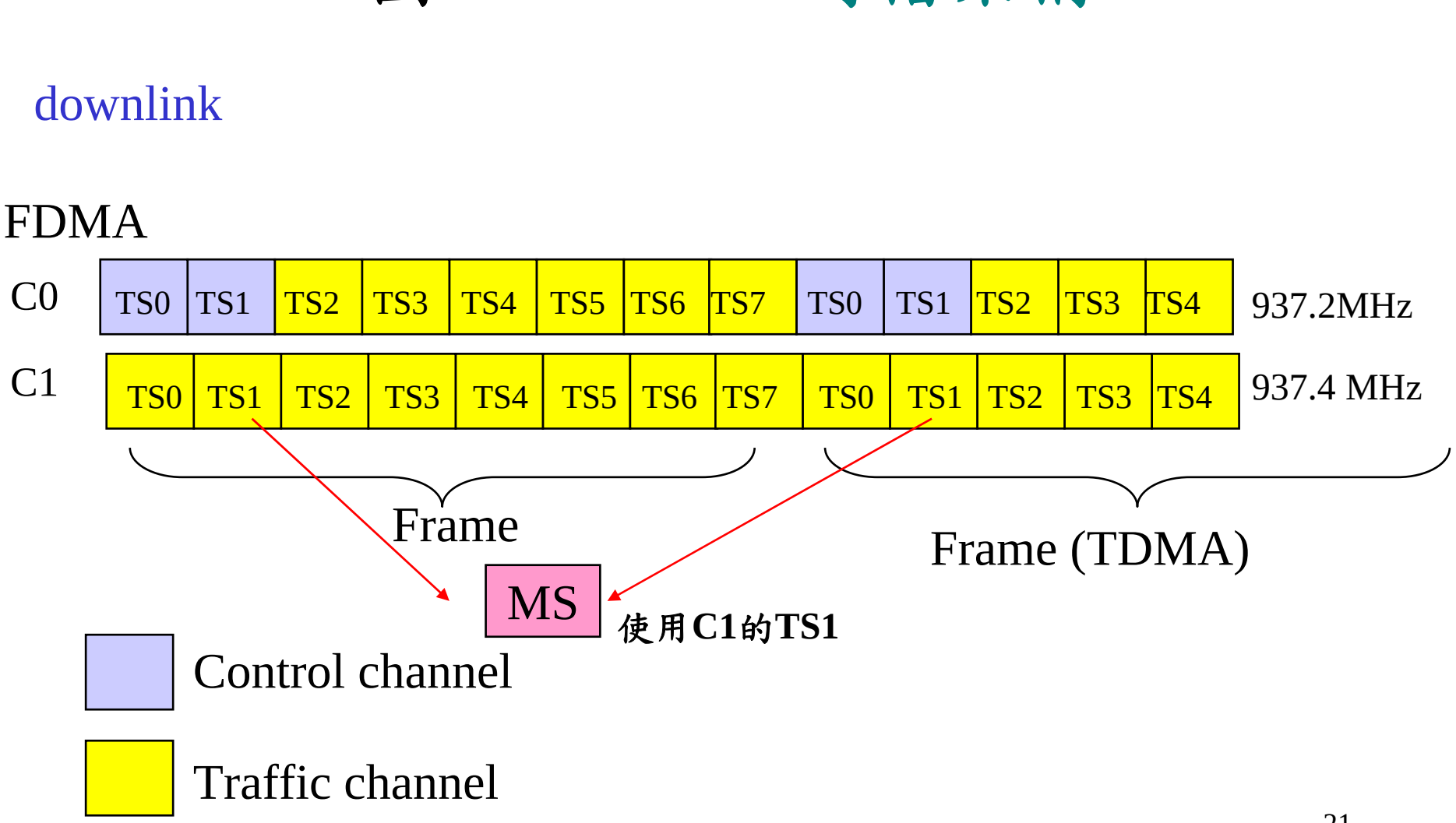
無線電介面 (1/2)

- 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

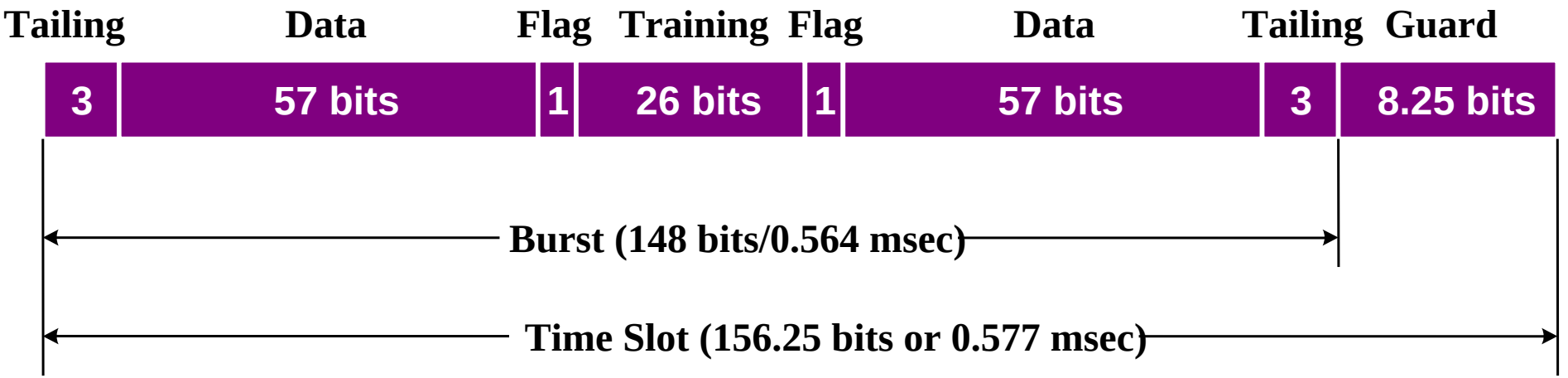
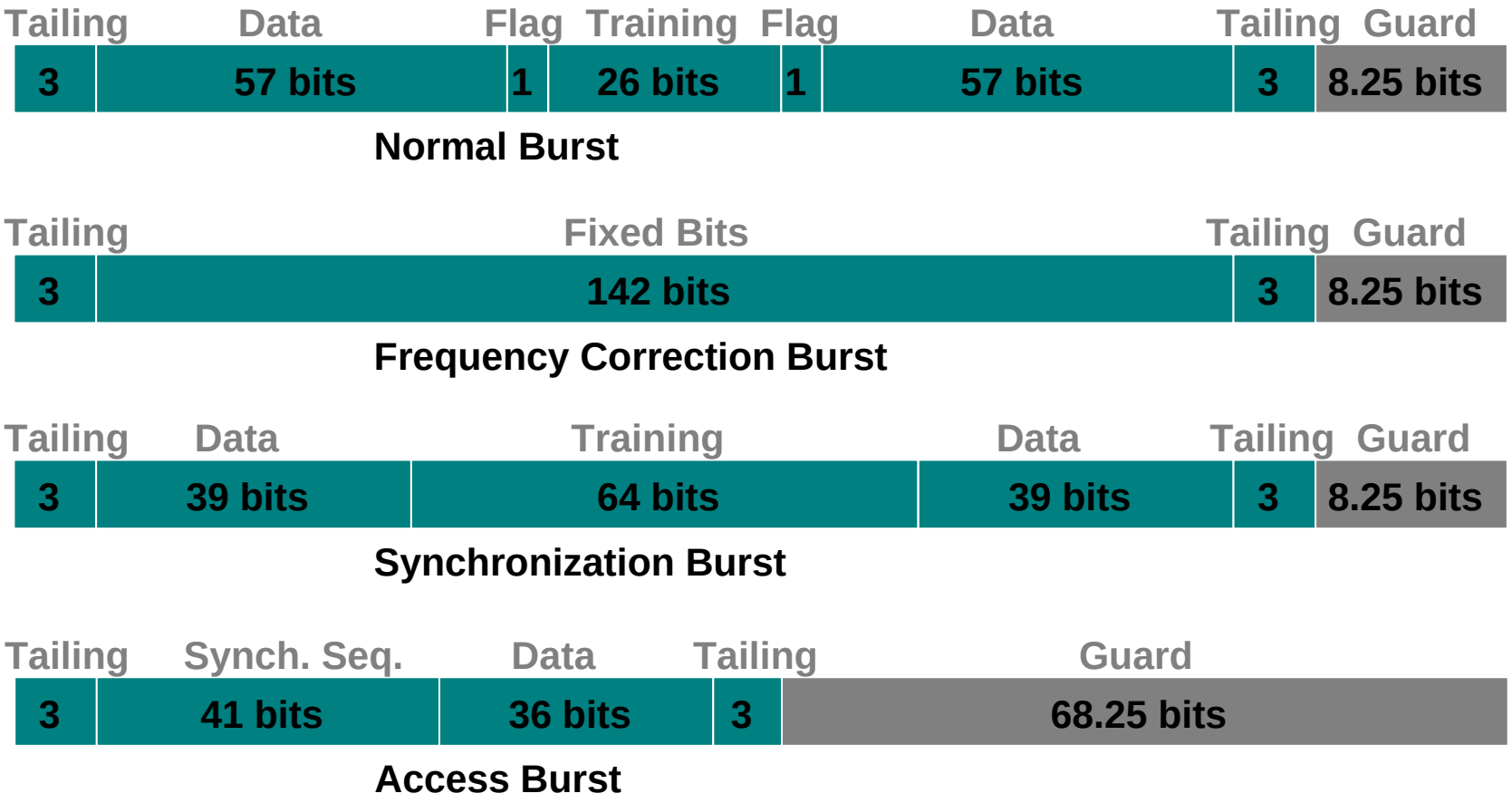


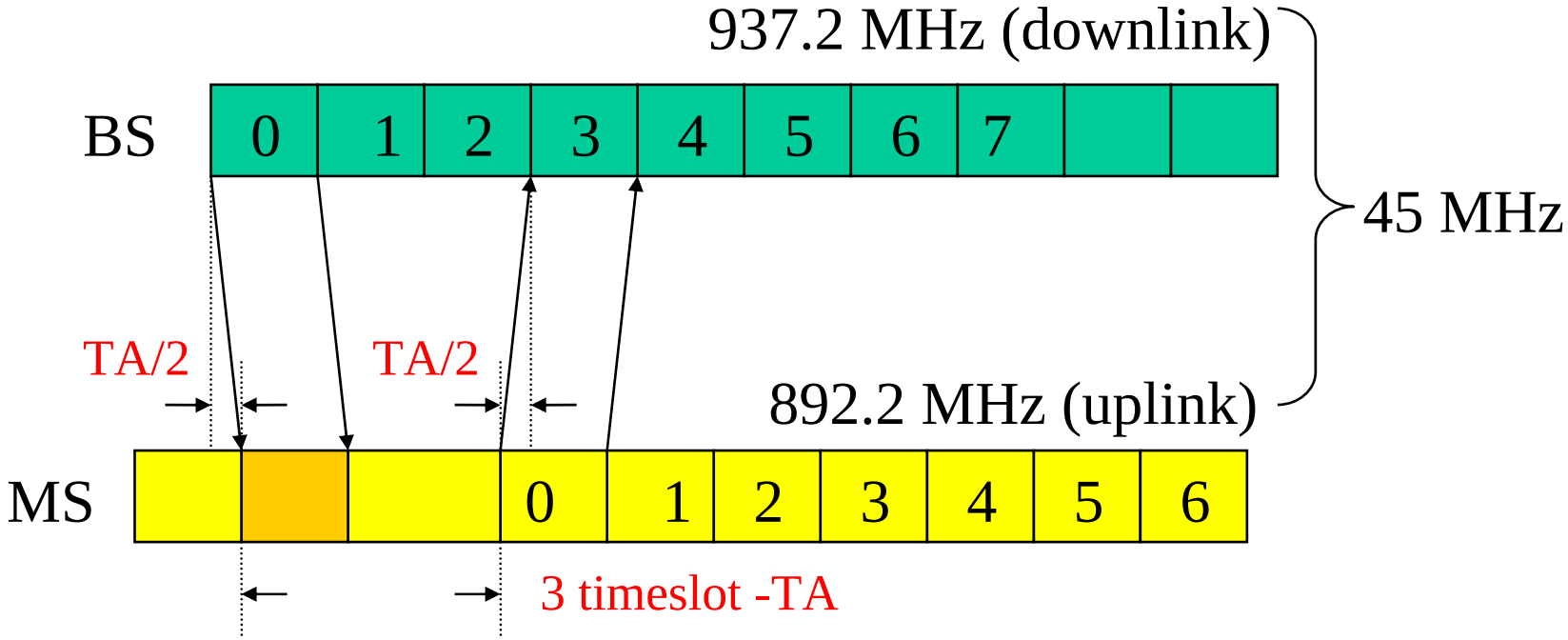
圖 6-5 GSM Bursts



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。

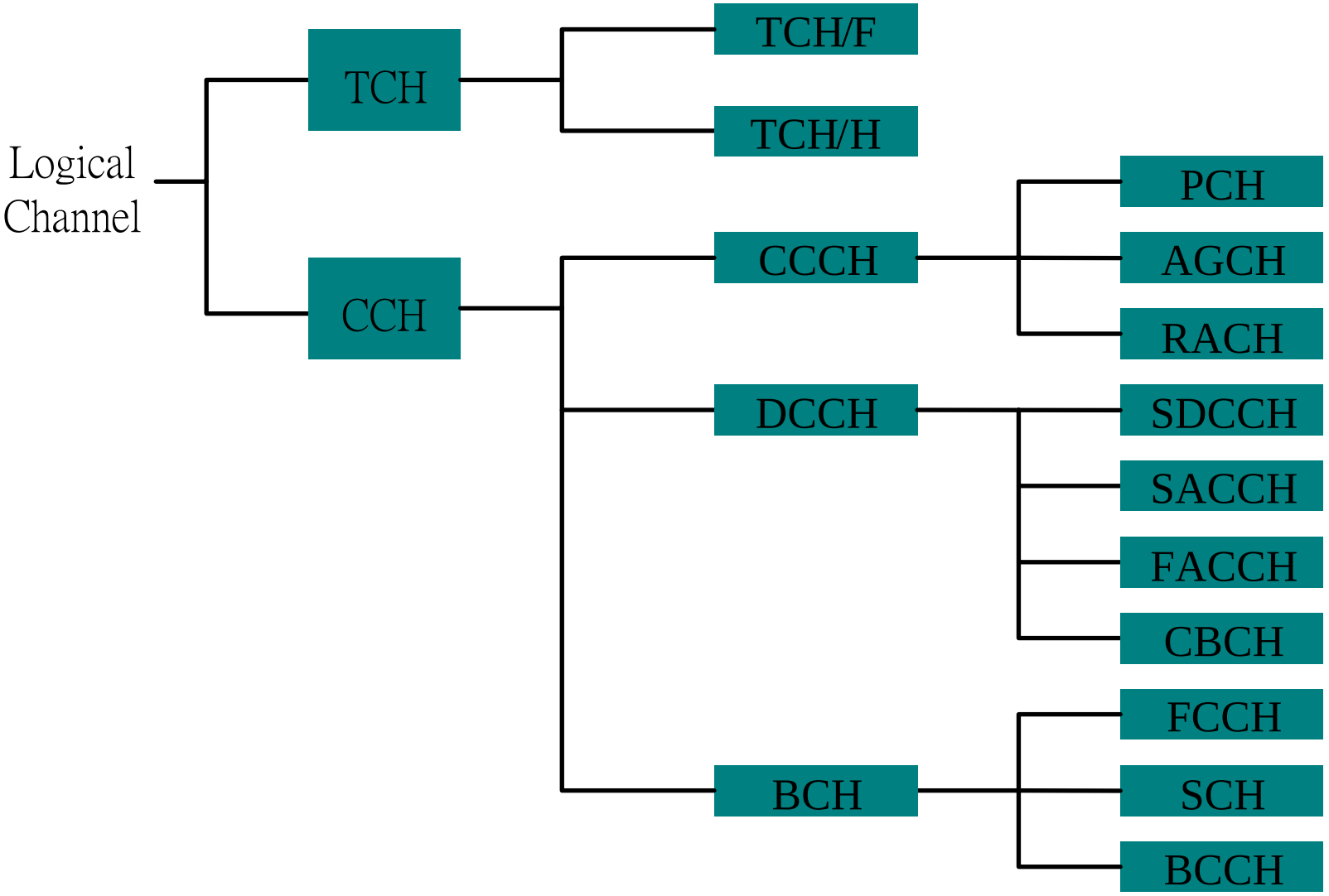
圖 6-6 Time Advance



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對一支手機間信令的通訊，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。

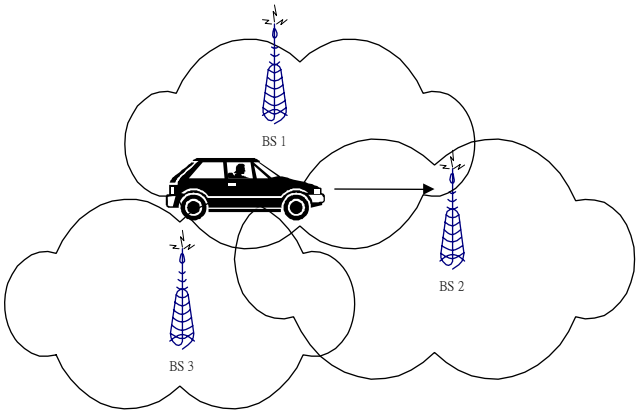
專屬控制通道（DCCH）(1/2)

- 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)

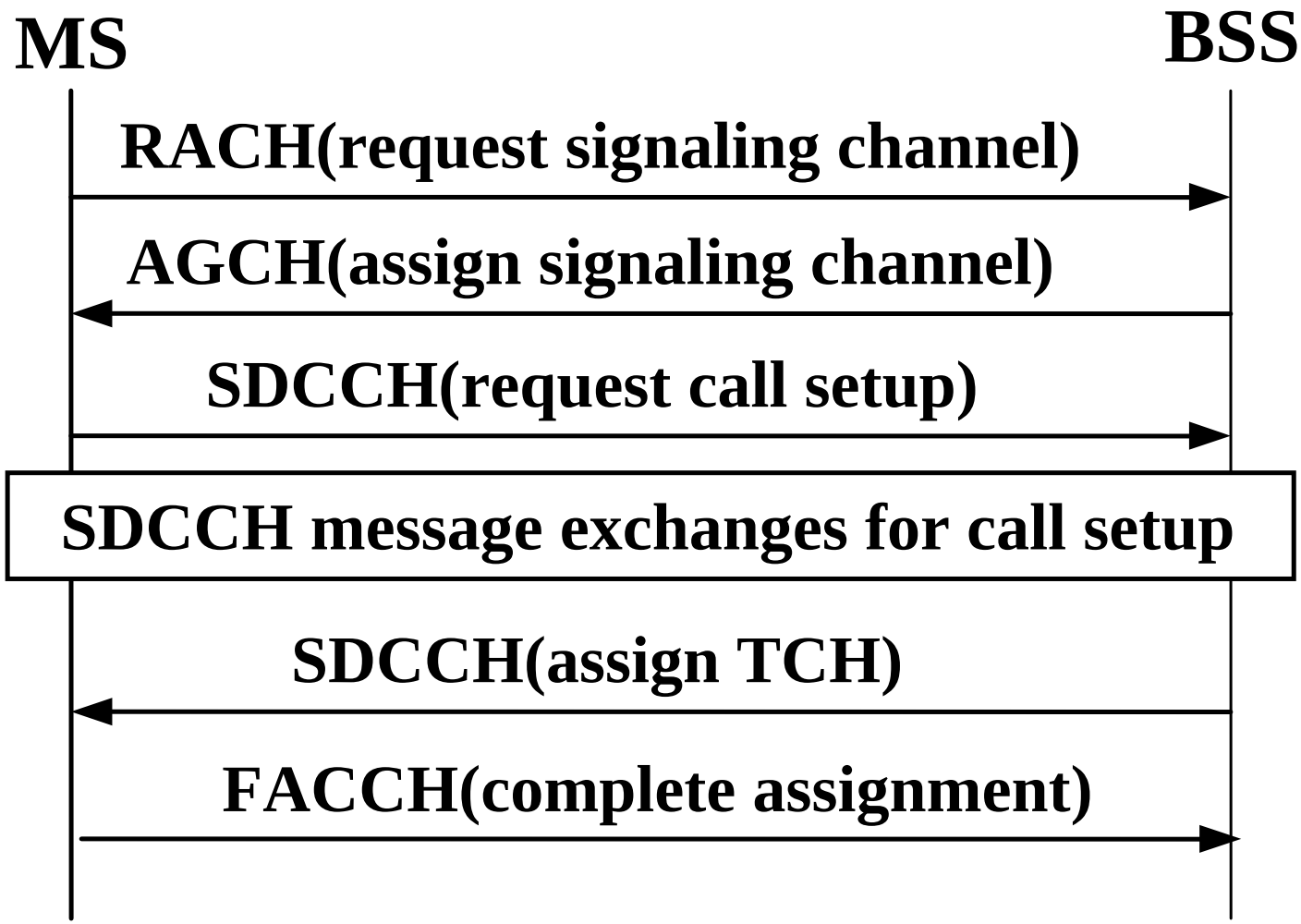
- 快速相關控制通道（Fast Associated Control CHannel，**FACCH**）
  - 傳送緊急控制信令（time-critical signaling），包括電話線路的設定、手機認證（authentication）以及交遞（handover）的信號。
  - **FACCH**佔用訊務通道的時槽。
- 細胞廣播通道（Cell Broadcast CHannel，**CBCH**）
  - 提供簡訊的廣播服務（short message service cell broadcast messages）。

手機註冊

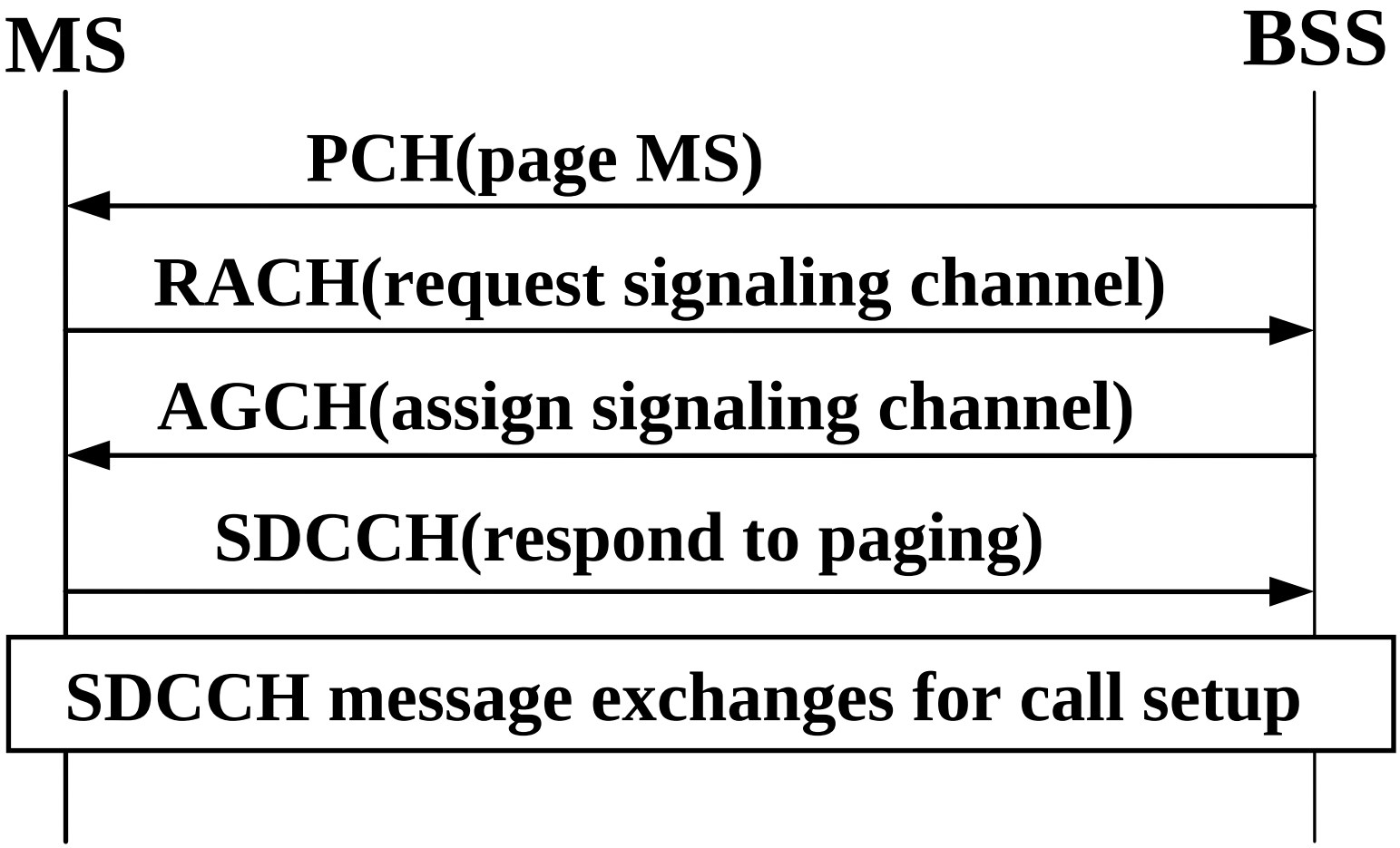


- 當MS開機後，會掃瞄屬於GSM的全部頻道。
- MS會找出訊號最強的頻道，判斷是否為承載 **BCCH** 的控制頻道。
- MS會利用 **FCCH** 校正自己的頻率以便與BTS的頻率同步。
- 由 **SCH** 可得到基地台的編號（BSIC）。
- 從 **BCCH** 則可得到細胞的編號，判斷是否是為所屬的 PLMN 的細胞。若不是則再繼續搜尋，直到找到可用的細胞為止。
- 接下來MS向MSC註冊。

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

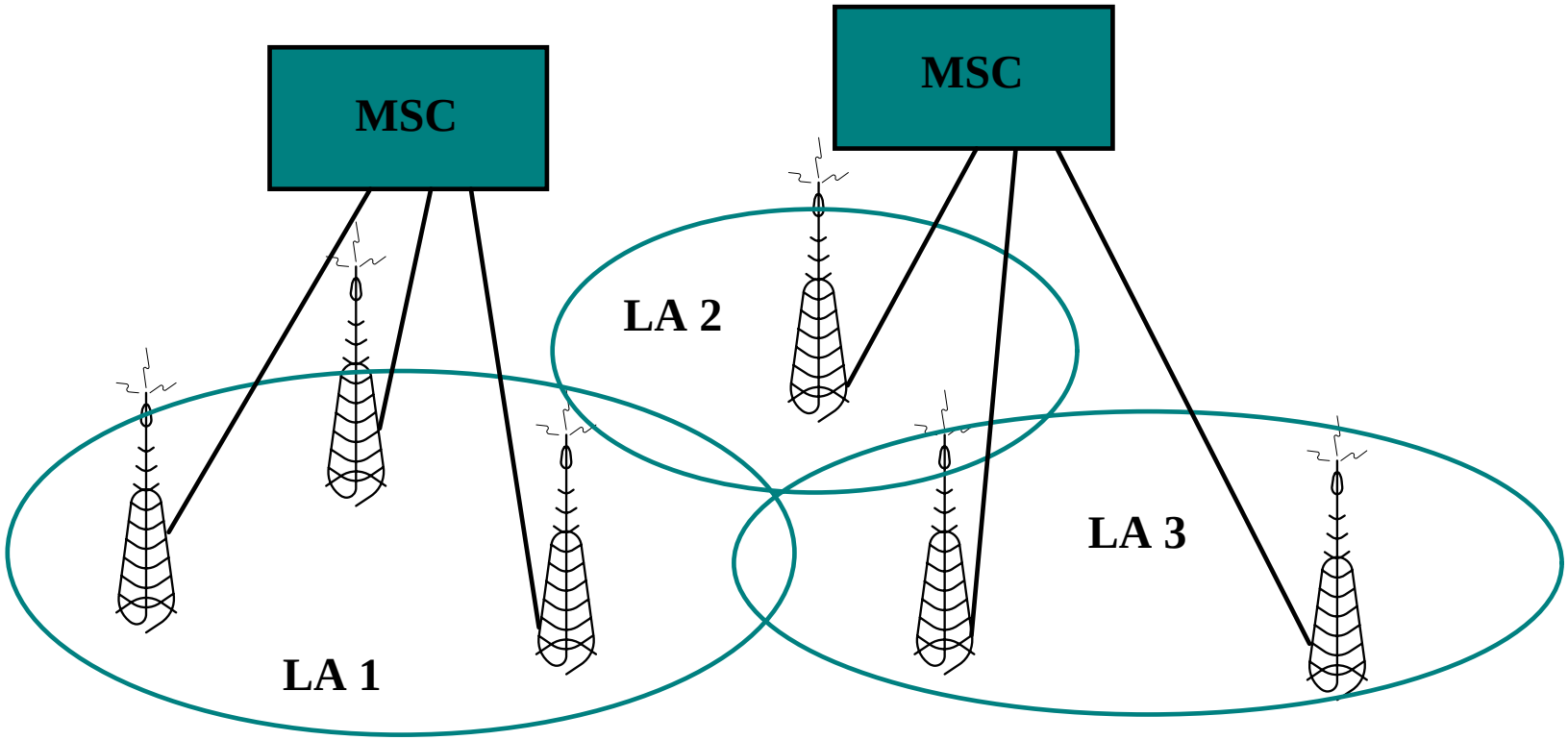
GSM 行動管理

- 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

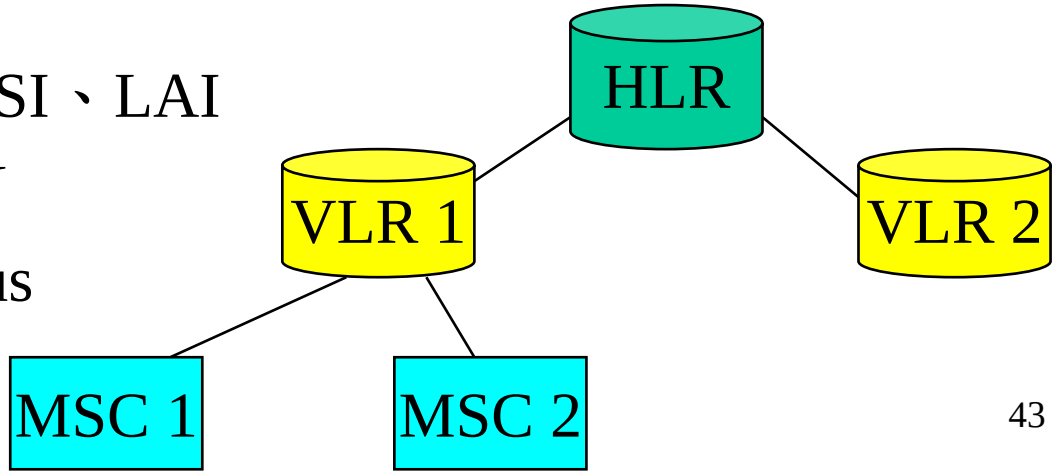
- GSM系統中和手機相關的識別號碼：
  - Mobile system ISDN (MSISDN)
  - Mobile Station Roaming Number (MSRN)
  - International Mobile Subscriber Identity (IMSI)
  - Temporary Mobile Subscriber Identity (TMSI)
  - International Mobile station Equipment Identity (IMEI)

圖 6-8 位置區域示意圖



兩層式的資料庫

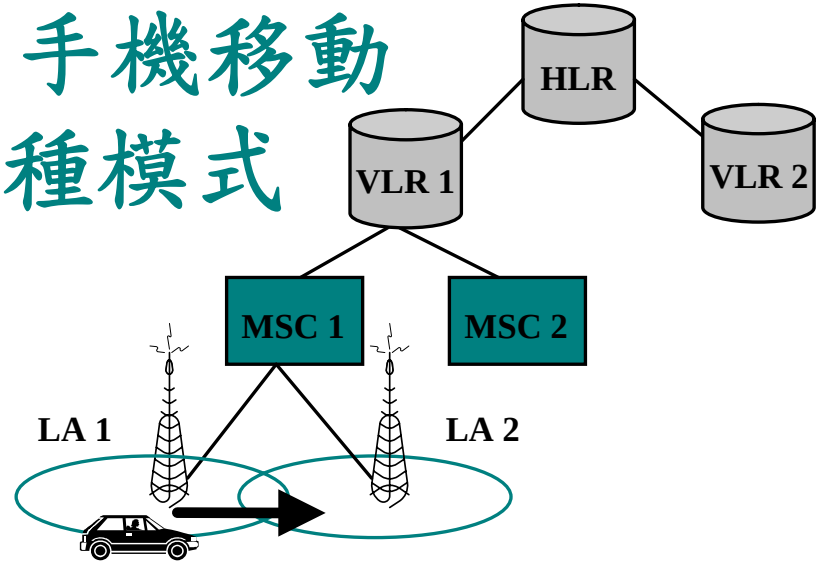
- 本籍註冊資料庫（Home Location Register，HLR）
  - MSISDN、IMSI、VLR ISDN、MSC ISDN與subscriber status
- 客籍註冊資料庫（Visitor Location Register，VLR）
  - MSISDN、IMSI、LAI
  - TMSI、MSRN
  - subscriber status



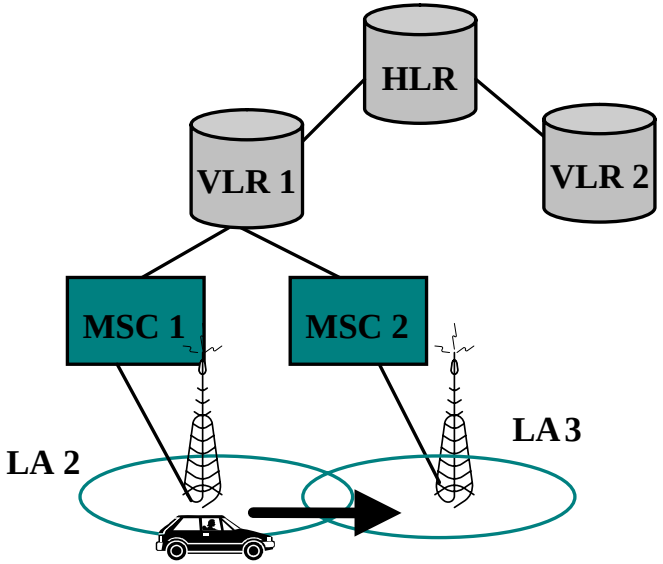
註冊程序

- 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。

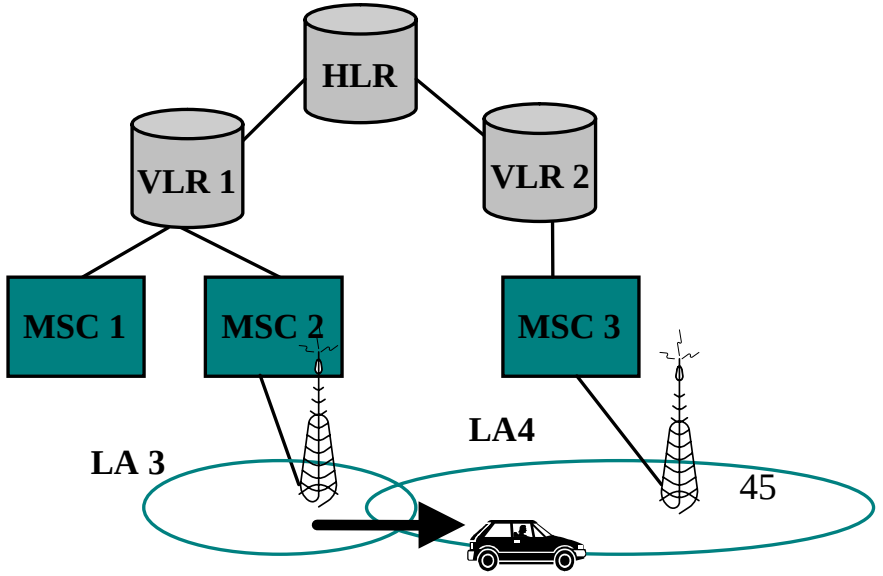
圖 6–9 手機移動的三種模式



(a) Inter-LA movement



(b) Inter-MSC movement



(c) Inter-VLR movement

圖 6–10 Inter-LA 的註冊流程

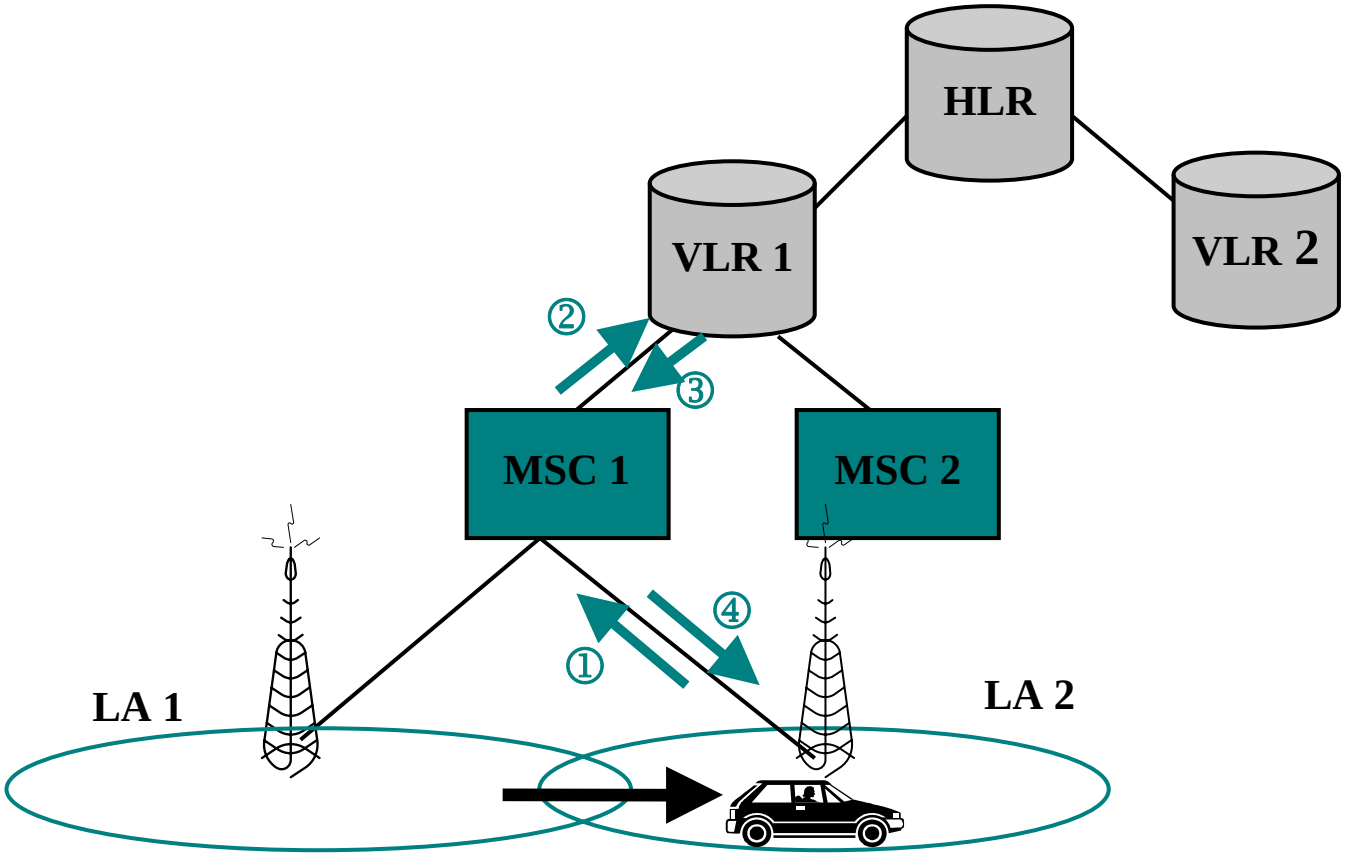


圖 6-11 Inter-MSC 的註冊流程

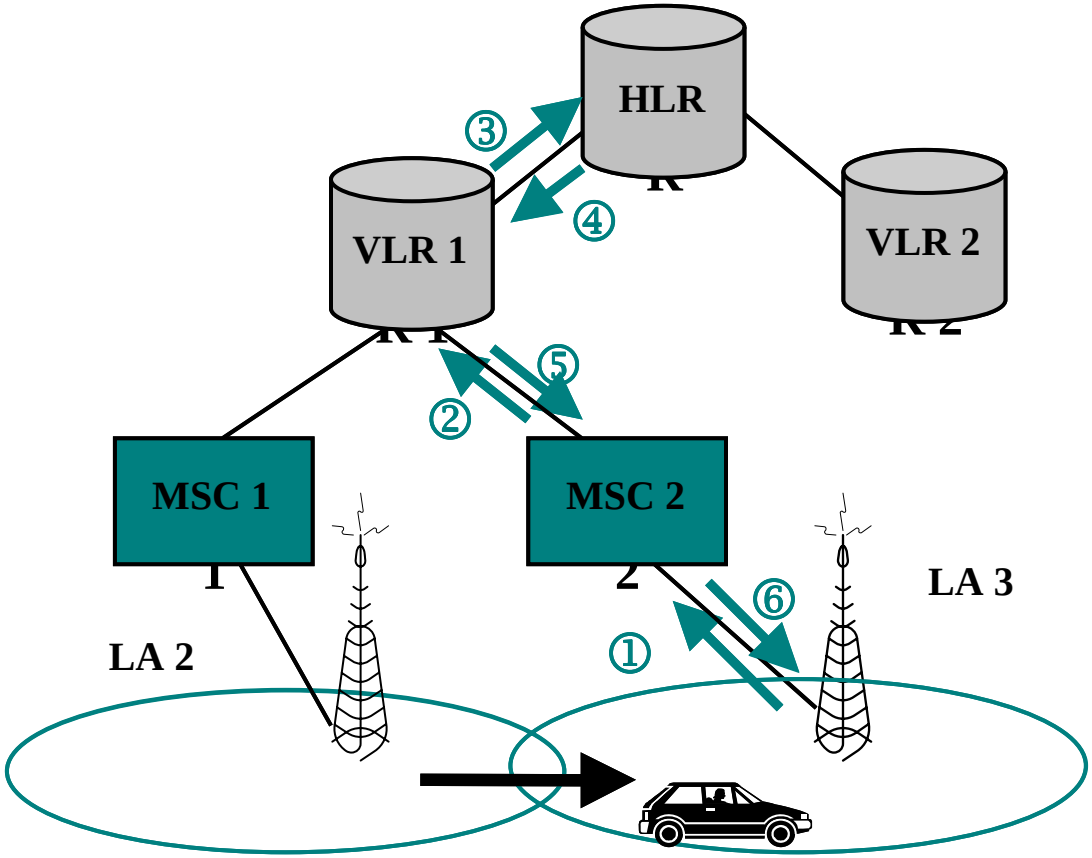
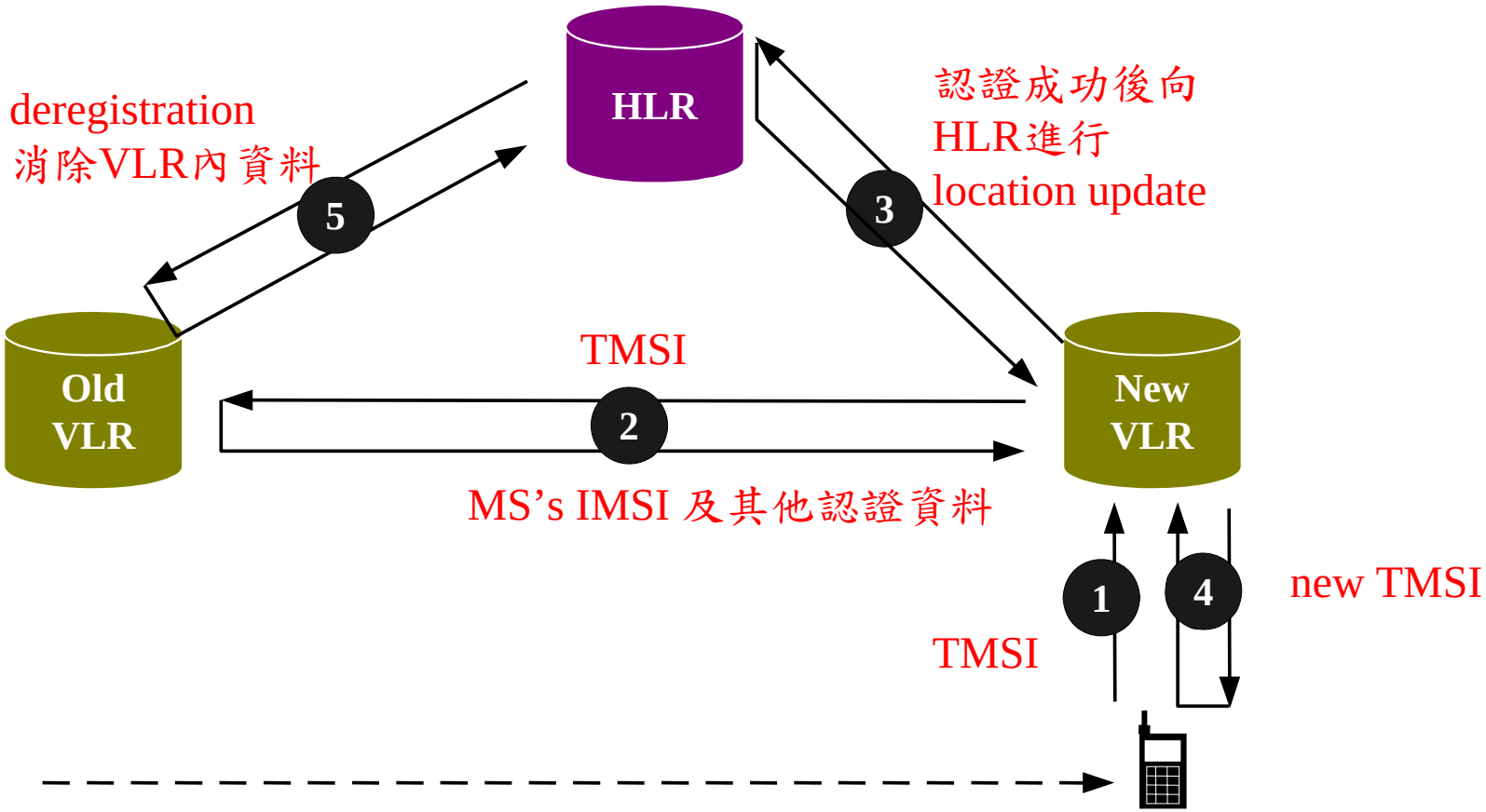


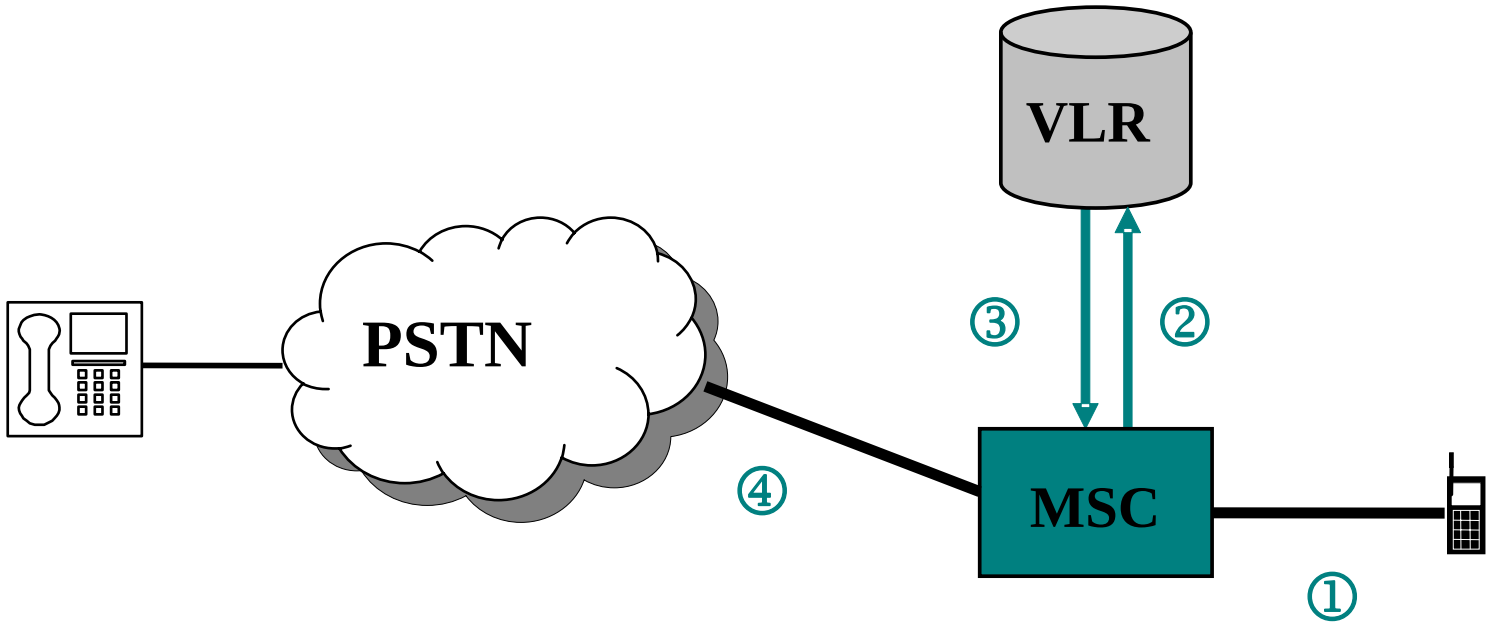
圖 6-12 Inter-VLR 的註冊流程



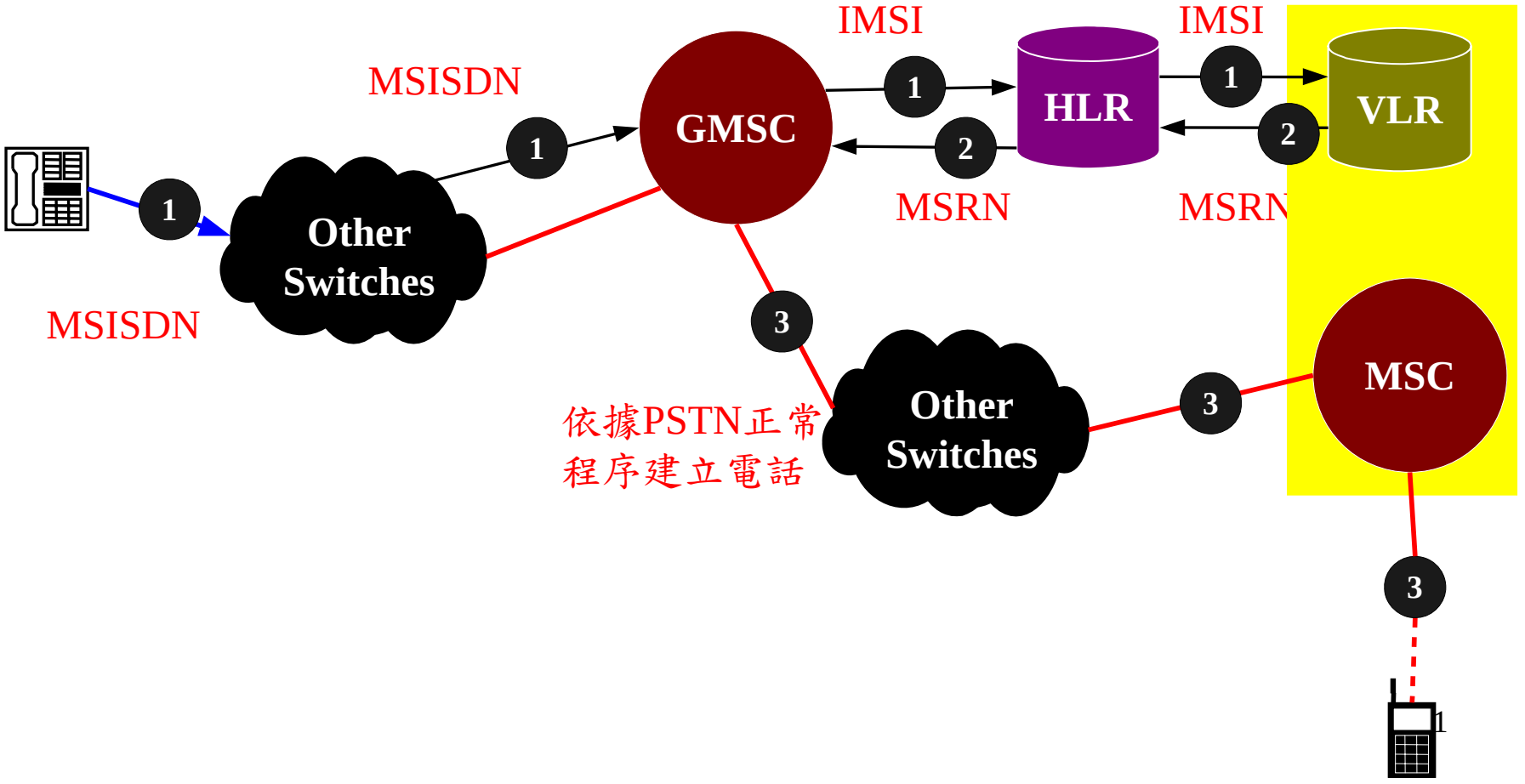
定期註冊（Periodical Registration）

- 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。

發話程序（Call Origination Procedure）



受話程序（Call Termination Procedure）



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

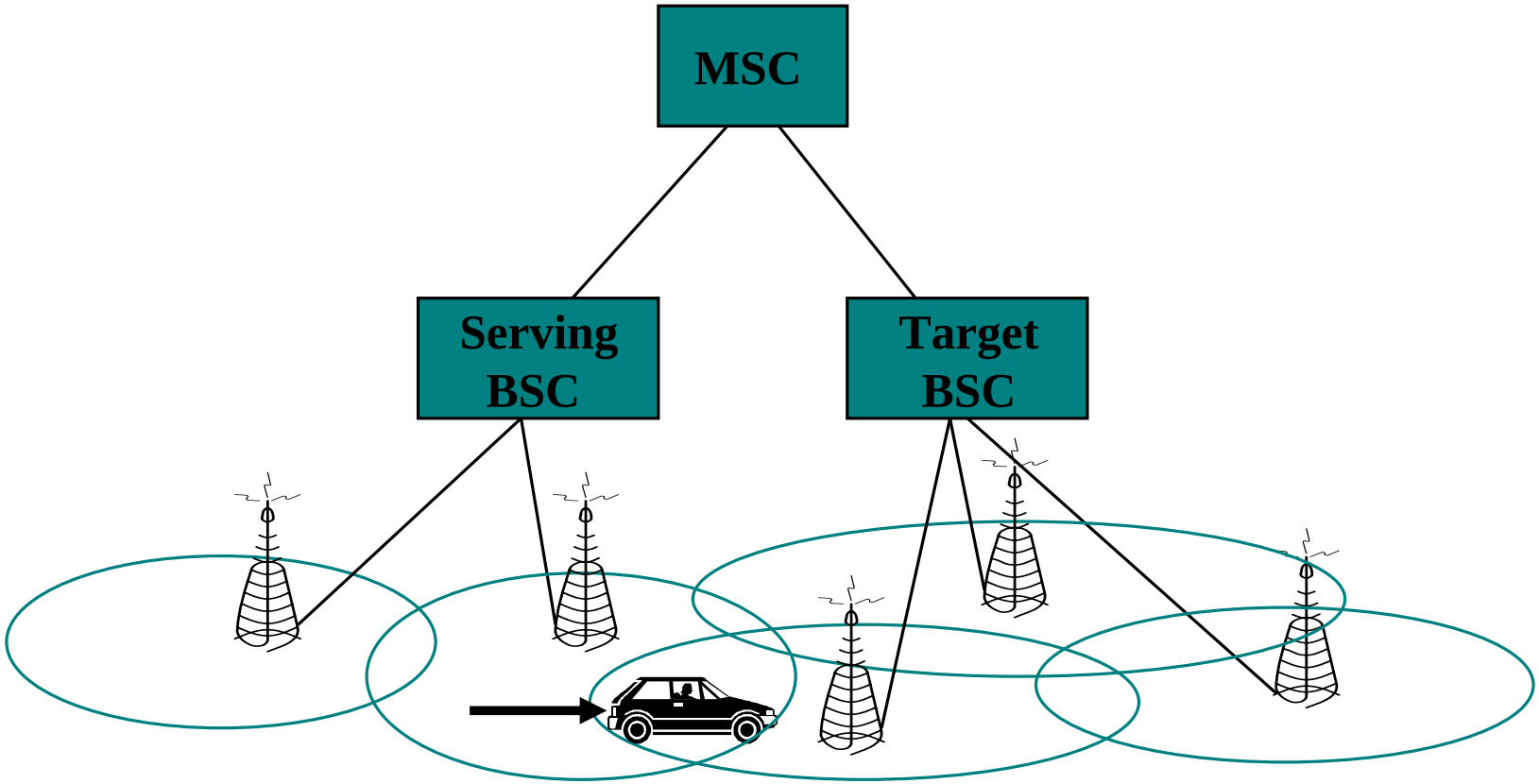
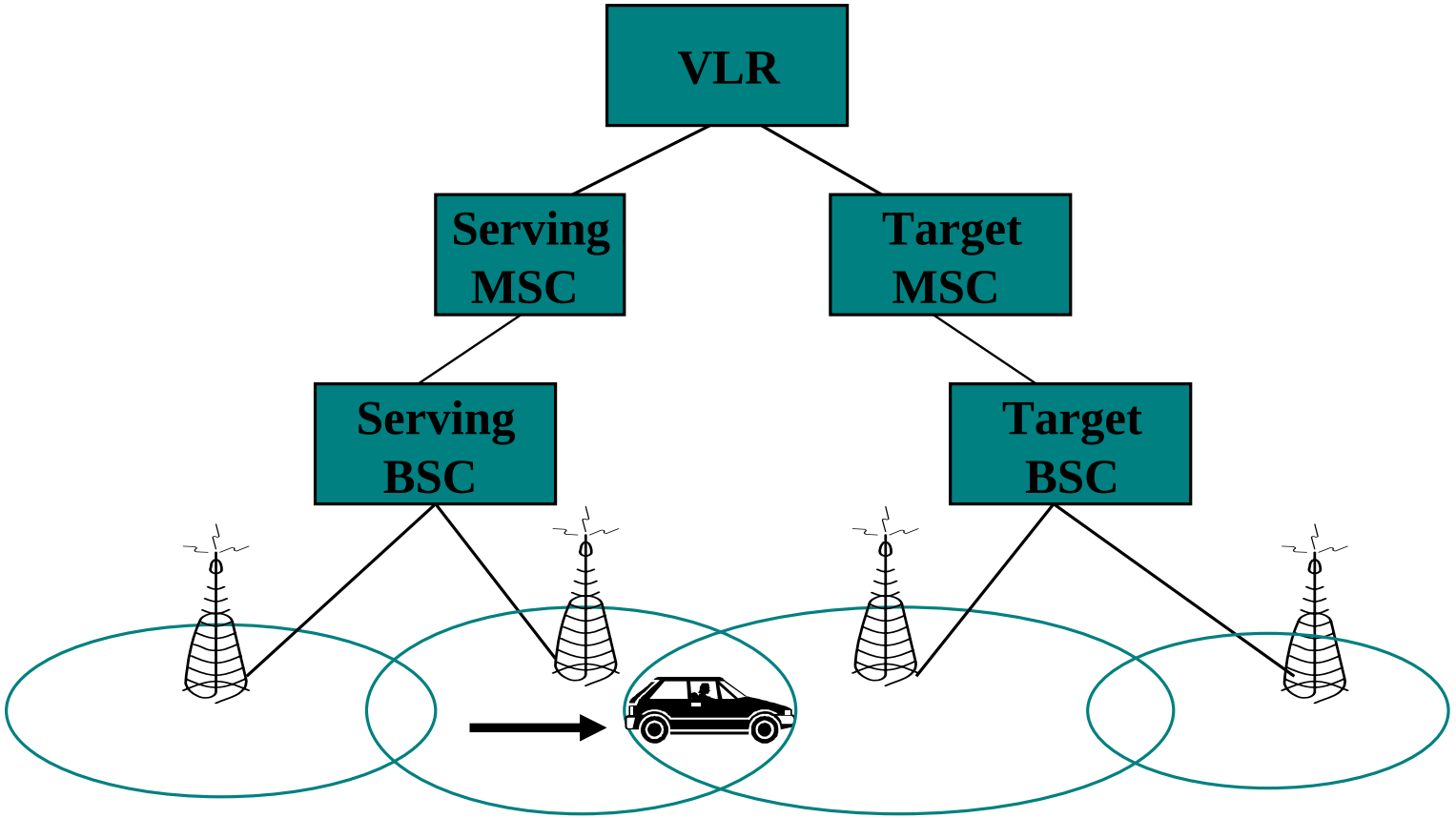


圖 6-16 Inter-MSC Handover



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。
  - 訊號加密（encryption）
    - ✓加密則是避免他人竊聽無線電鏈結的通話。

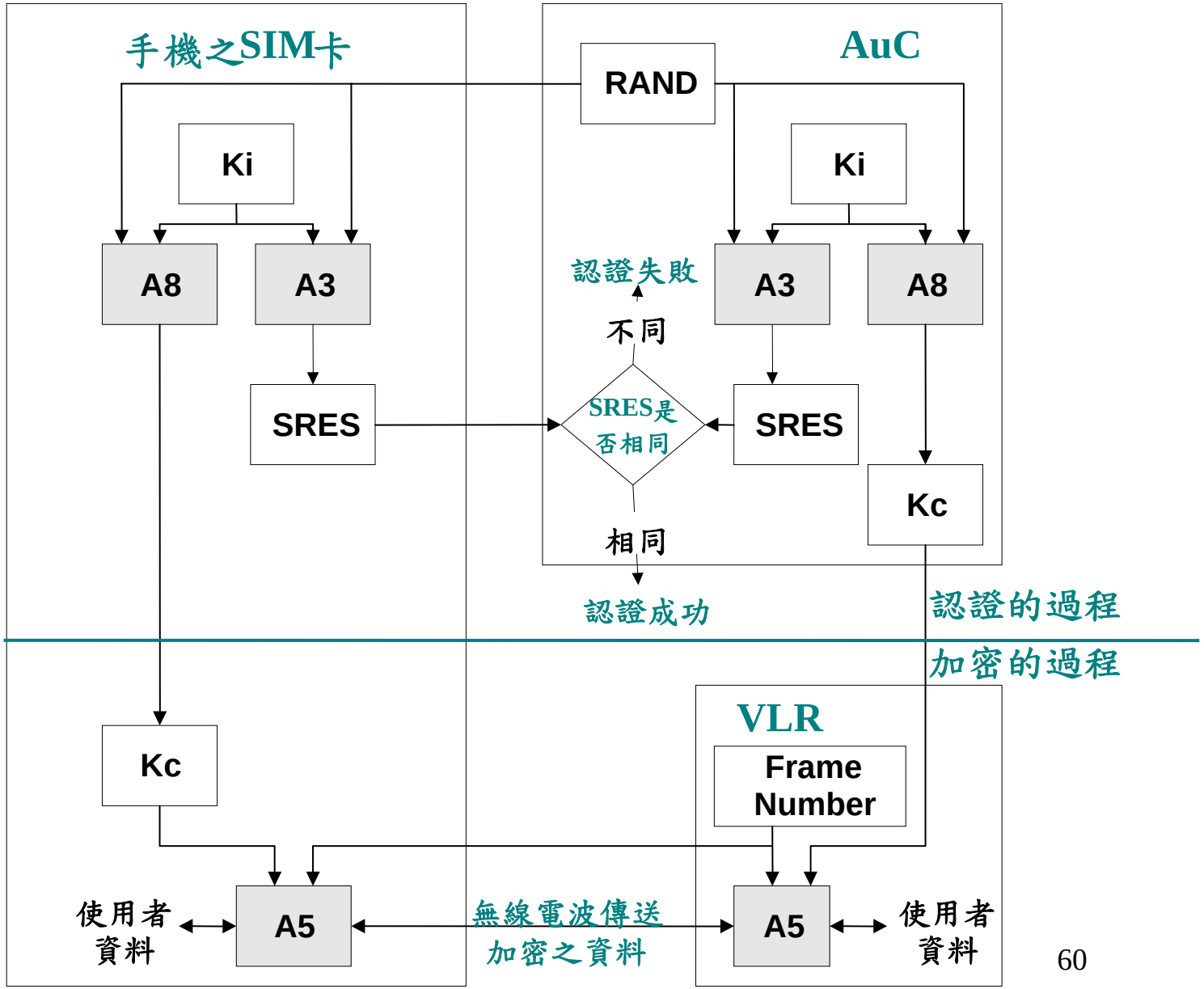
演算法

- 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。
- 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。

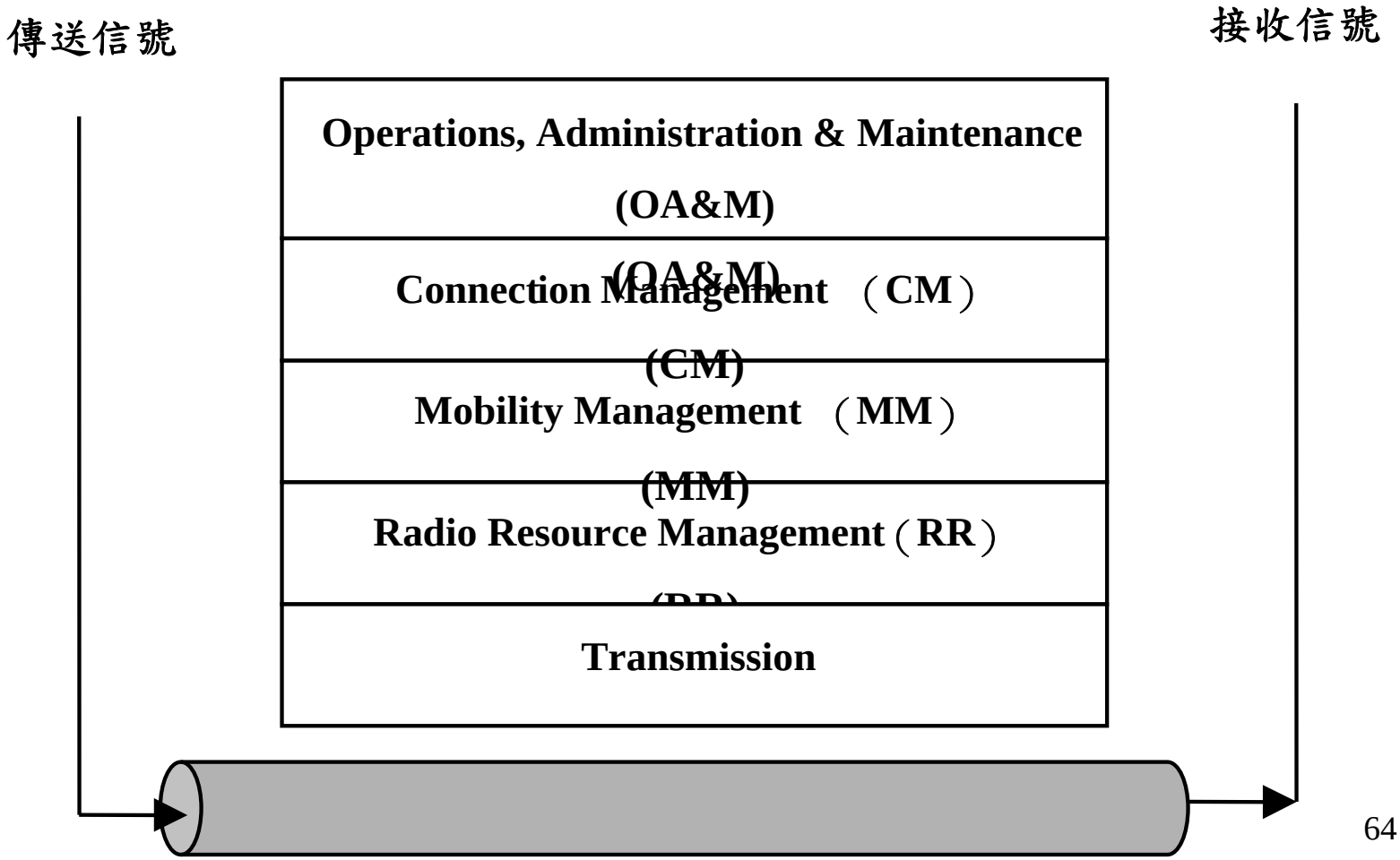
Section 6.6

GSM 功能性平面
GSM Functional Planes

GSM 功能性平面

- GSM 功能性平面描述 GSM 元件應如何運作以達到通話的目的。
  - 規劃各 GSM 元件應具備那些功能。
  - 元件間在達成特定功能時應該如何互動。
- 實作 GSM 系統，都是以 GSM 功能性平面做為基礎，把這些概念轉成實際的傳輸協定。
- 瞭解 GSM 功能性平面也會有助於瞭解 GSM 系統的運作。

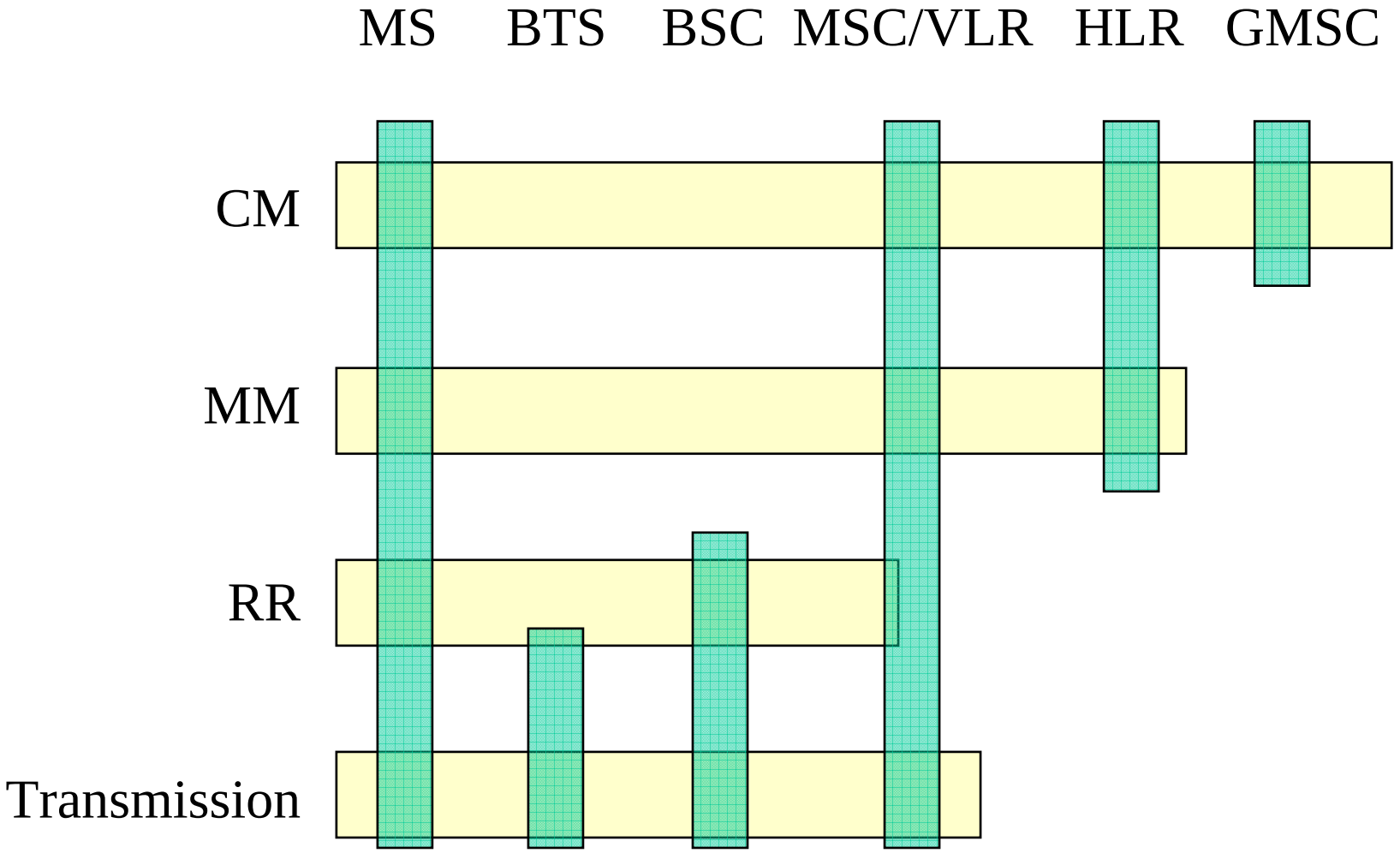
圖 6-18 GSM 功能性平面



傳輸平面

- 傳輸平面（transmission plane）
- 提供實體傳輸的方式，只與語音與資料的表示格式有關，確保使用者資料與控制信號都可正確的傳送到對方。
- 負責的工作項目包括調變（modulation）、編碼（coding）、多工（multiplexing）、格式化資料（format data）。

圖 6-19 GSM 元件與各功能性平面間的關係



無線電資源管理

- 無線電資源管理（Radio Resource management，RR）
- RR 管理無線電資源，負責建立 MS 到 MSC 間的連結（connection）。
  - 建立或釋放無線電鏈結。
  - 加解密。
  - 接收 MS 的無線電信號強度資料訊息的報告。
- 大部份 RR 的功能在 MS 與 BSC 執行，而 MSC 則會在 inter-MSC handover 時提供 RR 所需的功能。

行動管理

- 行動管理（Mobility Management，MM）
- MM 是行動通訊特有的功能性平面。
  - 管理用戶的資料庫，特別是位置的資訊。
  - 負責認證等安全事項。
- HLR、AuC、SIM 都與 MM 有關。
- MM 在 CM 的下層，代表 MM 與真實建立電話無關，且 MM 的完成（追蹤用戶位置）並不保證會建立通訊。

連結管理 (1/2)

- 連結管理（Connection Management，CM）
- 為使用者間建立電話或其他通訊服務，維護並在最後釋放資源。
- CM 可以分成 3 個子平面
  - 通話控制（Call Control，CC）
  - 增添服務管理（Supplementary Service management，SS）
  - 簡訊服務（Short Message Service，SMS）

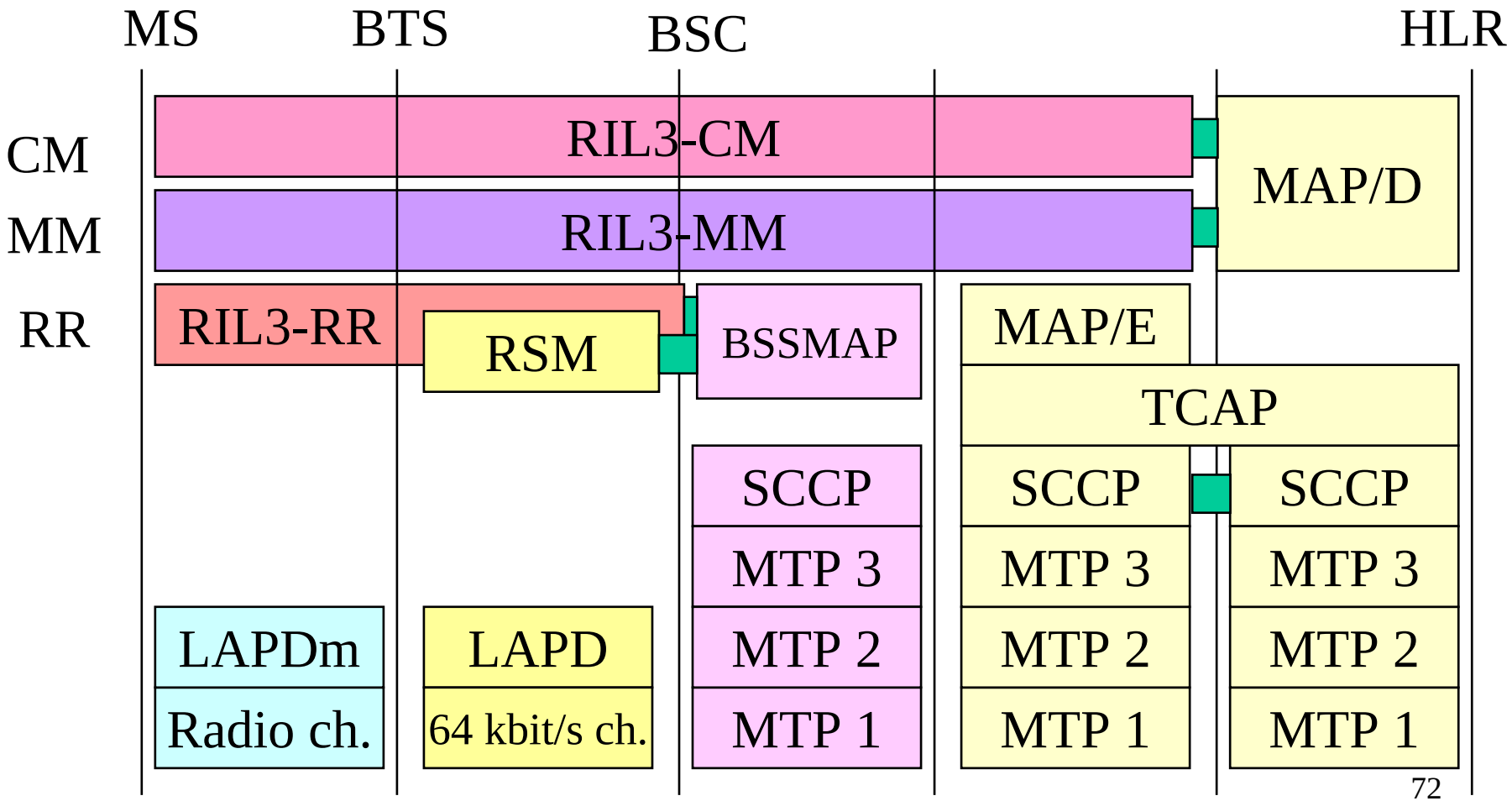
連結管理 (2/2)

- CC 選擇適當的傳輸路徑與方式，負責建立電話的所有事宜。
  - HLR、MSC/VLR 與 GMSC 都與 CC 相關。
- SS 是 GSM 在基本電話服務外，提供如電話轉接或話中插撥等服務，可以控制使用者電話進行的方式。
- SMS 是利用 GSM 的信令控制通道，傳送使用者資料。

營運管理維護

- 營運管理維護（Operations，Administration & Maintenance，OA&M）
- 管理各個傳輸設備，提供系統營運者監督，控制與操作系統的方法。
  - 觀察系統目前通話流量的控制
  - 測試備用的機器是否能立刻啟動
  - 追蹤進行電話的狀態
- OSS、 BSS 與 NSS 都會參與到 OA&M。

GSM 信令部份的通訊協定



Section 6.7

簡訊系統

Short Message Service，SMS

簡訊 (1/2)

- 簡訊透過控制通道（主要是**SDCCH**，偶而搶**SACCH**）來傳送簡訊。
  - 每一則簡訊能只有140位元組的資料量。
- 使用儲存與轉送（store and forward）的技術。
  - 簡訊儲存於稱為 SMSC（Short Message Service Center）的設備之中。
  - IWMSC 與 SMS GMSC 基本上都是 GMSC，均具備收送 SMS 的功能。
  - 參考圖 6-20 。

簡訊 (2/2)

- SMS 為 CM 上的一個子系統，所有簡訊不論在無線電通道或是在 GSM 核心網路上，都是透過信令系統來傳送。
  - 要追蹤接收者手機的所在，需要 MM 的幫助。
  - RR 支援 **SDCCH** 等通道的使用。
  - 網路端的資料則是在 GSM MAP 上傳送。
- 簡訊的特色：
  - Low capacity
  - Cheaper
  - Best-Effort
  - Non Real-Time

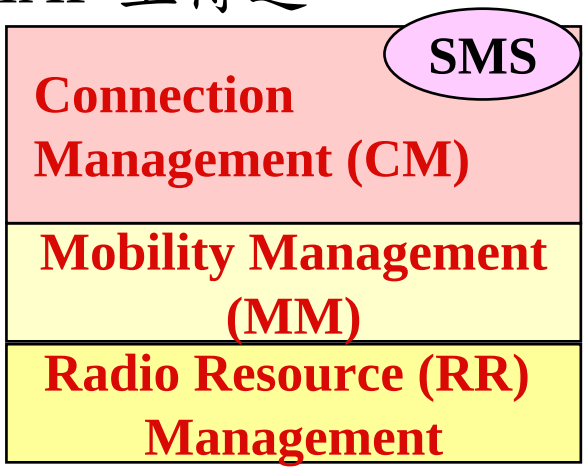
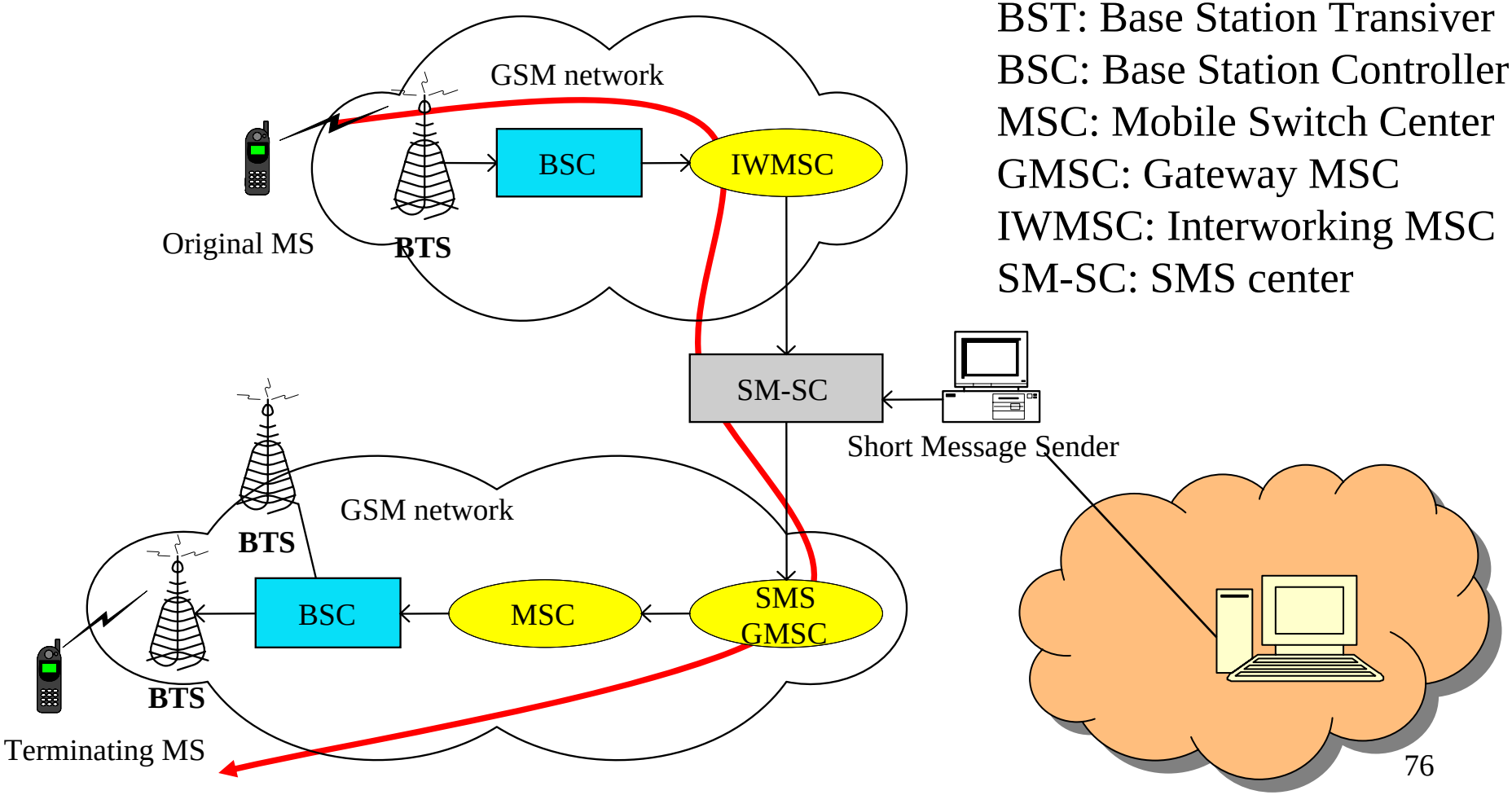


圖 6-20 SMS 的架構



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

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