

GSM System Overview

1

- 是 GSM 系統的入門，介紹 GSM 的各個子系統、無線電介面、手機註冊與打電話流程、安全性考量、資料傳送服務等基本常識。
- GSM 全名 Global System for Mobile Communication, 也稱為 Group Special Mobile, 泛歐數位式行動電話系統, 是現今具有最大佔有率的第二代行動通訊系統。
- 在探討 GSM 協定與架構的過程中, 會發現 GSM 與其他有線無線的通訊協定有許多相類似的地方. 那是因為 GSM 有許多 features 是依據 AMPS 與 IS-4, ISDN, 所以有許多它們的影子。
- 例如, 1984 年, 制定 network architecture, signaling protocol, open interface 的 GSM3 (a working group of GSM) 受到 ISDN 原則的鼓勵, 因此 service definition 和 signaling protocol 受的 ISDN 很大的影響. 其中之一, 便是使用 OSI (Open System Interconnection) 的 layered model.

Reference (1/2)

- [1] Wireless and Mobile Network Architectures ,
Y-Bing Lin and Imrich Chlamtac , Wiley
Computer Publishing.
- [2] Mobile and Wireless Networks , Uyless
Black , Prentice Hall.
- [3] The GSM System for Mobile Communication ,
Michel Mouly and Marie-Bernadette Pautel ,
published by the authors.

Reference (2/2)

- [4] Wireless and Personal Communications Systems , Vijay K. Garg and Joseph E. Wilkes , Prentice Hall.
- [5] Introduction to GSM , 陳俊宏 , 遠傳電訊教育中心。
- [6] GPRS and 3G Wireless Application , Christoffer Andersson , Wiley Computer Publishing.

Outlines

- Introduction
- GSM Architecture
- Air Interface
- Location Tracking and Call Setup
- Security
- GSM Data Services
- Unstructured Supplementary Service Data
- Summary

4

- 這個主題共分為以下幾個章節:
 - 先簡介 GSM 系統架構, 說明 GSM 的無線電頻道的使用方式.
 - GSM 會在資料庫中記錄手機的資料, 如手機的位置. 這部份在探討如何追蹤手機目前的位置, 來電時如何將電話轉接到手機所在的 BS.
 - GSM 為了避免手機被盜用與竊聽, 提供一系列認證與加解密的演算法.
 - 除了語音外, GSM 也提供數據資料的傳輸服務, 包括 HSCSD, GPRS 與 EDGE 的簡單介紹.
 - 提供多樣的應用, 可以增加系統的使用量, USSD 是一種 GSM 提供服務的方式, 像即時股務查詢便可透過 USSD 方式來實作.
 - 最後是 summary.

Introduction

5

- 簡介發展 GSM 技術所遵循的目標.
- 以下是 GSM 簡單的記事:
 - 1982 在 CEPT 內成立 “Group Spécial Mobile”
 - 1986 成立 Permanent Nucleus, 負責 GSM 標準的核心單位
 - 1987 選定 Main radio transmission techniques
 - 1989 GSM 成為 ETSI technical committee
 - 1990 Phase 1 GSM 900 定案, 開始改編 DCS 1800
 - 1991 First system 開始運作, DCS 1800 規格定案
 - 1992 所有在歐洲的 GSM 900 開始商業化

Introduction

- **G**lobal **S**ystem for **M**obile Communications (**GSM**) is a **digital** wireless network standard.
- It was developed by Group Special Mobile of Conference Europeenne des Postes et Telecommunications (**CEPT**) and European Telecommunications Standards Institute (**ETSI**).
- GSM Phases 1 and 2 define digital cellular telecommunications system.
- GSM Phase 2+ targets on Speech Codec and Data Service.

6

•GSM標準是由歐洲電信標準協會（European Telecommunications Standard Institute 或 ETSI）所製定的一種無線數位網路標準，目的在提供共通的服務給歐洲所有GSM使用者。

•ETSI 發展 GSM 的目的是要結束各系統不相容的問題, 所以要創造出一個全歐洲共同的 communication system structure. 但由於系統性能優越,而在全球電信市場上有極高的佔有率.

•GSM規格持續在演進中, 每一個階段有不同的訴求

•階段1, 2 主要是要發展蜂巢式數位通訊 (phase 1 只提供基本的服務如 call forwarding, call barring(除外), phase 2 加入像 fax 等 supplementary services), 階段2+在發展語音編碼技術與資料傳送的服務.

•GSM 想要包含許多常見的 services: speech, message handling (such as X.400), fax, emergency call (119), data service 等.

The Basic Requirements of GSM

(1/2)

- Basic Requirements set out by GSM
 - Original text as written by the committee in 1985
- Services
- Quality of Services and Security
- Radio Frequency Utilization
- Network
- Cost

7

•在一開始發展GSM技術,便訂下一些5個基本的需求,做為發展設計技術的依據.

•服務 (services)

- 不論手機在那一個已參與國際漫遊的地區,手機都應獲得系統業者的服務。i.e., GSM系統應提供服務的可攜性 (service portability)。
- 除了基本的電話服務外,應允許有最大的彈性以提供其他各種型態的服務,例如 ISDN-related services.
- 有線電話網路 (PSTN/ISDN) 已提供的服務與專屬於行動通訊的服務, GSM系統都需盡可能的具備。還要提供其他的設備,使行動通訊得以實現.
- 不論是在步行、車輛行走或是航行的船隻, GSM系統必須供應服務給所有不同行動能力的手機。但禁止在航空上使用 GSM.
- 除汽車外, GSM 應提供手持 MS 或其他種類的 MS 服務.

•服務與安全的品質 (quality of services and security)

- 從客戶使用的觀點, GSM電話的語音品質至少需優於類比式行動電話系統。
- GSM系統必須在不嚴重影響 "不需使用加密功能的用戶成本" 的考量下,提供使用者資訊加密的能力。

The Basic Requirements of GSM

(2/2)

- Basic Requirements set out by GSM
 - Original text as written by the committee in 1985
- Services
- Quality of Services and Security
- Radio Frequency Utilization
- Network
- Cost

8

•無線電頻道的使用 (radio frequency utilization)

- GSM系統在合理的成本下, 選擇能具有高無線電頻道使用效率, 和儘可能使用現有已成熟的用戶設備, 同時提供都市與鄉村地區新的服務。
- 系統應可在整個 890-915 MHz 和 935-960 MHz 間運作。
- 系統需能在整個配置的頻道上運作, 並與先前使用同一頻道的系統並存。

•網路 (network)

- 通訊網路系統上的元件識別碼 (identification plan) 與電話號碼的規劃 (numbering plan)應依據ITU Recommendation的定義。
- 系統設計必須允許不同網路使用不同的計費 (charging) 結構與費率。
- 通訊網路的交換與行動資料庫之間, 必需使用國際性的信令標準。
- 現存固接式公共網路不應為和 GSM 合作而被大幅修改。
- 在系統內必須做到 signaling information 與 network control information 的保護。

•成本 (cost)

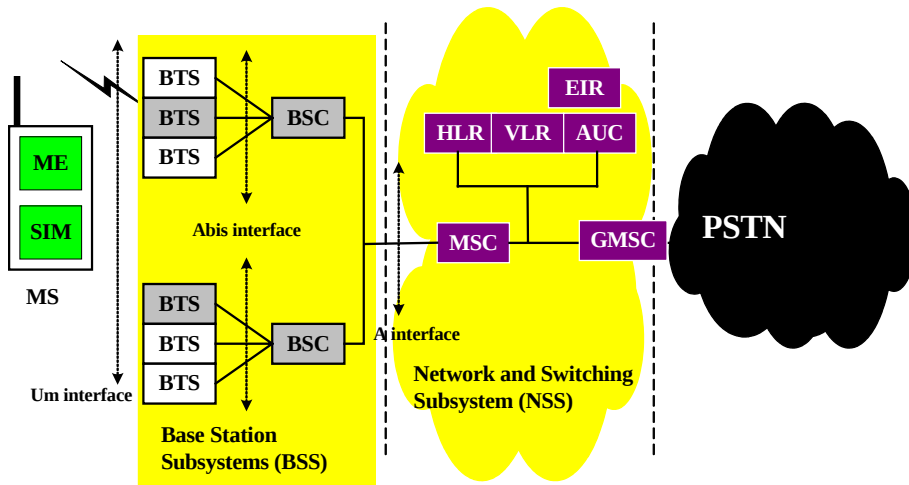
- 應從降低整體系統成本, 特別是手機的成本來考量系統參數的設定。

GSM Architecture

9

- 這個章節在說明GSM網路的架構,即GSM網路可視為那一些子系統的組成,並就各個子系統分別說明.

GSM Architecture



10

- GSM的手機（Mobile Station）透過無線介面（radio interface Um）與基地台系統（Base Station System或BSS）相互通訊。
- 基地台子系統以A介面（A Interface）連結到行動交換中心（Mobile Switching Center或MSC），與網路及交換子系統（Network and Switch Subsystem或NSS）相聯結。
 - 不同廠商中, NSS 也稱為 Switching system, BSS 也稱為 Base Station System.
- 因此GSM網路至少包含手機,基地台系統,後端的網路及交換子系統,三大部份.事實上還有一個網路營運中心負責監控整體網路的運作,如alarm的處理與問題的排除.
- 除此之外,要特別注意每個元件間都有制定標準的溝通（interface）,做為資料傳遞,控制訊令溝通的準則.
- 這裡面的 component 將會在後面慢慢介紹.

Mobile Station (MS)

- Also called Mobile Terminal (MT)
- The MS consists of two parts:
 - Subscriber Identity Module (SIM)
 - Mobile Equipment (ME)

11

- GSM手機由兩個部份所組成：第一個部份為使用者認證模組（Subscriber Identity Module或SIM），第二個部份為手機通訊模組（Mobile Equipment或ME）。
- 還把手機當成數據機使用，與終端設備(Terminal Equipment, TE)如PDA或PC相接。TEs 透過可手機來傳送語音或資料。



SIM



- A SIM contains subscriber-related information
 - A list of abbreviated and customized short dialing numbers
 - Short message
 - Names of preferred Networks to provide service
- **Personal Identity Number (PIN)** .
- SIM information can be modified:
 - By the subscriber either by keypad or a PC using an RS232 connection
 - By sending codes through short messages (network operators)

12

•SIM 是一智慧卡（記憶體晶片），專門儲存與使用者相關的資料。SIM有各種形式,我們現在最常見的為 plug-in SIM.

•SIM 可存電話名單（customized dialing numbers）與短訊息（short message），以及其他使用者相關資料。

•SIM有PIN與PUK.

•[4] SIM 包含下面資訊: IMSI + Ki + Subscriber information + Access control class+ Kc* + TMSI* + Additional GSM service* (如簡訊, 簡速撥號號碼)+ LAI* + Forbidden PLMN* (禁用) + PIN + PUK + BCCH Frequency List + Preferred (優先選用) PLMN list

•* means that term is updatable by the network (i.e,暫時的系統資料). 這些參數之後都有說明.

•另外有安全程序演算法(A3,A5,A6),Ki是這些演算法中用於驗證用戶的號碼,

•為了保護SIM卡不被他人使用,SIM 需以個人識別碼（Personal Identity Number或PIN）啟動,所以每次開機時都要輸入PIN。

•PIN為4到8個數字長的密碼. 設定方式: 按**04*舊PIN*新PIN*新PIN#

•若忘了PIN號碼,在嘗試輸入PIN但有3次錯誤之後,SIM卡就會被鎖住使門號無法使用.此時要向申請門號的廠商要求取得另一個數字PUK (PIN Un-lock Key),來解開被鎖住的SIM卡.但若自行嘗試輸入10次錯誤的PUK後,SIM卡就永遠被鎖定了 [5]. 設定方式: 按**05*PUK*新PIN*新PIN#

•[5]傳統的SIM的記憶體容量為8k或16k,提供主要的確認客戶及提供服務.

•[5]第二代的SIM使用32k的記憶體晶片.提供SIM Toolkit (STK) 功能. 可以

Mobile Equipment (ME)

- ME: non-customer-related hardware and software specific to the **radio interface**
- ME can not be used if no SIM is on the MS.
 - Except for emergency calls
- The SIM-ME design supports portability:
 - The MS is the property of the subscriber.
 - The SIM is the property of the service provider.

13

•通訊模組 ME 則包括一切與基地台通訊所需之無線軟體及硬體,包括控制模組與無線電模組。

•如此設計可使得

- MS 代表用戶.

- SIM 提供關於服務提供者相關資料. 當換不同系統, 手機過時, 只要不換 SIM 就不會改變.

•當 SIM 由手機取出後, 剩下之 ME 無法單獨使用。唯一例外為緊急電話 (美國之911或國內之119) 之撥話, 緊急電話是不須經由SIM。

•SIM 必須可以與不同的手機通訊模組相結合, 只要此手機 ME 的設計可與 GSM網路相容。

•當GSM手機初次和GSM網路接觸時, 手機通訊模組之特徵指數 (classmark) 會送至GSM網路, 而GSM網路則利用特徵指數來提供適當的無線介面與該手機連絡。

•平時不打電話時,只有在特定burst,才要醒來監聽 BS 的 broadcast 是否有來電 (稱為 idle mode)。

•為了手機省電,只有在打電話傳語音的時候, 系統才會分配MS一個專屬的 carrier (進入 dedicated mode), 也只有真正要傳語言時, 才會啟動 MS transmitter。

Base Station System (BSS)

- The Base Station System (BSS) connects the MS and NSS.
- BSS contains
 - Base transceiver station (BTS)
 - Base station controller (BSC)



14

- 基地台系統連接手機及GSM交換機。
 - BSS與MS間傳送與接收訊號
 - BSS會調節本身的電力消耗,可以省電也減少干擾.
 - BSS會測量手機的訊號強度,以告知手機進行功率控制.
- 基地台子系統包括兩個部份：基地收發台（ Base Transceiver Station或BTS ）及基地台控制器（ Base Station Controller ）。
- 通常 BTS 與 BSC 會放在一起, 或者 BSC 與 MSC 放在一起.

BTS

➤ Base Transceiver Station (BTS) contains

- Transmitter
- Receiver
- Signaling equipment specific to the radio interface in order to contact the MSs.
- **Transcoder/Rate Adapter Unit (TRAU)**
 - ✓ GSM-specific speech encoding/decoding and rate adaptation in data transmission

15

- 基地收發台 BTS 是 GSM 與 MS 之間的溝通管道。
- BTS 包括發射器、接受器(天線)、與手機通訊的無線介面相關之訊號處理的設備。
- BTS會收集所有MS送來的 signal 測量數據, 轉交給 BSC, BSC 利用這些數據做 channel assignment, 一個低干擾的 channel 就被稱為是 idle channel.
- 在通話過程中, MS 與 BTS 都會執行 signal strength measurement.
- BSC與MSC間會進行語音資訊的速率轉換. 這是由傳輸編譯碼與速率轉接器單元 (transcoder/rate adapter unit或TRAU) 的硬體來負責, 處理資料傳輸時, GSM所訂定的語音編碼與解碼、速率調整。在 spec 中是 BTS 的 sub-part, 但許多時候 TRAU 是置於 MSC 與 BTS 間, 如 Ericsson 便放在 BSC 與 MSC 之間, 減少 BSC 與 BTS 間的資料傳送。
 - Transcoding: 轉換 PCM 編碼的資訊成 GSM speech 編碼的資訊.
 - Rate adaptation: 調整傳輸資料的速度 : MSC- 64kbps-TRAU-BSC- 16kbps-BTS. 16kbps 中包含 13 kbps的traffic和3kbps的signaling.
 - Ericsson 稱BTS為RBS, TRAU為放置於 Ericsson 稱為TRC (Transcoder Controller) 的單元中, 位置在 MSC-TRC-BSC-RBS. TRC 也負責 discontinuous transmission. 若發現語音中有 pause, 則 TRAU 會產生 comfort noise 給 MSC/VLR.

GSM BTS (in YZU 3307-2)



16

- 這是放在元智的 BTS.

BSC (1/2)

➤ Base Station Controller (BSC)

- Radio channel assignment
- Call Setup
- Handoff management
- Connect to an MSC
- Connect to several BTSs
 - ✓ Maintain cell configuration data of these BTSs.
 - ✓ The BSC communicates with the BTSs via the A-bis.

17

•基地台控制器 BSC 負責基地台子系統之線路交換功能，並與GSM網路之行動交換中心相連。

•基地台控制器負責無線線路之分配（allocation）及回收（release），與手機交遞（handover），建立電話(如BSC要求LA中的BTS對MS做paging, 分配 traffic channel 給 MS) 的管理。

•一個基地台控制器可與數個基地收發台相連。BSC 可對 BTS 做 cell configuration(如給予frequency hopping sequence, 決定 frequency, 設定 power等), 這些configuration 會存於 BTS.

•基地台控制器與基地收發台之間以ISDN協定所謂的A-bis介面交談, 底層用 E1 or T1, 走 LAPD (Link Access on the D Channel) 協定。

•在城市鬧區這樣高話務量的地區，基地台控制器可以僅與一個基地收發台連接。在此情況下，基地台控制器與基地收發台將結合在一起而不需A-bis 介面。

BSC (2/2)

- The processor load of a BSC:
 - Call activities (around 20-25%)
 - Paging and short message service (around 10-15%)
 - Mobility management (handoff and location update, around 20-25%)
 - Hardware checking/network-triggered events (around 15-20%)
- When a BSC is overloaded, it first rejects location update, next MS originating calls, then handoff.

18

- 對 BSC 而言, 容量的規劃是非常的重要.
- 通常BSC會維持在80%的使用率,
- 以下是統計在 busy hours 時, BSC 的使用百分比:
 - Call activities (around 20-25%)
 - Paging and short message service (around 10-15%)
 - Mobility management (handoff and location update, around 20-25)
 - Hardware checking/network-triggered events (around 15-20%).
- 萬一工作在重,BSC會依優先權選擇必要的工作.
 - 首先,MS位置追蹤的工作先放棄(因與真正賺錢的電話接通無立即的效應). 再次手機無法打電話,最後才是悠關客戶滿意度的Handoff call 被迫被切斷.

NSS (1/2)

- Network and Switching Subsystem (NSS)
 - Telephone switching functions
 - Subscriber profiles
 - Mobility management
- Components in NSS:
 - **MSC**: provide basic switching function
 - **Gateway MSC (GMSC)**: route an incoming call to an MSC by interrogating the HLR directory.

19

- 網路及交換系統 NSS (或稱為 Switching System) 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。
- NSS由MSC,GMSC, HLR, VLR, AuC 與 EIR 等組合。
- MSC 執行基本的線路交換功能, 可以想成是功能較強的交換機, 也要負責計費的功能。
 - MSC 經由 A 介面 (A interface) 控制數個BSS。
 - MSC 負責 call set up, manage, clear connection, routing a call to the proper cell.
 - MSC 負責處理 common channel signaling 做為與NSS端的介面。
- GMSC 是特殊的 MSC, 連接 2 個網路, 是 PCN 與 PSTN 等其他網路連接的 gateway。
 - 任何的MSC加上適當的軟體, 能與HLR和外界網路溝通, 就可當成是 GSMC。

NSS (2/2)

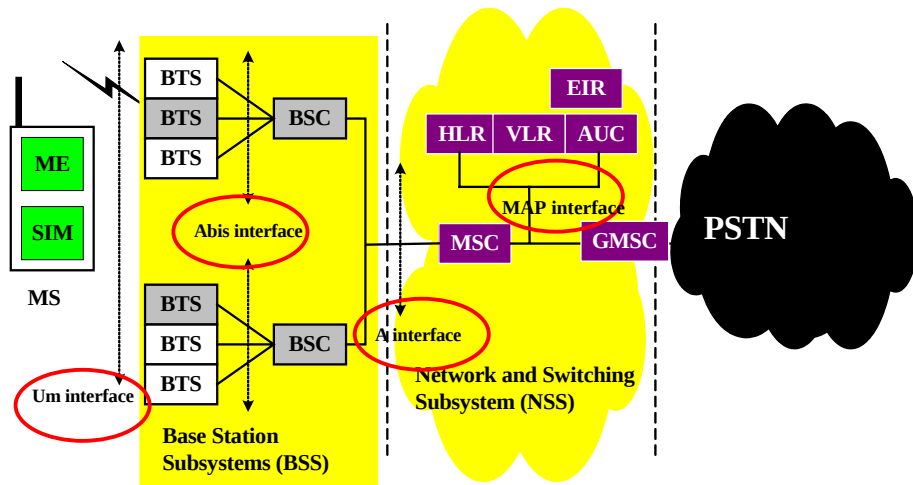
➤ Components in NSS (continuous):

- **HLR** and **VLR** maintain the current location of the MS.
- **Authentication Center (AuC)** is used in the security management.
- **Equipment Identity Register (EIR)** is used for the registration of MS equipment.

20

- HLR, VLR, AuC, EIR 都是一些維護用戶資料的資料庫。
- GSM網路利用 HLR 與 VLR 來尋找手機的位置。
 - HLR 提供用戶相關資訊, 如 IMSI, home subscription base, any supplementary services (ex: call forwarding), location of MS.
 - VLR 提供位在特定區域內用戶相關資訊, 包含用戶狀態 (switch on/off), any supplementary services.
 - VLR 的概念是為了減少到 HLR 的 traffic.
 - HLR 可以是 standalone 或和 MSC 做在一起, 但 VLR 通常會與 MSC 做在一起 (for Ericsson).
- 認證中心 (Authentication Center 或 AuC 或 AC) 的資料庫則用來認證用戶之真偽 ,
 - AuC 通常會與本籍註冊資料庫結合在一起。
- EIR 紀錄手機的型態,IMEI, 經由EIR的認證才確定是合理的手機. 通常用於當 MS 遺失時, 可以禁止手機打電話。
 - AuC/EIR 也可以 implemented together.

GSM Interfaces



21

- 在各個GSM元件間要互相溝通, 必須遵循一定的規範, 稱為介面 interface.
- 有下面這些主要常見的 GSM interface:
 - Um: MS與BTS之間的介面
 - Abis: BTS與BSC之間的介面
 - A: BSC與MSC之間的介面
 - MAP: MSC與其他資料庫 HLR, VLR, AuC, EIR 之間的介面.

Air Interface

22

- 這個部份說明 GSM 的 Air Interface, 包括 TDMA/FDD 的概念, Frame/ Burst 的架構, logic channels 的介紹, 用 call origination 與 call termination 做範例說明 logic channel 的使用方式.

Radio Interface - Um (1/3)

- The GSM radio link uses **TDMA/FDD** technology.
 - 890-915 MHz (uplink)
 - 935-960 MHz (downlink)
 - 124 pairs × 200 KHz
 - 8 time slots (bursts) per carrier
 - A frame consists 8 bursts (time slot) (each 0.577 msec for a time slot).
 - The length of GSM frame in a frequency carrier is 4.615 msec.

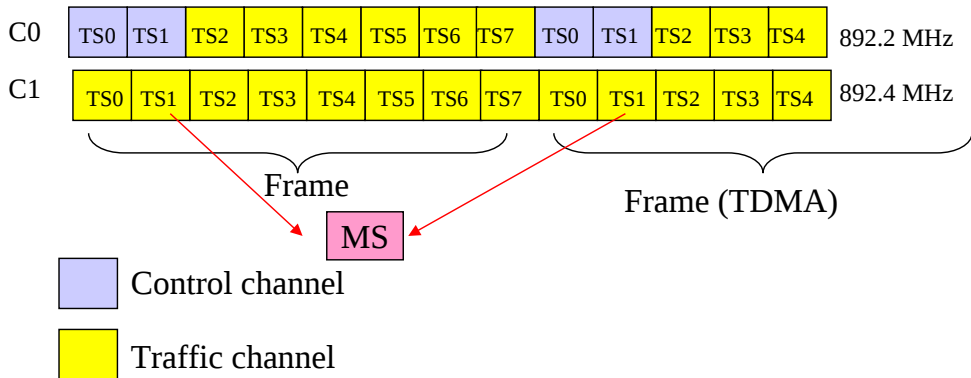
23

- The technologies of GSM are summarized as follows:
 - 由於空中的頻寬有限,所以GSM必須用一些方式使大家可以共享無線電資源: TDMA/FDD
 - 採用分頻雙工(Frequency Division Duplex, FDD),語音上傳與下傳走不同的頻道,所以需要一組(uplink 200kHz+downlink 200kHz)才能打電話.
 - 上傳 890-915 MHz for handset transmission (to BS), 共分成 124 carriers.
 - 下傳 935-960 MHz for base station transmission (to MS), 共分成 124 carriers.
 - Uplink與downlink各有25MHz的頻寬(Bandwidth)
 - FDMA:切割整個頻寬給各組頻道
 - 每個頻道間距為 200 KHz spacing, 所以共可分成 124 組
 - TDMA :每個頻道又依時間切割 4.615msec 的frame, 每個frame切成 8 個時槽.因此最多一個頻道可以給8個手機使用.
 - GMSK modulation
 - 當話務量多時, 可以再利用語音編碼的技術,在不影響太多音質的情況下將語音編碼量減半,提供更多人使用
 - 採用 13 Kbps RPE-LTP full-rate and 5.6 Kbps VSELP
- DCS 1800 與GSM 的技術差不多
 - 1710-1785MHz (uplink) and 1805-1880MHz(downlink)
 - Uplink與downlink各有75MHz的頻寬
 - 每個頻道間距為 200 KHz spacing, 所以共可分成 374 組
- 但因是所有GSM通訊廠商共享頻寬, 所以以遠傳為例只使用到:
 - 910.2-914.8MHz (uplink) and 955.2-959.8MHz(downlink)
 - 1732.6-1743.6MHz (uplink) and 1827.6-1838.6MHz(downlink)

Radio Interface - Um (2/3)

Downlink

FDMA



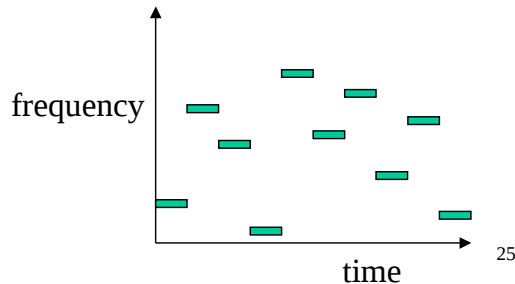
24

- GSM 的 TDMA 就是將每一個 carrier 依照時間切割成時槽(timeslot), 做為獨立傳送資料的基本單位.
- 每 8 個 timeslots 組成一個 Frame 最多可以分給 8 支手機使用, carrier 上不斷重覆著這些 Frame, 換言之, 8 個 MS 輪流使用這個頻道. 每支手機所得到的 timeslot, 就稱為一個通道 channel.
- 這些 channel 不見得都用於傳送語音, 有些要用於傳送控制資料. 傳送語音的稱為訊務通道(Traffic channel), 傳送控制訊號的稱為控制通道(Control channel).
- 每個 BS 需要兩個 channels 做為控制使用, 通常會選擇某一 carrier (稱為C0) 的第一個與第二個 timeslots (TS0, TS1) 做為 control channel. 其他做為 traffic channel.
- 若此 BS 有兩個 carrier (C0, C1), 則共有 $6 (C0) + 8 (C1) = 14$ traffic channels, 就是最多有 14 支手機可用此 BS 傳送語音或資料.

Radio Interface - Um (3/3)

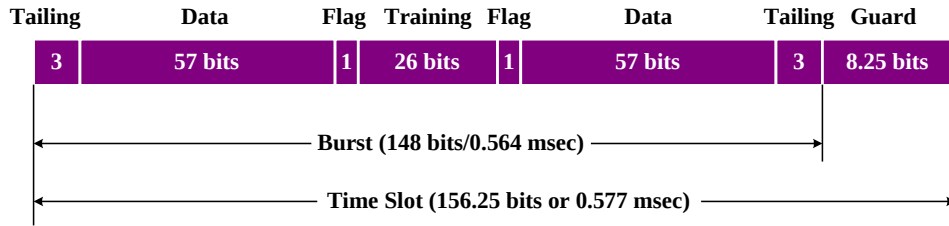
➤ To improve spectrum efficiency:

- Control of the transmitted power
- Slow frequency hopping
- Discontinuous transmission
- Mobile assisted handover



- 在 GSM 系統的設計中, 有許多的技術可增加頻道的有效性 (spectral efficiency), 雖然下面的方法會增加系統的複雜度, 但可在經濟效應上取得平衡:
 1. Control of the transmitted power (dynamic power control in MS and BTS): 在通話的過程中, 在維持一定的傳輸品質下, BS 和 MS 盡可能將平均的電力消耗減到最少, 也可減少對其他通訊的干擾 (interference). BSC 會利用 MS 測量訊號的數據, 每 480 ms 送出一控制信號, 決定 BTS 與 MS 的傳送 power.
 2. Frequency hopping: 透過慢速變換使用頻道, 將使用的頻道分散, 可增加傳輸的品質 (因為比較不會為固定某一範圍頻道被干擾而造成這些頻道都無法使用), 也可因為每一個通話中的頻道干擾的分散 (interference diversity), 增加 spectral efficiency.
 - GSM 定義 64 種 hopping sequence, 系統會分配不同的 hopping sequence 給不同的 carrier,
 - Fast frequency transmission 是傳輸一個symbol 就換許多頻道 (frequency change 比 modulation rate 高), security 較高.
 3. Discontinuous transmission: 依據 user data 的 type, 可萃取出有效傳輸的部份. 對於 speech, 利用 Voice Activity Detection (VAD) 的技術, 只需傳送有聲音的部份, (大約只剩下一半的資料量), 可以減少 interference.
 4. Mobile assisted handover: MS 提供對鄰近 cell 的測量, 讓 network 的 handover decision algorithm, 可以做 local optimization, 使 cell 所產生的 interference 減至最少.

GSM Burst Structure



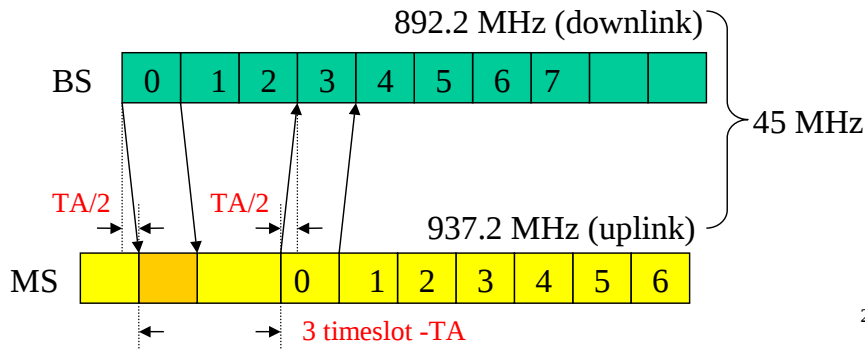
- Begin with 3 head bits, and end with 3 bits.
- Two groups are separated by an equalizer training sequence of 26 bits.
- The flags indicates whether the information carried is for speech/data, or signaling.

26

- GSM 的channel 都是以 burst 型式將資料放在 timeslots 中.
- Several burst formats are defined: normal burst, access burst, normal burst, F and S bursts for FCCH and SCH burst.
 - 上圖是 normal burst, 用於存放一般 traffic channels.
- Normal burst 中
 - 0.577 msec 中含 156.25 bits, 但 Data 只有 114 bits.
 - Three head and tailing bits are all logical zeros.
 - Training sequence is for synchronization.
 - Guard 是與下一個 burst 間的安全間隔.

Time Advance

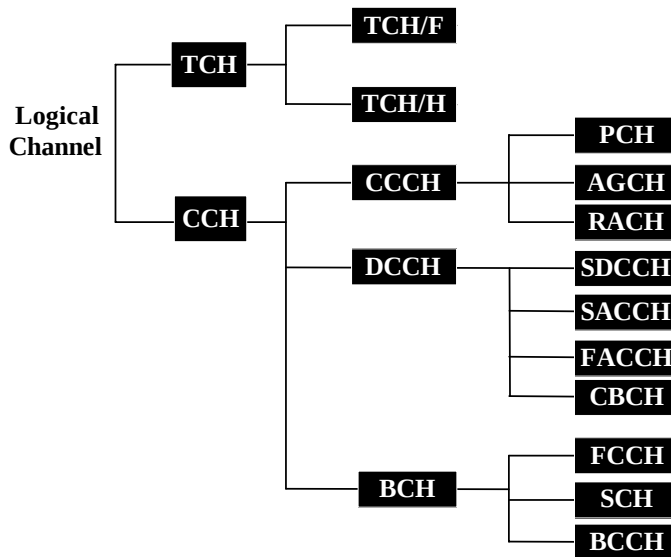
- **Timing Advance:** the exact shift between downlink and uplink seen by MS



27

- GSM 使用 FDD, uplink 與 downlink 使用不同的 timeslot, 在圖中, Downlink 後第三個 timeslot, MS 送出 uplink burst. 我們稱為 Traffic channel offset is 3 time slots.
- TA 是 BS 與 MS 的 round-trip delay, 若 BS 與 MS 間隔約 30km, round-trip delay 約為 0.2 ms.
 - 因為有 round-trip propagation delay, so MS 的發送時間要提前 TA.
 - The exact shift between downlink and uplink seen by the MS value is three time slots minus the timing advance value.
 - The timing advance (TA) is calculated by the BSS, based on the bursts received from the MS.
 - BS 會將 TA 傳送給 MS, 每秒兩次.
- 假設 MS 使用 time slot 2 傳送資訊, 則在 uplink 後, MS 會測量至少一個相鄰 cell 的信號強度.

Logical Channels



28

- 一個 BTS 與一個 MS 間用來傳送資訊的條通道稱為 physical channel.
- 在這個 physical channel 上依據所傳送的資訊來分類, 可劃分成許多 logical channels.
- GSM以多種的邏輯通道 (logical channels) 的概念來區分各系統控制訊號的用途與使用者資料, 與實際上無線電通道介面配置無關, 所以稱為 logical.
- 基本上, 分成 Traffic channel 與 control channel 兩大類.

Traffic Channel (TCH)

➤ **TCHs** are intended to carry user information (speech or data).

- **Full-rate TCH (TCH/F)**
 - ✓ Transmission speed: 13 Kbps for speech
 - ✓ Transmission speed: 9.6, 4.8 or 2.4 Kbps for data
 - ✓ **Enhanced full-rate (EFR) speech coders** for improving the speech quality
- **Half-rate TCH (TCH/H)**
 - ✓ Transmission speed: 6.5 Kbps speech
 - ✓ Transmission speed: 4.8 or 2.4 Kbps of data.

29

•資料傳輸通道（Traffic channel或TCH）是用來傳送使用者的語音或數據資料。

•依據資料傳送的速率區分, 分成 Full Rate 與 Half Rate。

•全速率資料傳輸通道（Full rate TCH或TCH/F）可傳送13Kb/s之語音或12、6、3.6Kb/s的數據資料。

•(Enhanced full-rate) EFR speech coders 可以用於增加語音的通話品質。

•1/2速率資料傳輸通道（Half rate TCH或TCH/H）則提供7Kb/s語音傳輸，或者是6或3.6Kb/s數位資料傳輸。

Control Channels (CCH)

- CCHs: to carry signaling information
- Three types of CCHs :
 - Common control channel (CCCH)
 - Dedicated control channel (DCCH)
 - Broadcast channel (BCH)

30

- 控制通道（Control channel或CCH）係用以傳送系統控制訊號（signaling）。
- 控制通道可分為數類, CCCH, DCCH, BCH。
- 這些通道的資源是由所有手機共享, 所以被稱為一般控制通道（common control channel）。

Broadcast Channels (BCHs)

- BTS broadcasts system information to the MSs through BCHs.
- Two types in BCH:
 - Broadcast Control Channel (BCCH) (downlink)
 - ✓ Access information for the selected cell
 - ✓ Information related to the surrounding cells to support cell selection
 - ✓ Location registration procedures in an MS
 - Frequency Correction Channel (FCCH) and Synchronization Channel (SCH)
 - ✓ The information allows the MS to acquire and stay synchronized with the BSS.

31

•FCCH、SCH、BCCH這些BCH是由基地台經傳送至手機的下行邏輯通道

•廣播控制通道（Broadcast Control Channel或BCCH）提供手機有關基地台的資料，手機便是利用這些資料來決定基地台的選擇及註冊程序之執行。

•頻率校正通道（Frequency Correction Channel或FCCH）及同步通道（Synchronization Channel或SCH）由基地台傳送至手機以維持二者間之同步

•FCCH 提供頻率校正的資訊，有連續的 142 個 0，可讓 MS 校正自己的頻率以維持BTS頻率上的同步。

•SCH包含Base Station Identity Code (BSIC) 和 Frame number，讓 MS 可以調整自己以和 BTS 的 frame structure 同步。

Common Control Channel (CCCH)

➤ Three types in CCCH:

- **Paging Channel (PCH)** (downlink)
 - ✓ Used by the network to page the destination MS in call termination
- **Random Access Channel (RACH)** (uplink)
 - ✓ Used by the MSs for initial access to the network
 - ✓ Collision may occurs.
 - ✓ Slotted Aloha protocol is used to resolve access collision.
- **Access Grant Channel (AGCH)** (downlink)
 - ✓ Used by the network to indicate radio link allocation upon prime access of an MS

32

•CCCH (Common Control CHannels) 用於傳送 point to point 的傳輸. 但是這些頻道是大家所共用.

•當有人要打電話給該手機，傳呼通道（Paging Channel或PCH）則用來呼叫手機。

•當手機要打電話，則手機可在隨機擷取通道（Random Access Channel或RACH）上，告知基地台欲使用無線線路。

•若數個手機同時使用同一個隨機擷取通道的時槽向基地台提出線路要求，便會造成碰撞（access collisions）。

•GSM使用分時槽Aloha協定（slotted Aloha protocol）來解決碰撞問題。

•基地台透過擷取允諾通道（Access Grant Channel或AGCH）告知手機其所要求使用的無線線路已獲基地台同意，可以開始通話。

•PCH 及 AGCH 是由基地台經傳送至手機的下行邏輯通道

•RACH 是由手機上傳至網路端的上行邏輯通道。

Dedicated Control Channel (DCCH)

(1/2)

- DCCH is for dedicated use by a specific MS.
- Four types in DCCH:
 - Standalone Dedicated Control Channel (SDCCH)
(down/uplink)
 - ✓ used only for signaling and for short message
 - Slow Associated Control Channel (SACCH)
(down/uplink)
 - ✓ Associated with either a TCH or an SDCCH
 - ✓ For non-urgent procedures
 - ✓ Power and time alignment control information (downlink)
 - ✓ Measurement reports from the MS (uplink)

33

•專屬控制通道（dedicated control channel, DCCH）是給各別手機使用, 也是用於傳送 point to point 的傳輸. , 但是做為像是電話線路設定這樣的訊息之專用溝通管道。

•DCCH 下有 SDCCH, SACCH, FACCH, CBCH.

•獨立專屬控制通道（Stand Alone Dedicated Control Channel或SDCCH）用以傳送系統call-setup控制訊號（signaling）及使用者之短訊息（short message）。

•慢速相關控制通道（Slow Associated Control Channel或SACCH）用來傳送非緊急的維運資訊如能量（power）及時差校正（time alignment）等控制資訊，以及由手機送至基地台的無線線路訊號測量結果(measurement report)。

Dedicated Control Channel (DCCH) (2/2)

➤ Four types in DCCH (continuous):

- Fast Associated Control Channel (FACCH) (down/uplink)

- ✓ Used for time-critical signaling, such as call-establishing progress, authentication of subscriber, or handoff.
- ✓ FACCH use TCH during a call.
- ✓ May cause user data loss.

- Cell Broadcast Channel (CBCH) (downlink)

- ✓ Carries only the short message service cell broadcast messages, which use the same time slot as the SDCCH.

34

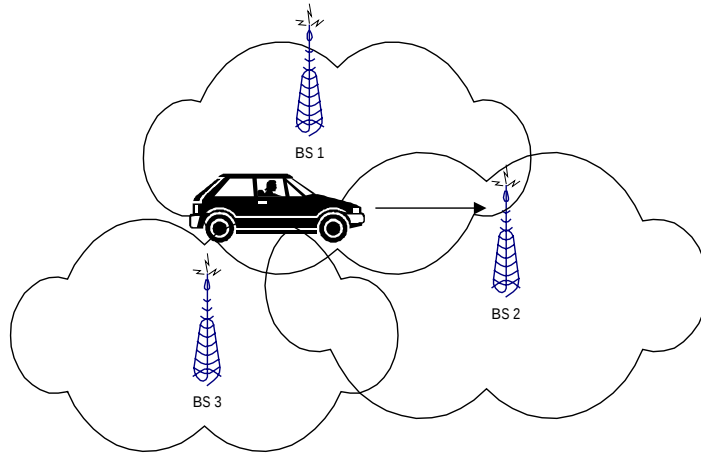
•快速相關控制通道（Fast Associated Control Channel 或 FACCH）用來傳送緊急控制信號（time-critical signaling）

- 例如電話線路設定、手機驗證（authentication）以及交遞（handover）的信號。

- FACCH 會佔用資料傳輸通道的時槽以爭取時間，但也因此會造成使用者資料之流失。

•細胞廣播通道（Cell Broadcast Channel或CBCH）是由基地台下傳送至手機的單向傳播，提供短訊息的廣播服務（short message service cell broadcast messages）。Ericsson 沒有提到 CBCH。

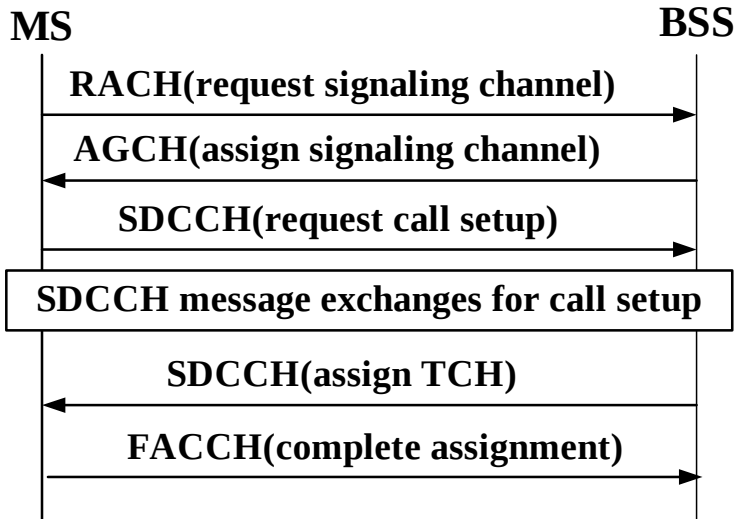
Registration



35

- 當 MS 開機後, 首先會掃描屬於 GSM 全部的頻道, 計算各頻道強度, 並把測量值存起來. MS 接下來會找出訊號最強的頻道, 判斷是否為 BCCH-carrier (i.e., 承載 BCCH (broadcast control channel) 的頻道). 如果是 BCCH-carrier, MS 就可取得 BS 的資訊, 看這個 cell 是否能是所屬的 PLMN. 若不是則再繼續搜尋,直到找到可用的 cell 為止.
- 利用 FCCH (Frequency Correction Channel) 使 MS 與 BS 同步.
- 由 SCH (Synchronization Channel) 可得到 BSIC
- BCCH 可得到 cell 的編號: CGI (Cell Global Identity), MS 由 CGI 可判斷是否是所屬的 PLMN 的 cell.
- MS 送出 IMSI 向 MSC 註冊.
- 這時 MS 進入所謂 idle mode, 這時 MS 會測量 signal strength 與 BER of the serving BTS. 若發現有收訊更好的 cell, 就會轉到 new cell 要求服務.

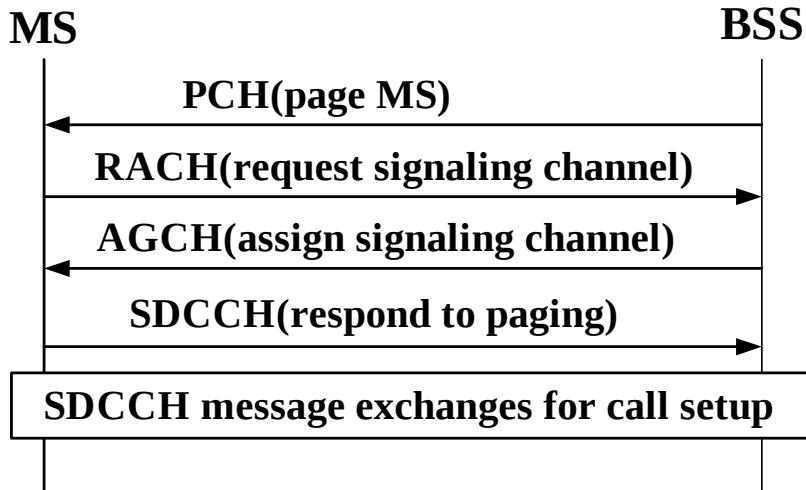
GSM Call Origination



36

- 這個範例說明 MS 想要打電話時所使用的 logic channel.
 1. MS 用 RACH 傳回請求通道的訊息
 2. BSC配置一個 SDCCH 給 MS, 並透過 AGCH 告訴 MS
 3. MS 用此 SDCCH 與 BSS 溝通, 送出所要撥打的電話號碼.
 4. 一旦電話接通, BSS 配置一個 TCH 給 MS
 5. MS 用 FACCH 通知 BSS 開始通話.(MS 不想等到下一個 SDCCH 才能回覆, 所以使用 FACCH)

GSM Call Termination



37

- 這個範例說明其他人想要打電話給 MS 時所使用的 logic channel.
- 1. BSC 要求 LA 下所有 BTS 以 PCH 廣播 MS 的 TMSI. (PERM_PAGE)
- 2. MS 聽到自己的 TMSI, 用 RACH 傳回請求通道的訊息(CHH_REQ)
- 3. BSC 配置一個 SDCCH 給 MS, 並透過 AGCH 告訴 MS (DSCH_ASS)
 - 直到 MS 得到 TCH 之前, MS 都會用此 SDCCH 與 BSC 溝通.
- 4. MS 透過 SDCCH 送與 call setup 相關得資訊 PAGE_RESP 給 BSS, 其中包含 TMSI 與 LAI.
- 5. BS 轉送 PAGE_RESP 給 MSC
- 6. MSC 通知 VLR 此 MS 有回應.(PAGE_RESP)
- 7. BSC 會分配一個 TCH 給 MS, 以傳送 voice. 若此 cell 所有的 TCH 都已經被佔據, BSC 會嘗試使用相臨 cell 的 TCH 來建立這通電話.
- Note: 是 BSC 做 channel assignment.

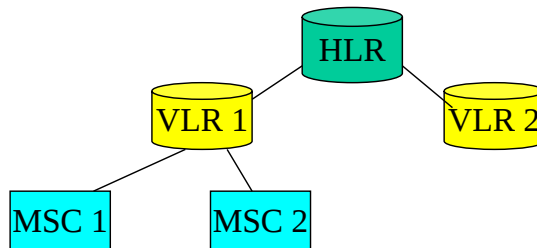
Location Tracking and Call Setup

38

- 這個部分說明 GSM 如何利用資料庫來做手機的位置追蹤 (location tracking) 與電話設定(call setup)的流程.

Two-level Hierarchical Strategy

- The current location of an MS is maintained by a two-level hierarchical strategy with the HLR and the VLRs.

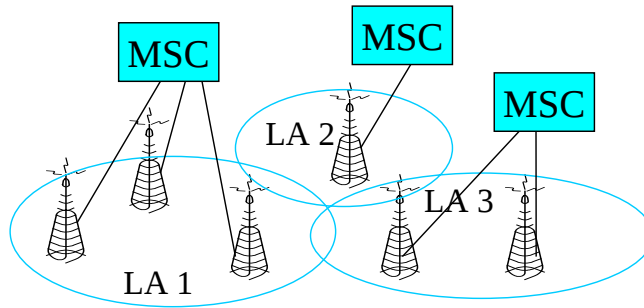


39

- GSM利用兩層式的資料庫來監控手機的位置。
- HLR 內存放使用者的一個永久記錄。
 - 記錄內容包括使用者資料 (user profile) 以及手機的位置。
 - 每個 MS 的記錄內容包括 MSISDN + IMSI + VLR ISDN + MSC ISDN + Subscriber Status
 - MSC ISDN 可能是為了 Security 的原因, 如 VLR crash 需 recovery. 所以 HLR 也要有.
- 每個或數個 MSC 則設有一個VLR。
 - 當手機由一 LA 移動至另一 LA 時, 藉由 VLR 之幫助執行一註冊動作, 使 HLR 獲知手機所在之區域。
 - 當要尋找一手機時, 就可查詢 HLR , 以便知道手機目前所在的VLR住址。
 - VLR 內每個 MS 的記錄內容包括 MSISDN + IMSI + LAI + TMSI + MSRN + Subscriber Status + HON
 - HON: MS 做 handover 的次數
 - IMSI 可產生 GT(Global Title) 以找到 HLR address
 - MSRN 是 VLR 自行產生,用於建立連到 MS 所在 MSC 的 trunk.

Location Area

- Location area (LA) is the basic unit for location tracking.
- Also, called as Registration area.



40

- GSM之服務範圍分割成許多位置區域（ Location Area 或 LA ），每個LA 由一個或數個BS 的涵蓋範圍所組成，做為記錄手機位置的基本單位。一個 MSC 可以包含一或數個 LA。
- 一個 MSC 所控制的地理範圍稱為 MSC area.
- 一個 MSC area 會切割成數個區域，稱為 Location area (LA). LA 是 GSM 紀錄 MS 位置的最小的單位。
 - 一個 MSC area 會切割成數個區域，稱為 Location area (LA). LA 是系統紀錄 MS 的最小的單位, 當 MS 來到一個新的 LA 就一定要做 location update, 所以LA 又稱為 Registration Area.
- 為達到對手機作位置追蹤的目的, MS 到 new LA, 就要做registration, location update.
 - 當手機到一個 LA 時, VLR 會為此手機產生一份暫時紀錄用來表示手機所在的區域(i.e., LA address).
 - 對每個手機來說, 在 HLR 中都會保有一份永久紀錄, 這份紀錄中會存放手機所在區域的 VLR.

Key Terms

➤ GSM uses some identifiers

- Mobile system ISDN (MSISDN)
- Mobile Station Roaming Number (MSRN)
- International mobile subscriber identity (IMSI)
- Temporary mobile subscriber identity (TMSI)
- Location area identity (LAI)
- International mobile station equipment identity (IMEI)

41

•GMS 有下面這些重要的識別號碼, 以下分別介紹. 由於 source 是很舊的書, 所以不見得是正確的.

•如果不想解釋太多, key terms 可以跳過.

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)
----------------------	------------------------------------	---------------------------

42

- 行動話機 MSISDN (Mobile Station ISDN Number) 即手機號碼(門號)。
 - MSISDN=CC+NDC+SN, 即電話號碼是由國碼-局碼-客戶碼所組成。
 - Example: CC=886 代表 Taiwan. 但在國內不用加國碼, 而在局碼前加長途碼 0.
- 當任何人欲打電話給一個GSM使用者, 必須撥該使用者之手機的ISDN號碼 (Mobile Station ISDN Number 或MSISDN)。
- MSISDN 這個號碼係定義於 CCITT Recommendation E.164。
- MSISDN 可用來找到手機的 HLR 的位址, GMSC 查詢 HLR 即可找到手機目前所在的 MSC 位置。

MSRN

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

43

•行動話機漫遊碼 MSRN 是用來尋找此 MS 的路由資訊, i.e., 是 MSC, VLR 等決定路由之用, 不供一般客戶使用.

• $MSRN = CC + NDC + SN$ 與 MSISND 有相同的格式.

•當 call delivery 時, HLR 接到 GMSC 查詢要求後, 從手機的記錄可找到該手機所在之 VLR 位址, 並要求 VLR 回覆手機的路由位址 (routable address) 。此路由位址稱為 MSRN. VLR 會送 MSRN 給 HLR.

•MSRN 由 MS 所在的 MSC 號碼產生. 每個 MSC 會分配到許多的 MSRN, 可以依序循環使用. 當 GMSC 收到 MSRN 後, 就會透過此路徑去尋找 MSC 來建立通話.

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)
---------------------------	---------------------------	--

44

•IMSI 又稱為 IMSN (international subscriber number), 是手機的永久密碼國際行動用戶號碼 (International Mobile Subscriber Identity或IMSI)。 IMSI 存在 SIM 卡, HLR, AUC, 及目前所在的 VLR 中。

•MNC 也可說是 network provider, 或 PLMN (public land mobile network) 的號碼。

•Example: MCC=466 是台灣, MNC=01 是遠傳

•Example: MNC =01 是 Telecom Australia, 234 是 UK Vodafone.

•IMSI 也用於 HLR/VLR 以找到 MS 的 PLMN.

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.

45

- 暫用性行動用戶識別碼係一暫用密碼，用來索引手機的永久密碼國際行動用戶號碼（International Mobile Subscriber Identity或IMSI）。
- 要避免 IMSI 在 air interface 上傳送, 所以以 TMSI 代替 identify MS itself.
- 當MS 開機完成註冊手續後, MSC/VLR 記錄下 IMSI, 然後送出 TMSI 做為臨時的識別碼. TMSI 是 VLR assign 給 MS. 當 MS 在這個 MSC/VLR 的服務範圍內, 都以此 TMSI 來加以識別.
- TMSI 是用於當 MS 到一個 new LA 時, 表明自己的身分(取代傳送 IMSI), 做 registration (location update) 用.
- 此外, 當 MSC 想要 paging a MS, 也會下令 LA 中所有的 BS 利用 PCH 做 broadcast the TMSI of MS.
- Length TMSI is no longer than 8 digits (TMSI structure defined by the operator), 另一參考書 [4] 寫 TMSI 最多有 32 bits.

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)

46

•位置區識別碼 LAI (Location Area Identity) 是每一個劃分尋找呼叫手機範圍 (Location Area, LA) 的識別碼.

•一個 LA 可能是 a cell 或 a group of cells, 一個 MSC 下會切割成數個 LAs.

•LAI 在 call termination 時用於找到 MS 所在的 LA, 在此 LA 下的所有 cells 都會 page 此 MS.

•In the Lin's Chapter 11

•LAI = Mobile Country Code (3-digit) + Mobile Network Code (2 or 3-digit) + location access code (16-digit)

•遠傳的設定 LAI = MCC (3-digit) + MNC (1-2 digits) + LAC (2 digits) ,
ex: 466-01-91 是 ROC-遠傳-遠傳教育中心

CGI

- Cell Global Identity
- $CGI = LAI + CI$
 - $= MCC + MNC + LAC + CI$
 - CI : Cell Identity

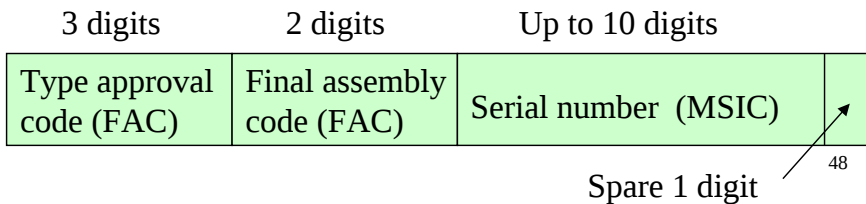
47

- 每個 cell 都有自己的識別碼 CGI (cell global identity), 由 LAI 加 CI 組成
 - Example: 相鄰兩個 cell 的 CGI = 466-01-91-1 與 466-01-91-2
- 當 MS 與 GSM 系統接通後, MS 就可由 BS 的廣播的 CGI 中得到自己所在位置的 LAI 與 CI. 當手機移到一個新的 LA, 就必須通知 MSC/VLR 使系統可得知 MS 所在的位置. 此動作稱為 Registration 或 Location Update.
 - MS 會蒐尋附近的所以基地台, 由 CGI 來判定是不是可以用的基地台 . 也用來判斷是否跨越LA要執行 registration. 若沒有, 則不獻通知 BTS.

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



•IMEI是每支手機出廠時給予之獨一無二的序號,稱為行動電話國際識別碼,可想成手機的身份證.

•手機開機後,輸入*#06#, 就會顯現出手機的IMEI. My IMEI=449 20 8300251418.

•但國內目前尚未提供IMEI認證的工作.

•當此 GSM component passes conformance and interoperability tests, 則會獲得此 TAC.

•FAC 是用來指出最後的製造商.

•SNR 是每一組 TAC/FAC 下一個獨一無二的序號. 由製造商給予編號.

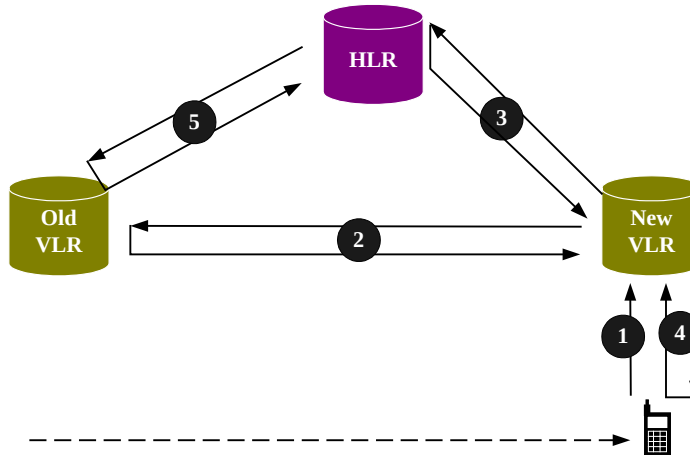
Identifiers and Components

號碼	HLR	VLR/MS	BSC	BTS	MS
MSISDN	✓				✓
MSRN		✓			
IMSI	✓	✓			✓
TMSI		✓			✓
LAI		✓	✓		✓
CGI				✓	
MSC號碼	✓				

49

- 分辨手機用戶會使用: IMSI, TMSI, MSISDN
- 分辨基地台會使用: CGI
- 分辨手機搜尋範圍會使用: LAI
- 分辨MSC會使用:MSRN
- 在完成開機註冊程序後, VLR 會建立此 MS 的資料, 接著再向 HLR 註冊, HLR 會更新 MS 的 VLR 欄位, 並通知原 VLR 將此 IMSI 從其中消除.

MS Registration Process (1/2)



50

•當 MS 在待機狀況(idle, 沒有通話)且四處漫遊(roaming), 可能會測得鄰近的 BS 之訊號強度, 並由其 BCCH (Broadcast control channel) 得到 CGI (包括 CI 和 LAI). 如果新的 BS 訊號較佳, MS 會改用新的 BS 之 channel. 這時有幾種狀況:

- New BS 與 old BS 有相同 LAI: 因為仍在相同的 paging area 中, MS 不會通知 MSC/VLR, 只要保持與 new BS 的 BCH (Broadcast channel) 同步.
- New BS 與 old BS 有不同 LAI: 必須進行位置更新的程序 (location update) 或 registration. 又分成以下的 cases:

- Intra-MSC movement: 新舊 BSs 屬於同一 MSC 管轄範圍, 此時只要更改 VLR 的資料, 不會動到 HLR. (因為 HLR 並不會記錄 LAI)

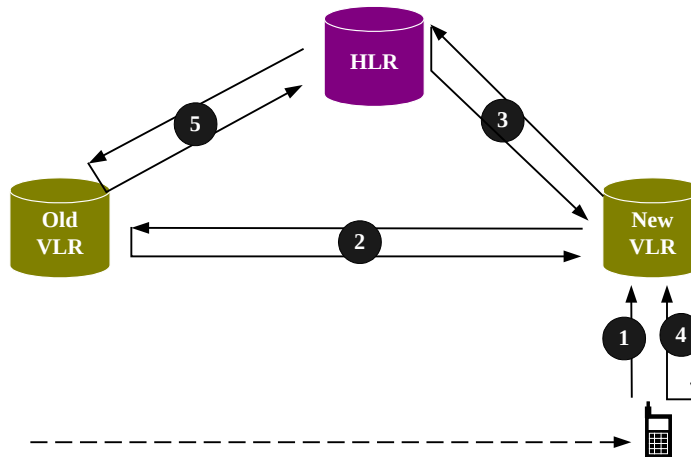
- Inter-MSC movement: 新舊 BSs 屬於不同 MSC 的管轄範圍但在相同 VLR 的管轄下, 此時要更改 VLR 與 HLR 的資料, i.e., MS 要重新進行認證與註冊程序.

- Inter-VLR movement: 新舊 BSs 屬於不同 VLR 的管轄下, 此時要更改 VLR 與 HLR 的資料, i.e., MS 要重新進行認證與註冊程序.

•這裡討論的是 inter-VLR movement 或 inter-MSC 的 registration. 藉由上圖的註冊程序, HLR 隨時可知道手機的正確位置。

•HLR, VLR 利用上述的 identifiers 來記錄手機目前的位置.

MS Registration Process (2/2)



51

•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。

•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2後，HLR 會送一訊號至舊的 VLR，要求將手機的記錄消除

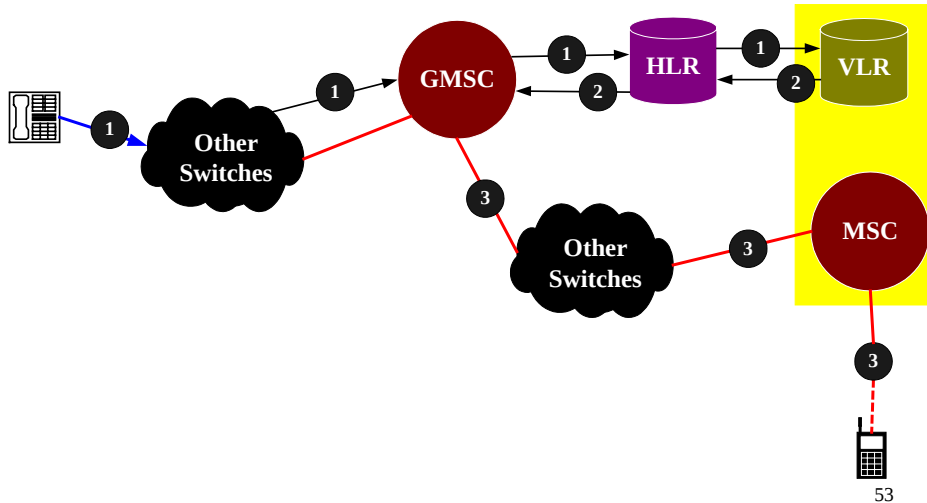
Periodically Registration

- The MS periodically send registration messages to the network.
- The period is 6 minutes to 24 hours.
- Periodic registration is useful for fault-tolerance purposes.

52

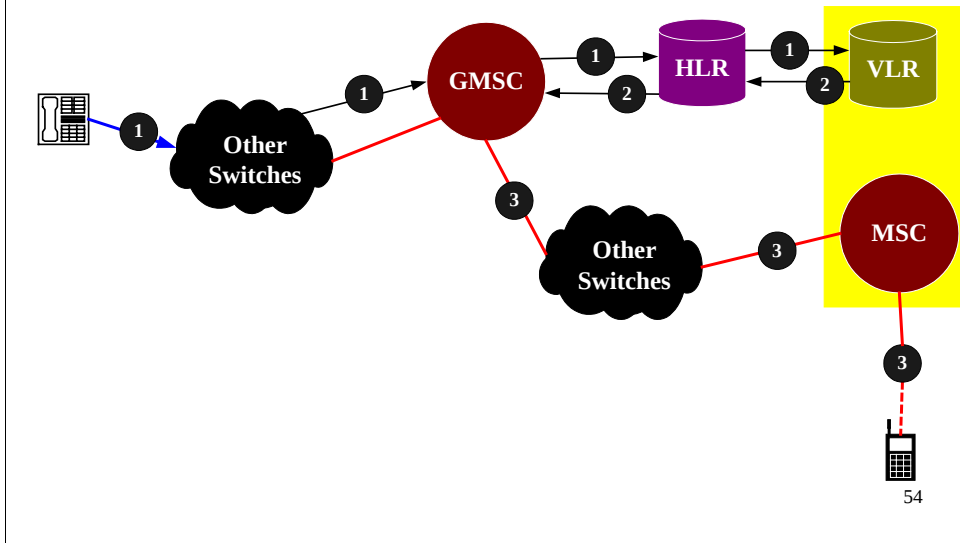
- MS 在 roaming 時, 藉由註冊程序, HLR 隨時可知道手機的正確位置。
- 但 GSM 亦要求手機定期向網路再註冊 (re-registration) 。
- 其週期範圍為6分鐘至24小時。
- 要求 periodically registration 的一些原因:
 - Re-registration 的設計是用來增加 GSM 網路之容錯性。
 - 當 VLR 或 HLR 損毀, re-registration 可加速資料庫的重建。
 - 若手機的 SIM 取出或關機時, 則手機會自動送一個國際行動用戶號碼離開 (IMSI detach) 的訊號至GSM網路, 將其位置資料消除, 系統便不再監控 MS。如果因為某些原因系統沒有收到 IMSI detach, MSC/VLR 不曉得 MS 實際上已經關機, 利用 periodically registration 的機制, 若 MSC/VLR 沒有在規定時間內收到定期註冊的訊號, 就當 MS 已經關機。

The Mobile Call Termination (Delivery) Procedure (1/2)



- Call termination 又稱為 call delivery.
- GSM的通話控制與IS-41類似。
- 假設發話者為 PSTN 使用者。當任何人欲打電話給一個GSM使用者，必須撥該使用者之手機的ISDN號碼 (Mobile Station ISDN Number 或MSISDN)。
- PSTN 分析 MSISDN 就可知道 MS 是屬於那一個 PLMN, 就將此 MSISDN 轉到此 PLMN 的 GMSC 處理。
- 接著 GMSC 會分析 MSISDN 以得知負責此 MS 的 HLR 的位址，查詢 HLR 即可找到手機目前所在的 MSC 位置。

The Mobile Call Termination (Delivery) Procedure (2/2)



•基本的GSM受話程序如上圖所示。

•Step 1:

•如同一般的撥號，MSISDN號碼會被送到公共電話網路之交換機。

•但由於一般的電話交換機並無能力處理MSISDN，但分析 MSISDN 就可知道 MS 是屬於那一個 PLMN，故該撥號要求會被轉送到此 PLMN 之 GMSC 來處理。

•MSISDN經由 GMSC 之解讀，獲得 HLR 之位址，並送一訊號至 HLR 來查詢手機位置。

•HLR 接到查詢要求後，將 MSISDN 轉成 IMSI，並從手機的記錄可找到該手機所在之 VLR 位址，並要求 VLR 回覆手機的路由位址（routable address）。此路由位址稱為 MSRN。

•Step 2:

•VLR 收到查詢要求後，先判斷 MS 是否 active (通話中)? If not, 找到手機的手機漫遊號碼（Mobile Station Roaming Number或MSRN），並將該MSRN經由 HLR 送回到GMSC。MSRN指示手機所在之 MSC

•Step 3:

•接收到MSRN後，GMSC 則根據 MSRN 將電話線路架設至該 MSC，MSC 會依 LAI 呼叫 MS，MS 回應後撥號者即可與手機通話。

Handover

55

- Ericsson 的作法: 當 MS 在通話中, 會進入工作模式(active mode). 對 GSM 系統而言, MS 被要求每 480 ms 就回報一次目前所在的 BS 的平均收訊品質 (ex: 在 480ms 內的 Bit error rate, BER 平均值), 回報給 BSC. MS 也要測量附近所有 BSs 的訊號強度(BCCH 之 carrier), 回報給 BSC.
 - 每一個 BTS 的測量值會標上 BTS 的編號, 已以確保一對一的對應. 所以 MS 必需從 SCH (time slot 0, carrier 0) 上得到 BTS 的 identity. 訊號最好的前 6 個 neighboring cells 的資料會用 SACCH 傳給 BTS.
 - 由於 MS 並未與 neighboring cell 同步, 所以最少要 8 timeslots 才能找到 BCCH 的 timeslot 0, 所以這樣的測量必須在 idle frame 時進行.
 - 測量 signal 是在 MS 上傳後到下一次 BTS 下傳前的時間.
 - 當 MS 在通話時, 目前所在的 serving BTS 也會對 MS 上傳的訊號強度回報給 BSC.
 - BSC 會分析 MS 與 BS 的測量報告(measurement report), 決定應由那一個 BS 來 serve 此 MS.
- 若 BSC 決定由 new BS 取代 old BS 來繼續傳送語音給 MS, 就稱為交遞(handover).
- 在 MS 通話過程中, 通話的線路就不斷的接到 new BS, 系統此時是不做 location tracking. 因此當通話結束後, MS 必須向所在的 MSC/VLR 進行 registration process.

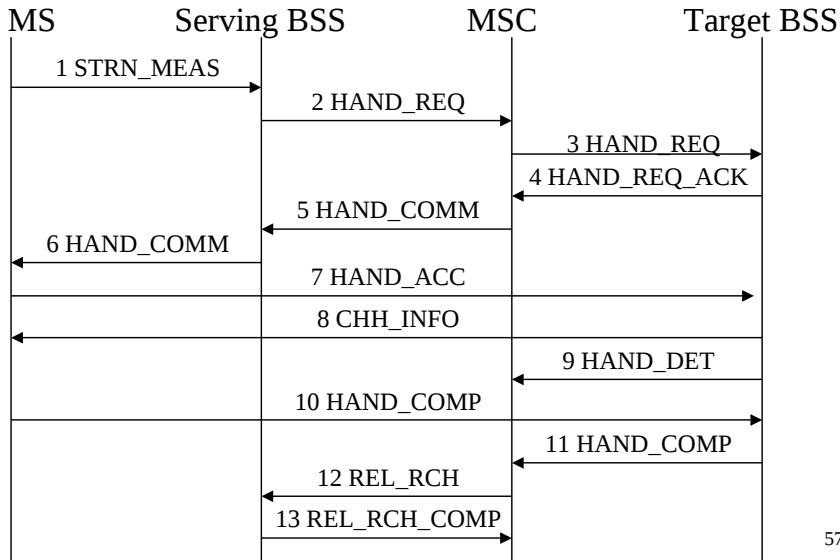
Handoff

- Three basic kind of handoff:
 - Intra-BSS
 - Intra-MSC (inter-BSS)
 - Inter-MSC
- We discuss the intra-MSC and inter-MSC handoff.

56

- Handover 是 GSM 的說法, 和 handoff 指相同的事.
- Ericsson 的作法是所有的信號測量數據都集中於 BSC, 所以由 BSC 決定要 handoff 到那一個 cell 及啟動 handover 的程序. 即使是 Inter-BSS handover, 必須通知 MSC/VLR, 但 MSC/VLR 並不會改變 BSC 的要求, 就好像是由 BSC 控制, 因為 MSC 並沒有real-time的連結相關資訊.
- Handover 和 roaming 一樣, 以新舊 BS 間的關係程度, 分成下面幾種 cases:
 - Intra-BSS: 新舊 BTS 屬於同一個 BSC 的管轄範圍, 這時 BSC 就直接下命做 handover.
 - Intra-MSC 或 Inter-BSS: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.
 - Inter-MSC:新舊 BTS 屬於不同一個 MSC 的管轄範圍.
- 以下的範例為跨不同 BSC 時的作法.

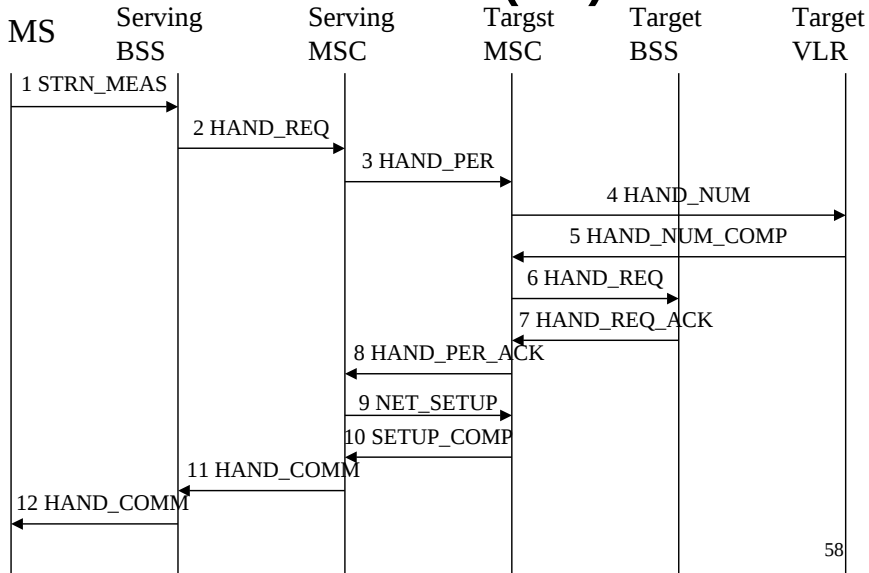
Intra-MS



57

1. MS 送出 STRN_MEAS 訊息給 serving BSS. 此訊息中包含信號強度的資料. Serving BSS 發現需要做 handoff.
2. Serving BSS 送 HAND_REQ 給 MSC, 此訊息中列出所有可以服務 MS 的 target BSSs.
3. MSC 檢查是否有旗下 BSS 是在 candidate 中, 如果有就設定此 BSS 為 target BSS, 進行 intra-MS handoff. 此時需要兩 resources, 一是 MSC 與 target BSS 間的 trunk, 另一項是 radio channel. MSC 保留下 trunk 並送 HAND_REQ 給 target BSS. 此訊息中包含需要服務的 cell area 的 ID (以找出合適的 BTS), MSC-BSS 間 trunk 的 ID, 與 encryption key Kc.
4. BSS 保留適當的 resource, 再送回 HAND_REQ_ACK 給 MSC, 此訊息中包含保留之 radio channel 的 ID.
5. MSC 送 HAND_COMM 給 serving BSS, 通知 target BSS 與 new radio channel ID.
6. Serving BSS 將此訊息 HAND_COMM 轉送給 MS.
7. MS 使用 new radio channel 送出 HAND_ACC 與 target BSS 通訊.
8. Target BSS 送回 CHH_INFO.
9. Target BSS 告訴 MSC 他已經進行 handoff.
10. Target BSS 與 MS 交換訊息做 synchronization, 與找尋適當的 time-slot . 完成後, MS 送 HAND_COMP 給 target BSS.
11. 同時間 MSC 將 voice trunk 轉到 target BSS. 一旦 MS 與 BSS 完成 synchronization 與建立傳送 signal 的連線, BSS 將 HAND_COMP 送給 MSC, 表示 handoff 已經完成.
12. MSC 送 REL_RCH 給 serving BSS, 要求釋放 old radio channel.
13. 此時 serving BSS 收回所有給 MS 的 resource, 將 REL_RCH_COMP 送給 MSC.
 - GSM spec. 要求整個 open interval gap (從 MS 轉到 new radio channel 到完成 synchronization) 不可以有 90% 超過 150ms.

Inter-MS (1/2)



58

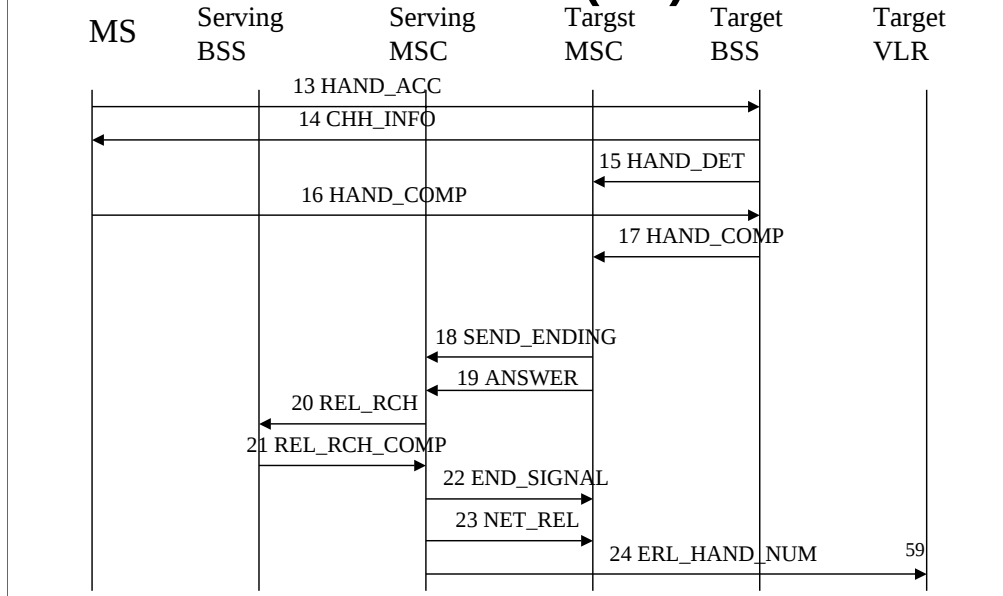
- * 表示和 Intra-MS handoff 不同的地方。
- 1. MS 送出 STRN_MEAS 訊息給 serving BSS. 此訊息中包含信號強度的資料. Serving BSC 發現需要做 handoff.
- 2. Serving BSS 送 HAND_REQ 給 MSC, 此訊息中列出所有可以服務 MS 的 target BSSs.
- 3. *MSC (稱為 serving MSC) 發現 MS 已經離開他的服務範圍, 而到另一個 MSC(稱為 target MSC) 之下, Serving MSC 會用 target MSC 的 directory number 建立起到 target MSC 的 voice trunk, 如同一般轉送電話的過程, PSTN 端是完全不曉得的. Serving MSC 送給 target MSC 訊息 HAND_PER.
- 4. *Target MSC 送出 HAND_NUM 給 VLR, 要求分給一個 TMSI.
- 5. *VLR 送回包含 TMSI 的 HAND_NUM_COMP 訊息給 target MSC.
- 6. Target MSC 並送 HAND_REQ 給 target BSS. 此訊息中包含需要服務的 cell area 的 ID (以找出合適的 BTS), MSC-BSS 間 trunk 的 ID, 與 encryption key Kc.
- 7. BSS 保留適當的 resource, 再送回 HAND_REQ_ACK 給 MSC, 此訊息中包含保留之 radio channel 的 ID.
- 8. *Target MSC 送 HAND_PER_ACK 給 serving MSC, 表示他已經準備好可以進行 handoff.

9. *Serving MSC 送 NET_SETUP 給 target MSC 表示要設立通話.

10. *Target MSC 回應 serving MSC 訊息 SETUP_COMP.

11. Serving MSC 送 HAND_COMM 給 serving BSS 通知 handoff 完成. BSS 與

Inter-MSC (2/2)



- * 表示和 Intra-MSC handoff 不同的地方.

13. MS 使用 new radio channel 送出 HAND_ACC 與 target BSS 通訊.

14. Target BSS 送回 CHH_INFO.

15. Target BSS 告訴 Target MSC 他已經著手進行 handoff.

16. Target BSS 與 MS 交換訊息做 synchronization, 與找尋適當的 time-slot . 完成後, MS 送 HAND_COMP 給 target BSS.

17. 同時 target MSC 將 voice trunk 轉到 target BSS. 一但 MS 與 BSS 完成 synchronization 與建立傳送 signal 的連線, BSS 將 HAND_COMP 送給 MSC, 表示 handoff 已經完成.

18. *Target MSC 送 SEND_ENDING 給 Serving MSC 表示 handoff 完成.

19. *若 MS 轉到 new radio channel 開始通話, Target MSC 送 ANSWER 給 Serving MSC.

20. Serving MSC 送 REL_RCH 給 serving BSS, 要求釋放 old radio channel.

21. 此時 serving BSS 收回所有給 MS 的 resource, 將 REL_RCH_COMP 送給 Serving MSC.

22. *Serving MSC 送 END_SIGNAL 給 target MSC.

23. *Serving MSC 釋放所有 network resource, 並送 NET_REL 給 target MSC.

24. *Target MSC 送 ERL_HAND_NUM 給 VLR, 結束與 VLR 間的連結.

Security

60

- 由於第一代大哥大系統有諸多安全上的問題，造成盜打與監聽上的缺失，因此在 GSM 設計時就相當重視通訊安全。

Security

- GSM security is addressed in two aspects: authentication and encryption.
 - Authentication avoids fraudulent access by a cloned MS.
 - Encryption avoids unauthorized listening.

61

- GSM的安全措施由兩個方向來考量：手機認證（ authentication ）及訊號加密（ encryption ）。
- 認證係用以防止他人假冒手機以盜用GSM服務。
 - 手機認證的時機，包含電話的設立、註冊、手機位置的改變與新增或減少服務功能。
- 加密則是避免他人竊聽無線線路的通話。
 - 當雙方協調好加密之 key 後，通話內容便可以進行加密。
 - i.e., 仍究有些時候是 plain code in the air.
- GSM 使用自己獨一無二的演算法，選擇用 token-based system using security triplets, 不使用 IS-41 的 Shared Secret (Key) Data (SSD).
 - SSD : network and phone share the secret key.

Parameters

➤ Parameters:

- **Ki** is used to achieve authentication.
 - ✓ Ki is stored in the AuC and SIM.
 - ✓ Ki is not known to the subscriber.
- **RAND.**
 - ✓ A 128-bit random number generated by the home system.
- **SRES** is generated by algorithm A3.
- **Kc** is generated by algorithm A8 for the encryption.
- **Frame Number.**
 - ✓ A TDMA frame number encoded in the data bits.

62

•以下介紹用於 GSM 認證與加密所用到的一些參數:

•用於 Authentication:

•**密秘鑰匙** (secret key, or authentication key) Ki

•Ki 只存在兩個地方：GSM的認證中心 AuC 及手機的使用者認證模組 SIM，所以VLR, 使用者並不會知道 Ki 的值。

•在設計 GSM 的安全系統時, 便希望 service provider 可以全然控制 security system, 而不要將 secret data 流通到其他的 system.

•GSM 的 system in Europe 便是以 country 為單位. 因此, 她們認為 intersystem communication 的需求很小.

•所有的 authentication 都在 HLR 執行.

•**RAND**: 認證中心所產生的一個128位元的亂碼 (random number) 。

•使用 Ki 及 RAND 來執行一個A3演算法。A3 會產生簽署結果 (Signed Result或SRES) 。

•此時認證中心及手機都執行 A3 產生 SRES。

•用於 Encryption:

•Kc 是由 A8 所產生的結果，用來做無線通道上資料之加密鑰匙 (encryption key or cipher key) 。

•Kc 是會改變的.

•Frame Number: 8 time slots form a frame

Algorithms

➤ Authentication Algorithms:

- **A3.**

- ✓ Authentication function.
- ✓ In AuC and SIM

➤ Encryption Algorithms:

- **A8.**

- ✓ To generate the encryption Key
- ✓ In AuC and SIM

- **A5.**

- ✓ An algorithm stored in the MS (handset hardware) and the visited system.
- ✓ Used for the data ciphering and deciphering

63

•手機A3演算法，是由手機自己原籍的GSM系統選定的。若手機漫遊到一新的GSM系統，此新的GSM系統並不會知道手機的A3演算法，所有的認證都只在手機的自己原籍之GSM系統進行。

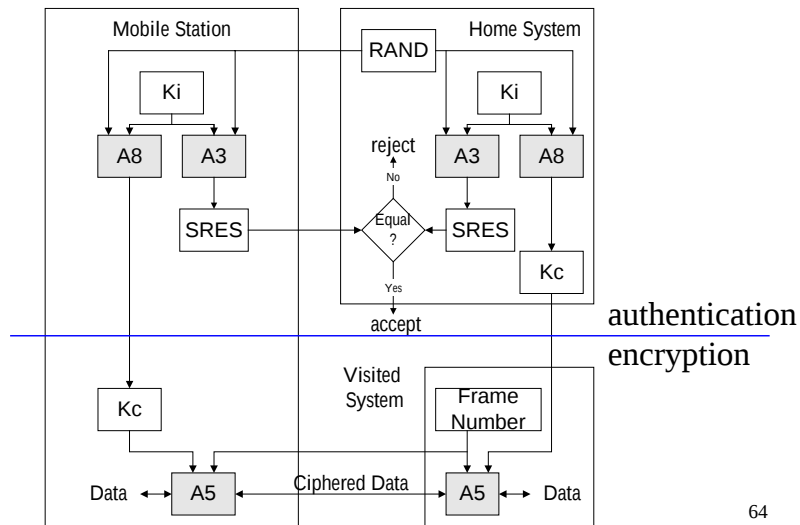
•**Note that** if (SRES, RAND) generated by the AuC are sent from the HLR to the visited VLR in advance, the comparison can be done at the visited VLR. Discussed later.

•不像GSM，IS-41的認證動作可以是在手機漫遊的系統中執行。

•A8也是由手機原籍的GSM系統選定的。

•所有GSM系統業者均使用相同的A5演算法。基本上GSM的安全認證措施是比較不易被破解的。

Authentication and Encryption



64

- 這張圖說明各個參數與演算法所在的位置, 與認證, 加密的過程.
- 認證過程是利用一密秘鑰匙 (secret key) K_i .
 - 欲驗證一手機時, 認證中心先產生一個128位元的亂碼 (random number) , 稱為 $RAND$ 。
 - 認證中心將 $RAND$ 亂碼送至手機, 此時認證中心及手機都使用 K_i 及 $RAND$ 亂碼來執行一個所謂的 A_3 演算法。
 - 執行 A_3 會產生 $SRES$ 。然後手機將產生之 $SRES$ 回認證中心, 與認證中心所產生之 $SRES$ 做比較。
 - 若結果相符則驗證成功, 否則手機的要求就會被駁回。

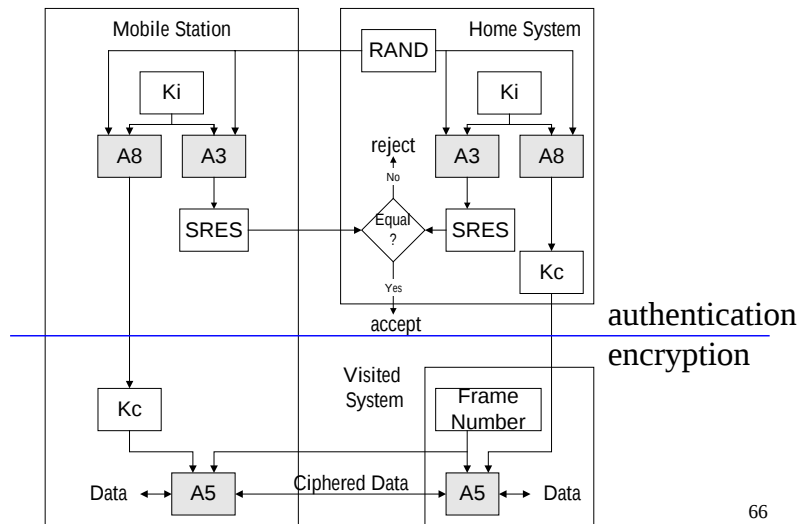
Authentication by Triplet

- Triplet: RAND, SRES, Kc
 - AuC→HLR→VLR in advance
- Example: Authentication in registration
 - New VLR uses LAI to find old VLR.
 - Old VLR sends triplets to new VLR.
 - New VLR challenges MS by using RAND and SRES.

65

- MS 認證需要 Ki, RAND, 然而為了維護 Security, 所以 Ki 只存在 SIM 與 AuC/HLR 中. 但是如果所有的認證都要到 AuC/HLR 才能做, AuC/HLR 顯然會負擔太重. 因此, GSM 因此在實際的系統上, 採用折衷的方法:
- 當 MS 移動到一個新的 system 時, VLR 會向 AuC/HLR 要一些 security 資料, 稱為 triplet (通常 HLR 會給予 3-5 個 triplet).
- 每個 triplet 包含 3 個資料: RAND, SRES, Kc.
 - 其中 SRES 是用 RAND 與相對應 MS 的 Ki 所計算出來的. 因此當進行 authentication challenge 時, VLR 可以直接送 RAND 給 MS, 用 SRES 與 MS 送回之 SRES 比對
 - 若數據正確則送 Kc 給 MS, 做為加解密使用.
 - HLR 先計算好 SRES 的值, 如此 VLR 就不需要 Ki, A3, A8 進行計算.
- 例如, MS 做 registration 時, MS 會送 TMSI 與 LAI 給 network.
 - New VLR 利用 LAI 找到 old VLR, 並向 old VLR 要相關 authentication 資料. (unused triplets and location of HLR)
 - New VLR 會進行 challenge. MS 會計算結果 SRES 並回傳給 VLR, VLR 比較兩方的數據是否相同, 以判別是否是合法手機.
 - New VLR 確認後才會向 HLR 做 location update.
 - New VLR 會給予 MS 新的 TMSI
- 對 VLR 而言, VLR 會一次向 HLR 要多組 triple (ex. 5 組 triples)
 - 一旦此 triple 已使用過, 則被丟棄不用 (mark used), 要使用下一組 triple. 或者系統業者會訂定每一 triple 可使用的次數上限, 到達上限, 則

Encryption



66

- 在執行A3 (for authentication) 時，手機與認證中心亦同時執行另一演算法A8 (to generate the encryption Key Kc)。
- 利用 Ki 與 RAND, A8 產生 Kc，係用來做無線通道上資料之加密鑰匙 (encryption key)。
- 認證中心將 Kc 送至手機所在的基地台，基地台會將其TDMA的時框號碼 (frame number) 送至手機。
- 手機及基地台同時使用加密鑰匙 Kc 及 frame number，執行加密與解密的演算法A5，將傳至對方的資料加密，並將收到的資料解密。

GSM Data Services

67

- 資料的傳輸是必然的趨勢, 因此在 GSM 演進的過程中, 不斷的加入新的元素, 以提供 Data Communications.
- 以下會談到 HSCSD, GPRS 與 EDGE

Data Services

- GSM phase 2 standard supports two data services:
 - Short Message Services (SMS)
 - Bearer Services are similar to the ISDN services, and the maximum data rate is 9.6 Kbps.
- GSM phase 2+ standard supports two data services:
 - High-Speed Circuit-Switched Data (HSCSD) for high-speed file transfers and mobile video applications
 - General Packet Radio Service (GPRS) for burst data applications such as e-mail and WWW

68

•在GSM Phase 2支援兩種資料傳輸的服務：短訊息服務（short message services）和送遞訊息服務（bearer services）。

•Bearer service 是一種類似 data circuit duplex 服務，但最高的傳輸速度只有9.6Kb/s。

•手提電腦或 PDA 透過PC card與手機相連接，便可要求GSM提供這樣的服務。

•此時在GSM網路端會在手機與公共電話網路之介面開道間，建立一條電路交換式連線（circuit-switching connection），以傳送資料。

•這條連線上的無線電通道與有線線路，即使不傳送資料也都會一直保留著，直到使用者終止服務。

•GSM Phase 2 沒有提供分封交換式傳輸（packet-switched transmission）

•ETSI 繼而提出 GSM Phase 2+ 標準的主要訴求，就是要提供有效率的數據服務。有人把GSM Phase 2+ 稱做是 GSM +. 把 EDGE 稱為 GSM ++, EDGE 請見最後的投影片。

•提出高速電路交換數據（High Speed Circuit Switched Data或HSCSD）以及一般封包式無線電服務（General Packet Radio Service或GPRS）

•目的在提供高速檔案傳輸、行動視訊（mobile video）與類似電子郵件大量與WWW資料的應用。

•HSCSD 仍為 circuit-switching。

•GPRS採用的分封交換技術較能符合數據傳輸的burst特性。

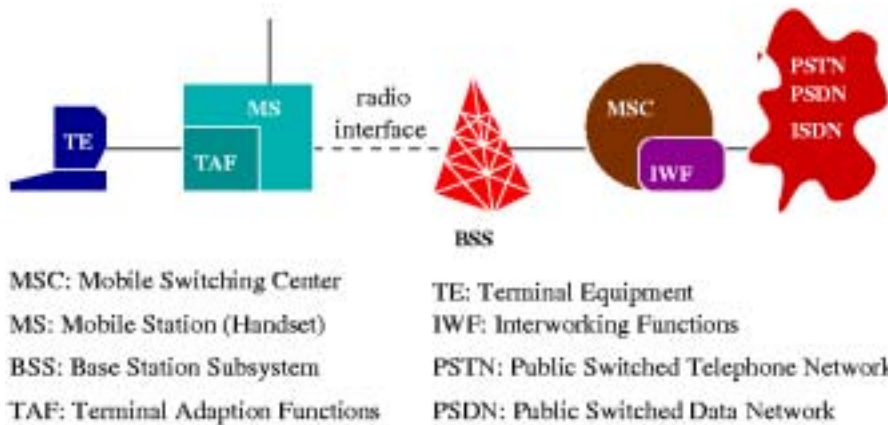
HSCSD

- High-Speed Circuit-Switched Data (HSCSD)
 - A circuit-switched protocol for large file transfer and multimedia applications
- **Radio link protocol (RLP)** in HSCSD to support multi time-slot operation
 - Up to 8 time slots can be used
 - Data rate of HSCSD
= no. of time slots × Data rate of one timeslot
- The physical layer of HSCSD is the same as that for the Phase 2 GSM data services.

69

- HSCSD是為了高速檔案傳輸與多媒體應用而制定的電路交換式傳輸協定。
- HSCSD 讓手機同時間最多可擴增到8個時槽來做資料傳輸，使得資料傳輸速率大幅增加。
- 同時利用資料壓縮（data compression）的技術，增加傳輸速率。
- HSCSD的無線電介面與目前GSM系統相同。只是可以使用多個 timeslot 來傳送。
- 改進後的HSCSD之無線電連結協定（Radio Link Protocol或RLP），可支援多個時槽的運作。
- In June 1999, Nokia announced Card Phone 2.0 for HSCSD with 43.2 Kbps.

HSCSD Architecture



70

- HSCSD的系統架構圖。
- 使用者是在電腦這樣的終端設備（Terminal Equipment或TE）進行資料的運算，並與手機相連。
- 利用手機上的終端改編功能（Terminal Adaption Function或TAF），將終端設備間資料轉換成為手機的一般無線電傳輸，以無線電介面傳送到基地台子系統。再連結到交換機行動交換中心，以網路跨網函式（interworking function或IWF）將資料做協定轉換並送到外界的網路。
- TAF 與 IWF 兩個端點間的服務（end-to-end service）有密切的關鍵。
- 傳送相關資料連結間的其他經過之GSM實體，就與此服務無關，他們只是提供了送遞訊息的能力。

GPRS

- General Packet Radio Service (GPRS)
- A packet-switched protocol
- GPRS radio link protocol
 - To guarantee fast call setup procedure and low-bit error rate for data transfer between the MSs and the BSs
- A new infrastructure is introduced to GPRS for the packet services.

71

•GPRS是為了提供像WWW這樣，使用者需耗費許多時間閱讀，偶爾傳送大量數據的應用而提出的分封交換協定。

•不像HSCSD，既有的GSM網路無法提供封包傳送的模式，所以GPRS必須有自己的傳輸網路（transport network）。

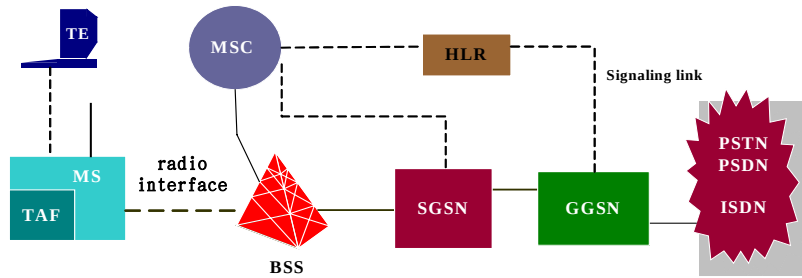
•GPRS radio link protocol 主要是規定手機與基地台之間，physical layer、MAC層以及RLC層彼此之間在相互通訊時所必須遵守的協定。

•GPRS 利用現有 GSM 的 physical channels，建立自己的 logic channels。

•RLC/MAC層的功能，就是要讓許多用戶共享這些數據通道，透過空中介面的實體層來傳送資料。

•GPRS supports up to 100 users with one to eight channels.

GPRS Architecture



HLR : Home Location Register

VLR : Visitor Location Register

MSC : Mobile Switching Center

BSS : Base Station Subsystem

TAF : Terminal Adaption Function

SGSN : Serving GPRS Support Node

GGSN : Gateway GPRS Support Node

TE : Terminal Equipment

PSTN : Public Switched Telephone Network

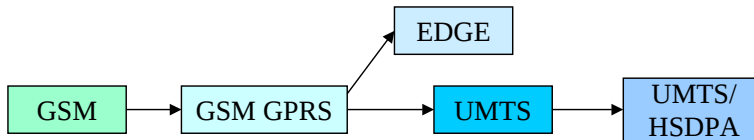
PSDN : Public Switched Data Network

72

- 上圖是 GPRS傳輸協定的架構。
- 在手機與終端主機的網路層之上，可以根據應用程式的需求，採用不同的協定。例如在應用程式下可使用TCP/IP 傳送，對此GPRS並不加以限制。
- 在GPRS網路上，封包的發送端與接收端這兩個的GPRS支援節點之間，使用所謂的GPRS隧道協定（GPRS Tunnel Protocol或GTP）。它主要的功用是透過附加路由資訊（包裝）的方式，將上層的X.25或IP應用程式的協定數據單元，經由GPRS骨幹網路來傳送，並依據應用程式的需求，提供不同服務品質（Quality of Service或QoS）。
- 詳情請參考 GPRS.ppt

EDGE

- Enhanced Data Rates for Global Evolution or Enhanced Data Rates for GSM Evolution
- Cost-efficient upgrade to existing GSM/GPRS and TDMA networks.
 - EDGE does not change much of the core network.
 - No additional spectrum is necessary.



73

•GSM 的演進可用上面的圖表示, EDGE 可視為 GSM 或美洲使用 TDMA 系統的一個 3G 的演進 (revolution). 若是跳到 UMTS, 我們會用革命(Revolution)來形容.

•GSM (voice, 9.6 kbps) → GSM GPRS (約 80 kbps) (in GSM+)

→ EDGE (240 kbps) (in GSM++)

→ UMTS → UMTS/HSDPA (更高容量的語音與資料傳輸)

•GSM+ 提出 HSCSD (High Speed Circuit Switched Data) 與 GPRS (General Packet Radio Services) 可提供有限的數據服務. HSCSD 是利用多個 timeslot 同時傳輸以增快傳輸速率, GPRS 是改用 packet switching 的技術.

•GSM++ 為 EDGE (Enhanced Data rates for GSM Evolution), 利用不同的調變技術, coding scheme 來提高其在空中的傳輸速率與效率, 使得在一個 timeslot 中, 可以傳送更多的資料.

•EDGE 並沒有更動許多 core network 部份, 所以是比較 cost-efficient migration.

EDGE

- EDGE accelerates speeds over the air.
 - 8PSK
 - 9 Coding Scheme (8.4kbps~ 59.2kbps)
 - 384kbps when using 8 timeslot
 - E-GPRS: packet-data services
 - E-HSCSD: high-speed, circuit-switched service
- QoS supported

74

- Data 在空中傳送時, bit 會被編碼(coded)成為 symbol.
- GSM 用的是 GPRS/GSM coding Gaussian Modular Shift Key (GMSK), 一個 bit 編碼成一個 symbol.
- EDGE 用的是 8PSK, 三個 bit 編碼成一個 symbol, 所以可以增加 bit rate.
 - 可已想見 receiver 必需更先進, 訊號品質必須更好, 才能正確判斷出所代表的 symbol.
 - 由於無線訊號受環境影響, EDGE 提供了 9 種編碼方式 (coding schemes) (GPRS 只有 4 種), 且可以在一個連結中交換使用不同的編碼方式, 以維持正確的傳輸.
 - EDGE 的 bit rate 是 MSC-1: 8.4kbps~ MSC-9: 59.2kbps
 - 當使用全部 8 個 timeslot, 最高傳送速度可到 384 kbps.
- EDGE 提供的服務可以用在舊的系統: GPRS 與 HSCSD. 就形成 E-GPRS 與 E-HSCSD.
- 不像 GPRS PCU 沒有能力處理不同 data streams, EDGE 有提供與 WCDMA 相似的 QoS 能力.

Unstructured Supplementary Service Data

75

- 人們會要求業者提供一些新的服務(supplementary services), 例如利用手機也能提供股票, 期貨, 外匯資訊的查詢.
- 如果說當 GSM 不斷改進, 加入一些新的服務, 手機也要不斷的更新, 才能處理這些 services. 若是系統業者為了新的服務更改了系統, 舊的手機便無法使用, 這樣的做法並不是很適當.
- 因此有了 USSD 這樣的方法, 讓 GSM 業者可以快速的提供新的 services.

USSD

- These new services may not be supported in old MSs.
- To support the new services in old MSs, USSD was introduced in GSM 02.90, 03.90, and 04.90 Spec.
- USSD is used as a GSM transparent bearer.
- The USSD service node (in MSC, VLR or HLR) provides the new service.

76

- 一般而言, user 鍵入電話號碼, 按下撥號鍵, MS 能理解這些動作, 並開始工作.
- 當 MS 不瞭解 user 鍵入的 the text string (usually, telephone number), the MS 則使用 USSD 這個功能將這些文字傳送到網路端 (without understand the text). 位於網路端的主機 USSD service node (就是資料庫) 則會解讀這些 text, 並提供相對應的服務.
 - Ex: 遠傳的 *128*股票代號# 就可查詢股價市值.
 - 要回傳給 MS 的資訊, 則是透過SMS傳回 MS.
- USSD 便是一個這樣的傳輸機制, 以傳送這些服務.
 - MS 透過 SS7 傳送 message 給 USSD service node (或 USSD gateway), 是走 signaling, 而非 voice or data.

The Usage of USSD

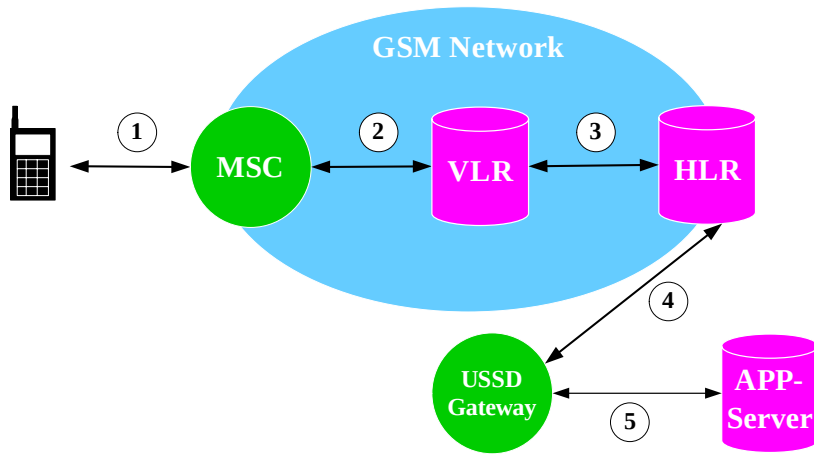
- USSD is flexible in terms of message length and content.
- It uses all digits 0-9 plus “*” and “#” keys.
- A USSD string is a command code
 - Typically 2 or 3 digits followed by several parameters
 - The parameters provide supplementary information.
 - The whole string ends with “#”.

* 159 * 5288128 #

77

- 使用 USSD 就像是輸入一串命令, 命令可以自由設計傳送訊息的內容與訊息長度, 而與 USSD 無關.
- 基本上有一定的格式與規範.
- The USSD string is sent out in the same manner as placing a call.
- 例如 If we specify command code 159 for call forwarding 電話轉接, the USSD string *159*5288128# is sent by the MS.
 - The network will forward all incoming calls to 5288128.

USSD Architecture



78

- USSD 提供一個 MS, MSC, VLR, HLR 之間溝通的介面。
 - 如果 USSD service node 在 MSC, 則 USSD message 只在 (1) MS-MSC 間傳送.
 - 如果 USSD service node 在 VLR, 則 USSD message 透過 (1) (2) 在 MS-MSC-VLR 間傳送.
 - 如果 USSD service node 在 HLR, 則 USSD message 透過 (1) (2) (3) 在 MS-MSC-VLR-HLR 間傳送.
- 以即時股票查詢系統做為範例, 我們想要將 USSD service node 放在 HLR 上. 因此手機可隨時得知股票訊息.
 - 缺點是 HLR 不大可能做股票查詢的功能. 會增加 HLR 的負擔.
- 因此必須獨立出此 USSD service node, 形成圖中架構。
 - USSD gateway 翻譯 USSD message 且轉送給適當的 server.
 - Application server 做 stock query server.
 - USSD gateway 與 HLR 是透過 GSM MAP 溝通; USSD gateway 與 application server 是透過 TCP/IP 溝通.

Summary (1/2)

- GSM Architecture
 - MS, BSS, NSS
 - Radio Interface
- Location Tracking
 - Registration
 - Mobile Call Termination
- Security
 - Authentication
 - Encryption

Summary (2/2)

- Data Services
 - HSCSD
 - GPRS
- USSD Services
- EDGE