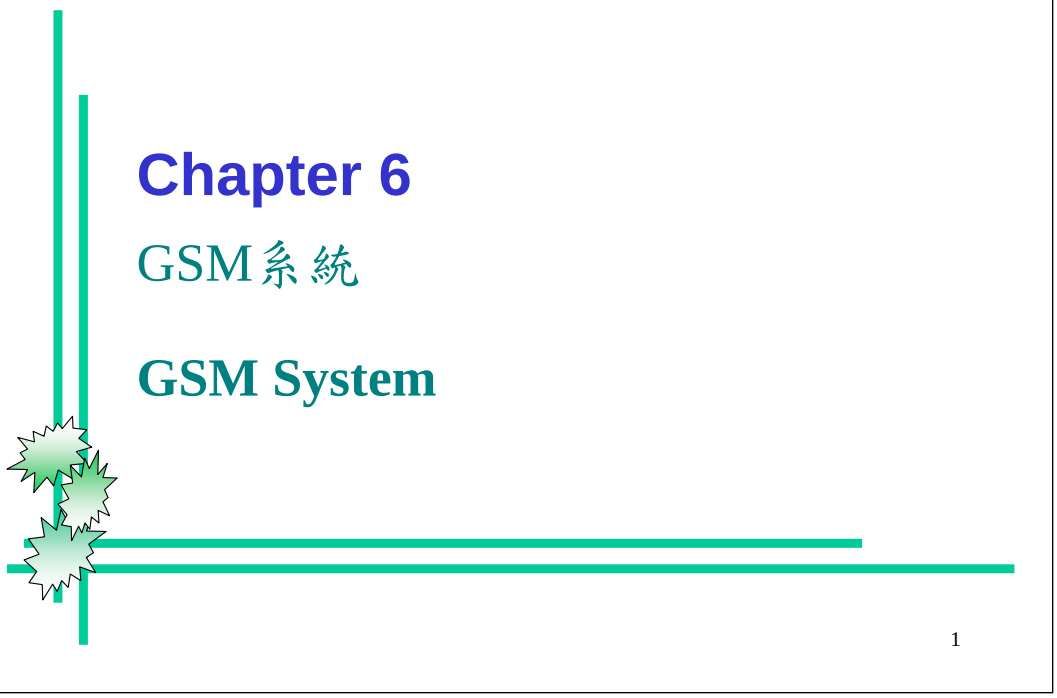

Chapter 6
GSM系統
GSM System
1

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

3

Section 6.1

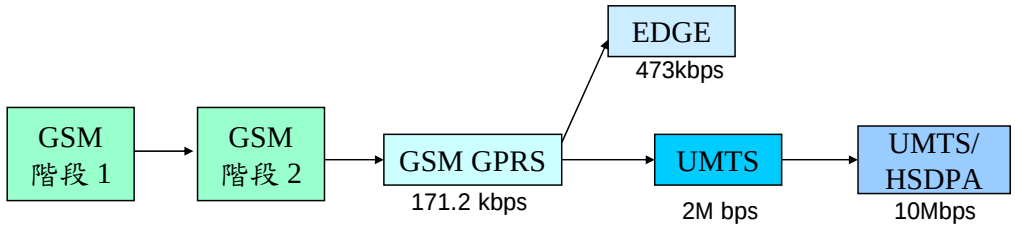
GSM 現況介紹
GSM Overview

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

5

圖 6-1 GSM 演進


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

6

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。

7

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

8

Section 6.2

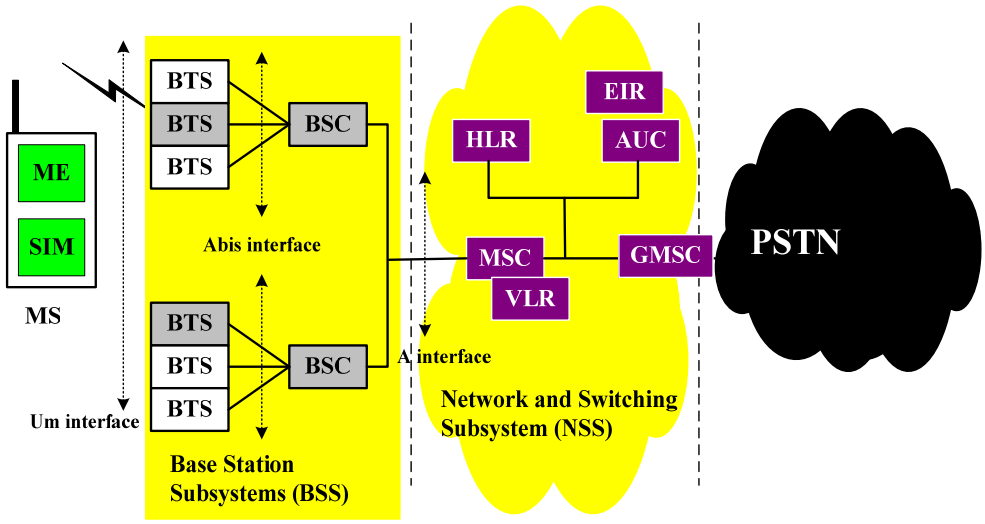
GSM 系統架構
GSM Architecture

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。

10

圖 6-2 GSM 系統架構圖



11

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。

12

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。

13

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。

14

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。

15

•GSM MAP是架在SS7之上為傳送行動網路控制訊號所寫成的軟體工作平台。

•習慣上NSS元件間的介面通稱為GSM MAP，而不再提底層的SS7網路。

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。

16

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

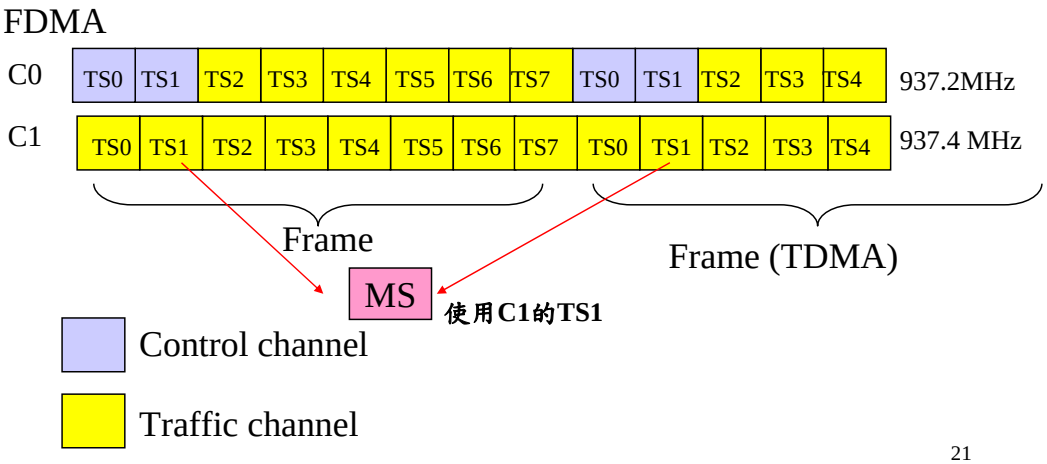
19

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



21

DCS 1800

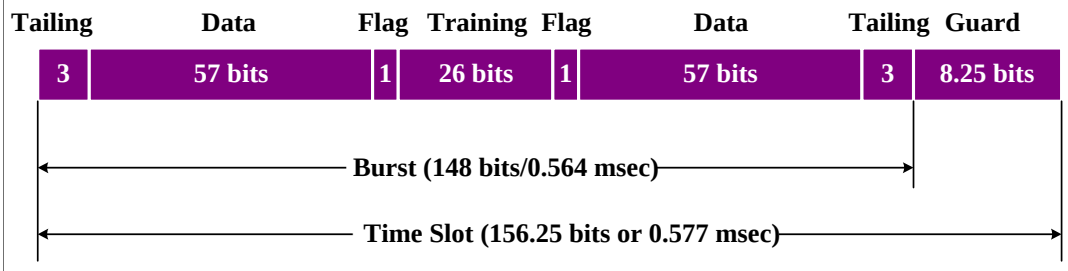
- 以GSM標準架構為基礎
- 使用1710-1785 MHz（uplink）與1805-1880 MHz（downlink）頻段的標準，稱為DCS 1800（Digital Cellular Standard 1800）或GSM1800。
- 美國使用1900MHz頻段的GSM系統，就被稱為DCS1900或GSM1900。
- 整合GSM與DCS1800可形成微細胞/巨細胞（microcell/macrocell）的架構。

22

GSM 的資料結構

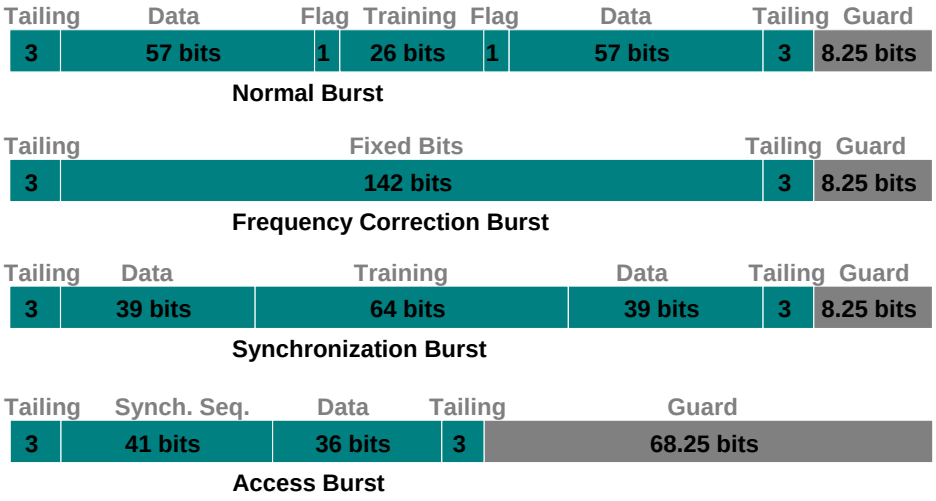
- 透過GSM傳送的資料都是以burst的型式加以封裝，再將資料放入時槽中傳送。
- 時槽內容包括burst與guard time。
- Burst的種類：
  - Normal burst用於傳送使用者語音或數據資料。
  - F burst放置基地台廣播的信號，讓MS校正頻率，以維持與基地台頻率上的同步。
  - S burst放置基地台廣播的信號，讓MS校正時間，以維持與基地台時間上的同步。
  - A burst是當手機想要打電話時，上傳A burst告知基地台欲使用無線電資源。

圖 6-4 Normal Burst



24

圖 6-5 GSM Bursts



25

•F Burst（Frequency Correction Burst）：F burst只在**FCCH**上傳送，Data欄位有連續的142個0，可讓MS校正自己的頻率以維持BTS頻率上的同步。

•S Burst（Synchronization Burst）：在**SCH**上傳送。特別加長爲64 bits的Training sequence，讓MS可以校正自己的時間。這是因爲S burst是第一個MS需要做demodulation的burst（F burst不須要demodulation），因此S burst的training sequence特別長。Data欄位傳送基地台識別碼（Base Station Identity Code，BSIC）和以及Frame number，MS得以取得與BTS的frame structure同步。

•A Burst（Access Burst）： 在RACH上傳送。像是手機主動打電話，則手機可在RACH上傳送A burst，告知基地台欲使用無線線路。由於可能同時有兩支MS在同RACH上同一個time slot，同時送出A burst，就會發生collision。

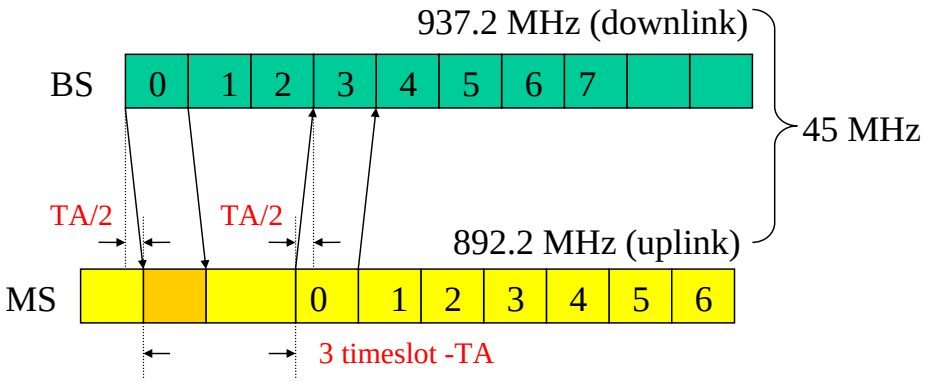
> •MS送出的A burst，事實上是MS與BTS溝通的第一個訊號，此時MS與BTS之間的同步不見得做得很好。爲使A burst能夠被BTS正確收到，A burst中只存放最基本的資訊讓BTS瞭解，因此A burst特別短，當MS晚一些才送出A burst，也能在Guard time結束前，被BTS收下。然而A burst又不能太短，讓一個time slot容下兩個A burst，因此A burst占了83 bits，比整個time slot（156.25 bits）的一半長了一些些。

•D Burst（Dummy Burst）：BTS沒有資料要傳送時所送出的空的burst。Mixed bit是modulating bit states。

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



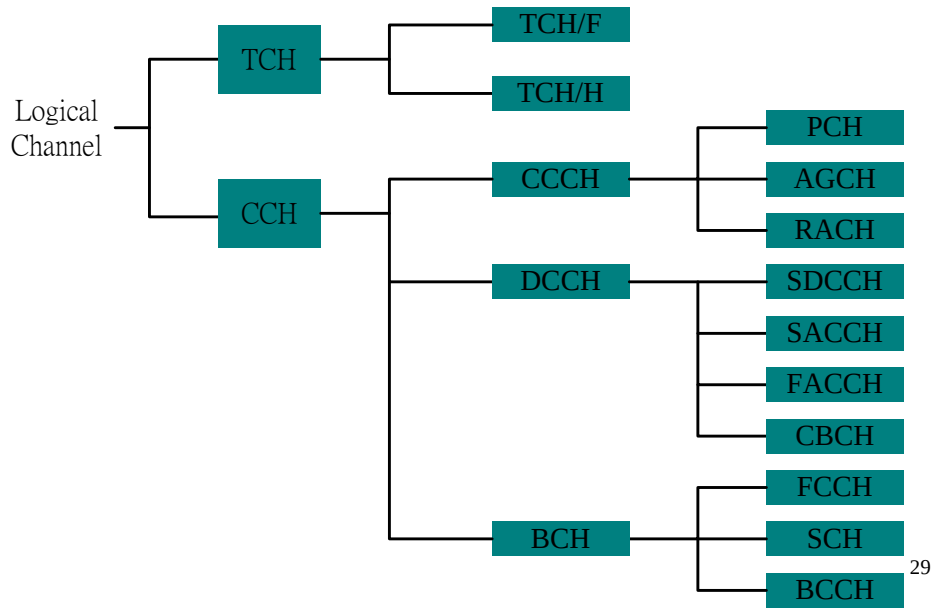
27

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。

28

圖 6-7 GSM 邏輯通道



•一個 BTS 與一個 MS 間用來傳送資訊的條通道稱爲 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， 所以稱爲 logical。

•基本上，分成 Traffic channel 與 control channel 兩大類.

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。

31

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。

32

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。

33

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)。

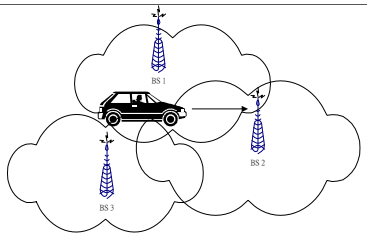
34

專屬控制通道（DCCH）(2/2)

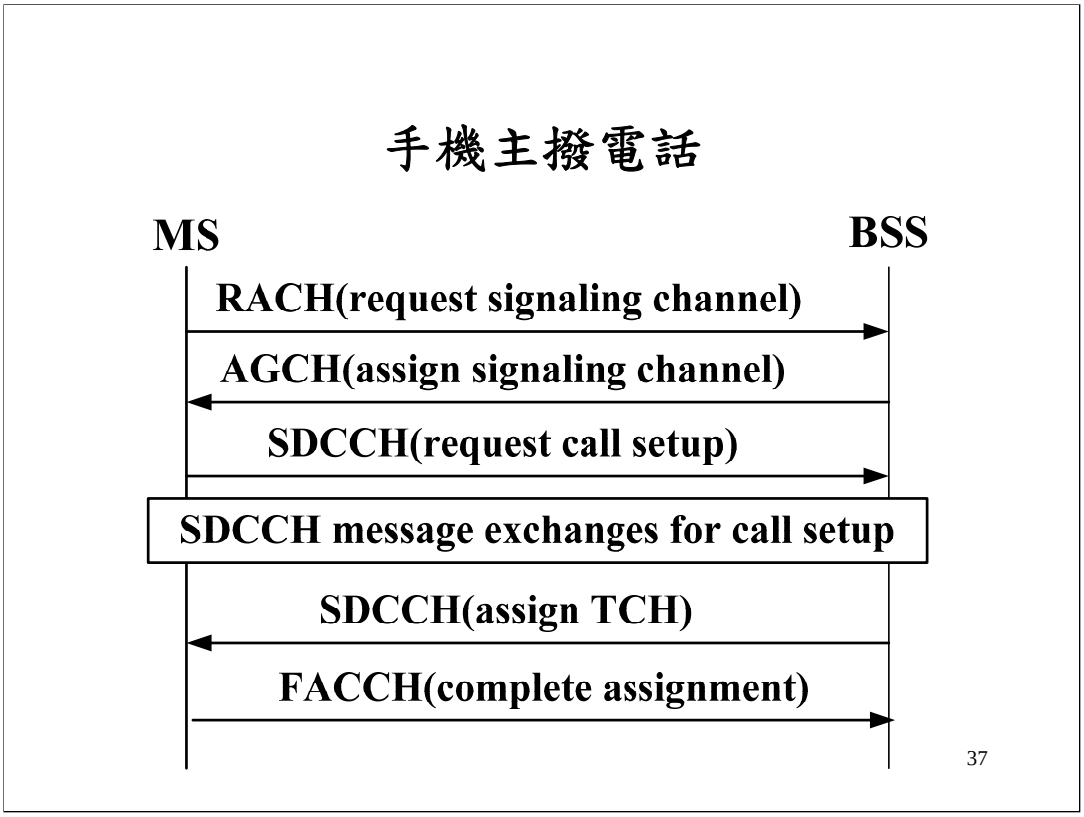
- 快速相關控制通道（Fast Associated Control CHannel，**FACCH**）
  - 傳送緊急控制信令（time-critical signaling），包括電話線路的設定、手機認證（authentication）以及交遞（handover）的信號。
  - **FACCH**佔用訊務通道的時槽。
- 細胞廣播通道（Cell Broadcast CHannel，**CBCH**）
  - 提供簡訊的廣播服務（short message service cell broadcast messages）。

35

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。



•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

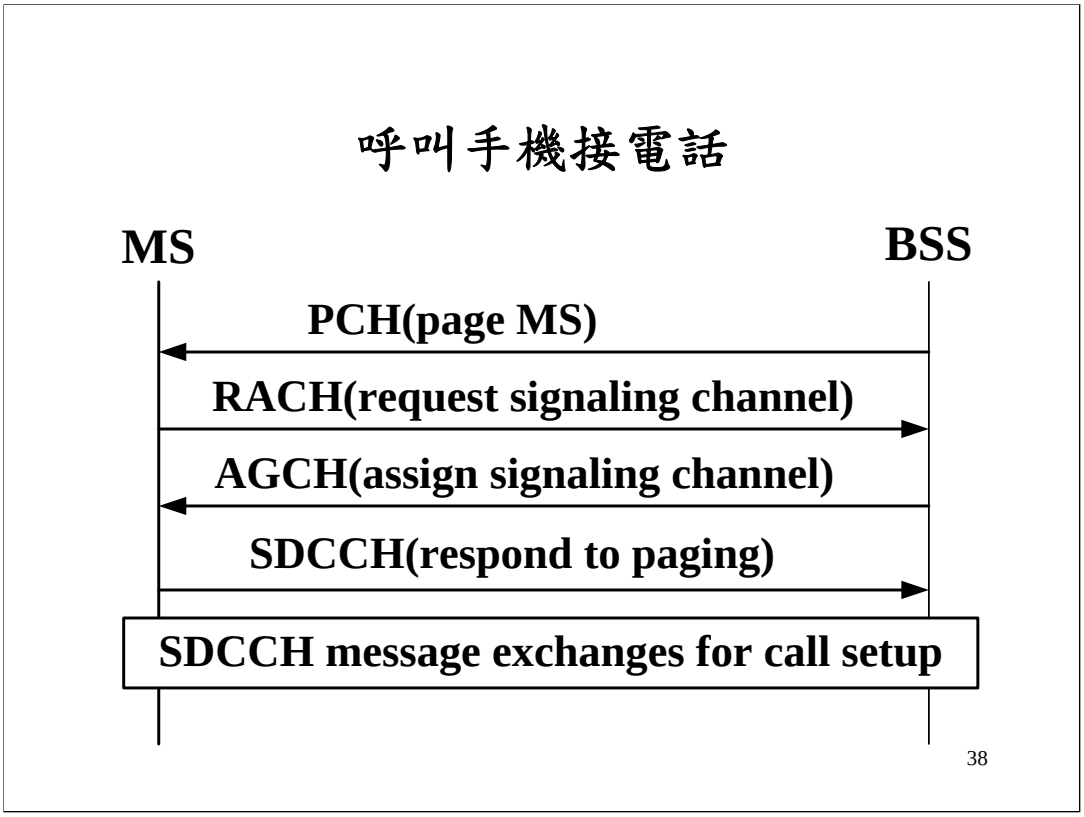
3.MS 用此 SDCCH 與 BSS 溝通, 送出所要撥打的電話號碼.

4.一旦電話接通, BSS 配置一個 TCH 給 MS, 收回 SDCCH.

5.MS 用 FACCH 通知 BSS 開始通話.

•不管是 call origination, call termination, 或是其他 user service, location update, 一定要先有 radio link 後才能夠送信令進一步溝通. 所以如果是 mobile initialization, 一定是從 RACH 開始, MS 送要求 radio resource 的request 給 BSC. BSC 問過 BTS 是否有資源後, 分配一個無線電通道給 MS. BTS 把這個 response 傳回給 MS 就會透過 AGCH.

•如果是 call termination, 由 network initialization, 就會多一個 paging 的動作.



•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)

- •PCH 上的 paging request message 若使用 TMSI, 最多可一次 page 4 個 MS.

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) 關於 IAM 等訊息

- •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.BSC 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.

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)

41

•行動話機的 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.

•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。

•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.

•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 又稱爲 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.

•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.

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

•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.

•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

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

•行動話機的 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）。此路由位址稱爲 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 又稱爲 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 做爲臨時的識別碼. 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.

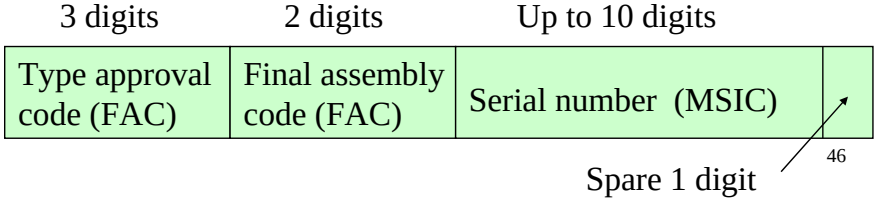
•TMSI 是用於當 MS 到一個 new LA 時, 表明自己的身分(取代傳送 IMSI),做 registration (location update) 用.

•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.

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,稱爲行動電話國際設備識別碼,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.

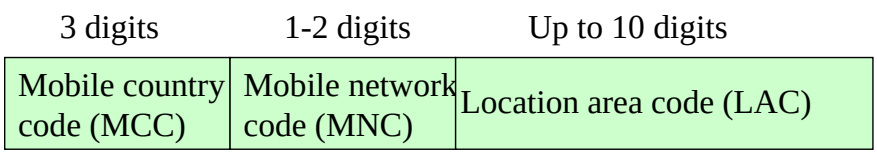
•當此 GSM component passes conformance and interoperability tests, 則會獲得此 TAC.

•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.

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



47

•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

48

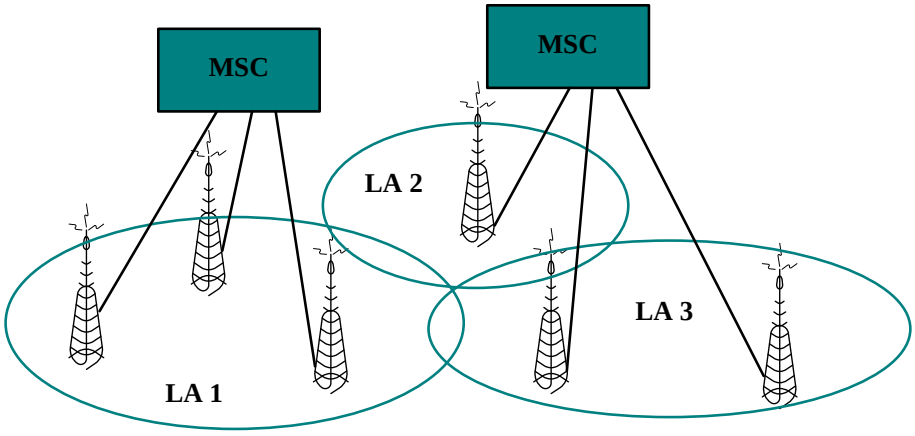
•每個 cell 都有自己的識別碼 CGI (cell global identity), 由 LAI 加 CI 組成

•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. 此動作稱爲 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, 則不去通知 BTS.

圖 6-8 位置區域示意圖

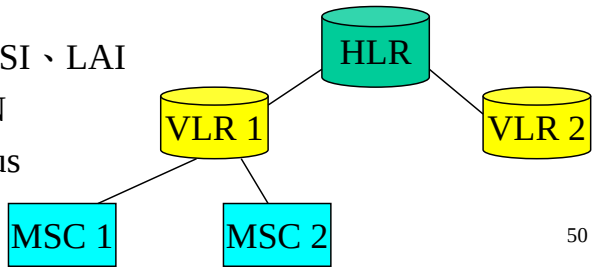


49

•GSM將服務範圍切割成許多位置區域（Location Area，LA），做爲GSM記錄手機位置的基本單位，換言之就是尋找呼叫手機的基本範圍。

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

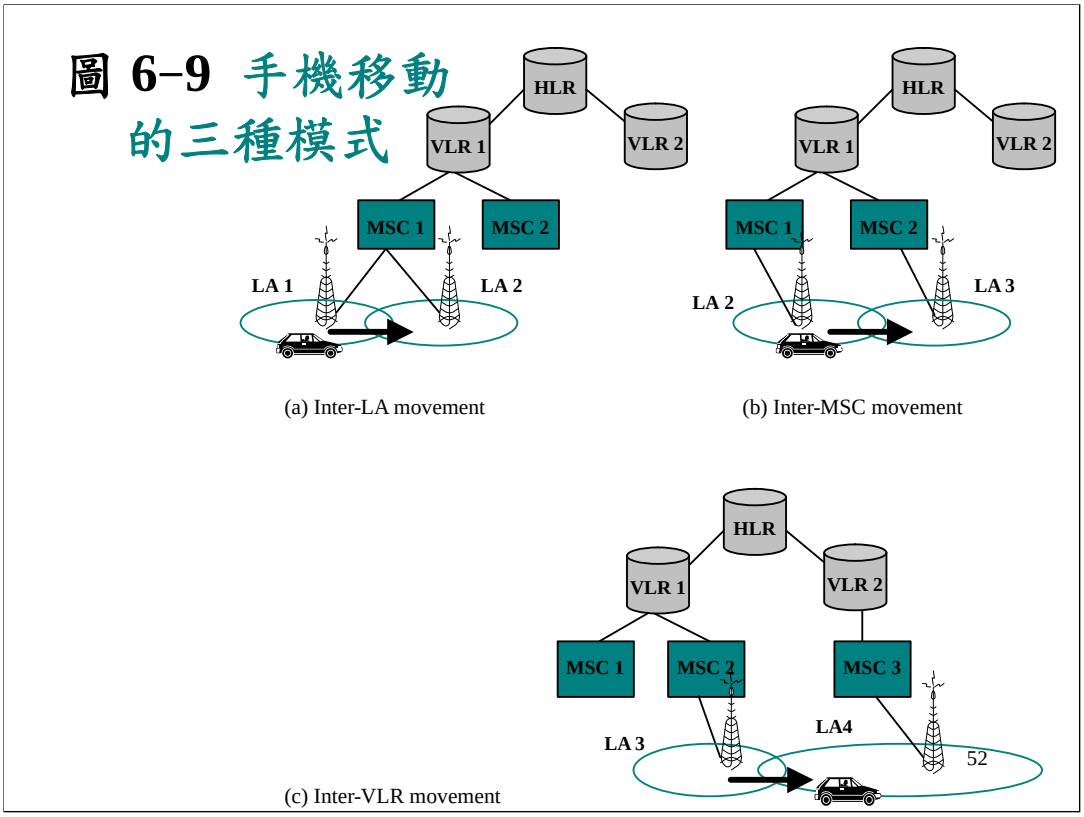


50

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。

51



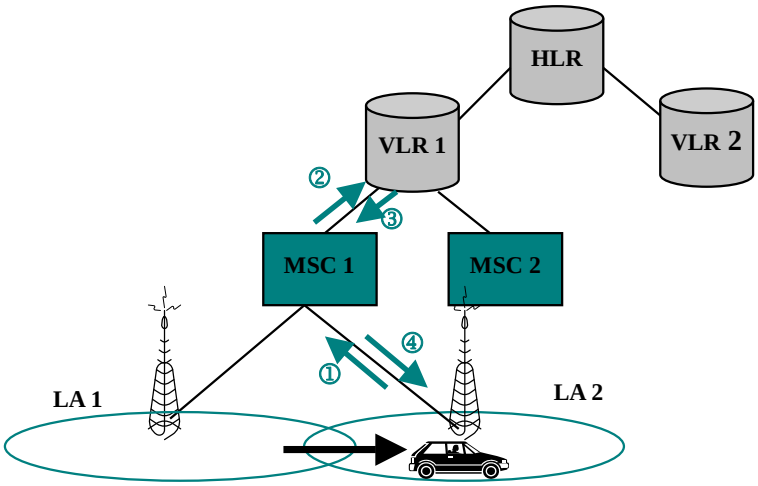
•當 MS 在待機狀況(idle, 沒有通話)且四處漫遊(roaming), 可能會測得鄰近的 BS 之訊號強度, 並由其 BCCH (Broadcast control channel) 得到 CGI (包括 CI 和 LAI). 如果新的 BS 訊號較佳, MS 會改用新的 BS 之 channel. 這時有幾種狀況:

- •New BS 與 old BS 有相同 LAI: 因爲仍在相同的 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. (因爲 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. 藉由下頁的圖的註冊程序，HLR 隨時可知道手機的正確位置。

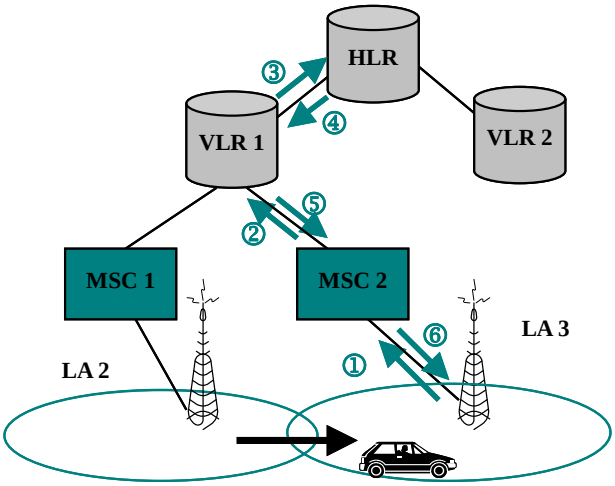
•HLR, VLR 利用上述的 identifiers 來記錄手機目前的位置.

圖 6-10 Inter-LA 的註冊流程



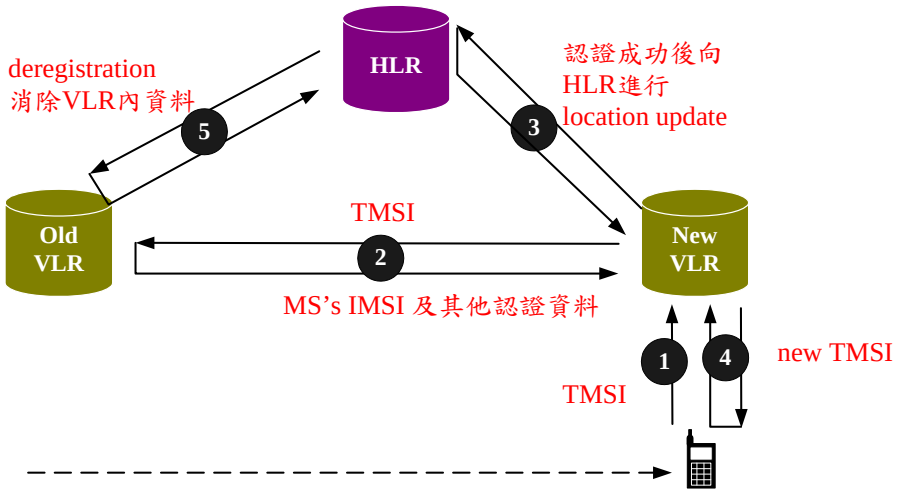
53

圖 6-11 Inter-MSC 的註冊流程



54

圖 6-12 Inter-VLR 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 MSC 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。

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.

56

•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 MSC 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。

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。

57

•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 MSC 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。

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。

58

•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 MSC 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。

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。

59

•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 MSC 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:

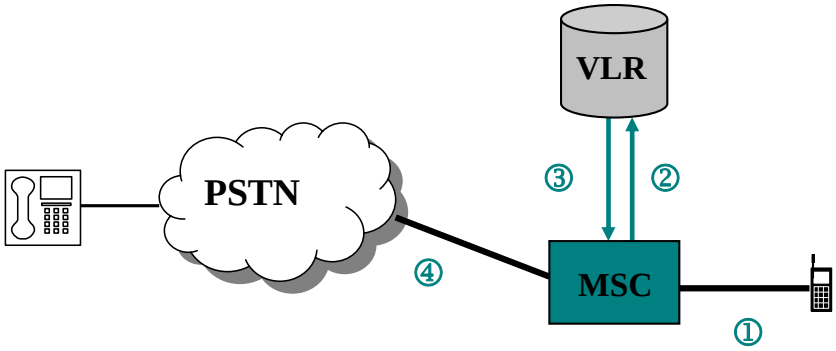
•在步驟3後，HLR 會送一訊號至舊的VLR，要求將手機的記錄消除。

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。

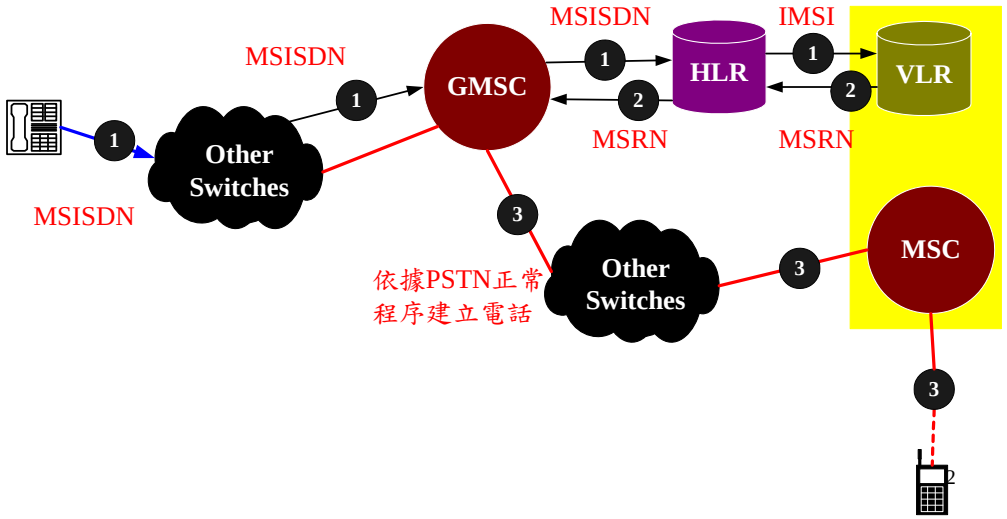
60

發話程序（Call Origination Procedure）



61

受話程序（Call Termination Procedure）



•Call termination 又稱爲 call delivery.

•GSM的通話控制與IS-41類似。

•假設發話者爲 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。

•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IAM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）。此路由位址稱爲 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:

交遞

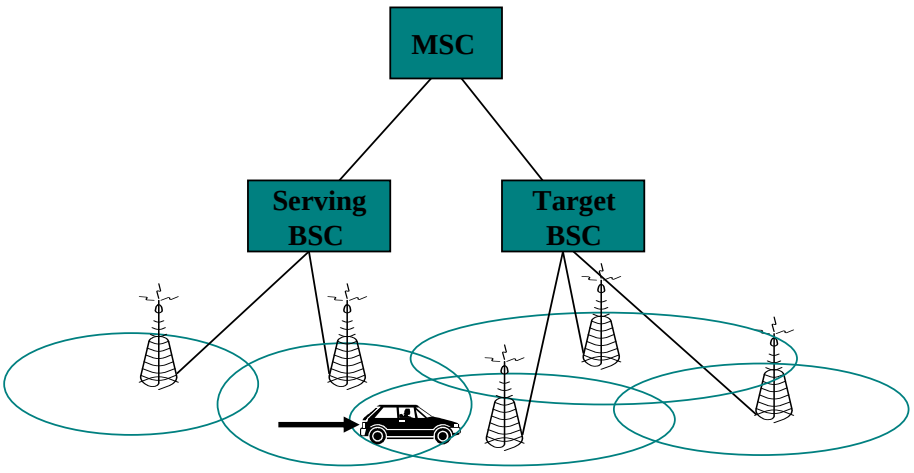
- 手機輔助交遞（Mobile-Assisted Handoff，MAHO）
- 由網路端主控且下決定進行交遞
- MS測量附近的BTS的訊號強度。
- 服務手機的BTS也會將MS語音上傳的訊號強度回報給網路端。

63

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

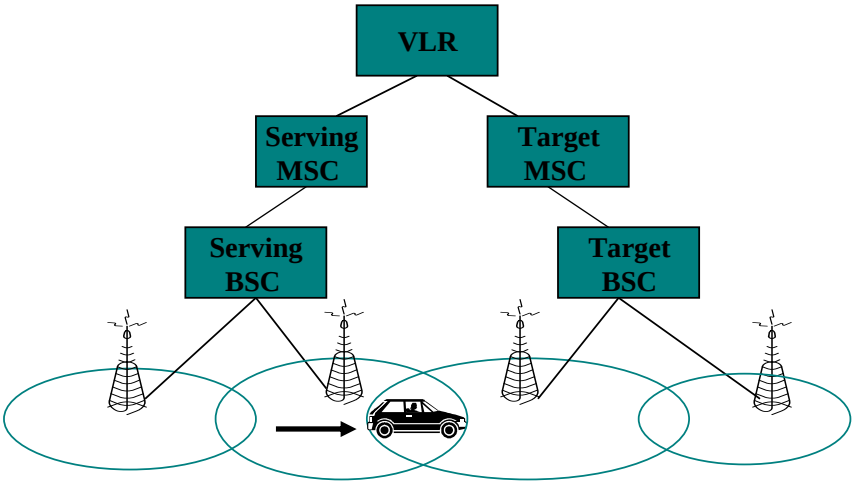
圖 6-15 Intra-MSC Handover



65

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 檢查是否有旗下 BSS 是在 candidate 中, 如果有就設定此 BSS 爲 target BSS, 進行 intra-MSC handoff. 此時需要兩 resources, 一是 MSC 與 target BSS 間的 truck, 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.
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.

圖 6-16 Inter-MSC Handover



66

- * 表示和 Intra-MSC 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 (稱爲 serving MSC) 發現 MS 已經離開他的服務範圍, 而到另一個 MSC(稱爲 target MSC) 之下, Serving MSC會用 target MSC 的 directory number 建立起到 target MSC之間的 trunk.
4. *Target MSC 送出 HAND_NUM 給 VLR, 要求取得MS的資料.
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 target BSS 與 new radio channel ID.
12. Serving BSS 將此訊息 HAND_COMM 轉送給 MS.
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.

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

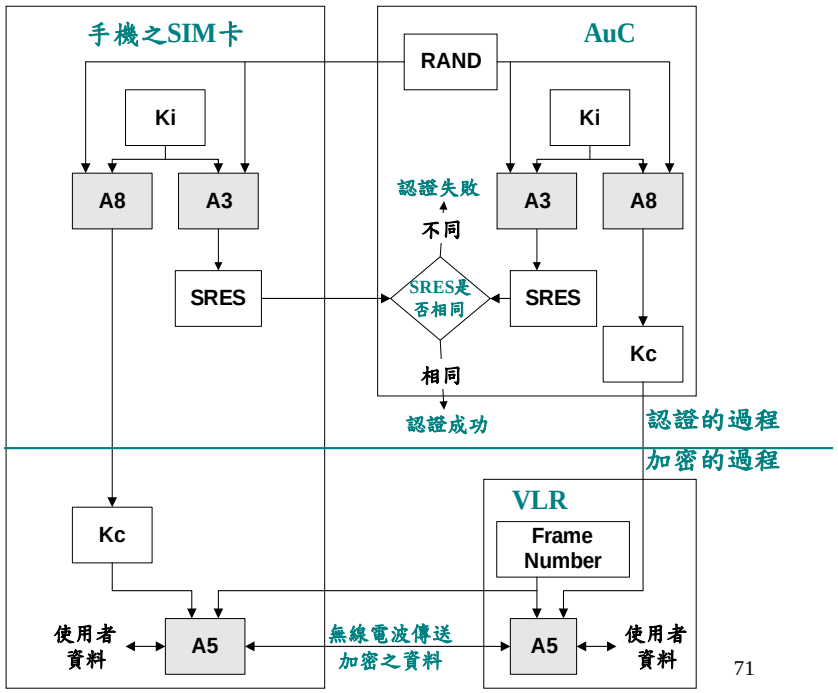
- 認證演算法
  - **A3.**
    - ✓用於認證的函數。
    - ✓只存於 AuC 和 SIM 卡中，用戶無法取得。
- 加密演算法
  - **A8.**
    - ✓用於產生加密鑰匙 (encryption key)。
    - ✓只存於 AuC 和 SIM 卡中，用戶無法取得。
  - **A5.**
    - ✓存於手機與所有的 visited system (如 BSS, VLR)。
    - ✓用於資料的加密 (ciphering) 與解密 (deciphering)。

69

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



•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.

•認証過程是利用一密秘鑰匙（secret key）Ki。

- •欲驗証一手機時，認証中心先產生一個128位元的亂碼（random number），稱爲RAND。
- •認証中心將 RAND 亂碼送至手機，此時認証中心及手機都使用Ki及RAND亂碼來執行一個所謂的A3演算法。
- •執行 A3 會產生 SRES。然後手機將產生之 SRES 回認証中心，與認証中心所產生之 SRES 做比較。
- •若結果相符則驗証成功，否則手機的要求就會被駁回。

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。

72

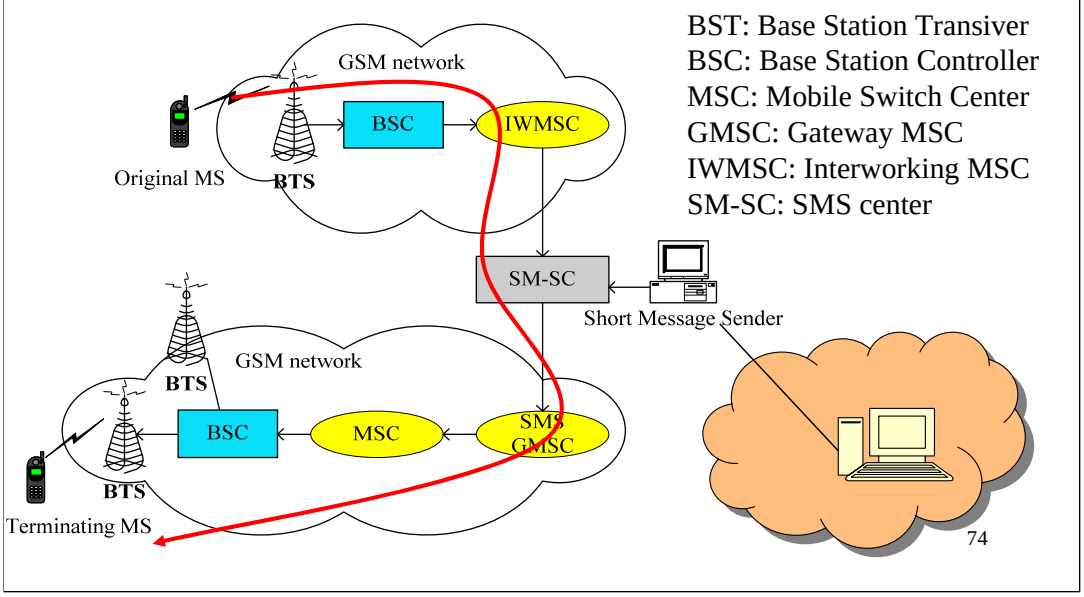
Section 6.7

簡訊系統
Short Message Service，SMS

73

•將SMS 架構作一個介紹，並說明傳送及接收的動作

圖 6-20 SMS 的架構



•簡訊服務中心**SM-SC (Short Message Service Center)** 負責 store and forward 簡訊.

•IWMSC 是接收 MS 送來的 short message, 並轉送給 SM-SC

•簡訊閘道行動交換中心 (Short Message Service Gateway MSC；SMS GMSC) 是接收 SM-SC 的要求, 對 MS 定位, 找出所在的 MSC, 再轉給 MSC 要發送的 short message.

•MSC: broadcast the SMS to all its BSSs.

•BTS: page the MS.

•考慮 MS 送 short message 給其他 MS 這一段的 steps. (Mobile Originating)

•**Step 1**: MS 送出的 short message 會先被送到 **IWMSC (Inter-working MSC)**.

•**Step 2**: short message 都會被傳送到 **SM-SC (Short Message Service Center)** 儲存. 簡訊服務中心在收到簡訊之後，便能根據該簡訊的需要而傳遞回應至發訊者。

•**Step 3**: 檢查 short message 的目的地, 再分別送出.

- •然而由手機發送簡訊, 會受限於手機按鍵介面不佳的因素, 因此有一些技術爲此發展出來:
  - •Predictive Text Input Algorithm: 設定一些 hot key (ex: 注音輸入法), 存於 MS 中, 減少 key in 次數.
  - •QWERTY keyboard: MS 附有 QWERTY keyboards

•考慮 SM-SC 送 short message 到 MS 這一段的 steps. 可能是 MS 送出的簡訊, 或由 Internet 上的 PC 做 page (Mobile Terminating)

•**Step 2**: SM-SC 透過簡訊閘道行動交換中心 (Short Message Service Gateway MSC；SMS GMSC) 將該簡訊傳送至目的地之 GSM 網路。SM-SC 並不會直接接到一般的 MSC.

•**Step 3**: 如同 GSM roaming protocol 的規範, GMSC 要找出 MS 所在的 MSC, 並將此 short message 轉送到 MSC.

•**Step 4**: MSC 要求 BSS 下所有 BTS 將 short message 以 broadcast 方式傳送

Mobility Databases

75

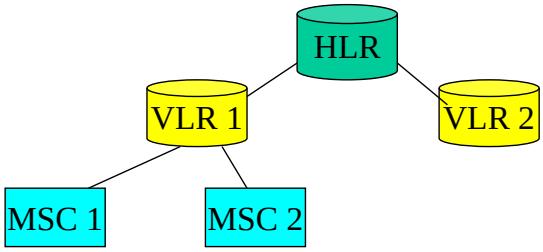
•在個人通訊服務系統中, 必須隨時記錄 MS 的動向, 所有的資料都會存在行動資料庫: VLR 與 HLR.

•以上所提到的 location update, call delivery 過程中都會用到 HLR 或 VLR 的資料, 所以我們將更深入了解 VLR 與 HLR 所包含的資訊.

•如果 HLR 或 VLR 發生意外 fail, 則系統無法找到 MS 正確的位置. 因此我們有必要仔細討論 HLR 與 VLR 的內容, 與討論當它們 crash 時, 如何應變處理.

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.



76

•GSM採用階層式(hierarchical)的資料庫管理架構.

•HLR是一個管理手機用戶資訊的資料庫.

•VLR是一個負責管理手機所到訪服務區域的資料庫.

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

77

•HLR 包含下面三類的資料:

- •每個MS的記錄內容包括 MSISDN + IMSI + VLR ISDN + MSC ISDN + Subscriber Status.

•MS information :

- •IMSI (國際行動用戶識別碼, 存取網路時作識別用途)
- •MSISDN (手機號碼)

•Location information:

- •VLR address (手機所在地的VLR位址)
- •MSC address (手機所在地的MSC位址)

•Service information:

- •Service subscription (用戶簽訂的服務) ex. call forwarding, international call,...
- •Service restriction (限制用戶的服務) ex. call barring
- •supplementary services (加值服務)

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

78

•VLR 包含下面三類的資料:

- •VLR 內每個 MS 的記錄內容包括 MSISDN + IMSI + LAI + TMSI + MSRN + Subscriber Status + HON.

•MS information

- •IMSI
- •MSISDN
- •TMSI

•Location information:

- •MSC address
- •LAI

•Service information: call forwarding, international call,...(subset of HLR)

Two Issues of GSM Mobility Databases

- **Fault Tolerance.**
  - If the database 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.

79

•因爲所有的動作都需要資料庫的支持, 所以一旦 database 發生狀況, 就會有狀況. 這裡我們將討論兩種 database 會出問題的情況:

•Fault Tolerance: 當位置資料庫損毀時, 位置資訊的遺失或毀壞將嚴重降低系統能提供給用戶的服務品質.

- •因此下面的章節將介紹一些 GSM failure restoration 的作法, 另外提出一相關的論文在探討如何盡量加速 GSM restoration 的時間.
- •這裡分別討論 VLR 與 HLR failure 的狀況.

•Database Overflow: 資料庫的容量是固定的, 因此當有太多的 MS 進到某一 VLR 的範圍, 使 VLR full, 再當有 MS 進入則沒有相對應的 record 可用, 因此無法註冊, 當然也無法或得 service. 這種狀況稱爲 VLR overflow.

- •下面的章節將介紹一些相關的論文, 探討如何盡量處理 VLR overflow.

VLR Failure Restoration

80

•當有太多的 MS 進到某一 VLR 的範圍, 使 VLR full, 再當有 MS 進入則沒有相對應的 record 可用, 因此無法註冊, 當然也無法或得 service. 這種狀況稱爲 VLR overflow. 這裡將介紹一些相關的論文, 探討如何盡量處理 VLR overflow.

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.

81

•VLR 內的資料如前所述分爲三大類. 當 VLR之前有failure時, 這三類的資料可分別在不同的時機重建獲得:

- •Mobile station information (IMSI 等): 當 VLR 第一次與 HLR 或 MS 接觸, 就可以得到 MS 的相關資料.
- •Location information (MSC ISDN 等): 當 VLR 第一次與 MS 接觸, 就可以得到 MS 的位置.
- •Service information: 當 VLR 第一次與 HLR 接觸, 就可以得到 此 HLR 下所有 MS 的相關資料.

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

82

•但是在 VLR 出錯之後, 如何 VLR 才能與 MS 或 HLR 做接觸?

•Answer: 只在下列三種事件發生時, VLR 才會有與 HLR 或 MS 接觸的機會, 獲得最新的正確資料, 才會啓動 VLR record restoration.

- •MS registration
- •MS call origination
- •MS call termination

•底下分別說明這三種狀況.

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.

83

•當 MS 進行 registration 時 (for example: periodical registration), 由於 VLR 沒有 MS 的任何資料, 因此會把這次註冊當作是 inter-VLR movement.

•VLR 依據 inter-VLR movement, 要求 MS 用的一般正常註冊程序進行.

•MS 會送出 old VLR ISDN 與 TMSI 給 VLR, 但是因爲所有資料都流失, VLR 無法判讀 TMSI 是否正確, 只好要求 MS 傳送 IMSI, 以確認身份.

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.

84

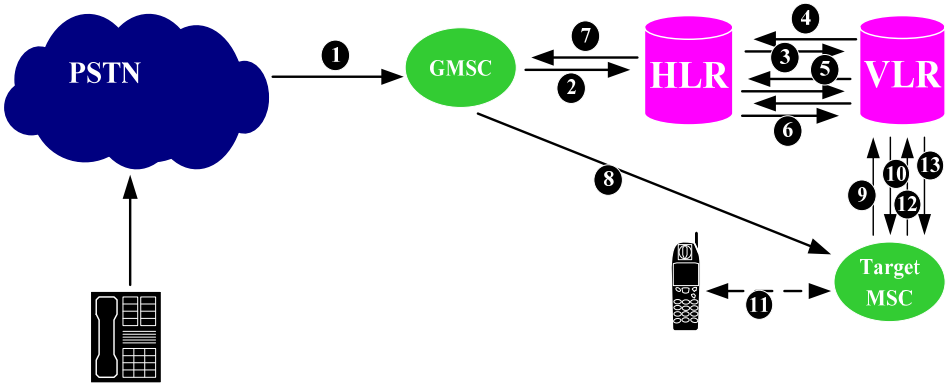
•當 MS 想要打電話時, MSC 會將 MAP_SEND_INFO_OUTGOING_CALL 的訊息轉送給 VLR.

•但由於 VLR 沒有 MS 的任何資料, 因此會把這個要求當成是 system error, 將 MS 視爲 unidentified subscriber.

•VLR 回絕此要求, 並要求 MS 進行同 inter-VLR 的 location registration.

•如此 VLR 便建立起 MS 的資料.

Restoration－Call Termination Message (1/2)



85

•當有人要打電話給此 MS, VLR 會利用此機會做 recovery.

•**Steps 1-3**. 就如同一般電話建立程序的前三個步驟, VLR 收到 HLR 要求提供 MS 的 MSRN, (MAP_PROBIDE_ROAMING_NUMBER).

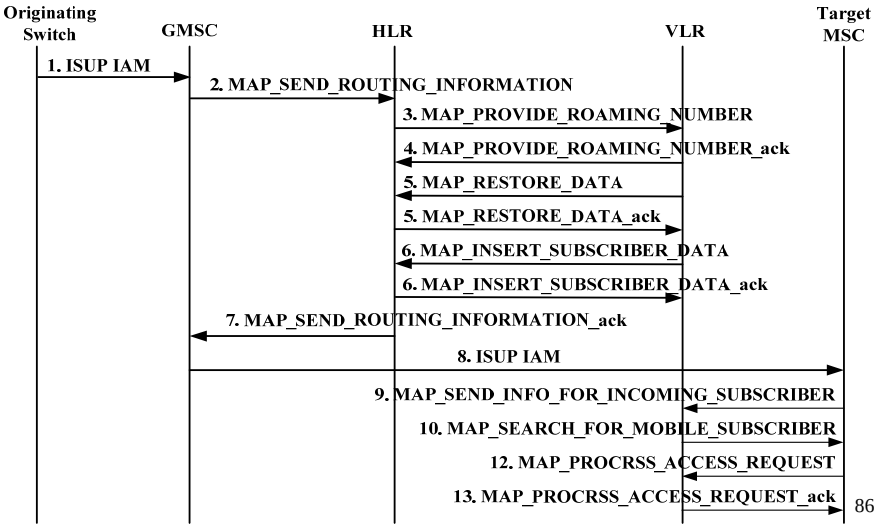
- •VLR 依據 HLR 送來之 IMSI 尋找 MS 的 record, 但由於 VLR 沒有 MS 的任何資料.
- •因此會幫 MS 建立一個新的 record. i.e., VLR 相信 HLR 的資料.

•**Steps 4-7**. VLR 會利用 HLR 送來的 MSC ISDN, 產生 MSRN, 送給 HLR 與 gateway MSC以便後來建立通話連線.

•**Steps 5-6**.

- •VLR 利用與 HLR 通信的機會, 進行 restoration. VLR 送 MAP_RESTORE_DATA 給 HLR.
- •HLR 回應 MAP_INSERT_SUBSCRIBER_DATA 有關用戶服務資訊的訊息給VLR.
- •此後, VLR record 便已被 recovered.
- •然而, VLR 中仍有許多資料沒有辦法由 HLR 取得, 包括 location information (LAI), TMSI.
- •注意: Step 4.與 Step 5.是可以平行同時執行的.

Restoration－Call Termination Message (2/2)



•延續上一頁的程序:

•**Step 8.** gateway MSC 在 Step 7.收到 HLR 送來的 MSRN 之後, 便送出 SS7 ISUP message IAM 到 target MSC.

•**Step 9-11**.

- •target MSC 此時還沒有 MS 的 LAI 資訊.
- •爲建立通話, MSC 送出 MAP_SEND_INFO_FOR_INCOMING_CALL 到 VLR 詢問 LAI.
- •不幸的是, VLR 也沒有 LAI 的資訊.
- •所以 VLR 便送 MAP_SEARCH_FOR_MOBILE_SUBSCRIBER到 MSC, 要求 MSC 來決定 MS 所在的 LA.

•**Steps 12-13**.

- •於是 MSC 在其所轄的所有 LA 發出對 MS 的呼叫.
- •若呼叫成功的話, MSC 送出 MAP_PROCESS_ACCESS_REQUEST 訊息將 MS 所在的 LA 位址送回 VLR.
- •此時 VLR record 的關於 MS 的 location information 就被 recovered.

•注意

- •MAP_SEARCH_FOR_MOBILE_SUBSCRIBER 是耗費資源的動作, 因爲 MSC 之下的每個 BTS 都必須執行這個呼叫動作.
- •爲了避免廣域呼叫 (Wide Area Paging), GSM 系統應週期性地要求 MS 主動作重新註冊 (re-register) 的動作.

HLR Failure Restoration

87

•此部份探討當 HLR failure 時, HLR 如何做 restoration.

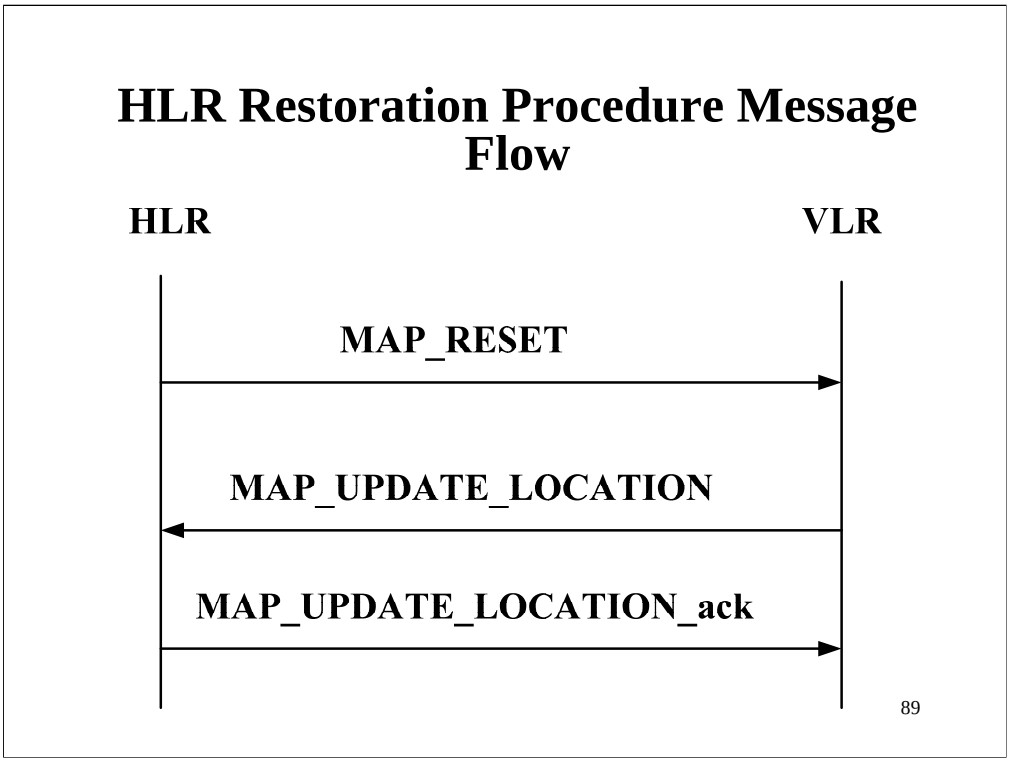
HLR Failure Restoration

- 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.

88

•HLR 發生錯誤還原的方式:

- •HLR 應該本身配置有像磁帶, 硬碟這類的非揮發之備份系統.
- •針對少量像是 service information 這樣的資料 (如提供 call forwarding), 要在 HLR update 時就同時存入 backup storage.
- •針對少量像是 location update 這樣的資料 (如 VLR, MSC ISDN), 要定期在每一個 check-point 做備份.
- •當 HLR 損壞時, 則由備份資料存回 HLR 中. 所以 service information 永遠是對的, 但 location information 就可能是過期的資料.



•當 HLR 損壞時, 則將備份資料存回 HLR 中.

•但由於備份中 location update information 並不是最新的, 所以會有一段時間的資料是 lost. 這段時間我們稱爲 uncovered period. 即最後一次備份到 HLR 損壞的時間.

•在 uncovered period 中送到 HLR 的資料會遺失, 所以無法回復. 需要系統主動進行下面的 restoration 的動作.

- •Step 1. HLR 送一個 SS7 TCAP 訊息 的 MAP_RESET 給該 HLR 掌管的所有 MS 所在負責區域的所有 VLRs.
  - •這些 VLR 將每一個 MS 的資料都用一個 SS7 TCAP 訊息 的 MAP_UPDATE_LOCATION 送回給 HLR.
  - •各個 VLR 不可以同時將MS 的資料送到 HLR, 會造成 traffic congestion.

Questions in HLR Restoration Procedure

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

90

•HLR 的 restoration 並不夠完整.

•例如 MS 若在 uncovered period 才移動到某些 VLR, 而且 backup 的資料中也沒有其他任何 MS 最後是在這個 VLR. 所以 HLR 就不會有此 VLR 的資料, 更不會通知這個 VLR 送 update 資料.

•HLR 就不知道在故障前最後一次check-point time時, 手機所屬的 VLR 位址.

•因此, HLR 就不知道要去對這個 VLR 作如同上一頁的 MAP_RESET 動作.

•要改善這個問題, 因此有人提出 VLR Identification Algorithm, 簡稱爲 VIA.

VLR Identification Algorithm (VIA)

91

•爲了解決 standard 中 HLR 的 restoration 並不夠完整的問題, 因此有人提出 VLR Identification Algorithm, 簡稱爲 VIA.

•以下將說明 VIA 的作法.

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

92

•VIA 識別演算法:

- •VIA 的精神在記錄最後一次 backup 後, 所有與曾經與 HLR 接觸過的 VLR. 如此在做 HLR restoration 時, 就不會 loss 任何 VLR, 沒有通知到.
- •因此 VIA 識別演算法可在 HLR 發生故障後, 確實找出所有VLR.

•需在HLR內多加上一個資料結構.

•也需加上一些處理程序:

- •檢查點程序 Check-point procedure
- •註冊程序 Registration procedure
- •還原程序 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***.

93

•爲簡化複雜的說明, 我們假設每個 VLR 只包含一個 MSC.

•爲了實做 VIA, 我們需要儲存更多的資料, 因此要增加 database 的 data structure.

•HLR 加上包含所有在 uncovered period 有送來 MS update 的 VLR 的 list. 必須每當有 MS update 時即立即修改此 list, 存於非揮發 storage.

•此 list 稱爲 VLR_List*.

•所以在 HLR 損毀重建時, 只要對 VLR_List* 中的 VLR 送出 MAP_RESET 即可.

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*.

94

•爲了更減少網路上 restoration 的 traffic, VIA 又增加下面的 data structure:

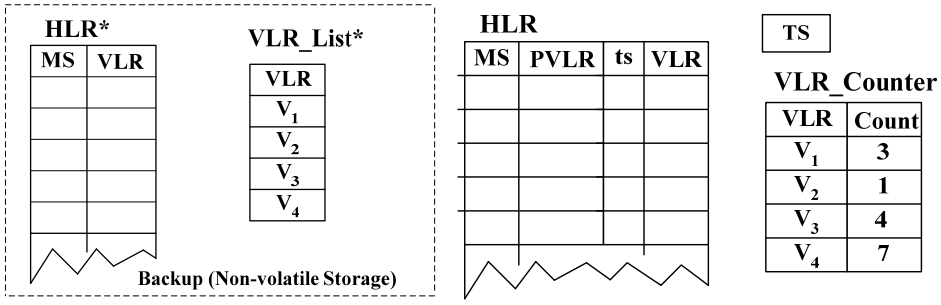
•HLR* : 記錄每一個 MS 的資料, 各需要 2 個欄位.

- •ts: (time stamp) 此 record 最後一次修改的時間.
- •PVLR: (previous VLR) 在最後的 check-point 時, MS 所在的 VLR.

•對整體 HLR 也要增加 2 個欄位:

- •TS: 最後 backup 的時間 (check-point 時間).
- •VLR_Counter: 每一個 VLR 都有一個相對欄位 (VLR,Count), Count 是在 uncovered period 才進入此 VLR 的 MS 的個數.
- •如果在 uncovered period 間, 有 MS 進入一個 VLR, 但又在期間內離開, 這樣的無效的 MS 是不需算在 VLR_Counter 中的 count n.

VIA Data Structure



95

•VIA 的資料結構.

•Backup 需存於非揮發 storage.

•VLR_List* 包含所有在 uncovered period 有送來 MS update 的 VLR.

•HLR* : 記錄所有 MS 的資料

- •每一個 MS 需要如下 2 個欄位
  - •ts: (time stamp) 此 record 最後一次修改的時間.
  - •PVLR: (previous VLR) 在最後的 check-point 時, MS 所在的 VLR.

•對整體 HLR 也要增加 2 個欄位:

- •TS: 最後 backup 的時間 (check-point 時間).
- •VLR_Counter: 每一個 VLR 都有一個相對欄位 (VLR,Count), Count 是在 uncovered period 才進入此 VLR 的 MS 的個數.

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;

96

•VIA Procedure 1: Check-pointing, 在 VIA 中, HLR 資料結構定期按以下檢查步驟作備份

- •Step 1. 對每一個位置紀錄都存入備份.
- •Step 2. TS設爲檢查的時間.
- •Step 3.
  - •HLR[p].ts 設爲 TS, 表示手機位置已更新, 時間則是最近的檢查時間.
  - •HLR[p].PVLR 設爲手機現在的位置 HLR[p].VLR
- •Step 4. 將 VLR_Counter 及 VLR_list* 設爲空的, 表示在 TS 時沒有一個 VLR 有新的漫遊手機.

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;

97

•VIA Procedure 2: Registration, 假設手機 p 在時間 t 時移動至 VLR Vnew, 則 Vnew 會送一個 MAP_UPDATE_LOCATION 訊息到 HLR, HLR便執行註冊動作.

•Step 1. 更新 HLR 資料結構

•Vold ← HLR[p].VLR

•HLR 送出 MAP_CANCEL_LOCATION 訊息到 Vold, Vold 內關於 p 的資料被刪除.

•新的 Vnew 紀錄被存到 HLR[p].VLR 中.

•told 被存放起來作未來之用.

•HLR[p].ts 更新爲 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;
   }
}
```

98

•Step 2. 更新在 VLR_Counter 內 Vnew 的 Count 欄位.

•若 HLR[p].VLR <> HLR[p].PVLR (表示 p 已換到 Vnew,) 則

- •若 VLR_Counter[Vnew] 存在, 則將 VLR_Counter[Vnew].Count 加1 .
- •反之, 即 VLR_Counter[Vnew] 不存在, 則新增一份 VLR_Counter[Vnew] 及一份 VLR_List*[Vnew], 並將 VLR_Counter[Vnew].Count 設爲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];
   }
}
```

99

•Step 3. 更新在 VLR_Counter 內的 Vold 的 Count 欄位.

- •若 told > TS (表示手機在 uncovered period 時才移動到 Vold) 且 Vold <> HLR[p].PVLR (表示手機在t之前已移出 Vold) 則
  - •將VLR_Counter[Vold].Count 減1. (表示手機雖曾移動到 Vold, 但已經移出, 是無效而不必紀錄的).
  - •若VLR_Counter[Vold].Count 爲0時, 則順便將 VLR_Count[Vold] 和 VLR_List*[Vold] 刪除.

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;
}
```

100

•VIA Procedure 3: Restore

- •Step 1. 將 TS 設爲目前的時間.
- •Step 2.
  - •對每一筆在 HLR 內的位置紀錄 p , 將備份資料 HLR[p]*.VLR 還原回 HLR[p].PLVR 及 HLR[p].VLR
  - •並將 HLR[p].ts 設定爲 TS
- •Step 3. 對每一筆在 VLR_List* 中的 VLR 紀錄均發出 MAP_RESET 訊息到其對應的 VLR, 要求執行一般的HLR還原程序.

VLR Overflow Control

101

•資料庫的容量是固定的, 因此當有太多的 MS 進到某一 VLR 的範圍, 使 VLR full, 再當有 MS 進入則沒有相對應的 record 可用, 因此無法註冊, 當然也無法或得 service. 這種狀況稱爲 VLR overflow. 這一章節將介紹一些相關的論文, 探討如何盡量處理 VLR overflow

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

102

•VLR 所存放的 record 的數量可以動態改變.

•有可能 VLR 的紀錄數量比 HLR 還多.

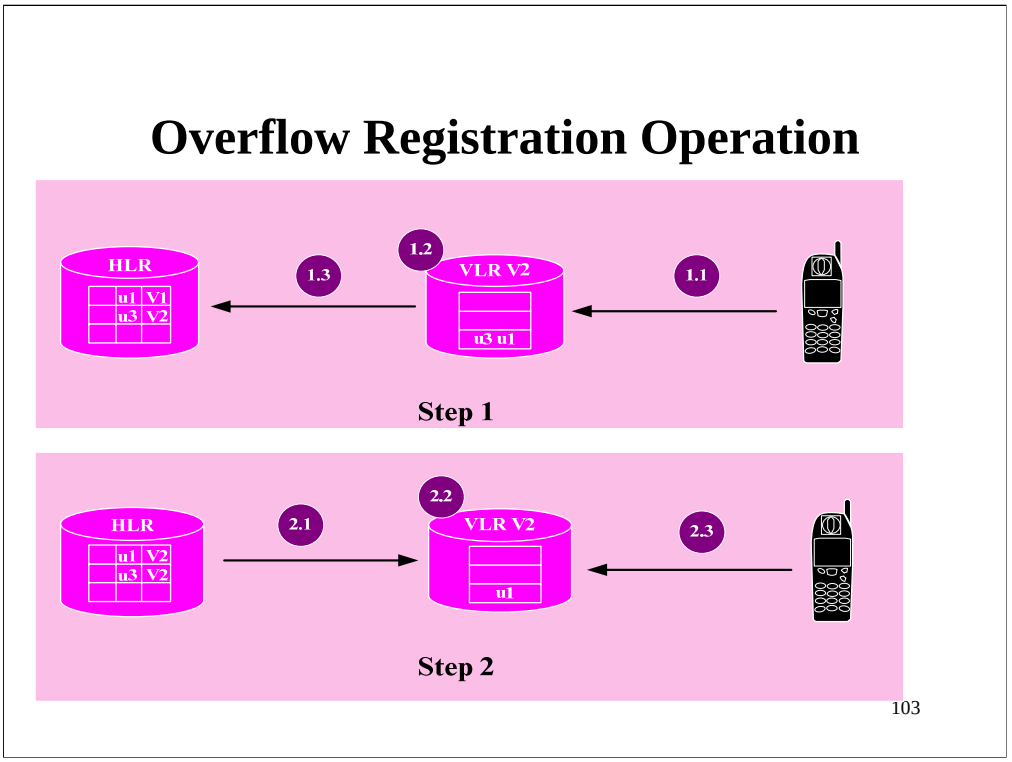
•如果大量的行動用戶在短時間內同時移動到某個 LA 時, VLR有可能因此發生overflow問題.

•當 VLR 已滿載時, 再進入此區的行動用戶不能再向它註冊.

•由於 VLR overflow 是無法解決的 (除非增加硬體設施), 所以在 paper 中提出我們必須修下面的 message flow, 盡可能讓 new arrival MS 獲得服務.

•底下會提到的 message flow 包括 registration, cancellation, call origination, call termination 的處理, 都需要做進一步的修改.

•當然要負出代價. 在 VLR 中正確的 record 被犧牲, 存放 new arrival MS 的資料, 萬一犧牲者想打電話或要接電話, 就要花費更多的程序救回來.



•Step 1: Registration Request:

- •Step 1.1: normal registration.
- •Step 1.2: VLR V2 is full. VLR 使用 replacement policy 選出 u3 的 record 被 deleted, 改存 u1 的 data.
- •Step 1.3: VLR forward registration request to HLR. VLR 通知 HLR u3 的 record 因 overflow 而被 deleted.

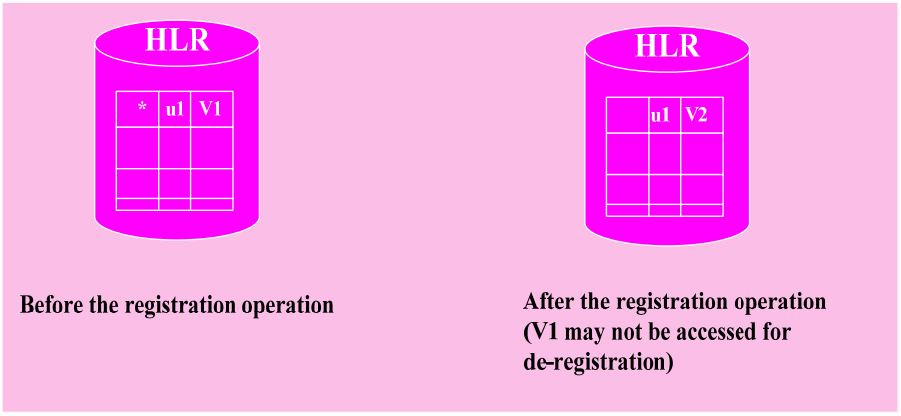
•Step 2: Registration Response:

- •Step 2.1: HLR 修改 u1 的 record, 並註明 u3 在 VLR 因爲 VLR overflow 已經無 record.
- •Step 2.2: HLR 送給 VLR u1 的 profile.
- •Step 2.3: VLR 送 ack 給 u1.

•Note that:

- •u3 被稱爲 overflow user.
- •replacement policy 有不同的 heuristics. 例如, randomly, select the oldest record, select an inactive record.

Cancellation Operation with Overflow VLR



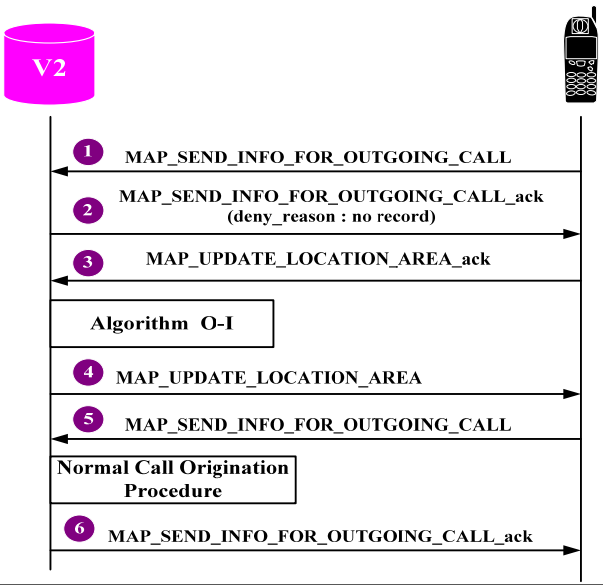
104

•如果 VLR1 overflow, 且選擇 u1 是 overflow user.

•因爲 overflow user 在 HLR 會被標示 * 表示 u1 在 VLR 1 已無資料, 所以當 u1 roaming 到 VLR 2, VLR 2 無法從 VLR 1 得到任何 u1 的資料.

•所以 VLR 2 在進行完 u1 的 registration 後, HLR 不會送 de-registration 給 VLR 1, 只會更改 u1 的 record (* 不見了).

Call Origination with Overflow VLR



105

•如果 VLR 2 overflow, 且選擇 u1 是 overflow user.

•若 u1 想要打電話, 就會發生 VLR 2 沒有 u1 的資料的問題.

•Solution:

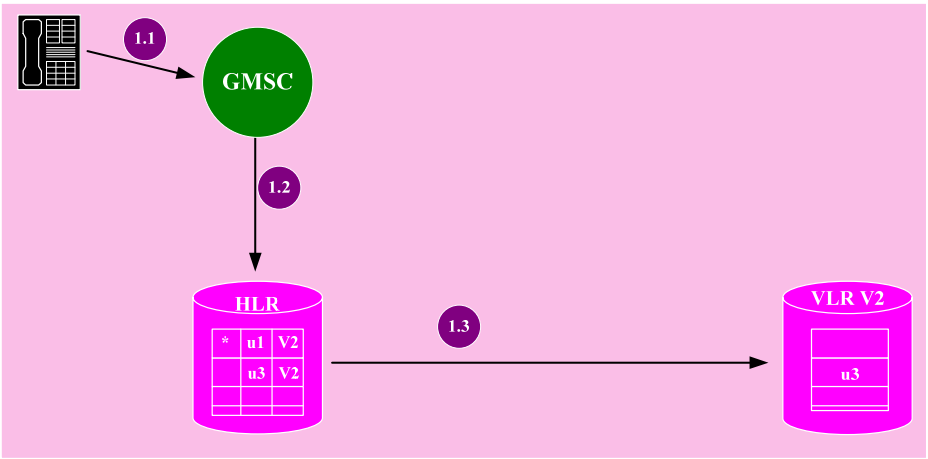
•Step 1: MS sends the call origination request to VLR 2.

•Step 2: VLR 2 沒有 u1 的資料. 不允許 u1 打電話.

•Step 3: u1 重新 registration. 但若此時仍造成 VLR 2 overflow, 則 “Overflow Registration Operation” 就會被執行.

•Step 4: MS 重新要求 call origination request. VLR 2 進行正常的打電話程序.

Call Termination with Overflow VLR (1/2)



106

•如果 VLR 2 overflow, 且選擇 u1 是 overflow user.

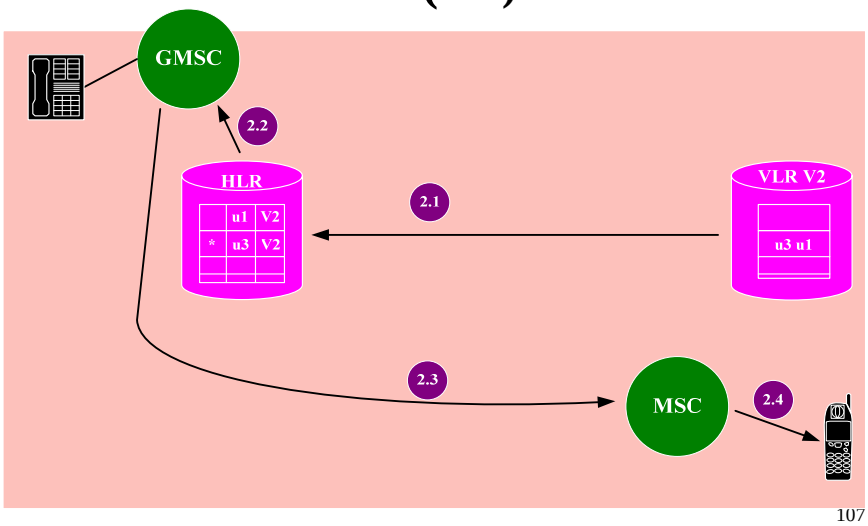
•若有 PSTN user 想要打電話給 u1, 就會發生 HLR 發現 VLR 2 沒有 u1 的資料的問題.

•Solution:

•Step 1: Location query

- •Step 1.1: Call party 打電話給 u1, 此通話被轉送到 GMSC.
- •Step 1.2: GMSC 將詢問 u1 位置的要求送到 HLR.
- •Step 1.3: HLR 有標示 * 表示 u1 在 VLR 1 已無資料, 但是 HLR 仍嘗試將 u1 user profile 附在 location query 後送到 VLR 2, 找尋 u1 的位置資料.

Call Termination with Overflow VLR (2/2)



•Step 2: location response

- •Step 2.1:
  - •如果此時 VLR 2 is not full, 則爲 u1 建立一 record.
  - •如果此時 VLR 2 is full, 則爲將 u3 取代, 爲 u1 建立一 record, “Overflow Registration Operation” 就會被執行.
  - •VLR 2 傳回 routable address.
- •Step 2.2: HLR 傳回 routable address. 若 u3 被取代, 會被標示*.
- •Step 2.3: Switch 依據 routable address 建立到 u1 所在 MSC 之間的 trunk.
- •Step 2.4: MSC page u1. 完成 call path 的建立.

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