

IS-41 Network Signaling

1

IS-41 是 AMPS, IS-136, IS-95 等系統所使用的核心網路的訊號交換系統。在這個部分，我們將介紹 IS-41 的 mobility management 與 security。雖然在台灣主要是採用 GSM 系統，但是對 IS-41 有所了解，可以做為一個與 GSM MAP 比較的對象，以討論各個通訊系統的優劣，進一步了解訊號系統設計的精神。

Reference

- [1] Wireless and Mobile Network Architectures ,
Y-Bing Lin and Imrich Chlamtac , Wiley
Computer Publishing.
 - Chapters 5, 6.
- [2] Mobile and Wireless Networks , Uyles
Black , Prentice Hall.
 - Chapters 6, 7.
- [3] Wireless and Personal Communications
Systems , Vijay K. Garg and Joseph E.
Wilkes , Prentice Hall.
 - Chapter 10.

Outlines

- Introduction to IS-41 Protocol
- Mobility Management Using TCAP
- IS-41 Authentication
- Call Control for Without-sharing (WS) Scheme
- Call Control for Sharing Scheme
- Summary

3

- 這個檔案介紹下面各個項目:
- 簡介 IS-41 協定
- 在 IS-41 中使用 TCAP 作 Mobility Management
- IS-41 的身分驗證的方式
- 在 IS-41 中有提供兩種認證的模式, Without-sharing (WS) Scheme 與 Sharing Scheme. 以下分別說明這兩種的電話控制. 同時比較此兩種模式的網路 traffic.
- Summary

Introduction to IS-41 Protocol

4

- 這部份簡介 IS-41 協定與 AMPS.
- 我們會詳細介紹 IS-41 各層協定, 與其運作的方式.

AMPS

- Analog cellular system in 1G
- Advanced Mobile Phone System
 - Bell Labs
 - Allow the reuse of radio frequencies by using concepts of cells
 - EIA/TIA-533 is the formal specification for AMPS air interface.
 - EIA/TIA Interim Standard 41 (IS-41 or ANSI-41) is the protocols defined for PCS Network (PCN) intersystem operations.

5

- AMPS 規格在 state diagrams 和 time-transition diagrams 風行前就寫好了.
- AMPS 的前身是 IMTS, 由 Bell Labs 主導.
- 為了增加 capacity, AMPS 採用 cell 的概念, 來實現 frequency reuse.
- AMPS 的 air interface 的正式規格稱為 EIA/TIA-533.
- AMPS 的網路管理協定的規格稱為 EIA/TIA Interim Standard 41 (IS-41 or ANSI-41), 用於定義 PCS Network (PCN) 上的 intersystem operations.

Identification Numbers

➤ Three identification numbers are used in AMPS:

- Mobile serial number (MSN) or Electronic serial number (ESN)
 - ✓ 32-bit uniquely identifies a cellular unit
- System identification number (SID)
 - ✓ 15-bit assigned to cellular systems
 - ✓ FCC assigns one SID to each cellular system
- Mobile identification number (MIN)
 - ✓ 34-bit number
 - ✓ Derived from the MS's 10-digit directory telephone number

6

- AMPS 中有三個重要的 ID: SN, SID and MIN. 另外每個手機有 10-digit 的電話號碼,
- MSN 是 32-bit 的手機之序號, 又稱為 ESN, 燒在手機的 ROM 中.
 - bits 24-31是 MFR code (8-bit Manufacturer's code),bits 18-23: reserved, bits 0-17: Serial number (assigned by manufacturer)
 - 當 AMPS 剛發展出來, 用戶很少, MSN 與 MIN 透過 air interface 傳送, 用來當做 authentication 使用.
- SID 是 15-bit 的系統業者的號碼, 由 FCC 分配給 cellular system.
 - 手機傳送 SID 告知到 BS 自己所屬的 cellular system, 如此 BS 知道要與那一個 system 溝通.
- MIN 是由手機的 10-digit 電話號碼所產生出來的 34-bit number.
 - MIN 34 bits 包含 MIN1 (24 bits 或 7-digital directory number), MIN2 (10 bits 或 3-digital area code).

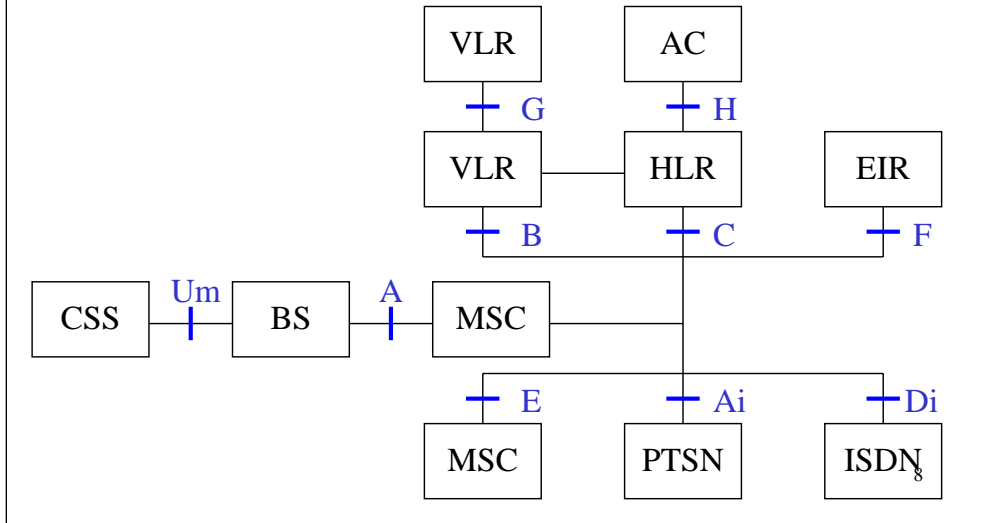
IS-41

- IS-41 is designed to use to manage **the network side** of the cellular call.
 - IS-41 is a partner to AMPS.
 - Comparable to GSM MAP
- IS-41 relies on
 - Layered protocols
 - X.25 and SS7 to support its lower layer operations

7

- IS-41 是設計於使用在 AMPS 上, 管理網路端的通訊協定.
 - IS-41 可說是 AMPS 的夥伴.
 - IS-41 與 GSM MAP 是相對等的協定, 可以互相比較, 了解彼此間的優劣.
- IS-41 架構在 layered protocol 的觀念上, 並使用 X.25 及 SS7 以支援下層的運作.

IS-41 Entities and Reference Points



- 這是 IS-41 Entities及 Reference Points 的概念模型, 與其他 PCS 或 GSM 的 model 相似.
- 各 entity 可能包含數個 function entities 及設備內部的 reference points.
- 圖中 reference points 用於描述 IS-41 各實體之間的介面與程序關係.
 - Ex: AMPS 中的 Um interface 是與 mobile station 及 land station 之間相關的運作.

Entities

- AC (Access Control)
- BS (Base Station)
- CSS (Cellular subscriber station)
- EIR (Equipment identity register)
- HLR (Home location register)
- ISDN (Integrated services digital network)
- MSC (Mobile switching center)
- PTSN (Public telephone switched network)
- VLR (Visitor location register)

9

•IS-41的組成實體:

- AC (Access Control)
- BS (Base Station)
- CSS (Cellular subscriber station)
- EIR (Equipment identity register)
- HLR (Home location register)
- ISDN (Integrated services digital network)
- MSC (Mobile switching center)
- PTSN (Public telephone switched network)
- VLR (Visitor location register)

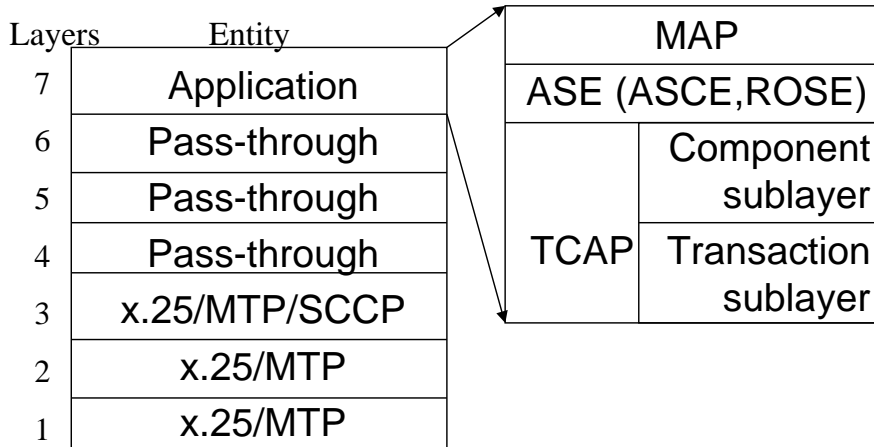
ID for IS-41

- IS-41 uses identifiers of AMPS.
- In addition, IS-41 uses
 - Switch number (SWNO)
 - ✓ It uniquely identifies a particular switch within a group of switches.
 - Switch identification (SWIN)
 - ✓ SWIN is the parameter derived from the concatenation of the SID and SWNO.

10

- IS-41 使用 AMPS 所定義的 identifiers.
- IS-41 上的 switch 必須有一個號碼來指定, 這個 ID 分成兩部份
 - SWNO 可想成是一個 cellular system 下之 switches 的特殊號碼.
 - 所以再加上 cellular system 的 ID (SID), 就可表示一個 unique 的 switch id (SWIN).

IS-41 and OSI



11

- IS-41 遵循 OSI (Open Systems Interconnection) model 的架構.
- IS-41 最底下三層可以選擇用 X.25 或 SS7 的架構 MTP.
 - MTP (Message Transfer Part).
 - SCCP (Signaling Connection Control Part) class 0 位在 OSI layer 3 和部份的 layer 4.
- OSI 的 layer 4-6 在 IS-41 沒有定義.
- 對於 OSI Layer 6 (presentation layer) 的格式轉換, IS-41 是使用 ISO/ITU-T transfer syntax (ex: 1984=X.409, 1988=X.209). 這部份的標準稱為 “Formats of the Messages”.
- Application layer 在下面再詳細說明.

Sublayers in Layer 7

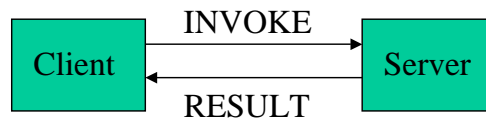
- Mobile application part (MAP) makes use of two OSI layer 7 protocols: ACSE and ROSE.
- ACSE: Association control service element
 - to bind two applications together
- ROSE: Remote operations service element
 - ROSE is invoked during ongoing transfer of IS-41 messages.
- ACSE and ROSE are grouped together as ASE (Applications service elements).

12

- 在 Layer 7, 真正負責網路管理等應用相關的程式寫在 MAP 中.
- MAP 會呼叫下層的 ACSE 與 ROSE 幫忙完成網路上的連結.
 - ACSE 是一種 housekeeping 的工具, 並沒有與 MAP 呼叫下層幫忙傳送 IS-41 message 的程序有關.
 - 例如 entities A 和 B 想要連結在一起, ACSE 就會幫忙設定 A 與 B 間的關連 (association). 但 ACSE 就只有這項功能.
 - ROSE 用於提供傳送 message 的服務給上層 APs. 見下面投影片.
- ACSE 與 ROSE 合稱為 ASE, 用於提供上層 user 指定的服務.

ROSE

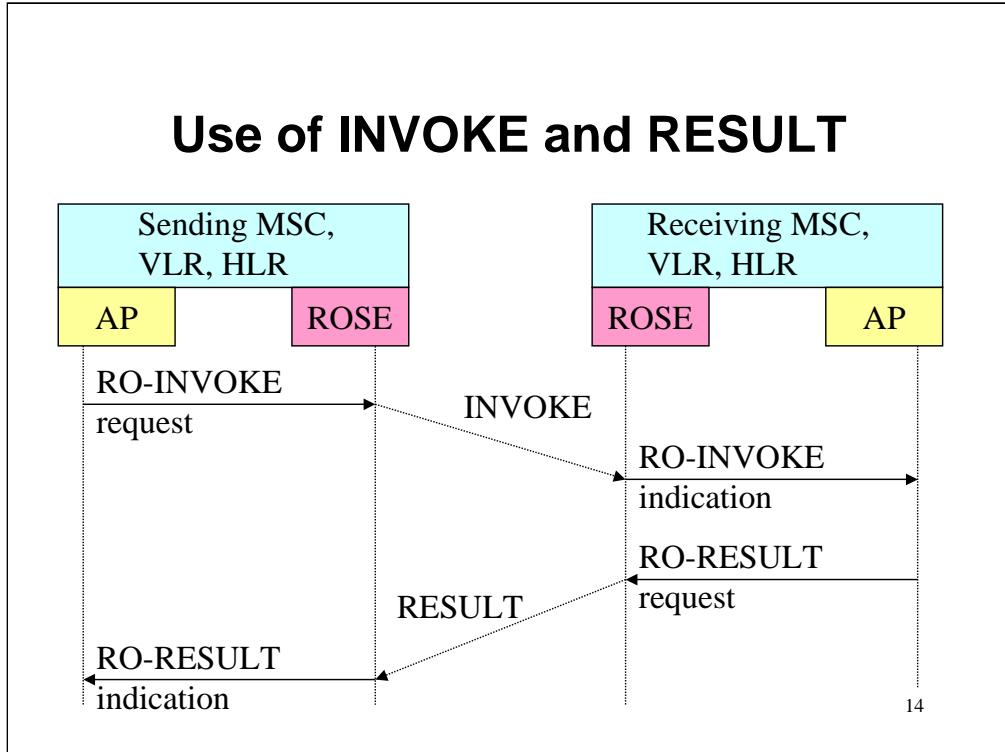
- The OSI implementation of remote procedure call (RPC) is ROSE.
- Client server model
 - INVOKE v.s. RESULT
- Connectionless



13

- MSCs, VLRs, HLRs 之間是 asymmetric, 適合使用 RPC 的方式溝通.
 - 當做 client 的一方, 並不在乎 server 真正的 location, 只要有送達需求即可.
- ROSE 就是一種 remote procedure call 的機制.
 - ROSE 是 connectionless, 沒有 timer, 沒有 retry, 也沒有 state diagram 的機制來追蹤目前操作的情形.
- ROSE 使用的是 Client-server model:
 - Client 送出 INVOKE (呼叫, 祈求, 請求幫助)
 - Server 回應 RESULT (經處理後的回應)
- 不同的狀況有不同的回覆 RESULT
 - RESULT 可以是 success 或 failure.
 - 也可以是宣稱當 success 或 failure 時不須回覆. 則 No response or confirm 的訊息會含在 AP 送來的 message 中.
- RESULT 必須含有 INVOKE ID, 以表明對應於那一個 operation.

Use of INVOKE and RESULT



- 這張圖說明 ROSE 的運作. 上層 MAP 中某一個 AP, 呼叫 ROSE 做 RPC, 建立與對方的連結.
- 當 ROSE 的上層 AP 要求 ROSE 服務, 傳送 message 給對方:
 - AP 提出 request.
 - 上層(AP)用 request 要求下層(ROSE)給與服務, 下層(ROSE)用 indication 上層(AP)給與服務.
 - ROSE 送出 INVOKE.
 - 對方 ROSE 將收到的訊息回傳給 AP (使用 indication).
- 當對方 AP 處理完後, 以類似方式 (request) 要求 ROSE 傳回 RESULT.
- 收到 RESULT, ROSE 以 indication 上傳給 AP.

ROSE and TCAP

- IS-41 uses ROSE and TCAP.
- ROSE and TCAP provide **transaction-based operation** with invoke and result messages.
 - ROSE is invoked during ongoing transfer of IS-41 messages.
 - TCAP provides the ability to exchange information between applications using *non-circuit-related* signaling.
- As a general practice those ROSE operations are mapped into the TCAP message header.

15

- ROSE 下層的 TCAP 則是 SS7 中用於傳送訊息的機制。
- TCAP 提供各節點間 non-circuit-related (與設立電話線無關的) 訊息的傳送, 提供各種上層應用服務 (ex: MAP, IS-41, 位於 SCP database 的 080免費電話服務, 信用卡服務, 封閉用戶群, 大量資料的傳送, 操作及維護的應用),
- TCAP 也用於定義不同 components 間的 syntax (各 machine 會使用不同的 syntax), 在傳送 message 前, 都要先轉成 machine-independent syntax, 對方收到後, 再轉回自己的 syntax.
 - TCAP 使用稱為 Basic Encoding Rules (BER) 的 standard. (與 OSI transfer syntax 非常相同).
- ROSE 與 TCAP 均是使用 transaction-based operation with invoke and result. 真正在實作時, ROSE 都被 mapped into 到 TCAP message 的 header 中.

Mobility Management Using TCAP

16

- 這裡將介紹用 TCAP 來做 mobility management.

TCAP

- TCAP: Transaction Capabilities Application Part
- TCAP are operations involved in two signaling point. The operation is not related to individual network. It is related to a specific information query or updating.
- TCAP serves all its users in an application-independence manner.
- TCAP users are MAP, INAP, OMAP, ... etc.

17

•TCAP 與下層連結的網路無關, 下層可以是 SS7 的 SCCP/MTP, 也可以是 TCP/IP, X.25.

•TCAP 服務上層的 users, 可能是 MAP (message application part), INAP (intelligent network application part), OMAP (Operation Maintenance Administration Part). 但 TCAP 的運作與 application 無關, 只是提供一種建立兩個 signal point 通話的方式.

Mobility Management Using TCAP

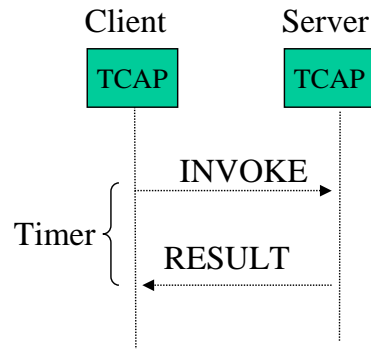
- More than 50 TCAP operations are defined in IS-41 for three purposes:
 - (1) Inter-MSC Handoff
 - (2) Automatic Roaming
 - (3) Operations, administration, and maintenance
 - For example: RegistrationNotification, RegistrationCancellation, and HandoffMeasurementRequest.

18

- IS-41 為提供 mobility management, 便制定了 50 種 TCAP operation.
- 這些 TCAP operation 依照其目的可分為下列三種:
 - Inter-MSC handoff: 處理 handoff
 - ex:HandoffMeasurementRequest.
 - Automatic roaming: 處理 roaming, 做 location tracking
 - ex: RegistrationNotification, RegistrationCancellation,
 - OA&M: 網管的功能
- [1] Table 5.1 列出部分的 operations.

IS-41 Transactions

- Most IS-41 transactions are two-message, query-response transactions.
- IS-41 TCAP use SCCP class 0 connectionless service.
- Every IS-41 TCAP accompanies a timeout constraint.



19

•這裡說明利用 TCAP, 建立起網路兩端的連結, 為了某一個目的, 整個訊息往返的過程, 稱為一個 Transaction.

•每一個 transaction 是執行一個動作, 送出端送出 Query 型式 (packet type) 的 INVOKE (component), 接收端送回 RESPONSE 型式 (packet type) 的 RESULT (component).

•每個 IS-41 的 TCAP transaction 都會伴隨逾時 (time out) 的考量. 在 client 送出 INVOKE 後, 就會啟動一個 timer, 若是在 timer expire 前一直收不到 RESULT, 即發生 time out, client 就會把它視為 error (即視為收到一個 RETURN ERROR 的 TCAP 訊息), 回應給上層的 MAP.

•TCAP 使用 SCCP class 0 connectionless (非固連式) service, 所以不保證來自同一個 node 的 message 會依序傳送到達, 但可快速到達.

•因此 IS-41 transaction 採用 two-message (包含一個 query 和一個 response), 就可以確保訊息的順序. 即使是單向的 IS-41 訊息 (沒有 response), 也可確保訊息的順序.

•大部份的 IS-41 transactions 都是 two-message query-response transaction. 只有2 個例外.

•FlashRequest 這個 operation 有一種是 Unidirectional.

•一個包含 FacilitiesDirective 的 TCAP transaction 共含有 3 個 messages.

Component Sublayer

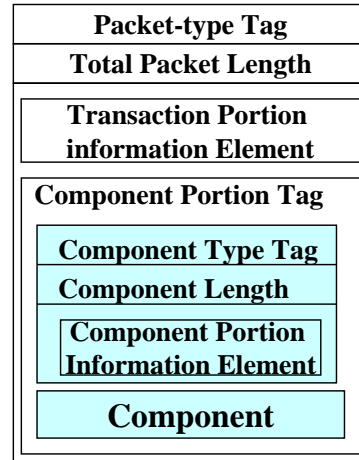
Transaction Sublayer

TCAP Format

➤ A TCAP message consists of two portions:

[Transaction, Component]

- **Transaction** portion specifies the **package type**.
- **Component** portion specifies the **number** and the **types of components** (operations) to be performed.



20

• 每一個 TCAP message 包含兩個部份:

• Transaction 通訊交易部份: 用於記載封包的型態 (packet type), 指的是此 transaction 中雙方往來之順序的關係. 誰是啟始, 何時表示我 (可以是 client 或 server) 要結束 transaction. 每一次 transaction 都會以成對的 Transaction ID (TID) 以決定這次的 transaction.

• OTID (originating TID) 表示發送端與 DTID (destination TID) 表示接收端. (每一次訊息的來回都用相同的 OTID 與 DTID).

• Component 內容部份: 用於, 指的是 client-server 之間對應的關係, 記錄要求對方 (server) 執行的動作型式 (component type) 與相關 information 或回應對方 (client) 執行結果或 error 的原因. 也會有 Component ID (INVOKE ID).

The Package Types in TCAP Messages in IS-41

- Some of 7 IS-41 packet types:
 - **QueryWithPermission**
 - **ConversationWithPermission**
 - **Response**
 - **Unidirectional**
- IS-41 transaction always
 - Begin: a query message
 - End: a response message.

21

•請參考 Reference [2] Table 7-2, IS-41 Transactions (Messages) 列出 IS-41 messages 的意義與操作.

•Packet Type 指的是此 transaction 中雙方往來之順序的關係. 誰是啟始, 何時表示要結束 transaction.

•**QueryWithPermission** 詢問: 代表開起此 TCAP transaction 的第一個 message, 並通知對方有權可送回 Response 結束此 transaction.

•**ConversationWithPermission** 交談: 代表此 TCAP transaction 的第二個到倒數第二個 message, 並通知對方有權可送回 Response 結束此 transaction.

•**Response** 回覆: 代表此 TCAP transaction 的最後一個 message.

•**Unidirectional** 單向: 唯一的訊息, 不需任何的回覆.

•一個 IS-41 transaction 永遠都是以一個 query message 開始, 而以 response 做為結束.

The Component Types in TCAP Messages in IS-41

- Some of IS-41 component types:
 - **INVOKE(Last)**
 - ✓ **Last** : The operation is the last component in the component portion.
 - **RETURN RESULT(Last)**
 - **RETURN RESULT(not Last)?**
 - **RETURN ERROR**
 - **REJECT**

22

•Component 內容部份: 指的是 client-server 之間對應的關係. 用於記錄要求對方執行的動作型式 (component type) 與數目, 如所需要的 information 或 error 的原因.

•**INVOKE** 呼叫: 要求對方 (server) 執行一個動作.

•例如 RegistrationNotification 有一項是是 INOVKE (Last) & QueryWithPermission.

•**RETURN RESULT** 回覆結果: 代表執行完對方 (client) 的請求 (INVOKE), 並將執行結果送回.

•如果一個節點收到 INVOKE, 完成工作執行完畢後就回傳 RETURN RESULT.

•**RETURN ERROR** 回覆錯誤: 代表執行失敗, 並將錯誤原因送回.

•例如 INOVKE 中的 MIN 並不在此 HLR 管轄範圍內.

•**REJECT** 拒絕: 代表 server 拒絕執行 INVOKE 的任務. 例如內容不正確, 格式錯誤.

•當 SS7 node 收到 REJECT, 則會停止 timer, 結束目前工作, 並執行錯誤修正.

•若 component 中包含 Last, 則表示這是最後一個動作 (若伴隨 QueryWithPermission, 表示此 transaction 只執行一個動作).

Example: REGNOT

- Registration Notification (REGNOT) is an operation in the IS-41 messages:

From: VLR

To: HLR

Component Type

Package Type

INVOKE (Last)

Query WithPermission

RETURN RESULT (Last)

Response

(Function: Status report: the visitor has been registered and is active)

RETURN ERROR

Response

REJECT

Response

23

- REGNOT 是從 VLR 送往 HLR, 作註冊通知之用的 message.
- 下面表示可能的 component type (Component part) 與 packet type (Transaction part)

Example: FlashRequest

- The operation FlashRequest has a package type Unidirectional.

From: Serving MSC

To: Anchor MSC

Component Type

Package Type

INVOKE (Last)

Unidirection

Function: To convey information for call control.

- Note: no response is expected from the anchor MSC, and no TCAP transaction is established.

- FlashRequest operation 的 package type 是 Unidirectional 的.

Example: FacilitiesDirective

- The TCAP transaction, including the operation FacilitiesDirective, consists of three message exchanges.

Component Type

INVOKE (Last)

RETURN RESULT (Last)

RETURN ERROR

REJECT

Package Type

Query WithPermission

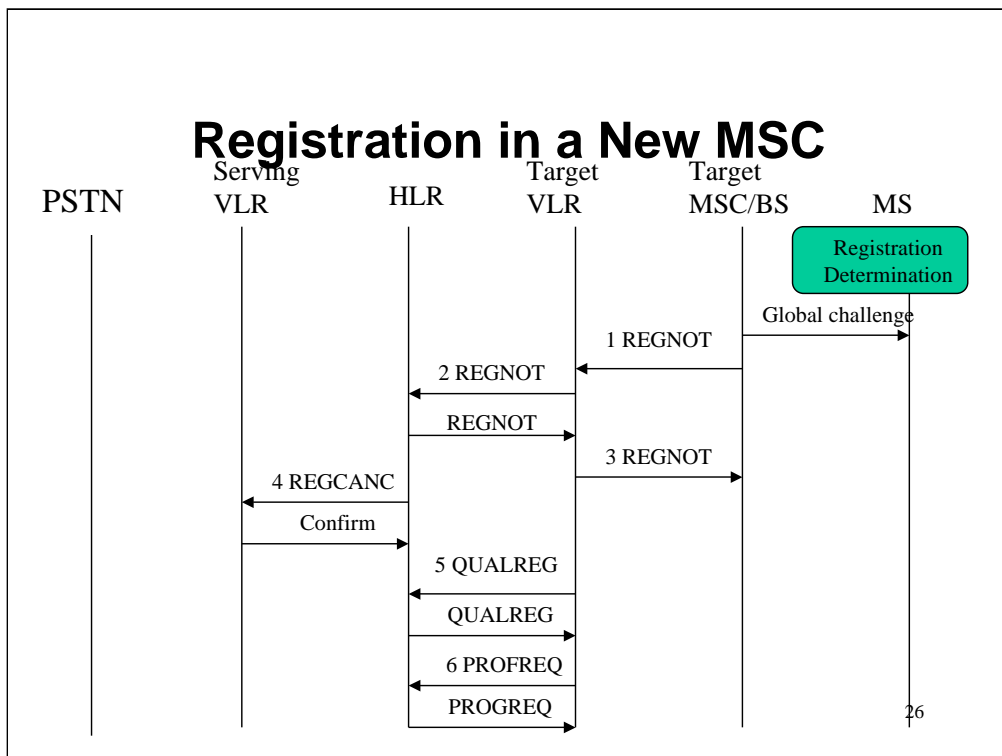
Conversation

WithPermission

Response

Response

- 好像少了 RESULTN RESULT (Last) & Response.



•我們以下面的例子說明 IS-41 的運作: 當 MS 進入一個 new MSC, 決定要換系統. IS-41 便被使用於修改 VLR, old /new MSC 的資料.

•MS 會先 listen 新的 BS, 在一個 control channel 上 broadcast 的 RAND. MS 向 MSC/BS 註冊, 送出 MIN, RAND 與其他 parameter.

•**Step 1:** BS 驗證 RAND. 成功後送 REGISTER 給 MSC. MSC 轉送給 VLR.

- Step 1 包含參數 MIN, MSN, qualification information code, system type code (表示 system 的製造商), 3-digital identifier of the specific system (MSC ID 包含 2-byte SID (system ID) 和 1-byte SWNO (switch number), 用於指出此 system 的 ID).

- 若 serving/target MSC 在同一個 VLR 下, 則 VLR 不會向 HLR 做進一步的 registration.

•**Step 2:** VLR 發現 MS 並不在自己的管轄中, 送出 REGNOT (RegistrationNotification) 給 HLR. VLR 會送給 HLR 的 message 包含 MIN, MSN.

- HLR 修正自己的 database record. 送回 RESULT.

•**Step 3:** VLR 送回 RESULT 給 MS.

•**Step 4:** HLR 送 REGCANC (RegistrationCancelation) 給舊的 VLR, 包含 REGNOT 中所有參數. HLR 可在任意時間傳送.

- Old VLR 回應 Confirmation message 給 HLR, 此 message 中包含 CHCNT 的值.

•**Step 5:** VLR 送 QUALREQ (qualification request) 給 HLR, 主要是做 authentication 與決定是否為有效的要求.

Messages for Registration

- Messages involved for mobile registration:
 - Registration notification (REGNOT)
 - Registration cancellation (REGCANC)
 - Qualification request (QUALREQ)
 - Profile request (PROFREQ)

27

- 與 mobile registration 有關的 messages :
 - Registration notification (REGNOT)
 - Registration cancellation (REGCANC)
 - Qualification request (QUALREQ)
 - Profile request (PROFREQ)

Message Parameters for Registration

- The messages parameters for registration operations are:
 - Mobile identification number (MIN)
 - Mobile serial number (MSN or ESN)
 - Qualification information code
 - MSC ID of serving MSC
 - System my type code of VLR
 - System my type code of HLR
 - Origination indicators

28

•列出這些用於 registration 的參數, 讓大家瞭解原來有這麼多資料需要收集, 才能找到手機目前的所在位置.

•MIN: 10 digit 的 subscriber ID

•Mobile serial number: 32-bit 手機 ID

•Qualification information code 指出在 registration 時所需要的品質.

•ex: validation and profile 或 validation only.

•MSC ID 包含 2-byte SID (system ID) 和 1-byte SWNO (switch number) , 用於指出此 system 的 ID.

•System my type code 是每一個 mobile equipment vendor 所被assigned 的 id. 如 5 for GTE equipment, 6 for Motorola equipment, 7 for NEC equipment.

•Origination indicators 指出 MS 所訂閱的打電話型態, ex: local only, international, etc.

Location Request

- The location request message (LOCREQ) must contain four parameter:
 - Dialed digits
 - MSC identifier
 - System my type code
 - Billing ID field

29

- 另外一個範例, 說明要求得到 MS 的位置要有那些參數.
- Dialed digits 是對方的電話號碼
- System my type code 指出自己的製造廠.
 - System my type code 是每一個 mobile equipment vendor 所被assigned 的 id. 如 5 for GTE equipment, 6 for Motorola equipment, 7 for NEC equipment.
- Billing ID field 是存放 anchor MSC 的 ID, 用於 billing records.

IS-41 Authentication

30

- 在 IS-41 中有提供兩種認證的模式, Without-sharing (WS) Scheme 與 Sharing Scheme. 以下分別說明.

EIA/TIA-51

- The EIA/TIA Telecommunication Systems Bulletins (TSB) 51
 - Authentication
 - Voice privacy
 - Singling message encryption
- IS-41 Revision C
- The TSB-51 algorithm is based on private key cryptographic techniques.
 - Shared Secret (Key) Data (SSD)
 - Known in AuC and MS only

31

- 當 AMPS 剛發展出來, 用戶很少, MSN 與 MIN 透過 air interface (沒有加密) 傳送, 用來當做 authentication 使用. 然而有人截取 air 上的 message, 得到別人的資料. 因此只要修改自己的手機, 就可以接打電話, 讓別人付費.
- 為了解決這樣的問題, EIA/TIA 提供一些解決 authentication, voice privacy, singling message encryption 的方案, 並加入 IS-41 Revision C 及以後的版本.
- 這部份在探討 2 個 authentication 的 algorithm: sharing scheme & WS.
- 基本上 TSB-51 使用 shared secret (key) data (SSD) 的方法, 此 SSD 存在 handset 與 network (AuC) 兩端, 做為認證之用.
- The PCS versions of CDMA, PACS, CDMA/TDMA, TDMA and W-CDMA 均 support SSD.
- Authentication 分成 global challenge 與 unique challenge.
 - Global challenge 是整個 system access 的一部份, 會在 call origination, page response (termination), registration 時進行
 - Note that 只有到新的 VLR 才要做 authentication, handover 也是.
 - Unique challenge 是當特別情況, 如 MSC 發現 registration failure and after a successful handoff), MSC 主動要求 MS 做 authentication. (BS 會送一個特別的 RANDC 讓 MS 做 CAVE)

Authentication Schemes

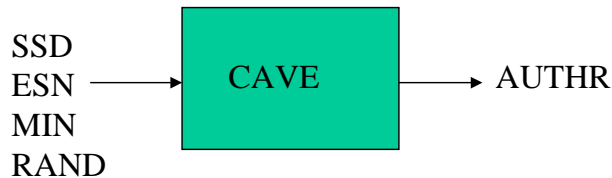
- Two authentication schemes proposed in TSB-51:
 - Without-sharing (WS) scheme
 - ✓ SSD is known to authentication center and the MS only.
 - Sharing Scheme
 - ✓ SSD or some aspect of SSD are known to the visited system, too.
 - ✓ The visited system authenticates MSs at call origination or delivery.

32

- TSB-51 有兩種 authentication schemes:
 - Without-sharing (WS) scheme
 - SSD 只有 authentication center 和 MS 知道.
 - AuC verifies AUTHR and COUNT from MS.
 - Sharing Scheme
 - SSD 與一些與 SSD 相關的演算法等, 也可以告訴 visited system.
 - Visited system 可以在 MS 打電話或接電話時對 MS 進行認證.
- 在 sharing scheme 中, 由於在 VLR 做 authentication, 看起來會減輕網路上的 traffic, 且會使 call setup time 減少. 然而, 這個 scheme 在 registration 時會需要比較多的 message exchanges.
- 因此 operators 就會面臨 tradeoff between two schemes.
 - 若在兩次 registration 間, call origination/ termination 很多很多, (i.e., call frequency \gg mobility), 這樣的 user 適用 sharing scheme.
 - 相反的, 對於 high mobility user 而言, 必須經常做 registration, SSD 反而會增加許多的 traffic, 所以這樣的 user 適用 WS.
 - 如果 user 的 mobility rate 和 call frequency 經常改變, 無法用 sharing scheme 或 WS 含概, 作者便提出兩種 adaptive algorithms, 可以在 sharing scheme 與 WS 間轉換, 隨時挑選適當的 scheme.

Shared Secret (Key) Data (1/2)

- The CAVE (Cellular Authentication Voice Encryption) algorithm are installed in AuC and MS.
 - SSD, ESN, MIN and RAND are used to generate the authentication result (AUTHR).
 - RAND is a random number obtained from the MSC/BS.



33

- 當 MS 根據 BS 所傳來的訊息得知以進入一個新 location area 時, 必須要經過一個 認證的程序以獲得 PSP 的服務, MS 會利用 SSD, ESN, MIN 和從 PCS service provider 所獲得的隨機號碼 (RAND) 來執行行動電話認證及語音加密演算法 (Cellular Authentication and Voice Encryption 或 CAVE), 此演算法會產生一個註冊的認證結果 (Authentication Result 或 AUTHR).
- CAVE, SSD 只有 AuC 與 MS 知道.

Shared Secret (Key) Data (2/2)

- Parameters for registration:
 - AUTHR
 - ESN
 - MIN
 - RANDC: the most significant 8-bits of RAND
 - COUNT: call history count
- Secret key for voice call:
 - VPMASK (voice privacy mask)
 - SMEKEY (signaling message encryption key)

34

•MS 提供 AUTHR, ESN, MIN, RANDC and COUNT 參數給 MSC/BS, 請求註冊.

- RANDC 是 RAND 最前面 8 bits 的值

- COUNT 也稱為 history count

- 它代表 MS 註冊, 打電話出去, 接電話等等的次數.

- 存於 MS 及 AuC 中

- Also called CHCNT

•VPMASK 與 SMEKEY 是由 AuC 產生, 送給 MSC/BS, 做為與 MS 間通話使用.

•voice call 中使用的加密密碼:

- VPMASK (voice privacy mask) 用於 MS 與 BS 之間的經由 air interface 的語音傳送.

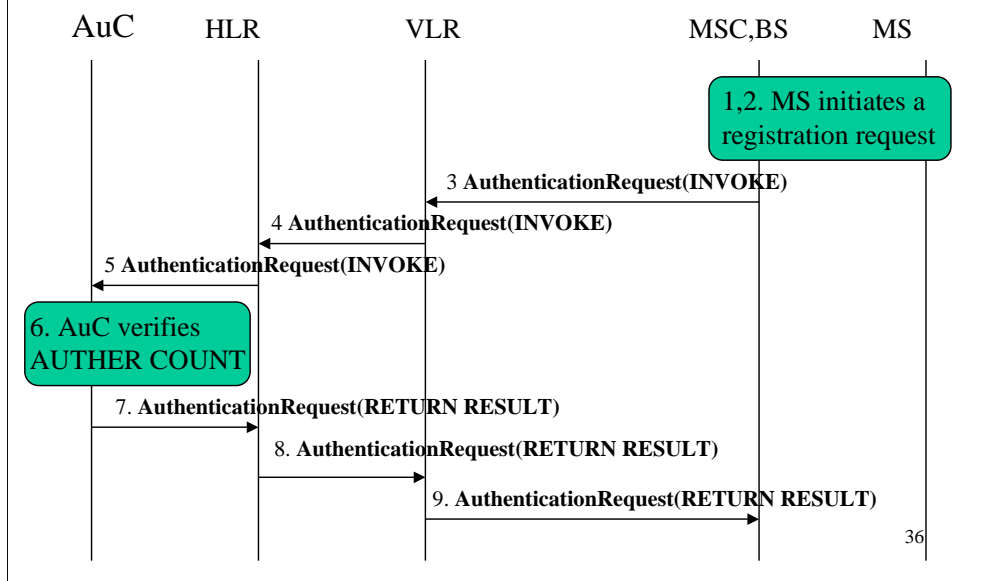
- SMEKEY (signaling message encryption key) 用於對目前各種 signaling message 的資訊加密.

Call Control for Without-sharing (WS) Scheme

35

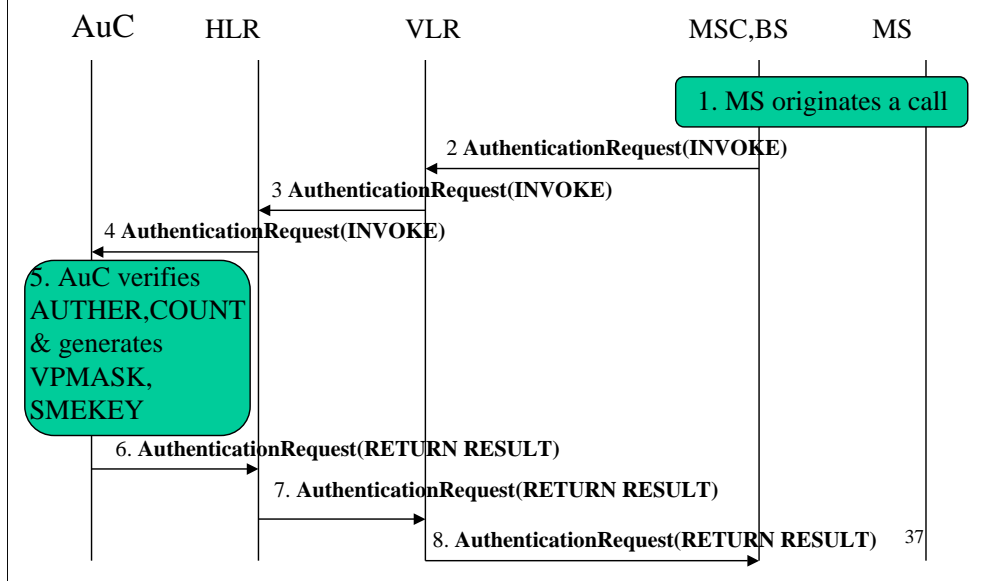
- 以下分別說明Without-sharing (WS) Scheme 的電話控制.

The WS for MS Registration



- BS 會在一個 control channel 上一直持續定期 broadcast RAND (稱為 global challenge)
 - Step 1: 當 MS 進入一個 new MSC, 決定要做 registration. MS 會 listen 此 BS 的 RAND, 使用 CAVE 產生 AUTHR.
 - Step 2: MS 送出要求 registration 的要求, 其中包含 AUTHR, MIN, ES, RANDC, COUNT
 - BS 會先檢查 RANDC 是否相同.
 - Step 3: forward 給 VLR
 - Step 4: forward 給 HLR
 - Step 5: forward 給 AuC
 - Step 6: AuC 亦執行 CAVE, 與 MS 送來的 AUTHR 比對. 同時也檢查自己的 COUNT 是否與 MS 的相同.
 - Step 7: AuC 將結果傳回 HLR. 如果認證錯誤, 會傳回 AuthenticationRequest (RETURN ERROR).
 - AuC 也會傳回 new SSD MS. 不只是 registration, 有時 AuC 也會給 MS 一個 new SSD.
 - Step 8: forward 給 VLR
 - Step 9: forward 給 MSC
- 共 6 messages.
- 若是有 TMSI, 就可傳送 old TMSI 取代 MIN.
- 一旦 MS 獲得認證, MSC/BS 則會傳送 RegistrationNotification 的訊息向

The WS for Call Origination



- Step 1: 當 MS 想要打電話時, 會使用 CAVE 產生 AUTHR, VPMASK, SMEKEY. MS 送出要求 registration 的要求, 其中包含 AUTHR, MIN, ES, RANDC, COUNT
- Step 2: forward 給 VLR
- Step 3: forward 給 HLR
- Step 4: forward 給 AuC
- Step 6: AuC 進行 authentication 並將結果傳回 HLR. 如果認證錯誤, 會傳回 AuthenticationRequest (RETURN ERROR). AuC 也會將 VPMASK 與 SMEKEY 傳給 MSC/BS.
- Step 7: forward 給 VLR
- Step 8: forward 給 MSC

The WS for Call Termination

- Normal call setup procedure
- MSC pages the MS
- MS responds to the page and executes the CAVE algorithm
 - MS sends AUTHR, COUNT, ESN, MIN and RANDC.
- Established a voice channel

38

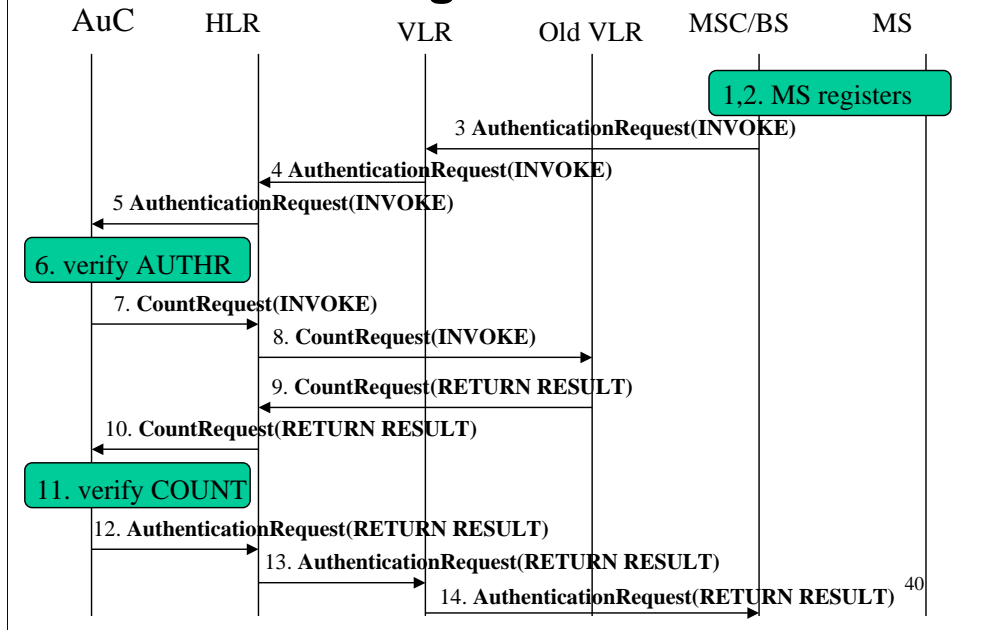
- Call 的建立程序是將 trunk route 到目的 MSC, 而後 MSC 呼叫 MS.
- MS 回應呼叫的方法是執行 CAVE algorithm, 並送出 AUTHR, COUNT, ESN, MIN and RANDC.
- 被呼的 MS 成功作身分驗證後, 呼叫與被呼叫方便為此 call 建立一個 voice channel.

Call Control for Sharing Scheme

39

- 在 Sharing scheme, VLR 可以直接對 MS 作 authentication, 而不須將 authentication request forward 到 AuC.
- 額外的 overhead 是因為 old VLR 有目前的 COUNT 值, 而 AuC 必須從 old VLR 取得 COUNT 值.
- 在某一次 call origination/termination 後, VLR 也會有 CAVE 與 SSD. 便可以直接進行 authentication.
- 見 call origination 的 figure.
- 最後會比較此兩種模式的網路 traffic.

The Sharing Scheme for MS Registration



- BS 會在一個 control channel 上一直持續定期 broadcast RAND (稱為 global challenge)

- Step 1: 當 MS 進入一個 new MSC, 決定要做 registration. MS 會 listen 此 BS 的 RAND, 使用 CAVE 產生 AUTHR.

- Step 2: MS 送出要求 registration 的要求, 其中包含 AUTHR, MIN, ES, RANDC, COUNT

- BS 會先檢查 RANDC 是否相同.

- Step 3: forward 給 VLR

- Step 4: forward 給 HLR

- Step 5: forward 給 AuC

- Step 6: AuC 亦執行 CAVE, 與 MS 送來的 AUTHR 比對.

- 然而, AuC 並沒有 current value of COUNT, 因此必須向 old VLR 取回 COUNT.

- Step 7: AuC 送出 CountRequest (INVOKE) 給 HLR

- Step 8: HLR forward 此訊號給 old VLR.

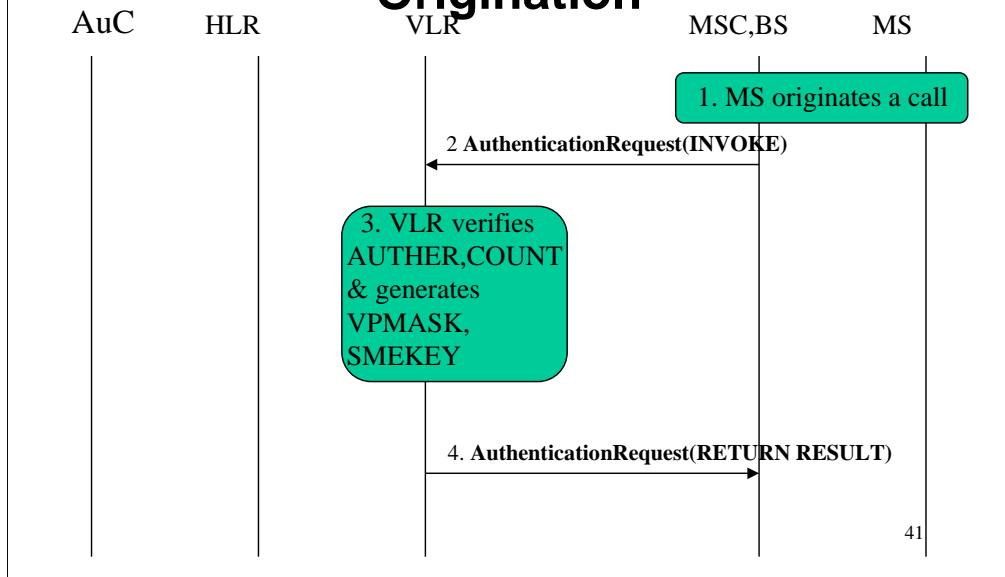
- Step 9: old VLR 用 CountRequest (RETURN RESULT) 傳回 COUNT, VPMASK, SMEKEY 值給 HLR.

- Step 10: HLR forward 給 AuC

- Step 11: AuC 驗證 old VLR 與 MS 的 COUNT.

- Step 12: AuC 將結果傳回 HLR. 如果認證錯誤, 會傳回 AuthenticationRequest (RETURN ERROR)

The Sharing Scheme for Call Origination



- Step 1: 當 MS 想要打電話時, 會使用 CAVE 產生 AUTHR, VPMASK, SMEKEY. MS 送出要求 registration 的要求, 其中包含 AUTHR, MIN, ES, RANDC, COUNT

- BS 會先檢查 RANDC 是否相同.

- Step 2: MSC forward 給 VLR

- Step 3: VLR 進行 authentication (AUTHR 與 COUNT) 並將結果傳回 MSC. 如果認證錯誤, 會傳回 AuthenticationRequest (RETURN ERROR). 也會將 VPMASK 與 SMEKEY 傳給 MSC/BS.

- 如果 VLR 沒有 MS 的資料, 便會向 HLR 要求, 如同 registration 的程序.

- Step 4: forward 給 MSC

- 只有兩個 messages, 所以 sharing scheme 適用於常打電話的 users.

Summary

- The IS-41 Protocol
- Mobility Management Using TCAP
- IS-41 Authentication
- Call Control for WS and Sharing schemes