

Signaling System No.7

- SS7

1

介紹 Signaling System No. 7 的運作方面。由於AMPS或GSM等通訊系統的核心網路訊號系統都大量擷取SS7的運作模式，因此專門列出此一部分來介紹電信網路的演進，SS7的架構與特性，以了解為何採取SS7做為電信網路訊號交換的背景。如果希望對GSM或3G的運作要更徹底了解，最好能對SS7有初步的認識。

Reference (1/2)

- [1] *Wireless and Mobile Network Architectures* , Y-Bing Lin and Imrich Chlamtac , Wiley Computer Publishing.
 - Chapters 2 and 5.
- [2] 第七號共通信號系統概論 , 湯鴻沼 , 全華科技圖書股份有限公司。
- [3] *Telephone Network and PBX Software* , Yi-Bing Lin , 維科出版社。
- [4] *Mobile and Wireless Networks* , Uyless Black , Prentice Hall。 Appendix A.

Reference (2/2)

[5] SS7信號系統，林添財，中華電信訓練所教材。

Outlines

- Introduction
- Signaling System Number 7 (SS7) Protocol
- Components and Links of SS7
- PCS/PSTN Call Control Using ISUP
- Summary

4

- 在簡介中, 首先介紹電信網路訊號系統中的基本元件, 與訊號系統的分類.
- 以下我們將介紹 SS7 的架構, 元件, 與各元件間的連結方式. 進一步說明當 PSTN 與 PCS network (PCN) 以 SS7 相連的介面.
- 我們將以 PSTN 先打電話時 (land-to-mobile), 與 PCS MS 先打電話時 (mobile-to-land), 建立與結束通話的流程, 來說明相關的 signaling.

Introduction

5

- 依照中華電信公司的分類, 電信網路分為專線網路與公眾通信網路. 其中公眾通信網路又分為行動通信網路 (包括無線電叫人系統如 BB Call, 與陸地行動電話系統如 GSM), 與固定通信網路 (包括公眾電話交換網路即PSTN, 如家用電話公共電話, 與公眾數據交換網路即 PSDN, 如 ADSL). 公眾電話交換網路即PSTN 又細分為市內電話交換網路, 長途電話交換網路與國際電話交換網路. 公眾數據交換網路即 PSDN 又細分為電路交換(circuit-switching, i.e., dial-up) 與分封交換 (packet-switching).
- 在這個章節中, 首先介紹一般有線電信系統 – 公眾交換電話網路 - 訊號系統中的基本元件.
- 接著說明甚麼是訊號系統, 傳送的訊號有那些種類, 那一些目的.
- 再來說明訊號系統的兩大種類: CAS 與 CCS.
- 其中 SS7 是屬於 CCS 的一份子.

Public Switched Telephone Network (PSTN)

➤ Three components:

- Customer premises equipment (CPE)
 - ✓ Telephone set, private branch exchanges (PBX)
- The transmission facilities
 - ✓ Trunks and subscriber lines
- The switching system
 - ✓ Central offices (CO), tandems

6

•PSTN 為傳統的公眾電話網路,基本上為電話服務所設計,屬於 circuit-switching (電路式交換網路),目前國內已大致數位化,且採用 SS7, intelligent network, ISDN 等技術以提供更多樣的服務.

•在電信系統中的元件可以分成 3 個大項:

•Customer premises equipment (CPE): 客戶端用於接收電信服務的電信設備,如電話機,交換機(PBX)

•The transmission facilities:電信網路系統中用於傳送訊號,資料的傳輸設備,如接到家中的電話線(稱為 subscriber line)與個交換機間的電話線(稱為 trunk)

•The switching system: 又稱為 Exchangers, 是電信網路中執行電話交換功能的設備,如交換機. 在電信網路中必需把電話由一個節點轉接到另一個節點,最後才能接通兩端點開始通話. 交換系統就是在為客戶轉接電話到正確的路徑.

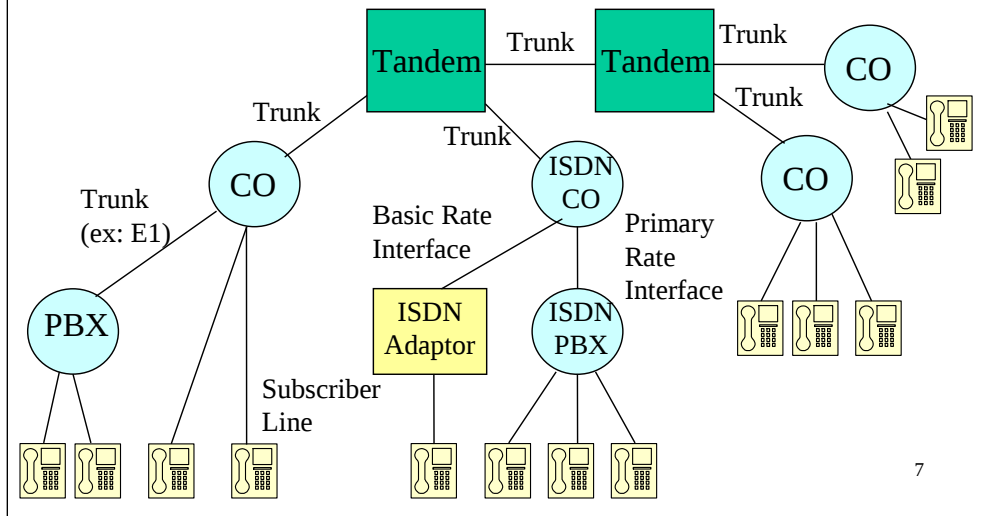
•Central office (CO) 是指直接連到家中電話的那些交換機,也稱為 End office (端局).

•Tandem 是一種連結 trunk 的交換機. Tandem 通常是不會直接連到客戶的終端設備 CPEs. 有兩大類:

•在相同的計費區域 (charging zone for local call) 中,區域性的 (local tandem) 會與區域 CO 相連.

•另一類為 Toll tandem (長途中心局) 或稱為 inter-exchange tandem 會連結來自不同計費區域的 Co 相連. 用來處理長途電話 (long distance calls).

PSTN Architecture



7

- ISDN: Integrated Services Digital Network

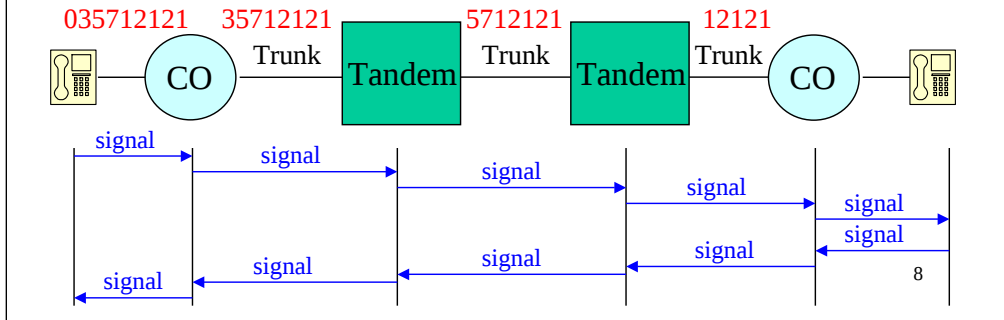
- ISDN 提供單一的, 數位連結給使用者, 可同時打電話與傳送資料或影音資訊.

- BRI: basic rate interface provides 2B+D. (B: 64Kbps voice, D: 16kbps signal)

- PRI: primary rate interface provides 23B+D. (B:64Kbps voice, D: 64kbps signal)

Call Setup and Release

- A call requires a communications circuit between two subscribers.
- The setup and release of connection is triggered by signals.



- 要能在兩個電話間通電, 必須在兩戶電話間建立通話的線路連結, 以傳送語音, 稱為 circuit connection.
- 但要建立起這樣一通電話, 需要一層一層的傳送控制信號 (signal), 以建立起通話連結, 這樣的過程通常為我們所忽略. 舉例而言, 打電話時按下並送出電話號碼, 就是一個傳送 signal 的過程.
- 電話號碼可以表示成 CC-AC-EC-LN, ex: 886-3-5712121 國碼 886, 國內區域號碼 AC, 再指到地區的交換機, 最後是用戶的編號. 利用電話號碼就可找到對方所在的 CO, 最後連到對方家中.
- 中間經過的交換機就好像電腦網路的 router, 也是以查表 (routing table) 的方式, 找到下一個 hop.
- 電信網路上的交換機, 必須要有下面的功能, 以提供系統的運作: 基本功能, 話務查測, 計費功能, 網路與設備管理, 維護功能.
 - 其中的基本功能包括: 相接 (interconnection), 接收情報 (information receiving), 控制 (control), 送出情報 (information transmitting), 引起注意 (altering), 忙線試驗 (busy testing), 侍候 (attending)與監視 (supervision).
 - 與類比式用戶介面相連的 central office, 還必須要有下面這些功能: 電源饋給 (Battery Feed), 超壓保護 (Over-voltage Protection), 振鈴作用 (Ringing), 監視信號 (Supervision), 碼化作用 (Codec), 岔路器 (Hybrid) 與測試 (Testing).

Signaling Systems (1/2)

- Besides delivering subscriber voice and data information, telecommunication network requires a signaling system.
- Tandems and COs perform all tasks for call controls.
- Signaling is the communication of control information between the signaling elements via some prescribed protocol.
 - For control call setup, administration, disconnect of the circuit

9

• 電信網路中,要互相溝通已完成 call connection, release 或計費等功能, 就必須要有一套完整的信號系統.

• Signaling system 像是電信網路的神經系統, signal 則是各終端設備與節點間的溝通語言.

• Signal 是為了控制, 管理, 切斷線路, 在各個 tandem 或 COs 所產生出來, 傳送給對方, 要求做適當的處理. 所有的 signaling elements 都事先要溝通好使用相同的通訊協定, 才能正常運作.

Signaling Systems (2/2)

➤ Two types of signaling functions:

- Supervisory signals

- ✓ Supervising
- ✓ Alerting
- ✓ Call process

- Address signals

Call process		1209	1336	1477	1633
Address signals	697	1	2	3	A
	770	4	5	6	B
Analog User-to-					
Network Signaling:	852	7	8	9	C
DTMF (Dual Tone					
Multiple Frequency)	941	*	0	#	D

Analog User-to-
Network Signaling:

DTMF (Dual Tone
Multiple Frequency)

10

•依照 signal 功能來分類:

•Supervisory signals are used to initiate a call request, to hold or release an established connection.

•Supervising 監視信號: 負責監控交換網路的 call connection 的程序, 送給 subscriber 和 switching system 關於 subscriber lines 與 trunk 是否 idle 或 busy 的訊息. 包括從發話方送出的啟動, 呼叫, 切斷, 從受話方送出的應答, 終話, 啟動完了, 復舊完了等信號.

•Alerting: 提供給 subscriber 得知某些狀況的訊息, 但不會出現在 call 中, 如 ring a called phone 或 off-hook warning.

•Call process 這樣的可聞信號: 僅由交換機對本身所連結的用戶送出, 提供給 subscriber 得知目前電話狀況的訊息, 如撥號音, 設備或中繼電路全忙音 (Reorder tone), 回鈴音 (ring back tone) 或 a busy tone (忙音).

•Address signals contain 被叫端用戶電話號碼, 由 caller 再撥號時產生的.

•CAS 中有 Dial Pulse 和 Dual Tone Multi-Frequency. CCS 則以 message 傳送出去.

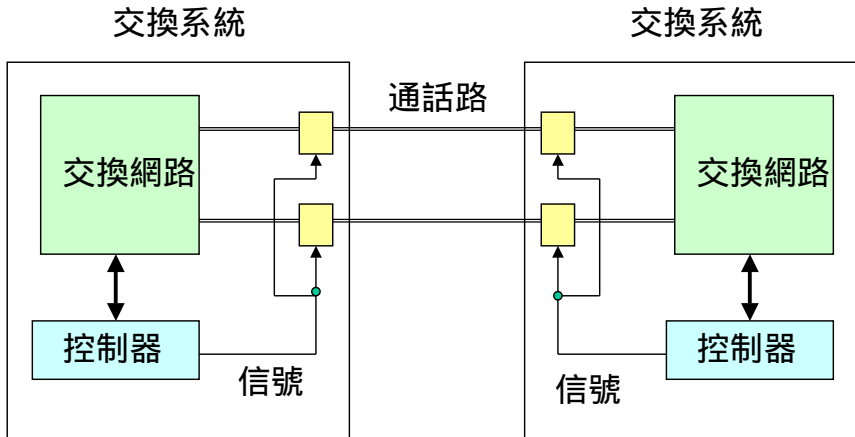
Interoffice Trunk Signaling

- Control information exchange among the switches is achieved by interoffice trunk signaling.
- Two approaches:
 - Channel associated signaling (CAS)
 - Signaling and voice shares the same *inband* channel.
 - Common channel signaling (CCS)
 - A separate *out-of-band* signaling network to carry signaling message.

11

- 在交換機與用戶端間的信號稱為 user-to-network signaling, 或 subscriber signaling.
- 若是在交換機 (可以是 CO 或 tandems) 要交換控制資訊, 則使用交換機之間幹線訊號 (Interoffice trunk signaling, 局間信號或稱為 network-to-network signaling, 或 inter-exchange signaling).
 - Interoffice trunk signaling 只與兩個交換機的互動有關.
 - 設計 interoffice trunk signaling 的重點是整體的效率與彈性.
 - 深受新的傳輸與交換技術所影響.
- CAS (通道附帶信號系統): 早期的信號系統使用的技術稱為 per-trunk, in-band signaling. 此種方法, the call control path 與實際的 speech 線路是相同的. 所以, call control signal 與 voice traffic 必須競爭搶用共同的通話路. 如 R1 Modified.
- CCS (共通道信號系統): signal 與 voice 使用不同的 channel. 約在 1950s and 1960s 為類比網路或稍後的數位交換機發展出來的.
 - 1976, AT&T 將自己發展的 Common Channel Interoffice Signaling (CCIS) 應用於 its toll network. 此系統被稱為 CCS6, 便是一個架在 CCITT Signaling System No.6 Recommendation 研發的系統.
 - R2 Interoffice Trunk Signaling 由 CEPT 在 1960 年發展出來, 用於短程的國際電話.
 - ISDN 這個網路系統也有使用 SS7.

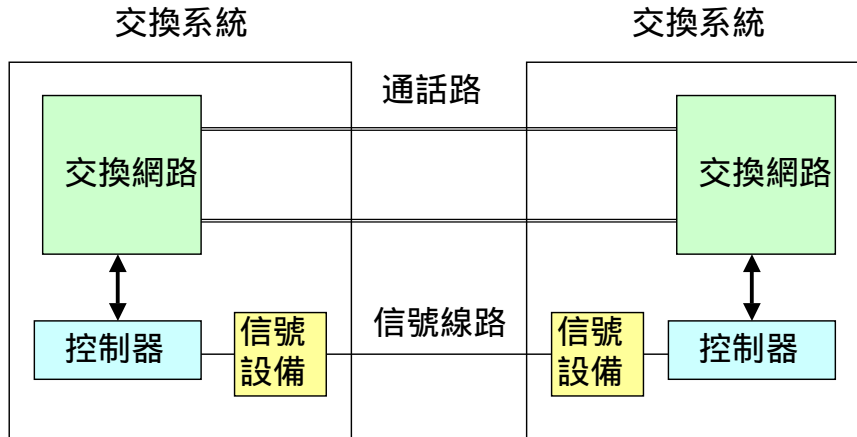
CAS Architecture



12

- Advantage of CAS (通道附帶信號系統): 不需分出一條 line 給 signaling.
- Disadvantages of CAS:
 - 會限制可傳送的 signaling type, 只能做 call setup and release.
 - 無法存取 database
 - Signaling rate 被限制在 30bps.

CCS Architecture



13

- CCS is a out-of-band signaling network, 訊號與用戶語音資料走不同實體路徑傳送的方法。
 - 利用分離通話路線與信號路線的方式, 可以提供電話網路上管理與控制的各種功能.
- CCS 可以提供的功能:
 - 傳送訊號以開啟或結束一通電話.
 - 可以測試得知網路上某些部份的狀況.
 - 可以控制網路上的流量.
- CCS: Ex: R2 signaling, signaling system number 7 (SS7).

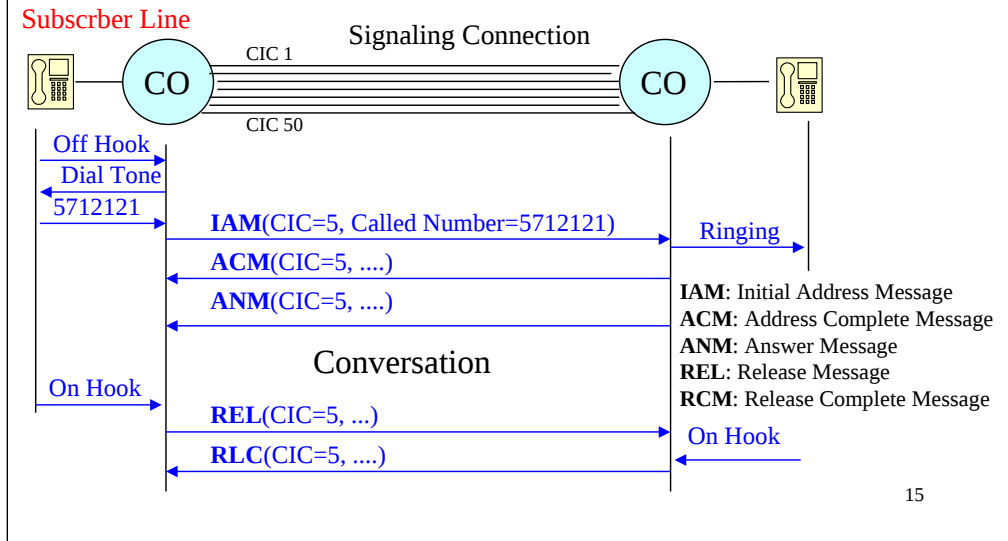
The Advantages of CCS

- Signaling can be efficiently delivered by using signaling links.
- Since the all attempts are released by the signaling links, better utilization of voice trunks can be expected.
- Singling can be performed during conversation.

14

- call control signal 與 voice traffic 不再需要競爭搶用共同的通話路。
- 減少電話設立的時間, 如此有較多的機會建立 offices 間的 redundant links 以提高 reliability.
- 當在建立一條 connection 時, 可以做 look ahead. 所以除非 connection 確定要建立了, 否則資源不需要真正保留下來,
- 高可靠度, 較快速的命令操作
- 可以讓 local exchange carrier 和 interchange carrier 來增加電話操作服務的功能.

Example of CCS



15

- 這些信號都是 ISUP 層的信號, ISUP 將在下一個部份提到, 處理建立, 釋放電話等工作.
- 如果對方 busy, 則 IAM 之後就會傳回 REL, 接下來 caller 送 RLC 結束此一回合.

Signaling System Number 7 (SS7) Protocol

16

- 這個部份開始說明 SS7 的架構, 每一個 layer 所使用的 protocol 的功能.

Signaling System No. 7

- The first CCS system is signaling system number 6 developed in the 1970s.
- The modern CCS system is SS7.
- SS7 is a dedicated data communication network and similar to the packet network.
 - SS7 follows ISO 7 layer architecture.
- SS7 is used for ISDN and PCS. Signaling between a PCS network and the PSTN are typically achieved by the SS7 network.

17

•從 1878 年開始有人工的電話交換機, 1892 年有 step-by-step switch, 1924 年有 crossbar switch, 1960 年有 stored program control switch, 1972 年有開始有 CCS 的使用, 如 CCIS 與 CCS No. 6.

•1970 中期 CCITT 開始設計SS6, 且在 1980 發表 SS7, 分別在 1984, 1988 有 improvement.

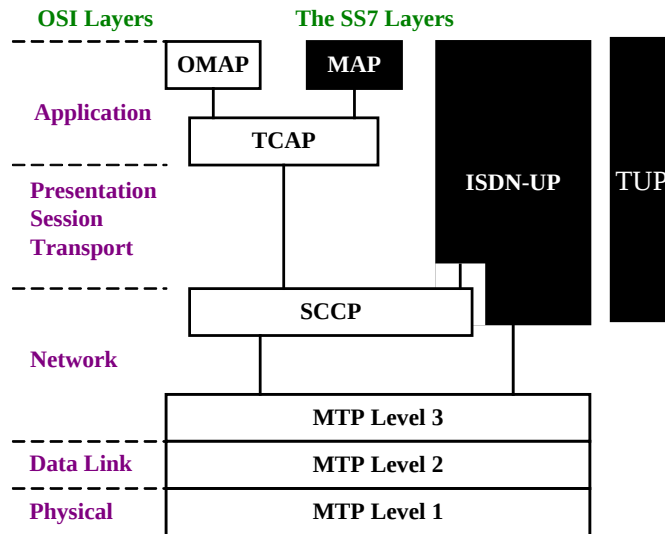
•SS6 使用 2400bps 的 data link 來傳送 signals. SS7 使用 64kbps 的 data link 來傳送 signals.

•SS7 是用於取代早期 plain old telephone service (POTS) 所用的信號系統, 可以傳送更多樣的信號, 以提供更多的服務.

•至今, SS7 已成為無線通訊系統所使用的 signaling system. 也使用於 satellite links. SS7 也經 CCITT 採納為 ISDN 的標準.

•PSTN 與 Intelligent network (IN), PCS, ISDN 或 Access network 都是透過 SS7 來溝通.

The SS7 Signaling Protocol



18

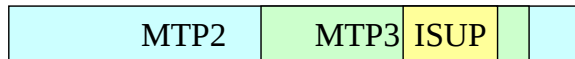
•這張是 SS7 協定的架構圖。

- TCAP: Transaction Capability Application Part 信息交易應用部
 - SCCP: Signaling Connection Control Part 信號連接控制部
 - TUP: Telephone User Part 電話用戶部
 - ISUP: ISDN User Part 整體服務數位網路用戶部
 - INAP: Intelligent Network Application Part 智慧型網路應用部, 也是 TCAP 的上層
 - MAP: Mobile Application Part 行動電話應用部
 - OMAP: Operation Maintenance Administration Part 營運維護管理部
 - MTP: Message Transfer Part 訊息轉送部
 - NSP: Network Service Part 網路服務部
- 右方是 SS7 每一個層次的協定, 左方說明所對應的 OSI 7 layers.
- 每個協定在下面會分別介紹。

The SS7 Protocol Layers (1/3)

➤ The Message Transfer Part (MTP)

- MTP Level 1 defines the physical, electrical and functional characteristics of the signaling.
✓ 100111010110000011100111001.....
- MTP Level 2 provides reliable transfer of signaling messages between two directly connected signaling points.
- MTP Level 3 provides the functions and procedures related to message routing and network management.



19

•MTP level 1 提供 signal link 的 bearer 實體. 通常是使用 64kbps 的 digital line 的 T1 or E1. (也可以是 analog 4 or 3kHz spacing).

- 定義於 ITU-T Q.702 建議書

- 定義電氣與功能特性, Coding, Time slot number, bit rate, framing, impedance bit invert.

•MTP level 2 藉由 MTP1 收送一些控制信號的方式, 建立相臨兩個元件間的連結. 其功能如 error detection and correction, flow control, signal unit delimitation and alignment (信號單元之界定與調正), initial alignment(初始調正). MTP level 2 是由 HDLC specification 演變而來.

- 定義於 ITU-T Q.703 建議書

- 定義信號鍊路 (signaling link) 之功能特性, 主要功能包括: 信號單元界定 (delimitation, 用一個flag=01111110做界限, 取出一個 signal unit, SU), 信號單元校驗 (alignment), 信號單元誤碼偵測 (error detection, 使用 sequence number), 信號單元誤碼更正 (error correction), 初始校驗 (initial alignment), 信號鍊路誤碼率監視 (signaling link error rate monitoring), 流量控制 (flow control)

- MTP2 會處理某些信號單元, 而某些信號單元會轉送到 MTP3 處理.

•MTP level 3 負責 signal 的傳送, 將 message 送到目的地, 並負責 network 的管理, 依據 network 的 status information 來控制目前 signal 的 routing 並重新組構信號網路設施.

- 定義於 ITU-T Q.704 建議書

- MTP3 分辨是否是自己的訊號, 不是則送到訊息路由, 轉送到適當元

The SS7 Protocol Layers (2/3)

➤ The Integrated Services Digital Network User Part (ISUP)

- Establishes *circuit-switched network* connections
- Ex: Call setup or release

➤ Signaling Connection Control Part (SCCP)

- SS7 message routing is performed at the MTP and the SCCP of a node.
- **Global Title Translation (GTT)**
- To transfer *Circuit-relative* and *non-circuit-related* signaling information

20

•ISUP 提供基本載送服務(i.e., call control: 建立voice線路, 數據傳送通話階段, 呼叫釋放階段)及增值性服務(包括指定轉接,直接撥入分機, 顯示caller 號碼, 群內通信, user to user signal), 檢查 call status, trunk management.

•ISUP 包含 2 POTS 使用者間, 2 ISDN 使用者間, 1 POTS 與 1 ISDN 使用者間 call control 的交換信號.

•ISUP 的訊號比其他(如TCAP)有更強烈時間控制上的需求.

•另外還有下面的 parts (和 ISUP 同級):

•Broadband ISDN User Part: 支援 broadband ISDN connections 的 setup/release.

•Telephone User Part (TUP): 提供國際電話呼叫控制信號.

•SCCP 提供 MTP 之附加功能, 以達成整個 network layer 應有的功能, 傳送 circuit-relative (提供 ISUP以建立 end-to-end connection, 但目前 ISUP直接連到MTP) 與 non-circuit-relative (如GTT 的 efficient routing services)

•PCS 的註冊與 cancellation 都是所謂 con-circuit-related 訊號

•基本上 SCCP 位於 OSI 第 3,4 層. (目標是有效率的路由工作), 沒有維護訊號的順序

•多個訊息的順序 (message sequence),由 TCAP 做, 也有考慮到 timeout constraint.

•SCCP 支援 connectionless (先建立 connection, 再傳送資料, 釋放連結, 像 TCP) 與 connection-oriented (不建立 connection, 像 UDP).

•若有電話撥出一個 MIN 號碼, 最原先處理這通電話的節點不見得有足夠的資訊可以指出真正的目的地 (因為不曉得手機在那裡), 所以相關的資訊要送

The SS7 Protocol Layers (3/3)

➤ Transaction Capabilities Application Part (TCAP)

- Provide the ability to exchange information between applications
- *Non-circuit-related signaling*

➤ The Mobile Application Part (MAP)

- Application of TCAP
- IS-41 & GSM MAP are implemented in MAP layer.

➤ The Operations, Maintenance, and Administration Part (OMAP)

21

•TCAP 提供各節點間 non-circuit-related 相關訊息的傳送, 並提供服務給上層
的各種應用 (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, 使用稱為 Basic Encoding
Rules (BER) 的 standard. (與 OSI transfer syntax 非常相同).

- IS-41 為提供 mobility management, 便制定了 50 種 TCAP operation
(for inter-MSC handoff, automatic roaming, OA&M).

- Intelligent network 也是 TCAP 的 AP, 但會改到 hardware.

- IS-41 的 TCAP 使用 SCCP class 0 connectionless service

- TCAP 的上層可以是 MAP, OMAP, INAP, ...etc.

•OMAP: network management 是 TCAP 上層的應用層, 負責網管的功能.

•MAP 也是TCAP 上層的應用層, 處理與 mobile 相關的應用服務.

- IS-41 與 GSM MAP 都是屬於這層的應用.

•ISUP 提供基本載送服務(i.e., call control: 建立voice線路, 數據傳送通話階段,
呼叫釋放階段)及增值性服務(包括指定轉接,直接撥入分機, 顯示caller 號碼,
群內通信, user to user signal), 檢查 call status, trunk management.

•另外還有下面的 parts :

- Broadband ISDN User Part: 支援 broadband ISDN connections 的
setup/release.(和 ISUP 同級)

- Telephone User Part: 提供國際電話呼叫控制信號.(和 ISUP 同級)

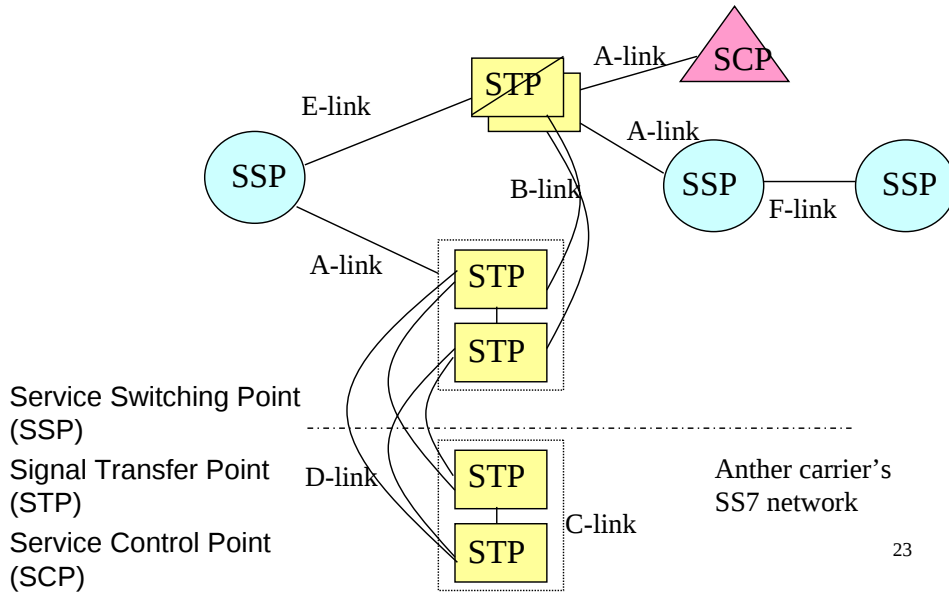
- BSSAP

Components and Links of SS7

22

- 這個部份說明 SS7 網路上的基本元件, 即各個節點所代表的含意與功能.
- 同時說明各節點間, 相互連接所使用的連結方式.
- 電信網路上為了 reliability, 設備都會以 redundant fashion 的方式佈署, signal 也會自動從另一路徑送出, 以避免其中之一發生錯誤. 雖然 links 間也會用於 traffic load share, 但決不會超過 45% 的負荷, 確保單一 link 可完成工作. Error recovery 也是 SS7 上必備確保訊號正確送達.

SS7 Network



23

- SSP: MSC, switch.
- SCP: HLR/VRL
- STP: router
- D-link: STP pairs cross different vendors, ex: PSTN and PCN
- B-link: two STP pairs in the same vendors

Components of SS7

➤ Three distinct components of SS7

- Service Switching Point (SSP)
- Signal Transfer Point (STP)
- Service Control Point (SCP)

➤ Note :

- *Trunks* connects SSPs to carry user data/voice information.
- *Signaling links* connect SCPs to STPs, and STPs to SSPs.

24

•SS7 上三種重要的元件:

- SSP: 一般的交換機, 負責電話的建立, 終止, 連接 subscriber 間的 trunk, 也負責 billing.
 - 在 PSTN, SSP 就是一般的電話交換機, 例如是 tandem 或 end office. 如果在 PCS, 則 SSP 就是 MSC.
 - SSP 與用戶端的 CPE 以 subscriber lines 相連, 接收 CPE 的信號且做出適當的 call processing. 所以, SSP 會處理所有收到啟動, 繞送, 終止電話的工作. SSP 是 SS7 訊號傳輸的 source 與 destination. 透過 STP, SSP 可傳送相關的訊息給其他 SSP 或向 SCP 提出要求.
- STP (信號轉送點): 一種特殊的交換機, 不送 voice 等 data, STP 利用 SS7 訊息上的位址欄位, 將 SS7 的 signal 轉送. 換句話說, 做 routing 的工作.
 - 為了 reliability 的需求, STP 都是成對出現. STP 為保護網路上的安全, 也會有 screening 的功能.
 - SS7 的功能類似 OSI layer 3.
 - 台灣 STP 直接架在 SSP 上.
- SCP 包含相關的 software & database 以提供更多的服務. 例如 0800 免付費電話 SSP 會詢問 SCP, SCP 找到真正的 address 並回傳給 SSP, SSP 才開始建立這通電話.
 - 在 mobile applications, SCP 可能是 HLR or VLR.
 - SCP 接收來自 SSP 的查詢, 並回應相關的資訊給 SSP.

Signaling Links of SS7

➤ 6 types of signaling links in SS7.

- A-link: access link
- B-link: bridge link
- C-link: cross link
- D-link: diagonal link
- E-link: extended link
- F-link: full associated link

25

- SS7 採用 64kbps, full duplex, digital transmission channel.

- 3 components of SS7 are STP, SCP, SSP

- A-link: STP-SCP, STP-SSP(如MSC,SMSC)

- 每一個 SSP or SCP 至少有一 signaling link, 即 *Access Link (A-link)*, 與 STP pair 相連.

- 因 MSC 是一種 SSP, 因此 A-link 可用來連接 MSC 與 PSTN STP pair

- 在北美, 一條 A-link 通常是 56kbps 的數位線路, 歐洲用 64kbps. 在 T1 或 E1 上傳送.

- The number of A-links between an SSP and an STP pair can be up to 128. Most switch suppliers have limited 16.

- E-link: 用於增加 reliability, 連接 STP 與另一個區域的 SSP, 當話務量增多時使用, 但實際上很少用到 E-link.

- B-link: 連接兩個 STP pairs 間的 STP-STP

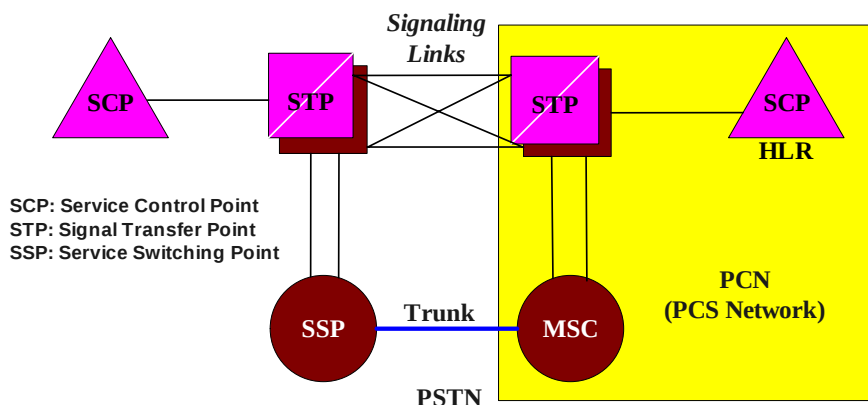
- C-link: 連接一組 STP pair 內的 2 個 STP. 除非網路有錯誤須要如此繞送, 否則 C-link 上只會傳送 status message.

- D-link: 即 Diagonal link, 連結不同 vendor 間的 STP-STP pair (ex: PSTN and PCN), 傳送 signals 的 link

- D-links are deployed in a quad arrangement with three-way path diversity. The maximum link set size is 64.

- Signaling links that connect STPs of different networks (e.g., PCN and PSTN) are called D-link.

Interconnection between a PCS network and the PSTN

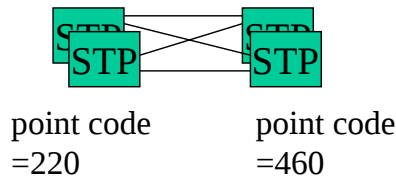


26

- 使用 SS7 做為 PCS 與 PSTN 之間的連接方式有許多種, 但接下來只說明其中的 4 種模式.
- 由圖上可以看到連線分成訊號 (signal) 與用戶語音 (trunk) 傳輸兩部份.
 - STP 與 STP (看成是 router) 間傳送控制訊號等訊息, 中間是以 D-link signaling links 相連接.
 - PSTN 的 SSP 與 PCS 的 MSC 間傳送使用者的語音與數據資料.
 - 如果 PSTN 間傳送 user data 的 SSP 是 Tandem, 則 Tandem 與 MSC 是用 Type 2A 的介面相連.
 - 如果 PSTN 間傳送 user data 的 SSP 是 End office, 則 End office 與 MSC, 是用 Type 2B 的介面相連.
- 由於某些服務, 像是 080 免付費電話, 一定是 tandem 來處理, 所以經由 Type 2B interface, 沒有辦理處理這一類的服務.
- 假如 PSTN 的 STP 直接與 MSC 相連, 而不透過 STP, 就會形成三角形的樣子, PSTN 的 STP 與 PCS 的 MSC 間, 是用以 A-links 直接互傳控制訊號.

Point Code

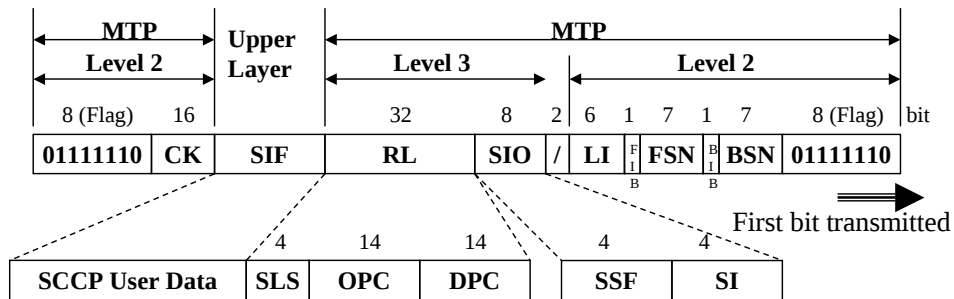
- Point codes (PCs) are addresses used for message routing in SS7 networks.
- Each SS7 network element is assigned with a unique point code.



27

- 每一個 SS7 的元件都會分配到(在自己或特定網路內)一個獨一無貳的號碼, 稱為 point code (點碼), 即 SS7 網路上各節點的位址. 利用這 14 bit 的 point code, 就可以指出 signal 所要傳送的地點.
- 如果是”國際信號點碼”, 全世界共分為 6 個區帶 (用 3 bit 代表此區帶的名稱), 接下來有 8 個 bit 代表區/網名稱, 最後用 3 bit 代表此區/網內的元件, 稱為信號點名.
 - 例如台北國際信號點碼為 4-150-1, 以10 進位表示為 9393. 高雄國際信號點碼為 4-150-2, 以10 進位表示為 9394.
 - 國內信號點碼則由系統業者自行設計. 但都會分配給每一元件一個獨一無貳的號碼.

SS7 Signal Unit Format



Example: SCCP message

BSN: Backward Sequence Number
BIB: Backward Indicator Bit
FSN: Forward Sequence Number
FIB: Forward Indicator Bit
LI: Length Indicator
SIO: Service Indicator Octet

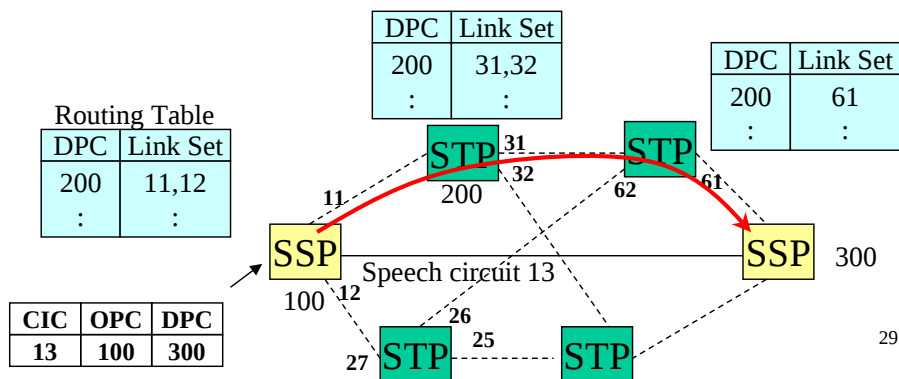
SI: Service Indicator
SSF: Sub-service Field
RL: Routing Label
DPC: Destination Point Code
OPC: Originating Point Code
SLS: Signaling Link Selection
SIF: Signaling Information Field

28

- SS7 的 signal unit 如同上面的格式, 下層 MTP 部份是所有 signal 都有的 (upper layer 不一定), 分成三大類:
 - Message signal unit (MTU): LI>5, MTP2 交給 MTP3 處理,
 - Link status signal unit (LSSU): 只在 MTP2 處理, 沒有 upper layer 與 level 3 的部份, 在 LI 後面有 8-16 bits 的SF (LI=1 or 2).
 - Fill-in signal unit (FISU): 只在 MTP2 處理, 沒有 upper layer 與 level 3 的部份 (LI=0).
 - LI: Length Indicator, 定出 Level 3 與 upper layer 部份的長度
- SS7 元件會判斷是那一種封包, 若是 FISU 或 LSSI 會收下來自己處理, 若是 MTU, 則會利用 RL (Routing Level) 決定轉送到那一個元件, 或是DPC相同, 而判斷是自己的封包往上層送.
- Flag=01111110 做為信號單元的界定(delimitation).
- FSN: Forward Sequence Number, BSN: Backward Sequence Number, 用於決定 message flow 的順序.
- Retransmission: 若 SS7 元件拒絕來自 Forward (Backward) 的訊息, 那麼就會將 BIB=1 (FIB=1) 要求對方重送 FSN (BSN) 的訊息.
- SSF: Sub-service Field, 用於區分網路種類(國際網路=00xx或國內網路=10xx),
- SI: Service Indicator, 用於區分訊息使用者 (MTP3=0,1/TUP=4/ISUP=5/SCCP=3).
- SIF: Signaling Information Field 承載上層資訊, 長度為 3-272 bytes

MTP Layer Routing

- **Destination Point Code (DPC)** = actual address of the destination node.
- Lookup tables is used in the MTP



- 傳送 SS7 的訊號, 路由的功能是在 MTP 與 SCCP 來執行.
 - 節點包括: SSP, STP, or SCP
- 對於 MTP 1-3, 這些信號的訊息, 會依據包含的 DPC 來傳送.
 - DPC 代表真正的目的地位址. MTP 會查表以找到正確的路由路徑.
 - OPC 代表真正的 originating 位址. OPC, DPC 與 SLS (signaling link selection) 都會放在 MTP 3 的 field 中.
 - 一路上 OPC 與 DPC 都不會更改, 比較像是 source IP 與 destination IP.
 - CIC 表示 voice 使用的線路號碼.
 - 若目的地 MTP 無法瞭解, 就要透過 SCCP 來運作.
- 在 SCCP 層的 address 為 called party address (PC+SSN+GT) 與 calling party address. SCCP 是跟據 GTT 來做 routing.

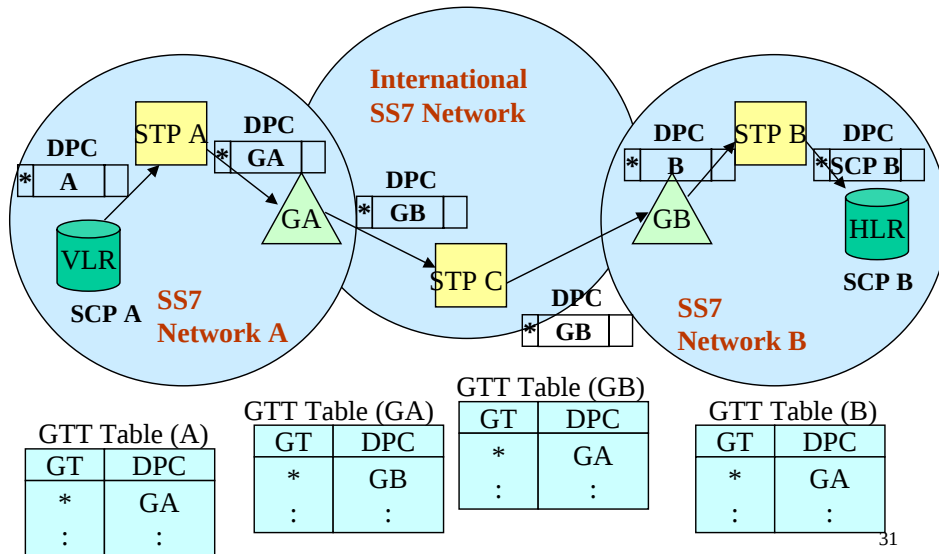
SCCP Layer Routing

- Global Title Translation (GTT) is a function defined within SCCP.
 - Performed at a STP or MSC.
- GTT is the process of translating a network layer address, dialed digits, or a service subsystem number (SSN), to the point code of the destination SSP.
- Routing based on GT translations
 - Called Party Address (PC+SSN+GT)
 - Calling Party Address (PC+SSN+GT)

30

- GTT: Global Title Translation 是 SCCP 中的一個 function.
- GTT 是一種利用電話號碼或像HLR/VLR的網路位址(SSN), 將訊息一層層送到與HLR/VLR相連之 SS7 元件的過程. 在這樣的過程中, 都要知道下一個 hop 的 point code. 所以才會說是轉成 point code.
 - 在 SCCP 層, 每一個 entity 會有一個 number SSN, 換句話說, SSN 是 ASE (application service entity) 的 address. 在傳送的訊號中, 會記錄目的地位址, 就是 SSN. 以 HLR 為例, 其 SSN 是 0000110. SSN 並不是真正的實體層位置.
- 以下以 800 電話為例, 說明整個流程的經過:
 - MSC 要處理一通 800 的電話, 送 request message 給俱有 GTT 功能的 STP.
 - STP 收到 800 translation services 的要求時, 要找出適當的 SCP 的位址, 而且將 request 轉送給此 SCP.
 - SCP 會將 800 xxx xxxx 的免付費電話號碼, 會被轉成標準的電話號碼 directory number. SCP 將話號傳回給 STP. (STP 上的 GTT 就是在找出可以將 message 轉送到這樣的 SCP 的下一個 hop 的 point code.)
 - STP 將真正的電話號碼回傳給 MSC.
- 當 STP 傳送訊息時, 遇到下層的 MTP1-3 無法處理的情況, SCCP 這一層就會執行 GTT 這個流程.

GTT Example

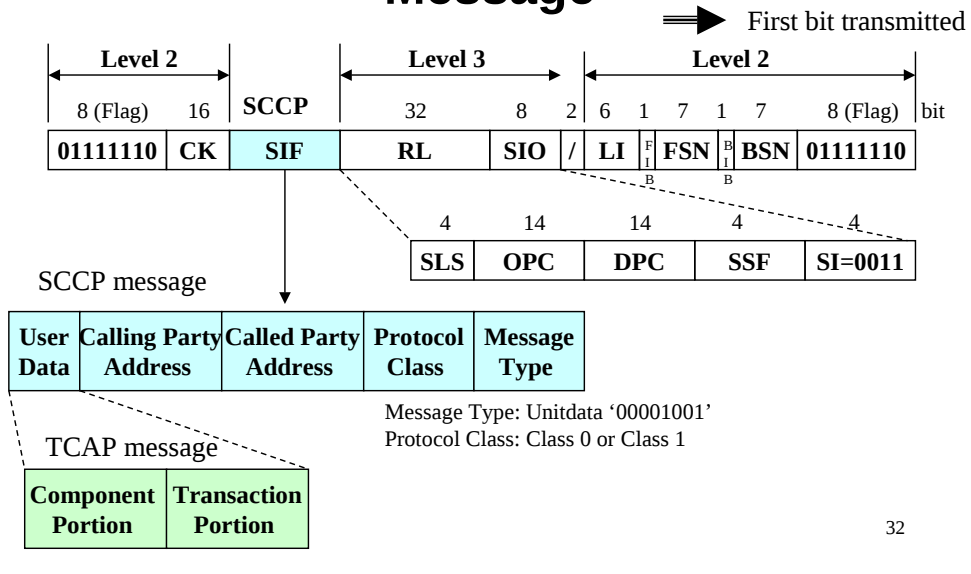


*: Global Title of HLR

•以下以手機新來到一個 VLR, VLR 要送一個訊息給手機所屬之 HLR 為例, 說明整個流程的經過:

- VLR 送 request message 給俱有 GTT 功能的 STP A.
- STP A 收到封包, 利用 address 與查詢GTT Table, 找出下一個 hop (GA) 的 point code, 填入DPC中, 將 request 封包送出.
- SSP GA 收到封包, 利用 address 與查詢GTT Table, 找出下一個 hop (GB) 的 point code, 填入DPC中, 將 request 封包送出.
- 經過STPC 的繞送(但 STP C 沒有做 GPP), SSP GB 收到封包, 利用 address 與查詢GTT Table, 找出下一個 hop (STP B) 的 point code, 填入 DPC中, 將 request 封包送出.
- STP B 收到封包, 利用 address 與查詢GTT Table, 找出下一個 hop (SCP B) 的 point code, 填入DPC中, 將 request 封包送出.
- 整個過程稱為 GTT (for SCP B)

SCCP Message Embedded TCAP Message



- 這是一個 SCCP message 包含 TCAP message.
- SSF: Sub-service Field, 用於區分網路種類(國際網路=00xx或國內網路=10xx),
- SI: Service Indicator, 用於區分訊息使用者 (MTP3=0,1/TUP=4/ISUP=5/SCCP=3).
- SIF: Signaling Information Field 承載上層資訊, 長度為 3-272 bytes
- CK: check bits.

PCS/PSTN Call Control Using ISUP

33

- 以下我們將介紹負責建立電話通路的 SS7 的 ISUP layer.
- 我們將以PSTN 先打電話時 (land-to-mobile), 與 PCS 先打電話時 (mobile-to-land), 建立與結束通話的流程, 來說明相關的 signaling.

Interactions between a PCN and the PSTN

- Interconnection Interfaces
- Message Routing
- Mobility Management
- Call Control

34

- 有了上述的連結 (interconnection), PCS 網路與 PSTN 網路之間就可以進行互動 (interaction). 這些互動分成 4 個主要的部份:
 1. 連結介面 (Interconnection Interfaces): 建立連結, 使 PCN 與 PSTN 可以互動.
 2. 訊息繞送(Message Routing): 在 PCN 與 PSTN 間會交換訊息, 因此這些訊息會經過許多元件來繞送.
 3. 行動管理(Mobility Management): 交換追蹤 mobile users 位置的訊息.
 4. 電話控制 (Call Control): 在 mobile user 與另一使用者間建立一個電話傳輸路徑.
- 底下會著重於 call control.

ISUP Message

➤ ISUP messages

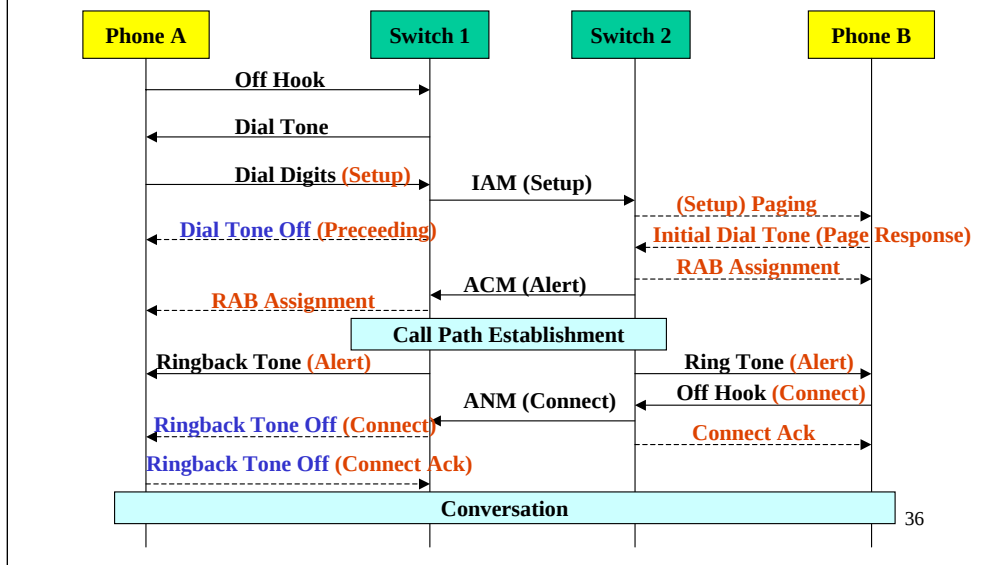
- Establishes *circuit-switched network* connections
- Call setup/release between the PSTN and a PCN.

➤ ISUP messages that are delivered by MTP routing.

35

- 連結 PCN 與 PSTN 的電話控制是使用到 SS7 的 ISUP 這個部份的訊息。
 - ISUP 專門使用於 call control, 建立與語音通道相關連結的通訊協定.
 - 在這裡電話兩端分別是 PCN 與 PSTN, 一樣也要用 ISUP 建立起通話管道.
 - ISUP 下層是 MTP, 因此由 MTP 負責繞送 ISUP 訊息.
- 以下我們將介紹使用 Type 2A with SS7 (tandem 接 MSC) 時, PSTN 先打電話時 (land-to-mobile), 與 PCS 先打電話時 (mobile-to-land), 建立與結束通話的流程.
- 如果是使用其他連結方面, 只有在傳送路徑, 傳送訊息上會稍做修改.

Basic Call Setup



•這是基本的建立起電話的程序. 兩支電話 Phone A 與 Phone B 透過 switch 建立起電話連線.

•Off Hook: 拿起話筒. Dial Tone: 聽到撥號音. Dial Digits: 撥電話號碼.

•Ring Tone: 電話聲響起. Ringback Tone: 等待的 ring.

•在 switch 間使用的就是 ISUP message. 其實與生活中打電話的經驗相結合, 就可猜到其意義.

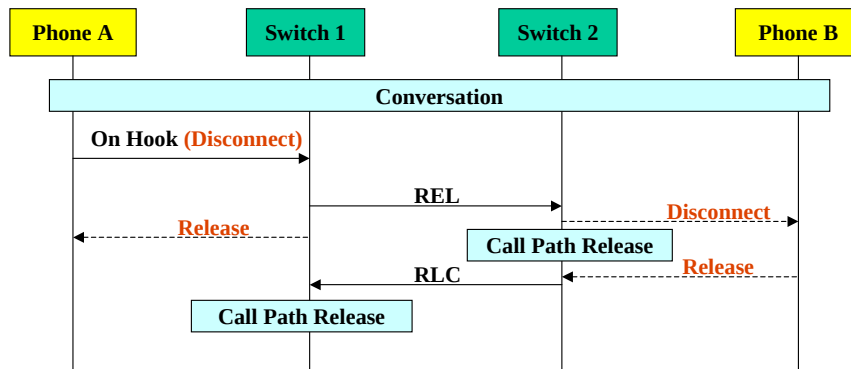
•**Initial Address Message (IAM):** 嘗試與對方建立 trunk

•**Address Complete (ACM):** 表示到對方的路徑可以導通, 送回 alert, 表示可以真正把 trunk 接起來

•**Answer Message (ANM):** 表示 Phone B 接電話了, 可以開始通話

•Phone 與 switch 之間黑色的 signal 是可聞信號.

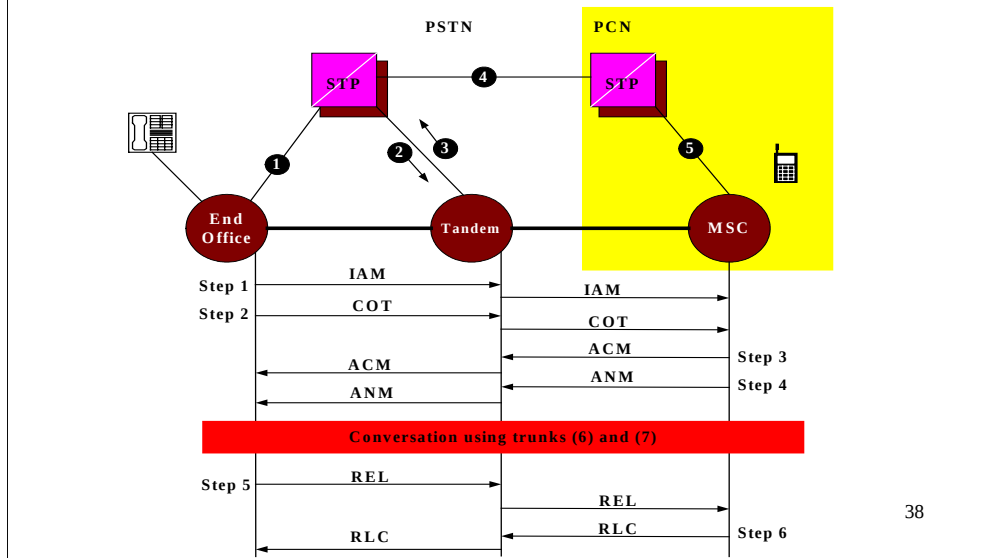
Basic Call Release



37

- 這是基本的掛電話的程序. 電話 Phone A 首先掛電話, 中止與 Phone B 間的電話連線.
- On Hook: 掛話筒.
- 在 switch 間使用的 ISUP message:
 - Release (REL):** 表示要結束電話連線
 - Release Complete (RLC):** 表示表示 trunk 已進入 idle 狀態
- 當 switch 收到 **Release Complete (RLC)** 後 0.5 到 1 秒, 才會真正釋放出 trunk.

Land-to-Mobile Call Setup and Release



38

•這是典型的經由 tandem 溝通的 Type 2A with SS7 (Tandem 接 MSC) Land-to-Mobile Call Setup and Release 訊息流程, 整個 signaling 的路徑為 (1) -> (2) -> (3) -> (4) -> (5), 或相反的路徑. 粗線是 trunk, 可能在過程中進行品質的測試, 但不送 signaling.

•**Step 0.** 當一般 PSTN 的電話撥出手機的電話號碼(MIN), EO (end office) 注意到這是無線電話的號碼. 假設 EO 有查問 HLR 的能力, 所以 EO 便送出一個詢問的訊息給 HLR, 希望得到手機的 temporary local directory number (TLDN).

•若是 EO 沒有查問 HLR 的能力, EO 會將 MIN 送到一個特殊的交換機 (i.e., GMSC) 尋求手機位置以建立通話.

•**Step 1.** EO 得到手機的 TLDN 後, 會送出 Initial Address Message (IAM) 給 PCN MSC, 開始傳送溝通訊號, 以建立通話的 trunk.

•EO 會將要傳送語音的線路標示為 busy, 而且將相關的資訊夾在 IAM 中送出給相連的 tandem. 例如在 IAM 中會標明是否須要做 continuity check. (路徑為 (1)->(2)->(3)->(4)->(5)).

•**Step 2.** 如果 EO 送給 tandem 的 IAM 指定要進行 continuity check, 便會進行 trunk 的測試, 以確保符合傳輸的品質. 當 continuity check 檢查完畢正常, EO 會送出 Continuity Message (COT) 給 tandem, 同時此 trunk 便已設定完成.

•**Step 3.** 當 MSC 收到 IAM, MSC 會呼叫 MS. 這時則可能會出現以下幾種狀況:

•**Event 1.** MS 正在打電話, 則可以用 call forwarding 或 call waiting 方式處理, 或者 MSC 直接傳回 Release (REL) 訊息給 EO, 並表示是因為 busy line situation 而終止通話.

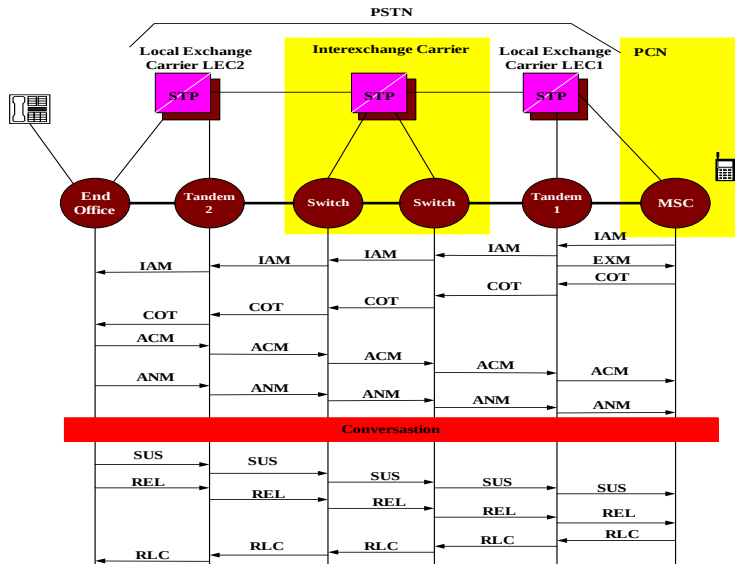
•**Event 2.** MS 處於 idle 狀態, MSC 便送回 Address Complete (ACM) 訊息給 EO (路徑為 (5)->(4)->(3)->(2)->(1)).

•**Event 3.** 如果 MS 沒有回應 (例如未開機), MSC 可以轉送電話到別處或傳回 REL 訊息給 EO.

•**Step 4.** 如果 MS 接電話了, MSC 送回 Answer Message (ANM) 給 EO, 開始通話.

•**Steps 5. and 6.** 假設 PSTN (calling party 發話端) 先掛電話, EO 送出 Release (REL) 以表示要結束電話連線, 接著 MSC 收到 REL, 並回覆 Release Complete (RLC), 表示 trunk 已進入 idle 狀態. 當 EO 或 tandem 收到 Release Complete (RLC) 後 0.5 到 1 秒, 才會真正釋放出 trunk.

Mobile-To-Land Call Setup and Release



39

•這是典型的經由 tandem 溝通的 Type 2A with SS7 (Tandem 接 MSC) Mobile-to-Land Call Setup and Release 訊息流程。

•因對方太遙遠, 整個通話的路必須經過 PCN → Local Exchange Carrier, LEC1 → Interexchange Carrier, IXC → LEC2 這樣的路徑。

•在建立電話的流程與 Land-to-Mobile 類似, 唯一不同在於與 MSC 相連的 Tandem 1, 可能會送出 **Exit Message (EXM)** 給 MSC, 表示 SS7 建立電話的資訊 (IAM) 已經成功的送到 IXC。

•如果 Tandem 1 已經從 IXC 收到 ACM, ANM, 或 REL, 或者 EXM timer 已經先 timeout (在 Tandem 1 送 IAM 給 IXC 開始啟動 timer), Tandem 1 就會送 EXM 給 MSC。

•但是如果收到含有測試失敗訊息的 **Continuity (COT)**, Tandem 1 就不會送 EXM 給 MSC。

•通話完整, 假設是 PSTN 端 (called party) 先掛電話, End office 就會送出 **Suspend Message (SUS)** 表示結束通話。

•EO 會設定 SUS timer, 且 EO 會在未來 14 到 16 秒間期望下面某一事件的發生:

•Event 1. MS (calling party) 也掛電話, MSC 端送來 **REL**. 此時 EO 就釋放 trunk。

•Event 2. PSTN 電話又接起來繼續通話, 因此 EO 送出 **Resume Message (RES)** 給 MSC, 並終止 SUS timer。

•Event 3. 如果 **SUS** timer 逾期, EO 也會終止 trunk 且送出 **REL** 給 MSC。

•相同的, 當 MSC 接到 SUS, 會設定 SUS timer, 而且 MSC 會在未來 10 到 32 秒間期望下面某一事件的發生:

•Event 1. (對應上面的 Event 1) MS (calling party) 掛電話, The MSC 送回 **REL** 要求 EO 就結束 trunk 的通訊。

•Event 2. (對應上面的 Event 2) MSC 收到 EO 送來的 RES, MSC 終止 SUS timer 繼續通話。

•Event 3. (對應上面的 Event 3) MSC 收到 EO 送來的 REL, MSC 終止通話.送回 FLC。

•Event 4. 如果 **SUS** timer 逾期, MSC 終止通話。

Summary

- SS7: out-of-band signaling method
- Components and Links of SS7
 - 3 components: STP, SSP and SCP
 - 6 links: A-F links.
- Interconnection between PCN and PSTN
- PCN/PSTN Call Control Using ISUP
 - Land-to-Mobile Call Setup/Release Procedures
 - Mobile-to-Land Call Setup/Release Procedures