

行政院及所屬各機關出國報告

(出國類別：實習)

赴芬蘭實習「GPRS 核心網路演進及增值服務設計」 出國報告

服務機關：中華電信股份有限公司

行動通信分公司

出國人：工程師 張進裕

股 長 龔榮津

助理工程師 吳豐任

專 員 鐘元良

出國地區：芬蘭

出國期間：民國 91 年 12 月 1 日至

民國 91 年 12 月 14 日

報告日期：民國 92 年 3 月 15 日

系統識別號:C09105765

公 務 出 國 報 告 提 要

頁數: 51 含附件: 否

報告名稱:

實習「GPRS核心網路演進及加值服務設計」

主辦機關:

中華電信行動通信分公司

聯絡人/電話:

陳月雪/23442808

出國人員:

龔榮津	中華電信行動通信分公司	網路維運處	股長
鐘元良	中華電信行動通信分公司	工務處	專員
吳豐任	中華電信行動通信分公司	台北營運處	助工
張進裕	中華電信行動通信分公司	高雄營運處	工程師

出國類別: 實習

出國地區: 芬蘭

出國期間: 民國 91 年 12 月 01 日 - 民國 91 年 12 月 14 日

報告日期: 民國 92 年 04 月 04 日

分類號/目: H6/電信 H6/電信

關鍵詞: GPRS

內容摘要: 職等四人奉中華電信總公司核准，赴諾基亞公司芬蘭訓練中心接受為期兩週之「GPRS核心網路演進及加值服務設計」實習，其目的在於藉著與系統廠商研討及學習，以增進本公司同仁對GPRS加值服務設計之規劃、設計、新服務及新功能之開發以及維運等技術；並期望瞭解GPRS核心網路未來之發展及趨勢，以供本公司未來規劃之參考。本報告內容彙整成章，摘要如下：前言第一章：Nokia GPRS Packet Core Release 2的特色第二章：GPRS Intranet Access Service 第三章：GPRS Internet Access Service 第四章：GPRS CDR資料分析第五章：GPRS LCS定位資訊系統第六章：感想及建議

本文電子檔已上傳至出國報告資訊網

摘 要

職等四人奉中華電信總公司核准，赴諾基亞公司芬蘭訓練中心接受為期兩週之「GPRS 核心網路演進及增值服務設計」實習，其目的在於藉著與系統廠商研討及學習，以增進本公司同仁對 GPRS 增值服務設計之規劃、設計、新服務及新功能之開發以及維運等技術；並期望瞭解 GPRS 核心網路未來之發展及趨勢，以供本公司未來規劃之參考。

本報告內容彙整成章，摘要如下：

前言

第一章：Nokia GPRS Packet Core Release 2 的特色

第二章：GPRS Intranet Access Service

第三章：GPRS Internet Access Service

第四章：GPRS CDR 資料分析

第五章：GPRS LCS 定位資訊系統

第六章：感想及建議

目 錄

	頁次
前言.....	5
第一章 Nokia GPRS Packet Core Release 2 的特色.....	7
1.1 簡介.....	8
1.2 動態 PDP CONTEXT 配置.....	9
1.2.1 Secondary PDP CONTEXT.....	9
1.3 QoS 支援.....	10
1.3.1 SGSN 支援的 QoS.....	11
1.3.2 GGSN 支援的 QoS.....	12
1.4 頻寬管理(Bandwidth management).....	12
1.5 系統等級追蹤(System Level Trace).....	13
1.6 計費資料產生最佳化.....	16
1.6.1 防止重複產生 CDR.....	16
1.6.2 S-CDR 的產生.....	17
1.7 預付卡服務.....	17
1.7.1 IN-based 預付卡服務.....	18
1.7.2 Server-based 預付卡服務.....	20
1.7.2.1 SGSN 特有的 Server-based Prepaid 功能.....	21
1.7.2.2 GGSN 特有的 Server-based Prepaid 功能.....	21
1.8 強化監聽功能.....	22
1.8.1 LIG 架構.....	22
1.8.2 新增加的一般功能.....	24
1.8.3 LIC 元件新功能.....	24
1.8.4 LIB 元件新功能.....	24
1.9 支援 GEA2(GPRS Encryption Algorithm).....	24
第二章 GPRS Intranet Access Service.....	25
2.1 GPRS VPN 概述.....	26
2.2 GPRS VPN 架構中相關 Tunneling 技術概論.....	26

2.3 GPRS VPN 網路架構without Virtual Router(VR).....	28
2.4 GPRS VPN 網路架構with Virtual Router(VR).....	30
2.5 於GPRS VPN 服務網路引進Virtual Router 之優點.....	32
第三章 GPRS Internet Access Service.....	34
3.1 GPRS VPN 網路架構with Virtual Router(VR).....	35
3.1.1 GPRS Internet Access Service 網路架構.....	35
第四章 GPRS CDR 資料分析.....	37
4.1 GPRS CDR 資料分析及監視工具.....	38
4.1.1 Nokia GPRS Traffica 概述.....	38
4.1.2 GPRS Traffica 功能.....	38
4.1.3 網路結構及摘要.....	42
第五章 GPRS LCS 定位資訊系統.....	46
5.1 GPRS 的定位功能.....	47
5.1.1 系統架構.....	47
第六章感想及建議.....	50

前 言

由於我國行動電話系統開放自由化後，業務競爭激烈，用戶成長迅速目前行動電話用戶已超過人口數，應是台灣另一項經濟奇蹟，但使用行動上網及行動商務服務不到 5%，距日本 NTT DoCoMo i-mode 的使用行動上網及行動商務服務人數達 60% 以上(2001 年)；J-PHONE 的 J-sky 的使用人數更高達其用戶數的 70%(2001 年)，也就是說 GPRS (General Packet Radio Service) 無線分封數據網路與無線通訊應用軟體協定(WAP)結合的第 2.5 代行動通信服務成長空間很大，尤其在用戶貢獻度 (Average Revenue per User, APRU) 持續下滑下情況下，提升其他行動增值服務的營收比重，如簡訊服務 (Short message service, SMS)，行動銀行、電玩、辦公室、企業網路以及現在的 MMS 與行動數據、行動寫真等服務以提高 APRU 是當務之急。

又現有行動電話業者 2.5G 之 GPRS 網路提供分封數據傳送平台，是發展非語音服務重要網路。具有永遠連接網路特性，2.5 業務都可轉移至 3G 系統。在 GPRS 經驗可用在 3G 系列，而 GPRS 成功之服務可移轉至 3G 系列，GPRS 將可帶動 3G 業務成長，相輔相成。但必須瞭解的是，目前不論 MMS、行動通訊以及行動寫真，需要的都是較多的頻寬，才可能提供較具品質的相關服務。儘管通信業者多強調，目前 2.5G 的頻寬，已經可以提供足夠的服務品質，但是目前數據傳輸的營收比重佔各家業者總營收皆不到 5%，若再以行動通訊的服務價格較高來推算，目前數據傳輸所佔電信業者頻寬的負載不高，所以 2.5G 的頻寬當然可以應付目前消費者對於資料傳輸的需求，但若以未來使用者如日本增加來考量，GPRS 核心網路系統升版暨服務功能擴充必須的。更是 GPRS 核心網路演進至 3G 及增值服務必要過程。尤其這次 GPRS 核心網路系統 Release 2 升版是依據 3GPP Release' 99 標準，所以升版後 GPRS 核心網路系統可同時支援 2.5G 與 3G，完成了 3G 核心網路先期演進。

本次 GPRS 核心網路系統升版暨服務功能擴充工程建設之緣由係因：

- GSM 用戶數總和大於台灣總人口數，語音用戶未來市場成長有限；目前數據增值服務用戶有限，有開發的潛能。
- 提供 GPRS Intranet Access Service、Internet Access Service 等新功能服務。
- 固網 Internet、ADSL 使用普遍，有轉移行動網的可能。

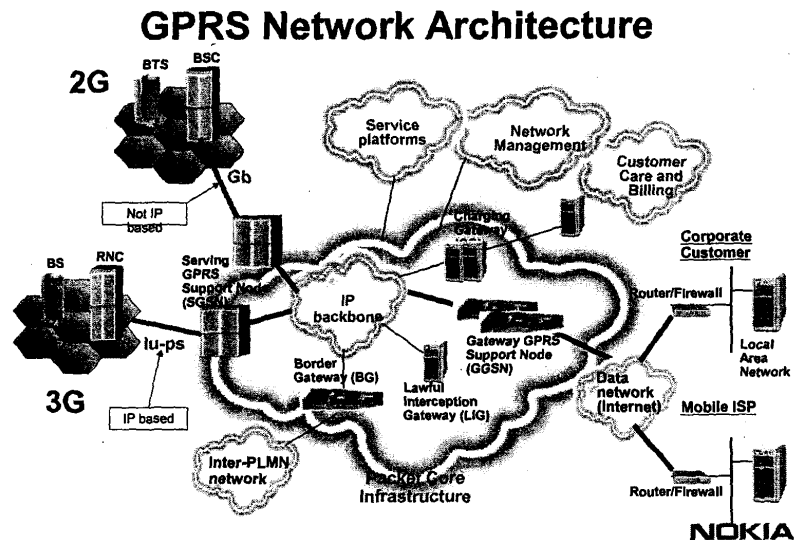
- 避免如日本 NTT DOCOMO 加值快速成長，設備不足所帶來服務品質降低之困擾。
- 3G 業務推展，視加值服務開展順利轉移至 3G，2.5G 與 3G 交遞(H.O)與互運(Interoperator)順利。
- 維運管理系統功能之提升。

第一章

Nokia GPRS Packet Core Release 2 的特色

1.1 簡介

Nokia GPRS Packet Core System Release 2 是以 3GPP Release' 99 為基礎。分封核心網路同時支援 2G GPRS 及 3G 的各種應用及服務，當然也支援 2G 及 3G 系統之間的互連。Nokia GPRS 網路包含以下網路元件：SGSN(Serving GPRS Support Node)、GGSN(Gateway GPRS Support Node)、CG(Charging Gateway)、BG(Border Gateway)、LIG(Lawful interception Gateway)、DNS(Domain Name Server)等。



Nokia GPRS 分封核心網路的優勢主要有以下幾點：

- Nokia 2G SGSN 在支援行動管理(Mobility management)功能方面相當突出：如 PDP context 更新數、位置更新數、忙時交遞以及支援 Gs 介面 (SGSN-MSC/VLR)。
- 系統容量(尤其是 PDP Context)足以支援大規模市場的各種應用服務。
- 穩定度及可靠度保證。
- 對於進展到 3G 及以 IP 為基礎平台的全 IP 化網路已有明確的方向。
- QOS 方面的支援能促進 GPRS 更廣為使用。
- IN-Based 及 Server-Based 預付卡服務支援即時存取計費和內容計費。
- NetAct(Network Management System)支援所有的網路元件
- 互連測試納入標準計畫內容的一部份。

1.2 動態 PDP CONTEXT 配置

在 HLR 中存放著用戶的 PDP CONTEXT 資料，而一個用戶可以擁有多組 PDP CONTEXT 紀錄。一組 PDP CONTEXT 紀錄包含各種資訊，如 PDP 型式、PDP 位址、進接點名稱(APN)以及定義當用戶漫遊到其他電信公司的 GPRS 網路時是否可以使用漫遊網的 GGSN 連接到外部 IP 網路。當話機已執行註冊程序後，它的 PDP Context 會從 HLR 傳送至 SGSN。用戶所擁有的 PDP CONTEXT 數目和 ACTIVE PDP CONTEXT 數目並無任何相關性。舉例來說，某用戶擁有一個 WILD CARD APN 的 PDP Context，此用戶可以使用此 PDP Context 紀錄啟動兩個 PDP CONTEXT。RELEASE 2 支援一個用戶最多可以擁有四個 ACTIVE PDP CONTEXT，但是超載控管(Overload Control)機制會限制此數量，但保證每一個用戶會擁有一個 ACTIVE PDP CONTEXT。

1.2.1 Secondary PDP CONTEXT

使用 Secondary PDP CONTEXT 的主要原因是讓用戶使用相同的 APN 啟動多個 PDP CONTEXT，每一個 PDP CONTEXT 使用相同的 IP 位址，但各使用不同的 QOS。

Secondary PDP CONTEXT 啟動程序和一般的 PDP CONTEXT 啟動程序幾乎一樣，但有一些不同的地方：

1. Secondary PDP CONTEXT 只能由手機端啟動。
2. 在 Secondary PDP CONTEXT 啟動過程中，參數大部份會參照 Primary PDP CONTEXT，唯獨 QOS 參數可能會和 Primary PDP CONTEXT 及其他的 Secondary PDP CONTEXT 不同。

Primary PDP CONTEXT 和 Secondary PDP CONTEXT 使用相同的 APN 及 IP 位址。使用與 Primary PDP CONTEXT 相同參數值的 Secondary PDP CONTEXT 都會和 Primary PDP CONTEXT 建立連結。當啟動 Secondary PDP CONTEXT 時，因為已經知道 APN 及 IP 位址，所以 SGSN 在處理 Secondary PDP CONTEXT 啟動程序時，就將 APN 選擇的程序予以忽略。

在 Secondary PDP CONTEXT 的撤銷過程中，只需要提出一次撤銷要求，而且此撤銷要求中包含拆除指標(Teardown Indicator)，則所有連結到 Primary PDP CONTEXT 的 Secondary PDP CONTEXT 都會一起撤銷。而不管是 MS、SGSN 或是 GGSN 所啟動了撤銷要求，這個拆除指標可以包含在所有的撤銷要求之中。在 Release

'97 中, PDP Context 撤銷可以針對單一 Primary PDP Context 或是 Secondary PDP Context 來執行, 所以拆除指標就沒有包含在撤銷要求之中了。

1.3 QOS 支援

3GPP TS 23.107 定義了 QOS 的概念及架構。Release '97 及 Release '99 兩組不同 QOS 屬性, 以及它們之間的對映關係, 都定義在這份規格書當中。而 Nokia GPRS Packet Core Release 2 都支援這兩組 QOS。在 IP 網路方面, IETF 組織定義一種稱為差異化服務(Differentiated Services, DiffServ)架構的概念, 使網路能夠提供具有 QOS 功能的服務。DiffServ 則是將具有相似 QoS 需求的 traffic 合在一起, 對同一類型的資料提供一致性的服務與相對性的保證, 而不是針對各別的 traffic session。每一類型的資料會有一個固定的 DSCP (DiffServ codepoint) 來區分, 傳遞資料時, 每一個 DiffServ node 會根據此類型資料的 DSCP, 依據相對應的 Per-Hop Behavior 在 DiffServ domain 上傳送。3GPP 的 QOS 屬性都對應到 DiffServ codepoints。

Nokia GPRS Packet Core Release 2 支援手機啟動一個 Primary PDP Context 外加最多三個 Secondary PDP Context。Secondary PDP Context 的 IP 位址和 Primary PDP Context 相同, 但 QOS 屬性是可以不一樣的。例如, 手機可以一方面以較低 QOS 的 PDP Context 來收電子郵件, 另一方面以較高 QOS 的 PDP Context 來對企業網路做檔案存取。不管手機端或是 GGSN 都可以對特定 PDP Context 的 QOS 的參數來做調整。

GPRS 話務方面支援 3GPP 指定的互動(Interactive)及背景(Background)話務等級。但是因為 GPRS 本來就不是即時類型的話務, 所以即使 GGSN Release 2 有支援如會談(Conversation)及串流(Streaming)話務等級的服務, 很可惜在 2G SGSN 是不支援的。互動等級話務是以低位元錯誤率(Bit Error Rate)及有限的傳輸延遲的方式來傳送的, 終端使用者使用的互動話務等級服務有瀏覽網際網路、資料庫存取及伺服器進接等。而背景等級話務是以低位元錯誤率來傳送, 但對傳送時間方面並不那麼敏感。這類話務的終端使用者是機器, 而像傳送電子郵件及短訊息就是這類型的話務。

1.3.1 SGSN 支援的 QoS

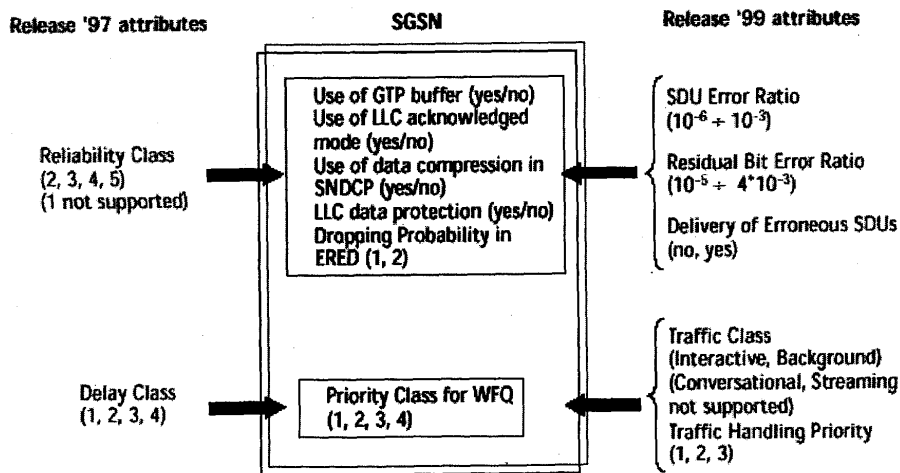
SGSN Release 2 支援以下 3GPP Release '97 的一些參數特性:

- 可靠度等級(Reliability Class)明確指出各種不同網路協定階層的傳輸模式，如 GTP、LLC 以及 RLC。
- 延遲等級(Delay Class)明確指出在 GPRS 網路中傳送 SDU(Service Data Unit)時所產生的端對端傳送延遲。

SGSN Release 也支援以下 3GPP Release '99 的一些參數特性

- SDU 錯誤率指的是遺失的 SDU 或是偵測為錯誤的 SDU 的比率有多少。
- 殘留位元錯誤率指的是所傳送的 SDU 中沒有被偵測到的位元錯誤比率，如果沒有要求做錯誤偵測，則指的是所傳送的 SDU 中的位元錯誤比率。
- 傳送錯誤的 SDU 指的是被偵測為錯誤的 SDU 到底是要傳送或是丟棄。
- 話務等級提供關於在 GPRS 上已做最佳化的應用程式的一些資訊。
- 話務處理優先權明確指出設定互動等級話務的優先權時所需要的資訊。

圖二指出這些參數對 2G SGSN 處理封包時會有什麼樣的影響。可靠度等級影響到 GTP 暫存區的使用，Acknowledged 模式的使用，其他還有 LLC 資料保護以及放棄封包資料等。而延遲等級則影響到封包資料傳送到 BSS 的優先順序。



Overview of supported attributes in the SGSN

1.3.2 GGSN 支援的 QoS

Nokia GGSN Release 2 支援 3GPP Release '99 的 QoS 規格。它支援以下 UMTS 的 QoS 參數:

- 話務等級: 會談、串流、互動及背景等級的話務
- 傳輸延遲指標
- 錯誤率
- 最大位元率
- 保證位元率
- 傳送順序
- 話務處理優先順序
- 優先權

以 PDP Context 的 QoS 參數為基礎的話, 3GPP 話務等級會對應到 IETF DiffServ Per HOP Behaviours (PHBs), 以下說明兩者的對應關係:

- 背景話務等級 -> DiffServ Best-effort PHB
- 互動話務等級 -> DiffServ Assured Forwarding PHB
- 串流話務等級 -> DiffServ Expedited Forwarding PHB
- 會談話務等級 -> DiffServ Expedited Forwarding PHB

以下的參數值可以對 PDP Context 設定:

- 即時最大位元率
- 會談最大位元率
- 串流最大位元率
- 互動話務處理優先權 1、2、3 的相關權值比重
- 對每個進接點(Access Point)的上鏈路封包, 加 DiffServ Code Point 標註

1.4 頻寬管理 (Bandwidth management)

資源保留是 IP 路由網路設計步驟的其中一部份, 而且僅用在即時話務上。要防止 IP 路由網路負載過重的情形發生, 可以藉由設定允許 GGSN 送到骨幹網路的最大即時話務量來達成。GGSN 也可以限制送到外部網際網路的話務量, 因此可以

符合業者間所簽訂的服務水準協議(Service Level Agreements)。

允許管制(Admission Control)是用來允許或拒絕PDP Context的啟動要求。當GGSN的總即時話務量是在設定的最大值以下時，則系統會接受即時的PDP Context。若相關的IP封包暫存區還有可用空間，則非即時的PDP Context仍會被系統接受。

GGSN會不斷地監看CPU及IP暫存區的負載狀況，所以允許管制及錯誤管理系統會一直監看系統資源。

1.5 系統等級追蹤(System Level Trace)

追蹤功能是系統等級特色之一，它是用來收集及記述用戶或是手機的活動狀況。在GSM網路中已經有追蹤的功能，但由於GPRS的加入，使得GSM網路增加了新的網路元件，所以舊的追蹤準則也改變了，也因此計有的追蹤功能必須要更新。追蹤功能會加在GPRS網路中所有的主要網路元件:Nokia SGSN、GGSN、BSS、HLR。

追蹤功能在3GPP Release '99並沒有完全標準化。在HLR-SGSN介面、SGSN-GGSN介面以及SGSN-BSC介面的啟動訊息則是已經標準化(3G TS 29.002 for MAP, 3G TS 29.060 for MAP, TS 08.18 for BSSGP)。

追蹤功能是一個很有效的幫手和發展工具，而且可以用來測試網路的完整性以及QOS，就如同行動電話用戶所感受的一樣。當有客戶投訴或是懷疑設備異常時，它可以用來解決系統異常或是驗證系統運作一切正常。

透過MML指令可以在NetAct(網路管理系統)啟動追蹤功能。所有從不同網路元件傳回的報告都會在NetAct中加以整合。利用Traceviewer應用程式則可以來管理追蹤功能及觀察追蹤資料。

如果使用的是CLASS B的行動電話，則須考慮到和GSM系統追蹤功能之間的互動關係。相關的資訊有可能來自於MSC及SGSN。如果手機只有執行GSM註冊，則資料只會來自MSC；若手機只有執行GPRS註冊，則資料只能來自於SGSN及GGSN。操作人員使用TraceViewer可以選擇執行GSM追蹤或是GPRS追蹤或是兩者皆執行。

由於 TraceView 只會接收 Nokia 網路元件所傳回的追蹤資料，所以如果 2G SGSN 或是 MSC/HLR 是使用其他設備商的網路元件，則必須先在該設備啟動追蹤功能，而後在 TraceViewer 啟動追蹤功能，如此 TraceViewer 才會開始接收追蹤資料。為了讓互連能順利達成，其他設備商提供的網路元件必須遵從標準規範。

追蹤的型態有三種：

- 本地用戶追蹤 Home Subscriber Trace
- 訪客用戶追蹤 Visiting Subscriber Trace
- 設備追蹤 Equipment trace

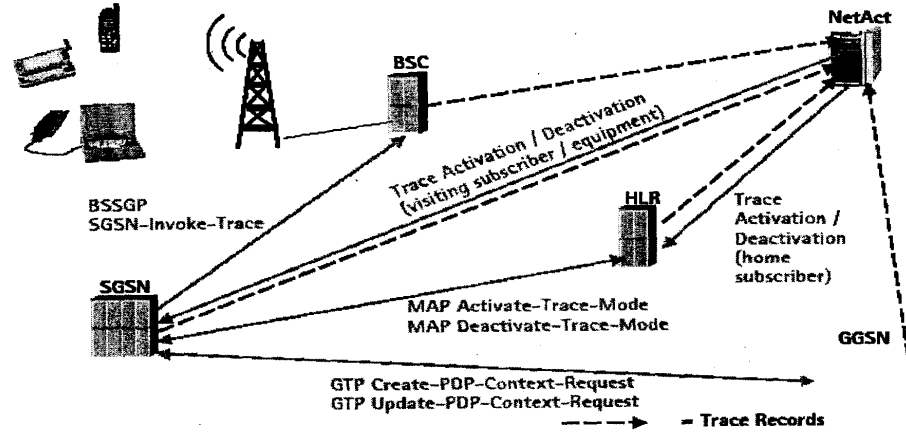
本地用戶追蹤是在 HLR 設定，而訪客用戶追蹤及設備追蹤則是在 SGSN 設定。在 SGSN 追蹤的活動狀況包括 GPRS ATTACH/DETACH、PDP Context Activation/Deactivation/Modification、Routing Area Update 及 SMS。而在 GGSN 追蹤的活動狀況則包括 PDP Context Activation/Deactivation/Modification。

系統等級追蹤也可以用來觀察用戶的活動狀態。送至 NMS 的追蹤報告則包含下列資訊：

- Event(例如 PDP Context Activation)
- Result(是否成功或是造成失敗的原因)
- Timestamp
- Access Point
- IMSI
- MSISDN
- 行動電話的 IP 位址
- SGSN 的 IP 位址
- GGSN 的 IP 位址
- Trace Reference
- Trace Trigger ID
- NMS Identity

在 HLR、SGSN、GGSN 及 BSS 所產生的追蹤紀錄會送到 NetAct。追蹤紀錄的傳送方式有兩種，第一種是先把追蹤結果儲存在本地的硬碟中，然後再將完

整的追蹤報告以 FTP 或 FTAM 的方式傳送至 NMS；第二種則是每當追蹤報告產生時，藉著 Q3 事件的方式將單一的追蹤結果送至 NMS。另外，追蹤報告傳送的方式是可以針對每個單一用戶來設定的。



Trace network architecture

在 NetAct(NMS) 中是透過 MML 指令來啟動追蹤功能。在 NetAct 中定義了其他網路元件的啟動資訊。啟動本網用戶追蹤是在 HLR 設定，而漫遊用戶及話機設備追蹤則是在 SGSN 設定。當本網用戶追蹤在 HLR 設定完成而且手機也在 SGSN 完成註冊之後，HLR 會對 SGSN 發送 MAP 訊息(Activate-Trace-Mode)來啟動追蹤，而 SGSN 會對 BSC 發送 BSSGP 訊息(SGSN-Invoke-Trace)來啟動追蹤。也就是說，HLR 會等到用戶狀態變成 Active，才會對 SGSN 啟動追蹤。

HLR 會對所啟動的追蹤保持密切注意。當用戶移動至另一個 SGSN 時，用戶的追蹤狀態會改變。首先 HLR 會解除舊的 SGSN 的追蹤，SGSN 則解除舊 BSC 的追蹤，然後 HLR 對新的 SGSN 啟動追蹤，SGSN 再對新的 BSC 啟動追蹤。在 Nokia HLR 可以設定是否對本網之外的網路啟動追蹤，當在 Nokia HLR 啟動本網用戶追蹤時，也可以定義是否要對 BSC 啟動追蹤。而漫遊用戶及話機設備的追蹤方面，即使用戶或話機設備沒有在 SGSN 註冊，還是可以在 SGSN 中設定。話機設備追蹤必須在用戶追蹤前先啟動，所以假如在同一個 SGSN 已經啟動用戶追蹤，那麼就無法啟動話機設備追蹤。

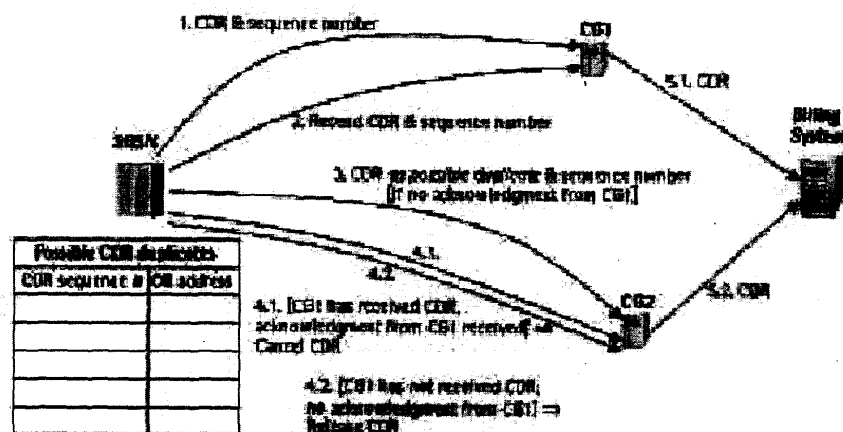
SGSN 可以藉著拒絕追蹤請求來限制同時啟動的追蹤數目。允許的追蹤數目最多 200 個，如果使用的追蹤量達到此數目時，SGSN 就不再啟動任何新的追蹤了。

1.6 計費資料產生最佳化

在 Release 2 中，對於計費資料的產生有一些不同的地方，尤其是 SGSN 產生的計費資料。其主要的目的是在減輕 IP 骨幹網路的負荷以及 BMS 的儲存空間。

1.6.1 防止重複產生 CDR

在 Release 2 中，GSN(含 SGSN 及 GGSN)以及 CG 必須負責防止傳送重複的 CDR 到 BMS。在 Release 2 之前，要防止這類情形發生只能靠 BMS 本身來防範。



Optimization of CDR Generation

透過 Data-Record-Transfer-Request 的 GTP 訊息，SGSN 傳送計費資料資訊及序號資訊給 CG。假如 CG 在預設的等待時間內沒有回應的話，SGSN 會嘗試送第二次，如果 CG 仍然沒有回應，那麼 SGSN 會將資料送至其他的 CG。當發生這種情況時，SGSN 並無法確定第一個 CG 是否有收到資料。可能的原因是第一個 CG 確實有收到計費資料，而且已經儲存成功，但是在送出回應給 SGSN 之前，CG 就已發生故障。還有可能的原因是，CG 送出的回應訊息已經遺失了或是 CG 根本沒有收到計費資料。為了確保 BMS 不會收到從不同的兩個 CG 送來重複的計費資料，在 SGSN 必須以下列方式來運作：

- SGSN 傳送 CDR 到第二個 CG，這 CDR 有可能是重複的 CDR。
- SGS 儲存可能是重複 CDR 的序號，以及傳送重複 CDR 的 CG 的 IP 位址。
- SGSN 會一直等待，直到故障的 CG 重新運作時，SGSN 會對此 CG 進行測試，以確認此 CG 之前是否有成功收到 CDR。
- 如果第一個 CG 有收到 CDR 的話，SGSN 會要求第二個 CG 刪除之前收到的那筆重複 CDR。
- 如果第一個 CG 確實沒有收到 CDR，則 SGSN 會通知第二個 CG 可以將那筆可能重複的 CDR 解除禁令。

但也有可能第一個故障的 CG 在經過很長的時間之後，仍然無法恢復正常運作。所以在 SGSN 必須定義一個最大時間的參數值，它是用來讓 SGSN 等待 CG 恢復正常運作。當等待時間超過時，SGSN 會根據新的參數來運作：SGSN 可能要求第二個 CG 刪除 CDR 或是解除禁令。如果刪除的話，可以確定決不會有重複的 CDR 送到 BMS；如果是解除禁令，則可以確定不會有任何 CDR 遺失。上面提到新的參數值可以透過 MML 指令來設定。

1.6.2 S-CDR 的產生

S-CDR 產生的機制也有做一些改變。一個新的參數稱為最少資料臨界值 (Minimum Data Threshold)。如果沒有達到此臨界值，CDR 是不會產生的。當超過指定的時間週期後，這時應該會產生另一筆新的 CDR，此時會再一次確認臨界值。如果仍然沒有超過此臨界值，CDR 仍然不會產生。如果這種情況持續好幾天，那麼必須尋求一個方式來強制產生 CDR。所以有另一個參數稱為 S-CDR 最大時間值 (Maximum S-CDR Duration)。如果超過此時間值，不管檔案中的資料有多少，都會產生 S-CDR。這兩個參數都可以透過 MML 指令來設定，而且對 M-CDR 及 SMS-CDR 檔案不會有任何的影響。

1.7 預付卡服務

預付卡是一種行動電話費用的付款方式，客戶可以預先將一筆錢存入預付卡帳號，再直接由此帳戶扣款來支付通信費用。許多國家的電信業者在電路交換的電話服務上推出預付卡後，都相當的成功。所以對嶄新的 IP 行動服務來說，預

付卡用戶是極待開發的一個市場。

在 GPRS System Release 1 中，Nokia 已支援 WAP over GPRS 的預付卡服務。在 Release 2，對本網用戶而言，預付卡已經擴展到支援所有的 GPRS 服務。達成的方法有兩種：IN-based 及 CDR-based 計費。兩者的差別可以參考以下表一的說明：

IN based prepaid	CDR based prepaid (Server based prepaid)
Excellent real time capabilities	(Delay of few minutes)
(Only access based charging: volume and/or time)	Both access and content based charging
Roaming possible with CAMEL architecture (Customised Applications for Mobile networks Enhanced Logic)	Works only in the home network.
Prepaid account in the Service Control Point (SCP)	Prepaid account in the Prepaid Server or in other Account Management System
Subscription Information in the HLR: GPRS-CSI, SMS-CSI	Subscription Information in the HLR: Charging Characteristics
Postpaid CDRs are generated but not used for charging	Specially marked CDRs are used for charging (prepaid CDRs)
Will be enhanced in the future.	Will be enhanced in the future.

Table 1: IN based prepaid and CDR based prepaid

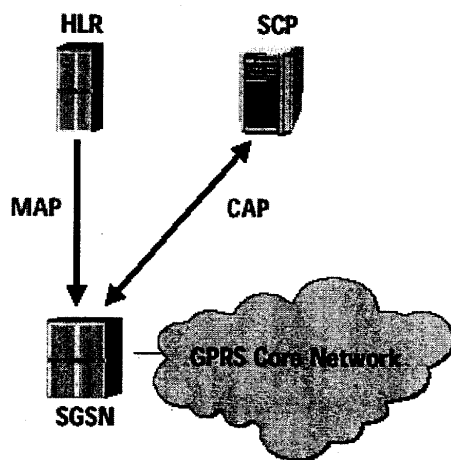
CDR-based 預付卡服務是現今可以針對內容來計費的唯一解決方案。另一方面，IN-based 預付卡服務則可提供較優異的即時處理能力。注意這兩種解決方案不是互相排斥，而是彼此有互補作用的。

1.7.1 IN-based 預付卡服務

IN-based 預付卡系統是唯一提供真正即時預付卡上網計費的解決方案。手機發出的簡訊以及 GPRS 資料量都可以即時計費。用戶所申請服務的資訊都存放在

HLR，而用戶請求以及協商後的 QOS 屬性會送至 SCP。SCP 不會影響 QOS 的水準，但是可以利用 QOS 的資訊來計費。IN 服務以及用戶的預付卡帳號都存放在 SCP，而 SCP 有權允許用戶發送簡訊或啟動 PDP Context。在允許用戶使用之前，SCP 會先檢查用戶預付卡帳號中的餘額。

針對支援 IN-based 預付卡服務，SGSN 是以 CAMEL phase 3 規格為基礎。SGSN 和 SCP 之間的介面以 CAP(Camel Application Protocol) 為基礎，而 SGSN 和 HLR 之間的介面則符合 3GPP MAP 的規範。所以整個系統可以很容易地升級到擁有完整的 CAMEL 3 功能。而 GGSN 並沒有連接到 IN 系統的介面。



IN Based Prepaid

如果由手機端啟動 PDP Context，根據 HLR 所給的資料，SGSN 會詢問 SCP，而 SCP 回覆 SGSN 是否可以繼續啟動此 PDP Context，也就是說，用戶的帳號中是否還留有餘額。如果還有餘額，則 SGSN 會獲得允許繼續啟動 PDP Context。而當 PDP Context 在 GGSN 啟動成功時，SGSN 會告知 SCP，此時 SCP 會允許用戶開始送收資料。當超過設定值(時間或傳輸資料量)時，SGSN 會再一次詢問 SCP，用戶的帳戶中是否還有餘額可以繼續送收資料。如果還有餘額的話，則重複上面的過程；如果沒有，則 SCP 會要求撤銷 PDP Context。

在手機送出簡訊時，SGSN 會詢問 SCP 是否可以送出簡訊。同樣的，如果餘額足夠，SCP 會允許送出簡訊；如果餘額不夠，就會拒絕送出簡訊。如果 SGSN 獲

得允許送出簡訊，它會將簡訊傳送的結果告知 SCP。如果傳送成功的話，SCP 會更新用戶帳戶餘額。

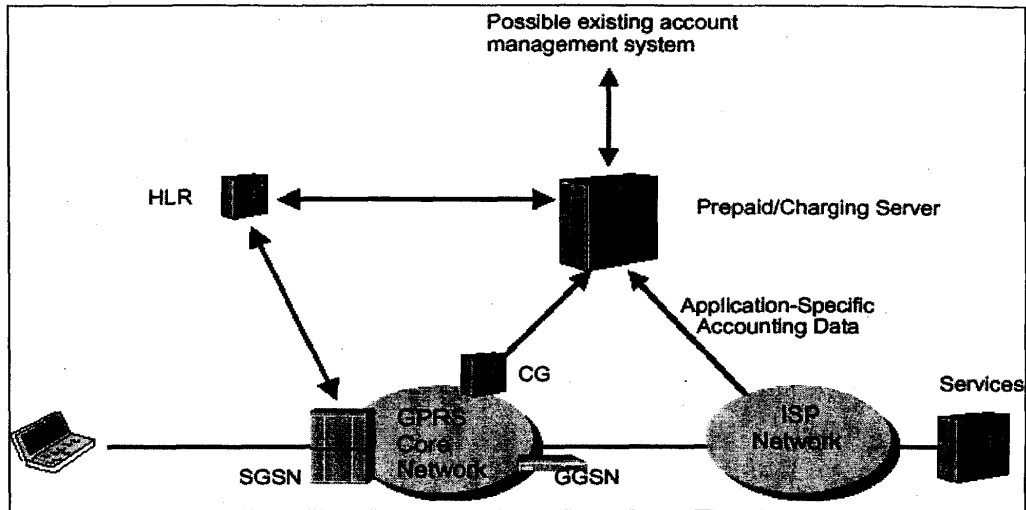
1.7.2 Server-based 預付卡服務

HLR 用戶資料的計費特性(Charging Characteristic)及用戶的 PDP Context 資料會顯示用戶是否為預付卡用戶。當手機執行 GPRS Attach、Inter-SGSN Routing Area Update 以及 HLR 的用戶資料有更動時，HLR 會將此資訊告知 SGSN。而啟動 PDP Context 後，SGSN 會將此資訊轉送給 GGSN。此機制是遵循 3G TS 23.060、3G TS 29.002 及 3G TS 29.060 等標準。

SGSN 和 GGSN 產生的 CDR 會經由 CG 送至預付卡伺服器(Prepaid Server)。預付卡伺服器也可以接收特定應用的計費資料，例如 NAWG(Nokia Artuse WAP Gateway)的計費資料。以下列出可供計費的項目：

- WAP 服務內容
- 傳輸資料量
- PDP Context 時間
- 進接點(APN)
- QOS 參數

預付卡伺服器會根據計費資料的內容來進行扣款，而當無任何餘額時，則透過 HLR 結束用戶 GPRS 服務。之後 SGSN 和 HLR 會拒絕用戶執行 GPRS 註冊，直到用戶帳戶再補充餘額為止。另外有預付卡餘額告知系統可以用來通知用戶預付卡帳戶的餘額狀況，以及隨時讓用戶補充預付卡帳戶的餘額。



Server Based GPRS Prepaid

預付卡計費資料和一般後付型(postpaid)計費資料主要不一樣的地方在於預付卡計費資料可以設定不同的臨界值，所以會產生較多的計費資料。在記費資訊(Charging Info)欄位值，也就是HLR用戶資料中的的計費特性，會指出此筆記費資料是屬於預付卡型或是一般後付型的計費資料。

1.7.2.1 SGSN 特有的 Server-based Prepaid 功能

對預付卡行客戶來說，SGSN 擁有近乎即時的計費資料處理及計費資料產生的能力。也就是說，業者可以自訂預付卡客戶產生計費資料的臨界值，而且可以很快將計費資料送至CG。

如果預付卡帳戶已無任何餘額時，HLR 將要求 SGSN 強制將用戶退出 GPRS 網路，而且拒絕之後的註冊要求；或者 HLR 會要求 SGSN 撤銷 PDP Context 並且拒絕任何 PDP Context 的啟動要求。當使用第二個方法時，用戶仍可繼續接收簡訊。

SGSN 可以針對 CDR-Based 預付卡用戶產生預付卡的 S-CDR、M-CDR、SMO-CDR 以及 SMT-CDR。在 SGSN 可以使用 MML 指令來啟動或抑制這類型的計費資料產生。在 SGSN，每個用戶最快每分鐘產生一筆 CDR。

1.7.2.2 GGSN 特有的 Server-based Prepaid 功能

Nokia GGSN Rel 2 支援 Server-based 預付卡計費功能。GGSN 能區分出哪些用戶是預付卡用戶，並且以更快的速度產生計費資料。當啟動 PDP Context 時，在計費特性(Charging Characteristic)這個欄位已經註明此用戶為預付卡用戶，而且 SGSN 會將 HLR 的用戶資料傳送至 GGSN，所以用戶資料也保存在 GGSN 的 PDP Context Table。不管是 SGSN 或是 GGSN 都不知道費率或是用戶的預付卡帳戶的餘額，所以 GGSN 會將預付卡 G-CDR 送至 CG，而 CG 也會立刻轉送至預付卡伺服器。如果用戶使用超出餘額的可使用量，連線將會因餘額用盡而停止，而預付卡伺服器也會從 HLR 將用戶 Disable。維運人員可以透過 GGSN 的瀏覽器使用者介面設定預付卡計費資料的產生機制。當超過設定的臨界值時，預付卡計費資料就會送到 CG。如果關閉預付卡功能，則預付卡用戶就和一般用戶完全一樣了。

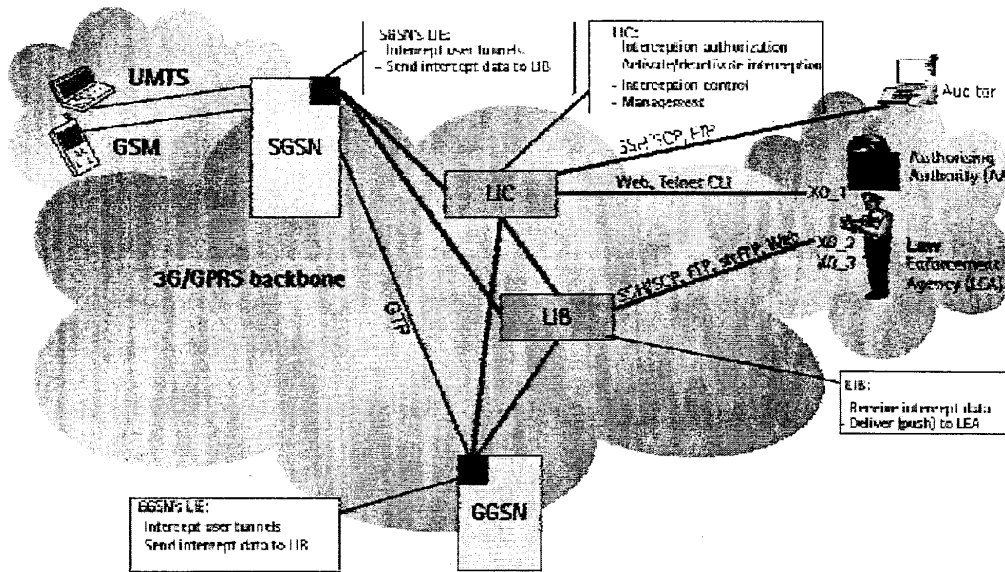
1.8 強化監聽功能

LIG(Lawful Interception Gateway)對於 GPRS 或是 UMTS 網路都是必要的網路元件，它提供調查人員合法監聽 2G 和 3G 行動電話的資料。它監聽的方式和傳統 GSM 的語音監聽方式已經完全不同。GSM 監聽主要是通話錄音，而 2G 及 3G 則是截聽行動電話和進接點之間送收的資料。多數國家的電信業者在 2G 和 3G 系統正式商業化運轉前，都必須符合有關當局的要求，而所有的歐盟國家都遵守這項規定。Nokia 的 LIG 和 GGSN 一樣都是以工業標準平台為基礎的系統，所以它提供電信業者建構 2G 和 3G 的電信監聽系統。

1.8.1 LIG 架構

LIG 的架構如下圖所示，它包含了以下主要的功能元件：監聽控制器(Lawful Interception Controller, LIC)、監聽瀏覽器(Lawful Interception Browser, LIB)以及監聽延展單元(Lawful Interception Extension, LIE)。監聽控制器是以 Nokia LC2500/3500 路由器產品為基礎，它主要是控制整個監聽期間以及提供調查局人員及檢察機構一個含 SSL(Secure Socket Layer)安全機制的瀏覽器介面。檢察機構透過此瀏覽器介面授權調查局監聽可能涉及刑案的行動電話用戶，而調查局人員也透過此瀏覽器介面來啟動或停止合法授權的監聽行動。可設定的

參數有 IMSI、IMEI 或 MSISDN。



Main functions and interfaces of LIG network elements

LIC 也包含了指令介面(Command Line Interface, CLI)，它在 LIC 及 GSM 網路的監聽管理系統(Lawful Interception Management System, LIMS)之間提供指令輸入的介面。而採用的是標準的 Telnet 連線。

LIB 和 LIC 一樣採用相同的 Nokia 路由器設備。這個網路元件會暫時儲存監聽相關資訊(Interception Related Information, IRI)以及通訊內容(Communication Content, CC)，之後再傳送到指定的調查局人員。傳送的方式有 FTP、SSH/SCP 或是 strFTP(Streaming FTP)等通訊協定。監聽相關資料也可以由遠端透過以 WEB 為基礎的 LEA 介面來瀏覽。Nokia 更可以依據不同國家提出的要求，將監聽相關資訊及通訊內容轉換成要求的格式版本，再傳送至監聽單位。

GGSN 中的 LIE 是以 GGSN Release 1.3 或更新的軟體版本為基礎。它是包含在 GGSN 設備產品中，不能單獨銷售。它主要是負責收集部分的 IRI 資料及 CC 資料，也就是用戶送收的資料。它也提供到 LIB 及 LIC 的 IP 連線。

2G-SGSN 中的 LIE 是以 SGSN Release 2.0 或更新的軟體版本為基礎。它也是包含在 SGSN 的產品中，無法單獨銷售。它主要是收集用戶的 IRI 及 CC 監聽資料。它也收集簡訊及用戶的位置資訊，精確度可達 CGI(Cell Global Identification)

等級。它也提供到 LIB 及 LIC 的 IP 連線。

1.8.2 新增加的一般功能

對 SGSN 監聽功能來說，提供了漫遊用戶監聽以及容量方面的改善。

1.8.3 LIC 元件新功能

LIC 新增加的功能有以下幾項：

- IMEI 監聽
- IRI 及 CC 資料可以設定不同的目的 IP 位址
- 自動啟動或停止監聽行動

1.8.4 LIB 元件新功能

LIB 新增加的功能有以下幾項：

- 位置及簡訊資料處理
- 可自訂格式的 LIB 資料以 strFTP 方式來傳送

strFTP 是一種以標準 FTP 為基礎的近乎即時的傳輸方式。當資料在 LIB 準備好時，就會馬上轉送到 LEA。strFTP 通訊協定允許將 IRI 及 CC 資料傳送到不同的目的地。

1.9. 支援 GEA2(GPRS Encryption Algorithm)

GPRS System Release 2 支援新的 GPRS 加密演算法 GEA2。GEA2 是屬於 3GPP R' 99 規格的一部份。它是使用在行動電話及 SGSN 之間的一種加密演算法，所以 SGSN 可以藉 GEA2 限制不支援加密的行動電話進接到 GPRS 網路來。在 SGSN 中，PAPU 的 IOCP-A 單元就是用來支援加密演算的硬體配備。它會產生加密演算所需的亂數值，然後再和從 AuC/HLR 所收到的加密金鑰(ciphering key, Kc)來執行加密演算。

第二章

GPRS Intranet Access Service

2.1 GPRS VPN 概述

虛擬私有網路 (Virtual Private Network; VPN) 就是在路由器內加入加密以及 tunneling 的功能，以軟體的技術將某些固定節點 grouping 起來，在網路上構築出一個虛擬的企業網路，例如 GPRS VPN 及國際網路 VPN 即是以 IP 網路為基礎的 VPN 技術或是服務。

以往企業用戶員工如果要在公司以外之地點存取企業內部網路資料進行商業之行為，除了安全顧慮等因素之外，主要之問題是不易尋找到能提供上網服務之地點。然而隨著商業模式的改變及行動用戶的增加，此問題已日益突顯，如何提供企業用戶能隨時隨地上網，已是刻不容緩之課題。GPRS VPN 的出現主要就是為了解決這個問題，企業只要向服務業者購買 GPRS VPN 服務，就可以隨時隨地透過無線上網方式存取公司內部資料、收發電子郵件、上傳下載檔案或進行其他之商業行為。

GPRS VPN 是架構於 GPRS 服務上的行動數據 VPN，其主要的服務訴求是在公眾 GSM 網路中提供具備保密性與可移動性之虛擬企業網路環境。為因應此服務之需求，GPRS VPN 須具備下述之基本功能：

- 傳輸資料之保密性。
- 須能對企業網路接取之使用者進行認證，並分配屬於企業網路之 IP Address 予通過認證的使用者。
- 需提供函蓋範圍廣範之行動無線接取環境。

2.2 GPRS VPN 架構中相關 Tunneling 技術概論

圖 2-1 所示為 GPRS VPN 架構之範例，由圖中可看到 GPRS 網路端與企業網路端之間建立了 GRE 及 IPSec tunnel，以下我們分別說明其必要性及功能。

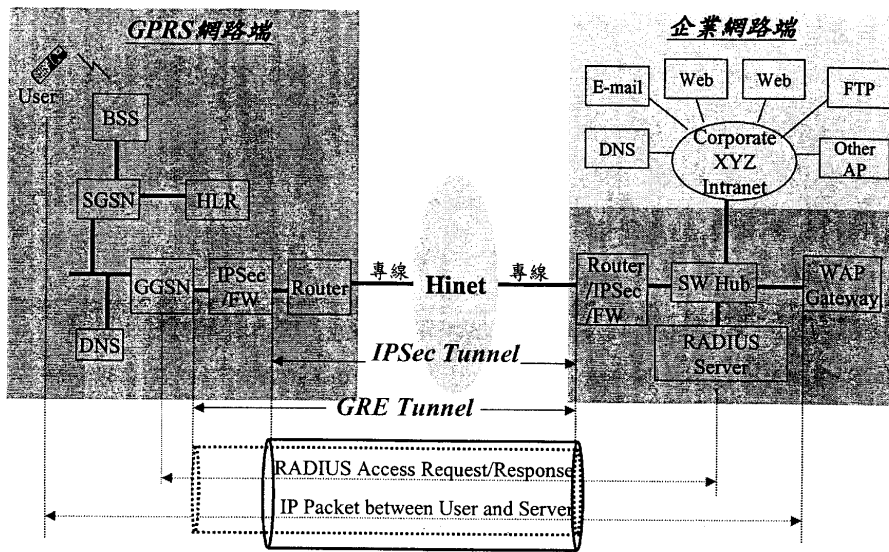


圖 2-1 GPRS VPN 架構之範例

1. GRE Tunnel :

在 GPRS VPN 的服務中，由於企業在其企業網路內使用 Private IP Address 並指派 Private IP Address 給予無線接取者。而使用 Private IP Address 可能面對之問題包括如何透過 Public Internet 傳送 IP 封包以及如何解決位址空間重疊之問題，因此 GPRS 網路採取了適當的 Tunneling 機制解決上述問題，此機制即所謂的 GRE Tunnel。

GRE Tunnel 之建立是基於 Routing 之考量。由於一個 GGSN 通常可以連接數個企業網路且於企業網路內部普遍使用 Private IP Address，其位址空間極可能彼此重疊或部份重疊，甚至於與 GPRS 網路元件使用之 Private IP Address 相同，使得 GGSN 無法依據 IP 封包 Header 中之 Destination IP Address 作出正確的 Routing。為了解決上述問題，我們可以將 GGSN 分割為數個 Virtual Router，每一個 Virtual Router 專屬於一個企業網路及其無線接取子網路；每一個企業網路與其無線接取子網路間傳遞之 IP 封包完全透過其專屬之 Virtual Router；兩個 Virtual Router 之間沒有路徑存在。由於 Virtual Router 之使用，因此不同之企業網路（及其無線接取子網路）間在邏輯上是完全隔絕的，因此企業網路及其無線接取子網路要使用什麼位址空間，完全由企業網路管理者自己決定，與其它企業重疊亦無所謂。

2. IPSec Tunnel :

IPSec (Internet Protocol Security 網際網路安全性協定)是一個工業標準網路安全協定。IP 網路通信提供透明的安全服務，保護 TCP/IP 通信免遭竊聽和篡改，可以有效抵禦網路攻擊，同時保持易用性。

IPSec 有兩個基本目標：

- (1) 保護 IP 資料包安全；
- (2) 抵禦網路攻擊提供防護措施。

IPSec 結合密碼保護服務、安全協定組和動態密鑰管理三者來實現上述兩個目標，不僅能使企業區域網路與撥號用戶、域、網站、遠端站點以及 Extranet 之間的通信提供強有力且靈活的保護，而且還能用來篩選特定資料流程。

IPSec 提供了兩種安全機制：認證和加密。證機制使 IP 通信的資料接收方能夠確認資料發送方的真實身份以及資料在傳輸過程中是否遭篡改加密機制通過對資料進行編碼來保證資料的機密性，以防資料在傳輸過程中被竊聽。

IPSec 協定組包含

- (1) 網路認證協定 Authentication Header (AH)
- (2) 封裝安全載荷協定 Encapsulating Security Payload (ESP)
- (3) 密鑰管理協定 Internet Key Exchange (IKE)
- (4) 以及用於網路認證及加密的一些演算法等。

其中 AH 協定定義了認證的應用方法，提供資料源認證和完整性保證；ESP 協定定義了加密和可選認證的應用方法，提供可靠性保證。在實際進行 IP 通信時，可以根據實際安全需求同時使用這兩種協定或選擇使用其中的一種。AH 和 ESP 都可以提供認證服務，不過，AH 提供的認證服務要強於 ESP。IKE 用於密鑰交換（將在以後部分討論）。IPSec 規定了如何在對等層之間選擇安全協定、確定安全演算法和密鑰交換，向上提供了訪問控制、資料源認證、資料加密等網路安全服務。

2.3 GPRS VPN 網路架構 without Virtual Router(VR)

GPRS VPN 可提供企業用戶透過專線、E1/Frame Relay、ADSL 以及 Internet 的方式與 GPRS 核心網路做界接，此多元的界接方式讓企業用戶能更彈性地依自己的需求做最有效的投資和應用。

以下是 GPRS VPN 各種界接方式之網路架構圖：

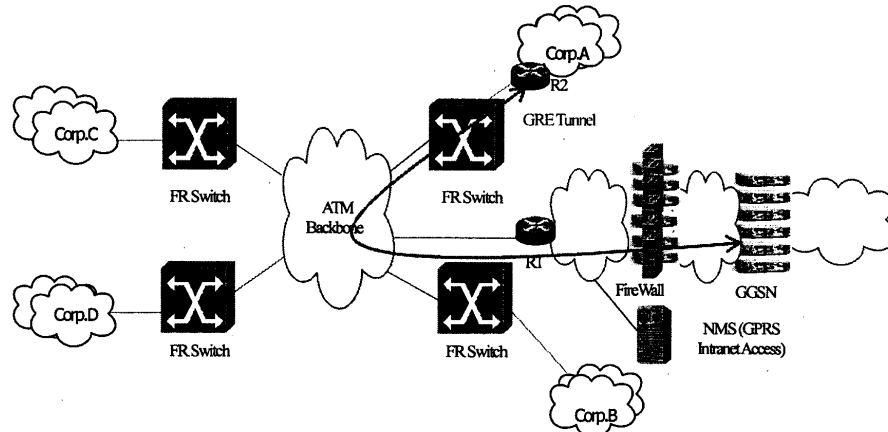


圖 2-2 GPRS VPN 透過 E1/Frame Relay 架構

本 GPRS VPN 架構（如圖 2-2）係提供企業用戶透過 E1/Frame Relay 之專線方式界接至 GPRS 核心網路，提供用戶穩定安全的傳輸品質。

本架構需建 GRE Tunnel，此 Tunnel 需由 GGSN 建至企業用戶端如 Corp A. 的 Router R2，以解決 Private IP 之 Routing 問題。

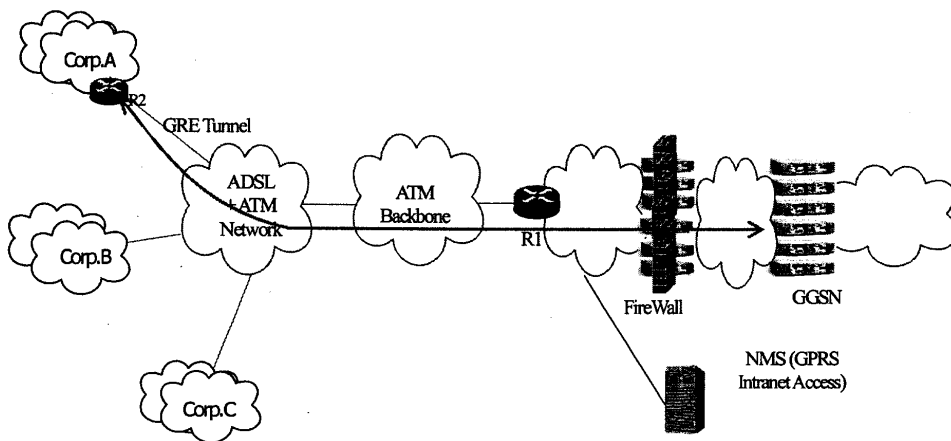


圖 2-3 GPRS VPN 透過 ADSL 架構

本 GPRS VPN 架構 (如圖 2-3) 係提供企業用戶透過 ADSL 之專線方式界接至 GPRS 核心網路, 提供用戶穩定安全的傳輸品質。

本架構需建 GRE Tunnel, 此 Tunnel 亦需由 GGSN 建至企業用戶端如 Corp A. 的 Router R2, 以解決 Private IP 之 Routing 問題。

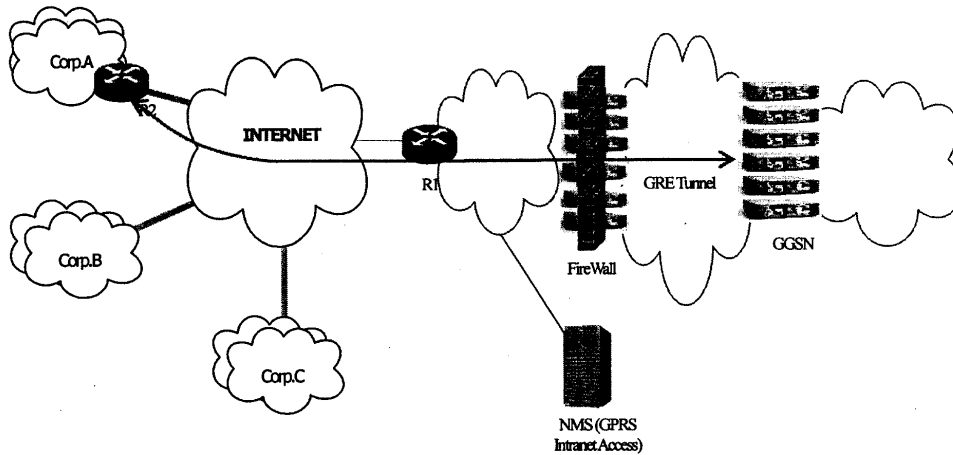


圖 2-4 GPRS VPN 透過 VPN/Internet 架構

本 GPRS VPN 架構 (如圖 2-4) 係提供企業用戶透過 Internet 之方式界接至 GPRS 核心網路, 提供用戶便利多元之界接方式。

本架構需建 GRE Tunnel, 此 Tunnel 亦需由 GGSN 建至企業用戶端如 Corp A. 的 Router R2, 以解決 Private IP 之 Routing 問題, 另由於此方案係於公眾網路上傳收資料, 因此需考量資料保密的問題, 如可使用 IPsec 等加密技術。

上述各種界接方式均需由業者之 GGSN 設備建 GRE Tunnel 至企業用戶端之設備, 若企業用戶端之設備不支援建立 GRE Tunnel 之功能, 將無法提供此類用戶 GPRS VPN 之服務, 此問題將於下節中提出一有效之解決方案。

2.4 GPRS VPN 網路架構 with Virtual Router(VR)

由於企業用戶端的 Router 未必支援 GRE Tunnel 建立之功能, 因此為解決

此問題, 提供企業用戶更彈性之介接方式, 可考慮於提供 GPRS VPN 服務業者之設備端引入具 Virtual Router 功能之設備來解決此問題。

以下是 GPRS VPN 引入 Virtual Router 之各種界接方式之網路架構圖：

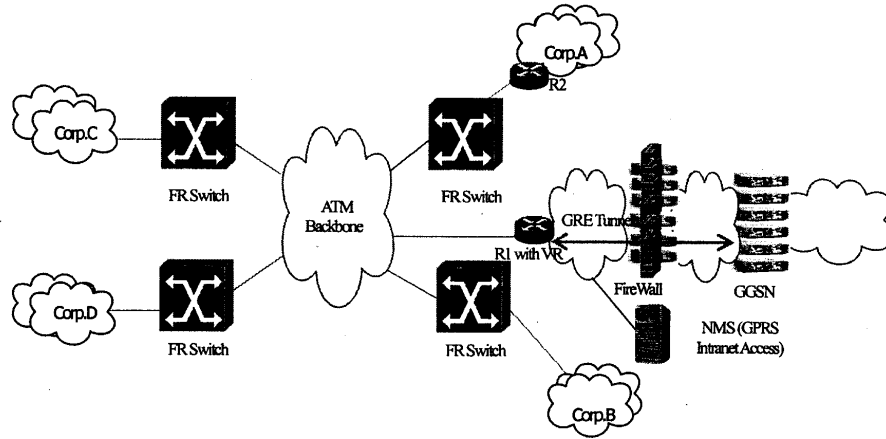


圖 2-5 GPRS VPN 透過 E1/Frame Relay 架構 with Virtual Router Function

本 GPRS VPN 架構 (如圖 2-5) 係提供企業用戶透過 E1/Frame Relay 之專線方式界接至 GPRS 核心網路, 由於在提供 GPRS VPN 服務之業者之設備端提供具備 Virtual Router 功能之 Router R1, 遂其 Tunnel 只需由 GGSN 建至 Router R1 即可, 不需建至 Corp. A 之 Router R2, 遂可解決企業用戶端設備無法支援 GRE Tunnel 建立之問題。

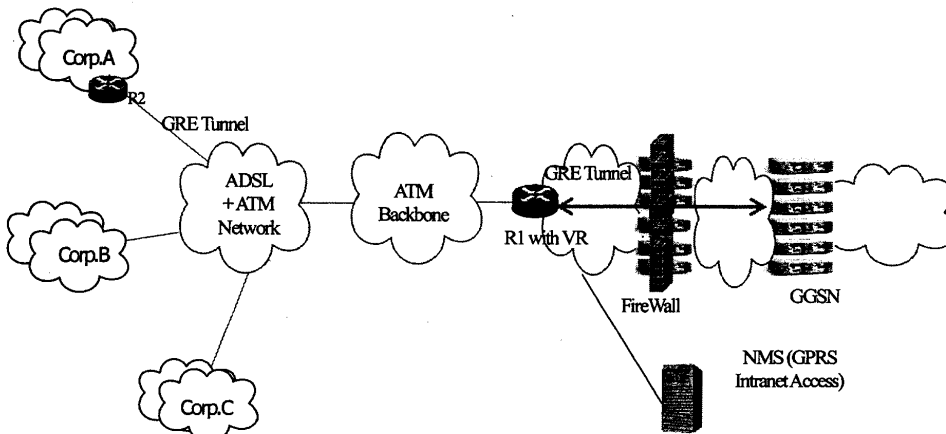


圖 2-6 GPRS VPN 透過 ADSL 架構 with Virtual Router Function

本 GPRS VPN 架構 (如圖 2-6) 係提供企業用戶透過 ADSL 之專線方式界接至 GPRS 核心網路，由於在提供 GPRS VPN 服務之業者的設備端提供具備 Virtual Router 功能之 Router R1，遂其 Tunnel 只需由 GGSN 建至 Router R1 即可，不需建至 Corp. A 之 Router R2，遂可解決企業用戶端設備無法支援 GRE Tunnel 建立之問題。

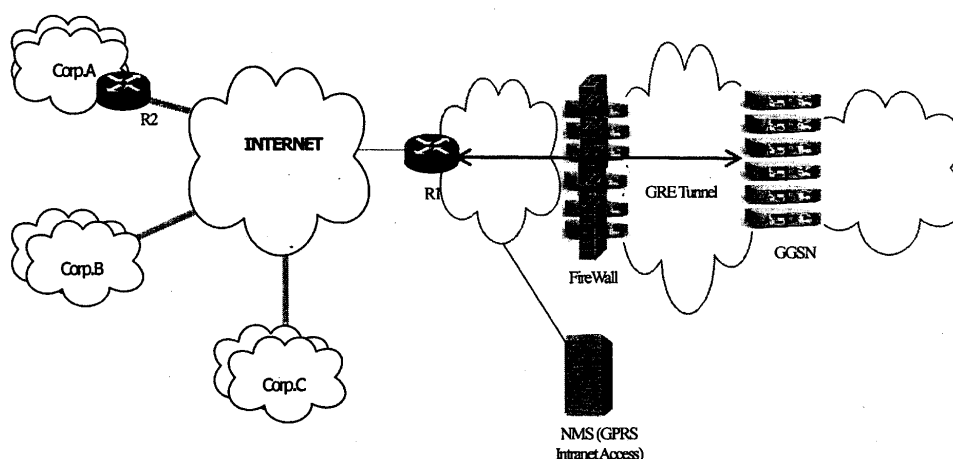


圖 2-7 GPRS VPN 透過 VPN/Internet 之架構 with Virtual Router Function

本 GPRS VPN 架構 (如圖 2-7) 係提供企業用戶透過 Internet 之方式界接至 GPRS 核心網路，由於在提供 GPRS VPN 服務之業者的設備端提供具備 Virtual Router 功能之 Router R1，遂其 Tunnel 只需由 GGSN 建至 Router R1 即可，不需建至 Corp. A 之 Router R2，遂可解決企業用戶端設備無法支援 GRE Tunnel 建立之問題。

本架構除需建 GRE Tunnel 外，在考量資料保密之議題，可使用 IPsec 等加密技術。

2.5 於 GPRS VPN 服務網路引進 Virtual Router 之優點

為解決企業用戶於申租 GPRS VPN 服務時，企業用戶端設備無法

支援 GRE Tunnel 之問題，遂於 GPRS VPN 服務網路引進 Virtual Router 之功能。

引進 Virtual Router 除了可以解決企業用戶端設備不支援 GRE Tunnel 功能外亦有許多優點，分述如下：

1. 提供客戶端局情設定之便利性：

若 GPRS VPN 服務網路未提供 Virtual Router，則 GRE Tunnel 需由 GGSN 建至企業用戶端之設備，企業用戶端需於其設備上配合 GRE Tunnel 相關參數局情之設定，常造成企業用戶之不便；若在提供 GPRS VPN 服務業者的設備端提供具 Virtual Router 功能，則 GRE Tunnel 只需由 GGSN 建至 Virtual Router 即可，所有相關 GRE Tunnel 之局情，均可由業者於其 GGSN 及 Virtual Router 設備上設定即可，企業用戶端之設備完全不需配合設定。

2. 提供維運、障礙處理之便利性：

由於 GRE Tunnel 相關局情均於提供 GPRS VPN 服務之業者端設備上設定即可，因此與企業用戶端關係較為單純，遂於平時之維運管理及障礙處理較為便利。

3. 快速供裝：

由於企業用戶端無需做 GRE Tunnel 相關局情之設定，遂可簡化供裝上之程序，提高工作上之效率。

第三章

GPRS Internet Access Service

3.1 GPRS Internet Access Service 概述

為配合前項 GPRS 企業網路接取服務，有效因應各種不同企業之需求，遂於 GPRS Core Network 建置一 GPRS Internet Access Service Network 提供用戶出至 Internet 之出口。

3.1.1 GPRS Internet Access Service 網路架構

GPRS Internet Access Service 可提供企業用戶透過專線、E1/Frame Relay、ADSL 的方式與 GPRS 核心網路做界接，此多元的界接方式讓企業用戶能更彈性地依自己的需求做最有效的投資和應用。

以下是 GPRS Internet Access Service 各種界接方式之網路架構圖：

1. GPRS Internet Access Service over E1/Frame Relay 網路架構：

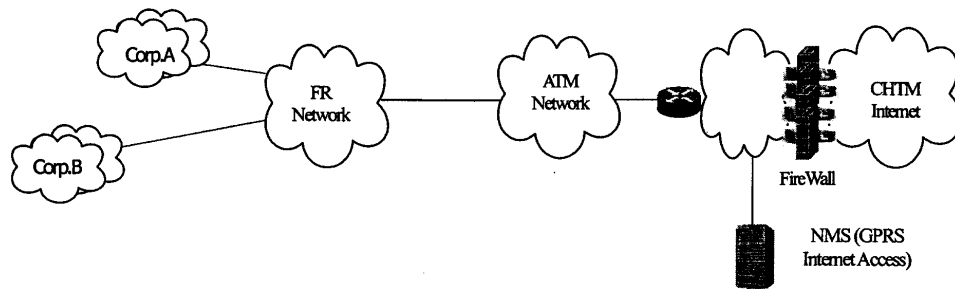


圖 3-1 GPRS Internet Access Service 透過 E1/Frame Relay 網路架構

本 GPRS Internet Access Network 架構（如圖 3-1）係提供企業用戶透過 E1/Frame Relay 之專線方式界接至 GPRS 核心網路，提供用戶可透過 GPRS Core Network 出至 Internet。

2. GPRS Internet Access Service over ADSL 網路架構：

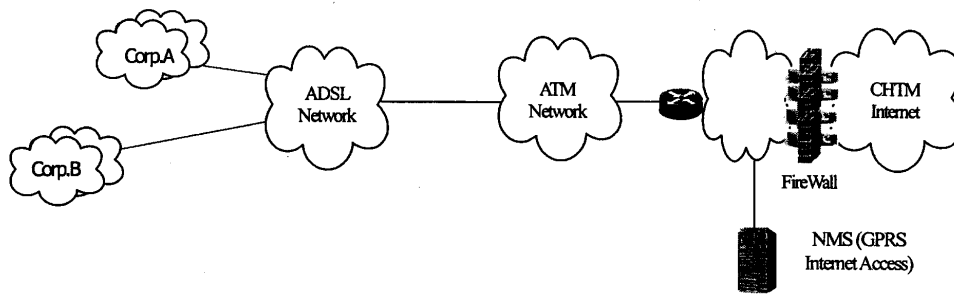


圖 3-2 GPRS Internet Access Service 透過 ADSL 網路架構

本 GPRS Internet Access Network 架構（如圖 3-2）係提供企業用戶透過 ADSL 之專線方式界接至 GPRS 核心網路，提供用戶可透過 GPRS Core Network 出至 Internet。

第四章

GPRS CDR 資料分析

4.1 GPRS CDR 資料分析及監視工具

4.1.1 Nokia GPRS Traffica 概述

Traffica 是一個分析及監視的工具，它提供可即時性監看網路話務的功能。Traffica 提供行動電話服務提供者（中華電信）即時監看終端用戶的方法。它並提供行動電話服務提供者排除網路障礙(Troubleshooting)功能，從監看用戶的每個 call attempt，簡訊傳送及 GPRS 每一個事件。

Traffica 提供可監看 GPRS 網路的功能。它允許行動電話服務提供者看即時監看 GPRS 網路問題的功能。它可從不同擷取名 Access Point Names 及成功 Attaches, Detaches 及 PDP context activations, modifications and deactivations 即時監看，並提供快速及容易 GTP 及 CDR 的系統狀態快速瀏覽。它並可幫助行動電話服務提供者即時尋找活動中的行動電話用戶。

4.1.2 GPRS Traffica 功能

SGSN (Serving GPRS Support Node) 管理經識別 (identifying) 並已登錄於 GPRS 網路及移動性管理的 GPRS 行動電話用戶。SGSN 並從 GPRS 行動電話用戶接收資料，且送資料至行動電話用戶。

SGSN 以四種報表型態送資料至 Traffica 即：SGSN RTT, SGSN PDP RTT, GTP Statistics 及 CDR Statistics，前兩種是即時性資料，後兩種報表型態則是每 15 分鐘傳送一次。

以下清單提供從 Traffica 擷取資料的幾個範例：

- Subscriber identity
- Mobile equipment identity
- Attaches & attach errors
- Detaches & detach errors
- Location information(LA, RA & Cell_Id)
- Routing area updates
- PDP context activation & PDP context activation errors
- PDP context deactivation & PDP context deactivation errors
- MO/MT SMS deliveries and delivery errors
- Access SMS deliveries and delivery errors
- Access Point Names

Traffica 讓行動電話服務提供者於 GPRS 線上 (online) 及離線 (offline) 資料監看及分析作業變成可能。

- 於線上 Traffica 方面, 資料於動態即時圖形中, 它能結合資料從不同 RTTs 欄位是可監看 (visualized)。圖形化可幫助行動電話服務提供者追蹤障礙, 例如 Attach 所引起的相關障礙或對不同 PDP context Deactivation down 到細胞層所引起的障礙。
- Traffica 允許行動電話服務提供者定義以異常基礎告警 (threshold based alarms) 的告警, 例如: 於任何 Routing areas 中告警可即時被觸發 (triggered) 當 Routing Area 更新失敗率超過五個百分比時。Traffica 告警可提供 NetAct 監視方面的應用。

圖 4-1 是說明 SGSN 從 GPRS 行動電話用戶接收資料, 及傳送資料至行動電話用戶的過程。SGSN 以 SGSN RTT, SGSN PDP RTT, GTP 及 CDR Statistic 資料型態傳送至 Traffica 流程架構。

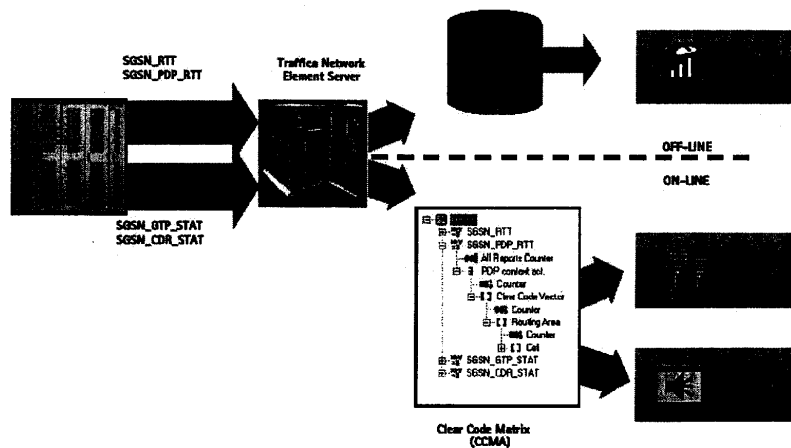


圖 4-1 Nokia GPRS Traffica

GPRS 的 Traffica 架構圖接收資料是存於嵌入式資料庫(embedded database) 用來提供資料分析用。Traffica 資料庫將 GPRS 事件及簡訊傳送以紀錄(record) 方式儲存。Traffic News 功能提供使用者於資料庫查詢擷取該筆紀錄的功能。Traffic News 允許多功能(versatile) 資料查詢, 以方便多方面的追蹤, 例如 PDP Context Activation 問題發生於 Location Area, 甚至尋找用戶位置, 用戶群及 GPRS 行動電話用戶設備。

1. 明碼矩陣 (Clear code Matrix)

CCMA(Clear Code Matrix)是一個號碼樹(counter tree)。它的功能是提供即時資料的儲存, 它提供即時圖形及告警。並附加提供可預先定義 CCMA, 它能製作屬於自己的 CCMA。

使用者它能控制以用戶所設公式定義收集資料送到 CCMA 及定義任意解析 over data。例如, 時間可是一秒, 一分鐘或一天。確認資料可能是出現於一分鐘, 從一天開始或一天結束, 例如一天有多少呼叫於網路元件中產生。

CCMA 樹的三種有成員型態, 它的架構如下:

- Time 等級是於根項目 CCMA 樹下, Time 等級 icons 以黃色顯示。
- 有四種節(node)型態: Expression, Group, Presence, and Vector。節成員 icons 以藍色顯示。
- 另有三個葉成員型態: Addition, Counter, and Move。葉子成員是實際資料儲存在 CCMA 及 icons 以紅色顯示。

2. 即時可看圖形 (Visualising with Real time Graphs)

於 CCMA 可收集即時可監看的圖形資料。Nokia 提供一個可展延選擇可預先定義即時圖形。一個能容易即時看內容從 Nokia 預先定義圖形中。這些 Nokia 圖形不能改變, 但它能利用它們圖形本身的基礎。它能定義它自己想要的圖形。使用者能依時間事先定義想蒐集資料。利用 Nokia 圖形並裁剪成業務上所需要

Noika GPRS traffica 一個可事先定義的即時圖形從延伸的選擇中, 說明如下:

- Attaches *et* attach errors
- Detaches *et* detach errors
- Routing area updates *et* errors
- PDP context activation *et* errors

- PDP context deactivation & errors
- MO/MT SMS & errors
- Used Mobile Types

甚至，圖形可以不同時間類型和圖形鏈結提供。

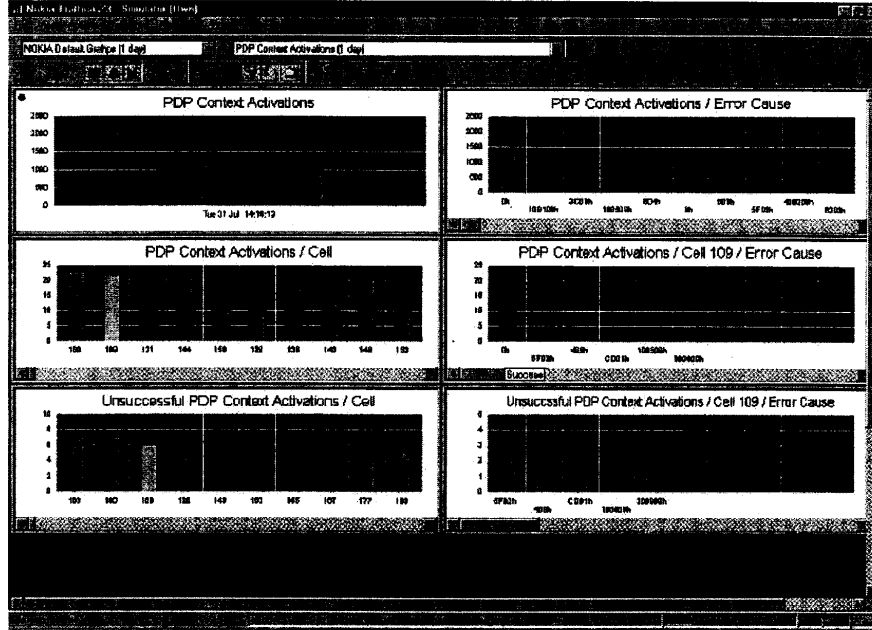


圖 4-2 可即時監看並具圖形的 Nokia GPRS Traffica

3. 監控 Traffica 告警 (Monitoring with Traffica Alarms)

Traffica 它提供自己定義告警的功能。它有三種不同型態的告警：Limit alarms, Delta threshold alarms 及 Burst alarms。另外有一些用戶可預先定義的內部 (internal) 告警。

- Limit，例如：呼叫數超出一天限定的量。
- Growth，例如：任何時間發生超出使用者定義任何 PDP 單元失敗 PDP context sessions 超出 20%。
- Burst SMS 簡訊失敗率超出 20%於 3 成功的時段。

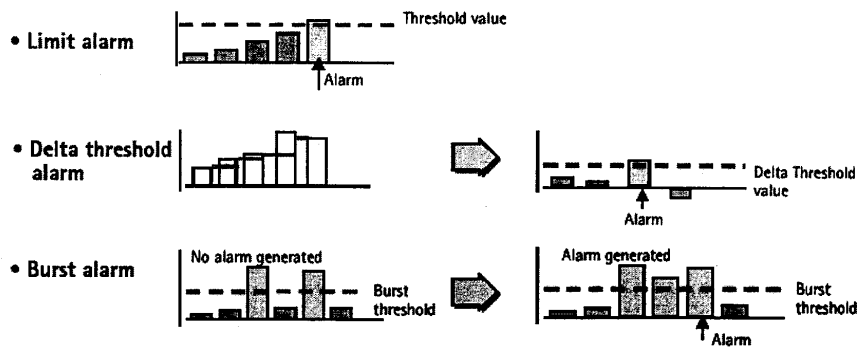


圖 4-3 可定義告警於 Nokia GPRS traffica

告警能從 TNES 送到 TS，甚至送到 NetAct 監視器。當任何人想要送告警至 NetAct 監視器。告警代號範圍從 34000 至 34499，請確認不同告警號碼對應不同告警。總之，嚴謹 (severity) 層的資訊，它不傳送至 NetAct 監視器。

Nokia GPRS traffica 提供以下告警：

- Traffica 告警送至 NetAct 監視器之應用。
- Traffica 內部告警。
- 三個不同使用者可定義之告警型態。

4.1.3 網路結構及摘要

Traffica 構成中華電信網路元件伺服器組成 Traffica Network Element Servers(TNES)對每一 SGSN release 2 對四個 GPRS 機房即一個 Traffica Server(TS)放置於 OMC 機房。

Traffica 對 GPRS TNES 透過 SGSN 收集即時資料，並以即時動態圖形及告警方式，提供資料庫每一筆詳細紀錄。

TNES 總是以可接受格式連接至一個網路元件。Traffica Server(TS)能連接銀幕即時圖形至網路拓璞，以利網路 Traffica 管理。它提供大筆資料查詢從 Traffic News client 進入資料庫。

Traffica 對 GPRS 資料能利用 NetAct Reporter 整合進行後端處理。Traffica 對 GPRS 資料而且能輸出至任何外部系統利用 Traffica Database Export 的選擇性輸出功能。

有三種主要功能於 Traffica Z3.1 它能幫助產生報表，從資料庫每一 TNES。

使用者可設定複雜條件去查詢資料庫從資料接取動作中。

圖 4-4 是說明 Traffica 透過 SGSN 收集即時資料作業情形。

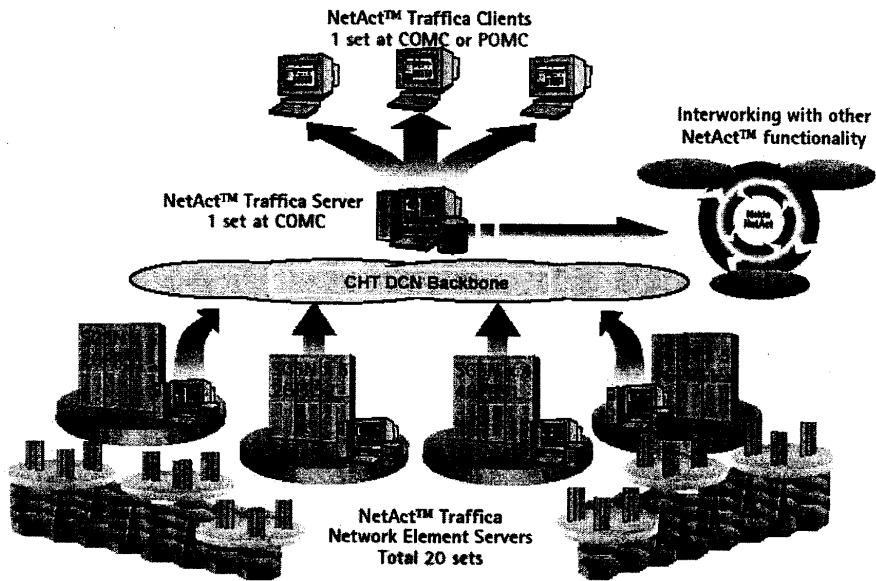
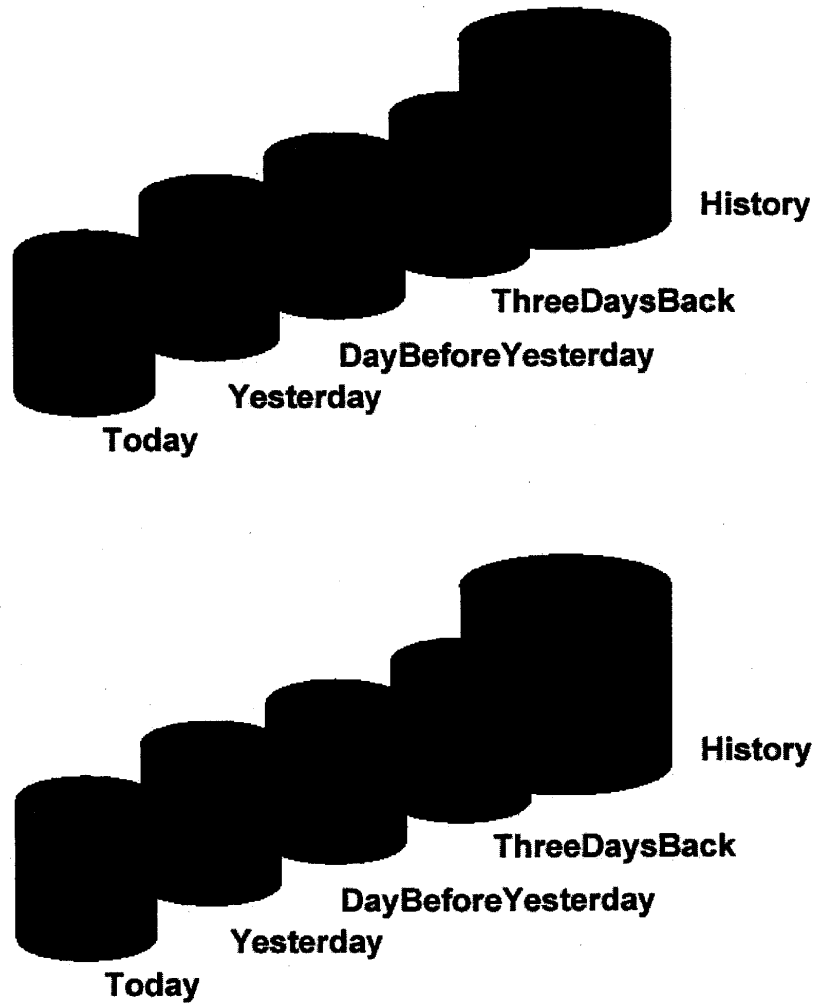


圖 4-4 Nokia Traffica 於中華電信 GPRS 系統之架構圖

以上網路架構介面連接是以 UDP/IP 為基礎。Traffica 網路元件伺服器是以 Solid 資料庫為基礎，每一資料庫檔案是以 24 小時方式儲存資料。新資料庫檔產生於每天晚上，舊的資料庫可至歷史資料庫中存取。

圖 4-5 是說明 Traffica Network Element Server 架構



Traffica 伺服器在 Traffica Architecture 它是負責即時圖形、告警及資料庫查詢伺服器。它而且執行管理工作例如 CCMA，圖形及告警定義及中央使用者管理。TS 可整合 Traffica fault 管理。

TNES 及 TS 架構如下：

Compaq ProLiant ML530

- Windows2000
- 2×Intel Pentium III Xeon GHZ

- 2048 MB RAM
- 12x36 GB Wide Ultra SCSI 15,000 rpm
- Smart Array Controller
- DLT driver
- 17" Monitor
- Compaq Hot Plug Redundant Power Supply
- 2xLAN card(10/100 Mbps)

第五章

GPRS LCS 定位資訊系統

5.1 GPRS 的定位功能

5.1.1 系統架構

GPRS 網路定位系統的網路架構是由位址伺服器與透過 GPRS 維運 (O&M) 從 Cell-ID 收集接取細胞資訊的系統組成。

1. 位置資訊乃透過維運網路出口擷取

網路維運系統 (NMS) 提供可監看 GPRS 網路功能。並提供中華電信即時監視網路監控是否發生障礙功能。並可即時監看以不同 Access 點及成功 attaches, detach 及 PDP context activations, modifications 及 deactivations 及提供系統快速及容易 GTP 及 CDR 狀況的瀏覽。它並幫助中華電信公司即時尋找活動中行動用戶功能。

SGSN(Serving GPRS support node)負責登錄於 GPRS 網路之用戶管理及移動管理。SGSN 並且從 GPRS 用戶端接收及傳送資料。

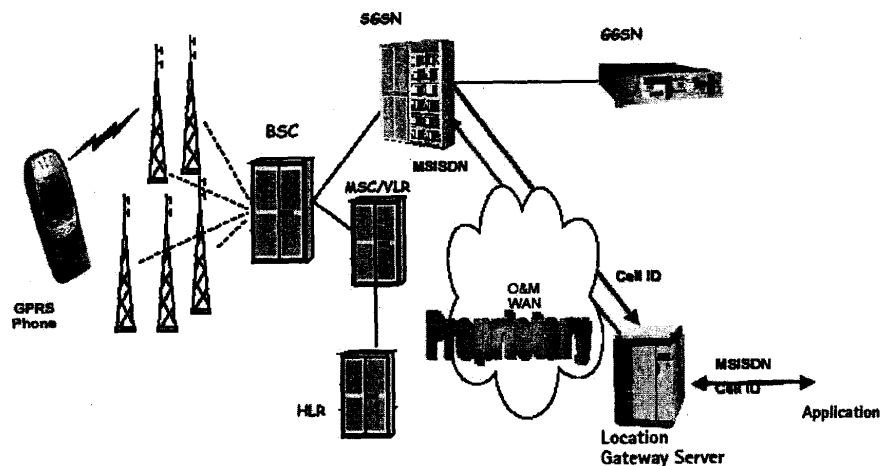


圖 5-1 經由維運網路接取位置資訊架構

位置是 SGSN 從維運網路收集的主要資訊。這些位置資訊如 LA, RA 及 Cell_Id。資料庫伺服器利用 GPRS NetAct 為 Cell ID 提供解決方案。

2. 位置伺服器細胞資訊資料庫查詢

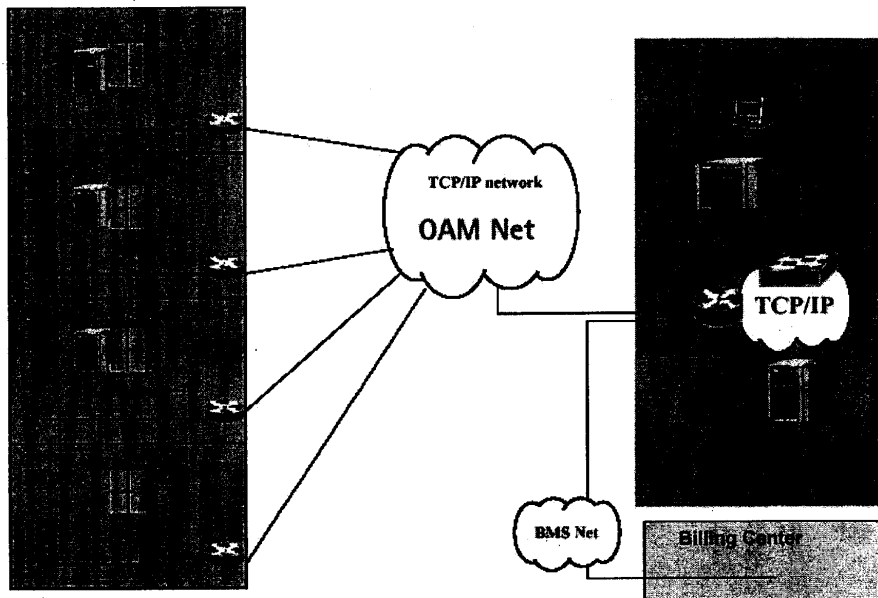
位置伺服器是用以處理位置資料查詢。這是 GMLC 介面且網路元件結 (node)。

不同伺服器傳送網路元件結需求給 MSC。需求是處理執行查詢資料庫透過 GPRS 核心的網路管理系統。

伺服器提供顧客(client)介面取 MSISDN 為輸入及 Cell_ID 為輸出的需求。這介面提供網路管理系統介面。它提供執行資料庫查詢網路管理系統的組成，根據 MSISDN 提供 Cell ID 的資訊。

3. 網路架構

圖 5-2 GPRS 接取位置資訊的網路架構



4. 系統整合及介面

■ 位置伺服器—應用 (位置查詢 Client 連結)

連結是提供位置資訊查詢用，應用伺服器已於前面章節說明。這連結透過 TCP/IP 網路以 Ethernet port 提供給伺服器。

■ 網路管理系統的介面內部查詢

位置資訊查詢是透過 GPRS OAM(DCN)網路進行連結。連結是透過 TCP/IP 網路以 Ethernet port 來提供伺服器。

5. 位置伺服器的硬體

位置伺服器的硬體結構如下：

- Compaq ProLiant ML530
 - Windows2000
 - 2×Intel Pentium III Xeon 1 GHz
 - 2048 MB RAM
 - 12×36GB Wide Ultra3 SCSI 15,000rpm
 - Smart Array Controller
 - DLT driver
 - 17" Monitor
 - Compaq Hot Plug Redundant Power Supply
 - 2×LAN card(10/100Mbps)

第六章

感想及建議

經由此次實習，提出下述幾點心得及建議：

1. 行動數據服務之提供，更將行動電話從語音的使用演進到可看與可互動的服務的全行動生活的服務，行動通信業者將再度面臨全新的競爭與市場佔有率得重新洗牌，日本行動上網的成功已成為全球行動電話產業典範，豐富的內容服務、多樣化的商業模式，加上先進而友善的人機介面、不斷創新的軟、硬體技術，讓人的印象相當深刻。而其中新的行動服務產業鏈的形成與行動通信業者在其中扮演的領導角色與提供完整之服務平台（如服務之上架機制與費率模式），皆是我中華電信值得學習與參考的經營模式。
2. 行動電話發展超乎預期，總用戶數已超過人口數；另網際網路與企業網路發展亦是非常神速，數據的訊務量成長速度亦遠大於語音訊務量成長；從此趨勢看來，結合行動電話及網際網路已經成為一股不可阻擋的趨勢；GPRS 即是因應這種趨勢而產生之重要技術。3G 也與 Nokia 公司完成採購簽約，GPRS 核心網路系統也是 Nokia 公司的產品，期望在此良好之行動數據寬頻網路加上 Nokia 公司手機與中華電信人才譜出動人的增值服務樂章。
3. 亞太行動寬頻於三、四月間將加入市場，因語音話務市場已飽和難以下手，其必以行動數據訊務作為主打項目，中華電信將可利用此次 GPRS 擴充及升版迎戰，加上我們全員行銷的團隊必須做好準備，如現有提供之增值服務全員都要熟悉，最好同仁皆是 GPRS 用戶，有道是最好的行銷者是最好的使用者，如此對客戶服務更能加強，在此新競爭者即將加入市場，市場將重新洗牌之關鍵時刻，做好萬全準備是最佳策略。
4. 3G 簽約建設中，並不代表 2.5G 之 GPRS 時代的結束，因為 3G 只代表客戶頻寬應用較大，新的服務應用還在開發中，而 2.5G 已有日本成功例子，成功是可預期的，何況 2.5G 應用也可在 3G 實現，也可以說 3G 未來，有待 2.5G 的成功。
5. 行動分公司的行銷皆掌握在區分公司的窗口，在這以客為尊的企業經營面向裡，最了解行動的人未直接服務客戶，及提供服務的人未直接面對客戶，客戶是否得到最佳的服務？提供的服務是否合乎客戶需求？這都值得商榷的，尤其在這技術層面高的行動通信行業裡，建議在大都會之窗口由行動分公司的行銷人員派駐，使客戶得到最佳服務，也能更瞭解客戶需求，而讓分公司規劃設計最適切的客戶服務。貼近市場，是商場致勝不二法則。
6. GPRS 未來要能增加更多的客戶，其成功之關鍵取決於新服務之開發及服務是否確實能符合市場之需求，尤其 3G 乃是以服務為決勝之關鍵，如何將 2.5G 成功地推廣至市場將是 3G 是否能成功的關鍵。