國 立 交 通 大 學

資 訊 工 程 學 系

碩 士 論 文

以 SIP 為基礎提供合法監聽之功能

Lawful Interception Based on SIP

指導教授：蔡文能　教授

研 究 生：彭俊豪

中 華 民 國 九 十 四 年 七 月

以 SIP 為基礎提供合法監聽之功能

Lawful Interception Based on SIP

指導教授：蔡文能　　Advisors：Wen-Nung Tsai

研 究 生：彭俊豪　　Student：Chung-Hao Peng

國 立 交 通 大 學

資 訊 工 程 研 究 所

碩 士 論 文

A Thesis Submitted to

Institute of Computer Science and Information Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of Master

in

Computer Science and Information Engineering

July 2005

Hsinchu, Taiwan, Republic of China

中 華 民 國 九 十 四 年 七 月

以 SIP 爲基礎提供合法監聽之功能

學生：彭俊豪　　指導教授：蔡文能 教授

國立交通大學資訊工程學系（研究所）碩士班

摘　　要

隨著網際網路的成長，在網路上的應用也變得越來越多，除了網頁的瀏覽(HTTP)、資料的傳輸(FTP)、信件的傳送(SMTP)這些基本之外，網路電話(VoIP)是近幾年快速興起的應用，有取代傳統電話的趨勢。網路電話指的是將通話語音經由 IP 網路封包交換技術傳送的新電話服務，跟傳統電話電路交換技術完全不同，因此網路電話有一些特性是傳統電話所沒有的，還有許許多多的優點：通話費便宜、可以直接在電腦上使用、使用方便等等，因此網路電話可說是商機無限。

網路電話有許多好處，也有一些問題需要克服，例如通話品質(QoS)、穿透防火牆或是 NAT 等等。當 VoIP 想要商業化並在市場上開始提供通話服務時，都會被國家的法律要求提供犯罪者的電話監聽，但是目前 VoIP 無法提供合法監聽的功能，傳統 PSTN 和 GSM 已經有一套正在運行的架構可以讓司法單位監聽使用傳統電話和行動電話通話的使用者，但是網路電話目前還無法達到此目的，因此在這裡希望可以提出一套讓 VoIP 有合法監聽功能的架構。

VoIP 在建立通話時常用到的標準協定是 SIP 這種網路協定，這種協定可以建立一通網路電話，修改一通網路電話，或是結束一通網路電話，因此這個合法監聽是以 SIP 網路協定爲基礎來提出一個架構，另外合法監聽有一些基本的要求，例如不能讓監聽目標發現受到監聽等等，這個架構也要能符合這些要求。

Lawful Interception Based on SIP

student：Chung-Hao Peng **Advisor：Dr.Wen-Nung Tsai**

Institute of Computer Science and Information Engineering
National Chiao Tung University

ABSTRACT

With the rapid growth of the internet, applications for the internet has become more and more popular, including HTTP, FTP, SMTP, and VoIP. Voice over IP(VoIP) is the application growing fast in recent years. It has the tendency to replace the traditional telephone. VoIP is the routing of voice conversations over the IP network. The voice data flows over a packet-switched network instead of a circuit-switched network. This brings a lot of advantages: low cost, convenient, and easy to use on the computer. Therefore, VoIP has many opportunities in commerce.

Despite of those advantages, VoIP is still facing some challenges, such as, quality of service(QoS) , traversing firewalls and NAT ,etc. For VoIP to be commercialized, it must support Lawful Interception which the Law Enforcement Agency of the country asks for. The conventional PSTN and GSM can support Lawful Interception for LEA, but VoIP does not yet. In this thesis, we proposed an Architecture for VoIP to support Lawful Interception.

The standard protocol which is often used in VoIP is the Session Initial Protocol(SIP). The SIP protocol can be used to set up, modify, and terminate an Internet telephone call. The LI-supported VoIP architecture we proposed in this thesis is based on SIP. A Lawful Interception system must fulfill certain requirements. In this thesis, we will illustrate how our VoIP architecture meets these requirements.

致　　謝

在努力之下，終於完成了我的畢業論文，中間經過了許多的困難與問題，也受到許多人的幫助，在此一一感謝。首先要感謝的是我的指導教授—蔡文能教授，在碩士班期間，他給我許多方面的指導，讓我受益良多，也成長了不少，在此十分的感謝。還有感謝我的父母，他們給我一個平穩的環境，讓我能夠在專心的學習，才有今天的我，感謝他們。接著要感謝的是實驗室的學長姐，感謝他們總是在我有疑惑時，給我忠告與建議，謝謝他們。接著感謝實驗室的同學與學弟們，大家一起工作、學習，互相幫忙，讓我有個難忘的碩士回憶，十分的感謝他們。最後，要感謝的人很多，在我沮喪或難過時，他們都能即時的給我幫助與支持，謝謝他們。

許多的感覺無法用言語形容，對於上面提到的所有人，在此致上我最深的謝意，謝謝你們。

目　　錄

表　目　錄

圖　　目　　錄

第一章、緒論

1.1 簡介

網際網路起源於美國，當初只是爲了軍事上的需要，因此美國國防部成立了ARPA[25]這個組織，網際網路的雛型就此誕生，後來漸漸的學術界也對 ARPA 研究的計畫產生了興趣，所以許多大學紛紛加入這個計畫，整個 ARPA 的網路也越來越大，不過在那個時候網路只用在學術和軍事上面，還沒有商業化，一直等到九零年代初期，有網路公司提供電子郵件服務之後，網際網路開始邁入商業化，快速的蓬勃發展起來。

台灣網路發展迅速，截至 2003 年 9 月爲止，經常使用者達 920 萬以上，網路普及率達 39%。其中約 50%屬於撥接用戶、25%使用寬頻，另外 25%屬無線行動上網用戶[26]。根據調查(圖 1)，到了 2004 年 3 月時，台灣使用寬頻上網的人口數已經超過 300 萬戶，上網普及率也達到了 39%，這表示網路已經和人們的生活息息相關。

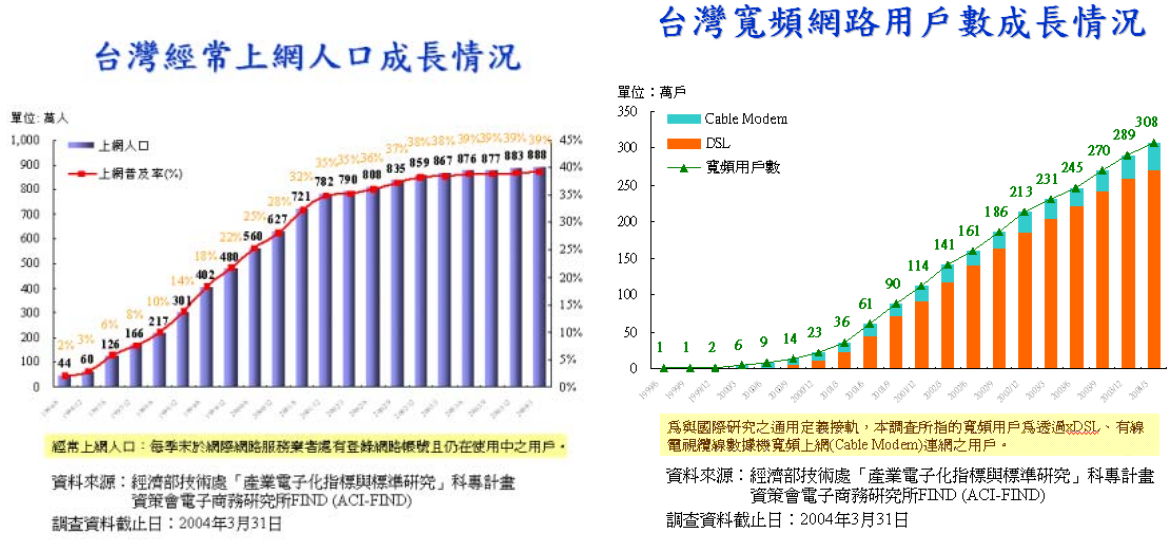

圖 1　台灣網路人口成長清況圖

(資料來源：經濟部技術處「產業電子化指標與標準研究」科專計畫)

隨著網際網路的成長，在網路上的應用也變得越來越多，除了網頁的瀏覽(HTTP)[3]、資料的傳輸(FTP)[4]、信件的傳送(SMTP)[5]這些基本之外，網路電話(VoIP)是近幾年快速興起的應用，有取代傳統電話的趨勢。網路電話指的是將通話語音經由 IP 網路封包交換技術傳送的新電話服務，跟傳統電話電路交換技術完全不同，因此網路電話有一些特性是傳統電話所沒有的，還有許許多多的優點：通話費便宜、可以直接在電腦上使用、使用方便等等，因此網路電話可說是商機無限。

1.2 動機與目的

網路電話有許多好處，也有一些問題需要克服，例如通話品質(QoS)、穿透防火牆或是 NAT 等等。當 VoIP 想要商業化並在市場上開始提供通話服務時，都會被國家的法律要求提供犯罪者的電話監聽，但是目前 VoIP 無法提供合法監聽的功能，傳統 PSTN 和 GSM 已經有一套正在運行的架構可以讓司法單位監聽使用傳統電話和行動電話通話的使用者，但是網路電話目前還無法達到此目的，因此在這裡希望可以提出一套讓 VoIP 有合法監聽功能的架構。

VoIP 在建立通話時常用到的標準協定是 H.323[6]和 SIP[7]這二種網路協定，這二種協定可以建立一通網路電話，修改一通網路電話，或是結束一通網路電話，因此這個合法監聽是以這二種網路協定爲基礎來提出一個架構，另外合法監聽有一些基本的要求，例如不能讓監聽目標發現受到監聽等等，這個架構也要能符合這些要求。

1.3 論文架構

在這篇論文中，總共分成六個章節，第二章的背景介紹會說明公眾交換電話網路和行動電話網路以及網路電話相關的資料與通訊協定，第三章的相關研究會介紹有關合法監聽的研究，第四章的系統架構會介紹本論文提出架構的細節，第五章模擬結果，第六章結論與未來發展。

第二章、背景知識

2.1 公眾交換電話網路

2.1.1 公眾交換電話網路簡介

公眾交換電話網路俗稱 PSTN，全名爲 Public Switched Telephone Network，是一般傳統的電話交換系統，也是全世界最大的電話網路，技術上是以電路交換(Circuit-Switched)方式進行傳輸，每次通話系統會爲通話雙方保留一條傳輸的頻寬，以 64Kbps 速率傳送語音，當電話接通，這段頻寬便爲通話雙方保留，只有通話雙方可以使用這條頻寬，直到通話雙方結束電話爲止，圖 2 爲 PSTN 網路架構圖。

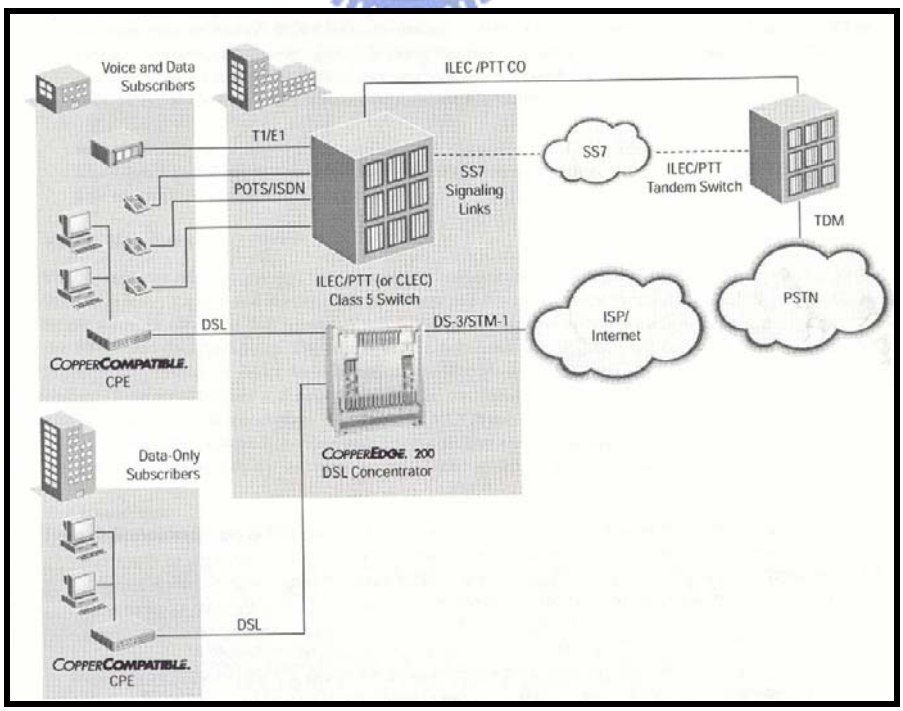

圖 2　PSTN 網路架構圖

2.1.2 公眾交換電話網路通訊協定

在這裡介紹最常見的通訊協定 Signaling System No.7(SS7)，在電信網路裡，智慧型網路是由 SS7 通訊協定所控制，使用於整體服務數位網路上，SS7 信號網路中各節點之功能設置乃依據其所扮演的角色而定，基本上可分爲信號點與信號轉送點兩種。信號點，一般所指的是：信號轉送端點、ISDN 交換機、服務交換點、臨時位址暫存器、服務控制點、永久位址暫存器(Address Register)與行動交換中心等，其中信號轉送端點亦具有部份信號轉送點之功能。

以下便一一介紹每一層之協定。

- MTP：SS7 的第一層爲信號數據鏈路層(Signaling Data Link Level)又稱爲實體層(Physical Level)，它定義信號鏈路之實體、電氣與功能特性，以提供實體鏈路接收傳送 SS7 信號。第二層稱爲信號鏈路層(Signaling Link Level)，它負責確保 SS7 信號訊息在實體層上收送的可靠度。第三層稱爲信號網路層(Signaling Network Level)，主要功能爲信號訊息處分及信號網路管理。以上三層合稱爲訊息轉送部(Message Transfer Part MTP)。信號數據鏈路包含一條雙向之傳輸鏈路(Transmission Link)，以及傳輸鏈路與第二層間之通信介面，以提供兩信號點間信號傳送之全雙工(Full Duplex)之實體通道。傳輸鏈路是由傳輸速率相同且方向相反之兩個傳輸通道組成，此傳輸通道僅能用來傳送信號，不可載有其他資訊。標準的傳輸速率爲 64kbps。
- SCCP：SCCP 是協助 ISUP 做點對點之交換，主要目的有四項：
  1. 提供 ISDN-UP(ISUP)建立點對點的信號連接(Signaling Connection)。
  2. 提供網管、維護中心與各交換局間(有 SP 功能者)建立信號連接。
  3. 用戶(如帳戶服務中心)與各交換局(SP 點)間建立信號接續，可直接傳送帳戶服務資料，而不用再運送磁帶。
  4. 供將來其他用戶部建立信號接續使用。
- TCAP：交易能力(Transaction Capabilities；TC)或稱交易能力應用部(Transaction Capabilities Application Part；TCAP)，在 SS7 網路中是屬於應用層(Application Layer)中的一個應用服務元件(Application Service Element；ASE)。其目的在於提供 SS7 網路中之信號節點對信號節點之間非電路接續相關訊息的傳送，並爲它們之間的各種應用提供一般性的服務。例如交換機與交換機間非電路接續相

關訊息的交換；交換機對網路服務中心資料庫作號碼翻譯(例如 080 服務號碼)皆可由 TCAP 所提供的服務來達成。

2.1.3 公眾交換電話網路的監聽方法

依照通訊保障及監察法，只要有足夠的事實可以證明相監聽的對象有相關罪嫌，就可以申請通訊監察書，通訊監察書應記載下列事項：

1. 案由及涉嫌觸犯之法條。
2. 監察對象。
3. 監察通訊種類及號碼等足資識別之特徵。
4. 監察處所。
5. 監察理由。
6. 監察期間及方法。
7. 聲請機關。
8. 執行機關。

前項通訊監察書，偵查中由檢察官依司法警察機關聲請或依職權核發，審判中由法官依職權核發，但是該管檢察官可以口頭通知執行機關先予執行通訊監察，第五條之通訊監察期間，每次不得逾三十日，第七條之通訊監察期間，每次不得逾一年[27]，圖 3 爲公眾交換電話網路的監聽架構。

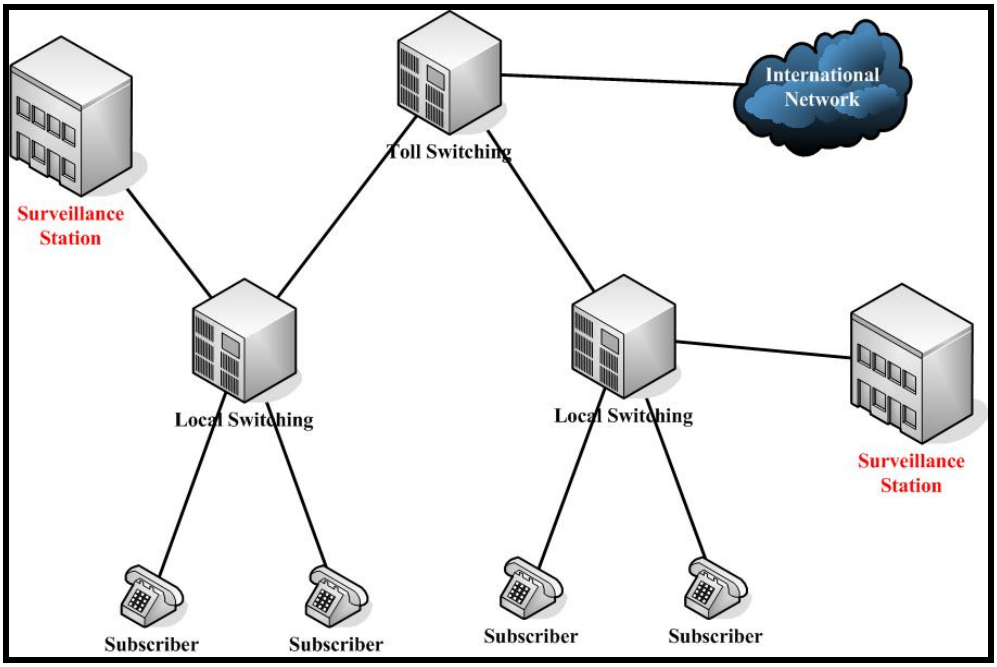

圖 3 公眾交換電話網路監聽架構

2.2 GSM

GSM 是 Global System for Mobile Communications 的縮寫，是第二代行動電話技術之一，它是由歐洲郵電管理聯合會(European Conference of Postal and Telecommunications Administrations 簡稱 CEPT)和歐洲電信標準協會(European Telecommunications Standards Institute 簡稱 ETSI)所發展出來的行動電話技術，歐洲郵電管理聯合會在 1982 年成立了一個叫 Groupe Spécial Mobile(GSM)的小組，目的是爲了發展新的行動電話系統，並符合一些要求，如：有好的通話品質、低成本、提供國際漫遊等等[28]。在 1989 年，GSM 小組轉移到歐洲電信標準協會，並於 1990 年提出第一版 GSM 標準，等到 1991 年正式開始營運，二年後也就是 1993 年總共有 22 個國家使用 GSM 系統[11]，根據統計，在 1994 年全世界有一百三十萬人使用 GSM[12]，到了 1997 年成長爲五百五十萬人，到現在 GSM 已經成爲全世界最普遍的行動電話技術了。

和第一代的行動電話(如：AMPS, TACS)技術相比，GSM 有更好的壓縮演算法和數位訊號處理功能，這使得 GSM 有不錯的通話品質，而且除了通話服務之外，GSM 還提供了資料服務，可以傳送使用者的資料，以及現在所有人最常使用的短訊服務，這也是以前的行動電話所沒有的功能，因此 GSM 挾帶這這些優勢席捲全球。圖 4 是 GSM 的基本架構示意圖。

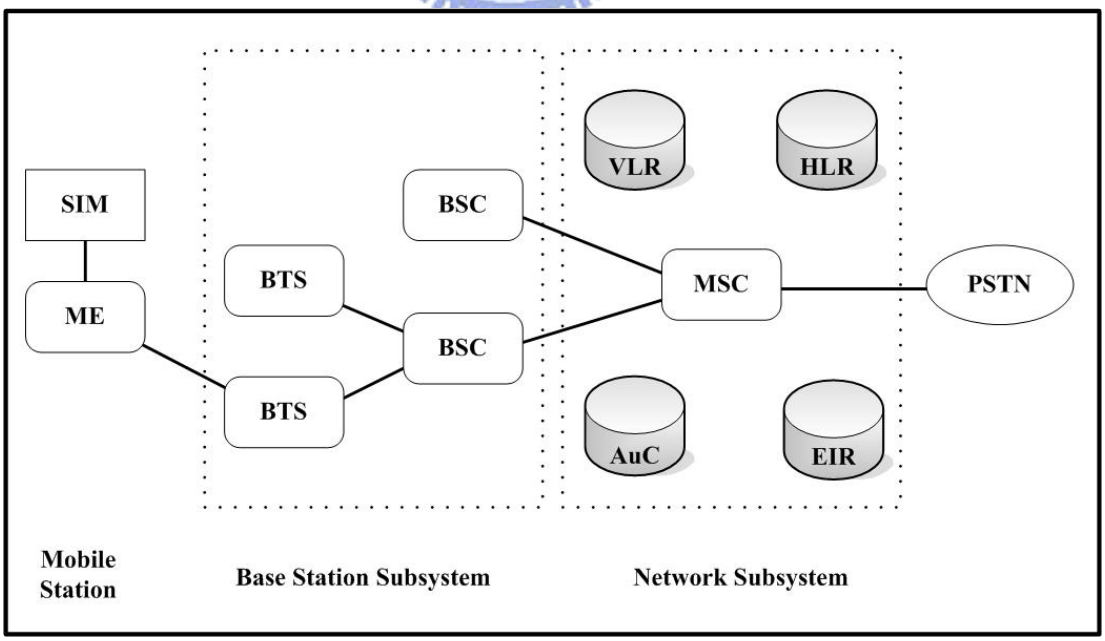

圖 4 GSM 基本架構圖

表 1 是 GSM 基本架構圖的說明：

表 1　GSM 基本架構說明

名　稱	說　　明
SIM	Subscriber Identity Module，裡面儲存了使用者的資料，如：電話號碼、電話簿等等
ME	Mobile Equipment，行動電話機身，俗稱手機，有很多廠商在生產，如 NOKIA、Motorola、Panasonic 等等
Mobile Station	包含了 SIM 和 ME，也就是行動電話加上 SIM 卡，這樣就可以使用電話公司所提供的服務，如：通話服務、簡訊服務等等
BTS	Base Transceiver Station，Mobile Station 經由無線電波和 BTS 建立連線，傳送語音資料
BSC	Base Station Controller，控制數個 BTS，將 BTS 傳來的資料做整理，另外也負責 handover 功能
MSC	Mobile services Switching Center，負責使用者註冊、認證、handover 等功能，並連接 PSTN
HLR	Home Location Register，儲存使用者的資訊以及所在位置
VLR	Visitor Location Register，儲存使用者目前的所在位置
EIR	Equipment Identity Register，儲存所有合法的 ME
AuC	Authentication Center，儲存每位用戶 SIM 卡裡的祕密金鑰，用來做認證以及加密等功能

GSM 的安全性分成二種，一種是認證，一種是加密，認證是爲了確認是否爲合法的用戶，所以使用者通話都需要認證，加密則是因爲 GSM 的通話因爲經由無線電波傳送，容易被有心人士從中攔截，取得通話內容，因此需要將通話加密，圖 5 是 GSM 認證和加密架構圖[13]，圖 6 是 GSM 的架聽架構圖。

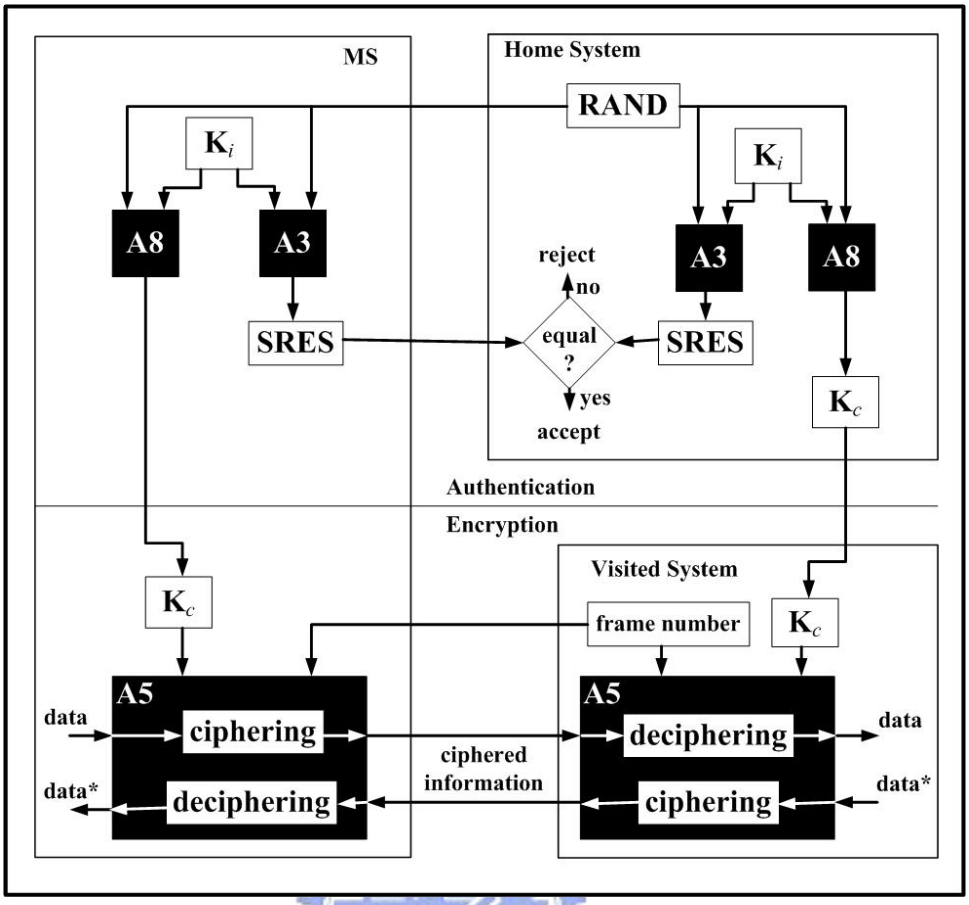

圖 5　GSM 認證和加密架構圖

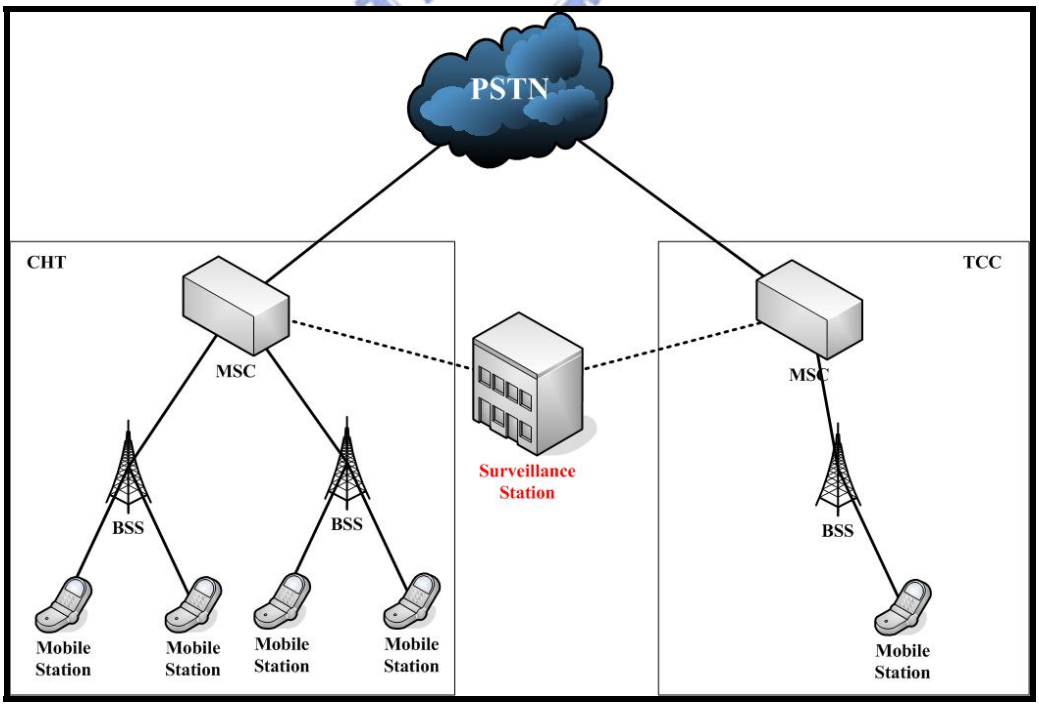

圖 6　GSM 監聽架構

2.3 網路電話

2.3.1 網路電話簡介

網路電話簡單來說，即是將聲音數位化之後，以一個個封包的方式，透過 IP 架構的網路傳送到收話端 。

Voice over IP 簡單來說，即是將聲音數位化之後，以一個個封包的方式，透過 IP(Internet Protocol)架構的網路傳送到收話端，相較於先前的電路交換(Circuit-Switched)有著網路資源運用更加充分，以達到同時可處理更多通電話連線的好處，並且成本更加低廉，所以廣受業界的矚目與推廣。

網路電話的演進可以分成三個階段來看(如圖 7 所示)：

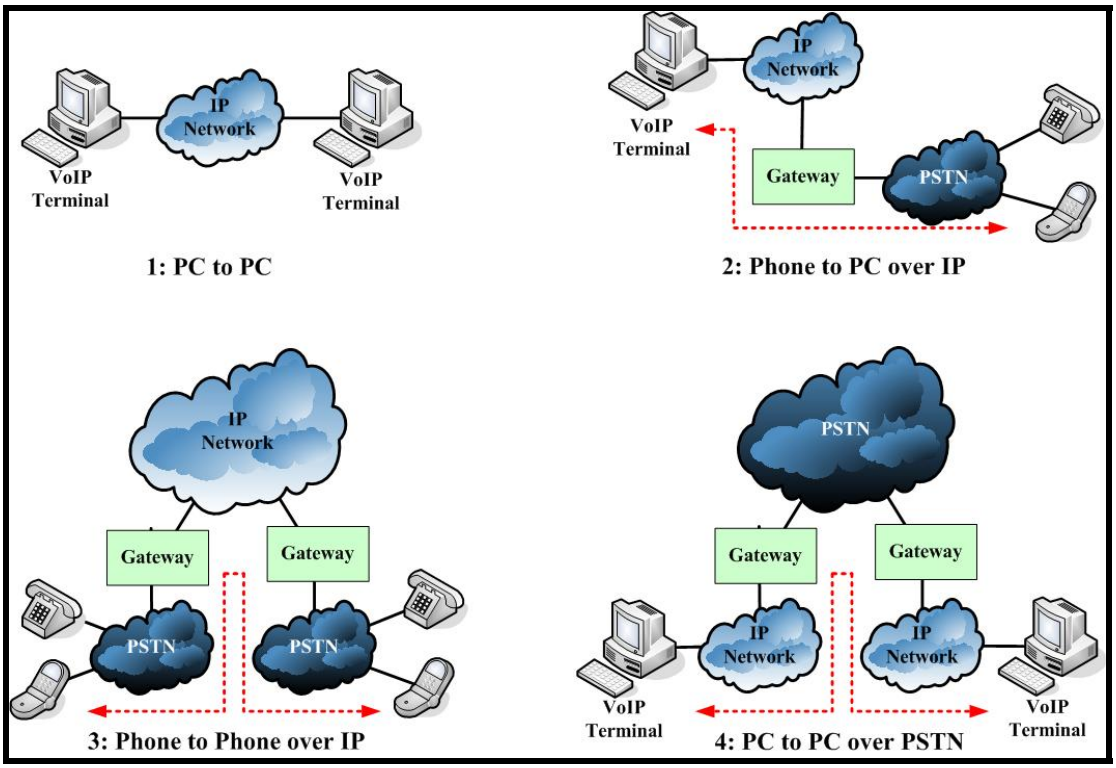

圖 7 網路電話演進圖

(1) PC to PC：這個是最早被開發出來的網路電話系統，利用軟體在 IP 網路上建立傳送聲音封包的連線，可以說是最簡單而且最容易的建構方法。第一個這種類型的產品是由 Vocaltec 於 1995 年 2 月所開發出來的 Internet Phone，這個軟體的需求配備爲 486/33-MHz PC、一張音效卡、麥克風，以及調變解調器(Modem)，可以算是 VoIP 的第一個商業軟體。近年來，這類的產品大行其

道，許多的軟體，如 Microsoft 的 MSN[29](採用 SIP 網路協定)、Yahoo 的 Yahoo 即時通[30](採用 H.323 網路協定)等都提供有網路電話的功能。另外於 2004 年 2 月推出了第一套以 P2P 爲基本架構的網路電話軟體 Skype[31]，以不錯的通話品質獲得廣大的好評。

(2) PC to Phone：由於目前電路交換式的電話系統仍然是分佈最廣泛的系統，所以如何將兩種不同的網路系統互相溝通，使得使用者可以輕易的使用個人電腦打電話到一般的公眾交換網路(Public Switch Telephone Network, PSTN)上，是電話服務業者最爲重視的一個部份。這一類的應用最早由 Net2Phone 這家公司於 1995 年 11 月提出 PC-to-Phone 的網路電話計劃。1997 年 12 月 ITXC 公司開始大量生產交換機伺服器，將 PC-to-Phone 產品商業化。例如最近 Seednet 正在推廣的“Wagaly Talk”[32]服務，是採用 H.323 網路協定。上一段所提及的 Skype 軟體也同樣具有 PC to Phone 的能力。

(3) Phone to Phone：發展網路電話的最終目標是希望能將聲音與資料系統的整合，以方便管理與控制，所以 Phone-to-Phone 系統的開發就是希望能取代傳統的電路交換式系統。Net2Phone 公司於 1997 年 9 月開始在美國推出 Phone to Phone 透過 IP 網路傳送的服務，許多的長途電話也漸漸的改用透過 IP 網路傳送以節省成本，可說是未來的趨勢與主流產品。2002 年 10 月 18 日，美國知名電話公司 AT&T 向 FCC 提出要求，希望 FCC 對 Phone-to-Phone 的 VoIP 規劃出一套合法的管理規則，但是 FCC 認爲 VoIP 是一套實驗與發展中的技術，所以對 AT&T 的提議持保留態度。2004 年 2 月 12 日，FCC 開始注意到現行 VoIP 產品的架構與管理混亂，各家業者的實作方式皆有所不同，於該日起，開始著手訂定 VoIP 相關的架構與管理規則，期望使所有 VoIP 業者的實作有一定的規則，達到公用網路管理的目標。

目前網路電話的服務以歐美國家推出的較多，因爲擁有較便宜的特性，頗受消費者的歡迎，所以每年成長也有一定的幅度，我們可以從 Allied Business Intelligent Inc.(ABI)於 2003 年對 VoIP 做的研究與推測(圖 8)中看出，未來 VoIP 市場的成長幅度是樂觀的。

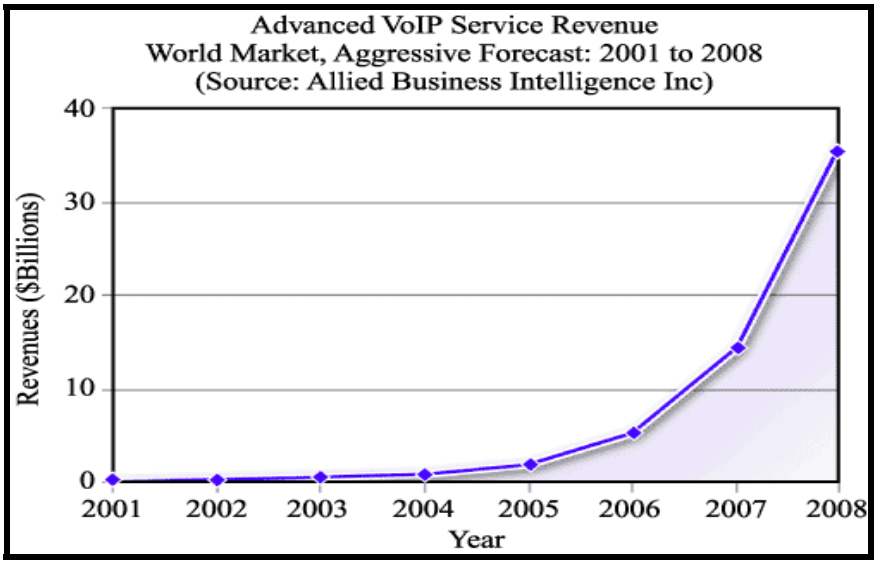

圖 8　世界網路電話市場成長預測圖
(資料來源：Allied Business Intelligence Inc)

同樣的，雖然亞洲的市場因爲電信業開放的腳步較爲緩慢，網路電話(VoIP)成長的速度相較於歐美國家來的遲緩，但是許多的調查與研究都顯示亞太地區網路電話的成長都是可以樂觀預期的，這方面可從 IDC 於 2002 年對亞太地區做的研究與預測(圖 9)可看出，成長的可能性。

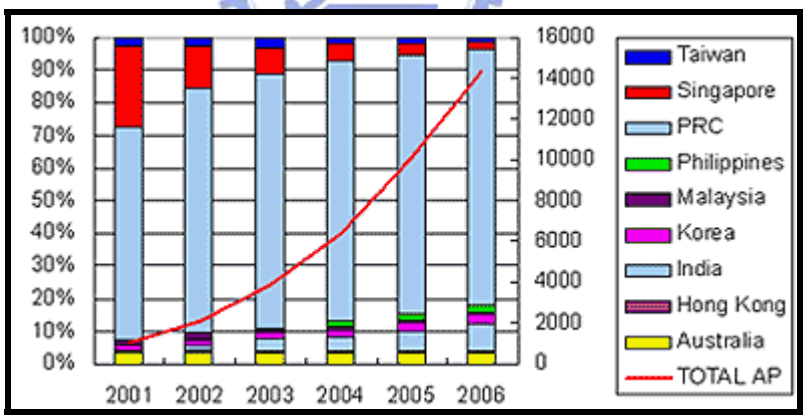

圖 9　亞洲網路電話成長預測圖
(資料來源：IDC)

美國 Trilium 公司對 VoIP 相關協定的實際安裝情況和未來前景進行了預測：2004 年，SIP 將達到全部 VoIP 相關安裝協定的 24%。H.323 雖然在 2001 年的佔有率非常高，達到 89%，但今後這一比例將會逐步下降，預計將降低到 35%左右[33]。

2.3.2 網路電話通訊協定

爲了可以順利的在公眾的 IP 網路上建立連線並傳送聲音的封包，一套公認的通訊協定(Protocol)是必要的。網路上兩大網路通訊協定訂定組織：ITU(International Telecommunication Union)與 IETF(The Internet Engineering Task Force)分別都訂定了適用於網路電話連線建立與中斷的通訊協定，到目前爲止共有幾個較爲廣泛使用的通訊協定，在此做簡單的介紹。

- RTP：Real-time Transport Protocol[19]，由 IETF 於 1996 年 1 月定義在 RFC1889，是一個用來傳送即時應用的通訊協定(包括聲音、影像…等)，定義有 RTP 封包標頭(Packet Header)與所傳送媒體相關的資訊…等。和 RTCP(RTP Control Protocol，RFC1890)搭配使用，是一套專門處裡媒體傳送的通訊協定，藉以和訊號封包分開傳送。
- H.323：Packet-based Multimedia Communications Systems，1995 年 3 月 28 日由 ITU-T 正式訂爲標準，是一套包含其他通訊協定的封包式多媒體通訊系統。因爲定義的較早，演化的版本也很多(於 2003 年 7 月出版第五版)，所以許多的系統都採用 H.323 的架構開發，如 Microsoft 的 NetMeeting 即是採用 H.323 的架構。H.323 最大的缺點爲系統龐大，內部結構複雜。
- SIP：Session Initial Protocol，於 1999 年 3 月定義於 RFC 2543，再版定於 RFC 3261。爲一套點對點(Peer to peer)以及主從式(Client/Sever)的傳輸架構，與 SDP(Session Description Protocol, RFC 2327)、RTSP (Real-Time Streaming Protocol, RFC 2326)、SAP (Session Announcement Protocol, RFC 2974)合爲 IETF 多媒體資料與控制架構(Multimedia data and control architecture)。SIP 最大的好處即爲簡單、彈性佳，適合用於智慧型掌上產品的開發。
- MGCP[9]：Media Gateway Control Protocol，於 1999 年 10 月由 IETF 定義在 RFC 2705，爲一套主從式(Master-slave)架構的通訊協定，運用於 Media Gateway Controller(MGC)與 Media Gateways(MGs)之間所傳輸的訊息規範上。MGCP 是一套純知識性的通訊協定，需要其他的通訊協定來詳細定出實作架構，Megaco/H.248[10]就是根據 MGCP 爲基礎所定義出的通訊協定。
- Megaco/H.248(Gateway control protocol)：爲 IETF(MEGACO)與 ITU-T(H.248)於 2000 年 11 月共同研究開發的通訊協定，與 MGCP 的用途類似，用於 MGC 與 MGs 的通

訊上，亦爲主從式(Master-slave)的架構。

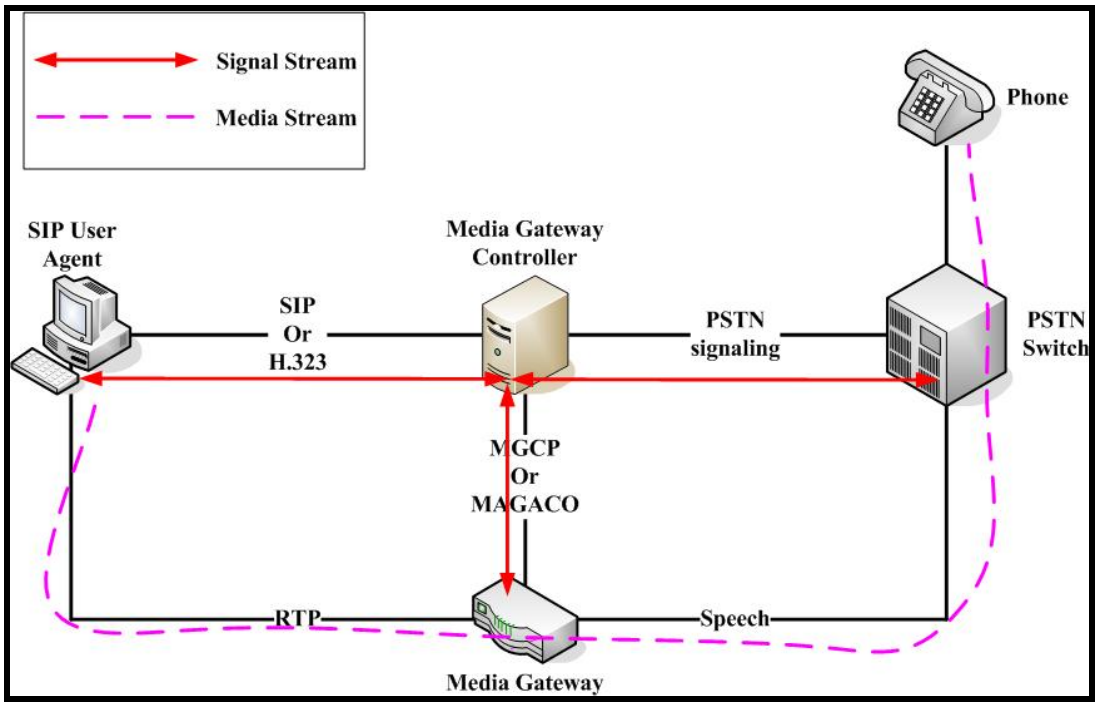

圖 10　各種 VoIP 通訊協定分工情況

以上爲目前用於網路電話的五個通訊協定，其中 H.323 與 SIP 主要用在通訊會期(Session)的建立與中止，以及媒體傳送的管理上。MGCP 與 MEGACO/H.248 主要是幫助網路電話與原先 PSTN 架構的相容性更佳所設計出來的(如圖 10)。接下來的章節我們將特別介紹 SIP 架構的細節部份。

2.3.3　Session Initial Protocol(SIP)

Session Initial Protocol，簡稱 SIP，是由 IETF 於 1999 年訂定出來的應用層(Application-Layer)通訊協定，主要是爲了多媒體通訊的建立、修改與中斷而訂定。其最大的特點爲簡單、靈活度高以及適用於智慧型裝備。底下我們將分架構與訊息交換兩大部份來介紹 SIP。

SIP 架構

SIP 爲一個主從式(Client-Server)的架構，由用戶端(Client)發出需求(Request)，伺服

器端(Server)接收到需求後，因情形發出適當的回應(Response)給用戶端，底下我們分別介紹 SIP 架構中的每樣實體(Entity)：

(1) Client：又稱 User Agent Client，爲一個應用程式，用來發出 SIP 訊息給伺服器或是其他的用戶。

(2) Server：主要用來對用戶端的需求做出正確的回應用，依功能可分成四類。

1. Proxy Server：作用就像一般區域網路(LAN)中的代理伺服器(Proxy)一樣，將從用戶端收到的需求傳到正確的伺服器或用戶，可分成有狀態性(Stateful)或是無狀態性(Stateless)。

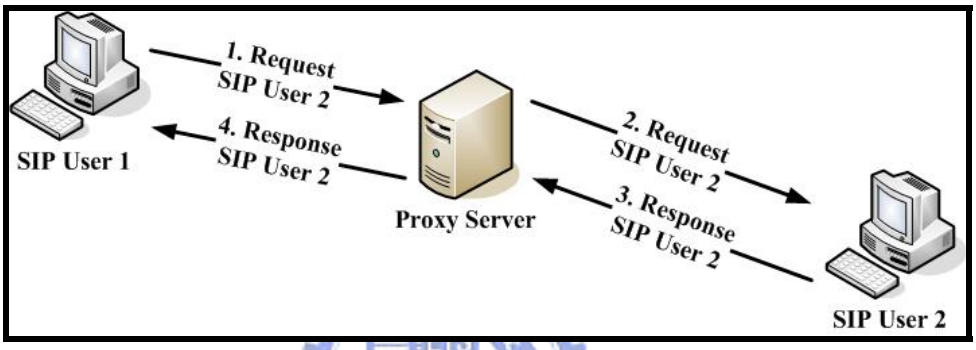

圖 11 SIP 代理伺服器(SIP Proxy Server)

2. Redirect Server：從用戶端收到需求，依據伺服器資料庫內的紀錄，得到用戶查詢的對應位置，回傳給用戶端，此伺服器無法發出 Invite message 給其他的實體(Entities)。

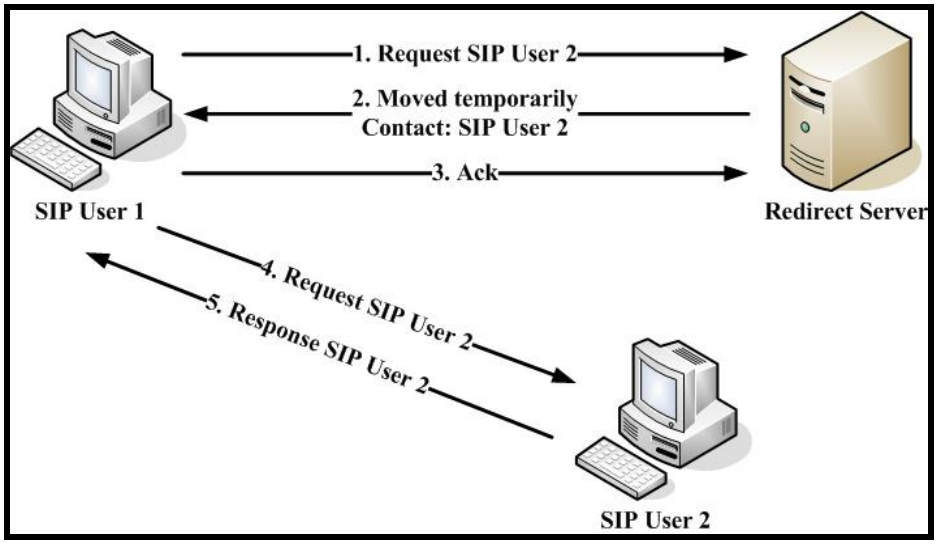

圖 12 SIP 重新導向伺服器(SIP Redirect Server)

3. Registrar Server：接受從用戶端發出的 Register 訊息，讓用戶註冊於伺服器上，包含用戶端的一些資訊如：位置、暱稱…等，通常會與 Proxy Server 以及 Redirect Server 合併在一起使用。

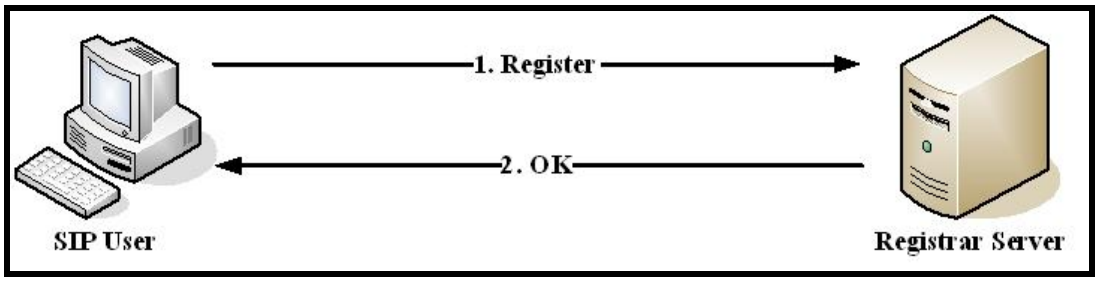

圖 13　SIP 註冊伺服器(SIP Registrar Server)

4. User Agent Server：接收從使用者(User)來的需求，並做出回應(發出需求到伺服器端，以得到回應)，通常與 User Agent Client 合併成一個裝置(Device)，稱做 User agent(UA)。

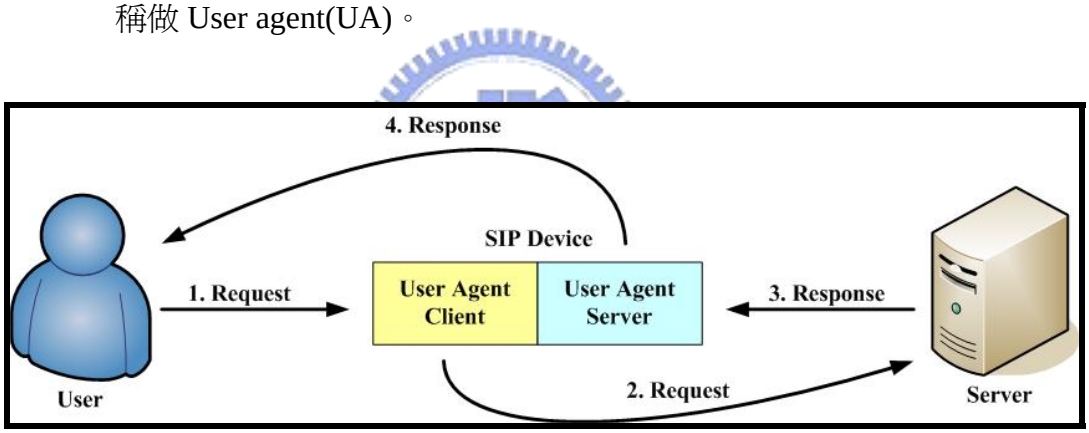

圖 14　SIP 使用者代理人(SIP User Agent)

SIP 訊息傳送

SIP 是一個以文字爲基礎(Text-base)的通訊協定，使用 ISO 10646 定義的字元，並使用 UTF-8 的方式編碼，所以 SIP 的訊息看起來類似於 HTTP 的訊息。用文字基礎傳送的缺點是與使用二進位方式表示的訊息相較，較占傳輸頻寬。

SIP 的需求(Request)訊息可以分爲六個基本類型：

(1) Invite：用來發出邀請、開起連線的訊息。

(2) ACK：用來確認最後的回應(Response)已經收到。

(3) BYE：用來結束連線用的訊息。

(4) OPTION：用來詢問伺服器的負載量(Capacity)等訊息。

(5) CANCEL：用來停止一個暫時行的需求(Request)。

(6) REGISTER：由 User agent client 發出，做爲登入(Login)或是註冊用的訊息，一個用戶可以對許多的伺服器註冊；對同一台伺服器也可接受同一位用戶多次的註冊動作。

底下我們用一個簡單的例子(圖 15)來介紹 SIP 建立一通連線的訊息交換：

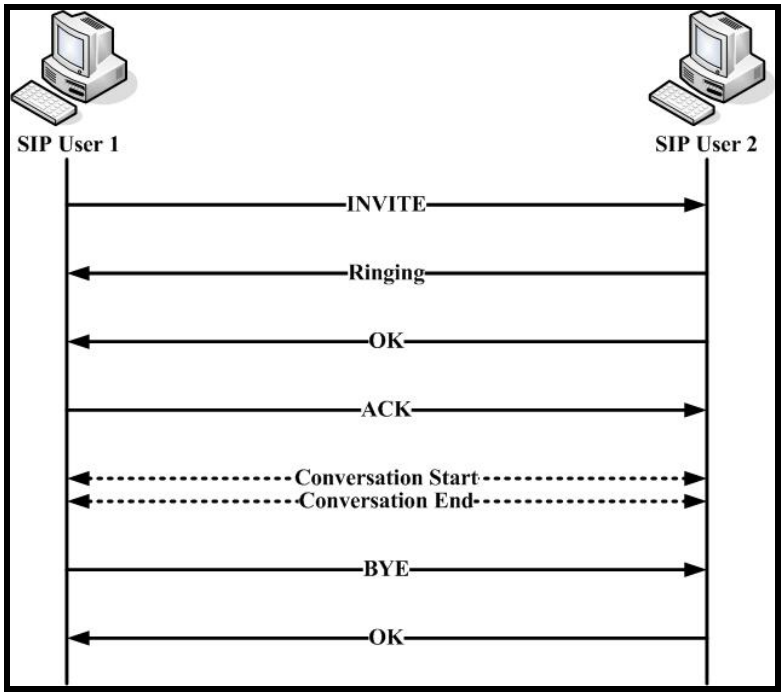

圖 15　基本 SIP 建立通話流程

首先由發話端(Caller)送出 INVITE 的訊息給收話端(Callee)，當收話端收到訊息後，會先發出鈴響，並傳回 Ringing 的訊息。當收話端拿起話筒回應時，會送出 200 OK 的訊息，發話端收到後，傳送 ACK 訊息，則通話正式建立。當通話結束時，任一端發出 BYE 訊息，由對方收到並回覆 200 OK 後通話正式結束。

通常用 SIP 建立網路電話的連線，會用 RTP 網路協定傳送語音資料，並且使用一些加密方法(如：DES, AES)將語音資料加密，不過在 2004 年的 International computer Symposium(ICS)有一篇論文，叫做 A study on VoIP Security[24]，在裡面他並不是用一般傳統加密方法將語音資料加密，而是用視覺加密以及資料分享的方式取代傳統的加密方式，結果顯示這篇論文提出的方法可以降低語音資料加密的時間。

第三章、相關研究

3.1 以 H.323 為基礎的四種合法監聽方法

這篇論文[20]提出四種在網路電話上的監聽方法，以 H.323[6]爲基礎，第一種是在匣道器(Gateway)上監聽，第二種是修改 Gatekeeper 使被監聽的網路電話封包會經過監聽的機器，第三種是網路電話的封包一定會經過監聽的機器，最後一種是把監聽的機器和交換器或集線器連接起來，只要是監聽的封包都會複製一份到監聽的機器。

1. 在匣道器上監聽

在匣道器上監聽這種方法可以用在當 H.323 網路電話打到公眾交換電話網路的時候，這裡的匣道器指的是連接 H.323 和公眾交換電話網路的機器，它可以在 H.323 和公眾交換電話網路的網際網路通訊協定之間做轉換。因爲所有的通話都會經過這台匣道器，所以可以在這裡監聽，當匣道器發現有通話需要被監聽時，它會將通話內容複製一份到一台專門放監聽資料的機器上，如圖 16 所示。

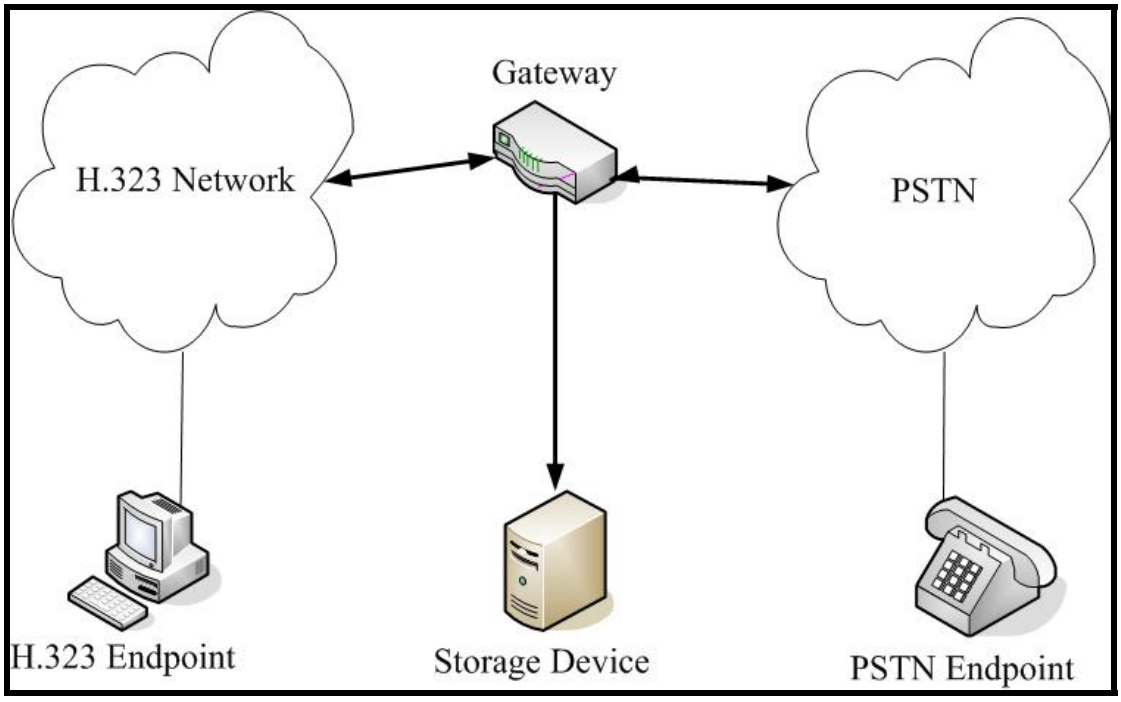

圖 16　在匣道器上監聽

這個方法並不侷限在 H.323 和 PSTN 網路上，它可以用在任何有二種電話系統的網路之上，因外爲了要能辨認出哪些通話需要被監聽，哪些不需要監聽，匣道器必須要有一份清單，這份清單上會列出需要被監聽的使用者，如果發話端是在 H.323 的網路內，可以從 Q.913 的訊息中取出 alias addresses 和 IP address 來辨認使用者，如果是收話端在 H.323 的網路內，可以從 gatekeeper 中得到使用者的 IP address，如此一來無論是發話端還是收話端都可以受到監控。

這個方法不需要在 H.323 網路中增加額外的機器，除了匣道器之外，也不需要修改其它的機器，所以只要在匣道器上新增一些功能，就可以達到監聽的效果，值得一提的是在匣道器上監聽不會影響通話的品質，也不會讓使用者發現被監聽，不過這個方法的致命傷在於它無法監聽在 H.323 網路裡面的通話，也就是說只要通話沒有經過匣道器，就英雄無用武之地了。

2. 利用 Gatekeeper 將被監聽的通話導向監聽設備

在 H.323[6]通訊協定中，gatekeeper 負責通話建立的工作，因此可以修改 gatekeeper 來達到監聽的目的，首先在 H.323 網路裡面增加一台監聽設備，它的工作是儲存監聽的資料，再來就是修改通話建立的流程，讓被監聽的通話導向監聽設備，這樣就可以把通話內容記錄下來，所以原本通話會變成發話端跟監聽設備建立連線，以及監聽設備跟收

話瑞建立連線。在 H.323 訊息中，RAS 訊息是 Registration, Admission and Status 的意思，ARQ 訊息是 Admission Request 的意思，ACF 訊息是 Admission Confirm 的意思，H.323 通話建立方式如圖 17 所示。

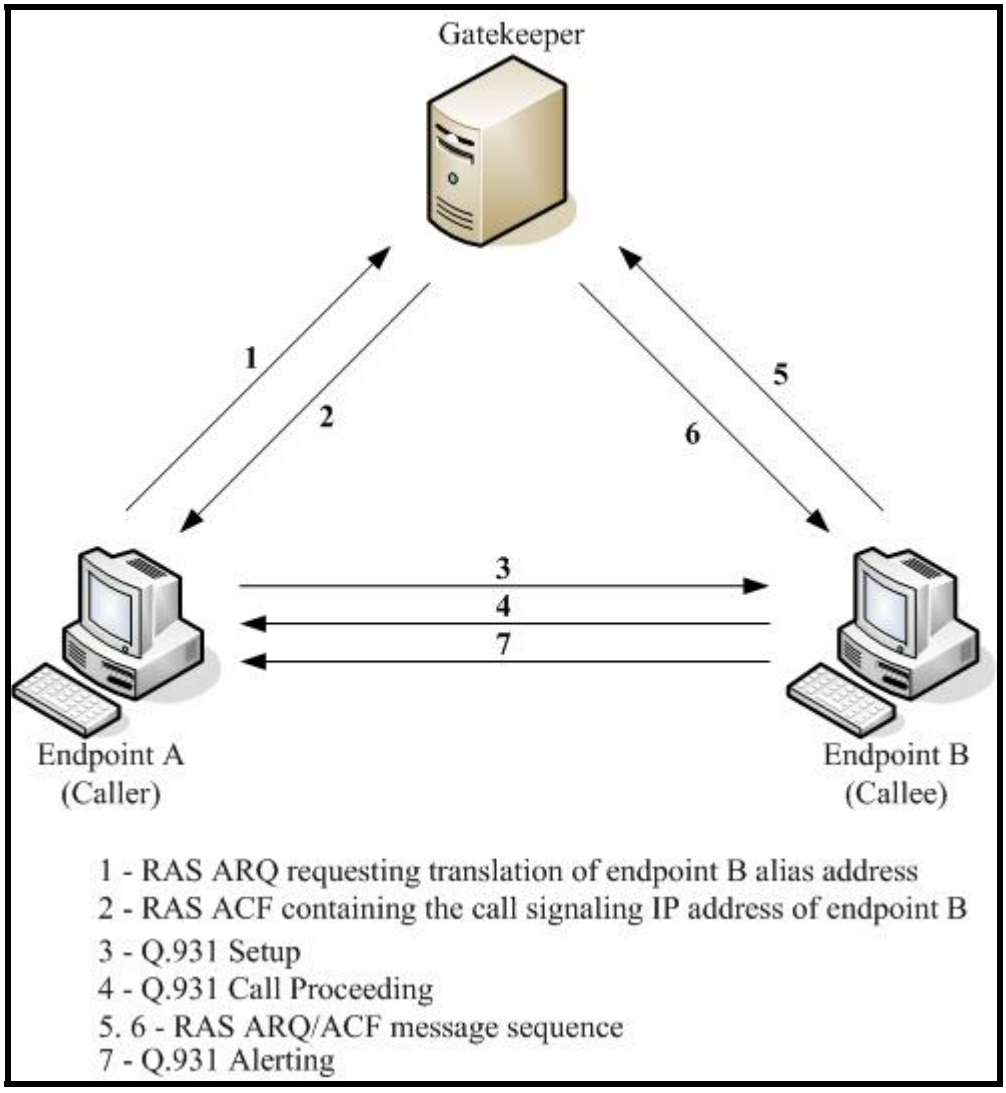

圖 17　H.323 通話建立步驟

一開始，發話端先送一個 ARQ 訊息給 gatekeeper(1)，ARQ 訊息裡面包含了收話端的 alias address，gatekeeper 會回覆一個 ACF 訊息(2)，ACF 訊息裡面包含了受話端的 IP address，如此一來發話端就可以利用這個 IP address 和受話端建立連線，之後雙方再交換 Q.931 Setup/Call Proceeding 訊息(3, 4)[21]，再來受話端會和 gatekeeper 交換 ARQ/ACF 訊息(5, 6)，最後受話端會送給發話端一個 Q.931 Alerting 訊息(7)[22]。

H.323 網路協定加入監聽之後建立通話的步驟會有所改變，首先當 gatekeeper 收到發話端送的 ARQ 訊息時(1)，會判斷發話端或受話端是否需要被監聽，如果需要監聽的

話，gatekeeper 會送一個訊息告訴監聽設備有一則通話需要做監聽(2)，這個訊息包含了發話端跟受話端雙方的 IP address，再來 gatekeeper 會回覆發話端一個 ACF 的訊息(3)，這個訊息原本內容應該有受話端的 IP address，但是 gatekeeper 把它改成監聽設備的 IP address，如此一來到時候發話端就會跟監聽設備建立通話連線，受話端也會和監聽設備建立連線，而監聽設備就可以成功的監聽這則通話，監聽設備會將所有經過它的訊息轉送出去(4-7, 10, 11)，所以通話雙方還是依照原本的步驟建立連線，最後監聽設備就可以將雙方的通話內容完全記錄下來，成功的達到監聽效果，建立的流程如圖 18 所示。

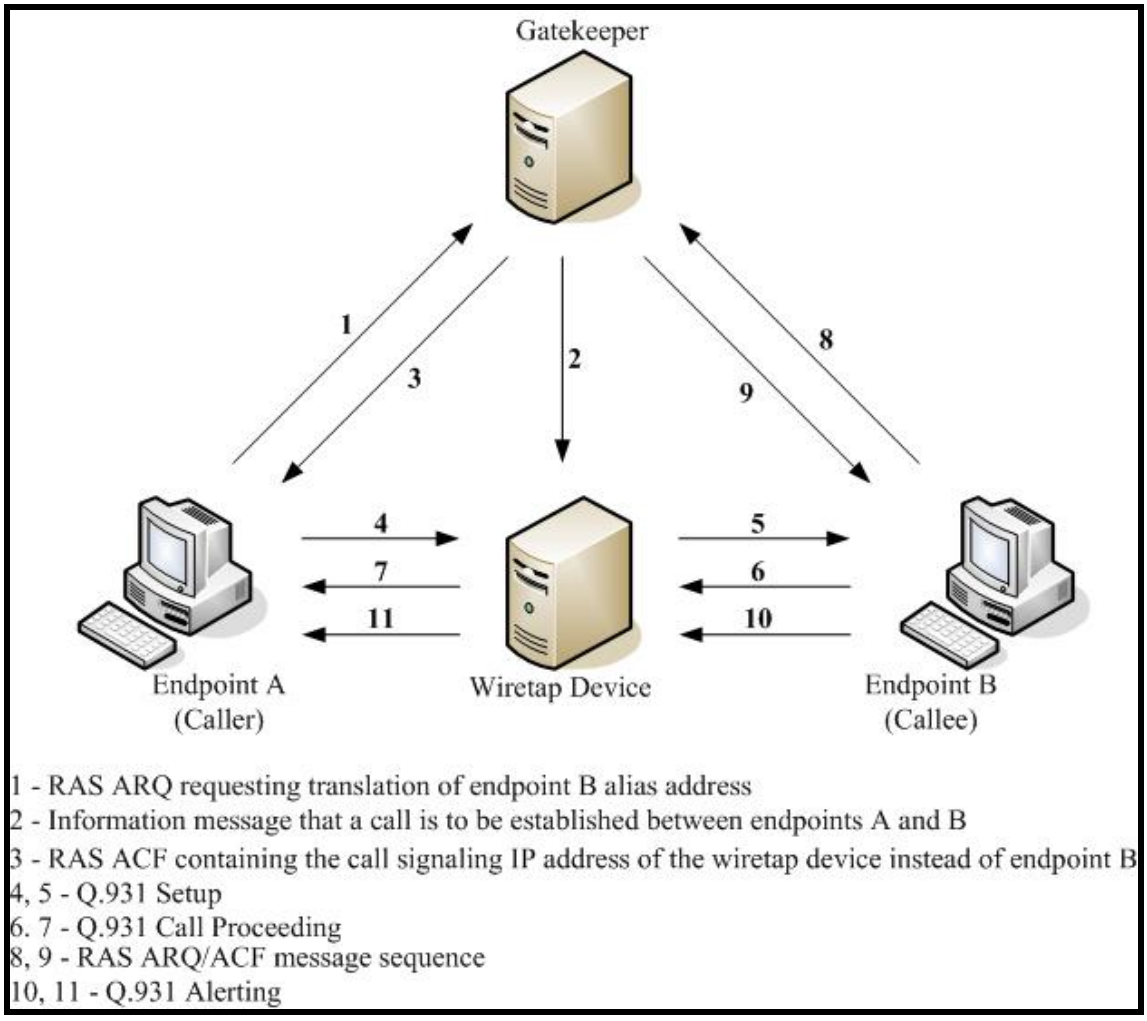

圖 18　H.323 加入監聽之後的通話建立步驟

這個方法需要在 gatekeeper 上做修改，而不需要更動其它 H.323 的設備，gatekeeper 要加入能和監聽設備溝通的功能，另外還要修改 ACF 訊息讓裡面包含了監聽設備的 IP address。不過這個方法有些問題，當通話被監聽時，發話端和受話端是和監聽設備建立

連線，如果有一方知道對方的 IP address，再比對現在建立連線的 IP address，就可以發現二者不相同，這樣監聽就被雙方發現了，另外一點就是這個方法會影響通話品質，在通話建立過程需要比較多的訊息傳送，而當雙方在通話時必須經過監聽設備，可能會增加封包的遺失、延遲等等。用這個方法的好處在於它可以監聽所有 H.323 的通話，而不像之前的方法只能監聽通過匣道器的通話。

3. 固定路徑監聽

這個方法是在 H.323 網路裡面加入一台監聽設備，並且讓所有的通話都一定經過這台監聽設備，無論通話是否需要被監聽，這是爲了要解決第二種方法的缺點，因爲所有的通話都會經過監聽設備，所以通話雙方就無法得知自己是否被監聽，這個方法其實和上一個方法很類似，不一樣的地方在於 gatekeeper 不需要判斷每則通話是否需要導向監聽設備，而是不管三七二十一的把所有通話都導向監聽設備所以也會像上一個方法一樣將通話分隔成二邊，一邊是發話端和監聽設備建立連線，一邊是受話端和監聽設備建立連線，這時候 gatekeeper 送給監聽設備的訊息除了帶有通話雙方的 IP address 之外，也要註明這次的通話需不需要受到監聽，換句話說就是需不需要把通話內容紀錄下來，這也跟上一個方法不太一樣，所以這個方法也需要修改 gatekeeper，以便加入這些功能，這個方法適合用於所有 H.323 通話監聽上面，而且不會被發現，可以說是完全符合合法監聽的要求，但是依然有一個缺點，此方法有可能會降低通話的品質，這個問題還需要想辦法來解決。

4. 隨機處理模式監聽

這個方法是將全部的交換器或是集線器都跟監聽設備做連接，並且這些交換器和集線器都必須讓所有經過它們的封包都複製一份到監聽設備那邊去，這樣一來就可以達到監聽的效果，所以監聽設備必須能夠過濾並取出所有封包的內容，而且它會有一份清單，根據那份清單來判斷哪些通話需要監聽，哪些不需要監聽，因此這台機器需要具備了解各種通訊協定的能力，例如 H.323 或是 RTP 等等的通訊協定都要能夠辨認得出來，這樣才能夠得到通話雙方的 IP address 和通話內容，這種方法有很多優點，它可以用在所有網路電話系統上，並不侷限在 H.323 網路，另外它也不會讓通話雙方發現被監聽，最後一點它解決了通話品質的問題，使用這種方法不會影響雙方通話的品質，一舉解決了之前方法的缺點。不過此方法有一項致命的缺點，就是必須要把監聽設備連接在所有的集線器或是交換器，要達成這個目標是非常困難的一件事，可以說幾乎是不可能的，

另外這個方法也受限於交換器和集線器的能力，當網路流量很大的時候有沒有辦法將所有的封包都複製一份給監聽設備，就算有辦法，最後這台監聽設備能不能過濾並且取出封包內容，判斷是否需要監聽也是一個問題。

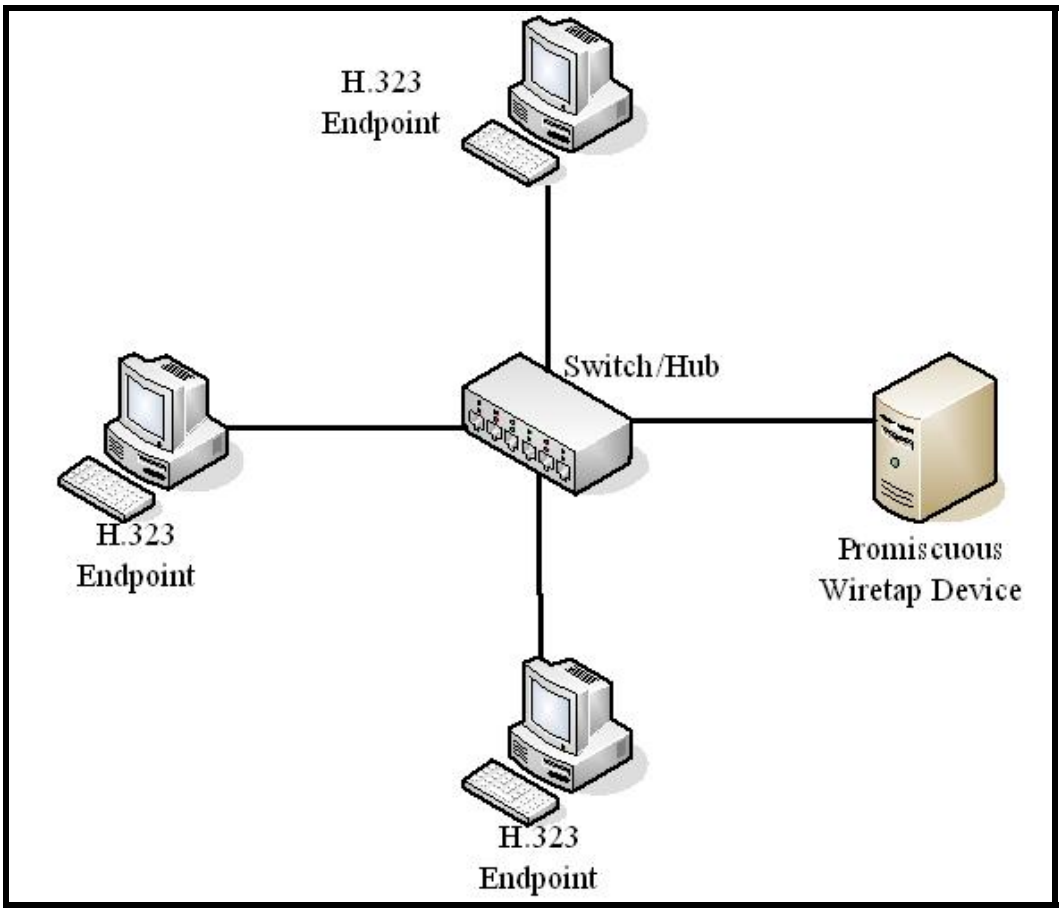

圖 19　Promiscuous 模式監聽設備

最後我們對這四種方法做個結論，第一種方法優點是不會被偵測，通話品質也不受影響，缺點是只能攔截部份通話，第二種方法優點是可以攔截全部通話，缺點是可能會被偵測，而且通話品質會受影響，第三種方法優點爲不會被偵測，也可以攔截全部通話，缺點爲通話品質可能受影響，第四種方法優點爲不會被偵測，也可以攔截全部通話，而且通話品不受影響，缺點爲花費成本太大，在現實世界幾乎是不可行的，表 2 爲四種方法的比較說明：

表 2　四種方法優缺點比較

	在閘道器上監聽	用 Gatekeeper 監聽	固定路徑監聽	隨機處理監聽
偵測性	不會	會	不會	不會
攔截通話	部份	全部	全部	全部

通話品質	不受影響	受影響	受影響	不受影響

3.2 思科提出的 IP 網路合法監聽架構

合法監聽是司法單位合法授權給服務提供者讓他們可以對聲音或是資料做監聽功能，以符合各個國家的法律要求，思科在此提出一個可以提拱 IP 網路合法監聽的架構，它可以提供基本的監聽功能，而在這個架構下監聽得到的資料有二種，一種是通話內容，也就是被監聽者所有的談話都被記錄下來，另一種是監聽相關資訊(Intercept Related Information)，簡稱 IRI，IRI 指的是和監聽目標有相關的資訊[1]，例如雙方的電話號碼，或是監聽目標曾經播過哪些電話等等…。

合法監聽有一些要求需要達成[2]，雖然這些要求可能隨著不同的國家而不同，在這裡列出一些合法監聽的要求：

- 不可以讓監聽對象發現自己受到監聽
- 監聽的裝置要放在安全的地方，不可以讓沒有授權的人任意操作或使用監聽功能
- 可以個別提供 IRI 資訊
- 如果 IRI 和監聽通話內容是分開來傳送，最後要有辦法能夠將兩者合併起來
- 如果服務提供者有對通話內容做加密的話，當他要將監聽結果送到司法單位，他有二種選擇，一種是先將通話內容解密然後送給司法單位，另一種是將通話內容和加密所使用的金鑰送給司法單位，讓司法單位可以對通話內容做解密。
- 如果監聽對象將通話內容做加密，但是服務提供者可以得到加密用的金鑰，那麼服務提供者要將這把金鑰送給司法單位
- 對同一個監聽目標可以同時監聽一個以上的通話
- 在未經授權之下，不可以任意進行監聽，除了監聽目標的通話內容和 IRI 之外，不可以將其它不相關的資訊傳送給司法單位

圖 20 是思科提出的監聽架構圖：

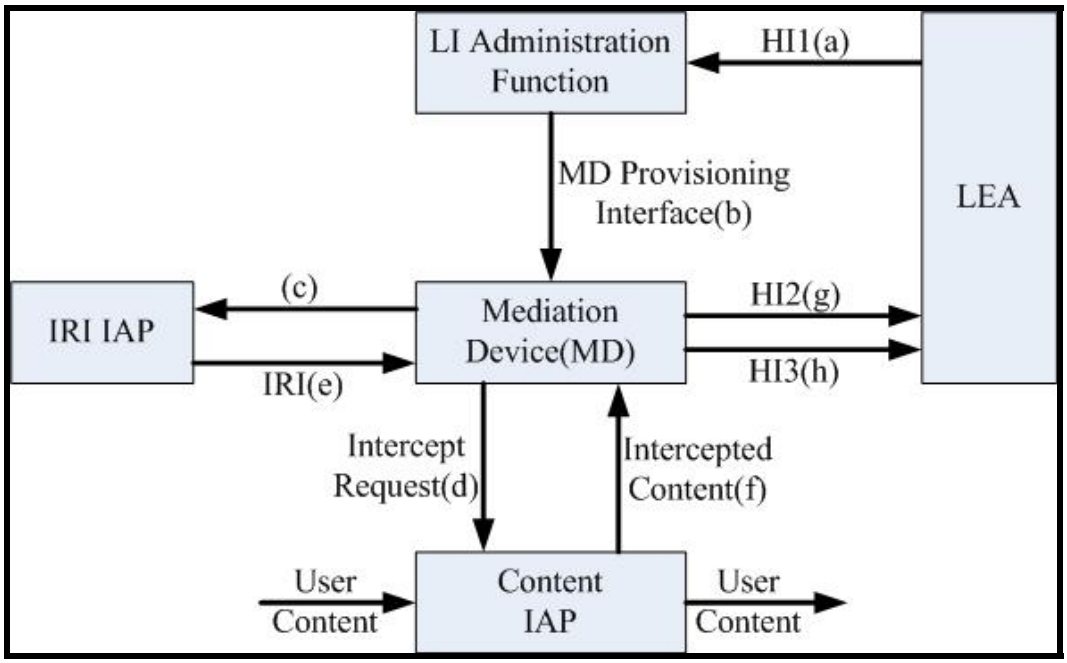

圖 20　監聽架構

再來一一介紹架構中的各個構成要素：

- LI 管理功能(LI Administration Function)：當司法單位得到法院的指令或授權，可以用這個管理功能來執行監聽，對於這個管理功能的使用權必須嚴密控制，任何沒有經過合法授權的人都不能使用此管理功能，從司法單位拿到監聽目標的資料時，通常需要轉換成監聽目標的網路身份才能進行監聽。
- 調解設備(Mediation Device)：MD 要求 IAP 進行監聽，並收集 IAP 回傳的結果，將這些結果轉換成司法單位要求的格式，最後才送給司法單位。
- 監聽設備(IAP)：Intercept Access Point，用來執行監聽動作的設備，可以是原本就有監聽功能的設備或是爲了監聽而新加入的設備。IAP 有二種類型，一種負責提供通話內容，一種負責提供 IRI。
- 通話內容監聽設備(Content IAP)：用來監聽經由 IP 網路傳送通話內容的設備。
- 相關資訊監聽設備(IRI IAP)：用來提供監聽相關資訊的設備。
- 司法單位(LEA)：Law Enforcement Agency，司法單位會送出監聽要求給服務提供者，之後再接收監聽結果。

表 3 是監聽介面的說明表：

表 3　監聽介面

界面(Interface)	說明

(a) HI1	Handover Interface 1 – 管理介面，司法單位經由這個介面傳送監聽資訊給管理功能
(b) MD Provisioning	調解設備(Mediation Device)供應介面，傳送一些參數給 MD，例如：監聽目標的資料、監聽持續時間、監聽類型等等…
(c) IRI IAP Provisioning	爲了取得監聽目標的 IRI 而提供更詳細的監聽目標資料，監聽持續時間等等…
(d) Content Intercept Provisioning	提供資料給負責監聽通話內容的 Content IAP
(e) IRI to MD	負責記錄 IRI 的設備傳送 IRI 給 MD
(f) Content to MD	負責監聽通話內容的設備傳送監聽結果給 MD
(g) HI2	Handover Interface 2 – MD 傳送 IRI 給司法單位的介面
(h) HI3	Handover Interface 3 – MD 傳送通話內容給司法單位的介面

想要進行監聽需要經過合法授權，監聽可以只針對通話內容做監聽，或是針對 IRI 做監聽，或是二者都一起監聽。MD 會收集 IAP 回傳的監聽資料，將這些資料轉換成司法單位要求的格式，再傳給司法單位，有一些問題值得考慮：

- 監聽目標所在位置：有時候在監聽目標尚未註冊之前，無法得知其所在位置，在這種情況下需要 IRI 提供相關位置的資訊(如 IP 位址和 port 號碼)讓通話監聽設備可以進行監聽。
- 通話內容加密：如果通話內容被加密而服務提供者有辦法得到加密用的金鑰，此時可以把金鑰當成 IRI 裡面的資訊送給司法單位，不過，有可能使用者雙方用自己的方式交換金鑰，此時服務提供者無法得知這把金鑰，就算把加密過的通話內容送給司法單位，也因爲無法解密以致於無法得知真正的通話內容。
- 讓監聽目標察覺：合法監聽的一個必要條件是不能讓監聽目標發現自己遭受監聽，假設我們監聽的是一個有經驗的目標，他懂得用 traceroute 指令檢查 IP 位址，他可以發現他自己的用戶端設備(customer premises equipment 簡稱 CPE)有異常的信號，他能夠察覺通話品質降低或是通話莫名其妙中斷。所以我們不會在用戶端設備上動手腳，因爲這麼很容易讓使用者發現，最恰當的通話監聽設備就是路由器(router)或是交換機(switch)，如圖 21 所示。

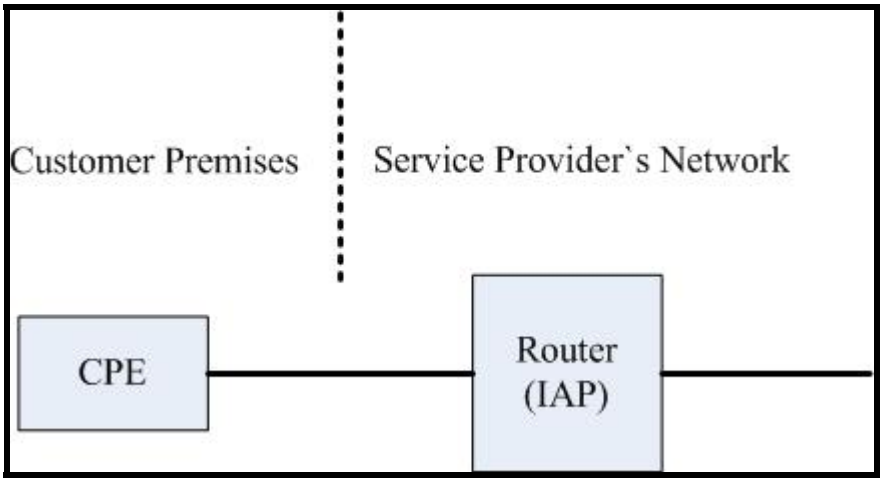

圖 21　通話監聽設備 – 路由器

- 未經授權的使用：通話監聽設備被濫用是一個很嚴重的問題，尤其是路由器被當作監聽設備時，因爲這些路由器有監聽的功能，所以需要做嚴格的管控，記錄(logging)和審查(auditing)是一種方式來檢查是否有未經授權的使用。
- 能力(Capacity)：加入合法監聽的功能之後，不能影響服務品質。

在這一段會針對通話內容監聽介面(d)來做討論，這個介面可以用 SNMPv3(version 3 of Simple Network Management Protocol)這種通訊協定來傳送資料，並建議使用 TAP-MIB，在[8]中會詳細說明爲何使用 SNMPv3 和 MIB 的理由。爲了能提供監聽、複製、封裝、和傳送通話資料的功能，MD 傳送給 Content IAP 的資料裡面應該包含：哪種封包需要被監聽、MD 的網路位址、以及封裝和傳送的格式，除此之外，監聽結束時間也要說明，這樣才不會因爲 MD 發生故障，無法通知 IAP 結束監聽導致監聽超過授權時間限制，MD 也要隨時監視 IAP 的狀況。

思科提出的合法監聽架構也可以用在數據服務上面，這時候的 IRI IAP 就是負責註冊、認證、授權的機器，如 RADIUS 伺服器，IRI 的內容包含使用者註冊的時間、使用者的身份、IP 位址或是其它可以用來監聽的資訊，一旦知道使用者的 IP 位址，就可以對他傳送的資料做監聽，雖然在數據服務的 IRI IAP 跟通話服務不同，但是 content IAP 其本上是一樣的。

爲了要保護監聽目標的敏感資料，隱藏監聽目標的身份，合法監聽必須有足夠的能力對抗一些網路威脅或是攻擊，像是有不法人士扮演 MD 的角色，想要取得監聽資料，或是像僞造訊息(message forgery)和重複傳送攻擊等會侵害隱私和機密的手段，MD 需要特別加以保護，因爲它可能會是最主要受到攻擊的設備。一般來說，所有的介面應該要

有認證和加密的功能，用來確認身份以及防止資料外洩，同樣的也要對訊息做完整性的檢查，以確保沒有不良份子故意竄改原本的訊息，或是防止重複傳送攻擊，其它的 IAP 也是要有保護資料不外洩的功能。

思科提出的合法監聽架構，是大概的說明合法監聽可能需要哪些設備配合，每個設備應該負責做什麼事情，是一般的合法監聽架構，但是細部方面沒有做詳細的說明，也沒有針對網路電話加以討論，所以如果電信業者想要真正應用在現實生活中，還有一段差距。

3.3 歐洲電信標準協會提出的合法監聽架構

歐洲電信標準協會(European Telecommunications Standards Institute 簡稱 ETSI)是歐洲地區的一個標準組織，在 1988 年建立。它建立的主要目地是爲了貫徹歐洲郵電管理聯合會(European Conference of Postal and Telecommunications Administrations 簡稱 CEPT)和歐洲共同體委員會(Commission of the European Communities 簡稱 CEC)確定的電信政策。

在這篇技術報告[14]中討論合法監聽在公共通訊服務中扮演什麼樣的角色、合法監聽的基本要求、對於存取服務監聽的討論、對於應用服務監聽的討論、對於智慧型網路監聽的討論、以及安全性的討論等等。

在原本的架構下增加合法監聽的功能，有一些原則需要遵守，不能影響原本服務的功能和品質，不能更改原本的架構，圖 22 是合法監聽的參考模型[17]。

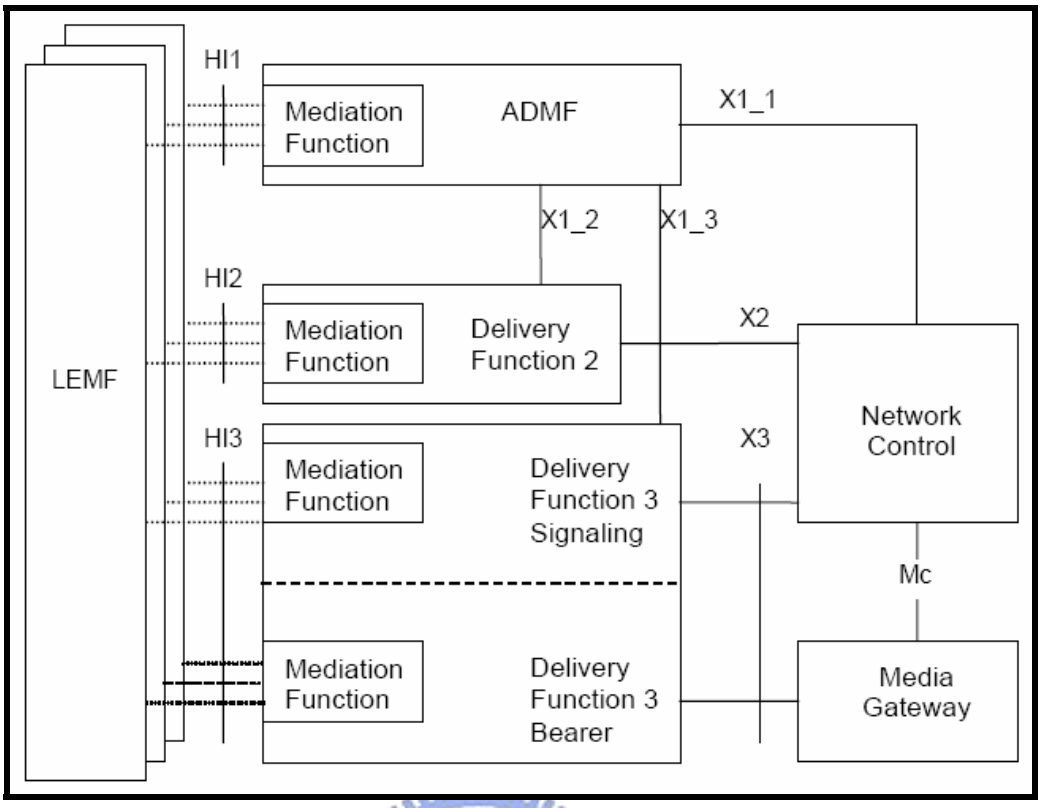

圖 22　合法監聽的參考模型圖

參考模型圖各部份說明如表 4 所示，是由[15][16]所定義：

表 4　參考模型圖的說明

名　稱	說　　明
LEMF	Law Enforcement Monitoring Facility，負責收出監聽要求以及接收監聽結果
ADMF	ADMinistration Function，是一個管理功能，它負責接收 HI1 送來的資料，經由 X1 傳送命令給網路設備要求監聽，並將監聽結果回傳給 MD/DF
Mediation Function	中介功能，負責將存取提供者(access provider)或是網路經營者(network operator)或是服務提供者(service provider)送來的資料傳給交遞介面
Delivery Function	傳送功能，傳送監聽結果給 LEMF
HI	Handover Interface，交遞功能，在 AP/NWO/SvP(電信服務提供者)和 LEMF 之間傳送資料的介面
X	Internal interface，電信內部網路介面

建立一個電信標準需要花很多時間，每處環節都要仔細思考，以合法監聽的標準來說，有許多組織參與制定標準，像是：國家司法代表、電信設備製造商、電信服務業者、第三方業者等等，國際標準會受到各個國家的規定影響，各個國家的規定是基於各國的法律和適合的標準，電信設備製造商會根據國際標準，再部分參考各國的規定來生產他們的合法監聽設備，電信業者必須符合國家的規定才可以營業，司法單位則是根據法律來進行監聽，圖 23 就是要說明制定標準的過程。

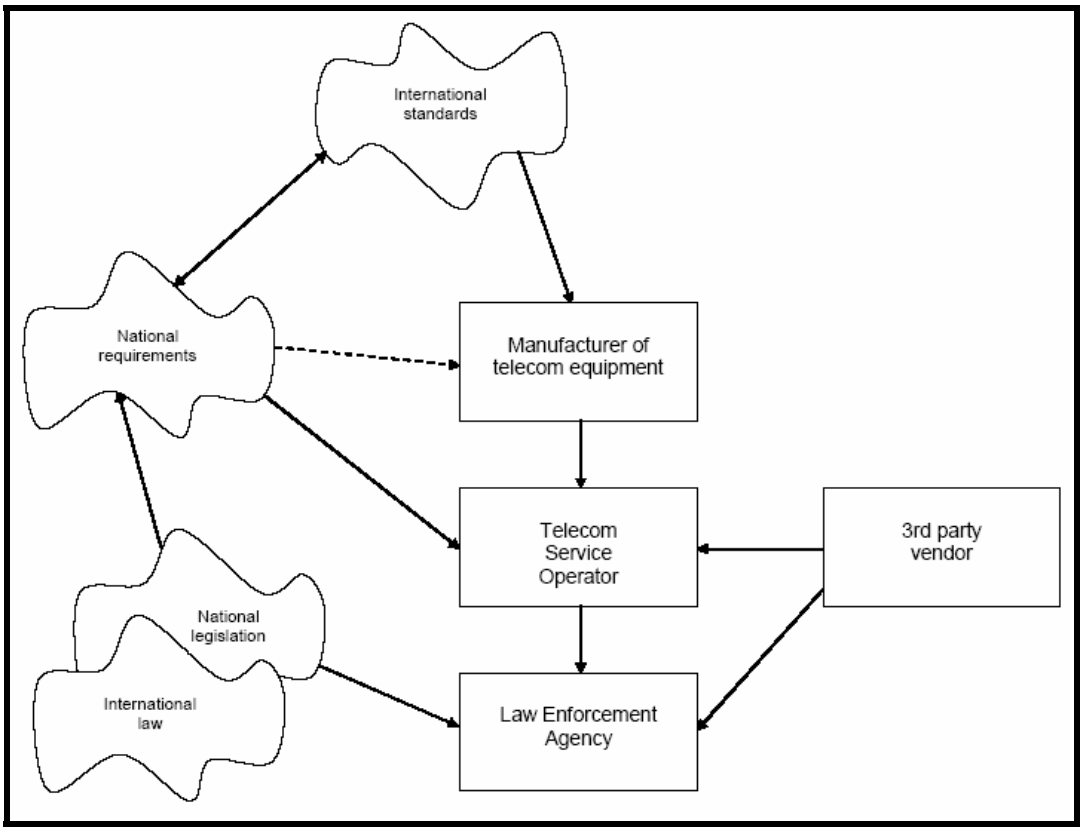

圖 23　制定標準的過程

隨著技術的進步，現在提供一項服務，背後可能用了好幾項不同的技術，因此可以用一個三層式的模型來表示，這三層可以套用到合法監聽系統上面，首先合法監聽系統可以利用服務層(Service Layer)來確認使用者的身份，利用控制層(Control Layer)來取得使用者的 IRI，利用連接層(Connectivity Layer)來拿到使用者的通話內容。如圖 24 所示，首先服務層提供使用者身份資料給監聽系統，當監聽系統發現有使用者需要監聽時，它會送出一個監聽要求給控制層，一旦控制層收到這個監聽要求，就會開始把監聽目標的 IRI 傳送給 MF/DF，然後控制層會送一個訊息給連接層，要求連接層將監聽目標的通話

內容複製一份給 MF/DF 或是直接送到 LEMF 那邊去。

表 5　三層式模型的說明

名　稱	說　　明
Service Layer	服務層，負責提供特定服務，像是網路存取服務、電話服務或是電子郵件服務，通常在這一層也會有認證、授權和結帳(Authentication, Authorization and Accounting 簡稱 AAA)的功能
Control Layer	控制層，接收服務層傳來的要求，用一些方法來提供上一層的服務
Connectivity Layer	連接層，接收控制層傳來的要求，建立服務所需要的連線

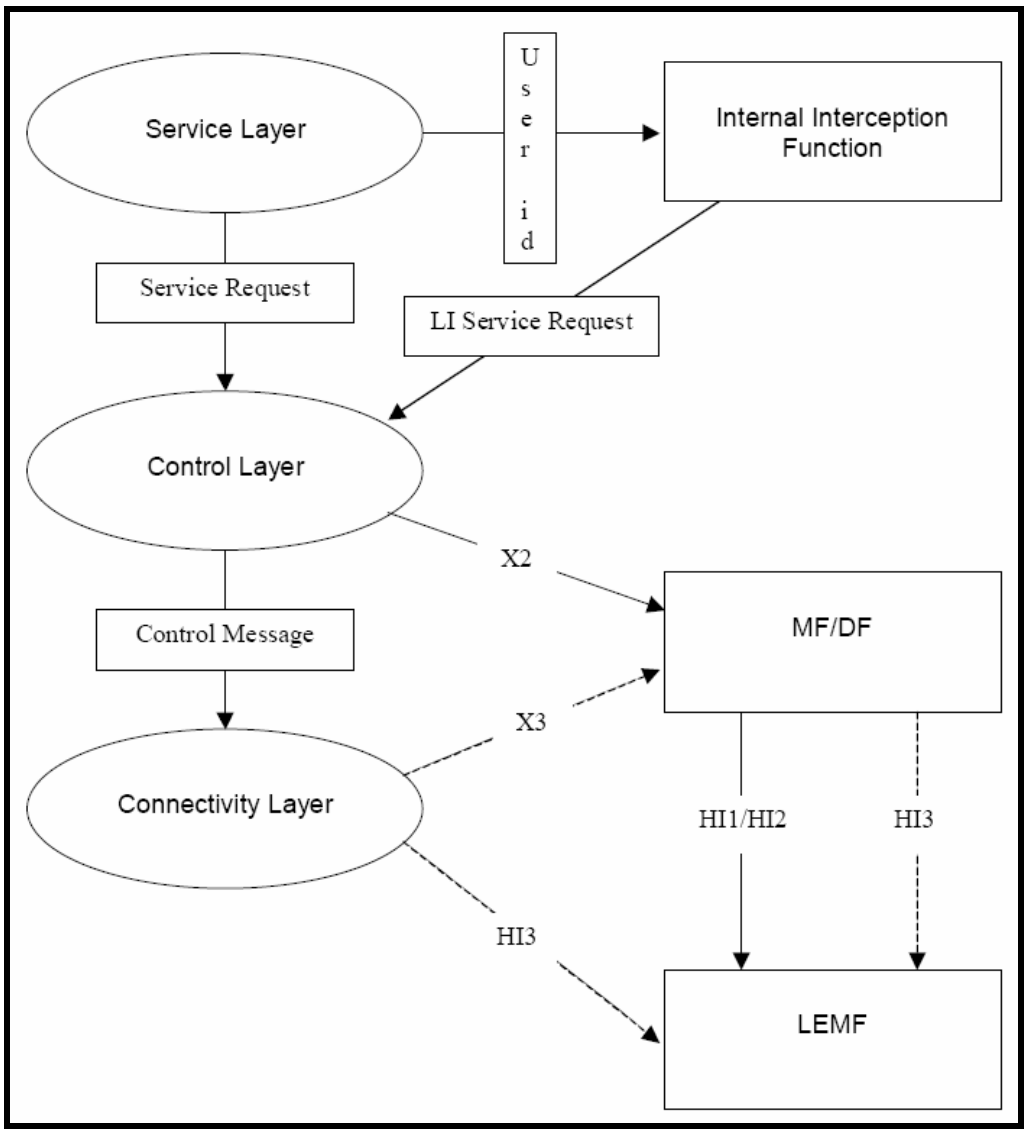

圖 24　合法監聽和三層式模式的關係

在合法監聽架構中，安全性也是值得重視的部份，爲了防止監聽系統遭受不良份子

的入侵或破壞，或是監聽資料被有心人士取得，一定需要有非常完善的安全機制來保護監聽架構，常見的危險[18]有僞裝成合法使用者來取得帳號密碼，得到控制權，從中取得監聽資料或是篡改監聽資料，或是用 DoS(Denial of Service)攻擊，試圖癱瘓合法監聽的功能，這些攻擊方法如圖 25 所示：

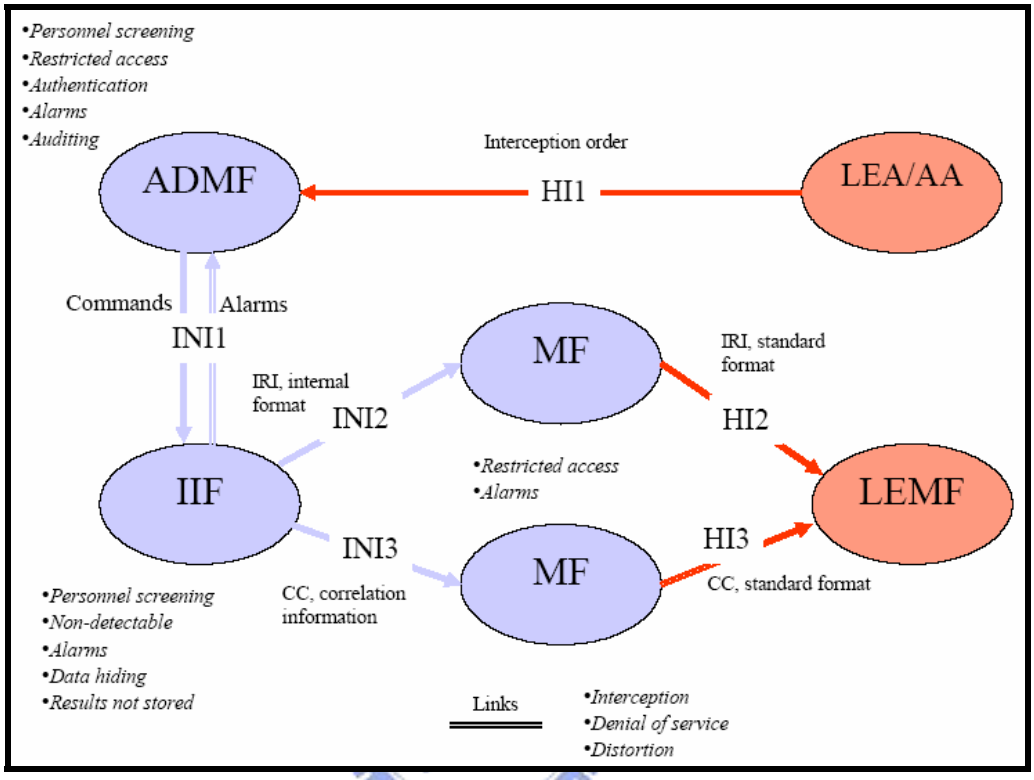

圖 25　合法監聽系統所受到的威脅

所以要加強系統的安全性，來防止系統被入侵或是破壞，在監聽資料方面，必須將資料做加密，這樣就算資料被不良份子以非法手段取得，他們也無法得知裡面的內容，另外在控制權限方面，存取合法監聽系統要經過嚴格的認證和授權才可以使用，而人員進出也要受到控制。

歐洲電信標準協會提出的合法監聽架構，和思科提出的很類似，其實思科也是參考歐洲電信標準協會的合法監聽架構才提出自己的架構，思科將調解設備獨立出來成爲一個設備，所以看起來比較簡單明瞭，歐洲電信提出的架構也是一般性的架構，所以也沒有針對網路電話做更進一步的說明，所以真正應用在網路電話上還是需要更多的討論和問題克服。

第四章、以 SIP 架構為基礎之合法監聽功能

4.1 系統簡介與假設

我們提出的系統架構結合了本編論文 3.2 小節中思科(Cisco)提出的合法監聽架構和本編論文 2.3.3 小節中 SIP 網路協定的架構，讓使用 SIP 網路協定建立的網路電話可以提供合法監聽的功能。

而且這個架構符合合法監聽的三項要求：第一項要求是不會讓監聽目標發現自己受到監聽；第二項要求是假如司法單位除了要監聽通話內容，還需要監聽相關資訊的話，必須要提供給司法單位；第三項要求是監聽結果有加密的話，必須提供加密的金鑰給司法單位。

除此之外我們提出的架構也有安全性，並假設使用者傳送出來的所有 SIP 訊息一定會經過 SIP 代理伺服器，而且使用者需要認證才可以使用網路電話的服務，也就是說使用者撥打電話給對方，或是從對方接受電話，一定要先經過認證並通過才可以，這個假設符合電信業者的營運目的，因爲這麼做的話，電信業者才能知道客戶打了多少電話，到時候有依據來計算通話費，電信業者才能收到錢，也可以提供合法監聽的功能，可以說是一舉二得，圖 26 說明 SIP 合法監聽網路示意圖。

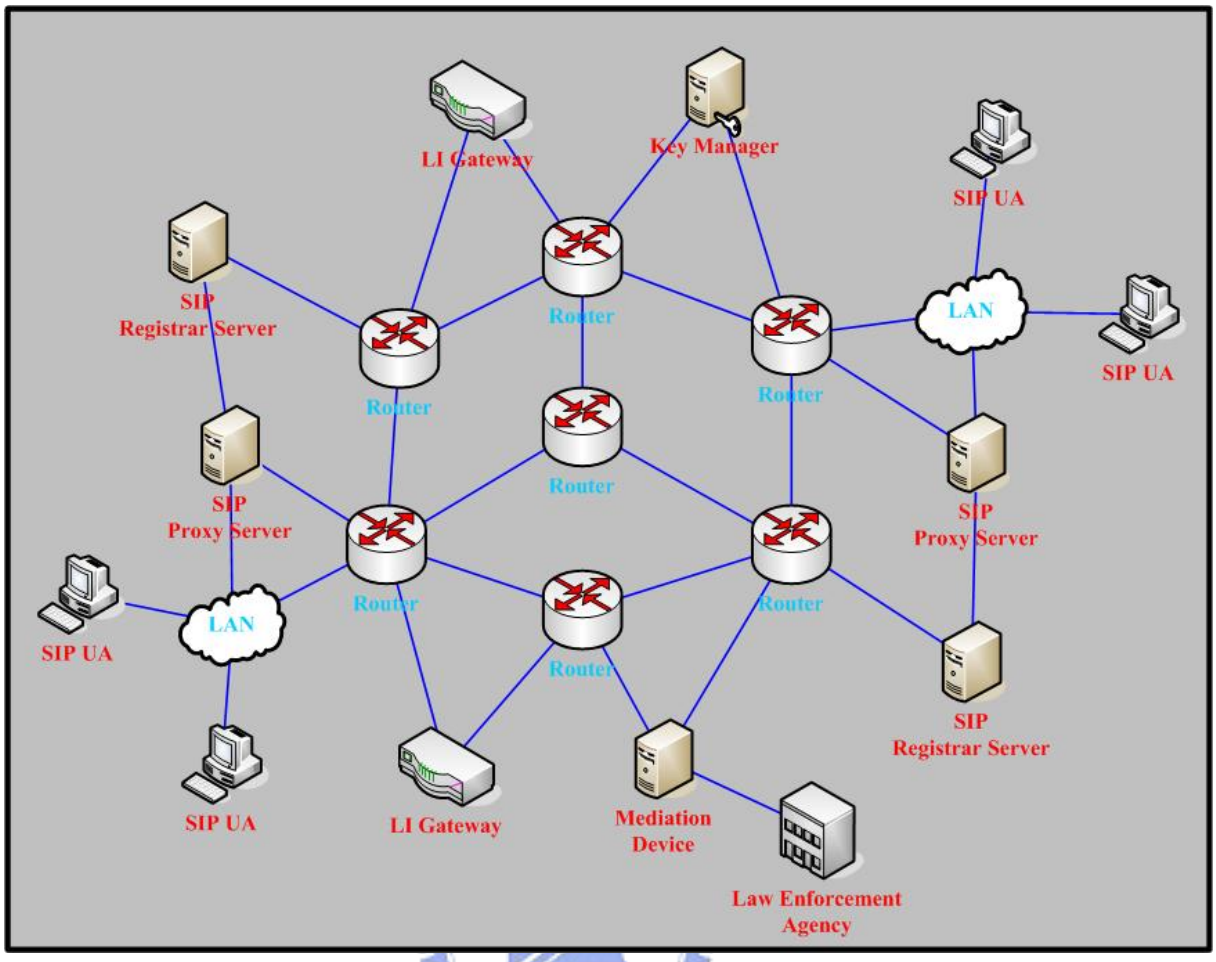

圖 26　SIP 合法監聽網路示意圖

4.2　系統架構

在這裡我們提出的系統架構是參考思科提出的合法監聽架構以及 SIP 網路協定架構，架構中有七種元件，每種元件負責不同的功能，我們會在後面做進一步的說明，我們的架構的元件有司法單位 LEA(Law Enforcement Agency)、合法監聽管理功能(LI Administration Function)，和調解設備(Mediation Device)、SIP 註冊伺服器(SIP Registrar Server)、SIP 代理伺服器(SIP Proxy Server)、合法監聽閘道器(LI Gateway)、金鑰管理元件(Key Manager)，金鑰管理元件是爲了讓系統更有安全性，這個元件的功能是管理合法監聽中將通話內容加密用的金鑰，可以說是非常重要的功能，後面我們會做更詳細的介紹。

在最後司法單位要求監聽結果中的監聽相關資料，我們可以從 SIP 代理伺服器(SIP

Proxy Server)取得，當 SIP 建立通話成功之後，我們會將被監聽的通話導向合法監聽閘道器(LI Gateway)，這個閘道器負責收集通話資料，並將監聽結果送到調解設備，再由調解設備把結果轉換成司法單位所要求的格式，最後就會把監聽結果送到司法單位手中，所以監聽結果中的通話內容，我們可以從合法監聽閘道器取得。

當這個架構運用在使用 SIP 網路協定建立網路電話上時，我們就可以讓 SIP 提供合法監聽的功能，而且不會更改原本 SIP 的架構，除了可以提供合法監聽的功能之外，這個架構也可以讓提供網路電話服務業者向網路電話客戶收取使用費，如何能達成這個目的，在於我們假設所有的 SIP 訊息都會經過 SIP 代理伺服器，所以每一通網路電話的建立時間和結束時間都會被記錄在這台 SIP 代理伺服器，網路電話服務業者就可以用這個記錄向每位客戶寄發帳單，依照客戶使用情形收取服務費。

在這裡舉一個例子來說明 SIP 架構加上合法監聽架構情形，如圖 27 所示：

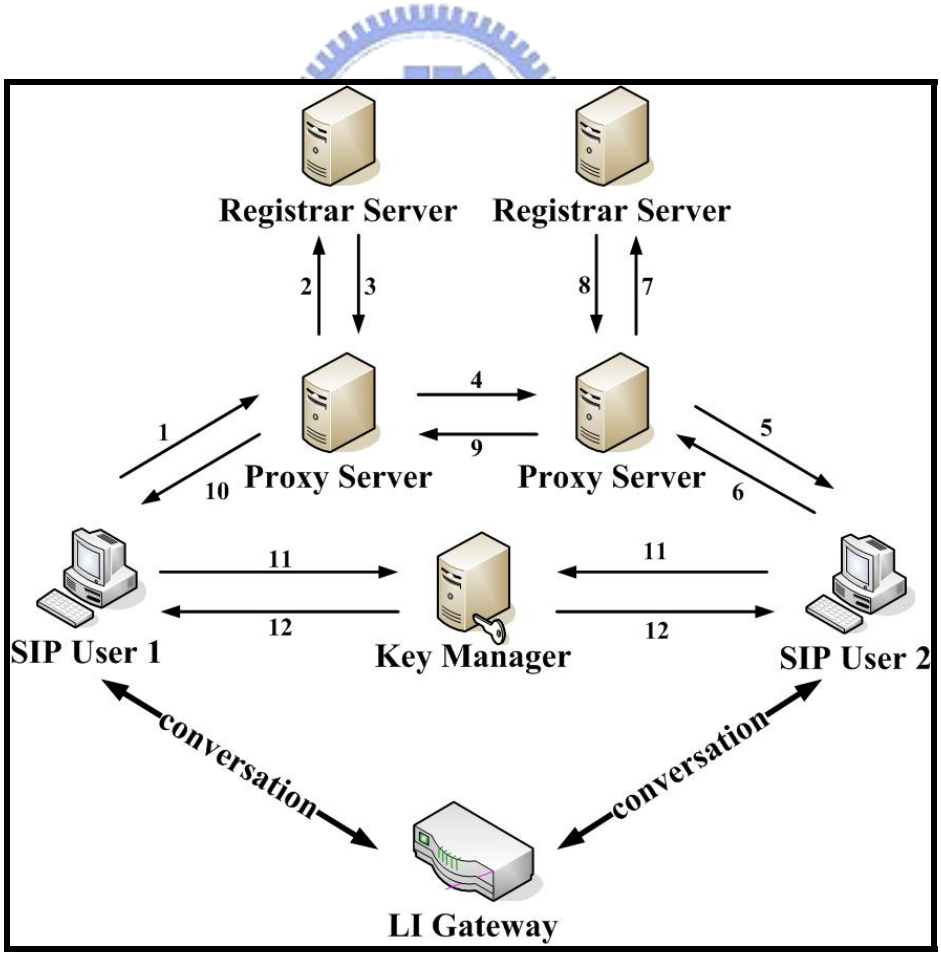

圖 27　SIP 結合合法監聽的範例

一開始 SIP 使用者 1(SIP User 1)想要打網路電話給 SIP 使用者 2(SIP User 2)，使用者 1 會發出 INVITE 的 SIP 訊息(1)，代理伺服器(Proxy Server)收到訊息之後，會向註冊伺服器(Registrar Server)確認使用者 1 的認證資料(2,3)，認證通過並且經過授權之後，代理伺服器才可以讓使用者 1 打網路電話，再來會將 INVITE 訊息傳送到使用者 2 那邊的代理伺服器(4)，代理伺服器再將訊息傳送給使用者 2(5)。

如果使用者 2 想要回應這通網路電話，會回傳一個 OK 的訊息(6)，代理伺服器接收到使用者 2 的訊息，同樣會向註冊伺服器確認使用者 2 的認證資料(7,8)，確定使用者 2 是合法使用者並且確定有權限可以接這通網路電話之後，才會將 OK 的訊息傳送給使用者 1 那邊的代理伺服器(9)，代理伺服器再將訊息傳送給使用者 1(10)，同時會指定使用者 1 和使用者 2 到時候通話所使用的 RTP 連線要和哪一台合法監聽閘道器做連線。

接下來使用者 1 和使用者 2 會需要加密通話用的金鑰，而這把金鑰是由金鑰管理元件(Key Manager)所產生並且維護，金鑰管理元件負責管理所有 SIP 建立通話之後將通話加密所用的金鑰，可以說是非常重要的部份，所以需要安全的控管。使用者 1 在和使用者 2 建立通話連線之前，會先跟金鑰管理元件建立加密的連線(11)，例如用 Diffie-Hellman 或是 RSA 交換金鑰，使用者 2 同時也跟金鑰管理元件建立加密的連線(11)，接著金鑰管理元件會把之後通話加密所使用的金鑰傳送給使用者 1 和使用者 2(12)。

最後使用者 1 和使用者 2 都會跟合法監聽閘道器建立連線，這時候使用者 1 和使用者 2 就可以開始通話，而且這些通話都會用金鑰管理元件所產生的金鑰來加密，也就是說合法監聽閘道器所監聽的通話是經過加密的，這樣可以防止電信業者想要取得監聽內容。

在我們的架構中，原本思科的監聽相關資訊監聽功能(IRI IAP)會被 SIP 網路協定中的 SIP 代理伺服器所取代，而通話監聽功能(Content IAP)則會被我們提出的合法監聽閘道器(LI Gateway)所取代，爲了讓司法單位可以解密監聽結果，金鑰管理元件會將通話加密金鑰送到調解設備，再由調解設備送給司法單位，可是通話加密金鑰在網路上傳送，有可能會被有心人士從中攔阻，想辦法破解這把金鑰，爲了讓本系統可以更有安全性，於是我們將金鑰管理元件和調解設備合而爲一，這樣就可以降低通話加密金鑰在網

路上傳送的風險。

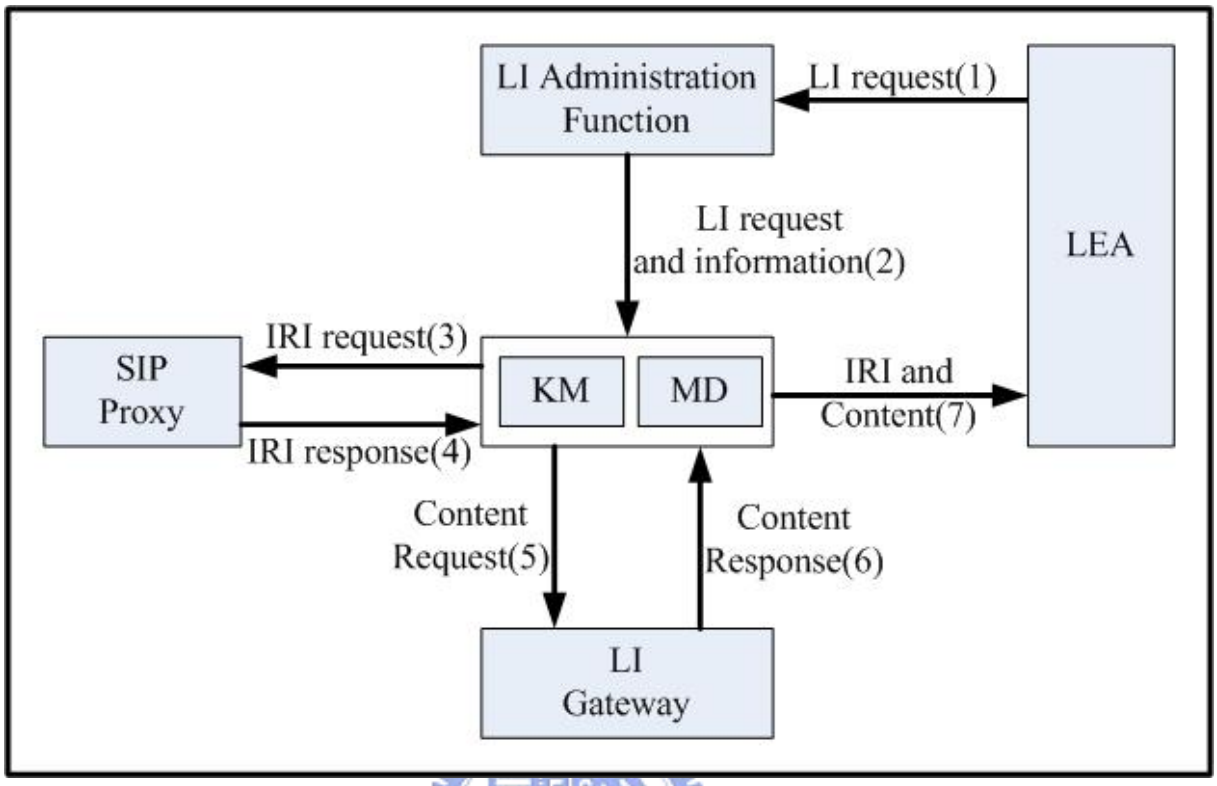

圖 28　系統架構圖

圖 28 是我們的系統架構圖，當司法單位從法官或是檢察官那裡取得通訊監察書之後，就可以開始執行監聽流程，一開始司法單位發出合法監聽要求給合法監聽管理功能(1)，合法監聽管理功能是一個使用介面，可以讓司法單位設定監聽的要求格式，如監聽目標的資料、監聽時間，以及監聽回傳結果的要求格式等等。

合法監聽管理功能收到司法單位的監聽要求之後，會把監聽的格式和要求傳送給調解設備(2)，調解設備接收到資料之後，就開始執行監聽的流程，他會先判斷使用者所在的網路負責的 SIP 代理伺服器，發出監聽相關資訊的要求(3)，因爲 SIP 代理伺服器會紀錄 SIP 使用者所傳送過的訊息，所以它可以提供監聽通話的建立時間、結束時間、持續時間、IP 位址等等監聽相關資料，最後再將結果回傳給調解設備(4)。

在 SIP 通話建立成功而且通話雙方準備開始傳送語音資料時，金鑰管理元件會和通話雙方建立安全連線(如：RSA 或 Diffie-Hellman)，並產生一把通話加密金鑰，利用安全連線將金鑰傳送給通話雙方，這時候調解設備會發出通話監聽要求給合法監聽閘道器

(5)，告訴合法監聽閘道器 LI ID 以及監聽結果回傳位址，此時合法監聽閘道器就會開始複製監聽通話，並將複製結果回傳到調解設備(6)，最後調解設備會把監聽相關資訊和監聽通話結果收集起來，並把結果轉換成司法單位要求的格式，最後將這些監聽結果回傳給司法單位(7)，同時因爲金鑰管理元件和調解設備合而爲一，所以調解設備也可以知道通話加密金鑰的內容，所以回傳的監聽結果也會包含這把通話加密金鑰，有了這把通話加密金鑰，司法單位可以把加密的監聽結果解密，得到法庭上所需要的監聽內容。

4.3 系統元件

在我們的架構中，每個元件所負責的功能以及動作，我們會一個一個作詳細說明，下面我們分在 SIP 相關元件以及合法監聽相關元件分別說明：

4.3.1 SIP 相關元件

在我們的架構中會用到 SIP 網路協定中 SIP 代理伺服器以及 SIP 註冊伺服器，其中 SIP 代理伺服器需要做一些修改。

SIP 註冊伺服器(SIP Registrar Server)

SIP 註冊伺服器負責 SIP 使用者的註冊以及認證的動作，當 SIP 使用者一開始使用 SIP UA 的時候，SIP UA 就會自動連上網路尋找適當的註冊伺服器以進行註冊，註冊的內容包含了使用者的 SIP URI、使用者的 IP 位址，使用者所訂購權限等等，有了這些註冊的資訊，在網路上有人想打電話給這位使用者，就可以根據使用者的 SIP URI 由這台註冊伺服器取得這位使用者的 IP 位址，如此一來 SIP UA 才知道 INVITE 訊息要送到哪裡。

當使用者想撥打網路電話或是想接受網路電話時，同樣的也需要先經過 SIP 註冊伺服器的認證和授權，圖 29 說明 SIP 使用者註冊以及認證過程。

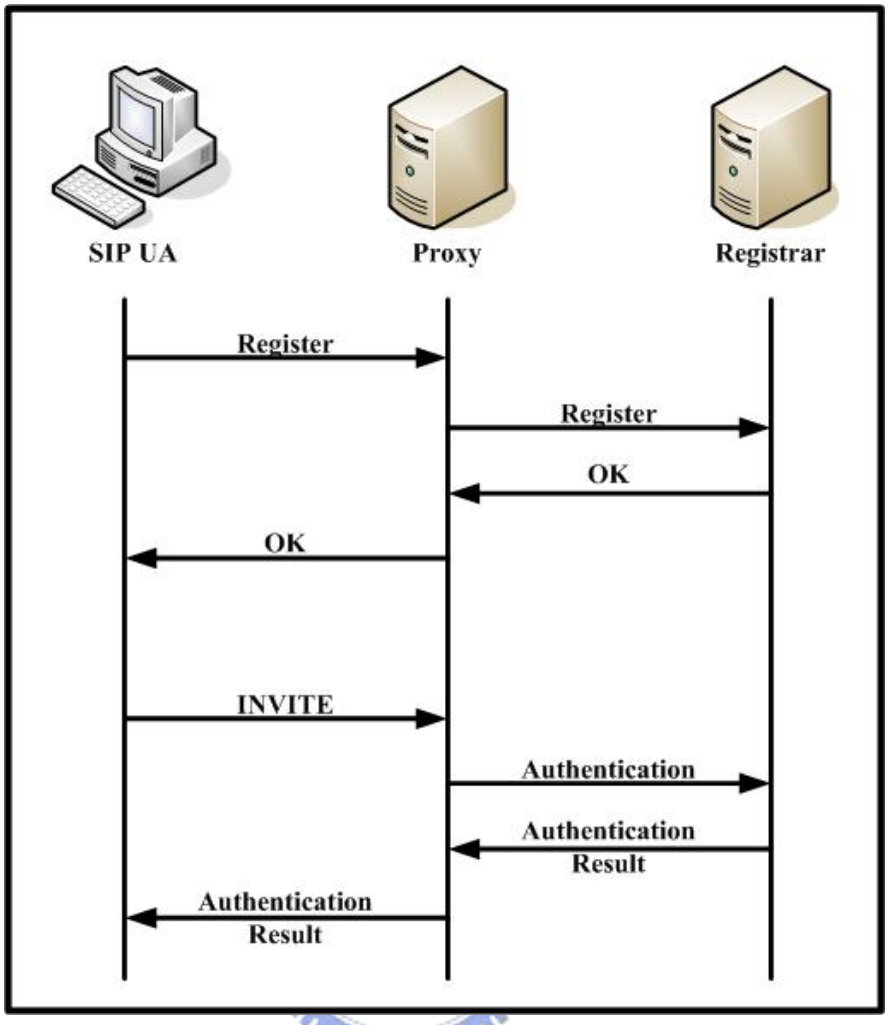

圖 29　SIP 使用者註冊和認證

SIP 代理伺服器(SIP Proxy Server)

SIP 代理伺服器負責傳送 SIP 使用者的訊息，類似 WWW 代理伺服器的功能，當使用者發出 SIP 的訊息或是接收 SIP 的訊息，都是由代理伺服器幫忙傳送接收，當使用者想撥打網路電話但是不知道對方的 IP 位址時，代理伺服器也會負責詢問註冊伺服器，在得知對方的 IP 位址之後將訊息傳送到正確的地方。

在我們的合法監聽架構下，SIP 代理伺服器除了要完成 SIP 原本所擁有的功能之外，還有一項重要的目的，代理伺服器要提供監聽相關資訊給調解設備，這是原本所沒有的功能，爲了要完成這個目標，代理伺服器要做一些修改，首先它必須要記住監聽通話的建立時間、結束時間、持續時間、IP 位址、還有使用者曾經撥打給哪些人，成功多少通

話、失敗多少通話等等，這些都是對司法單位在偵辦案件時很可能用得到的資訊，這些資訊最後都要整理傳給調解設備，讓調解設備將這些監聽相關資訊送到司法單位 LEA 那裡，圖 30 說明監聽相關訊息的傳送流程。

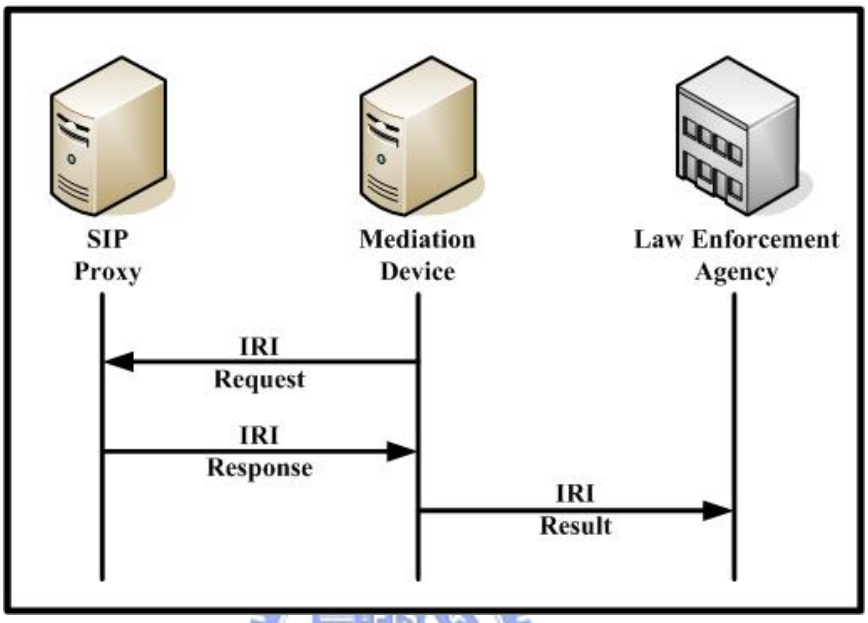

圖 30　SIP 代理伺服器傳送 IRI 流程

SIP 代理伺服器的另外一項功能就是指定 SIP 使用者通話 RTP 連線和哪一台合法監聽閘道器連接，當 SIP 的訊息最後出現 OK 的時候，SIP 代理伺服器就會在這個訊息裡面加入合法監聽閘道器的 IP 位址，如此一來 SIP 通話時的 RTP 連線就會和合法監聽閘道器做連接，可以監聽雙方的通話。

4.3.2　合法監聽相關元件

在我們系統架構中合法監聽有關的元件有合法監聽管理功能(LI Administration Function)、調解設備(Mediation Device)、金鑰管理元件(Key Manager)、合法監聽閘道器(LI Gateway)，以下一個一個做詳細說明：

合法監聽管理功能(LI Administration Function)

合法監聽管理功能爲司法單位執行監聽的使用介面，司法單位藉由這個管理功能輸

入監聽目標的資料、監聽時間，以及監聽回傳結果的要求格式，當司法單位得到法院的指令或授權，可以用這個管理功能來執行監聽，對於這個管理功能的使用權必須嚴密控制，任何沒有經過合法授權的人都不能使用此管理功能，從司法單位拿到監聽目標的資料時，通常需要轉換成監聽目標的網路身份才能進行監聽，例如監聽目標的 SIP URI 或是 IP 網路位址。

調解設備(Mediation Device)

調解設備是合法監聽管理功能和真正執行監聽的元件之間的溝通橋樑，當它接收合法監聽管理功能傳來的監聽要求，它會根據要求指定監聽目標所在的 SIP 代理伺服器提供監聽相關資料，以及網路電話通話經過的合法監聽閘道器執行通話監聽的動作，調解設備收集代理伺服器回傳的監聽相關資料，和合法監聽閘道器回傳的監聽通話資料，會將這些資料轉換成司法單位要求的格式，再將監聽結果回傳給司法單位。這個設備要有安全的防護，如果讓網路入侵者取得這台設備的使用權限的話，將會造成非法監聽，侵犯到個人的隱私權，圖 31 表示調解設備訊息流程。

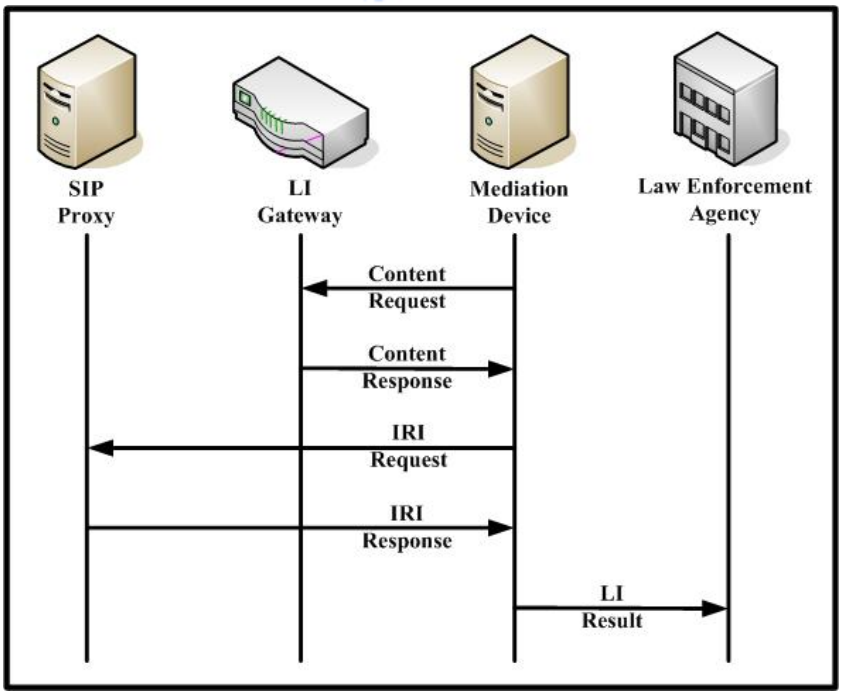

圖 31　調解設備傳送監聽資料流程

合法監聽閘道器(LI Gateway)

在 IP 網路環境中，資料傳送的路徑可能不固定，這是封包交換(Packet-Switched)的一項重要的特性，和電路交換(Circuit-Switched)最大的不同點，這項特點有好處也有壞處，好處在於可以節省網路使用頻寬，封包交換不像電路交換會佔用整條線路，在一條線路上可能有不同的封包在傳送，充分利用網路的資源，也大大的節省成本，所以 IP 網路才會快速的發展起來。

爲了能監聽網路電話，我們在網路上新增一個元件叫做合法監聽閘道器，然後將受到監聽的道話全部導向這台閘道器，合法監聽閘道器負責監聽通話內容，首先金鑰管理元件會傳送監聽資料給合法監聽閘道器，這份資料包含了合法監聽的編號、通話雙方的 IP 位址、監聽結果回傳 IP 位址，接著合法監聽閘道器會跟通話雙方建立連線，此時通話雙方會開始傳送語音資料，合法監聽閘道器會把通話雙方傳送過來的語音資料複製一份下來，最後會將這些語音資料，也就是監聽通話內容傳送到調解設備，由調解設備整合結果之後傳送到司法單位手中。

金鑰管理元件(Key Manager)

爲了加強網路電話的安全性，所有在網路上傳送的通話語音封包都應該要加密，這樣可以確保個人隱私，就算語音封包被有心人士從中攔截，因爲沒有加密的金鑰，也無法還原語音資料，可是這讓合法監聽無法執行，假如監聽的封包經過加密，就算將這些封包送到司法單位，司法單位沒有加密的金鑰，就無法解讀這些語音封包，造成無法監聽，爲了要讓網路電話既有安全性又可以合法監聽，我們加入了金鑰管理元件這個設備，以達成我們的目標。

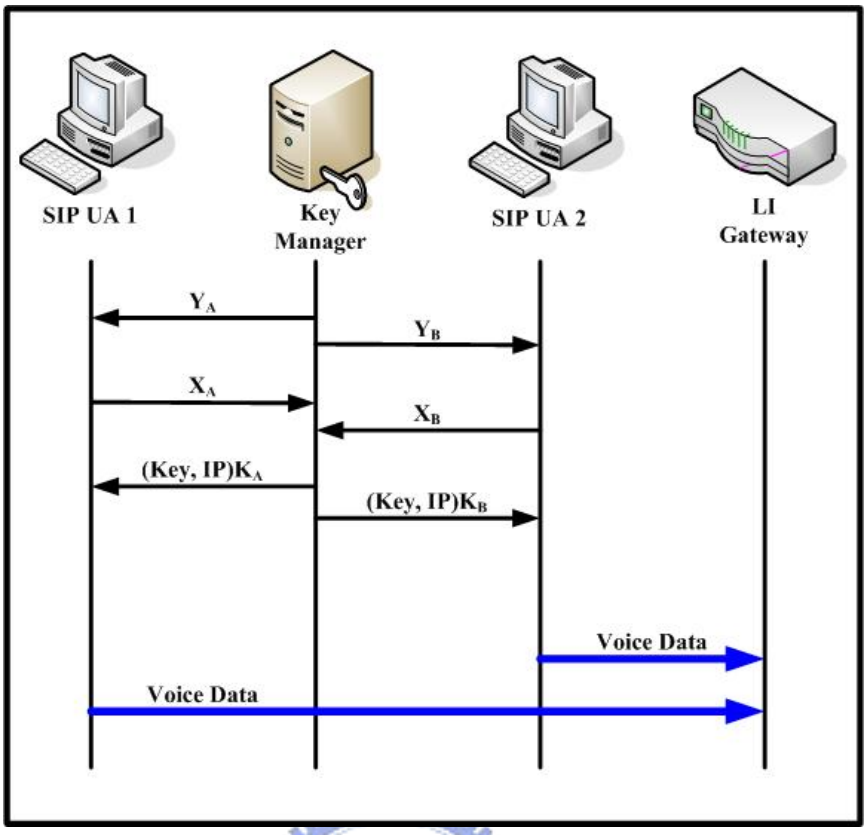

圖 32　金鑰管理元件訊息流程圖

金鑰管理元件的功能是負責產生網路電話通話加密的金鑰，並且管理所有網路電話通話使用的金鑰，當使用者成功建立網路電話之後，在還沒開始傳送語音資料之前，通話雙方會先跟金鑰管理元件建立安全的連線，可以用 Diffie-Hellman 或是 RSA 等等方法建立安全連線，建立安全連線之後，金鑰管理元件會產生一個通話加密金鑰，並透過安全連線傳送給通話雙方，通話雙方必須用這把金鑰加密通話，金鑰管理元件可以說是非常重要的系統元件之一，必須要做嚴格的管控以及使用認證，訊息流程如圖 32 所示。

4.4　系統安全性與可行性

4.4.1　安全性

我們提出的合法監聽系統架構中，金鑰管理元件和調解設備是最重要的一環，金鑰管理元件負責產生網路電話通話加密用的金鑰，並且管理所有目前還在使用網路電話通話的金鑰，而調解設備則是負責要求監聽相關資訊和監聽通話內容的設備，所以這二種

元件都需要有很高的安全性，不可以讓沒有經過授權的人存取這二種元件，最好這些元件是屬於公正的第三方那邊，這樣也可以避免電信業者可以輕易的存取或是控制這二種元件。

通話加密

在網際網路中，爲了讓在上面傳送的封包內容不外洩，最常用的方法就是將封包做加密，加密過的封包，就算被有心人士從中攔截，也很難將封包資料還原，所以現在有許許多多的加密方法和標準可以使用，但是對於合法監聽來說，如果封包經過加密，而沒有加密的金鑰的話，就無法得到原本封包的內容，也不能過達到合法監聽的目標，因此在合法監聽的架構之下，除了因爲安全性而將封包加密之外，還要讓合法監聽架構知道加密用的金鑰才算是符合合法監聽的目標。

在我們的合法監聽架構之下，所有網路電話的通話，都會被金鑰管理元件產生的金鑰加密，所以在傳送過程就算被有心人士取得，也無法知道裡面的內容，同時也可以防止電信業者取得監聽結果，因爲電信業者也拿不到加密所使用的金鑰，這把通話加密金鑰只有通話雙方，以及金鑰管理元件才知道，而金鑰在網路傳送過程是用加密的方式傳送，所以除了三方之外沒有其它人可以取得這把通話加密金鑰，所以可以保證通話內容是安全的。

司法單位或電信業者單方面無法監聽

最後監聽結果送到司法單位那邊，司法單位會需要通話加密金鑰來將監聽通話內容解密，以取得真正的通話內容，可以當作法庭上的證據，所以金鑰管理元件必須將通話加密金鑰送到司法單位，但是爲了防止司法單位沒有經過授權而任意監聽，我們會將通話加密金鑰用電信業者和司法單位的公開金鑰做二次加密，到時候解密的時候也需要電信業者和司法單位的私密金鑰解密，這樣就可以防止司法單位單方面的任意監聽，因爲要解密時還需要電信業者的私密金鑰。

4.4.2 可行性

我們提出的合法監聽系統架構，可以符合合法監聽的要求，合法監聽有三項要求需要符合，第一項是不能讓監聽目標發現自己受到監聽，第二項是除了提供通話監聽內容之外，還要提供監聽相關資訊，第三項是如果通話內容經過加密的話，需要將加密的金鑰送給司法單位，讓司法單位可以把加密的通話內容解密。

不讓監聽目標發現

合法監聽的第一項要求，不能讓監聽目標發現受到監聽，在我們的合法監聽架構之下，我們會有一台以上的合法監聽閘道器，這個架構有二個好處，一個就是可以混淆監聽目標的注意，另一個是可以分散通話，以達到負載平衡(load balance)的狀態。

當網路電話建立通話的時候，SIP 代理伺服器會將合法監聽閘道器的位址傳送給通話雙方，通話雙方再跟閘道器建立連線，可是 SIP 代理伺服器每次給通話雙方的位址可能不一樣，這樣就可以防止監聽目標發現自己受到監聽，另外 SIP 代理伺服器可以根據合法監聽閘道器的使用狀態，來判斷要讓通話雙方使用哪一台閘道器，這樣就可以達到負載平衡的目標。

提供監聽相關資料

合法監聽的第二項要求，司法單位要求的監聽結果，可以分成三種，一種是只要監聽通話內容、一種是只要監聽相關資料、最後一種是二者都要，也就是說監聽通話內容和監聽相關資料都要傳送給司法單位，所以當司法單位要求監聽相關資料時，合法監聽架構需要可以提供。

在我們的合法監聽架構下，要提供監聽相關資訊給司法單位，監聽相關資訊指的是和監聽目標有相關的資訊，包含了建立這通網路電話所傳送的訊息、控制網路電話的訊息、時間流程、如果可以的話甚至地理位置也算在裡面，舉凡電話號碼、電腦 IP 位置、通話時間等等，都可以是監聽相關資訊。我們可以讓 SIP 代理伺服器來達成這個要求，

因爲每一通網路電話的建立、修改、刪除都會經過代理伺服器，所以可以從代理伺服器取得通話建立時間、通話結束時間、通話持續時間、甚至連打過哪些網路電話，哪些通話建立成功、哪些通話建立失敗等等資訊都可以從代理伺服器取得，等到被監聽的通話結束之後，代理伺服器會把監聽相關資訊結果回傳給調解設備，調解設備再把結果以司法單位要求的格式封裝，最後傳送給司法單位，因此我們的合法監聽架構可以符合第二項要求。

將通話加密金鑰送給司法單位

合法監聽的第三項要求，假如通話內容是由電信業者所加密的話，爲了要讓司法單位有辦法解開加密的通話內容，可以用二種辦法：第一種方法是，電信業者先將加密的通話內容用通話加密金鑰解密之後，再將解密過的通話內容傳送給司法單位，另一種方法是，電信業者除了把加密過的通話內容傳送給司法單位，還要把加密通話用的金鑰傳送給司法單位，讓司法單位可以用這把金鑰解開加密的通話內容，在我們的合法監聽架構之下，我們使用的是第二種方法。

在我們的合法監聽架構下，爲了保證通話有安全性，所有網路電話的通話內容都要經過加密，這樣的話就算有人想竊聽通話而偷偷攔截通話封包，也會因爲不知道加密通話用的金鑰而無計可施，在我們的架構下，加密通話內容的金鑰是由金鑰管理元件所產生的，同時金鑰管理元件也會管理所有通話的通話加密金鑰，所以我們只要讓金鑰管理元件把通話加密金鑰傳送給調解設備，調解設備再把通話加密金鑰傳送給司法單位，司法單位就可以用這把金鑰解開加密過的通話，達成第三項要求。在我們的合法監聽架構下，我們把金鑰管理元件和調解設備合而爲一，這是爲了減少通話加密金鑰在網路上傳送的風險，這樣的話就省去金鑰管理元件傳送金鑰給調解設備這一個步驟，取而代之直接把金鑰傳送到司法單位手中，達成第三項要求。

第五章、系統模擬結果

5.1 模擬環境

在這一節我們會介紹模擬所使用的硬體、軟體等等，我們模擬所使用的硬體方面，CPU 爲 Intel Pentium-M 1.8 GHz 的筆記型電腦用 CPU，1GB 的 SDRAM。在軟體方面，使用的作業系統是 Microsoft 的 Windows 2000 server，網路傳輸模擬所使用的模擬器爲 Network Simulation 2[35]，NS2 是跑在 Cygwin[36]上面。

5.2 網路傳輸模擬

網路傳輸的延遲大至上可分爲傳送延遲(Propagation delay，5 μ sec/km)與排程的延遲(Queuing delay)，其中，傳輸延遲與資料大小無關，是存在於傳輸上的基本延遲，而排程延遲則發生在封包進入路由器(Router)到被送往正確的傳送連結上所需要的時間，這個部份與網路狀況以及封包的大小有著密切的關係，不同的聲音編碼方法會有不同的傳輸速度、封包大小、聲音品質也會不一樣，想要有比較好的聲音品質，可能需要傳送比較大的封包，而且封包傳送量也會比較多，如果想節省網路頻寬，可以選擇封包小、傳送量少的聲音編碼方法，不過相對的聲音品質就會比較差，表 6 爲各種聲音編碼方法的說明表[34]。

表 6　聲音編碼方法說明表

Compression method	Bit Rate (Kbps)	Payload size (Bytes)	packets/second	MOS score
G.711	64	160	50	4.1
G.726	32	80	50	3.85
G.728	16	60	34	3.61
G.729	8	20	50	3.92
G.723.1	6.3	24	34	3.9

我們假設合法監聽閘道器爲一台個人台腦，對外的頻寬爲 100Mbps，我們想要模擬這台合法監聽閘道器可以承受多少通監聽通話，而不會發生封包遺失(Packet lost)的情形，我們會對所有的聲音壓縮方法都加以模擬。我們模擬的網路環境爲有 5 個網路節點(node)，路由器(router)0 和路由器 1 爲網路電話封包來源，所有的網路電話都會經過這二台路由器，而傳送到合法監聽閘道器那邊，路由器 2 爲合法監聽閘道器網路封包出去會經過的第一個路由器，所以所有的封包都會經過這台路由器，合法監聽閘道器連接路由器 2，路由器 3 爲合法監聽閘道器傳送監聽結果給調解設備(MD)會經過的路由器，所有經過的連線傳送延遲(Link propagation delay)皆爲 10*ms*，表 7 爲模擬硬體和軟體環境，圖 33 爲模擬網路環境。

表 7　硬體和軟體環境

CPU	Intel Pentium-M 1.8GHz
RAM size	1 Gigabytes
OS	Microsoft Windows 2000 server
Simulation software	Network Simulation 2 (Version 2.28)
Link state	Delay：10 *ms*，Bandwidth：100Mb，Queue：droptail

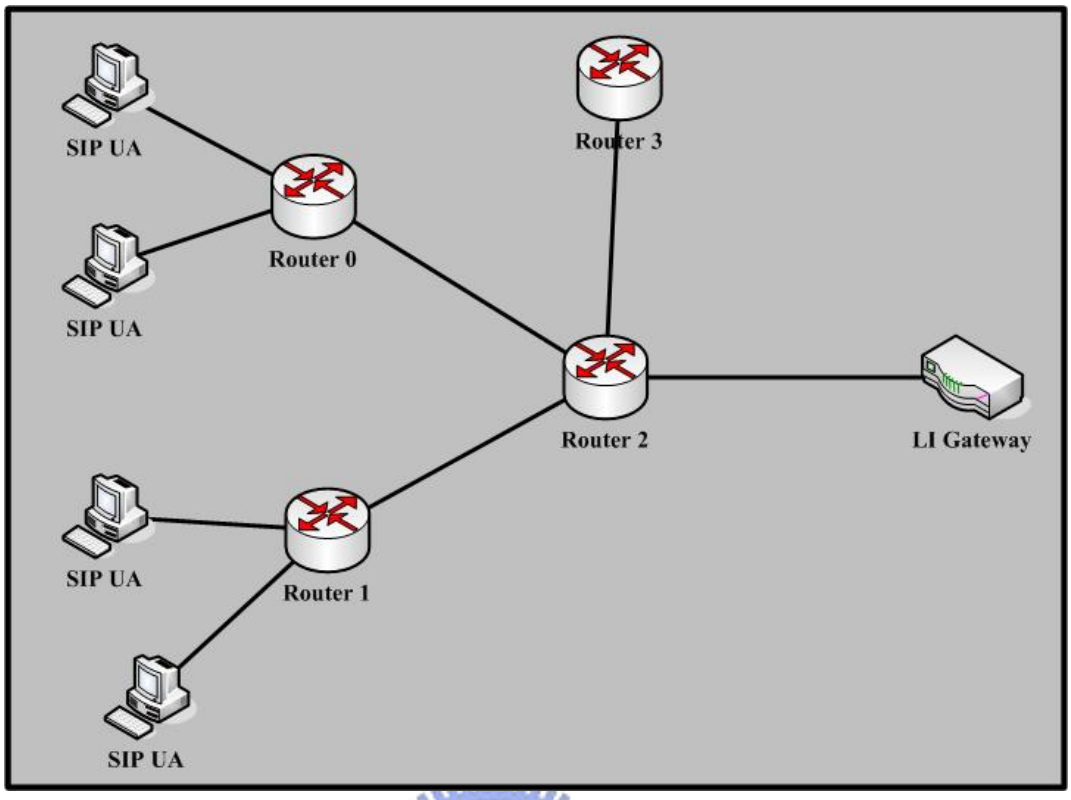

圖 33　模擬網路環境

在這裡我們模擬了 5 種聲音編碼方法：G.711、G.726、G.728、G.729、G.723.1，這些編碼方法是由 ITU-T 所定義的，它定義了一些在數位網路上傳送與多媒體部份的組織架構，ITU-T 也提出了 MOS(Mean Option Score)的觀念，將聲音由好到壞分成 1 到 5 這 5 個等級(MOS 5 品質最佳，MOS 1 品質最差)，由至少 30 個人聽過編碼後的聲音，給出分數後平均而得，是目前對聲音編碼評鑑的一個標準，通常 MOS 4 以上的分數比較適合商業化使用。

我們模擬網路電話的通話數跟封包遺失率的關係，從通話數 100 開始，一直模擬到通話數 1000，不過 G.711 在通話數 100 的時候還是有封包遺失，所以增加了通話數 90 這個模擬，最後我們將模擬結果做成圖表，圖 34、35、36、37、38 和表 8、9、10、11、12 是所有聲音編碼方法的模擬結果。

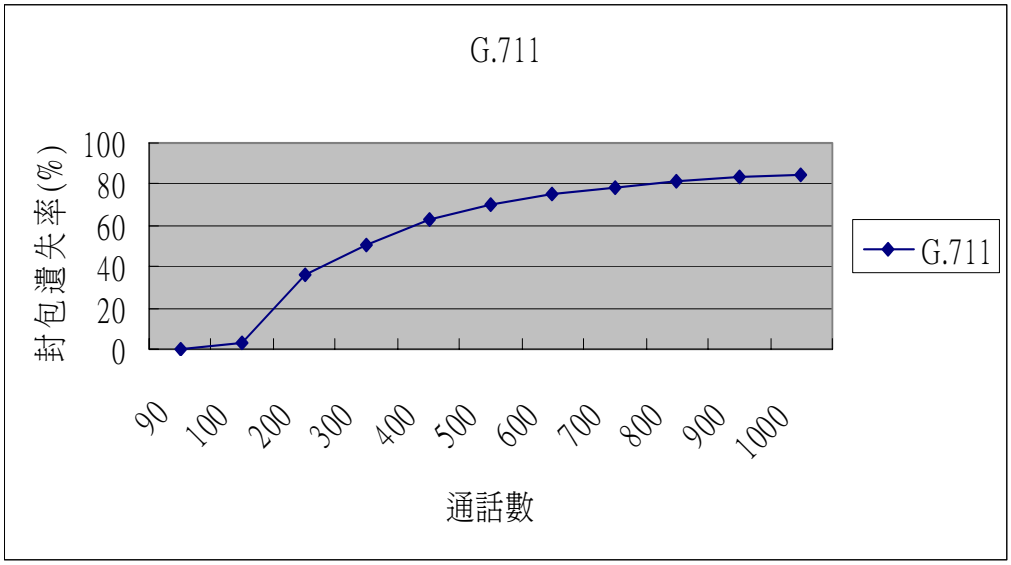

圖 34　G.711 的模擬結果

表 8　G.711 的模擬結果

通話數	90	100	200	300	400	500	600	700	800	900	1000
封包遺失率(%)	0	3.5	36.17	50.33	62.67	70.07	75.03	78.6	81.27	83.33	85

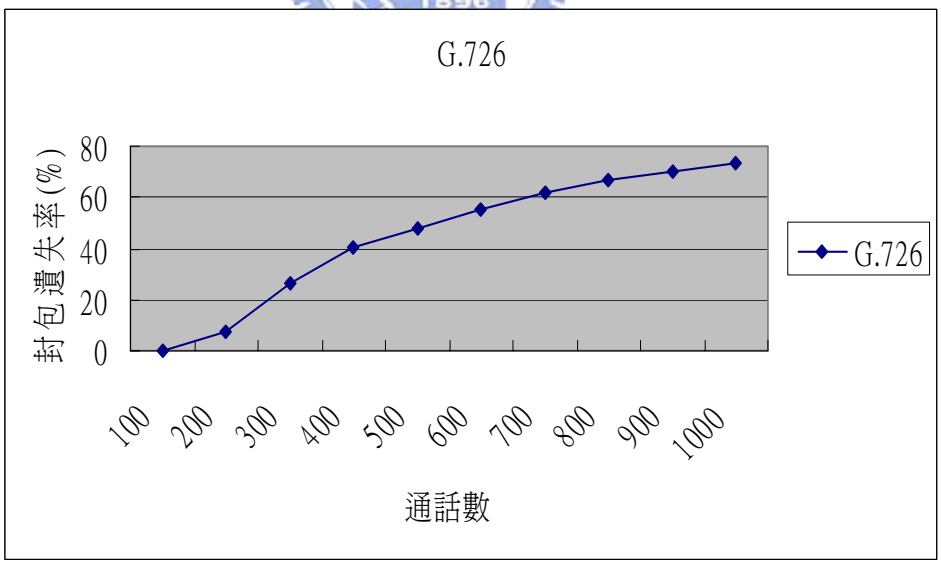

圖 35　G.726 的模擬結果

表 9　G.726 的模擬結果

通話數	100	200	300	400	500	600	700	800	900	1000
封包遺失率(%)	0	7.33	26.06	40.25	47.73	55.58	61.9	66.67	70.33	73.3

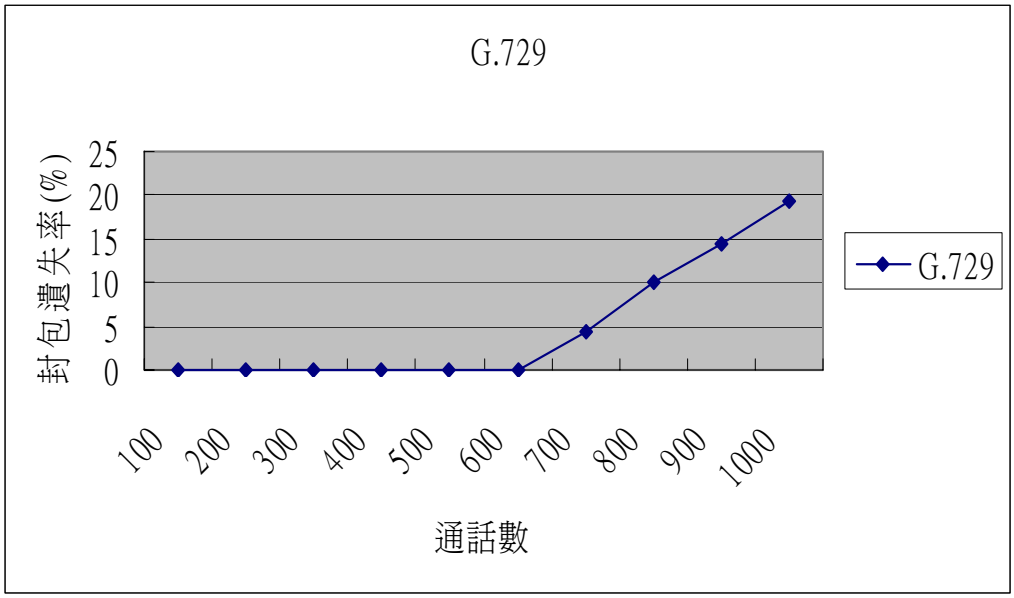

圖 36　G.729 的模擬結果

表 10　G.729 的模擬結果

通話數	100	200	300	400	500	600	700	800	900	1000
封包遺失率(%)	0	0	0	0	0	0	4.4	9.94	14.37	19.32

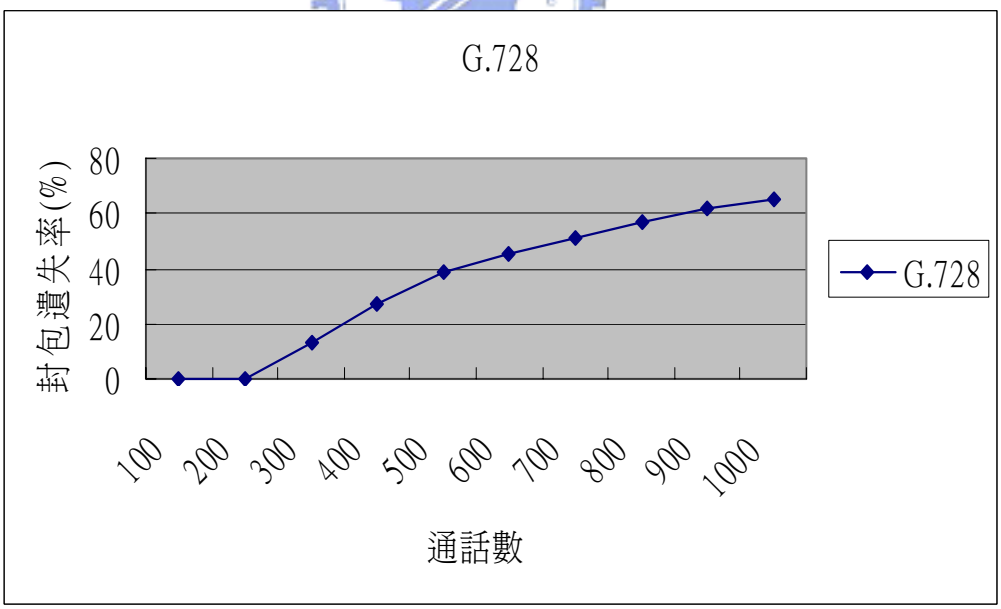

圖 37　G.728 的模擬結果

表 11　G.728 的模擬結果

通話數	100	200	300	400	500	600	700	800	900	1000
封包遺失率(%)	0	0	12.94	27.29	38.43	45.75	50.81	56.92	61.67	65.5

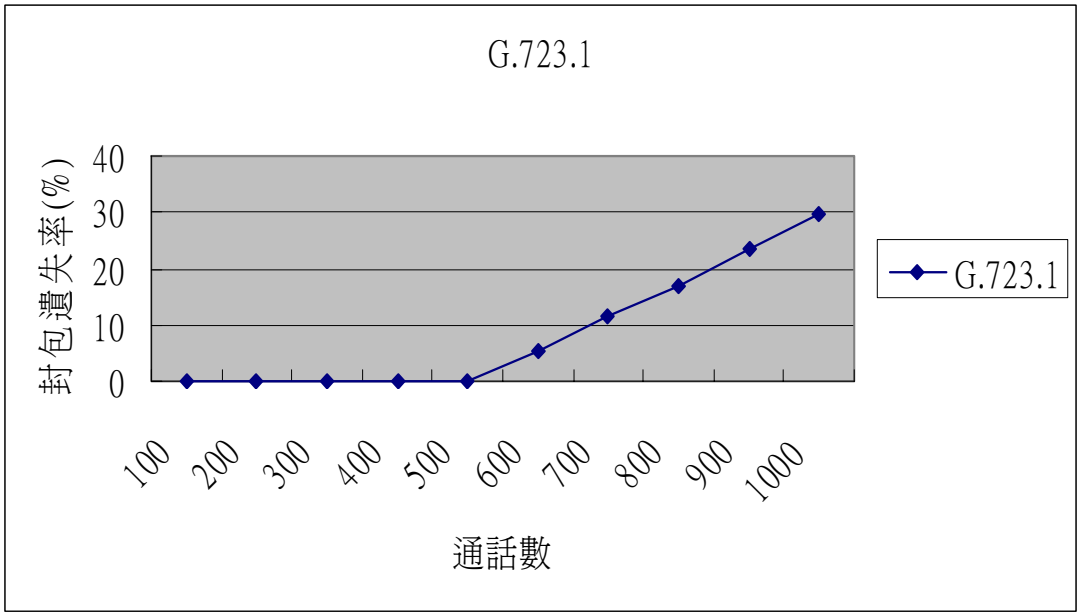

圖 38　G.723.1 的模擬結果

表 12　G.723.1 的模擬結果

通話數	100	200	300	400	500	600	700	800	900	1000
封包遺失率(%)	0	0	0	0	0	5.47	11.64	16.77	23.69	29.63

從模擬結果可以看得出來，封包遺失率跟通話數是成正比的關係，每種聲音壓縮方法都有一個臨界點，當超過這個臨界點之後就會開始發生封包遺失。G.711 的臨界點是在通話數超過 90，封包遺失率開始大幅度的上昇，到了通話數 700 左右漸趨平緩；G.726 的臨界點在通話數 100，超過之後和 G.711 一樣封包遺失率大幅上昇，到了通話數 600 左右漸趨平緩；G.729 的臨界點是在通話數 600，超過通話數 600 封包遺失率會成等加數列上昇；G.728 的臨界點在通話數 200，超過之後封包遺失率會先大幅度上昇，到了通話數 600 左右漸趨平緩；G.723.1 的臨界點是在通話數 500，超過之後封包遺失率會成等加數列上昇，綜合之上模擬結果，我們可以發現封包遺失率會跟封包大小、封包每秒傳送速度有關係，封包比較小，封包遺失率會比較低，封包每秒傳送速度比較低，封包遺失率也會比較低。

第六章、結論

6.1 討論與結論

在本篇論文中，我們結合了思科(Cisco)提出的合法監聽架構和 SIP 網路協定的架構，讓使用 SIP 網路協定建立的網路電話可以提供合法監聽的功能，我們提出一套合法監聽的架構，以思科所提出的合法監聽架構爲基礎，再加入 SIP 網路協定和金鑰管理元件(Key Manager)以及合法監聽閘道器(LI Gateway)，讓以後提供 SIP 網路電話服務也可以合乎法律的合法監聽要求。

我們提出的合法監聽系統架構，可以符合合法監聽的要求，合法監聽有三項要求需要符合，第一項是不能讓監聽目標發現自己受到監聽，第二項是除了提供通話監聽內容之外，還要提供監聽相關資訊，第三項是如果通話內容經過加密的話，需要將加密的金鑰送給司法單位，讓司法單位可以把加密的通話內容解密。

合法監聽的第一項要求，不能讓監聽目標發現受到監聽，在我們的合法監聽架構之下，我們會有一台以上的合法監聽閘道器，這個架構有二個好處，一個就是可以混淆監聽目標的注意，另一個是可以分散通話，以達到負載平衡(load balance)的狀態。

合法監聽的第二項要求，在我們的合法監聽架構下，要提供監聽相關資訊給司法單位，我們可以讓 SIP 代理伺服器來達成這個要求，因爲每一通網路電話的建立、修改、刪除都會經過代理伺服器，所以可以從代理伺服器取得通話建立時間、通話結束時間、通話持續時間、甚至連打過哪些網路電話，哪些通話建立成功、哪些通話建立失敗等等資訊都可以從代理伺服器取得，等到被監聽的通話結束之後，代理伺服器會把監聽相關

資訊結果回傳給調解設備，調解設備再把結果以司法單位要求的格式封裝，最後傳送給司法單位，因此我們的合法監聽架構可以符合第二項要求。

合法監聽的第三項要求，在我們的合法監聽架構下，爲了保證通話有安全性，所有網路電話的通話內容都要經過加密，這樣的話就算有人想竊聽通話而偷偷攔截通話封包，也會因爲不知道加密通話用的金鑰而無計可施，在我們的架構下，加密通話內容的金鑰是由金鑰管理元件所產生的，同時金鑰管理元件也會管理所有通話的通話加密金鑰，所以我們只要讓金鑰管理元件把通話加密金鑰傳送給調解設備，調解設備再把通話加密金鑰傳送給司法單位，司法單位就可以用這把金鑰解開加密過的通話，達成第三項要求。在我們的合法監聽架構下，我們把金鑰管理元件和調解設備合而爲一，這是爲了減少通話加密金鑰在網路上傳送的風險，這樣的話就省去金鑰管理元件傳送金鑰給調解設備這一個步驟，取而代之直接把金鑰傳送到司法單位手中，達成第三項要求。

所有網路電話的通話，都會被金鑰管理元件產生的金鑰加密，所以在傳送過程就算被有心人士取得，也無法知道裡面的內容，同時也可以防止電信業者取得監聽結果，因爲電信業者也拿不到加密所使用的金鑰，這把通話加密金鑰只有通話雙方，以及金鑰管理元件才知道，而金鑰在網路傳送過程是用加密的方式傳送，所以除了三方之外沒有其它人可以取得這把通話加密金鑰，所以可以保證通話內容是安全的。

當監聽結果送到司法單位那邊，司法單位會需要通話加密金鑰來將監聽通話內容解密，以取得真正的通話內容，可以當作法庭上的證據，所以金鑰管理元件必須將通話加密金鑰送到司法單位，但是爲了防止司法單位沒有經過授權而任意監聽，我們會將通話加密金鑰用電信業者和司法單位的公開金鑰做二次加密，到時候解密的時候也需要電信業者和司法單位的私密金鑰解密，這樣就可以防止司法單位單方面的任意監聽，因爲要解密時還需要電信業者的私密金鑰。

最後我們對合法監聽閘道器做了一些模擬，模擬不同的聲音編碼方法和不同的通話數對封包遺失率有什麼樣的關係，我們可以發現封包遺失率會跟封包大小、封包每秒傳送速度有關係，封包比較小，封包遺失率會比較低，封包每秒傳送速度比較低，封包遺失率也會比較低。因爲合法監聽不能遺失任何一個封包，所以我們最後可以得知合法監

聽閘道器對每種聲音編碼方法的最大通話數，也就是最多可以處理多少通網路電話，結果如表 8 所示：

表 13　合法監聽閘道器最大通話數

聲音編碼方法	G.711	G.726	G.729	G.728	G.723.1
最大通話數	90	100	600	200	500

6.2　未來工作

網路電話現在正是蓬勃發展的時候，但是所面臨的問題也不少，合法監聽就是其中一項，目前還沒有一個完整詳細的標準出現，我們這篇論文所提出的架構是以 SIP 爲基礎，以後還可以加入其他網路協定標準，全部整合在一起，如此一來希望可以促進網路電話的合法性，也可以幫助司法單位打擊犯罪，成爲破案的幫手。

另外我們提出的架構對於通話品質(QoS)多少會有影響，通話品質對於網路電話也是很重要的，有好的通話品質，客戶才會想用網路電話的服務，如何讓合法監聽盡量不影響到通話品質，這也是未來需要再進一步研究的地方。

最後就是合法監聽系統的安全性，在合法監聽架構中，安全性也是值得重視的部份，爲了防止監聽系統遭受不良份子的入侵或破壞，或是監聽資料被有心人士取得，一定需要有非常完善的安全機制來保護監聽架構，這部份也是未來需要更進一步深入探討的地方。

參考文獻

[1] ETSI TS 33.108 v6.7.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover Interface for Lawful Interception (Release 6).

[2] ETSI TS 101 331, Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies.

[3] IETF, Fielding, R., et al, "RFC2616: Hypertext Transfer Protocol -- HTTP/1.1", June 1999.

[4] IETF, Postel, J., et al, "RFC959: File Transfer Protocol", STD 9, October 1985.

[5] IETF, Klensin, J., "RFC2821: Simple Mail Transfer Protocol", April 2001.

[6] ITU-T Recommendation “H.323, Packet-based Multimedia Communications Systems”, International Telecommunication Union, Nov. 2000.

[7] IETF, Rosenberg, J., et al, "RFC3261: SIP: Session Initiation Protocol", June 2002.

[8] Baker, F., "Cisco Lawful Intercept Control MIB", Work in Progress, April 2004.

[9] IETF, Andreasen, F. and B. Foster, "Media Gateway Control Protocol (MGCP) Version 1.0", RFC 3435, January 2003.

[10] ITU-T Recommendation H.248.1, Gateway Control Protocol: Version 2, May 2002.

[11] C. Déchaux and R. Scheller. What are GSM and DCS. Electrical Communication, 2nd Quarter 1993

[12] Torbjorn Nilsson. Toward a new era in mobile communications. http://193.78.100.33/ (Ericsson WWW server).

[13] Yi-Bing Lin, Imrich Chlamtac, Wireless and Mobile Network Architectures, Wiley, New York, 2001, Page(s):164 - 165

[14] ETSI TR 101 943: “Lawful Interception(LI); Concepts of Interception in a Generic Network Architecture”, October 2004.

[15] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI);

Requirements of Law Enforcement Agencies".

[16] ETSI ES 201 158: "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".

[17] ETSI TS 133 107: "Universal Mobile Telecommunications System (UMTS); 3G security; Lawful interception architecture and functions (3GPP TS 33.107)".

[18] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

[19] IETF, H. Schulzrinne, et al, “RFC1889: RTP: A transport Protocol for Real-Time Application”, January 1996.

[20] Milanovic, A.; Srbljic, S.; Raznjevic, I.; Sladden, D.; Matosevic, I.; Skrobo, D.; “Methods for lawful interception in IP telephony networks based on H.323**”,** EUROCON 2003. Computer as a Tool. The IEEE Region 8 Volume 1, 22-24 Sept. 2003, Page(s):198 - 202 vol.1

[21] ITU-T Recommendation H.225.0. "Call Signaling Protocols And Media Stream Packetization For Packet-Based Multimedia Communication System", International Telecommunication Union, November 2000

[22] ITU-T Recommendation H.245. "Control Protocol For Multimedia Communication", International Telecommunication Union, July 2001

[23] IETF, IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

[24] Chia-Ming Sung; Ching-Cheng Lo; June-Hao Peng; Wen-Nung Tsai; “A study on VoIP Security”, International Computer Symposium, Dec. 2004, Page(s):1230 - 1237

[25] http://www.darpa.mil/

[26] http://investintaiwan.nat.gov.tw/zh-tw/env/telecom/internet.html

[27] http://www.ksjh.ttct.edu.tw/%E6%B3%95%E4%BB%A4%E8%A6%8F%E5%AE%9A/tanet/law/law-4.htm

[28] http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

[29] http://messenger.msn.com.tw/

[30] http://tw.messenger.yahoo.com/

[31] http://skype.pchome.com.tw/index.htm

[32] http://apply.seed.net.tw/apply/personal/pb/pb.asp

[33] http://www.ctiforum.com/technology/Voip/2001/09/voip0904.htm

[34] http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html

[35] http://www.isi.edu/nsnam/ns/

[36] http://www.cygwin.com/