Design and Implementation of SIP VoIP Monitoring System

Whai-En Chen, Li-Wen Hsu, Pin-Jen Lin and Chai-Hien Gan
Email: {wechen,lwhsu,pjlin,chgan}@csie.nctu.edu.tw

摘要

近年來由於國內寬頻網路環境日漸普及，各種網路應用服務如雨後春筍般出現，其中網路電話就是近來最熱門的話題之一。網路電話以其低廉的價格，強力衝擊了台灣原有的電信市場，但由於網路電話普及後可能成為犯罪的死角，因此電信總局不得不將監聽管理也列入政策開放之必要條件。本論文擬提出一個 SIP VoIP 監控系統，提供包括通聯記錄、監聽特定的使用者並通知檢調人員等功能。此外，電信國家型計畫 VoIP 平台已佈建有網路電話、網路電話伺服器及語音閘道器等設備，是一個相當完整的 SIP VoIP 實驗平台。在系統研發完成後，本論文將系統建置於電信國家型計畫 VoIP 平台上，期望以實際的系統驗證本論文所研發之 SIP VoIP 監控機制。

關鍵詞：NTP、SIP、VoIP、Monitoring

1. Introduction

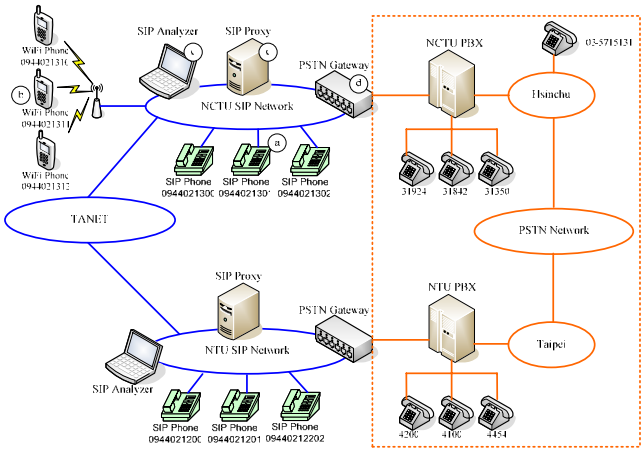
網路電話（Voice over IP，簡稱 VoIP）以其低廉的價格，強力衝擊了台灣原有的電信市場，但由於網路電話普及後可能成為犯罪的死角，因此電信總局將監聽管理也列入政策開放之必要條件。

交通大學 VoIP 實驗室所建置之電信國家型計畫 VoIP 平台(NTP VoIP Platform)，建置有網路電話、網路電話伺服器及語音閘道器等設備，是一個相當完整的 SIP（Session Initiation Protocol [2]）VoIP 實驗平台。然而此平台尚未提供監控相關的機制，因此本論文擬研發一個 SIP VoIP 監控系統，並於電信國家型計畫 VoIP 平台上驗證此系統的正確性。

1.1. NTP VoIP Platform

電信國家型計畫的 VoIP 實驗平台是一套以 SIP 為基礎之電話網路平台，目前此一平台範圍涵蓋台灣大學、清華大學、交通大學、成功大學、東華大學、靜宜大學等六所學校。圖一是台灣大學與交通大學連線範例，圖中虛線方框的部分表示傳統的電話網路，其他部分則表示 IP 網路。

This work was sponsored in part by NSC Excellence project NSC93-2752-E-0090005-PAE, NSC 93-2213-E-009-100, and NTP VoIP Project under grant number NSC 94-2219-E-009-002. IIS/Academia Sinica, and ITRI/NCTU Joint Research Center.



圖一、現有電信國家型計畫 VoIP 實驗平台

電信國家型計畫 VoIP 平台包括以下三種主要的元件：

(1) 網路電話：依照網路存取介面可分為使用乙太網路連結的網路電話（SIP Phone；圖一ⓐ）和使用無線網路802.11連結的無線網路電話（WiFi Phone；圖一ⓑ）。

(2) 網路電話伺服器（SIP Proxy；圖一ⓒ）：IP網路上的所有網路元件都必須有一個IP位址，網路電話也不例外。但由於IP位址不容易記憶，且網路電話設備有可能透過自動組態設定，如DHCP（Dynamic Host Configuration Protocol）等方式來取得IP位址。因此需要一台網路電話伺服器，來負責將一般人容易記憶的識別符號(如電話號碼 0944021300) 轉換為 IP 位址（如 140.113.131.1）。

(3) 語音閘道器（PSTN Gateway；圖一ⓓ）：由於IP網路與電話網路（Public Switched Telephone Network，簡稱PSTN）的信號不同，因此網路電話無法直接與PSTN電話通話。語音閘道器就是負責轉換兩者間的訊號，讓網路電話可以撥打給PSTN電話或手機。

關於網路電話識別碼的指派，因為考慮一般打電話的使用習慣，以及使用電話按鍵輸入的方便性，目前網路電話識別符號較常使用的是電話號碼。要達到轉換電話號碼與 IP 位址的功能，網路電話就必須在取得新的 IP 位址時，向網路電話伺服器註冊（Register），伺服器會將識別符號（即電話號碼）與 IP 位址的對應儲存至資料庫中以便將來查詢。當網路電話伺服器收到

查詢請求時，會先由受話方的電話號碼判斷是否屬於自己所負責的範圍。如果受話方號碼為此一伺服器所管轄，伺服器就會去資料庫找尋其對應的 IP 位址；如果受話方號碼（如傳統電話網路號碼 02-25663000）不是此伺服器所負責的，則此伺服器將根據其所設定的轉接規則，將請求轉給其他伺服器或是轉至語音閘道器。依照上述的規則，本計畫向 SIP/ENUM 申請前置碼為 0944021 的電話號碼，共一千門號碼從 0944021000 到 0944021999。網路電話號碼的指派方法是將號碼 0944021300 到 0944021399 分配給新竹地區，號碼 0944021200 到 0944021299 分配給台北地區。因此 SIP 伺服器可以從電話號碼的前置碼判斷出，此一通電話應該轉送給哪一台 SIP 伺服器處理。

以下舉例說明網路電話的運作，從網路電話 0944021300 撥打至市話 02-25663000，訊息會先傳給交大的 SIP 伺服器，SIP 伺服器由前置碼 02 判斷出此通電話是台北地區的號碼，就將訊息轉送給台大的 SIP 伺服器，台大的 SIP 伺服器發現號碼並非 0944021 開頭，因此送給 PSTN 閘道器轉接至市話。如果從交大網路電話 0944021300 撥打 0944021200，台大伺服器收到封包後，就可以判斷 09440212 開頭的電話是自己負責的號碼，接著就會查詢 0944021200 號碼所對應的 IP 位址，最後轉接至台大之網路電話。

1.2. Problem Definition

雖然目前國內 SIP VoIP 實驗平台功能已經相當完整，能夠提供網路電話與網路電話，或網路電話與市話或手機的通話能力，但這套系統仍欠缺了一套監控的機制。且在商用網路電話的運作中，檢調機關會要求提供合法的監聽機制，以免網路電話成為犯罪的媒介。

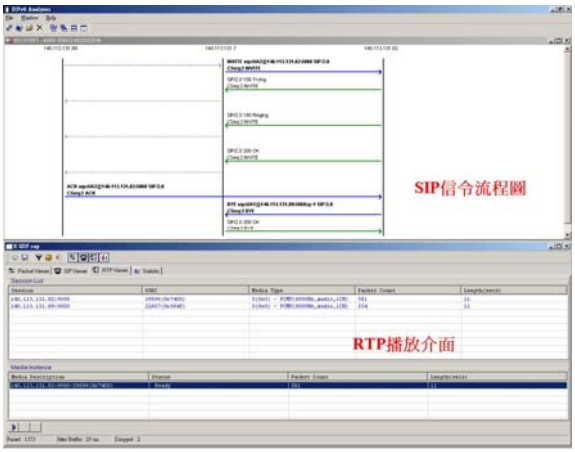
完整的監控系統應包含以下功能。第一、提供完整的通聯紀錄；第二、將指定的某通電話語音錄下，供檢調人員調閱。因此本論文的目標就是研發 SIP VoIP 監控系統，並在電信國家型計畫實驗平台架構上，驗證出上述兩項功能。

在設計這套監控系統的過程中，本論文還發現了一項具有研究價值的議題。在一般的情況下，RTP（Real-time Transport Protocol [4]）資料流的流量遠大於 SIP 控制訊號的流量。由於 RTP 資料流由 RTP Proxy 來負責，而 SIP 控制訊號則由網路電話伺服器來控制，因此 RTP Proxy 是系統效能的瓶頸。故本論文使用多台 RTP Proxy 建構成的負載平衡系統來提升系統效能，並使用數學模型來找出系統最適合的 RTP Proxy 數量。

2. Related Works

分析目前網路監控系統，可分為兩個主要的類型，第一類是讓網路上所有的交換器（如：Switches 或 Routers）支援監控功能，檢調機關必須事先知道路由並將監控系統連接上該交換器作監控。第二類是讓所有的網路資訊都匯集至交換中心，檢調單位可以在交換中心作監控。

SIPv6 Analyzer（如圖二所示）是一套 SIP 分析軟體，由交通大學資工系 VoIP 實驗室的賴建利等人開發。其功能包括繪出 SIP 信令流程圖以及播放 RTP 所承載的多媒體資料流等。這套分析軟體對於開發 SIP 相關應用服務，提供了一套簡單易用的工具。此一工具可以應用於第一類的監控類型。但若要達到完整的監控功能，則監控手續將非常繁雜。原因是 SIPv6 Analyzer 若要能監控一段通話，必須能擷取該電腦所發出的所有封包，才能做進一步過濾分析的動作。因此 SIPv6 Analyzer 必須與網路電話安裝於同一台電腦，或是和該網路電話位於同一集線器（Hub）或交換器上。換句話說，每當受監控者位置移動，如換了一台電腦，SIPv6 Analyzer 就必須跟其一起移動，造成監聽工作的不便。而且在受監控者使用無線網路電話的情況下，要掌握受監控者的移動情形將更加困難。因此本論文所提出的監控系統，是將受監控者的 RTP 封包導向至監控中心的監聽設備來進行監控，故可解決上述的問題。



圖二、使用 SIPv6 Analyzer 監聽

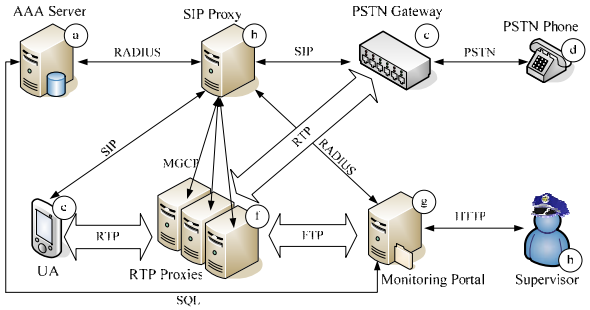
由於網路電話在真正開始進行通話之前，一定會先用 SIP 通訊協定和網路電話伺服器進行溝通。因此本論文提出透過增加網路電話伺服器的功能，讓 SIP 封包在經過網路電話伺服器時，網路電話伺服器可以修改 SIP 封包中所帶的 SDP（Session Description Protocol [1]）資訊。之後受監控者的網路電話照著被修改過的 SDP 資訊建立傳送語音的 RTP 資料流，就會被導向至本論文所開發的 RTP Proxy 上。RTP Proxy 收到 RTP 封包之後，複製一份並轉成 WAV 檔存下。而在網路電話建立通話時，網路電話伺服器會將 SDP 中發話方與受話方的資訊（位址與埠）交給 RTP Proxy，讓 RTP Proxy 可以正確地將封包送給通話的另一端。

由於電信國家型計畫 VoIP 平台所使用之網路電話伺服器 Iptel SER [5]的功能並無法滿足監控的需求，為了產生通聯記錄，本論文整合 Auth 模組與 Acc 模組，來設計一個的監聽控制模組（Monitoring Control Module），以達到上述修改 SDP 之功能。此外，在監聽網路電話部分，本論文研發了 RTP Proxy 擷取 RTP 封包，並轉換成可播放之 WAV 檔案格式。最後，為

了提供通知的功能與集中管理之網頁介面，本論文研發網路電話監控中心（Monitoring Portal），一方面與網路電話伺服器溝通以設定監控對象；另一方面集中儲存 RTP Proxy 所錄下之 WAV 檔，並於完成後以即時訊息（Instant Message）來通知檢調人員。為了提升系統整體效能，本論文採用負載平衡系統，利用多台的 RTP Proxy 來平均分攤 RTP 語音資料流的流量。因為每次連線的 RTP Proxy 不同，本監控系統不易被受監聽者得知被監控。

3. SIP VoIP Monitoring System

以下介紹監控系統中各個元件的功能及其在此系統中所扮演的角色。網路電話（User Agent；圖三ⓔ）在每次開機或取得新的 IP 位址時，都必須向網路電話伺服器（圖三ⓑ）做註冊和更新的動作。網路電話伺服器和 AAA（Authentication Authorization Accounting）伺服器（圖三ⓐ）用 RADIUS （Remote Authentication Dial In User Service [6]）來做認證的動作，以確認使用者的身份。爾後網路電話在撥打或接聽電話時，都會經由網路電話伺服器來做轉接，而網路電話伺服器在做轉送的同時，也會和 AAA 伺服器交換資訊以產生通聯記錄。



圖三、SIP-based VoIP 監控系統

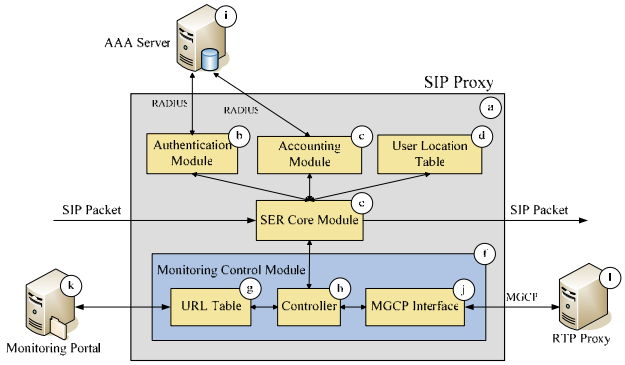
此外，網路電話伺服器還必須設法將語音的資料流導到 RTP Proxy（圖三ⓕ）上，因此網路電話伺服器和 RTP Proxy 之間必須要互相交換資訊，這兩者之間的溝通採用 MGCP（Media Gateway Control Protocol [3]）通訊協定。RTP Proxy 則必須將收到的 RTP 封包，正確的轉送給另一端的通話者，並將語音資料存下來，當錄音完成之後，使用 FTP（File Transfer Protocol）傳到監控中心（圖三ⓖ）上，監控中心存檔完畢之後，檢調人員（圖三ⓗ）就可以經由網路瀏覽器（Web Browser）來取得語音資料。

此例中語音閘道器（圖三ⓒ）則扮演另一個 SIP 網路電話的角色，其會建立起另一個與傳統電話（圖三ⓓ）之間的連線並轉換訊號。在此範例中，本監控系統可以監聽由 VoIP 撥到市話或手機之通訊。接下來說明網路電話伺服器、RTP Proxy 與監控中心之功能：

3-1 網路電話伺服器

網路電話伺服器主要的功能有二，其一是使用者認證並產生通聯記錄，其二是將要監聽的通話導向至RTP Proxy。目前電信國家型計畫所採用的網路電話伺服器中，已經有部分的功能可以直接套用於本文所描述的監控系統，因此我們直接採用這些現有的模組，並對其加以設定，以達到本論文所需之功能。

針對上述的兩項功能，本論文提出了以下的設計（圖四）。圖中的上半部份是SER原有的模組（圖四中ⓑⓒⓓⓔ），如前項所述，本論文對此部分進行研究，改變其設定來達到所需的功能。但由於SER中並沒有提供監控相關的機制，因此必須自行開發其中的的監聽控制模組，也就是圖四ⓕ的部份。



圖四、網路電話伺服器內部模組設計圖

接下來針對圖四來說明其中各模組的功能及運作流程。

(1) 通聯記錄產生的流程

所有經過網路電話伺服器的 SIP 封包都會先經過 SER 的核心模組（圖四ⓔ），經由認證模組（圖四ⓑ）確認完使用者的身份之後，再交由記錄模組（圖四ⓒ）來記下使用者的動作，以便於最後產生通聯記錄。這兩個模組裡面皆包含 RADIUS 介面，會以 RADIUS 通訊協定來和 AAA 伺服器做溝通。最後查詢使用者位址表（圖四ⓓ）來找到此封包受話端的位址，將此位址填入該封包後送出。

(2) 監聽的流程

也就是將通話導到 RTP Proxy 的過程。當封包通過 SER 的核心模組時，核心模組會將使用者的資料交由本論文所開發的監聽控制模組（圖四ⓕ）。該模組會先在 URL 表（圖四ⓖ）中查詢這通電話的通話者是不是在表中，來判斷這通電話是否需要監聽。不需監聽的通話，就可以由 SER 核心模組查詢使用者位址表後，直接將封包送出；需要監聽的通話，則經由 MGCP 介面（圖四ⓙ）和 RTP Proxy（圖四ⓛ）交換必要的資訊，交回給監聽控制模組去修改 SIP 封包中的 SDP 資訊後，再交回 SER 核心模組將修改後的封包送出。

(3) 網路電話伺服器和 RTP Proxy 間 MGCP 的溝通過程

網路電話伺服器中已事先設定 RTP Proxy 所使用的 IP 位址和埠。以下說明這兩者間的溝通過程：

①. 網路電話伺服器收到來自受話端 SIP 200 OK 的訊息後，向 RTP Proxy 發出 MGCP 的 CRCX（Create Connection）命令，裡面包含了：

- 兩個使用者的 IP 位址和通訊埠
- 兩端協定後所使用的語音編碼
- 此次通話的序號（Serial ID）

②. RTP Proxy 收到由網路電話伺服器發出的命令，為此通話做準備動作，完成後回應 200 OK 給網路電話伺服器，確認準備動作完成。

③. 此時網路電話伺服器才轉送受話端使用者 SIP 200 OK 的訊息給發話端，正式開始通話。

④. 網路電話伺服器收到使用者 SIP BYE 的訊息，在另一個使用者確認通話結束後，向 RTP Proxy 發出 MGCP 的 DLCX（Delete Connection）命令，以結束這一次的通話以及監聽動作。

⑤. RTP Proxy 收到由網路電話伺服器發出的命令，結束轉送 RTP 封包並進行後續的處理動作，正式結束這一次的監聽。

(4) 監控對象的設定

關於監控對象的設定，檢調人員可以在監控中心（圖四ⓚ的部份），直接將要監聽的對象寫入監聽控制模組的 URL 表（圖四ⓖ）中。

3-2 RTP Proxy

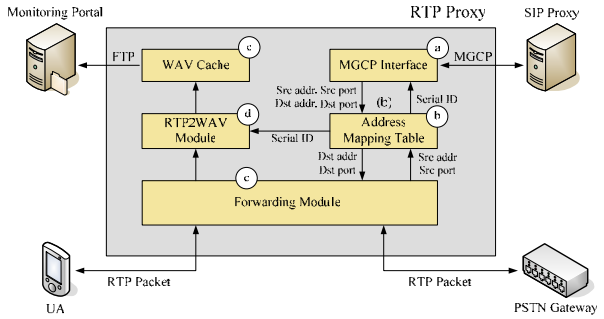
RTP Proxy的主要功能有二：第一是RTP封包的轉送（Forwarding），第二是將收集到的RTP封包轉成WAV檔存下。RTP Proxy中轉送的功能，包括轉送模組、位址對應表和MGCP介面。轉送模組內部採用UDP Socket來實作收送RTP封包的部份，UDP Socket可根據收到之sockaddr結構中之sin_addr與sin_port欄位，來獲取用戶端之位址和埠。轉送模組內部分成兩個不同的行程，其一負責收，另一則專門處理送的部份。行程之間的通訊，由於Unix系統中常用的IPC（Inter-Process Communication）方式中，pipe和FIFO均無法由程式設計者來管理其緩衝區大小，因此本論文採用shared memory的方式，來達到不同行程之間的通訊。本論文所設計的RTP Proxy內部模組圖如圖五所示，接下來針對圖五來說明其中各模組的功能及運作流程。

(1) 轉送RTP封包的流程

網路電話伺服器會經由MGCP介面（圖五ⓐ），把RTP封包的來源與目的的位址和埠寫入位址對應表（圖五ⓑ）。當轉送模組（圖五ⓒ）收到RTP封包時，會根據該封包中的來源位址和埠，從位址對應表中查到該封包真正的目的位址和埠，並將查到的位址和埠填入原封包的目的位址和埠後送出。

(2) 將RTP封包轉成WAV格式儲存的流程

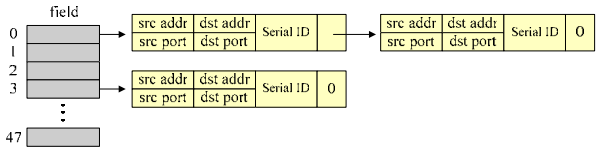
轉送模組收到RTP封包時，會將此封包複製一份，由RTP2WAV模組（圖五ⓓ）將之轉成WAV檔格式，並暫存在WAV暫存器（圖五ⓔ）中。等到RTP Proxy閒置時，WAV暫存器再用FTP將錄音檔上傳到監控中心。



圖五、RTP Proxy 內部模組設計圖

(3) RTP Proxy中之位址對應表

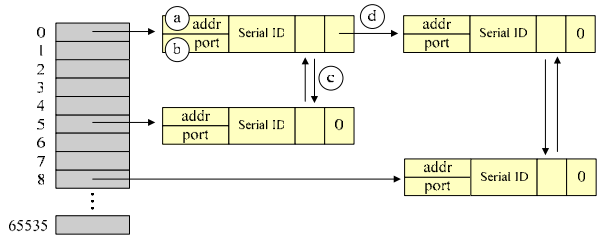
位址對應表有幾個要點，由於 RTP Proxy 所收到的每個 RTP 封包，都必須查一次位址對應表以取得目的地位址和埠。由此可見，位址對應表查詢的次數會相當頻繁。RTP Proxy 針對一通電話，只需對位址對應表做一次新增和一次刪除的動作，但可能會查詢數千次以上。因此我們進行位址對應表的設計時，把重點放在增進查詢的效能。



圖六、位址對應表的實作－普通的 hash table

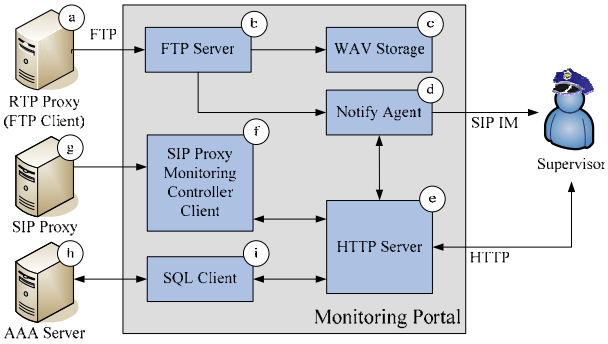
位址對應表最初是以普通的hash table來實作（圖六），但由於RTP資料流是雙向的，由一個位址和埠查到另一個位址和埠後，還需要從另一個位址和埠反查回來。因此若使用普通的hash table來實作，就必須要存兩份資料，因而造成空間的浪費。故我們提出了新作法。此新作法之資料結構如圖七所示，每個連結串列的節點除了有位址和埠的資料外，還包含了兩個指標，第一個指標指向搜尋的結果，第二個指標用來搜尋用。以第一個欄位為例，當搜尋到第一個節點時，如果addr（圖七ⓐ）和port（圖七ⓑ）和所要搜尋的位址和埠相同，則用第一個指標（圖七ⓒ）來取得結果，否則則用第二個指標（圖七ⓓ）來繼續搜尋下一個節點，以此類推。

最後的問題是hash function的設計。論文[7]詳細研究了以實體位址（MAC address）為輸入的hash function，分析並比較了如取前幾位元、CRC、checksum、XOR等方式的效能好壞，參考此篇論文，本論文中hash function目前採用CRC輸出16位元來當hash table的key。



圖七、位址對應表的實作使用雙重指標的hash table

3-3 監控中心



圖八、監控中心內部模組設計圖

監控中心的主要功能有二：第一是集中儲存錄音檔案。為了解決RTP Proxy同時處理許多通話而造成的高負荷的問題，本監控系統會採用多台RTP Proxy之架構，來平均分散RTP 的流量。但這也使單一受監控者的錄音檔分散於各個RTP Proxy中，造成管理上的不便。且監控人員如直接存取RTP Proxy上的錄音檔案，可能會影響到RTP Proxy的效能，因此需要一個地方（即監控中心）來集中儲存管理所有的對話錄音檔案。

第二是通知的功能及網路管理介面。當錄音檔案儲存完畢之後，可以透過Notify Agent（圖八ⓓ），以即時訊息的方式，通知檢調人員，在檢調人員收到通知後，可以經由網頁介面來存取通話的錄音記錄。根據上述的功能，我們所設計之監控中心內部模組如圖十一所示，接下來說明其中各模組的功能及運作流程：

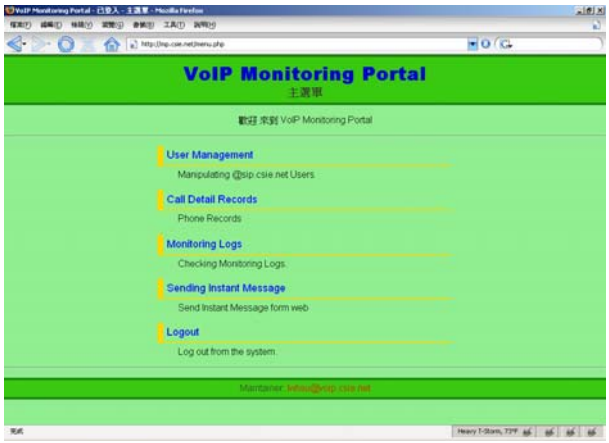
(1) 集中存取通聯記錄與錄音檔案

通聯記錄儲存在AAA伺服器（圖八ⓗ）上的資料庫中，監控中心透過SQL Client（圖八ⓘ）以網頁介面提供管理者查詢此一記錄（圖九）。

RTP Proxy（圖八ⓐ）完成錄音的工作後可以將錄音檔透過FTP上傳至監控中心上的FTP伺服器（圖八ⓑ）；而FTP伺服器將錄音檔案存入WAV Storage（圖八ⓒ）中。待檔案接收完成，FTP伺服器中的Notify Agent Plug-in會啟動Notify Agent（圖八ⓓ），以通知檢調人員。

(2) 通知的功能及網路管理介面

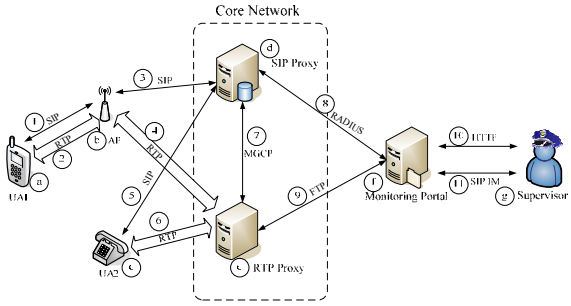
Notify Agent會以SIP即時訊息的方式通知檢調人員。在收到通知後檢調人員透過HTTP（Hyper-Text Transfer Protocol）伺服器（圖八ⓔ）上的網頁介面和監控中心連線。HTTP伺服器提供檢調人員以Web的方式存取WAV Storage中要收聽的錄音檔。關於設定監聽目標的部份，檢調人員透過網頁介面設定要監聽的對象，HTTP伺服器會以CGI（Common Gateway Interface）的方式控制監控模組客戶端（圖八ⓕ）將檢調人員的要求輸入網路電話伺服器（圖八ⓖ）。監控模組客戶端將監聽對象之URL寫入網路電話伺服器中監聽控制模組的URL表，即可完成設定。



圖九、監控中心網路管理主選單介面

4.Results and Performance Evaluation

圖十是 SIP-based 監控系統之展示環境，其中 UA1（圖十ⓐ）、UA2（圖十ⓒ）為兩個網路電話使用者，AP（圖十ⓑ）為無線網路存取點，SIP Proxy（圖十ⓓ）為網路電話伺服器，RTP Proxy（圖十ⓔ），Monitoring Portal（圖十ⓕ）為監控中心，Supervisor（圖十六ⓖ）為檢調人員。



圖十、展示環境介紹

成果展示步驟說明如下：

步驟一：檢調人員使用瀏覽器透過HTTP（圖十⑩），在監控中心加入使用者User01和User02。假設User01使用UA1，User02使用UA2，UA1與UA2向網路電話伺服器註冊。檢調人員在監控中心設定UA1為受監控對象，UA2為一般使用者，設定介面如圖十一所示。

步驟二：受監測者開始撥打電話，SIP信令由UA1經過網

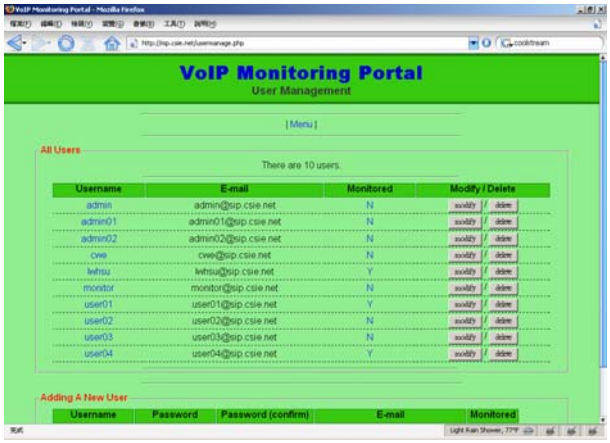
路電話伺服器，與UA2交換RTP資訊（路徑為圖十①③⑤）。此時網路電話伺服器以RADIUS（圖十⑧）在監控中心產生通聯記錄。收到SIP 200 OK訊息時，網路電話伺服器以MGCP（圖十⑦）要求RTP Proxy準備開啟RTP的連線。

步驟三：SIP信令完成後，UA1與UA2透過RTP Proxy進行通話（路徑為圖十②④⑥）。

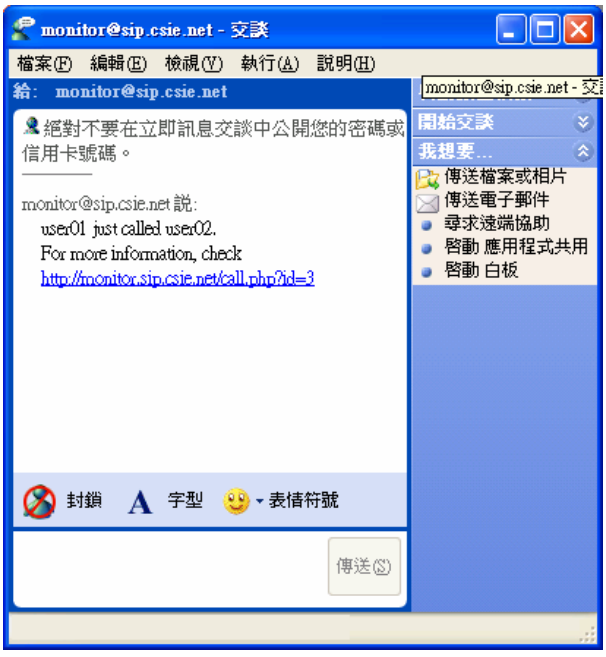
步驟四：通話完畢時，UA2送出SIP BYE訊息。網路電話伺服器收到BYE訊息時，以MGCP通知RTP Proxy結束RTP連線，並以RADIUS通知監控中心，紀錄通話時間。

步驟五：結束通話後，RTP Proxy將通話錄音檔案以FTP（圖十⑨）傳送至監控中心。監控中心以SIP即時訊息（圖十⑪）通知檢調人員。SIP即時訊息結果如圖十二所示。

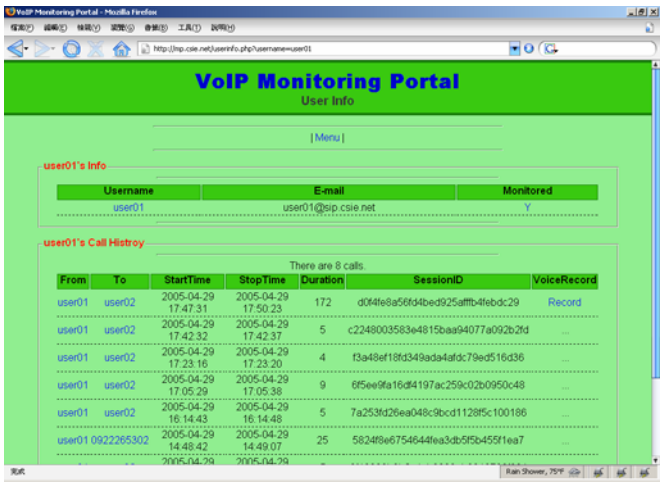
步驟六：檢調人員收到監控中心發出的SIP即時訊息後，可以從監控中心調出UA1的通聯記錄及該通話的錄音檔案（如圖十三）。



圖十一、在監控中心設定User01、User02監聽狀態



圖十二、收到監控中心發出之 SIP 即時訊息通知



圖十三、通聯記錄與錄音檔案下載介面

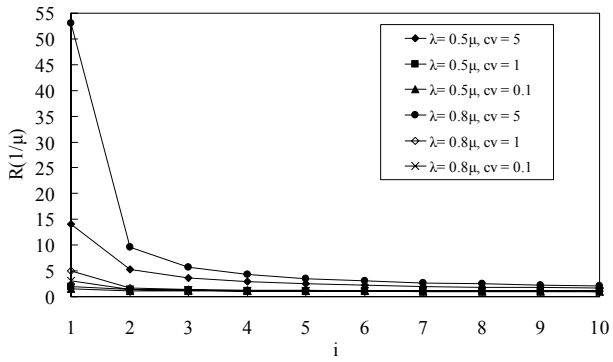
分析負載平衡系統架構之效能

針對負載平衡架構，我們最感興趣的是當RTP Proxy的數量可控制時，每個封包處理時間的期望值 $\overline{R} = E[R, i > 0]$ 為多少。假設RTP封包進入RTP Proxy的速率 λ 是以Poisson Distribution的方式分布，而RTP Proxy處理單一封包的時間 t_s 是以平均值為 $1/\mu$ 的General Distribution的方式分布。由於有 i 台RTP Proxy，故對每一台RTP Proxy而言，封包進入的速率為 $\lambda_i = \lambda / i$。且由於每台RTP Proxy均是獨立運作，故每一台RTP Proxy的行為可以用M/G/1來進行模擬。根據M/G/1的特性。參考[8]，$E[R,i]$ 可推導成下式：

$$E[R,i] = \frac{\rho_i(1+c_v^2)}{2\mu(1-\rho_i)} + \frac{1}{\mu},$$

$$\text{where } \rho_i = \frac{\lambda_i}{\mu} = \frac{\lambda}{i\mu} \qquad (1)$$

其中 $c_v = \mu\sqrt{Var[t_s]}$，$Var[t_s]$ 為 t_s 的變異數（variance）。根據上式，選擇不同的 λ 和 c_v，可得到以下的結果：



圖十四、RTP Proxy處理封包的效能模擬

圖十四描繪出在特定負載量下（即：$\rho = 0.8$ 或 $\rho = 0.5$），給定不同的c_v對於平均封包停留在系統之時間R（包含處理及等待時間）的影響。如圖所示，當c_v值較大時（即：c_v=5）及負載量 $\rho = 0.8$ 時，由單一Proxy Server來處理所有的RTP 封包時，其停留在系統之時間R高達50多倍之平均封包處理時間（$1/\mu$）。在經由提供多台之RTP Proxy後，我們可以大幅的減少其停留在系統之時間。例如當RTP Proxy由一台增加到兩台時，其效能可以提高約5倍，這是由於當只有單一伺服器時，較容易出現某個需要較多處理時間的RTP封包阻擋其後序封包的處理，造成其後序封包的等待時間大幅增加。另一方面，當c_v值較小時，則對於R之影響較小。經由此圖所示的結果，可提供我們了解在特定系統狀態下，我們需要多少台的RTP Proxy，才能在整個系統處理封包的效能較不會受到負載量與c_v的影響。例如當我們的VoIP系統可以忍受的平均停留在系統之時間為$4/\mu$以下時，在 $\rho = 0.8$ 及c_v=5時，本系統可選擇使用五台RTP Proxy，以符合系統之效能。

5. Conclusions

本論文研發之監控系統，已成功地在電信國家型計畫 VoIP 平台上加入了 SIP VoIP 監控的機制，提供通連記錄、網路電話監聽，以及即時訊息通知等功能。此一系統之實作已獲得 2005 年教育部通訊教育程式設計競賽大專組冠軍。關於系統效能部分，經過針對多台 RTP 伺服器之架構之效能評估，本論文發現建置五台 RTP 伺服器系統可以較不會受到負載量與處理時間變異數的影響。

6. References

[1] M. Handley, V. Jacobson, RFC 2327 SDP: Session Description Protocol, April 1998.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, RFC 3261 SIP: Session Initiation Protocol. June 2002.

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

[4] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, RFC 3550 RTP: A Transport Protocol for Real-Time Applications, July 2003.

[5] Iptel SER網站（http://www.iptel.org/ser）

[6] FreeRADIUS網站（http://www.freeradius.org）

[7] Raj Jain, A Comparison of Hashing Schemes for Address Lookup in Computer Networks, October 1992.

[8] S.M. Ross. Introduction to Probability Models. Harcount/Academic Press, 2000.