SIP VoIP 電話總機系統於 NAT 閘道器之設計與實作

陳景章　　蘇暉凱　　姚志臻　　劉柏廷*
中正大學電機工程學系
u9042048@ccu.edu.tw

摘要

SIP (Session Initiation Protocol) [1]是近幾年網際網路應用因應多媒體傳輸需求所快速發展出來的通訊協定，由於其結構簡單，彈性以及擴充性極佳，近年來逐漸受到重視與廣泛應用，越來越多的多媒體應用軟體和硬體都以 SIP 為主要的通訊協定。但 SIP 通訊協定的設計並無法通過 NAT 設備，而且在具 NAT 的網路環境，對於 VoIP 電話總機與電話轉接程序也無標準規範。本論文將探討防火牆與 NAT 對 SIP 造成的影響，透過 SIP ALG 之設計與實作，解決 SIP 通過 NAT 設備所發生的問題，並在此環境下實作 SIP VoIP 電話總機系統進行電話轉接、留言等電話服務。

關鍵詞：SIP (Session Initiation Protocol)，NAT(Network Address Translation)，SIP proxy server，IP telephony，ALG (Application Layer Gateway)

1. 前言

隨著網際網路 (Internet) 的快速發展，在網際網路上的應用越來越多，從早期的文字，到圖形、聲音與影像...等等。從 1996 年以來，網際網路電話一直是大家所關切的網路應用技術，其相關的通訊協定主要有 IETF (The Internet Engineering Task Force) 提出的 SIP 與國際電信聯盟 (ITU-T) 所提出來的 H.323 協定。SIP 是一個近年來受到廣泛注意與研究的協定，相較於 H.323，由於 SIP 的格式簡單，設計非常有彈性，所以較容易擴充，也比 H.323 容易實現，更由於 SIP 是 IETF 所提出，所以 SIP 與其它 IETF 所提出的協定，如 SDP (Session Description Protocol)，RTSP (Real-Time Streaming Protocol)，SAP (Session Announcement Protocol) 等協定相容性較 H.323 來的高。

在網際網路發展部分，由於 IPv4 之 Public IP 的不足，NAT (Network Address Translation) [NAT RFC] 廣泛被應用於企業網路與家庭網路。但由於 NAT 機制只轉換 Private IP Address 成 Public IP Address，而且在內部對外連線中，只管理 TCP Connection 資訊，讓該 TCP Connection 的反向封包可以回到內部 Private IP Address 之電腦終端。因此，NAT 對於在應用層中攜帶 IP Address 資訊，而且透過 UDP 傳輸的應用層通訊協定，會造成通訊中斷的問題，SIP 通訊協定即是一典型例子。

當 SIP 電話由內部網路 Private IP Address 之網路電話撥打到 Internet 之網路電話時，即會由於 NAT 機制的原因，而造成 SIP Phone 無法正確建立電話連線。另一方面，當 SIP 電話由 Internet 之網路電話撥打到內部 Private IP Address 之網路電話時，會由於 內部網路電話是 Private IP Address 而無法直接撥打到內部網路之電話，如果先撥打到 NAT 上之 SIP ALG，亦無法透過 SIP Phone 電話轉接之標準規範 [SIP Call Forwarding Ref] 將電話轉接到內部網路電話。

本論文之目的在 NAT 網路環境，於 NAT 閘道器設計與實作 SIP VoIP 電話總機系統，同時解決 SIP Phone 穿透 NAT 網路設備與外部網路電話撥打內部網路電話分機之轉接問題，並且提供如傳統電信網路之電話總機服務。本系統提供使用 NAT 環境的企業與家庭一個解決方案，不但沒有受到 NAT 的限制，反而將 NAT 擴展成具有電話總機功能的設備，讓內部網路電話也可以像一般具有 Public IP Address 之網路電話來使用。

2. SIP 標準簡介

SIP 是一個以文字格式為基礎的傳輸協定，在建立多媒體通訊時，會使用 SDP (Session Description Protocol) 來溝通彼此支援的多媒體能力以及多媒體傳輸的相關設定資訊，包含多媒體格式、網路位址以及通訊埠。當多媒體所需的資料溝通完成後，便會根據溝通後的結果使用 RTP (Real-time Transport Protocol) 來傳遞即時的聲音以及影像。SIP 運作的基本流程可參考圖 1:

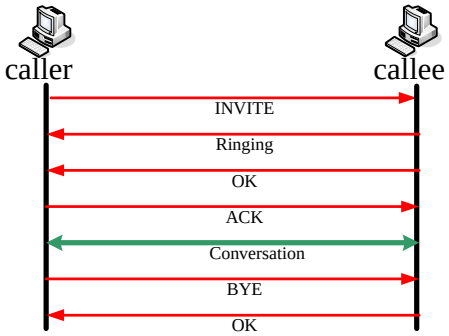

圖 1. SIP 在點對點環境下的運作流程

首先發話端 (caller) 送出 INVITE 給受話端 (callee)，其中利用 SDP 格式告訴對方自己的多媒體能力與自己即將在哪個通訊埠接收語音，接著發話端接收到 Ringing 的信號表示對方正在響鈴中，受話端接受通話後，回傳 OK 的訊息，利用相同的方式回應對方自己的多媒體能力與自己即將在哪個通訊埠接收語音，最後雙方根據之前所交換的資料，使用 RTP 傳送語音給對方。

由前述的流程可得知，SIP 主要是負責控制的信令 (Signaling)，真正傳送語音的時候，是利用 RTP 來傳送的。SIP 除了圖 1 的點對點通訊外，也定義了許多的通訊節點以利在大型網路透過來傳送，簡介如下：

- User Agent：SIP 的終端設備，是一台支援 SIP 的網路電話，可能是個人電腦，接上麥克風與喇叭。
- Redirect Server：告知發話端哪裡能找到受話端，並讓發話端重新作出邀請，並不幫忙傳送 SIP 封包。
- Proxy Server：向 Location server 查詢使用者所在位置的資訊，並盡可能幫忙發話端傳送 SIP 封包直到受話端收到為止。
- Registrar：接受使用者的註冊，並將目前使用者所在的位置資訊存放在 Location server。
- Location Server：通常為 Registrar 的資料庫，用來存放已註冊的使用者目前所在位置的資訊

3. 實驗環境與設計原理

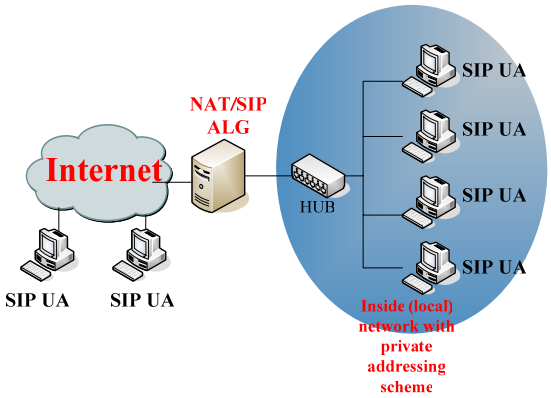

圖 2. 實驗環境

如圖 2 所示，在本論文的實驗環境中架設 NAT Server，讓 LAN 底下的電腦可以順利連上網路，並整合架設在 NAT server 上的 SIP ALG (Application layer gateway) 進行 VoIP 服務與通訊。Partysip 是一個架設 SIP proxy server 的開放原始碼軟體，該軟體是由法國的 WellX Telecom 公司在 1999 年所發表的，他們致力於提供可變通性和適用於中小型企業環境的軟體開發，所以我們藉由修改 Partysip 建立 SIP ALG，來解決 SIP 穿越 NAT 或是防火牆的問題。

3.1 SIP 穿越 NAT 或防火牆的問題

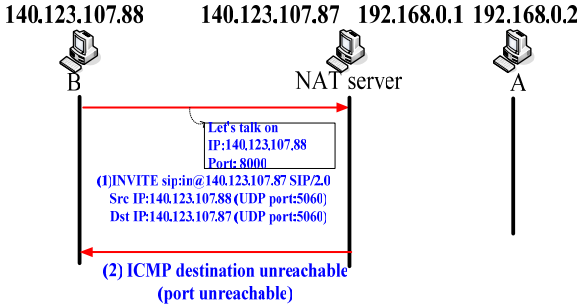

圖 3. 由 Internet 發話穿越 NAT 的情形

在本論文的實驗環境中，建立網路電話的情形有兩種：

1. 第一種是由位於 Internet 的使用者主動發出要求給位於 NAT server 內的使用者進行網路通訊。如圖 3 所示，位於 Internet 的使用者 B 想跟使用者 A 進行網路通訊，主動發出 SIP request “INVITE”到 NAT server，但是由於 NAT server 並沒有開啟此通訊埠的服務，所以會回應給使用者 B 一個 ICMP 的訊息，告知使用者 B 無法開啟此連接埠的服務。因為在 NAT server 內部的使用者 A 並不會收到來自使用者 B 的 SIP request “INVITE”，所以建立網路通訊勢必失敗，這是因為使用者 A 位於 NAT server 內部的 LAN 環境中，所有要到使用者 B 的封包都必須經過 NAT server，所以要到 NAT server 內部的訊息在 NAT server 就會被攔截，也因為 NAT server 並沒有開啟通訊

埠等待發話端的網路通訊要求，所以建立通話失敗。

2. 另一種如圖 4 所示，由位於 NAT server 內的虛擬位址 192.168.0.2 使用者 A 主動發出 SIP request 邀請位於 Internet 的使用者 B，此邀請訊息中包含了 SDP (Session description protocol) 訊息，告知使用者 B 自己的多媒體編/解碼能力與自己即將在虛擬網路位址 192.168.0.2 的通訊埠 9000 接收語音。當使用者 B 接起電話後，會發出 SIP 200 OK 的訊息給 NAT server，再由 NAT server 轉送到使用者 A，此訊息包含了 SDP 訊息，告知使用者 A 語音封包需要傳送到 140.123.107.88 的通訊埠 8000。當信令溝通完成後，使用者 A 的聲音封包經過 NAT server 可以被成功的傳送到使用者 B，而使用者 B 的聲音封包會被要求傳送到虛擬網路位址 192.168.0.2，這時候使用者 B 所在網路之路由器就會傳回 ICMP 的訊息，告知使用者 B 無法傳送到指定的目的地，所以建立網路通訊失敗。類似的問題也會發生在 SIP 經過防火牆的時候，假設防火牆允許使用標準的 SIP 通訊埠 5060 的封包通過，所以 A 和 B 可以順利的進行 SIP 訊息的交換，但是當 B 要送 RTP 封包給 A 的時候，或者當 B 要送 RTP 封包給 A 的時候，因為通訊埠不固定，會被防火牆擋住。

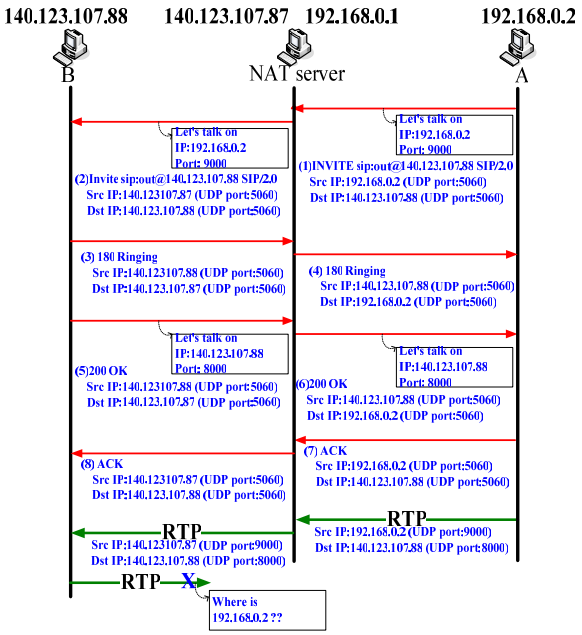

圖 4. 由 NAT 內部發話穿越 NAT 的情形

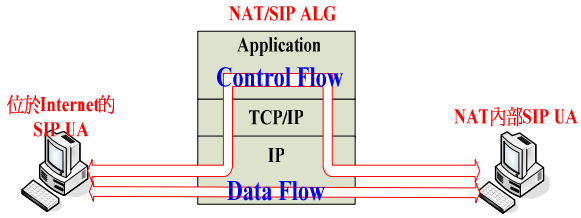

圖 5. SIP ALG 運作流程

3.2 讓 SIP 穿越 NAT 或防火牆的方法

目前有許多穿越 NAT 或防火牆的方法被提出來，其中 STUN(Simple Traversal of UDP Through NAT) [2]、TURN(Traversal Using Relay NAT) [3]、UPnP (Universal Plug and Play) [4] 都必須要有使用者端的 SIP 設備支援才可以穿透 NAT 與防火牆。本論文中利用防火牆或 NAT 設備配合外掛的程式來支援 SIP/RTP，這種方式的原理是透過與防火牆或 NAT 的緊密結合，延伸現有的功能，達到支援 SIP/RTP 的目的，而使用者端的 SIP 設備，並不需要額外的支援，就可以穿透 NAT 與防火牆，這種方式通常被稱為 SIP ALG (Application Layer Gateway)。

如圖 5 所示，成功建立一通網路電話必須完整建立好控制通道 (Control Flow) 與資料通道 (Data Flow)。控制通道的部分是利用 SIP 來建立的，特別的是當發話端發出 SIP request 的訊息給受話端，在經過 NAT server 的時候會經過 SIP ALG 的處理，將控制訊息內容中，包含有內部電腦之 Private IP Address 與 Private IP Address 之 URI 加以修改成 Public IP Address 再傳送給外部網路之受話端，而 SIP ALG 會根據受話端的回應做出適當的動作。透過 IP 層 IP Packet Redirect 之技術，將欲傳送到內部網路電話之 Media Channel Packet (RTP Packet) 導向到內部網路之網路電話；然而，欲送到外部網路之 Media Channel Packet，則透過一般 NAT 機制，將封包轉換到外部網路電話。所以透過此機制之設計，可以避免前述圖 4 的問題，進而成功地建立兩端的 RTP 資料通道。

4. 服務整合實作

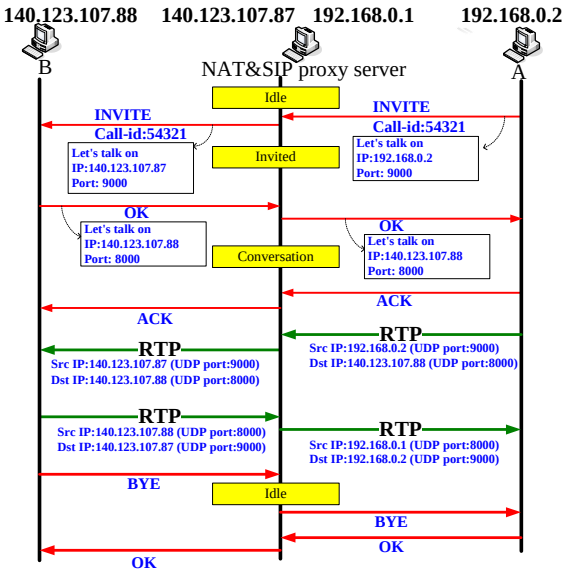

圖 6.NAT 內部發話的信令傳遞

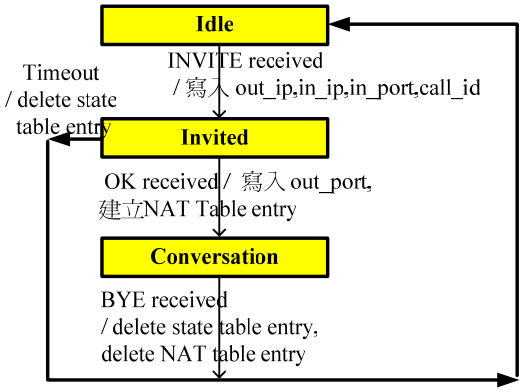

圖 7.內打外的有限狀態圖

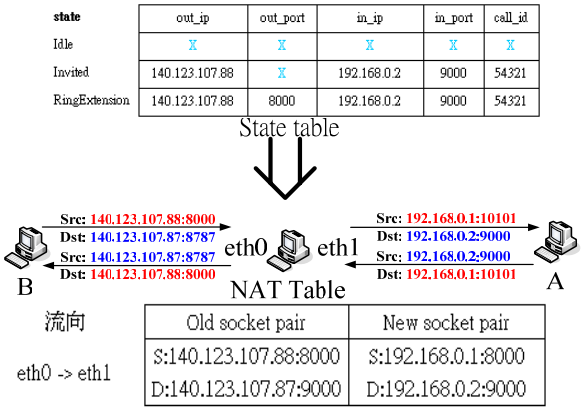

圖 8.NAT 內部發話的 NAT table 建立流程

4.1 由 NAT 內部發話穿越 NAT 的實作

Partysip 是一套免費的開放原始碼軟體，再配合由 oSIP 提供的函式庫可以整合 SIP registrar、redirect server、proxy server 為一體；經由我們的修改，使其具有 SIP ALG 的功能。

利用 SIP ALG 建立網路通訊的情況仍然是分成兩種，第一種是由位於 NAT server 內部的使用者主動發出 SIP INVITE 給位於 Internet 的使用者進行網路通訊。圖 6 為 NAT 內部發話的信令傳遞流程圖，圖 7 為其有限狀態圖 (Finite Sate Machine)；一開始 SIP ALG 狀態是處於 "Idle" state，表示正在等待使用者 A 發出 INVITE 訊息。

當收到從 NAT 內部的使用者 A 發出的 INVITE 訊息後，SIP ALG 將 SDP 中的虛擬網路位址修改為 SIP ALG 的 Public 網路位址，然後將修改完的 SIP INVITE 訊息傳送給使用者 B，接著寫入 state table 記錄目的地網路位址(out_ip)、來源網路位址(in_ip)、SDP 中語音封包傳送的通訊埠(in_port)、Call-ID，SIP ALG 狀態進入"Invited" state (記錄 Call-ID 的用意，在於識別與方便管理 state table 中該筆 Session 紀錄)，同時啟動 timer，時間設定為五分鐘。

如果在五分鐘以內都沒有收到任何同一個 Call-ID 的 SIP 訊息，SIP ALG 就會 timeout，刪除 state table 中該筆資料，進入"Idle" state；如果這時收到受話端的 SIP 200 OK 訊息，則我們可以擷取 SIP 200 OK 的 SDP 訊息中，語音封包傳送的通訊埠(out_port)，並根據 Call-ID 找尋到該筆紀錄的位置，寫入 out_port 補足 state table，然後立刻建立 NAT table，進入"Conversation" state，並照著 NAT Table 的規則轉送 RTP 語音封包，此時通話正式建立成功。當 SIP ALG 收到 SIP BYE 訊息，表示任一方想要結束通話，此時我們刪除 state table 與 NAT table 的相關紀錄，回到"Idle" state。

在我們的設計當中有兩個 table，state table 與 NAT table，state table 的目的是蒐集相關的資訊以便建立 NAT table，而且 state table 中的資料會隨著 state 的不同而改變，而 NAT table 就是 NAT server 的網路位址轉換規則，以圖 6 為範例，圖 8 的 state table 顯示該筆紀錄在每個 state 的情形，圖 8 的 NAT table 表示要將從使用者 B 的通訊埠 8000 傳送到 SIP ALG 通訊埠 9000 的 UDP 封包導入到使用者 A 的通訊埠 8000。

4.2 電話總機服務

考慮第二種的情形:由位於 Internet 的使用者主動發出 SIP request 邀請位於 NAT server 內部的使用者進行網路通訊。電話總機服務，我們使用兩段式的方法來建立使用者 A 與 B 的網路通訊。

1. 當 Internet 網路電話撥打到 SIP ALG，SIP ALG 會先將外來的電話接起來，然後播放語音訊息，告知使用者 B 在 NAT 內部各個使用者的分機號碼，並要求輸入分機號碼。
2. 當 SIP ALG 收集完分機號碼後，再對該分機

發出 SIP INVITE 的訊息。

此時 SIP ALG 的運作就像是兩個 User Agent，一個負責建立與位於 Interne t 的使用者之間的網路通訊，另一個負責建立與位於 NAT server 內部的使用者之間的網路通訊。

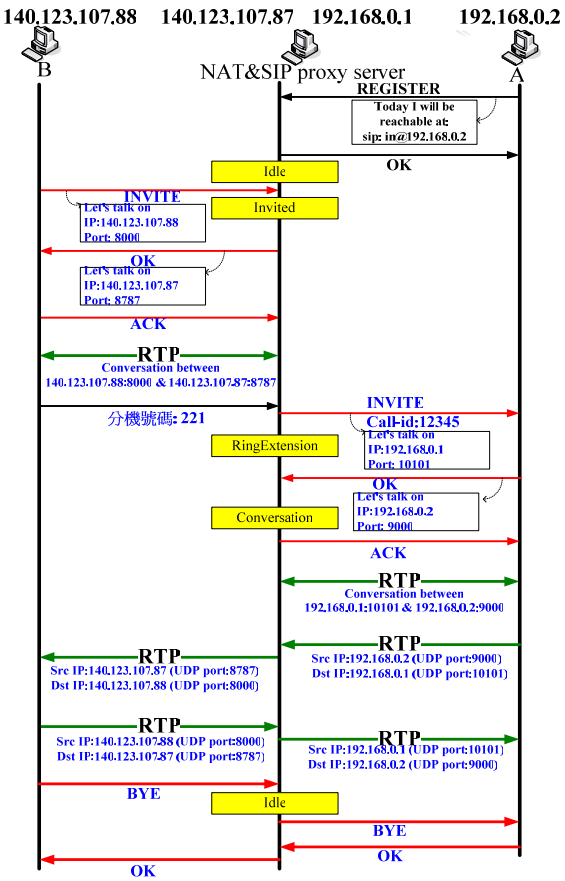

圖 9. 總機服務的信令傳遞

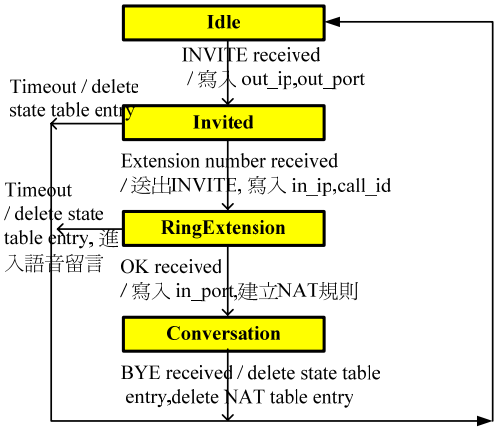

圖 10. 電話總機服務的有限狀態圖

表 1 分機號碼和 IP 對應表

分機號碼	IN_IP	alias
221	192.168.0.2	阿印
223	…	…

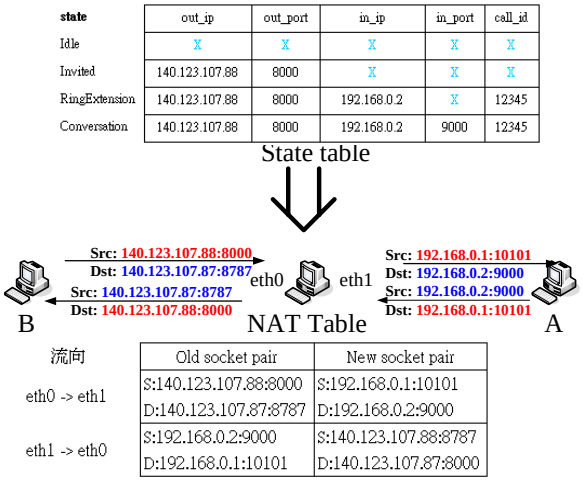

圖 11. 電話總機的 NAT table 建立流程

圖 9 為從 NAT 外部發話的通話建立流程圖，圖 10 為電話總機的有限狀態圖， 當 NAT 內部的使用者上線，會先對 SIP ALG 進行註冊動作，告知 SIP ALG 目前所在位置 (Private IP Address)，SIP ALG 再根據先前設定好的分機號碼與別名的對應，建立表 1。

一開始 SIP ALG 是處於"Idle" state，當收到從使用者 B 發出的邀請訊息後，記錄使用者 B 的來源網路位址 (out_ip)、SDP 訊息中語音封包傳送的通訊埠 (out_port) 於 state table，SIP ALG 的狀態進入 "Invited"，同時啟動 timer，時間設定為 5 分鐘，當 timeout 發生時，便自動地將此筆紀錄刪除。在成功的建立起 SIP ALG 與使用者 B 的網路通訊後，SIP ALG 會播放電話總機的語音訊息，告知使用者 B NAT 內部各個使用者的分機號碼，並要求輸入分機號碼，這時候使用者 B 輸入的分機號碼經過 SIP ALG 分析，配合事先已經建立的分機號碼與使用者網路位置對照表，可以得知欲通話的是使用者 A。

在進行轉接的同時， SIP ALG 會播放一段音樂給使用者 B 聽，再由 SIP ALG 對該分機送出 INVITE 訊息，並寫入使用者 A 的網路位址 (in_ip) 與 call_id 於 state table ，這時 SIP ALG 進入 "RingExtension" state，timer 重新啟動，當 timeout 發生代表使用者 A 並沒有接起電話，SIP ALG 會中斷與使用者 A 之間的網路通訊建立，刪除 state table 中的紀錄並且播放一段語音訊息給使用者 B，詢問要不要留言給使用者 A，當 B 留完言後或是選擇不留言時，SIP ALG 中斷和使用者 B 的網路通訊，並且回到 "idle" state。

而如果使用者 A 接聽電話，並且成功的建立 SIP AL 和使用者 A 的網路通訊，此時 SIP ALG 根據 Call-ID 可以找到該筆紀錄的位置，並寫入使用者 A 所使用的語音 RTP 封包通訊埠 (in_port) 補足 state table，然後立刻建立 NAT table，如圖 11 所示，並依照 NAT table 的規則轉送封包。從使用者 B 的通訊埠 8000 傳送到 SIP ALG 的 UDP 封包導入到使用者 A 的通訊埠 9000；從使用者 A 的通訊埠 9000 傳送到 SIP ALG 的 UDP 封包導出到使用者 B 的通訊埠 8000。

5 結論

本論文在 NAT 閘道器上設計與實作 SIP ALG 與 SIP 語音總機服務系統，在具 NAT 設備之網路環境中，提供兩段式 SIP 電話轉接與電話留言功能。進而解決 SIP 穿越 NAT 或防火牆，以及 Internet SIP 網路電話撥打 NAT 內部網路電話所面臨的問題。在 NAT 網路環境中，未來我們將朝向 SIP ALG 相關多功能的加值服務發展。相信本論文之服務整合和系統整合成果，對未來網路服務應用的發展，能提供一個新的構思。

參考文獻

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

[2] J. Rosenberg J. Weinberger C. Huitema R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, IETF, March 2003.

[3] Rosenberg, J., "Traversal Using Relay NAT (TURN)", draft-rosenberg-midcom-turn-02, March 2003.

[4] UPnP forum, Internet Gateway Device(IGD), V1.0 For Universal Plug and Play Version1.0, http://www.upnp.org, November 19, 2001