建立及分析 SIP-bases VoIP 穿透 NAT 機制

Construct and analyze SIP-based VOIP traversal over NAT mechanisms

趙啟時　呂思霈　黃柏鈞

逢甲大學通訊工程系所

D9157856@fcu.edu.tw

摘要

由於 NAT 的發展，使用一台 NAT 來轉換 IP 位址，使 NAT 內部的主機可以跟 NAT 外部主機相互通訊，因此，解決了 IPv4 IP 不足的問題，但卻也帶來了另外的難題。如本研究所要介紹的 VoIP 穿透 NAT 問題。因為 NAT 只處理網路層及傳輸層的資訊，當屬於應用層的 SIP 資訊，在通過 NAT 時，NAT 並不會修改 SIP 訊息(封包中應用層部分，包括 SIP 標頭和 SIP 本體)中所帶的 IP 位址與通訊埠，這些 SIP 訊息中的資訊在經過 NAT 之後將會發生錯誤。因此，本研究將使用三種透通技術---Session Controller、STUN 以及 VPN，解決 VoIP 在 NAT 環境裡所遇到的問題，並分析三種解決方案的特性(是否支援 SIP UA、是否需要 NAT 支援、是否需要額外伺服器)、佈署的便利性(設定難易度、通訊延遲、DHCP 的影響)和限制(是否可穿越對稱式 NAT、是否可穿越多層 NAT、是否需要額外公眾 IP、SIP UA 是否需要支援對稱式 RTP)。本研究部署 SIP、NAT、STUN、Session Controller 和 VPN 伺服器，構成 VoIP 平台，經過封包的分析，來發現 VoIP 實際上的問題，並且比較三種透通技術的優缺點，以期能提供企業部署 VoIP 平台時的參考。

關鍵詞:VOIP、SIP、防火牆穿透、STUN、Session Controller、VPN

Abstract

Due to the development of NAT, using NAT to translate IP address can let the hosts inside NAT connect to the outside. Therefore, it solves the problem of insufficient IP, but it also brings other difficulties. For example, “the problem of VoIP traversal over NAT” that is introduced in the present research is one of them. NAT only handles the information on network and transport layer; thus when SIP information, part of the application layer, passes through NAT, NAT does not modify SIP messages (which include IP address, port in header field and body on the application layer). These SIP messages may cause errors after passing through NAT. Therefore, this research implement three kinds of transparent technologies-- Session Controller、STUN and VPN, to solve the problems in the NAT environment. Besides the characteristics (Whether they support SIP UA, need NAT support or need extra server), the availability of disposition (Configure difficulty, communication delay, and the influence of DHCP) and limitation (Passes through symmetric NAT and multi-storey NAT, and if SIP UA needs to support symmetric RTP) of these three schemes are also analyzed. This study disposes SIP, NAT, STUN, Session Controller and VPN servers to construct VoIP platform, and after analyzing packages, the actual problems of VoIP are discovered. Finally, this paper compares the advantages and defects of the three kinds of transparent technologies to provide enterprises with the references for disposing VoIP platform.

Keyword: VOIP、SIP、NAT Transparent、STUN、Session Controller、VPN

1. 前言

SIP 即 Session Initial Protocol 的簡稱，由 IETF 所設計及發展的應用層控制協定（Application-layer Control Protocol），此協定設計的目標是容易建置、具可擴充性及彈性，其主要是用於建立、更改及結束一個或多個參與者的通話。在目前的網路環境中，由於 IPv4 地址資源的限制或出於網路安全的考慮，NAT 設備廣泛存在，如何使工作在應用層的 SIP 協議穿越 NAT 是 SIP 應用研究中的一個重要問題。

NAT 技術目前主要應用於 IP 及 UDP/TCP 層，即對 IP 封包的地址及端口埠進行轉換，而 SIP 協議是基於 UDP/TCP 之上的應用層控制協議，SIP 封包標頭中含有很多關於路由、接續 SIP 信號和建立呼叫連接的地址資訊，而且真正的媒體連接資訊是放在 SDP，即 IP 封包的負載中傳遞的，這部分的私人網地址在穿越 NAT 時不能被轉換，因而造成 SIP 信號尋址不成功或媒體通道不能建立。

對於一個基於 SIP 的電話呼叫，可以分為兩部分：第一部分是信號，也就是建立呼叫的協議消息；第二部分是實際傳輸的 RTP 媒體流，在兩個終端設備或終端與閘道器之間。信號部分的 NAT 穿越，相對簡單，因為在典型的 SIP 系統中，終端離開 NAT 後的第一站通常為默認的代理伺服器，只要代理伺服器將對方的消息發送到接收包的源地址，即可穿越 NAT。對於媒體流，由於是基於即時傳輸協議（RTP）和採用動態分配 UDP 埠方式，終端用戶在實際傳輸媒體流之前是無法預知對方媒體流的對外埠的。當終端用戶處在 NAT 之後時，問題變得更加複雜。SIP/NAT 問題就是 SIP 訊息及媒體流能否順利穿越 NAT 的問題。隨著語音和視訊的蓬勃發展，SIP/NAT 問題已成為基於 SIP 的 VoIP 技術，在 NAT 設置的網域和企業網路中推廣應用的最大障礙。

2. 系統架構

要組成 SIP 網路架構共可分為四個部份：User Agent、Redirect Server、Proxy Server、Registrar。

（一）User Agent

UA 是有通話能力的終端節點，通常以應用程式的方式在使用者電腦中，也可以是手機、PDA、PSTN 閘道器等等。UA 依行為不同分為 User Agent Server（UAS）和 User Agent Client（UAC）。

（二）Proxy Server

Proxy 的功能就是轉送 SIP 訊息，將發話方建立通話邀請的訊息，經由 Proxy 轉送給受話方。

（三）Registrar

Registrar 的功能是儲存註冊的資料，其內建資料庫，當 UA 向它註冊時，會把 UA 的資料儲存在資料庫中，最主要儲存的資料是 SIP URI 對應的 IP 位址。Registrar 其實是一個應用程式，通常與 Proxy 共置於同一部機器及系統中。在建立通話之前，必須要先向 Registrar 註冊，才可以建立通話。

（四）Redirect Server

Redirect Server 的功能是重新導向請求。當受話方沒有回應或是表示離開時，表示受話方已經不再原本的位置，Redirect Server 會向 Location Database 查詢受話方新的位置，然後請發話方再送一次建立通話邀請的訊息到受話方新的位置。而 SIP 基本的通話流程為下圖 1:

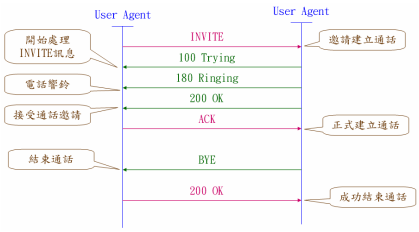

圖 1 通訊流程

SIP 通話流程（包含 Proxy），如下圖 2：

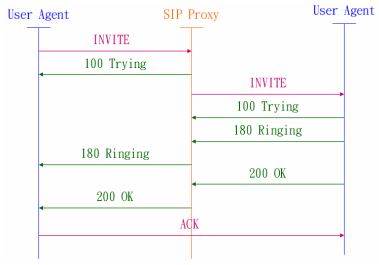

圖 2 包含 proxy 的通訊流程

當 NAT 遇上 SIP 時，其系統架構如圖 3。SIP 訊息是從內部網路傳送出去，所以 Contact 裡的 IP 位址會是私有 IP 位址 192.168.0.2。因為當建立通話邀請從 192.168.0.2 這個私有 IP 位址送出時，經過 NAT

只會處理網路層 IP 位址，把私有 IP 位址 192.168.0.2 改成公眾 IP 位址 140.134.30.149，並不會處理屬於應用層的 SIP 訊息，也因此 SIP 通話就會出現問題，導致無法正常運作。因此，我們提出了 3 種方法---STUN、Session Controller、VPN 來解決目前 NAT 所遇到的瓶頸。

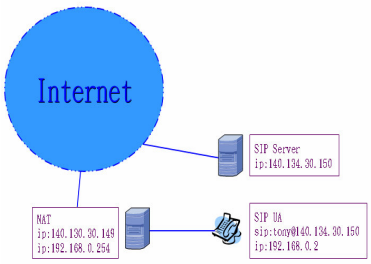

圖 3 NAT 與 SIP 架構

3. 系統元件

由上可知，若能將 SIP 訊息中的私有 IP 位址和通訊埠修改為正確的公眾 IP 位址和通訊埠，則公眾網路上的 SIP 設備就可以將封包正確地送達私有網路內的 SIP 設備。為了要克服 SIP 穿越 NAT 的問題，我們採用三種 NAT 通透技術--STUN、Session Controller、VPN。根據設計理念不同，將這些機制分為三大類，第一類是直接取得一個可用的公眾 IP 位址，使用虛擬私有網路(VPN)的解決方式即屬此類。第二類是由私有網路內的 SIP 設備聯合其他伺服器，取得封包送出 NAT 後，網路層和傳輸層上的 IP 位址和通訊埠，用以修改欲送出的 SIP 訊息，靜態指定、STUN 則屬此類。最後一類則是由公眾網路上的 SIP 設備(Session Controller)修改 SIP 訊息中的 IP 位址與通訊埠。

3.1 STUN

STUN（Simple Traversal of User Datagram Protocol Through Network Address Translations）為伺服器/客戶端架構的通訊協定，STUN 客戶端為在私有網路內的 SIP UA，而 STUN 伺服器則是置放在公眾網路上，STUN 客戶端在需要得知對應 IP 位址與通訊埠時，會先以相同的來源 IP 位址與通訊埠送封包給 STUN 伺服器，由 STUN 伺服器告知此封包被 NAT 轉換後的來源 IP 位址和通訊埠，透過此協定讓內部設備知道 NAT 配置給它的對外 IP 是多少。如圖 4 為 SIP UA 註冊流程圖。

內部 SIP UA 先向 STUN Server 詢問對外 IP 是多少，所以發送一個 Binding Request 的訊息，然後 STUN Server 收到後，就回傳一個 Binding Response 的訊息，告知內部 SIP UA 的對外 IP。內部 SIP UA 知道後，送出註冊訊息給 SIP Server 時，訊息內的 Contact 欄位就改成對外 IP 是 140.134.30.149。

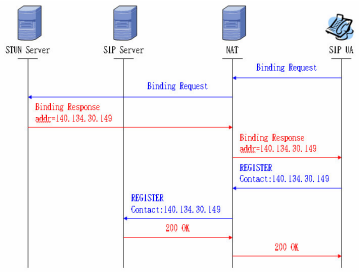

圖 4 SIP UA 註冊流程圖

STUN 訊息分為 Binding Request 和 Binding Response 兩種訊息，Binding Request 是要求知道內部設備的對外 IP；Binding Response 是回應告訴內部設備的對外 IP。下圖 5 為其架構圖。

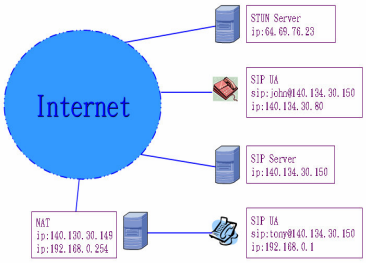

圖 5 STUN 架構圖

一開始內部 SIP UA 會送 Binding Request 訊息，這個動作隨時都會作，因為對外 IP 有可能會有變動，所以內部 SIP UA 常常要會去詢問 STUN Server。而 STUN Server 如何得知內部 SIP UA 的對外 IP，其實很容易，從接收到封包的來源端 IP 位址就可以得知。內部 SIP UA 知道它的對外 IP 後，就開始送出建立通話邀請的訊息，當完成通話邀請後，就會開始通話，而整個通化流程將化一般的 SIP 通化流程沒有什麼差異，因為其 Contact 欄位已經不受 NAT 私有 IP 的影響了。

3.2 Session Controller

第二種透通技術是 Session Controller，利用 SIP

Proxy 和 RTP Proxy 達到透通的目的。SIP Proxy 負責 SIP 訊息的處理和轉送，而 RTP Proxy 則負責 RTP 封包的處理和轉送。SER 本身具有 SIP Proxy 的功能，加上使用 SER 內建的模組 nathelper，其功能可以修改 Contact 欄位和 SDP 內的資料；RTP Proxy 的功能是封包轉送器，SIP Server 藉由 socket 和 RTP Proxy 溝通，讓 RTP 封包經由 RTP Proxy 轉送出去。

在 nathelper 模組中，會使用到二個 Exported Function：

（一）fix_nated_contact（）

修改 Contact 欄位，將 Contact 欄位修改成公眾 IP 位址，而公眾 IP 就是從封包中來源端的 IP 位址得知。因為原本封包中來源端的 IP 位址是私有 IP 位址，但是已經經由 NAT 轉換成公眾 IP 位址。由圖 6 可以看到上面 Contact 欄位是原本的私有 IP 位址，下面則是經過修改的 Contact 欄位。

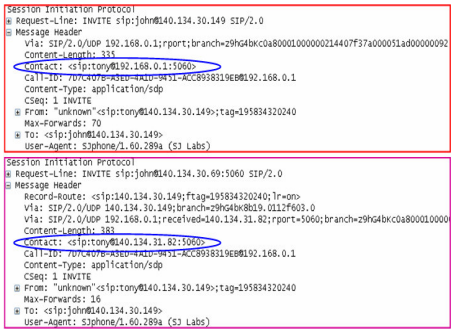

圖 6 fix nated contact

（二）fix_nated_sdp（）

修改 SDP 內的資料。由圖 7 可以看到上面圈起來的地方原本是私有 IP 位址，經過修改過後，變成下面的公眾 IP 位址，主要是讓 RTP 可以透過 RTP Proxy 轉送。

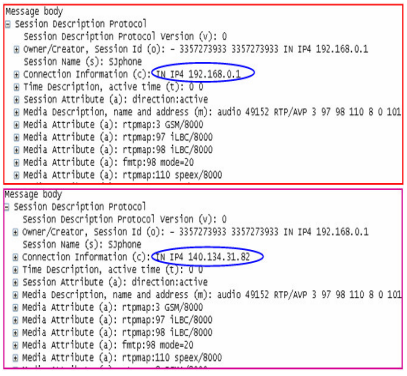

圖 7 fix nated sdp

由於要修改 Contact 欄位，因此需要修改 SER 的設定檔。如圖 8。透過 SER 可以用來判斷 SIP UA 是否在 NAT 內。nat_uac_test（“3”）表示 Contact 屬於私有網路的判斷，如果符合這個條件就修改 Contact 欄位為公眾 IP 位址。如果 SIP 訊息是 INVITE，表示要建立通話邀請的訊息，代表有使用到 SDP，那除了修改 Contact 外，SDP 的內容也要作修改，修改完後，flag 上標記為 1，代表 SIP UA 在 NAT 內。

```
route {
    # initial sanity checks -- messages with
    # max_forwards==0, or excessively long requests
    if (!mf_process_maxfwd_header("10")) {
        sl_send_reply("483","Too Many Hops");
        break;
    };
    if (msg:len >=  max_len ) {
        sl_send_reply("513", "Message too big");
        break;
    };
    if (nat_uac_test("3")) {
        append_hf("Alex-hint: NAThelper\r\n");
        fix_nated_contact(); # Rewrite contact with source IP of signalling
        if (method == "REGISTER" || ! search("^Record-Route:")) {
            if (method == "INVITE") {
                append_hf("Alex-hint: SDP rewritten\r\n");
                fix_nated_sdp("3"); # Add direction=active to SDP
            };
            log("LOG: Someone trying to register from private IP, rewriting\n");
            force_rport(); # Add rport parameter to topmost Via
            setflag(6); # Mark as NATed
        };
    };
}
```

圖 8 SER 設定檔

第二種透通技術 Session Controller 是利用 SER 內建模組 nathelper，使 SIP Server 擁有修改 Contact 欄位的功能，加上 RTP Proxy 的輔助，完成 NAT 透通。它不需要額外的 Server，而第三種透通技術 VPN，則跟第一種透通技術一樣，也需要額外的 Server。

3.3 VPN

虛擬私有網路（Virtual Private Networks, VPN）的定義是利用網際網路建立通道（tunnel），提供有效且安全的傳輸，交換私有訊息。其用途有兩種，一種是通過網際網路實現遠端用戶存取，另一種是通過網際網路實現網路互連。如圖 9，為 VPN 架構圖。首先內部 SIP UA 和 VPN Server 建立通道，再

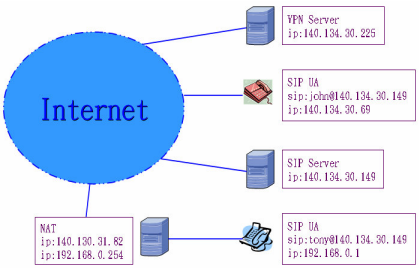

圖 9 VPN 架構圖

透過 TCP 和 VPN Server 連線，最後，SIP UA 即可透過 VPN Server 向 SIP Server 做註冊的動作。

VPN 要建立通道，使用的通道技術（tunneling），是將其他協定的封包重新封裝（encapsulate）在新的標頭中，經由通道傳輸，傳達目的地後，再解開封裝的封包。建立通道的通道協定有三個：點對點通道協定（PPTP-Point to Point Tunneling Protocol）、第二層轉遞（L2F-Layer 2 Forwarding）、第二層通道協定（L2TP-Layer 2 Tunneling Protocol）。如圖 10，為其本文使用 PPTP 協定，在建立通道後的整個連線過程。

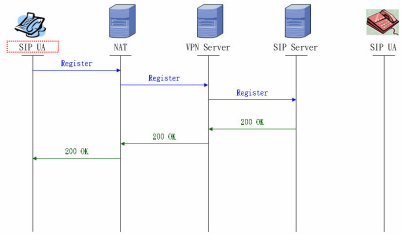

圖 10 完整連線圖

建立通道後，內部 SIP UA 要向 SIP Server 註冊，內部 SIP UA 傳送註冊訊息，會先經過 NAT，這時 SIP 訊息內的 Contact 已經是 VPN Server 所分配的 IP。註冊訊息會經過 NAT 傳到 VPN Server，而 VPN 會解開封包取得目的地，之後便把封包傳到目的地 SIP Server，當 SIP Server 收到註冊訊息，儲存完資料後，就回送一個註冊成功的訊息。而 SIP 訊息經過 VPN Server 要到內部 SIP UA 時，這時 VPN Server 會使用封裝。最後到達目的地，便會自動解封裝，並且完成註冊程序。

4. 透通技術之效能分析與結論

透過透通技術設備支援表、透通技術方便性表和限制性，來分析這三種透通技術的差異。表 1，

項目 / 透通技術	SIP UA	NAT	額外伺服器
STUN	需要	不需要	需要
Session Controller	不需要	不需要	需要
VPN	需要	不需要	需要

表 1 透通技術設備支援表

第一項是透通技術是否需要 SIP UA 支援。STUN 和 VPN 都需要 SIP UA 的支援，SIP UA 需要設定支援 STUN 的功能，才能扮演 STUN Client 的角色，向 STUN Server 要求對外的 IP 位址；SIP UA 也需要設定支援 VPN 的功能，才能扮演 VPN Client 的角色，向 VPN Server 建立通道。而 Session Controller 只要修改 SIP Server 的設定檔，不需要 SIP UA 支援。第二項是透通技術是否需要 NAT 支援。三種透通技術都不用 NAT 支援。第三項是透通技術是否需要額外的伺服器。STUN 需要有 STUN Server；Session Controller 需要有 RTP Proxy；VPN 需要有 VPN Server，所以三種透通技術都需要額外的伺服器。

項目 / 透通技術	設定難易度	通訊延遲	DHCP
STUN	次容易	最短	無影響
Session Controller	最容易	次短	無影響
VPN	最困難	最長	無影響

表 2 透通技術方便性

表 2，第一項是設定的難易度。Session Controller 只要修改 SIP Server 的設定檔，在啟動 SIP Server 後，就不需要做任何的設定，所以最容易。STUN 需要 STUN Client 設定 STUN Server 的 IP 位址和埠號，容易程度僅次於 Session Controller。VPN 則需要設定 VPN Server、還需要進行登入的動作，因此會比較複雜。第二項是通訊延遲，雙方建立通話連線的時候，會需要額外的時間來達到 NAT 透通，這個額外的時間就是通訊延遲。STUN 在每次建立通話連線時，都需要一小段的時間，來詢問內部 SIP UA 送出的封包從 NAT 出去後的 IP 位址和埠號。Session Controller 會有較長的時間延遲，因為 SIP 和 RTP 封包，全部都需要經由 Session Controller 的轉送，就是要經過 SIP Proxy 和 RTP Proxy 的處理。而時間延遲最久的是 VPN，因為所有的封包在經過 VPN Server 時，都要做封裝和解封裝的動作，因此造成長時間的傳輸延遲。第三項是當內部 SIP UA 所在的環境是使用動態 IP 位址分配（Dynamic Host Control Protocol, DHCP）時，是否會造成影響。結果三種透通技術並不會受到任何影響。而三種 VoIP 透通技術，除了 VPN 外，都滿常見到，VPN 之所以不常用，因為 VPN 的通訊延遲長，最重要的是，VPN 會浪費額外的 IP 位址分配給內部 SIP UA。

表 3，RFC-3489 第五章中根據處理 UDP 連線的方式，將 NAT 分為四種類型： Full Cone NAT、

Restricted Cone NAT、Port Restricted Cone NAT 和 Symmetric NAT，這三種機制中只有 STUN 無法穿越 Symmetric NAT。這是因為來源和目的地的 IP 位址及通訊埠搭配來分派對公眾網路的通訊埠，即只要封包的來源或目的地的 IP 位址或通訊埠不同，對

項目 / 透通技術	是否可穿越對稱式 NAT	是否可穿越多層 NAT	是否需要額外公眾 IP 位址	SIP UA 是否需要支援對稱式 RTP
STUN	否	是	否	否
Session Controller	是	是	否	是
VPN	是	是	是	否

表 3 NAT 限制性

應到的通訊埠就會不一樣。第二項，這三種機制皆可解決。此外，這三種機制中只有 VPN 需要額外的公眾 IP 位址；而只有 Session Controller 需要 SIP UA 支援對稱式 RTP。

以 SIP 為基礎所建構的 VoIP 是目前熱門的網路應用服務之一，而因為 NAT 的影響所造成的問題，本研究已提出解決方案。但是三種透通技術並沒有哪一種兼具方便、簡單、快速和通用的特性。STUN 需要不斷地詢問對外 IP，需要額外建置及管理 STUN Server；Session Controller 傳送封包都要經過 SIP Proxy 及 RTP Proxy 的處理；VPN 需要設定 VPN Server，以及長時間的通訊延遲。因此，在 IPv6 還未普及的情況下，VoIP 穿透 NAT 的問題，還是有探討的重要性，以期找尋較佳的解決方案。

參考文獻

[1] 電信研究雙月刊 第 35 卷第 2 期 VoIP 安全性機制--防火牆技術研究。

[2] VPN 虛擬私有網路，林宜宏著。

[3] 網路電話（IP 電信）系統規劃與建置，陳文生著。

[4] NTP VoIP 平台之 SIP 穿越 NAT 機制教學文件 http://yalin.tw/tanet2004/nat_traversal_of_sip_sdp.pdf。

[5] B.Gleeson, A.Lin, J.Heinanen, G.Armitage, A.Malis,"A Framework for IP Based Virtual Private Networks",IETF RFC-2764, February 2000。

[6] Ethereal: A Network Protocol Analyzer, http://www.ethereal.com/。

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

[8] iptel.org SIP Server: SIP Express Router, http://www.iptel.org/ser/。

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

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

[11] M. Handley, V. Jacobson, "SDP: Session Description Protocol", IETF RFC-2327, April 1998

[12] R. Droms, "Dynamic Host Configuration Protocol",IETF RFC-1541, October 1993

[13] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", IETF RFC-2616, June 1999。

[14] PortaOne nathelper RTP Proxy, http://www.portaone.com/resources/downloads/index.html。

[15] P. Srisuresh, M. Holdrege,"IP Network Address Translator (NAT) Terminology and Considerations", IETF RFC-2663, August 1999。

[16] Session Controller 設定，http://www.csie.nctu.edu .tw/~yhsung/voip/ser.html。

[17] SJphone, http://www.sjlabs.com。

[18] voip-info.org: RTP Symmetric, http://www.voip-info.org/wiki-RTP+Symmetric

[19] VPN , http://www.poptop.org。