SIP Traversal over NAT Mechanisms on NTP VoIP Platform

Ya-Lin Huang, Whai-En Chen, Quincy Wu and Yi-Bing Lin
Department of Computer Science and Information Engineering
National Chiao Tung University
{huangyl,wechen,solomon,liny}@csie.nctu.edu.tw

摘要

隨著網路頻寬的增加以及無線網路的普及，有越來越多的網路應用服務被開發出來，其中 VoIP 就是近來網際網路中最炙手可熱的應用之一。電信國家型計畫在兩年前開始佈建以 SIP 為基礎的 VoIP 平台，希望藉由平台建置與整合測試，發現 VoIP 實際應用上的問題並加以解決。由於每一個網路電話都需要一個 IP 位址，因此在佈建 VoIP 平台時，會遇到 IP 位址不足的問題。目前解決此問題最常見的方法是，使用一台 NAT 轉換器來轉換 IP 位址，使 NAT 內部的主機可以跟 NAT 外部主機相互通訊。然而 NAT 只會處理網路層與傳輸層的資訊，因此 SIP 訊息中所帶的 IP 位址與通訊埠，在經過 NAT 之後就會發生錯誤。本文將介紹在電信國家型計畫的 VoIP 平台中，利用虛擬私有網路、靜態指定、STUN、通用隨插即用以及 Session Controller 等五種機制穿越 NAT 的運作原理，並加以詳細分析比較，以期能提供國內廠商研發 VoIP 產品，以及後續在 TANET 或 TWAREN 上建置 VoIP 平台時的重要參考。

關鍵詞：NAT, Session Controller, SIP, STUN, UPnP, VPN。

1. 前言

我國寬頻網路與無線網路在政府推動下蓬勃發展，各種網路應用如雨後春筍般出現，其中 VoIP (Voice over IP)網路電話應用就是目前最炙手可熱的應用之一。電信國家型計畫預見到此一趨勢，在兩年前便開始佈建以 SIP (Session Initiation Protocol [4])為基礎之 VoIP 整合測試平台(簡稱 NTP VoIP 平台)。在 NTP VoIP 平台上，SIP 網路電話(SIP User Agent，簡稱 SIP UA)分別使用 SIP 與 RTP (Real-time Transport Protocol [3])為信令協定和傳輸影音資料的協定。本計畫在建置網路電話系統時發現，每一台網路電話都需要一個 IP 位址，因此產生了 IP 位址不足的問題。目前網路位址轉換(Network Address Translation，簡稱 NAT [7])機制最常被用來解決此一問題。NAT 轉換器介接於私有(private)網路和公眾(public)網路之間，可將私有 IP 位址轉換為公眾 IP 位址，讓私有網路上的主機可以和公眾網路上的主機通訊。然而 VoIP 所使用的 SIP 信令是屬於應用層(application layer)協定，NAT 轉換封包標頭時，並不會修改 SIP 訊息(指封包中應用層部分，包括 SIP 標頭(header field)和 SIP 本體(body))中所帶的 IP 位址與通訊埠(port)，因此這些 SIP 訊息中的資訊在經過 NAT 之後將會發生錯誤。此一問題不但在 NTP VoIP 平台上會發生，目前在校園無線區域網路漫遊環境中使用無線網路電話(WiFi SIP Phone)時也會遇到相同的問題[1]。為了提供 SIP 穿越 NAT 的解決方案，本論文將依序介紹在 NTP VoIP 平台上的實驗環境，定義穿越 NAT 之問題，以及討論五種穿越 NAT 的機制，如何取得公眾網路的 IP 位址與通訊埠，並比較這些機制的優缺點。最後，本文將分別以設備製造商與網路服務提供商的觀點，提出合適的穿越 NAT 解決方案，以期提供未來在 TANET 或 TWAREN 網路中，研發與佈建 VoIP 設備時的重要參考。

本論文為國科會計畫「SIP-based B3G 前置整合實驗計畫」所支持，計畫編號為 NSC-92-2219-E-009-032，計畫執行期間為 92 年 11 月至 93 年 12 月。

2. 測試環境介紹

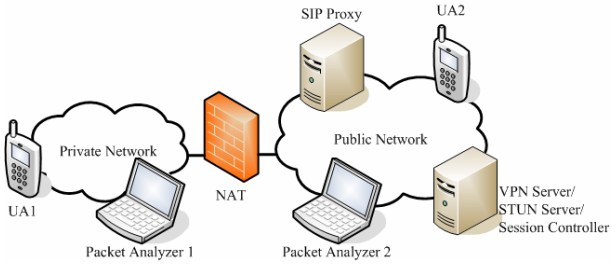

圖 1 測試環境

圖 1 顯示在 NTP VoIP 平台中用來驗證穿越 NAT 機制的測試環境。為了讓讀者可以複製實驗環境，圖中的 NAT 是使用微軟[12] Windows XP 加上兩張網路卡所設定成的，此 NAT 可以支援通用隨插即用(Universal Plug and Play，簡稱 UPnP [16])的功能，且為 Full Cone NAT 可以讓 STUN (Simple Traversal of UDP through NAT [5])機制穿越。UA1 是在私有網路的 SIP UA，為 Snom 200 硬體電話[15]或 Windows Messenger 4.7 [18]；UA2 則是在公眾網路的 SIP UA，使用 Windows Messenger 4.7。Packet Analyzer 1 和 Packet Analyzer 2 分別位在私有網路和公眾網路中，並使用 Ethereal [10]開放程

式碼軟體擷取網路上傳送的封包來確定封包內容之正確性。最後則是在公眾網路上的各種伺服器，包括有使用 IPtel SIP Express Router v0.8.11 [11]架設的 SIP Proxy、VPN (Virtual Private Network [2]，亦稱虛擬私有網路)伺服器、STUN 伺服器和 Session Controller。本論文限於篇幅，將會著重於各機制如何穿越 NAT 的原理分析，想要建立相同實驗環境者可以參考文件[13]中的介紹，實作出本文所提出之各種穿越 NAT 的機制。

3. 問題描述

NAT 的架構如圖 2 所示。圖中 NAT 左端為私有網路，當中的主機被分派使用 192.168.0.0/24 的私有 IP 位址，而 NAT 右端網路卡(IP 位址為 140.113.131.89)連接公眾網路。由於私有 IP 位址無法在公眾網路上路由(route)，因此私有網路中主機送出的封包會被 NAT 攔截，將網路層(network layer)中的來源 IP 位址取代為 NAT 在公眾網路的位址(如：140.113.131.89)，並將傳輸層(transport layer)中的來源通訊埠修改為 NAT 上一可用的通訊埠(如：10080)，並且在對應表(mapping table)中建立轉換的對應關係。公眾網路的主機欲傳送給私有網路主機的封包，則是會傳送到 NAT 對應的通訊埠上，由 NAT 修改網路層和傳輸層目的地資訊後，送給私有網路中的主機。

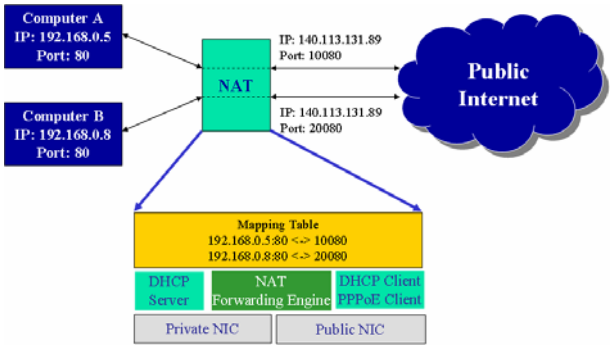

圖 2 NAT 架構圖

由於 NAT 只修改封包中網路層和傳輸層的資訊，並不處理 SIP 訊息所攜帶的內容，因此若公眾網路上的主機使用 SIP 訊息中攜帶的私有 IP 位址和通訊埠作為封包的目的地，此封包將無法在公眾網路上路由，如此私有網路內的主機收不到公眾網路上主機所傳送的封包。

在 SIP 訊息中有兩個帶有 IP 位址和通訊埠的標頭與路由有關，分別為“Contact”和“Via”。“Contact”是用來告知對方此後的請求訊息(request message)可直接送達的位置，因此若此標頭內容為私有 IP 位址及通訊埠，公眾網路上的 SIP 設備便無法將請求訊息正確傳給私有網路內的 SIP 設備。當請求訊息被送出時，SIP 設備會加入一個含有自己 IP 位址的“Via”，並將此“Via”放在整個 SIP 訊息中所有“Via”的上方。當目的地 SIP 設備準備要送出回應訊息(response message)時，會將請求訊息中的所有“Via”原封不動的複製到回應訊息中，SIP 節點將依序檢查"Via"欄位所帶的位址資訊，以便將封包依照原路徑反向送回。若“Via”帶有私有 IP 位址及通訊埠，則回應訊息無法回到私有網路內的 SIP 設備。圖 3 即為“Contact”和“Via”標頭攜帶私有 IP 位址及通訊埠的例子。

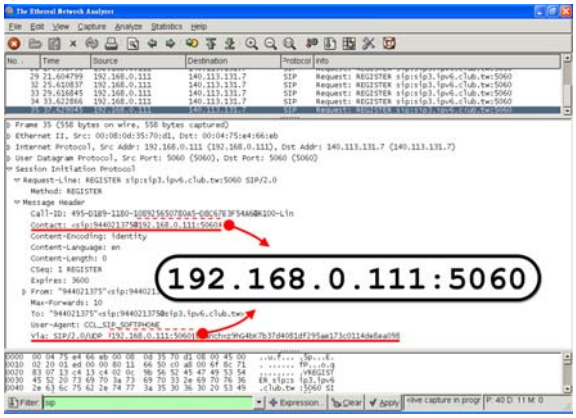

圖 3 SIP 訊息中的“Contact”和“Via”

除了標頭部份的問題外，在 SIP 訊息本體的 SDP [6]中，“c”欄位和“m”欄位分別帶有欲接收 RTP 封包的 IP 位址與通訊埠。若這些欄位(“c”和“m”)填入的是私有 IP 位址和通訊埠，則通話建立後的 RTP 影音封包將無法送到正確的位置(如圖 4)。

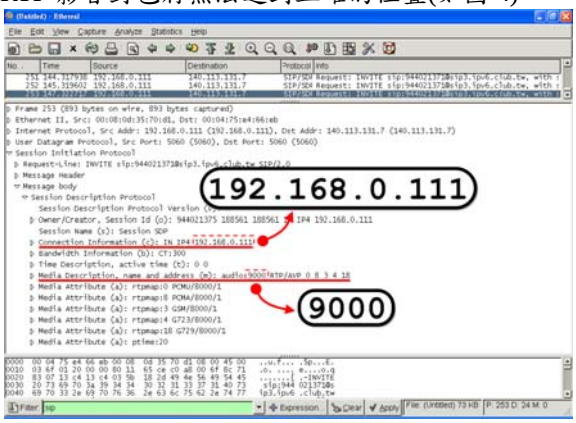

圖 4 SDP 中的“c”和“m”

4. SIP 穿越 NAT 的解決方法

由上述的介紹可以得知，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。接下來將介紹五種解決方法，分別為虛擬私有網路、靜態指定、通用隨插即用、STUN 和 Session Controller。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，取得封包出了 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、UPnP 和 STUN 皆屬此類。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。

4.1 虛擬私有網路

虛擬私有網路以建立通道(tunnel)的技術，讓實體上在不同網域的主機，邏輯上看來像是在同樣的網域內。

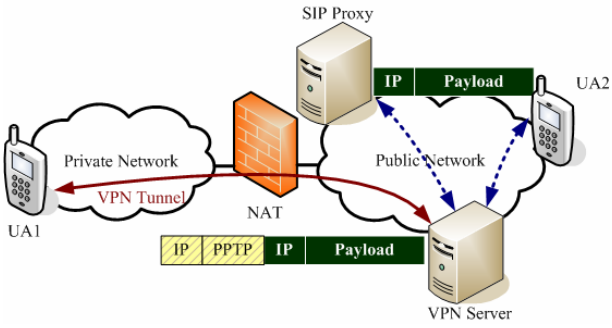

圖 5 VPN 架構

VPN 客戶端建立 VPN 通道連線至 VPN 伺服器後，作業系統會在主機上產生一個虛擬的網路連線介面，並且將此介面設定為預設的傳輸介面。在非刻意指定路由的情形下，所有的封包都會使用此介面的 IP 位址，並經由此介面傳送至網路上。虛擬網路連線介面的 IP 位址由 VPN 伺服器指定，若 VPN 伺服器分派公眾 IP 位址給 VPN 客戶端，則 VPN 客戶端就會擁有一個具有公眾 IP 位址的網路連線介面，即此 VPN 客戶端可被視為在公眾網路上的主機，因此不會有任何 NAT 所造成的問題產生。

以圖 5 的例子來看，私有網路內的 UA1 和 VPN 伺服器建立連線後，所有 UA1 欲送出的封包(反白部分)都會被 VPN 連線使用的通訊協定(如圖 5 使用 PPTP)封裝起來(斜線部分)，將封包先送到 VPN 伺服器，再由 VPN 伺服器將封包解開後，送到該封包的目的地位址。因此圖中斜線部份 IP 的來源會是 UA1 的私有 IP 位址，目的地會是 VPN 伺服器；反白部分 IP 的來源則為 UA1 從 VPN 伺服器所取得的公眾 IP 位址，而目的地則是 SIP Proxy 或 UA2。

4.2 靜態指定

“靜態指定”就是手動設定將私有網路中主機的IP位址IP_A與通訊埠$Port_A$，對應到被NAT轉換後的公眾網路IP位址IP_B與通訊埠$Port_B$，在本文的表示法為(IP_A:$Port_A$, IP_B:$Port_B$)。若NAT收到封包來自私有網路且來源是IP_A:$Port_A$，便改成IP_B:$Port_B$轉送到公眾網路路由。若封包來自公眾網路而目的地是IP_B:$Port_B$，便改成IP_A:$Port_A$後送往私有網路。

使用靜態指定，必須在SIP UA以及NAT上設定至少兩組的IP位址和通訊埠對應關係，其中(IP_A:$Port_{A1}$, IP_B:$Port_{B1}$)是給SIP使用，而(IP_A:$Port_{A2}$, IP_B:$Port_{B2}$)給RTP使用。若SIP UA還要傳輸影像，則必須要設定第三組對應關係(IP_A:$Port_{A3}$, IP_B:$Port_{B3}$)給傳送影像的RTP使用。如此SIP UA在填寫SIP訊息中具有IP位址及通訊埠時，便填寫IP_B:$Port_{B1}$，而網路層和傳輸層的IP位址及通訊埠則為IP_A:$Port_{A1}$。此後公眾網路上的主機將封包送至SIP訊息所指定的IP位址及通訊埠(IP_B:$Port_{B1}$)時，封包便可順利送達NAT，然後藉由NAT的轉換送達私有網路中的SIP UA，是故此方法可以穿越NAT。

4.3 通用隨插即用

通用隨插即用是由微軟等廠商聯合推出的網際網路通訊協定，目的是讓網路設備連接上線後，能夠偵測到其他 UPnP 設備且自動完成設定。使用 UPnP 解決穿越 NAT 的問題的技巧在於，所有具有 UPnP 的 NAT 設備都加入一個群播群組(IP 位址為 239.255.255.250)，並於通訊埠 1900 等待 UPnP 客戶端的查詢。由支援 UPnP 的 SIP UA 和 NAT 利用 UPnP 訊息彼此溝通，協調出 NAT 對應表中 IP 位址及通訊埠的對應關係。協調訊息交換過程如圖 6 所示。當 SIP UA (UPnP 客戶端)上線後，會發送群播(multicast; 239.255.255.250，通訊埠為 1900)訊息尋找 NAT 設備(在 UPnP 中扮演 Internet Gateway Device，簡稱 IGD)，NAT 收到此訊息後，因為已經知道 NAT 所在的位址(ip_of_IDG)，因此用單一傳播(unicast)來傳遞，並且告知 NAT 的 IP 位址(如圖 6 步驟 1、2)，此後 SIP UA 和 NAT 溝通的訊息皆使用單一傳播來交換訊息。

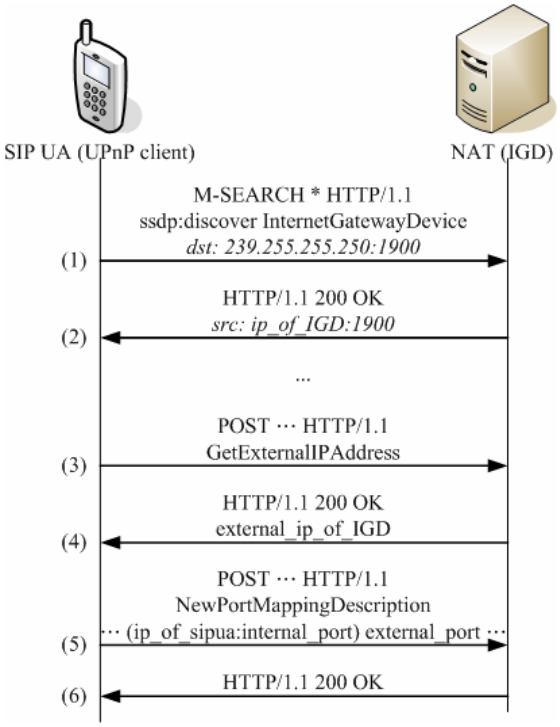

圖 6 UPnP 協調 IP 位址及通訊埠流程

SIP UA 和 NAT 之間使用 UPnP 交換的訊息以

HTTP[9]通訊協定為基礎，將欲傳送給對方的資訊放置在 HTTP 的承載(payload)部分。以取得 IP 位址為例，SIP UA 發送 HTTP 訊息給 NAT，詢問 NAT 在公眾網路上的 IP 位址(如圖 6 步驟 3)。NAT 收到後，便將 IP 位址放置在回應訊息中的承載部分，回應 SIP UA 的要求，此時 SIP UA 就知道將被對應的公眾網路 IP 位址(如圖 6 步驟 4)。通訊埠的取得方式並非由 NAT 告知，而是由 SIP UA 將本身的 IP 位址及通訊埠和希望使用的外部通訊埠通知 NAT(如圖 6 步驟 5)，要求 NAT 產生新的 IP 位址及通訊埠對應關係。NAT 確認 SIP UA 要求的外部通訊埠為閒置狀態後，便直接使用 HTTP 的回應訊息告知成功(如圖 6 步驟 6)。若非閒置狀態則告知失敗，SIP UA 必須修改通訊埠後重新送出要求。

4.4 STUN (Simple Traversal of UDP Through NAT)

STUN 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。STUN 運作流程如圖 7。

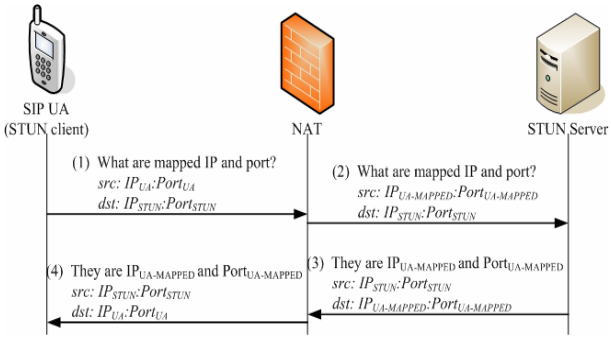

圖 7 STUN 運作流程

SIP UA利用STUN通訊協定將封包送往STUN伺服器(如圖 7 步驟 1)，此封包經過NAT的轉換到達STUN伺服器後(如圖 7 步驟 2)，STUN伺服器便將此封包網路層和傳輸層的來源IP位址及通訊埠($IP_{UA-MAPPED}$:$Port_{UA-MAPPED}$)回應給SIP UA(如圖 7 步驟 3)。因此SIP UA收到回應後便可得知內外部IP位址以及通訊埠的對應關係(IP_{UA}:$Port_{UA}$, $IP_{UA-MAPPED}$:$Port_{UA-MAPPED}$) (如圖 7 步驟 4)，在填寫SIP訊息中路由相關的IP位址及通訊埠時，就填入$IP_{UA-MAPPED}$:$Port_{UA-MAPPED}$即可。

4.5 Session Controller

Session Controller 主要由 SIP Proxy 和 RTP Proxy 所組成，SIP Proxy 負責 SIP 訊息的處理和轉送，而 RTP 封包則交由 RTP Proxy 負責。本計畫所使用的 SIP Proxy 是包含 nathelper 模組的 IPtel SIP Express Router (SER)，而 RTP Proxy 則是由 PortaOne 所開發[14]。在 SIP Proxy 上所撰寫穿越 NAT 的虛擬程式碼如圖 8 所示，當有 SIP 訊息送往 Session Controller 時，SIP 要求訊息會被加入“Record-Route”的標頭(如圖 8 第 01 行)，如此可以確保之後所有的 SIP 訊息都會經過此 Session Controller，而 Session Controller 會擁有整個通話過程的掌控權。收到 SIP 訊息時，Session Controller 利用此封包中的網路層來源 IP 位址和通訊埠，比對應用層所攜帶的資訊是否相同，便可得知此 SIP 訊息是否來自私有網路的 SIP UA (如圖 8 第 02 行)。若是，則表示“Contact”和“Via”標頭內的 IP 位址和通訊埠皆不正確，因此 Session Controller 會將“Contact”標頭內的 IP 位址和通訊埠修改為網路層和傳輸層所得到的資訊(如圖 8 第 03 行)。而對於“Via”標頭的處理，則是在內容尾端多加兩個標籤(tag)：“received”和“rport”，分別記錄下此封包的來源 IP 位址以及通訊埠，如此當回應訊息回送到 SIP Proxy 時，SIP Proxy 就根據“Via”內的“received”和“rport”來轉送此回應訊息(如圖 8 第 05 行)。

```
01 record_route();  //add "Record-Route" header into SIP message
02 if( nat_uac_test() ){ //test if UA is behined NAT
03         fix_contact();
04           //modify the IP and port info. in "Contact"
05         add_received_rport_to_via();
06           //add extra tags, "received" and "rport", into "Via"
07 };
08
09 if( method=="REGISTER" ){
10         //handle "REGISTER" procedure
11 }
12 else if( method=="INVITE" ){
13         use_rtp_proxy();
14           //notify RTP Proxy to reserve resource for RTP relay in future
15           //also modify the "c" and "m" field in SDP of UAC
16
17         //handle "INVITE" procedure
18         //waiting for response from UAS
19         if( response=="200 OK" ){
20                 use_rtp_proxy();
21                   //modify the "c" and "m" field in SDP of UAS
22         };
23 }
24 else{
25         //handle other types of messages
26 };
```

圖 8 Session Controller 中穿越NAT的虛擬程式碼

完成了“Contact”和“Via”標頭的處理，若 SIP 要求訊息為“REGISTER”，便將處理後的“Contact”和“To”標頭資訊儲存起來即可，但若為“INVITE”或是“200 OK”訊息內帶有 SDP，則需要 RTP Proxy 的協助才能夠讓 RTP 封包也穿越 NAT，詳細流程如圖 9。Session Controller 呼叫 use_rtp_proxy()函數(如圖 8 第 13、20 行)將雙方的 SDP 中的“c”與“m”欄位分別修改為 RTP Proxy 的 IP 位址與通訊埠，而原本點對點傳送的傳送方式，就會改成雙方皆和 RTP Proxy 建立通話，由 RTP Proxy 負責轉送和控制雙方 RTP 封包的傳輸。

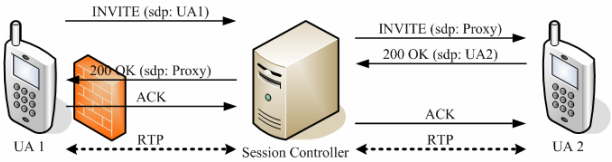

圖 9 Session Controller - INVITE 訊息流程

在 UA1 尚未送出 RTP 封包之前，在 NAT 內部並沒有建立 IP 位址與通訊埠的對應，Session Controller 也不知道應該將 RTP 封包送到 NAT 的哪個通訊埠去，故先將欲送給 UA1 的 RTP 封包暫存起來，待 UA1 送出第一個 RTP 封包後，再將暫存的 RTP 封包全數送到該位置。

5. 分析與比較

由於各種機制運作有其不同的適用環境和特性，接下來將以三個表來分析各種機制的優缺點。

表 1 穿越 NAT 之機制比較一：需要支援的設備

項目 / 機制	SIP UA	NAT	額外伺服器
VPN	是	否	是
Static Assignment	是	否	否
UPnP	是	是	否
STUN	是	否	是
Session Controller	否	否	是

表 1 比較採用各種機制所需的設備支援。對於 SIP UA 而言除了 Session Controller 之外，其他四種機制都需要特別修改 SIP UA 的程式碼。使用 VPN 在客戶端必須要能夠建立 VPN 連線，使用靜態指定的客戶端需要有可填寫 IP 位址和通訊埠對應關係的介面，使用 UPnP 的 SIP UA 需要支援 UPnP 客戶端的功能，使用 STUN 的 SIP UA 需支援扮演 STUN 客戶端角色。而使用 Session Controller 僅需要將 SIP Proxy 的位置設定為 Session Controller 的 IP 位址即可，此功能幾乎市面上所有 SIP UA 都已能提供，因此不需要對 SIP UA 做特別的修改。在 NAT 支援方面，只有 UPnP 需要 NAT 扮演為 UPnP IGD 角色的特別支援。雖然靜態指定也需要有能夠設定靜態對應 IP 位址和通訊埠的介面，然而一般 NAT 都已提供，所以和 VPN、STUN 以及 Session Controller 等三種機制一樣，不需要 NAT 額外的支援。VPN、STUN 和 Session Controller 分別需要在公眾網路架設 VPN 伺服器、STUN 伺服器與 Session Controller 設備，其他機制則不需要。

表 2 穿越 NAT 之機制比較二：限制性比較

項目 / 機制	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 位址	SIP UA 是否需要支援對稱式 RTP
VPN	是	是	是	否
Static Assignment	是	是	否	否
UPnP	是	否	否	否
STUN	否	是	否	否
Session Controller	是	是	否	是

表 2 比較各種機制之適用環境。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，這五種機制中除了 STUN 無法穿越 Symmetric NAT 外，其他各種機制皆可穿越所有類型的 NAT。而 STUN 無法穿越的原因在於 Symmetric NAT 會以來源和目的地的 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，對應到的通訊埠就會不一樣。由 SIP UA 送往 STUN 伺服器所使用的通訊埠會不同於送往 SIP Proxy (或 SIP UA)的，故 STUN 在 Symmetric NAT 的環境下會失效。至於多層 NAT 的環境，除了 UPnP 之外的機制皆可解決此問題。UPnP 之所以無法穿越多層 NAT，是因為 SIP UA 發送的群播尋找 NAT 的訊息，只會被最接近的 NAT 接收到，SIP UA 向此 NAT 詢問到的 IP 位址會是私有 IP 位址，而非最外層 NAT 的外部公眾 IP 位址。此外，這五種機制中只有 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 [17] (使用同樣的通訊埠收送 RTP 封包)，不過目前幾乎市面上所有 SIP UA 都具有此特性，因此這項限制影響不大。

表 3 穿越 NAT 之機制比較三：使用方便性比較

項目 / 機制	設定難易度	通訊延遲	IP 改變是否造成影響
VPN	較困難	最長	否
Static Assignment	最困難	最短	是
UPnP	最容易	次短	否
STUN	次容易	次短	否
Session Controller	最容易	較長	否

表 3 以使用者的角度來比較各種機制。就設定難易度而言，UPnP 和 Session Controller 均不需任何額外的設定，最為容易。次之為 STUN，僅需設定 STUN 伺服器的 IP 位址和通訊埠。較困難的是 VPN，必須設定 VPN 伺服器以及登入 VPN 伺服器的使用者名稱和密碼。而最困難的是靜態對應，必須將多組的 IP 位址和通訊埠設定到 SIP UA

上。而通訊延遲方面，最短的是靜態對應，其延遲僅在 NAT 轉換封包的 IP 位址和通訊埠時，這延遲也是任何一種機制都會遇到的。次短為 UPnP 和 STUN，除了 NAT 延遲外，在每次建立通話前都需要一小段時間，用以取得封包出了 NAT 後使用的 IP 位址和通訊埠。Session Controller 會有較長的延遲時間，是因為所有 SIP 和 RTP 封包的傳送，都會加上經由 Session Controller 轉送的延遲。而延遲時間最長的是 VPN，這是因為所有的封包都會經由 VPN 伺服器作封裝和解封裝的動作(甚至還需要加解密)，因此造成大量的傳輸延遲。

當 SIP UA 所在環境是使用動態 IP 位址分配服務(Dynamic Host Control Protocol，簡稱 DHCP [8])時，除了靜態指定需要重新在 SIP UA 和 NAT 上設定 IP 位址及通訊埠的對應關係，較為麻煩之外，其他機制皆不被影響，即當 IP 位址有所改變時，僅需重新啟動機制且執行 SIP UA 的註冊流程即可。

這五種機制中，除了 VPN 外，其他各種方法皆十分常見。VPN 之所以不在 VoIP 中廣泛被使用的原因，除了其通訊延遲很長，造成通話品質不良外，最重要的原因是其違背了使用 NAT 的最初用意—IP 位址不足(既然 IP 位址已不敷使用，就無法讓 NAT 內部的 SIP UA 皆能擁有各自的公眾 IP 位址)。

以網路電話製造商的角度來看，使用 UPnP 解決穿越 NAT 問題會是較好的選擇，這是因為 UPnP 不需要使用者任何設定、不需要架設伺服器，且不受 DHCP 的影響，通訊延遲也只有在建立通話之初的一小段時間而已。但若考量使用者所在環境可能有舊型的 NAT 無法支援 UPnP，那麼就必須同時支援靜態指定或 STUN 機制，如此 SIP UA 功能才足以適用任何 NAT 環境。

對於網路服務提供者(Internet Service Provider，簡稱 ISP)而言，Session Controller 機制將會是首選。因為採用 Session Controller 機制，ISP 不需考慮使用者的 SIP UA 或 NAT 可支援的機制，使用者只需將 SIP Proxy 設定為 Session Controller，而 ISP 只需要在網路上佈建 Session Controller 設備，故使用此方法可以免除 ISP 額外的負擔。

6. 結論

以 SIP 為基礎之 VoIP 是目前最受歡迎的應用之一，但是在國內開發或佈建 VoIP 設備常常需要解決穿越 NAT 的問題。此一問題在 NTP VoIP 整合測試計畫中已經獲得解決，因此本文將電信國家型計畫之成果與國人分享，介紹了五種可以讓 SIP 網路電話穿越 NAT 的機制，並提供這些機制的優缺點比較。希望本文能解決在國內網路環境中使用 VoIP 的問題，並促進國內 VoIP 的研發與推動。

參考文獻

[1] 楊詠淇、唐可忠、黃偉航、陳偉文、蔡志宏。“校園無線區域網路漫遊環境建置現況與其網路電話應用”，submitted to TANET2004。

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

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

[4] 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.

[5] 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.

[6] M. Handley, V. Jacobson, “SDP: Session Description Protocol”, IETF RFC-2327, April 1998.

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

[8] R. Droms, “Dynamic Host Configuration Protocol”, IETF RFC-1541, October 1993.

[9] 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.

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

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

[12] Microsoft Corporation, http://www.microsoft.com/

[13] NTP VoIP 平台之 SIP 穿越 NAT 機制教學文件, http://tingfan.csie.org/~huangyl/tanet2004/nat_traversal_of_sip_sdp.pdf

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

[15] snom technology AG – Voice over IP (VoIP) SIP Phones, http://www.snom.com/index1_en.php

[16] UPnP(TM) Forum, http://www.upnp.org

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

[18] Windows Messenger for Windows XP, http://www.microsoft.com/windows/messenger/