結合中繼連線與點對點直接連線以穿透網路位址轉換器之方法

Method of Combining Relay Connection with P2P Direct Connection for NAT Traversal

陳律翰　林宏偉　王慶堯
Lyu-Han Chen, Hong-Wei Lin, Ching-Yao Wang

中文摘要

現今網路技術快速發展，連網裝置的數量也愈來愈多且多樣化，為了解決IP位址短缺及提升網路安全性，大部份的連網裝置都會透過網路位址轉換器(Network Address Translator；NAT)與其它裝置互聯，由於NAT會提供網路位址的轉換，並對封包的傳輸有所限制，導致裝置與裝置之間的傳輸會因封包無法穿透NAT而出現問題。因此，如何穿透NAT變成一個重要的研究議題。使用中繼伺服器(Relay Server)的協助來穿透NAT雖然有較高的成功穿透率，但有傳輸效率及浪費網路頻寬等問題，為了提升傳輸效率及節省網路頻寬，很多研究都著重在如何以點對點(Peer-to-Peer; P2P)的方式來穿透NAT，但在對稱式(symmetric) NAT裝置愈來愈普及的情況下，使用點對點的方式來穿透NAT的成功率仍顯不足。有鑒於此，在這篇論文中，我們先後建立中繼連線及點對點直接連線，並提出一個協同式NAT穿透方法，以兼顧成功穿透率、傳輸效率及節省網路頻寬的使用。

Abstract

Nowadays, with the rapid growth of Internet technologies and the proliferation of diverse devices connected to the Internet, most devices connect with each other through Network Address Translator (NAT) in order to handle the shortage of IP address and promote network security. Since NAT is a methodology of remapping one IP address space into another and restricting packet transmission, packets transmitted between devices are most likely blocked by NAT. Therefore, how to traverse NAT is an important research issue. Although traversing NAT by the aid of a relay server has a higher success rate, it may encounter the problems of poor transmission efficiency and waste of network bandwidth. In order to enhance transmission efficiency and economize the use of network bandwidth, many researches put emphasis on Peer-to-Peer (P2P) NAT traversal. However, since the symmetric NAT devices are more and more popular, the success rate of P2P NAT traversal is still insufficient. In view of this, in this paper, the relay connection and the P2P direct connection are established in succession. A collaborative NAT traversal method is proposed to enhance success rate of NAT traversal as well as transmission efficiency and economize the use of network bandwidth.

關鍵詞(Key Words)

網路位址轉換(Network Address Translator；NAT)
中繼伺服器(Relay Server)
點對點 (Peer-to-Peer；P2P)
網路位址轉換穿透 (NAT traversal)

1 · 前言

現今網路技術快速發展，加上物聯網(Internet of Things; IoT)[1][2]的觀念也愈來愈成熟，所有物品、裝置可以通過射頻識別等信息感測設備與網路連接，實現智能化應用和管理周邊設備的目的，也因如此，連上網路的裝置愈來愈多，裝置與裝置之間的資料傳輸也愈來愈多元，除了訊息的傳輸外，還有大量的多媒體資訊(e.g., 聲音及影像串流)。

另一方面，為了提升網路安全性，裝置與裝置之間的網路環境也愈來愈複雜，根據統計至少有超過70%的連網裝置都會透過NAT與其它裝置互聯，由於NAT會提供網路位址的轉換，並對封包的傳輸有所限制，因此常導致裝置與裝置之間的資料無法直接傳輸，因此如何穿透NAT是一個重要的研究議題。

現行網路上的NAT大致分成四種型態，分別為一對一(Full Cone) NAT、位址限制(Address Restricted Cone) NAT、埠限制(Port Restricted Cone) NAT及對稱式NAT [3]，若傳輸的兩端裝置分別使用這四種NAT，其點對點直接資料傳輸的成功與否可用表1簡單的作說明。符號「O」表示兩端裝置只要知道其所連接之NAT外部位址就一定可以成功傳輸，符號「H」表示就算在對稱式NAT一端之裝置無法正確預測NAT外部位址之通訊埠，只要再透過hole punching[4]技術也可成功傳輸資料，符號「 - 」表示就算使用hole punching技術，兩端的資料傳輸也不一定可以成功。由於對稱式NAT對於封包進出的限制最為嚴格，且因為對稱式NAT在現行網路環境中愈來愈普及，對於點對點之間網路傳輸成功率也帶來更多的不確定性。

而現行穿透NAT的方法大致分成三種。第一種方法是藉由中繼伺服器的協助來建立中繼連線[5]，這種方法由中繼伺服器來處理網路位址的轉換協調，因此能有很高的NAT穿透率，但需要額外的頻寬，提高了傳輸成本，且傳輸

表 1　兩端裝置使用不同NAT之點對點傳輸情形

A/B	一對一	位址限制	埠限制	對稱式
一對一	O	O	O	H
位址限制	O	O	O	H
埠限制	O	O	O	–
對稱式	H	H	–	–

的延遲時間較長，傳輸效率相對較低。為了降低成本同時提高傳輸效率，很多研究致力於提升點對點NAT穿透率[4]，要達到此目的，需要其他一些技術的支援，例如：NAT型態辨識[6]、通訊埠預測技術[7]、hole punching[4]等，但是如同前面所述在對稱式NAT網路環境愈來愈普遍的情況下，點對點NAT穿透率仍顯不足。因前兩種方法各有其缺點，更有研究[8]融合了前面兩種方法，先嘗試點對點NAT穿透，若失敗再採用中繼伺服器的協助來穿透。現行的Interactive Connectivity Establishment (ICE, RFC 5245)即採用此機制，但若等點對點NAT穿透失敗再採用中繼伺服器協助來穿透NAT，會造成連線延遲時間較長的問題。而且若初次嘗試點對點NAT穿透失敗，則會採用中繼連線，不會再嘗試以點對點的方式傳輸，也因此降低傳輸效率、提高了傳輸成本。綜合上述方法，對於NAT穿透都有不足的地方，在這篇論文中，我們先後建立中繼連線及點對點直接連線，並提出一個協同式NAT穿透方法，以兼顧成功穿透率、傳輸效率及節省網路頻寬的使用。

這篇論文其它的章節安排如下。第二章節會介紹一些相關文獻研究，第三章節會介紹在本論文所提出的協同式NAT穿透的方法，最後，在第四章節會對這篇論文做結論。

2 · 相關文獻

在這個章節，我們對協同式NAT穿透方法做相關文獻的檢索、探討，並說明先前研究所提出之方法的缺點。在[9]中，提出一裝置可以先與其他裝置建立一主要點對點傳輸通道，此裝置並可以利用此主要傳輸通道再建立多條次要點對點傳輸通道，若偵測主要傳輸通道失敗或傳輸品質降低，則次要傳輸通道可以取代原本的主要傳輸通道成為之後傳輸的主要通道，

在這個方法當中，並沒有考慮使用中繼伺服器來穿透NAT，故若在對稱式NAT的網路環境下，仍然很容易造成無法穿透NAT的情況。

在[10]的研究當中，會先判斷點對點直接穿透NAT是否可行(請參考表2，其中第一欄及第一列分別代表兩端裝置所連接之NAT型態，中間的數字代表在這樣的網路環境下點對點直接穿透NAT是否可行，1.0代表可行，0.0代表不可行)，若可行，則嘗試建立點對點直接連線，若判斷點對點直接穿透NAT不可行，或是建立點對點直接連線失敗，則會使用中繼伺服器來建立中繼連線，並用中繼連線傳送資料。

表 2　判斷點對點直接穿透NAT之可行性

A/B	Unknown	Full Cone	Port Restricted	Symmetric
Unknown	0.0	1.0	0.0	0.0
Full Cone	1.0	1.0	1.0	1.0
Port Restricted	0.0	1.0	1.0	0.0
Symmetric	0.0	1.0	0.0	0.0

本圖表引自[10]

在這個方法當中有幾個缺點，第一，當一端裝置為對稱式NAT且另一端裝置為對稱式NAT或埠限制NAT時，在這個研究當中都判斷為點對點直接穿透NAT不可行，然而，在這些網路環境下，只要適當運用埠預測技術及hole punching技術，利用點對點的方式仍有可穿透之機會。第二，如同[8]，仍會有連線延遲的問題。

在[6]的研究當中，裝置與裝置之間可以先利用隧道(tunneling)技術透過中繼伺服器來穿透NAT，建立中繼連線後即可開始傳送資料，因此不會有傳輸延遲的問題，中繼連線建立後再嘗試建立點對點直接連線，若點對點直接連線被成功建立，則可利用點對點直接連線傳送資料，並於適當時機(e.g., 當點對點直接連線傳輸速率優於中繼連線時)終止中繼連線；若點對點直接連線沒有成功建立，則使用中繼連線傳輸。在這個方法當中，在點對點直接連線可以建立卻建立失敗的情況下，未再重新做埠預測跟設定，因此也未再嘗試建立點對點直接連線，導致傳輸的效率降低、傳輸成本提高。

3．協同式NAT穿透方法

由於藉由中繼伺服器的協助能有很高的NAT穿透率，另一方面，點對點NAT穿透率雖然較低，但使用點對點連線傳輸能提升傳輸效率並降低傳輸成本，因此這個研究的概念是兩端裝置分別先後與對方嘗試建立中繼連線及點對點連線，並用一協同機制來決定何時需採用中繼連線機制、何時採用點對點連線機制來傳輸以達到穿透NAT並兼顧傳輸效率、傳輸成本等目的。

基於這樣的機制，若點對點直接連線可建立成功，則可利用點對點直接連線傳輸以提升傳輸效率，同時並將中繼連線刪除以減少中繼轉傳成本；若點對點直接連線無法建立或是被判斷可建立卻建立失敗，則可直接用中繼連線來傳輸，也不會造成因需要等待建立連線而造成之傳輸延遲。另外，在點對點直接連線被判斷為可以建立卻建立失敗的情況，通常都是因為NAT外部的通訊埠被佔用而導致連線建立失敗，因此在這種情況，則在利用中繼連線傳輸的同時仍會持續嘗試建立點對點直接連線，待點對點直接連線建立成功，則可進一步將中繼連線刪除。整個方法運作的流程可以參考圖1，具體的方法如下說明。

3.1 裝置與NAT之資訊蒐集及交換

本方法在一裝置嘗試與另一裝置連線或是當一裝置接受其他裝置連線的請求時，會先與中繼伺服器註冊，以便之後建立中繼連線，接著會透過STUN伺服器的協助來取得與裝置連接之NAT的外部IP位置[11]，並搭配埠預測演算法來預測與裝置連接之NAT的外部埠配置(以下稱為映射埠)以便透過映射埠來傳送封包，如多媒體串流等。

做完映射埠預測，接著會做與裝置連接之NAT型態辨識[7]，並將點對點直接連線所需資訊(i.e.,裝置所在本地網路位址、與裝置連接之NAT外部IP位址及預測之映射埠、及NAT型態等資訊)與另一裝置交換，另外，若映射埠無法預測，則映射埠值為0。

3.2 建立中繼連線

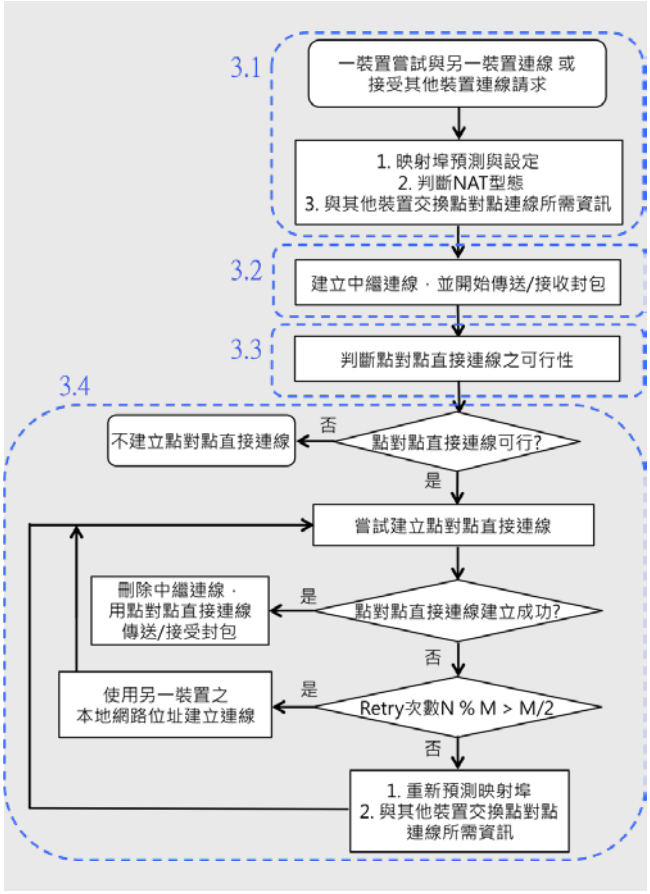


圖 1　運作流程圖

當裝置收到另一裝置之點對點直接連線所需資訊，則可先透過中繼伺服器穿透NAT以建立中繼連線，並開始透過中繼連線傳送與接收資料。接著可使用連接兩端裝置之NAT的型態及映射埠這兩個資訊來判斷裝置間之點對點直接連線之可行性。

3.3 點對點直接連線之可行性判斷

由於在對稱式NAT中每一NAT內部位址對應不同的目的地，都對應到不同的NAT外部位址，且NAT外部位址的配置有的是有規則性的，有的則是沒有規則性的，因此對稱式NAT之映射埠有的是可預測，有的是不能預測的，而一對一NAT、位址限制NAT及埠限制NAT這三種型態之NAT之映射埠皆可預測，根據不同型態NAT的特性，點對點直接連線可行性的判斷可整理成表3。

3.4 協同式NAT穿透

若依上述判斷方法判斷點對點直接連線不可行，則不建立點對點直接連線，只透過中繼連線傳送/接收資料；若判斷點對點直接連線可行，則會利用接收到的點對點直接連線所需資訊之與裝置連接之NAT外部IP位址及預測之映射埠嘗試與另一裝置建立點對點直接連線，若點對點直接連線成功建立(即封包可透過所建立的點對點連線正常接收)，則會馬上刪除中繼連線，使用點對點直接連線來傳送/接收資料以提升傳輸效率、降低傳輸成本。另一方面，若點對點直接連線被判斷可行但卻因映射埠被佔用而建立失敗(即資料無法透過所建立之點對點連線正常接收)，則會再次嘗試建立點對點直接連線。

當再嘗試建立點對點直接連線，裝置會重新作映射埠之配置，包含發送請求至某台STUN伺服器以獲得目前NAT映射埠配置的情況，依據目前的情況做接下來的映射埠配置，並再次與其他裝置交換點對點直接連線所需資訊，重新利用新收到的點對點直接連線所需資訊之與裝置連接之NAT外部IP位址及預測之映射埠再嘗試與另一裝置建立點對點直接連線，待點對點直接連線成功建立，再將中繼連線刪除改由使用點對點直接連線進行傳輸。

然而，如果多次嘗試建立點對點直接連線皆失敗，則裝置會改用收到的點對點直接連線所需資訊之裝置所在本地網路位址與另一裝置建立點對點直接連線，會採用此機制是因為有些無線網路基地台並不支援NAT loopback，在這種情況，若兩端裝置同時連上此基地台(i.e., 兩端裝置皆連接到同一個NAT)時，用NAT外部位址來建立連線是無法建立成功的。

3.5 實施方式及流程

茲舉一例以更細部說明本方法。請參照圖2，此方法用於通訊裝置A與通訊裝置B之間要建立多媒體串流的連線(RTP連線)，通訊裝置A

表 3　點對點直接連線可行性判斷

連線之一端點	連線之另一端點	點對點連線可行性
映射埠可預測	映射埠可預測	可行
映射埠不可預測(對稱式)	映射埠不可預測(對稱式)	不可行
映射埠不可預測(對稱式)	映射埠可預測 (埠限制)	不可行
映射埠不可預測(對稱式)	映射埠可預測 (對稱式)	不可行
映射埠不可預測(對稱式)	映射埠可預測 (位址限制)	可行 (hole punching)
映射埠不可預測(對稱式)	映射埠可預測 (一對一)	可行 (hole punching)

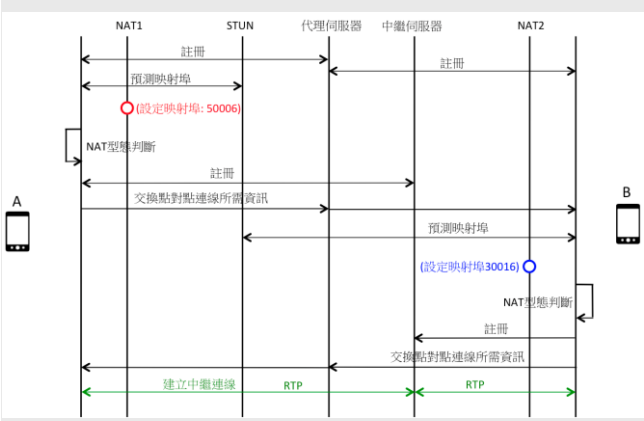


圖 2　運作流程範例

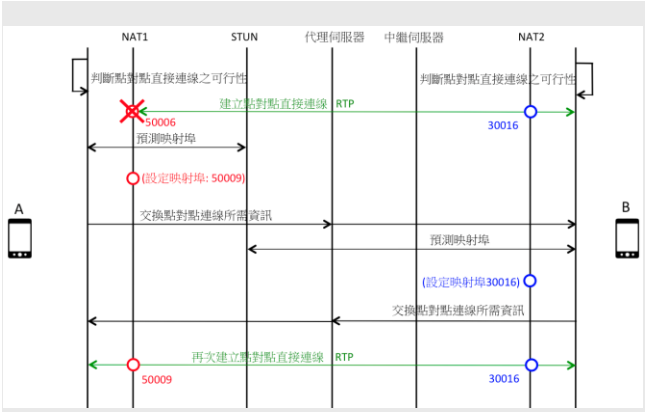


圖 3　運作流程範例

與通訊裝置B分別連接至NAT1及NAT2，以下逐步說明執行步驟。

步驟1：通訊裝置A與通訊裝置B會先向代理伺服器進行註冊，代理伺服器之後就可以協助處理訊息的轉送。

步驟2：要預測NAT1之下一個可使用的映射埠以用來傳送多媒體串流資料。通訊裝置A會向STUN伺服器發送請求，STUN伺服器收到請求後會回傳NAT1之NAT外部位址(含映射埠)，通訊裝置A會以這些資訊嘗試預測NAT1下一個使用之映射埠並作設定。

本方法在實施的時候，為了讓預測更準確，我們會先分別對四個架設在NAT1外部之STUN伺服器的位址發送請求，而這四個STUN伺服器會分別回傳與裝置連接之NAT1的外部位址(含外部IP及映射埠)，若這四個回傳的映射埠是有規則性的，那我們就可以依此規則來預測接下來要與其它裝置傳輸多媒體串流所使用的映射埠，例如若四個STUN伺服器分別回傳之映射埠為50002、50003、50004及50005，我們即可得知每次配置映射埠的規則為上次所使用的映射埠加1，則我們就可以預測接下來可以使用50006映射埠來傳輸多媒體串流資料，而在這邊我們會針對四個STUN伺服器發送請求(而非三個)的目的是為了容錯，例如若四個STUN伺服器分別回傳之映射埠為50002、50004、50005及50006，我們仍可預測接下來可以使用50007映射埠與其他裝置交換資料。在圖2中，此預測之映射埠值為50006。

步驟3：通訊裝置A會判斷NAT1之型態。可利用通訊裝置A透過NAT1發送多個請求給STUN伺服器的某個通訊埠，並要求STUN伺服器從其原來之通訊埠或不同之通訊埠回傳NAT1之外部位址，透過檢視通訊裝置A是否能收到STUN伺服器回傳的資訊來判斷NAT1的類型。

步驟4：通訊裝置A會與中繼伺服器註冊，接著並透過代理伺服器傳送NAT1之點對點直接連線所需資訊到通訊裝置B。

步驟5：當通訊裝置B接收到通訊裝置A傳送的資訊及連線請求，B也會執行相似的步驟，作映射埠預測及設定、NAT2型態判斷、與中繼伺服器註冊及傳送NAT2之點對點直接連線所需資訊到通訊裝置A。

步驟6：通訊裝置A與通訊裝置B會經由中繼伺服器建立一中繼連線並開始利用RTP傳送多媒體串流資料。

步驟7：參照圖3，透過中繼連線傳送多媒體串流資料的同時，通訊裝置A與通訊裝置B會根據表3判斷點對點直接連線之可行性，若點對點直接連線可行，則彼此會根據接收到的點對點連線所需資訊之NAT外部位址(含IP及映射埠)與對方建立點對點直接連線。

步驟8：若有一方(在圖3中為通訊裝置A)無法從點對點直接連線接收封包，則表示NAT1外部位址之映射埠可能被佔用而導致封包傳輸失敗，這個時候通訊裝置A會再向STUN伺服器發送請求，以重新預測NAT1下一個使用之映射埠，並重新設定映射埠值，例如為50009，之後，通訊裝置A重新傳送新的NAT1的點對點直接

連線所需資訊到通訊裝置B。

步驟9：通訊裝置B收到新的資訊後，同樣也需要再次預測NAT2之映射埠，因為NAT2之型態若為對稱式NAT，其每次建立連線之映射埠都會改變，再重新設定完映射埠後，一樣會傳送NAT2之點對點直接連線所需資訊給通訊裝置A，之後，兩端裝置便可利用新收到的點對點直接連線所需資訊之NAT外部IP位址及預測之映射埠再次建立點對點直接連線，若建立成功，則可刪除中繼連線。

基於上述所提出的方法，我們使用市面上普遍可見的無線分享器來作實驗，兩端裝置分別連上各式無線分享器，不同的無線分享器呈現不同的NAT型態，其點對點直接連線之成功率實驗結果如表4所示。有部分裝置連到D-link無線分享器，在雙方協調好映射埠之後，當要開始傳輸多媒體串流資料時，這些裝置的資料卻是從另外一個隨意選擇的映射埠送出而不是當初協調好的映射埠，當這種情形發生，若另外一個裝置之NAT型態為埠限制或是對稱式NAT時，將導致點對點直接連線傳輸失敗，如表4之符號「x」所處之情形，在這種情形發生時，只能使用中繼連線來傳輸，但如表4所示，大部分點對點直接連線傳輸是可行的。

表 4　點對點直接連線之成功率

A/B	MacBook pro	AirPort Express	TP-Link TL-WR841	Buffalo WZR-HP-G300	HUAWEI WS-330	D-link-809	D-link-615
MacBook pro	ok	ok	ok	ok	ok	ok	ok
AirPort Express	ok	ok	ok	ok	ok	ok	ok
TP-Link TL-WR841	ok	ok	ok	ok	ok	x	x
Buffalo WZR-HP-G300	ok	ok	ok	ok	ok	x	x
HUAWEI WS-330	ok	ok	ok	ok	ok	x	x
D-link-809	ok	ok	ok	ok	ok	ok	x
D-link-615	ok	ok	ok	ok	ok	x	ok

本論文所提出的方法，藉由先建立傳輸成功率較高的中繼連線，再嘗試建立傳輸效率較高、傳輸成本較低的點對點連線，而可節省使用者等待嘗試建立點對點連線的時間，並且盡量使用傳輸效率較高、傳輸成本較低的點對點連線，可同時具有傳輸效率更高、傳輸成本更低的方式且傳輸成功率更高的效果。

4．結論

本篇論文提出一個協同式NAT穿透的方法。兩端裝置先後建立中繼連線與點對點直接連線，中繼連線於建立後即可傳送接收封包以減少延遲時間，待點對點直接連線建立成功後，再將中繼連線刪除，使用點對點直接連線傳送接收封包，以提升傳輸效率、降低傳輸成本。

有鑑於點對點直接連線被判斷為可以建立卻建立失敗的情況，通常都是因為NAT外部的通訊埠被佔用而導致連線建立失敗，因此當這種情況發生時，本篇論文的方法會在中繼連線傳輸的同時仍持續嘗試建立點對點直接連線，待點對點直接連線建立成功，則可進一步將中繼連線刪除，要持續嘗試建立點對點直接連線也必須要持續更新映射埠，而且本論文也有考慮到無線基地台不支援NAT loopback的情況，讓整體的點對點NAT穿透率更為提升，更符合現實的網路環境。

參考文獻

[1] M. Humayun Kabir, M. Robiul Hoque and S-H. Yang, “Development of a smart home context-aware application: A machine learning based approach,“ International Journal of Smart Home, Vol. 9, No. 1, pp. 217-226, 2015.

[2] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. Stefanizzi and L. Tarricone, “An IoT-aware architecture for smart healthcare systems,“ IEEE Internet of Thisngs Journal, Issue 99, pp.1-12, March, 2015.

[3]http://www.cs.nccu.edu.tw/~lien/Writing/NGN/firewall.htm

[4] B. Ford, P. Srisuresh and D. Kegel, “Peer-to-peer communication across network address translators,“ in Proceedings of USENIX Annual Technical Conference, pp. 179-192, 2005.

[5] Traversal Using Relays around NAT (TURN): Relay Extensions to Session

Traversal Utilities for NAT (STUN), RFC 5766, 2010.

[6] Y. Kudo, and Ichinomiya, “Device having capability to switch from tunneling communication to P2P communication with other device under the control of network address translation devices,” U.S. Patent 8 200 841, Jun. 12, 2012.

[7] S. Guha, Y. Takeda and P. Francis, “NUTSS: A SIP-based approach to UDP and TCP network connectivity,“ in Proceedings of ACM SIGCOMM Workshops, pp. 43-48, 2004.

[8] Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC 5245, 2010.

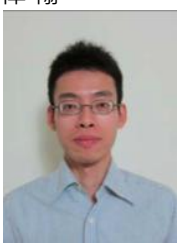
[9] Berkat S. Tung, Barry A. Whitebook, Joe S. Abuan, H. Jeong, Y. Yang and R. Garcia, “Apparatus and method for establishing and utilizing backup communication channels,” U.S. Patent 8 819 244, Aug. 26, 2014.

[10] Andrew H. Vyrros, Jeremy Matthew Werner and Patrick Gates, “Apparatus and method for inviting users to online sessions,” U.S. Patent 8 412 833, Apr. 2, 2013.

[11] Session Traversal Utilities for NAT (STUN), RFC 5389, 2008.

作者簡介

陳律翰



現任工研院資通所智慧聯網資訊系統與技術整合部工程師，國立台灣大學資訊工程學系博士，專長為行動計算、室內定位、嵌入式系統開發。

林宏偉

現任工研院資通所智慧聯網資訊系統與技術整合部工程師，加州州立理工大學資訊科學碩士，主要研究領域為H.323、SIP協議通話技術、小波轉換影像處理。

王慶堯

國立交通大學資訊工程學系博士，現任工研院資通所智慧聯網資訊系統與技術整合部經理，主要研究領域包括：資料探勘、智慧聯網、服務導向架構、遠距健康照護。