



交通大學

National Chiao Tung University

LAB 117
&
VoIP LAB



SIP Traversal over NAT Mechanisms on NTP VoIP Platform

Whai-En Chen

Research Assistant Professor

Dept. of Computer Science and Information Engineering

National Chiao Tung University

Email: wechen@mail.nctu.edu.tw

TEL: +886-3-5731924



Outline

- Introduction to SIP and NAT
- NAT Problem Definition
- NAT Solutions on NTP VoIP Platform
- Comparison
- Conclusion



Windows Messenger Installation

The screenshot shows the Microsoft download page for Windows Messenger 5.0 in Chinese. The browser address bar shows the URL: <http://www.microsoft.com/downloads/details.aspx?FamilyID=77c3799f-6398-4193-8002-ba55594c1e&DisplayLang=zh-tw>. The page title is "Windows Messenger 5.0 - 繁體中文". The left sidebar contains navigation links like "下載中心首頁", "下載類別", and "資源". The main content area has a "快速資訊" (Quick Info) table:

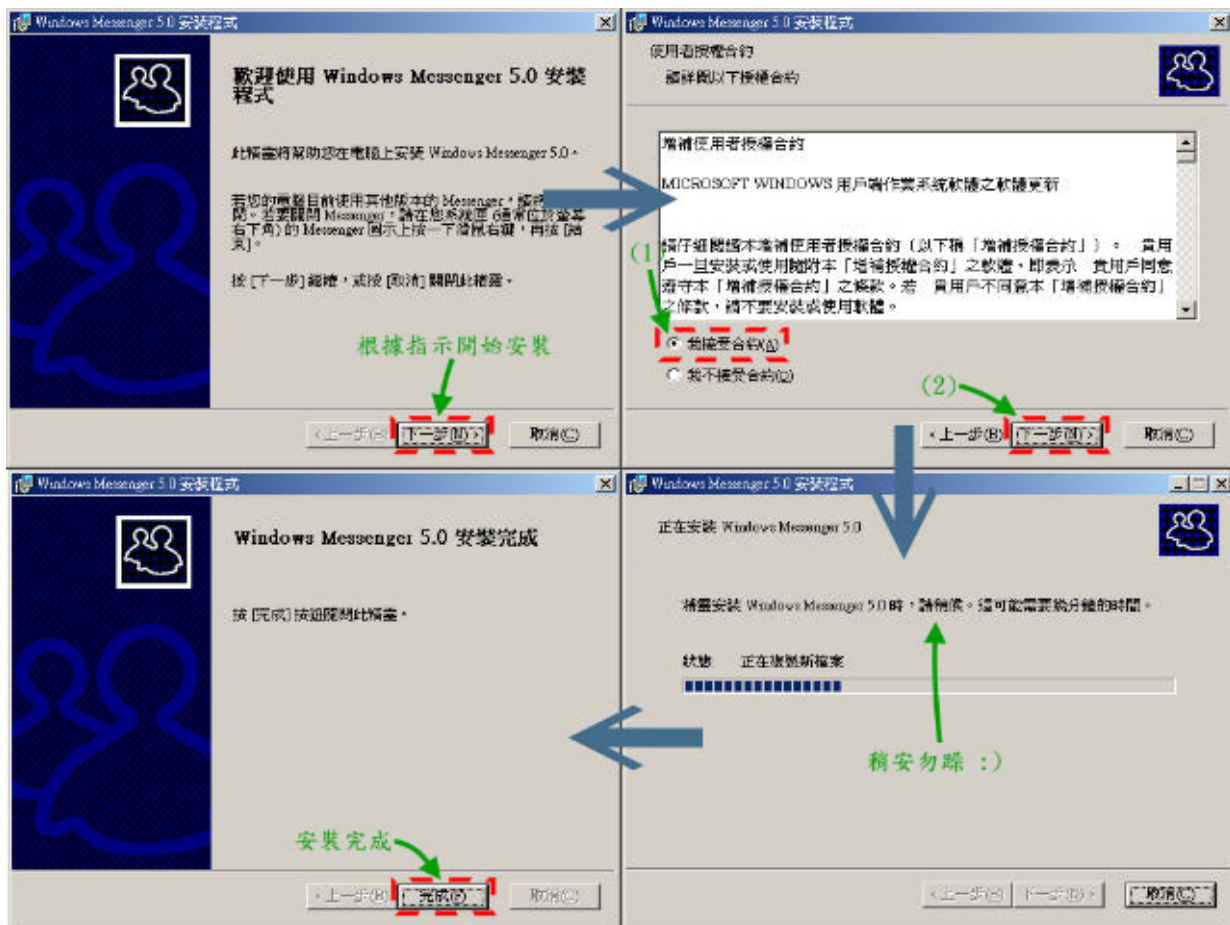
快速資訊	
檔案名稱:	install.exe
下載項目大小:	8455 KB
發佈日期:	2003/10/22
版本:	5.0

Below the table is a "下載" (Download) button. A red dashed box highlights the "下載" button and the "更換使用語言" (Change language) dropdown menu. A green arrow points to the "下載" button with the annotation "(2) 按此處下載". Another green arrow points to the "更換使用語言" dropdown with the annotation "(3) 儲存成檔案". The page also includes a "說明" (Description) section with instructions in English:

- Click the **Download** link to start the download, or choose a different language from the drop-down list and click **Go**.
- Do one of the following:
 - To start the installation immediately, click **Open** or **Run this program from its current location**.
 - To copy the download to your computer for installation at a later time, click **Save** or **Save this program to disk**.

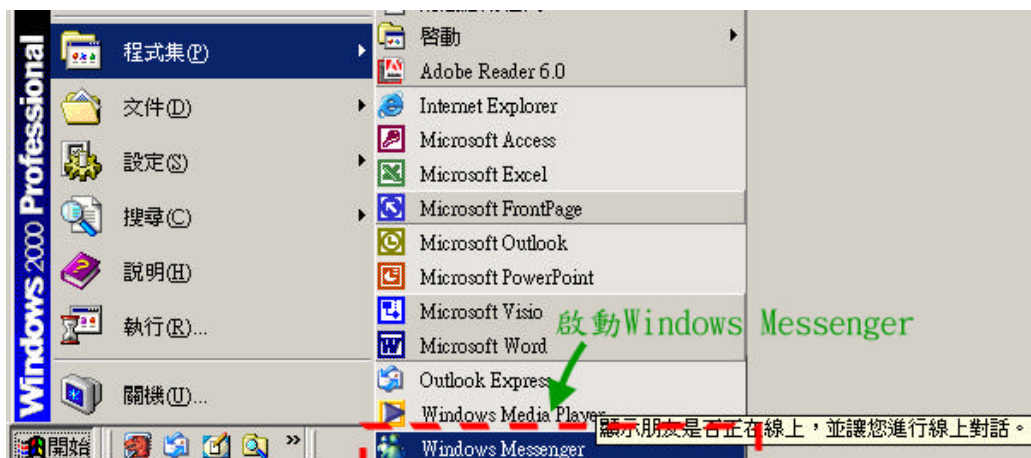


Step-by-step Installation



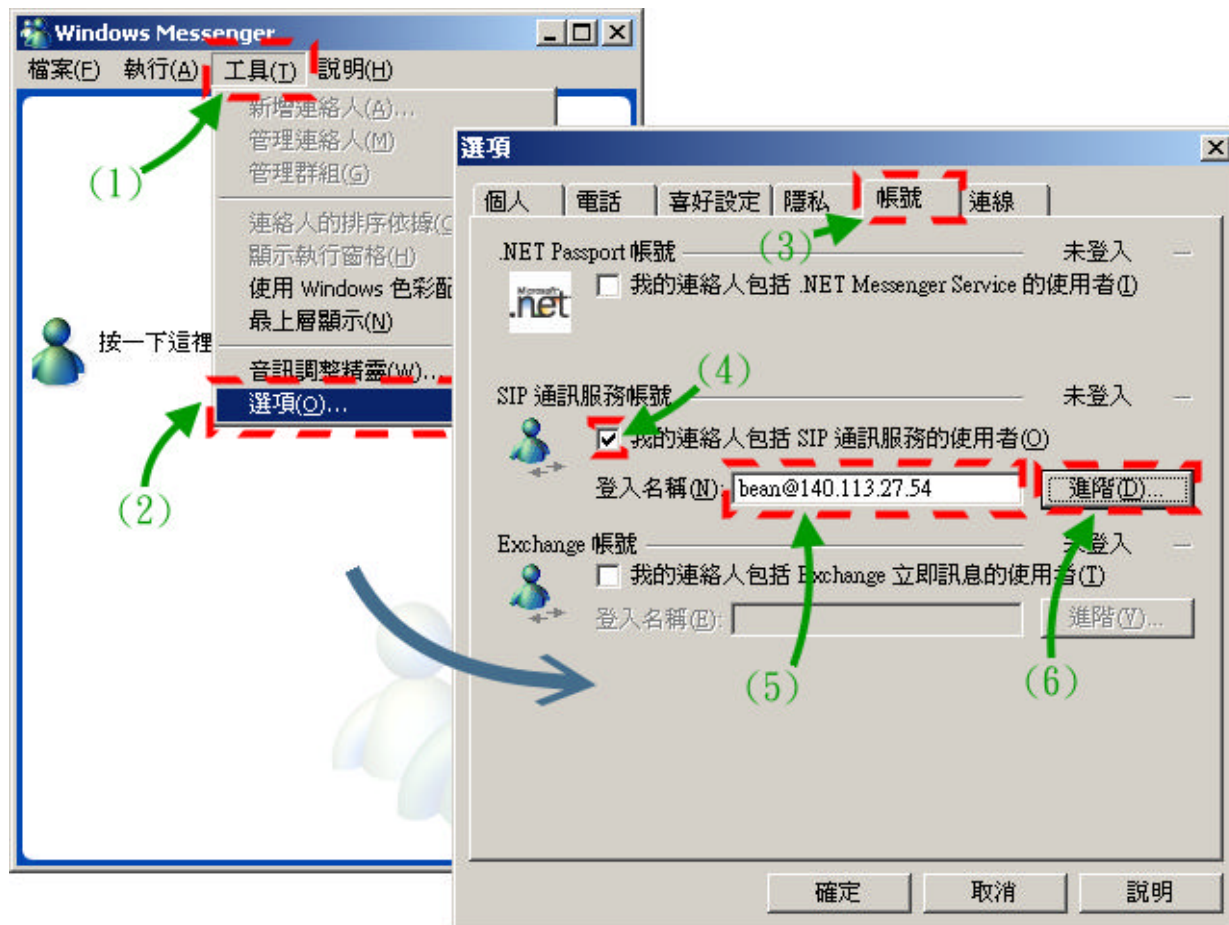


Windows Messenger Getting Start





Windows Messenger Configuration





SIP Server Configuration

SIP 通訊服務連線設定

選取應使用何種方法來設定您的通訊服務連線：

☐ 自動組態(A) (1)

☒ 組態設定(C)

伺服器名稱或 IP 位址(S): 140.113.27.54

連線使用：

☐ TCP(T)

☐ TLS(L)

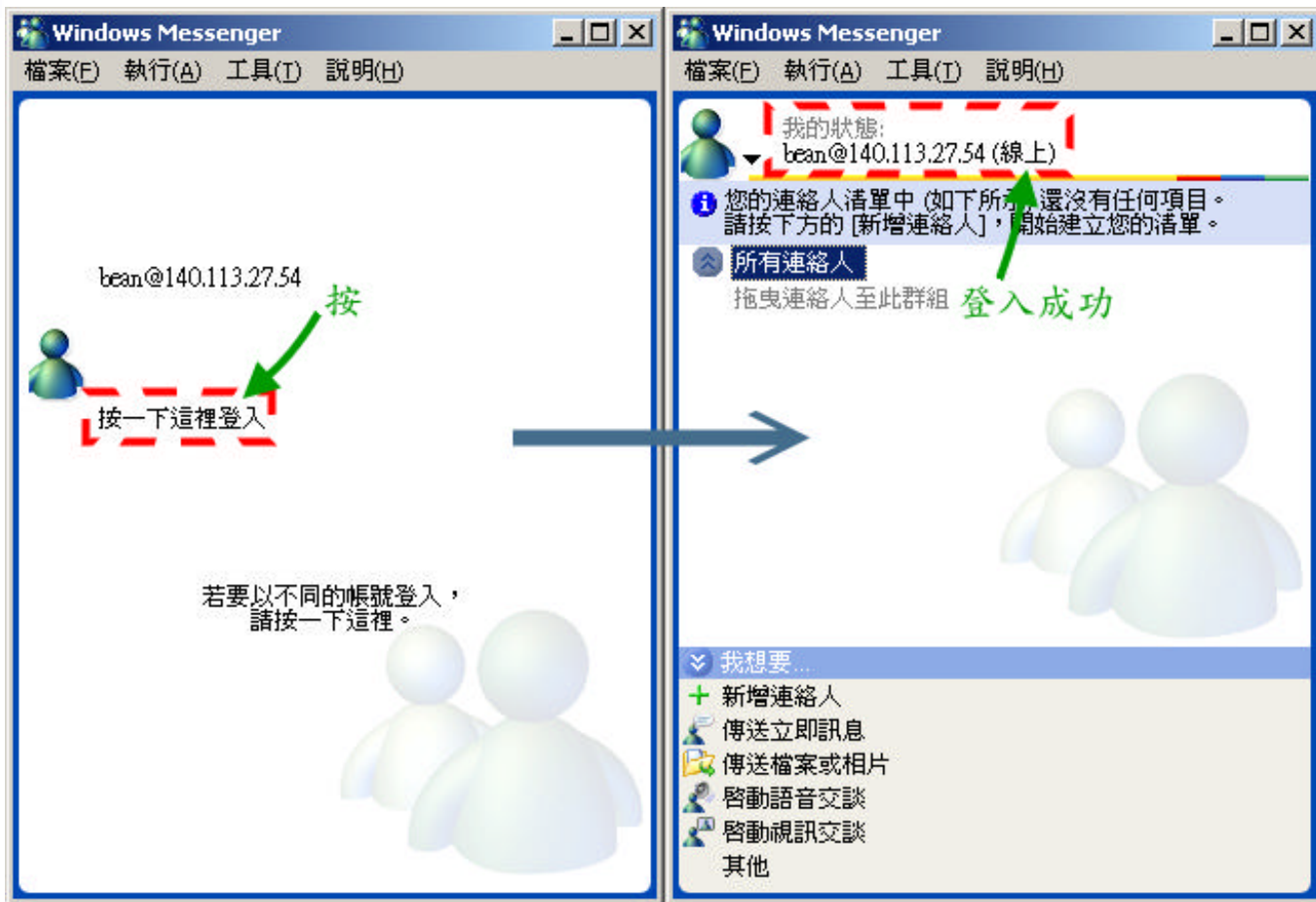
☒ UDP(U) (2)

(3)

確定 取消 說明

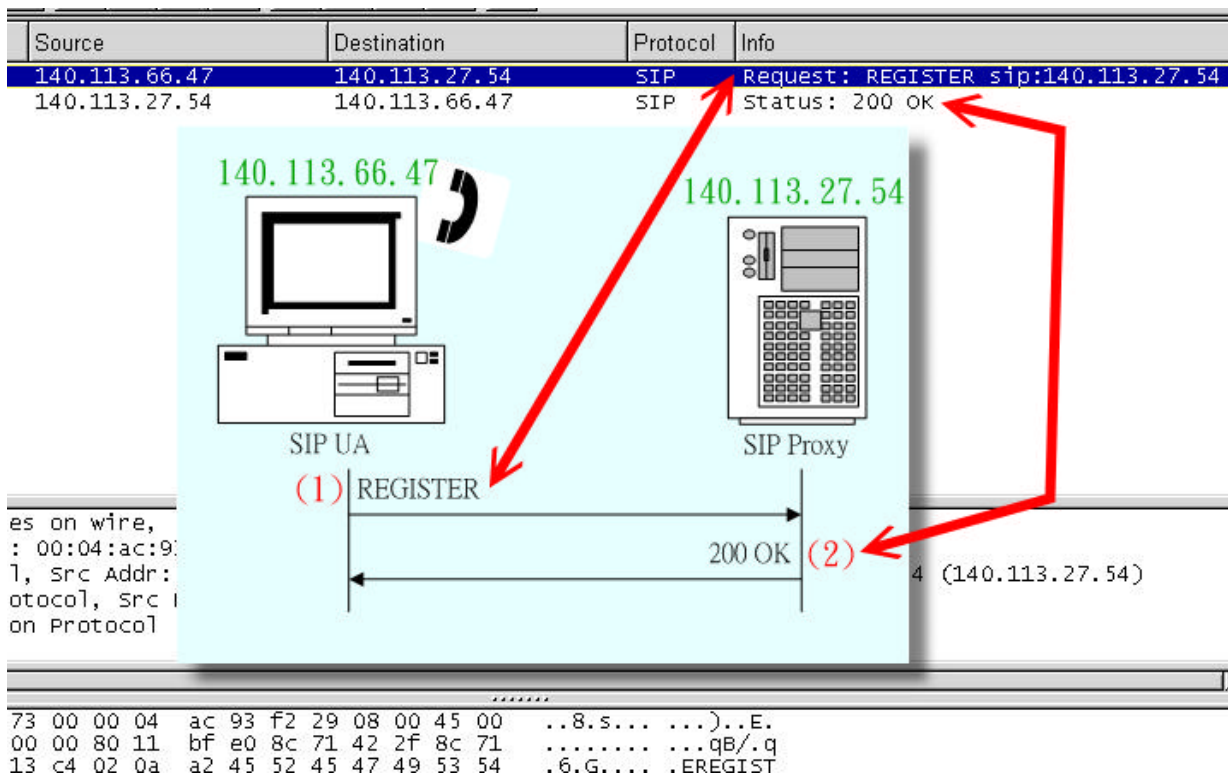


Login



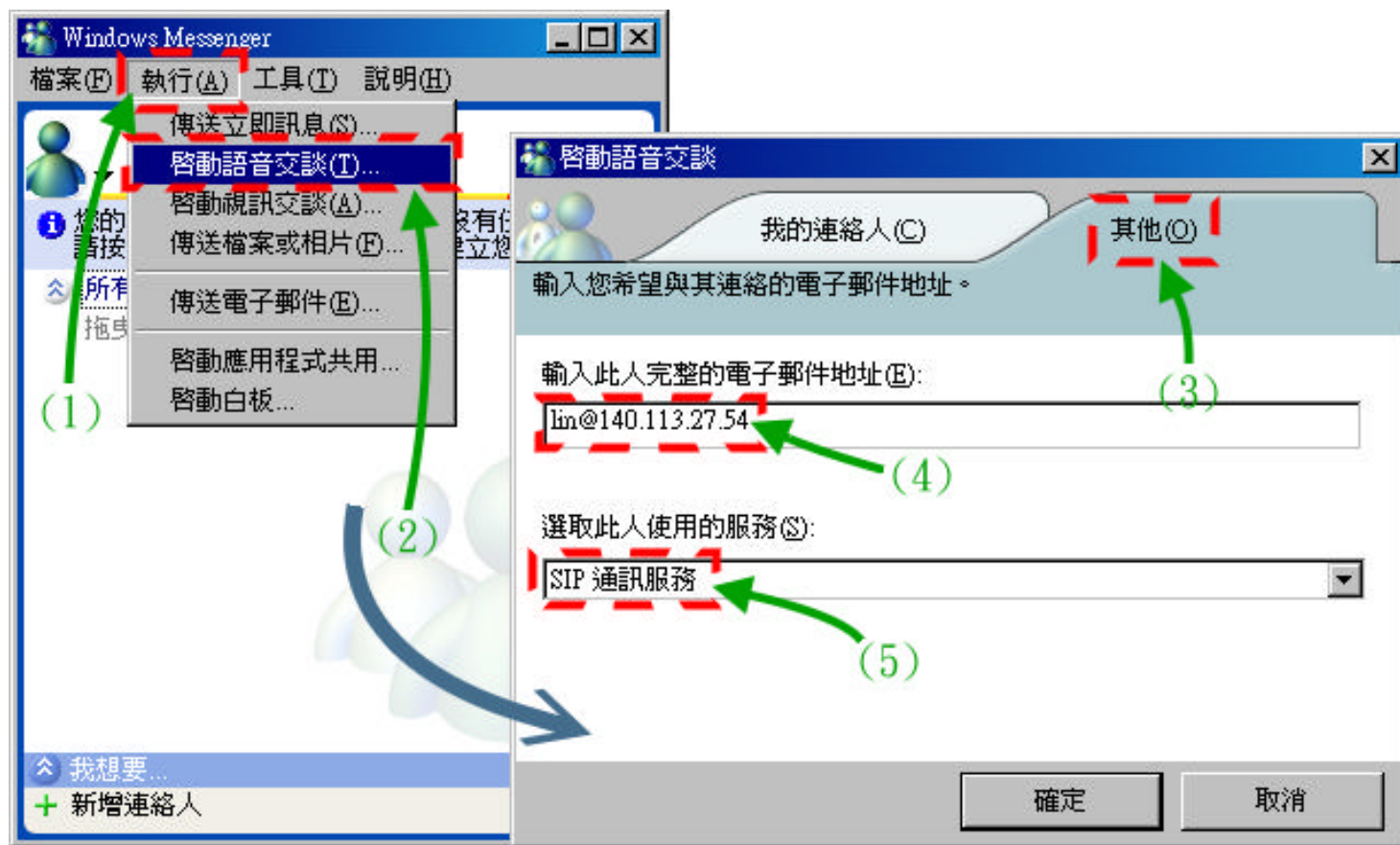


SIP Registration



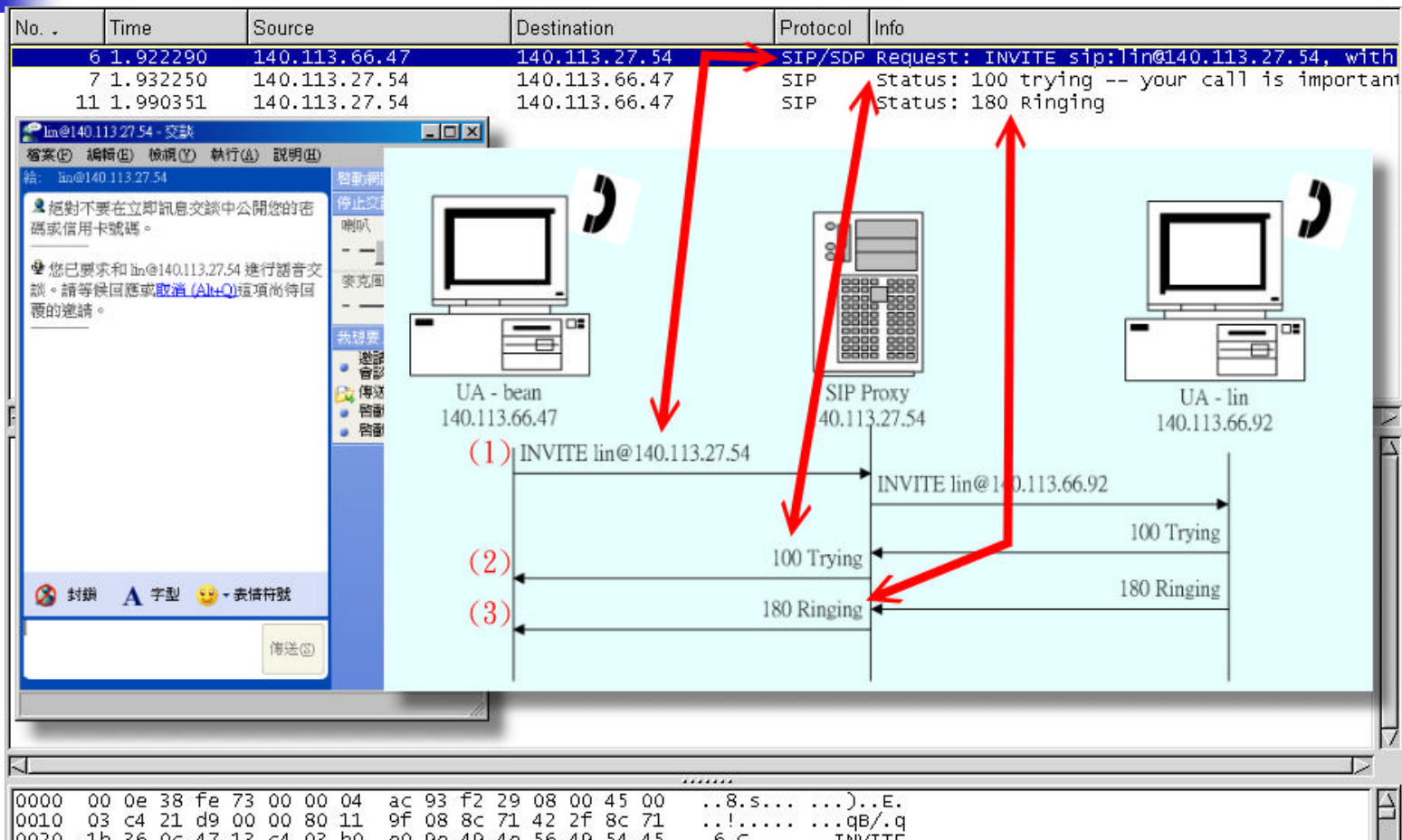


Dialing



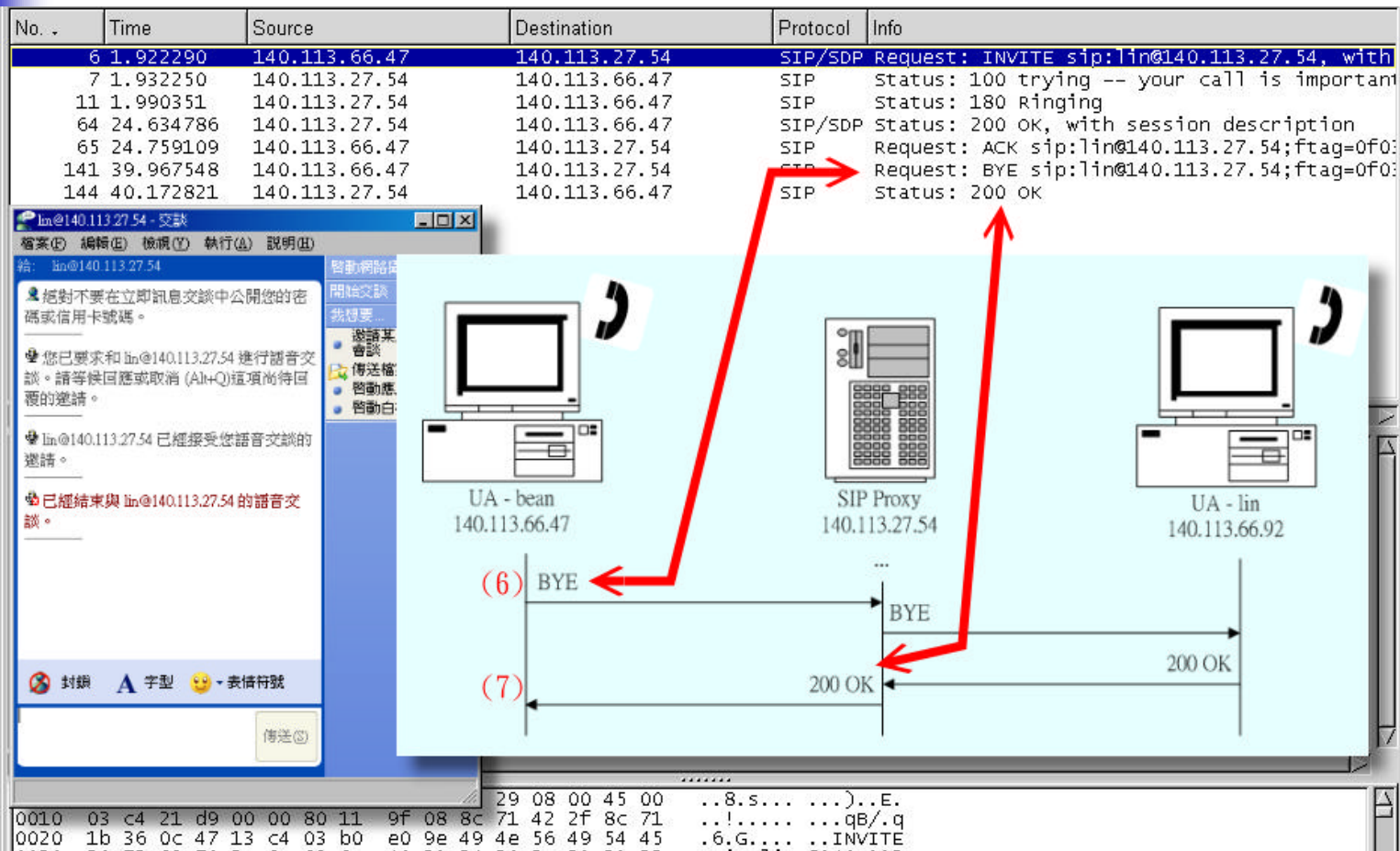


SIP INVITE Transaction



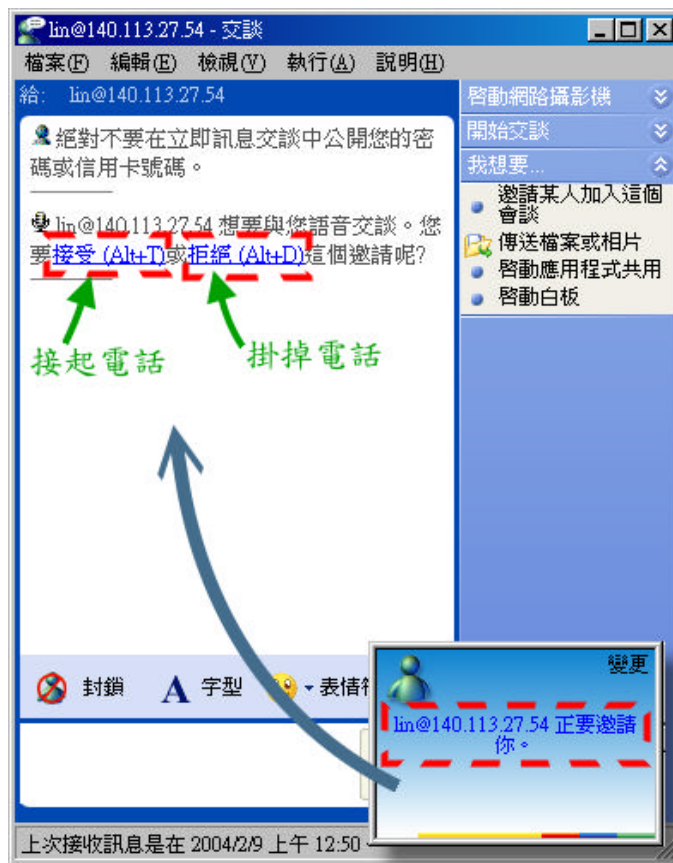


BYE Transaction



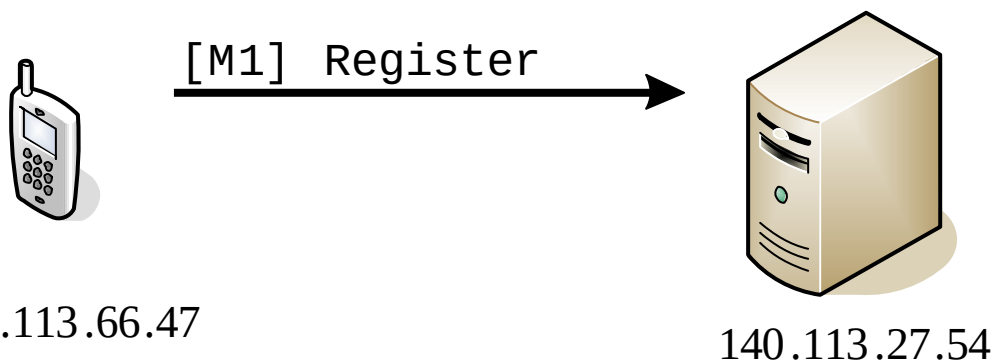


Accept a Call





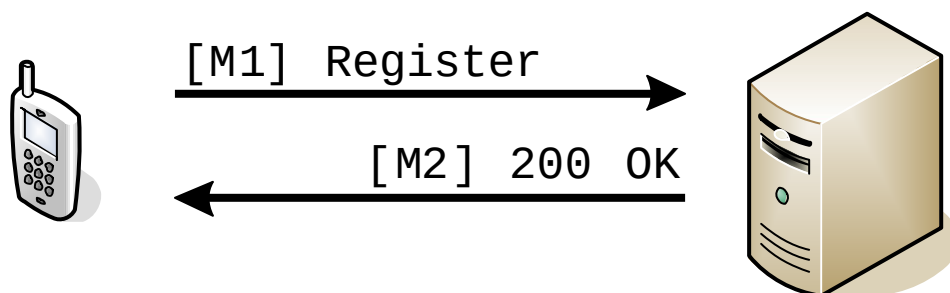
Registration Message Flow [1/2]



```
[M1]
REGISTER sip:140.113.27.54 SIP/2.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 70
From: <sip:bean@140.113.27.54>;tag=1209612b2a094c97b5473a6c8fca13a6;epid=04de356250
To: <sip:bean@140.113.27.54>
Call-ID: 8db46488bc4d4f6fb85476d9f3a68e62@140.113.66.47
CSeq: 1 REGISTER
Contact: <sip:140.113.66.47:12264>;methods="INVITE, MESSAGE, INFO, SUBSCRIBE, OPTIONS,
BYE, CANCEL, NOTIFY, ACK, REFER"
User-Agent: RTC/1.2.4949 (Messenger 5.0.0468)
Event: registration
Allow-Events: presence
Content-Length: 0
```



Registration Message Flow [2/2]



bean@140.113.66.47

140.113.27.54

```

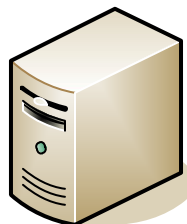
[M2]
SIP/2.0 200 OK
Via: SIP/2.0/UDP 140.113.66.47:12264
From: <sip:bean@140.113.27.54>;tag=1209612b2a094c97b5473a6c8fca13a6;epid=04de356250
To: <sip:bean@140.113.27.54>;tag=23567a396f2ab8c57a5581f34ecc9f8b.1f1f
Call-ID: 8db46488bc4d4f6fb85476d9f3a68e62@140.113.66.47
CSeq: 1 REGISTER
Contact: <sip:140.113.66.47:12264>;q=0.00;expires=3600
Server: Sip Express router (0.8.11 (i386/freebsd))
Content-Length: 0
Warning: 392 140.113.27.54:5060 "Noisy feedback tells: pid=76137
req_src_ip=140.113.66.47 req_src_port=3074 in_uri=sip:140.113.27.54
out_uri=sip:140.113.27.54 via_cnt=1"
    
```



Call Message Flow [1/15]

[M01] INVITE

bean@140.113.66.47



140.113.27.54

lin@140.113.66.92



[M01-1]

INVITE sip:lin@140.113.27.54 SIP/2.0

Via: SIP/2.0/UDP 140.113.66.47:12264

Max-Forwards: 70

From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250

To: <sip:lin@140.113.27.54>

Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47

CSeq: 1 INVITE

Contact: <sip:140.113.66.47:12264>

User-Agent: RTC/1.2

Content-Type: application/sdp

Content-Length: 525

[M01-2]

v=0

o=- 0 0 IN IP4 140.113.66.47

s=session

c=IN IP4 140.113.66.47

b=CT:1000

t=0 0

m=audio 42522 RTP/AVP 97 111 112 6 0 8 4 5 3 101

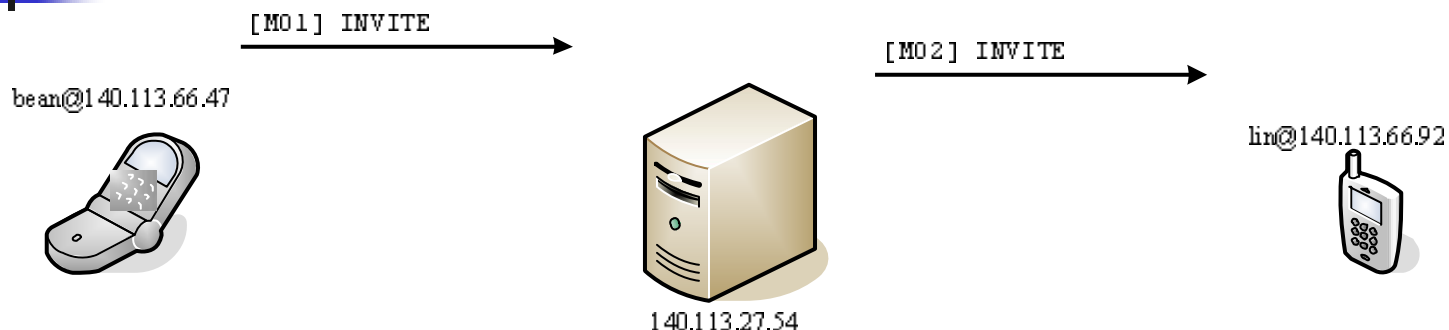
k=base64:cReawB4kZs5su1tjK/1MLU2txhPZd3UfpkfafZeSwo

a=rtpmap:97 red/8000

...



Call Message Flow [2/15]



[M02-1]

```

INVITE sip:140.113.66.92:15450 SIP/2.0
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK944c.70b18621.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 69
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 INVITE
Contact: <sip:140.113.66.47:12264>
User-Agent: RTC/1.2
Content-Type: application/sdp
Content-Length: 525
  
```

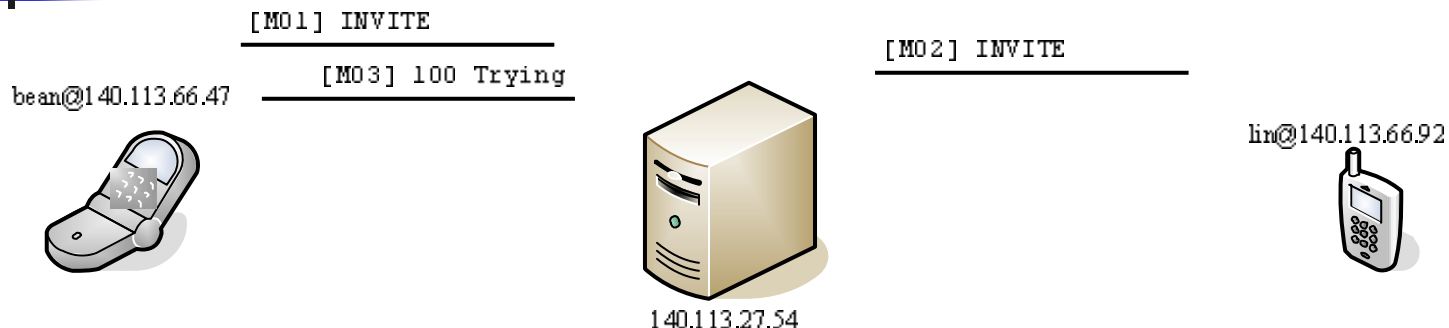
[M02-2]

```

v=0
o=- 0 0 IN IP4 140.113.66.47
s=session
c=IN IP4 140.113.66.47
b=CT:1000
t=0 0
m=audio 42522 RTP/AVP 97 111 112 6 0 8 4 5 3 101
k=base64:cReawB4kZs5su1tjK/1MLU2txhPZd3UfpkfafZeSwo
a=rtpmap:97 red/8000
...
  
```



Call Message Flow [3/15]

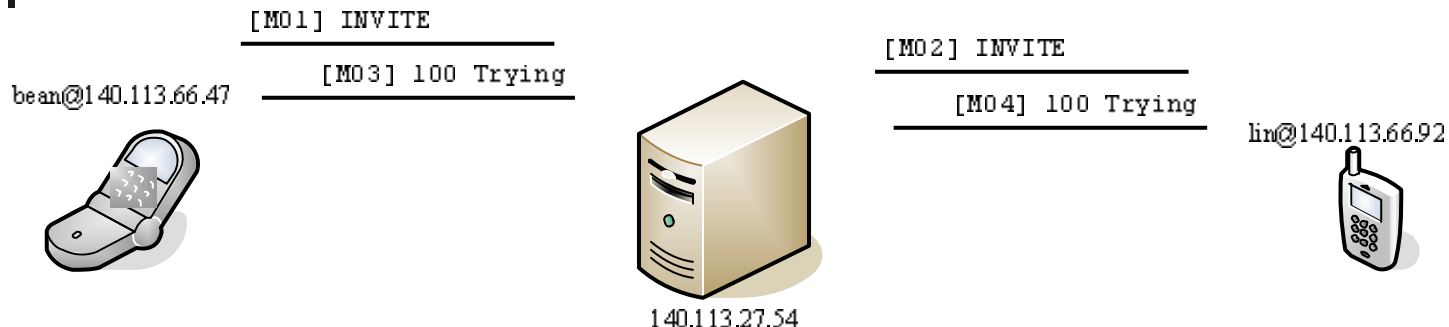


[M03]

```
SIP/2.0 100 trying — your call is important to us
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 INVITE
Server: Sip Express router (0.8.11 (i386/freebsd))
Content-Length: 0
Warning: 392 140.113.27.54:5060 "Noisy feedback tells: pid=76137 req_src_ip=140.113.66.47
req_src_port=3074 in_uri=sip:lin@140.113.27.54 out_uri=sip:140.113.66.92:15450 via_cnt==1"
```



Call Message Flow [4/15]



[M04]

SIP/2.0 100 Trying

Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK944c.70b18621.0

Via: SIP/2.0/UDP 140.113.66.47:12264

From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250

To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a

Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47

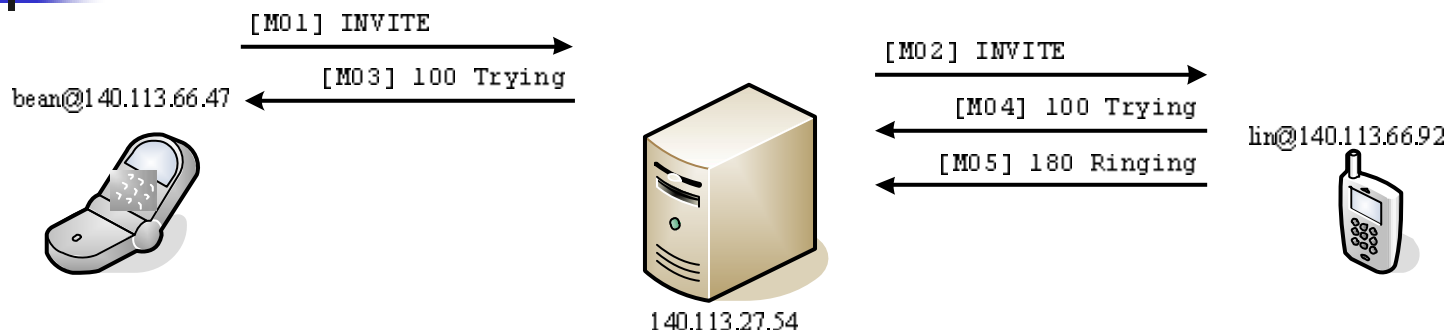
CSeq: 1 INVITE

User-Agent: Windows RTC/1.0

Content-Length: 0



Call Message Flow [5/15]



[M05]

SIP/2.0 180 Ringing

Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK944c.70b18621.0

Via: SIP/2.0/UDP 140.113.66.47:12264

From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250

To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a

Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47

CSeq: 1 INVITE

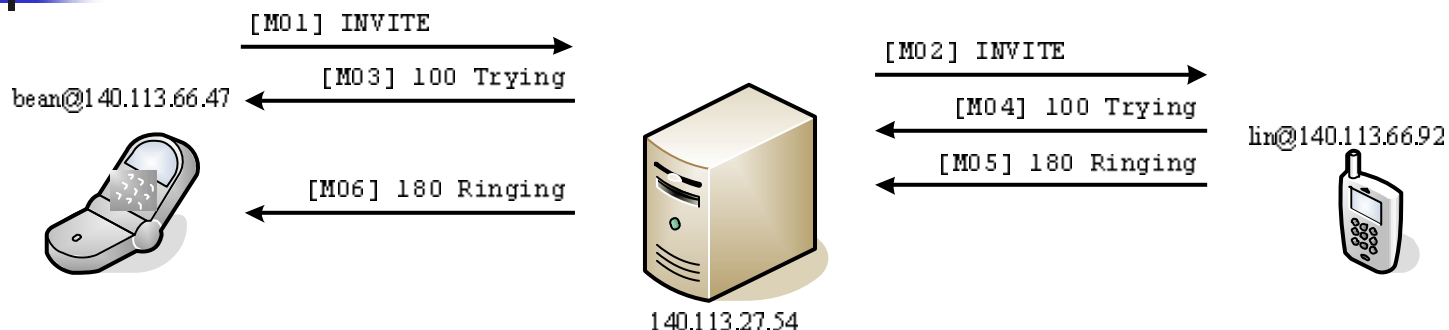
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>

User-Agent: Windows RTC/1.0

Content-Length: 0



Call Message Flow [6/15]



[M06]

SIP/2.0 180 Ringing

Via: SIP/2.0/UDP 140.113.66.47:12264

From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250

To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a

Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47

CSeq: 1 INVITE

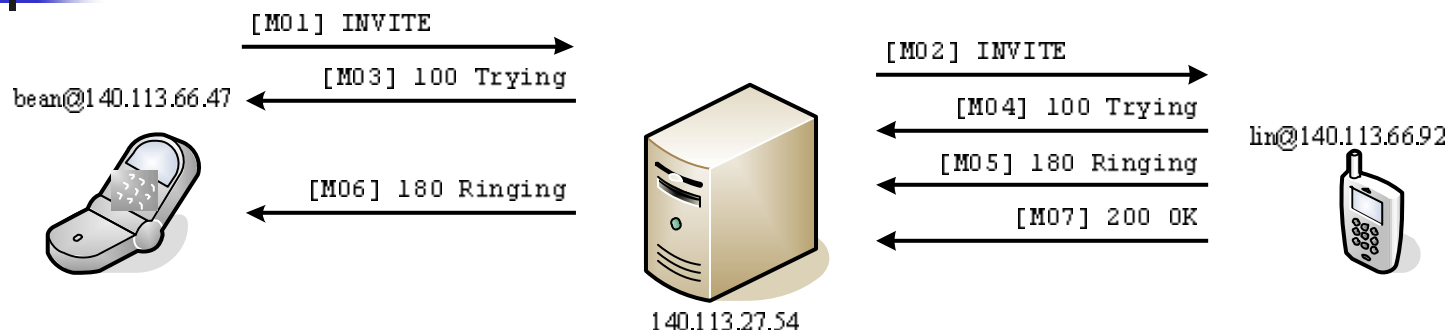
Record-Route: <sip:lin@140.113.27.54>;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>

User-Agent: Windows RTC/1.0

Content-Length: 0



Call Message Flow [7/15]



```

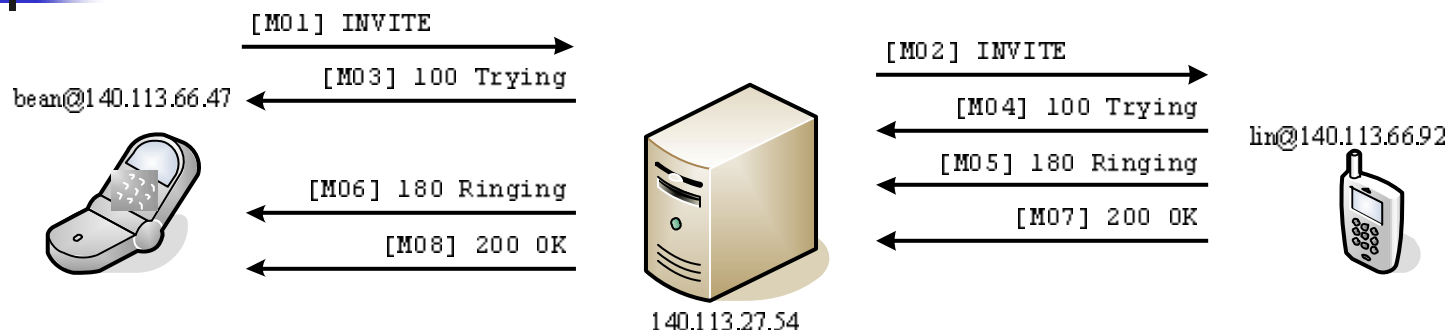
[M07-1]
SIP/2.0 200 OK
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK944c.70b18621.0
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 INVITE
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Contact: <sip:140.113.66.92:15450>
User-Agent: Windows RTC/1.0
Content-Type: application/sdp
Content-Length: 455
    
```

```

[M07-2]
v=0
o=R100-Lin 0 0 IN IP4 140.113.66.92
s=session
c=IN IP4 140.113.66.92
b=CT:1000
t=0 0
m=audio 27644 RTP/AVP 97 111 112 6 0 8 4 5 3 101
a=rtpmap:97 red/8000
...
    
```



Call Message Flow [8/15]

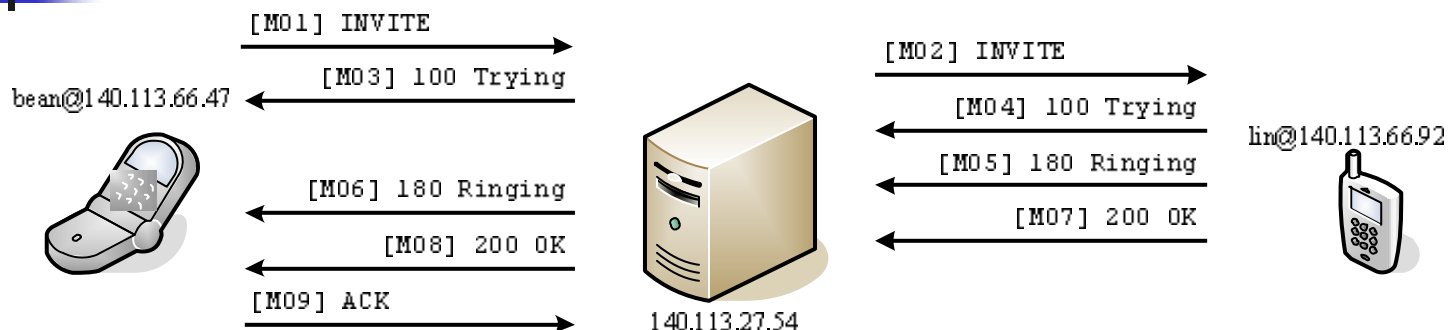


[M08-1]
SIP/2.0 200 OK
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 INVITE
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Contact: <sip:140.113.66.92:15450>
User-Agent: Windows RTC/1.0
Content-Type: application/sdp
Content-Length: 455

[M08-2]
v=0
o=R100-Lin 0 0 IN IP4 140.113.66.92
s=session
c=IN IP4 140.113.66.92
b=CT:1000
t=0 0
m=audio 27644 RTP/AVP 97 111 112 6 0 8 4 5 3 101
a=rtpmap:97 red/8000
...



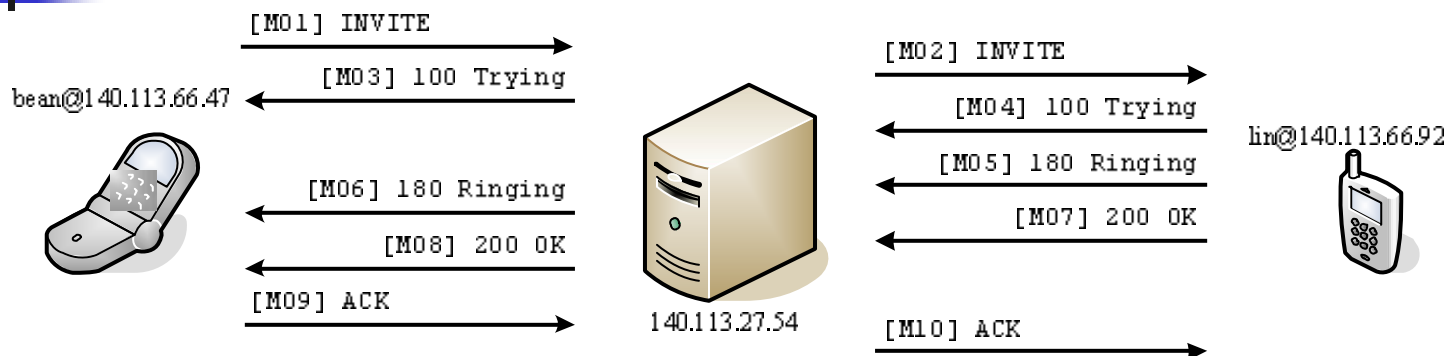
Call Message Flow [9/15]



[M09] **140.113.66.92**
ACK sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on SIP/2.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 70
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 ACK **140.113.27.54**
Route: <sip:140.113.66.92:15450>
User-Agent: RTC/1.2
Content-Length: 0



Call Message Flow [10/15]



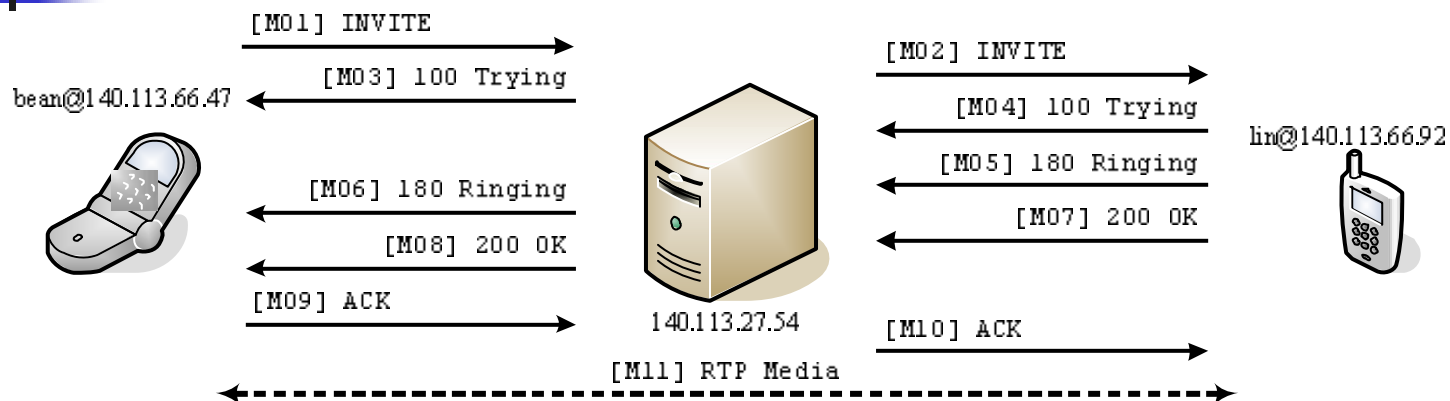
[M10]

```

ACK sip:140.113.66.92:15450 SIP/2.0
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Via: SIP/2.0/UDP 140.113.27.54;branch=0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 69
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 ACK
User-Agent: RTC/1.2
Content-Length: 0
    
```

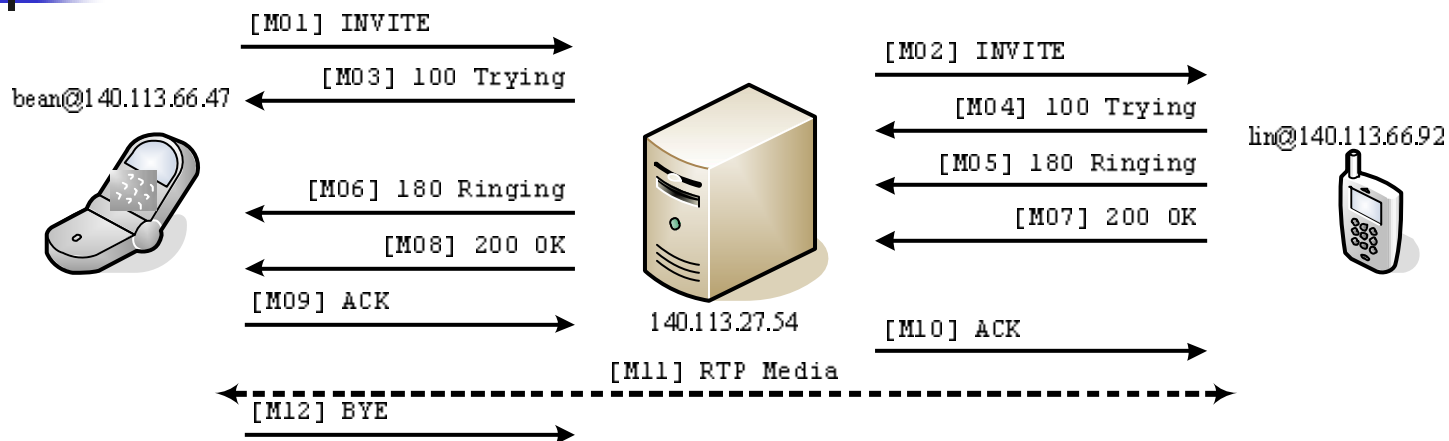


Call Message Flow [11/15]





Call Message Flow [12/15]



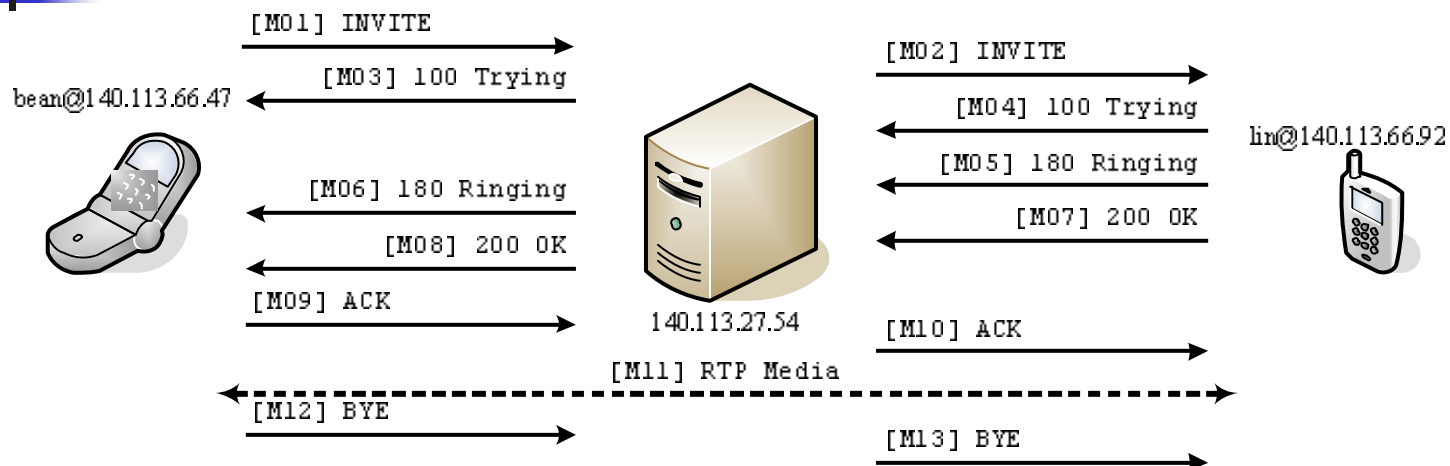
[M12]

```

BYE sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on SIP/2.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 70
From: "bear@140.113.27.54" <sip:bear@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 2 BYE
Route: <sip:lin@140.113.27.54>
User-Agent: RTC/1.2
Content-Length: 0
  
```




Call Message Flow [13/15]



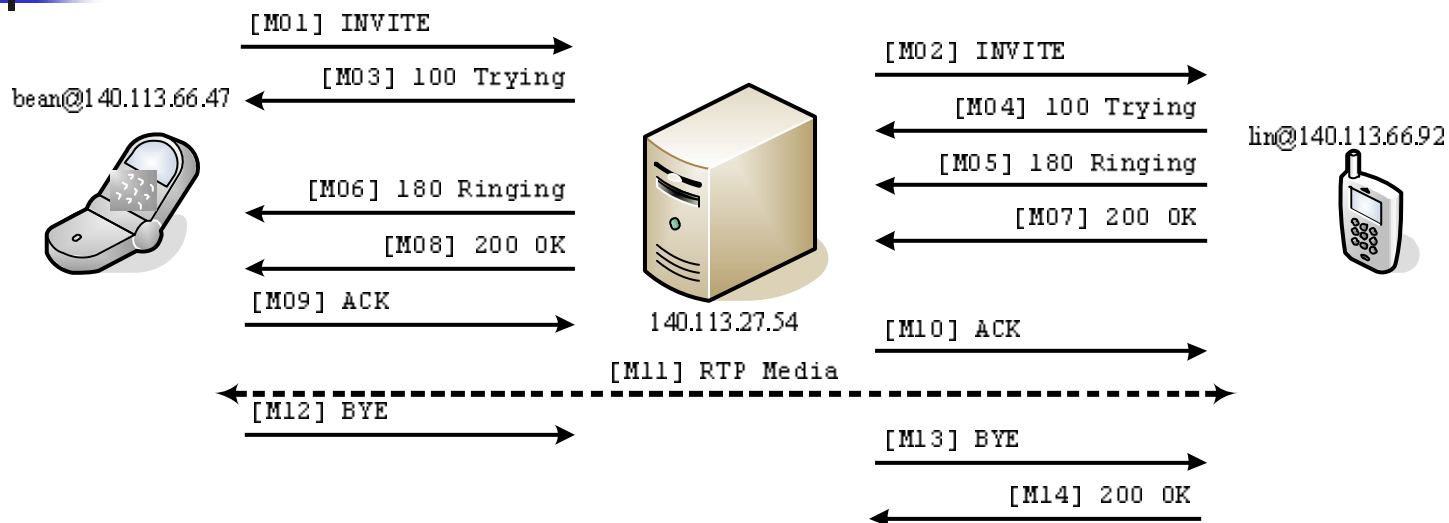
[M3]

```

BYE sip:140.113.66.92:15450 SIP/2.0
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK644c.887cba62.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 69
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 2 BYE
User-Agent: RTC/1.2
Content-Length: 0
    
```



Call Message Flow [14/15]



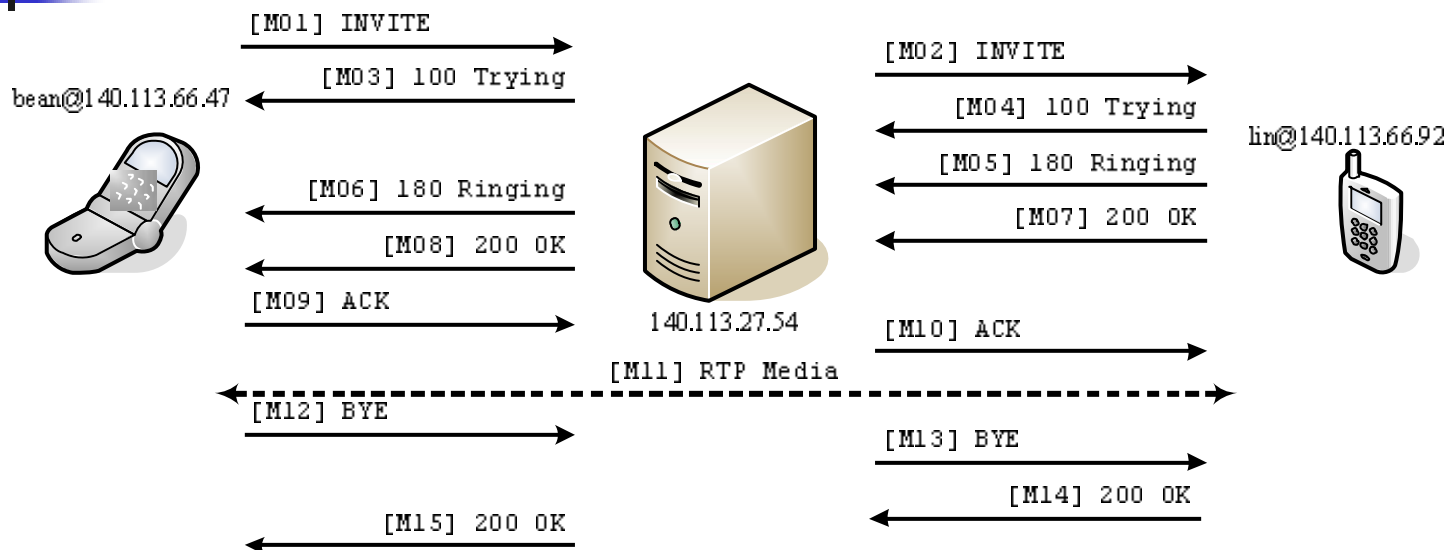
[M14]

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK644c.887cba62.0
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 2 BYE
User-Agent: Windows RTC/1.0
Content-Length: 0
    
```



Call Message Flow [15/15]



[M15]

SIP/2.0 200 OK

Via: SIP/2.0/UDP 140.113.66.47:12264

From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250

To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a

Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47

CSeq: 2 BYE

User-Agent: Windows RTC/1.0

Content-Length: 0

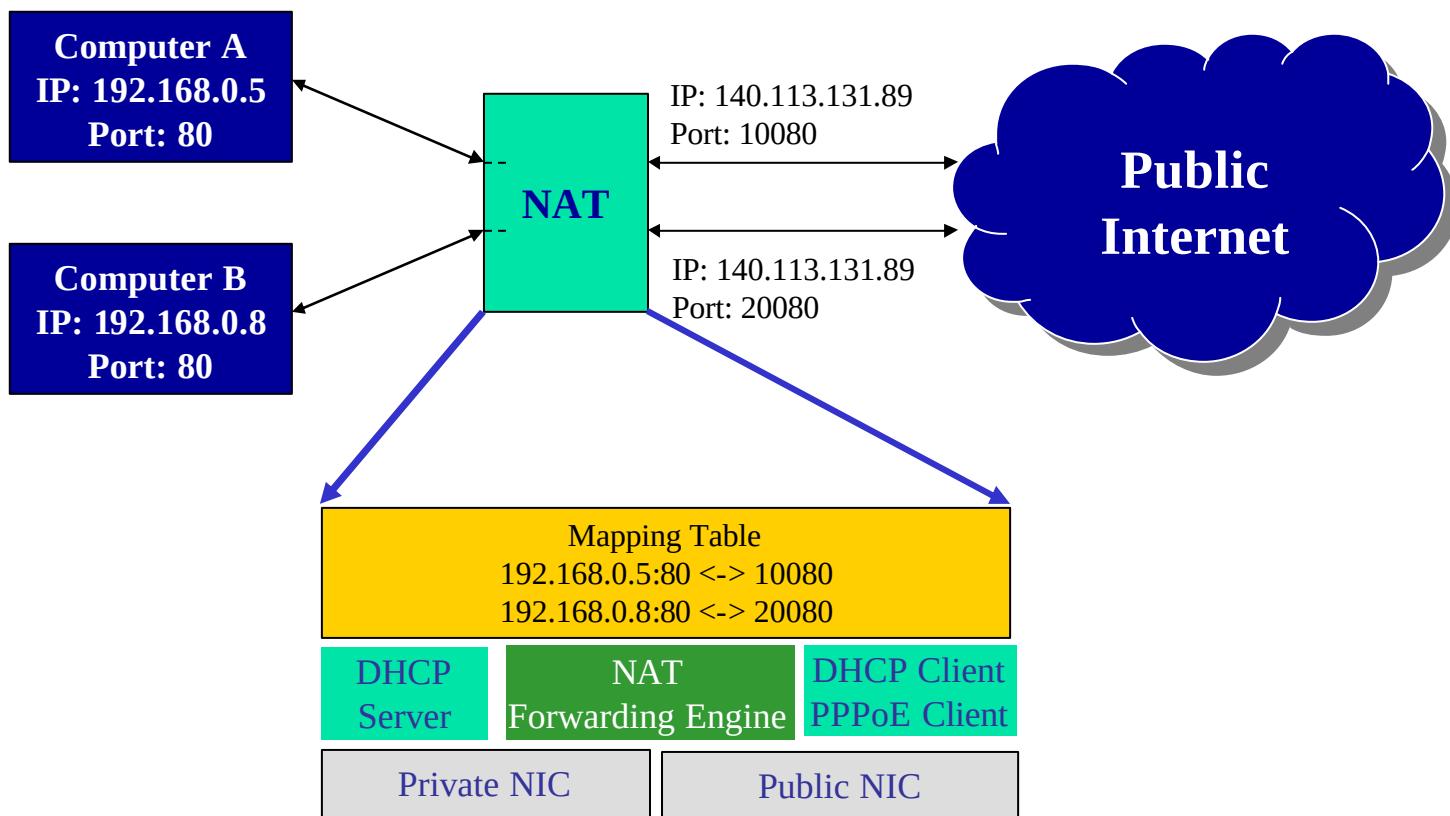


What is NAT

- NAT - Network Address Translation
 - RFC 3022 - Traditional IP Network Address Translator
 - RFC 1918 - Address Allocation for Private Internets (BCP 5)
 - RFC 2993 - Architectural Implications of NAT
 - RFC 3027 - Protocol Complications with the IP Network Address Translator
 - RFC 3235 - Network Address Translator (NAT)-Friendly Application Design Guidelines
- Convert IP Address (with Port multiplexing) between private and public realm
- Works on network and transport layers
- Transparent for Application



NAT Schematic





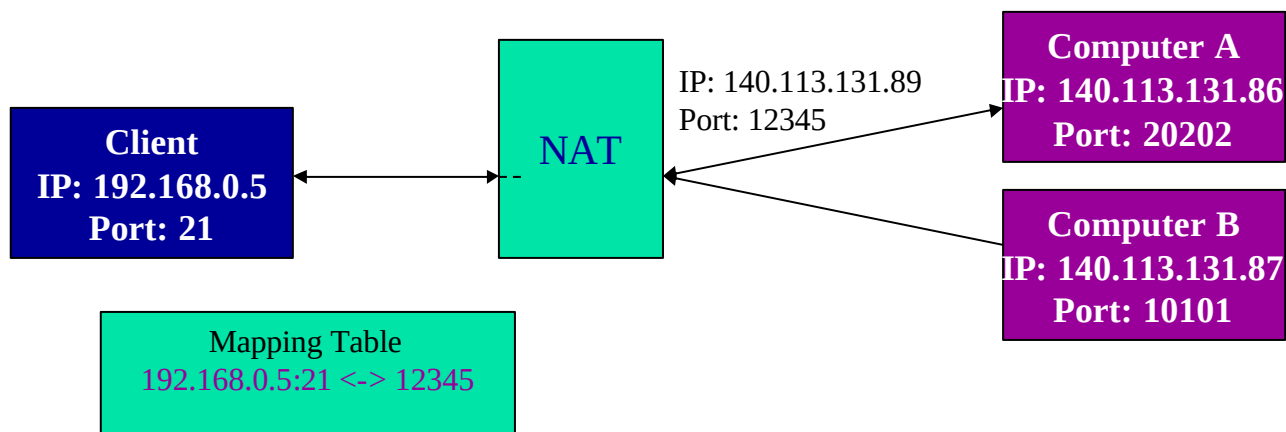
Types of NAT

- **Fully Cone**: map an internal IP and port to a public port
- **Restricted Cone**: Fully Cone with IP filtering
- **Port Restricted Cone**: Fully Cone with IP and port filtering
- **Symmetric**: build IP and port mapping according to a session ID



Fully Cone NAT

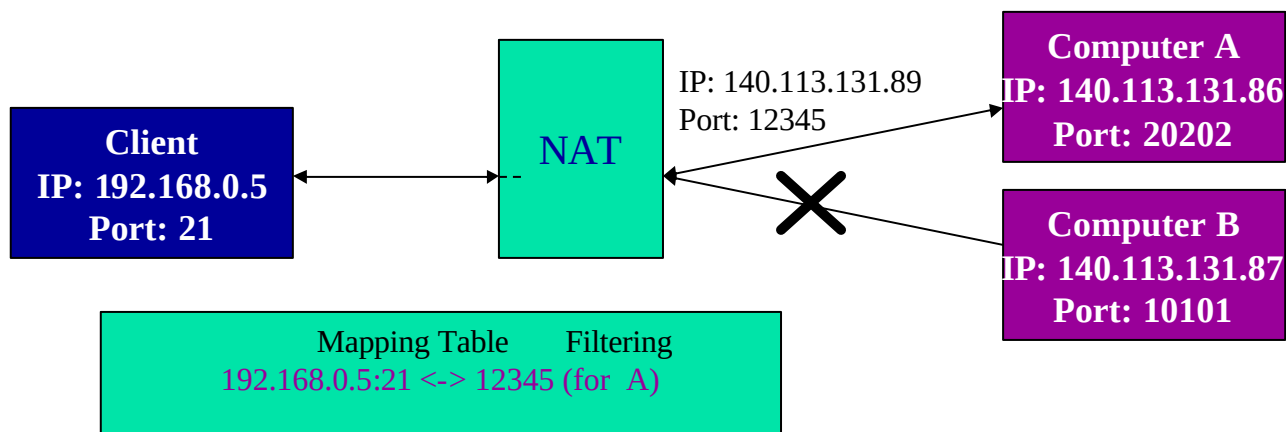
- Client sends a packet to public address A.
- NAT allocates a public port (12345) for private port (21) on the client.
- Any incoming packet (from A or B) to public port (12345) will be dispatched to private port (21) on the client.





Restricted Cone NAT (1/2)

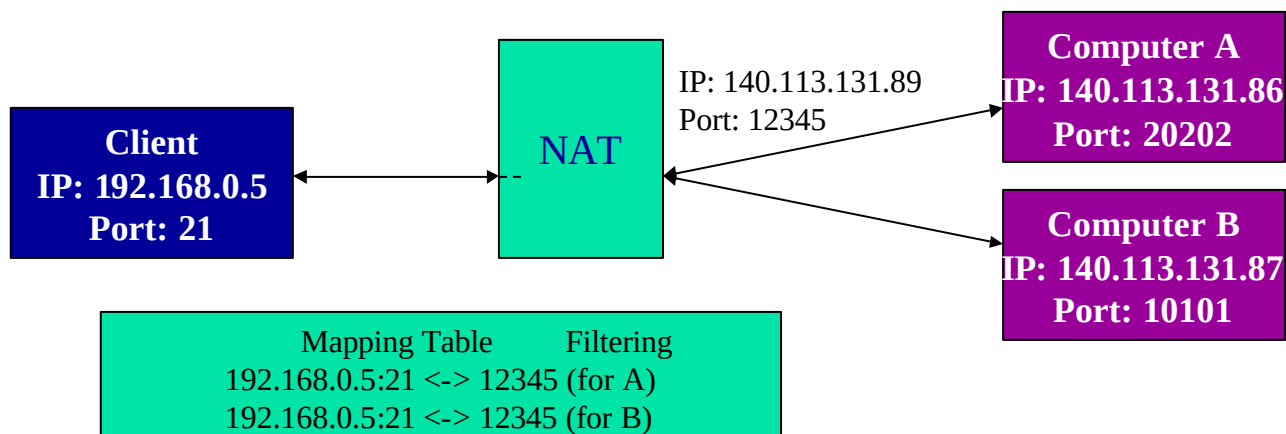
- Client sends a packet to public address A.
- NAT allocates a public port (12345) for private port (21) on the client.
- Only incoming packet from **A** to public port (12345) will be dispatched to private port (21) on the client.





Restricted Cone NAT (2/2)

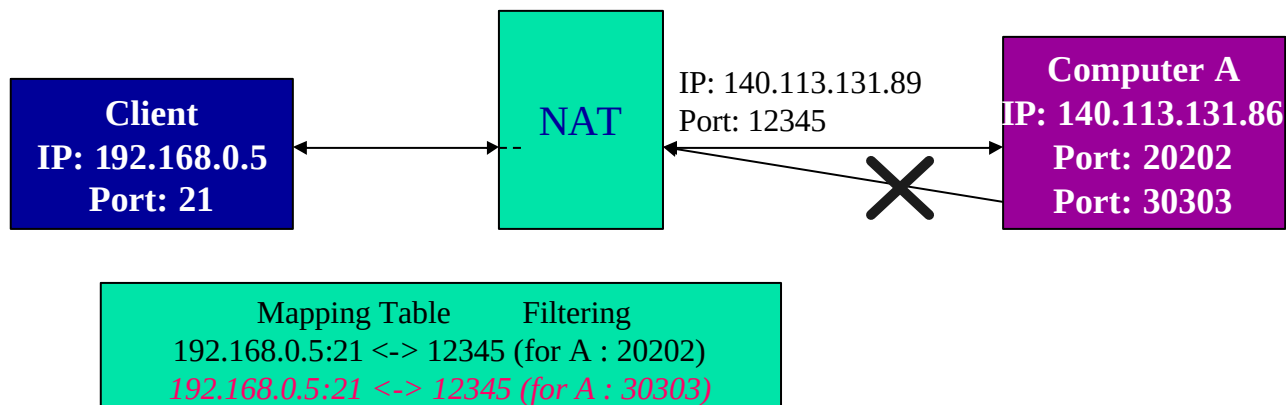
- Client sends another packet to public address B.
- NAT will **reuse** allocated public port (12345) for private port (21) on the client.
- Incoming packet from **B** to public port (12345) now will be dispatched to private port (21) on the client.





Port Restricted Cone NAT

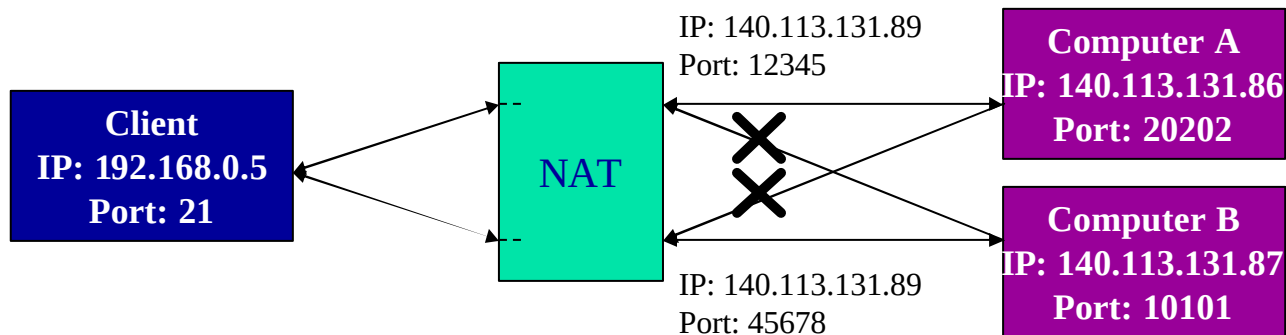
- Client sends a packet to public address A port 20202.
- NAT will allocate a public port (12345) for private port (21) on the client.
- Only incoming packet from address A and port 20202 to public port (12345) will be dispatched to private port (21) on the client.





Symmetric NAT

- NAT allocates a public port each time the client sends a packet to different public address and port
- Only incoming packet from the original mapped public address and port will dispatch to private port on client



Mapping Table		Filtering
192.168.0.5:21	<-> 12345	(for A : 20202)
192.168.0.5:21	<-> 45678	(for B : 10101)



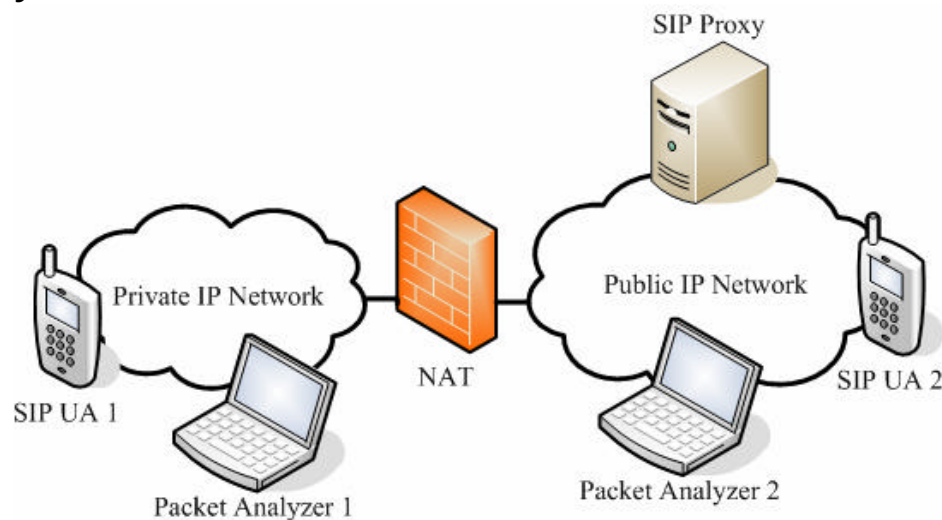
SIP and NAT

- NAT converts IP addresses in IP Headers
- Problem 1:
 - SIP/SDP is an application-layer protocol but contains IP address/port information, which is **not translated** by NAT
- Problem 2:
 - Private client must send a outgoing packet first (to create a mapping on NAT) to receive incoming packet



Testing Environment

- SIP UA 1: User Agent behind NAT (Private Domain).
- SIP UA 2: SIP UA outside NAT (Public Domain).
- SIP Proxy: IPtel SIP Express Router (SER) v0.8.11.
- NAT: Windows XP with 2 NICs
- Packet Analyzer 1 & 2: Ethereal





The Problem (1/2)

- Due to private address, the Via and Contact header fields in SIP messages sent by UA1 are incorrect.
 - With incorrect **Via** header, **responses** of messages sent by UA1 cannot be routed back.
 - With incorrect **Contact** address in **REGISTER** messages, call server cannot inform UA1 the incoming calls.
 - UA1 can only act as a calling party.



Incorrect REGISTER Message

The Ethernet Network Analyzer

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
29	21.604799	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:sip3.ipv6.club.tw:5060
32	25.610837	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:sip3.ipv6.club.tw:5060
33	29.616845	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:sip3.ipv6.club.tw:5060
34	33.622866	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:sip3.ipv6.club.tw:5060
35	37.629045	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:sip3.ipv6.club.tw:5060

▶ Frame 35 (558 bytes on wire (558 bytes captured))

▶ Ethernet II, Src: 00:08:0d:35:70:d1, Dst: 00:04:75:e4:66:eb

▶ Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)

▶ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

▼ Session Initiation Protocol

 ▼ Request-Line: REGISTER sip:sip3.ipv6.club.tw:5060 SIP/2.0

 Method: REGISTER

 ▼ Message Header

 Call-ID: 495-D1B9-1180-108925650780A5-D8C67E3F54A6@R100-Lin

 Contact: <sip:944021375@192.168.0.111:5060>

 Content-Encoding: identity

 Content-Language: en

 Content-Length: 0

 CSeq: 1 REGISTER

 Expires: 3600

 ▶ From: "944021375"<sip:944021375@sip3.ipv6.club.tw>;tag=944021375-1089256507

 Max-Forwards: 10

 To: "944021375"<sip:944021375@sip3.ipv6.club.tw>

 User-Agent: CCL_SIP_SOFTPHONE.....

 Via: SIP/2.0/UDP 192.168.0.111:5060;branch=z9hG4bK7b37d4081df295ae173c0114de8ea098

0000 00 04 75 e4 66 eb 00 08 0d 35 70 d1 08 00 45 00 ..u.f...Sp...E.

0010 02 20 01 ed 00 00 80 11 66 50 c0 a8 00 6f 8c 71 fP...o.q

0020 83 07 13 c4 13 c4 02 0c 9b 56 52 45 47 49 53 54 VREGIST

0030 45 52 20 73 69 70 3a 73 69 70 33 2e 69 70 76 36 ER sip:s ip3.ipv6

0040 2e 63 6c 75 62 2e 74 77 3a 35 30 36 30 20 53 49 .club.tw :5060 SI

Filter: sip + Expression... Clear Apply <live capture in progr P: 40 D: 11 M: 0



The Problem (2/2)

- When UA1 initiate a call, the connection information (**c** and **m**) for media establishment in SDP are also incorrect.
 - UA2 gets a private peer address, the **RTP** packets from UA2 cannot be routed to UA1.
 - Media can only be sent from UA1 to UA2.



Incorrect Fields in SDP of INVITE Message

(Untitled1) - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

251	144.317938	192.168.0.111	140.113.131.7	SIP/SDP Request: INVITE sip:944021371@sip3.ipv6.club.tw, with :
252	145.319602	192.168.0.111	140.113.131.7	SIP/SDP Request: INVITE sip:944021371@sip3.ipv6.club.tw, with :
253	147.322717	192.168.0.111	140.113.131.7	SIP/SDP Request: INVITE sip:944021371@sip3.ipv6.club.tw, with :

Frame 253 (893 bytes on wire, 893 bytes captured)

Ethernet II, Src: 00:08:0d:35:70:d1, Dst: 00:04:75:e4:66:ab

Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Request-Line: INVITE sip:944021371@sip3.ipv6.club.tw SIP/2.0

Message Header

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): 944021375 188561 188561 IN IP4 192.168.0.111

Session Name (s): Session SDP

Connection Information (c): IN IP4 192.168.0.111

Bandwidth Information (b): CT:300

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 9000 RTP/AVP 0 8 3 4 18

Media Attribute (a): rtcpmap:0 PCMU/8000/1

Media Attribute (a): rtcpmap:8 PCMA/8000/1

Media Attribute (a): rtcpmap:3 GSM/8000/1

Media Attribute (a): rtcpmap:4 G723/8000/1

Media Attribute (a): rtcpmap:18 G729/8000/1

Media Attribute (a): ptm:120

0000 00 04 75 e4 66 ab 00 08 0d 35 70 d1 08 00 45 00 ..u.f...Sp...E.

0010 03 6f 01 20 00 00 80 11 65 ce c0 a8 00 6f 8c 71 .o.e....o.g

0020 83 07 13 c4 13 c4 03 5b 18 2d 49 4e 56 49 54 45[.-INVITE

0030 20 73 69 70 3a 39 34 34 30 32 31 33 37 31 40 73 sip:944 021371@s

0040 69 70 33 2e 69 70 76 36 2e 63 6c 75 62 2e 74 77 ip3.ipv6.club.tw

Filter: sip

Expression Clear Apply

File: (Untitled) 73 KB P: 253 D: 24 M: 0



Solving NAT Traversal Problems

- Targets
 - Discover mapped **public IP & port** for private IP & port
 - Use mapped public IP & port in application layer message
 - Keep this mapping valid
- Timing Issue
 - NAT will automatically allocate a public port for a private address & port if need.
 - NAT will release the mapping if the public port is “idle”
 - No TCP connection on the port
 - No UDP traffic on the port for a period (1 min~5 min)
 - Keep a TCP connection to target
 - Send UDP packet to target every specified interval



NAT Traversal Solutions

- Static Mapping
- VPN (Virtual Private Network)
- UPnP (Universal Plug-and-Play)
 - UPnP Forum - <http://www.upnp.org/>
- STUN (Simple Traversal of UDP Through Network Address Translators)
 - RFC 3489
 - Works except symmetric NAT
- Session Controller
 - B2BUA+RTP Proxy



交通大學

National Chiao Tung University

LAB 117
&
VoIP LAB

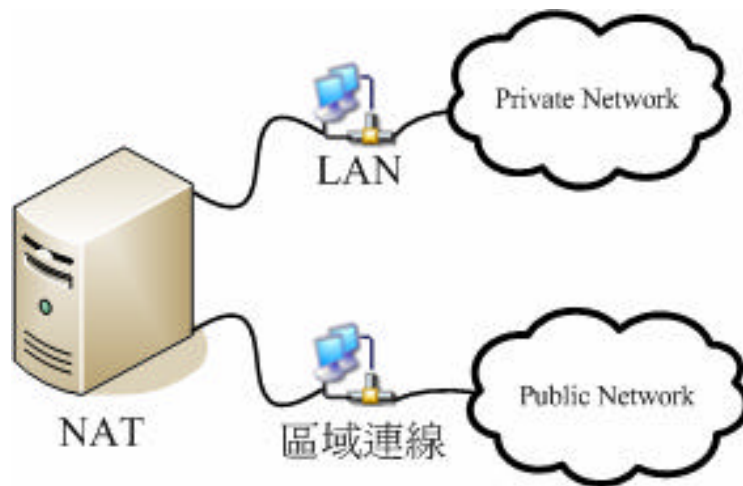


NAT Configuration- Using Windows XP with 2 NICs



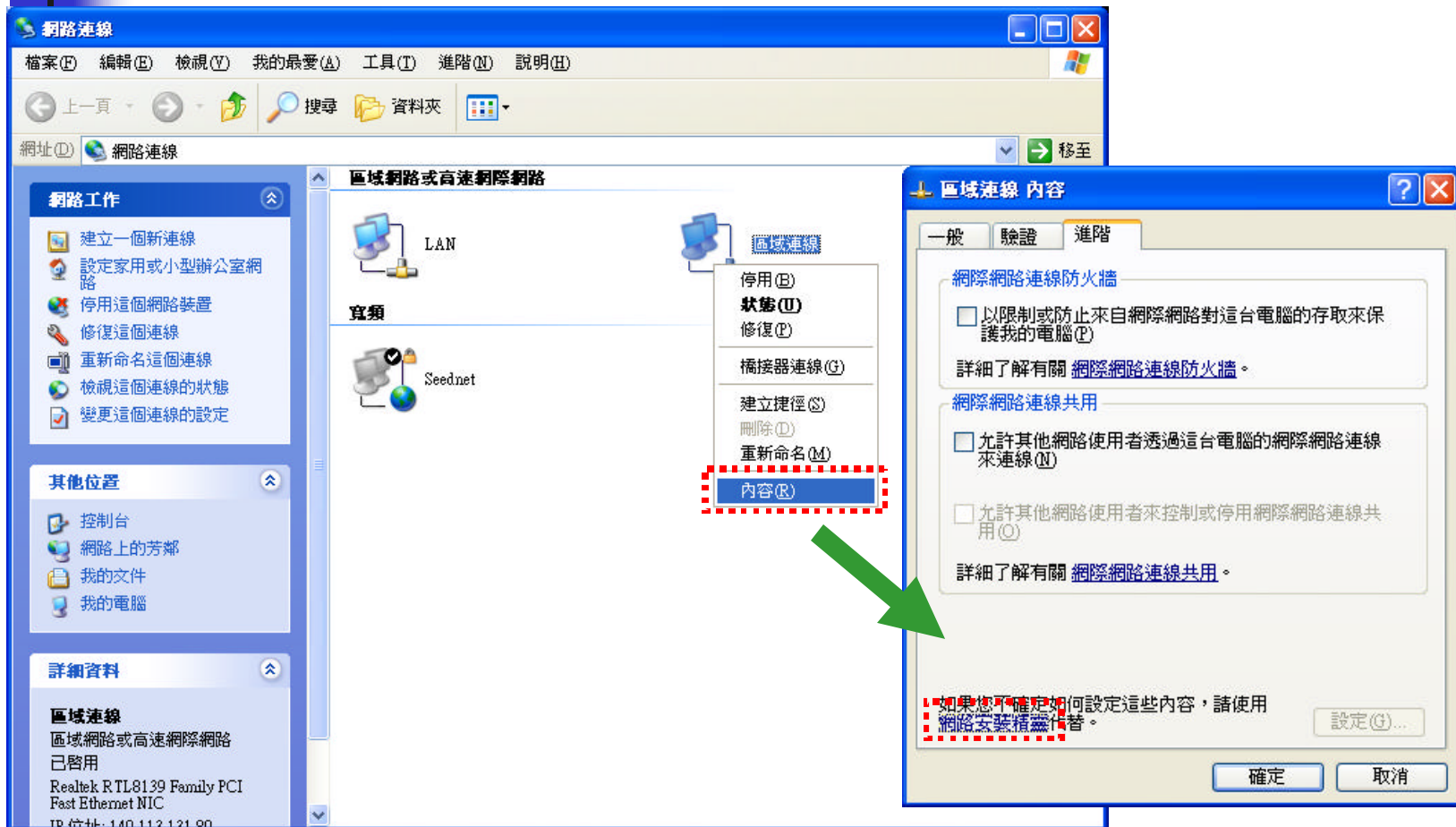
NAT of Windows XP with 2 NICs

- 使用Windows XP架設NAT需要兩張網卡
 - 區域連線
 - 區域連線2
- 將“區域連線”連接NAT內部網路；而“區域連線2”連接NAT外部網路





NAT of Windows XP Setup (1)





NAT of Windows XP Setup (2)

網路安裝精靈

歡迎使用網路安裝精靈

這個精靈將協助您設定這個電腦來執行於您的網路。網路讓您可以：

- 共用網際網路連線
- 設定網際網路連線防火牆
- 共用檔案和資料夾
- 共用印表機

請按 [下一步] 繼續。

網路安裝精靈

選擇連線方式。

選擇對這個電腦最適當的敘述：

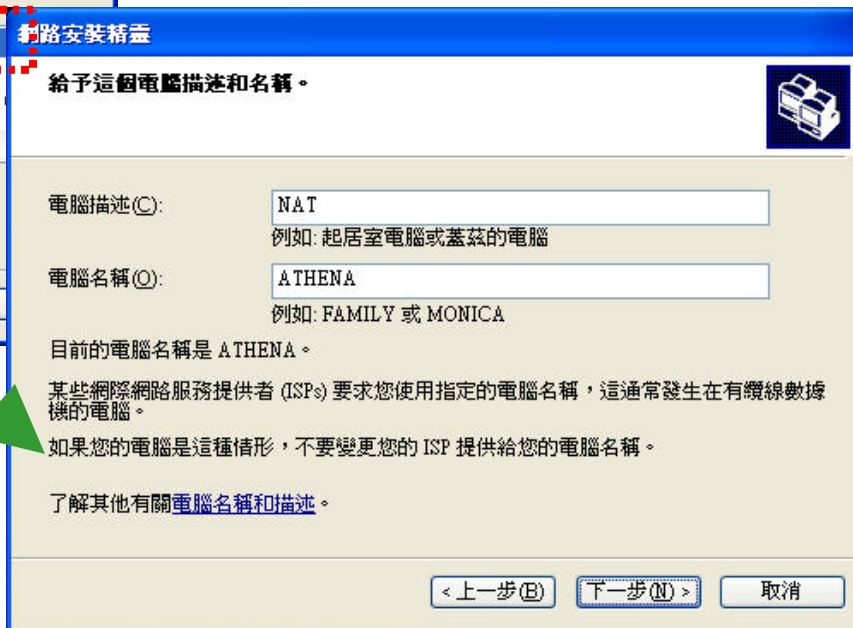
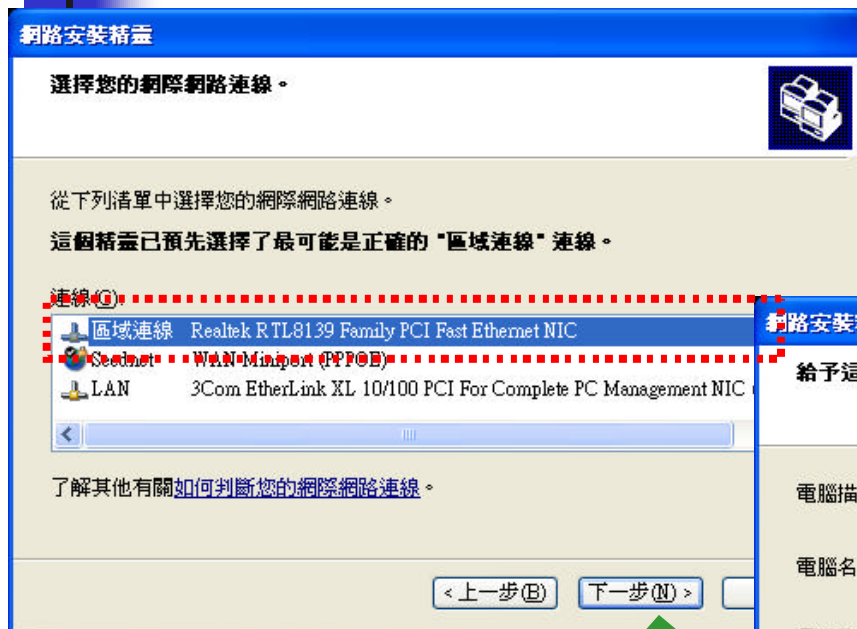
- ☒ 這個電腦直接連接到網際網路，其他在我的網路上的電腦經由這個電腦連接到網際網路 (C)
[檢視範例。](#)
- ☐ 這個電腦經由其他在我的家用網路上的電腦或經由住家閘道連接到網際網路 (M)
[檢視範例。](#)
- ☐ 其他 (O)

了解其他有關[家用或小型辦公室網路設定](#)。

< 上一步 (B) 下一步 (N) > 取消



NAT of Windows XP Setup (3)





NAT of Windows XP Setup (4)

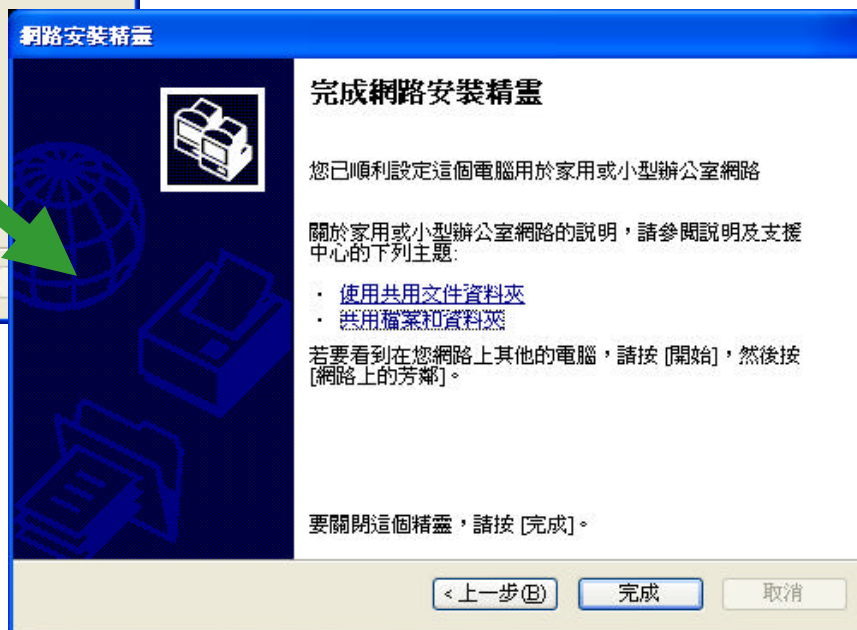
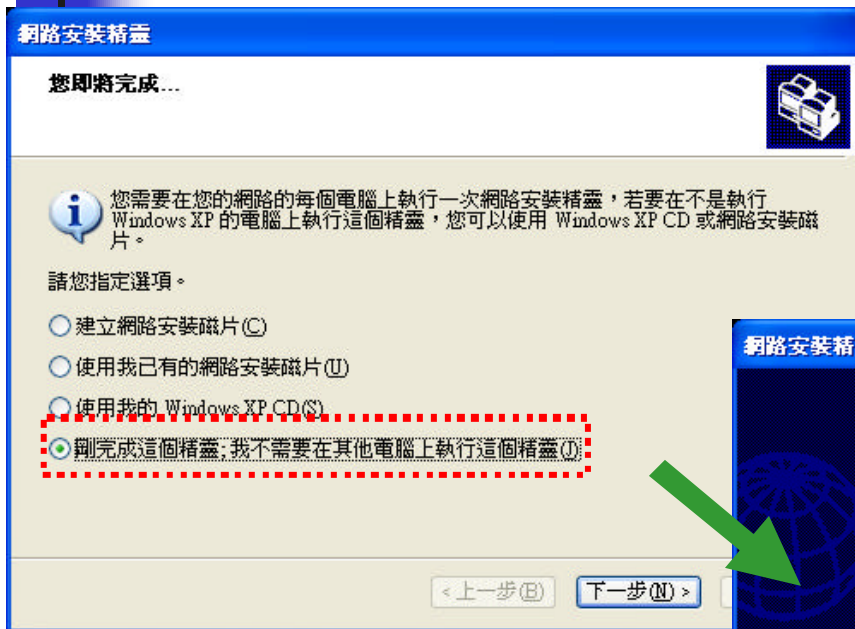
The screenshot displays the Windows XP Network Setup Wizard in Chinese. It consists of three overlapping windows:

- 命名您的網路 (Name your network):** The first window shows the 'Workgroup name (W):' field with 'MSHOME' entered. Below it, an example says '例如: 家用或辦公室'.
- 請稍候... (Please wait...):** The second window shows a progress bar and icons for a computer, a monitor, and a house. It states: '精靈正在為家用或小型辦公室網路設定這個電腦，請稍候。這個程序可能需要幾分鐘時間。' (The wizard is setting up this computer for a home or small office network. Please wait. This program may take a few minutes.)
- 準備套用網路設定... (Preparing to apply network settings...):** The third window shows a list of settings to be applied:
 - 網際網路連線設定: (Internet connection settings)
 - 網際網路連線: (Internet connection)
 - 網際網路連線共用: (Internet connection sharing)
 - 網際網路連線防火牆: (Internet connection firewall)
 - 網路設定: (Network settings)
 - 電腦描述: (Computer description)The '網路設定' (Network settings) section is expanded, showing 'NAT' selected. At the bottom, it says '若要套用這些設定值，請按 [下一步]。' (To apply these settings, press [Next]).

Green arrows indicate the flow from the first window to the third, and from the third window to the '下一步(N) >' button in the second window.



NAT of Windows XP Setup (5)





交通大學

National Chiao Tung University

LAB 117
&
VoIP LAB

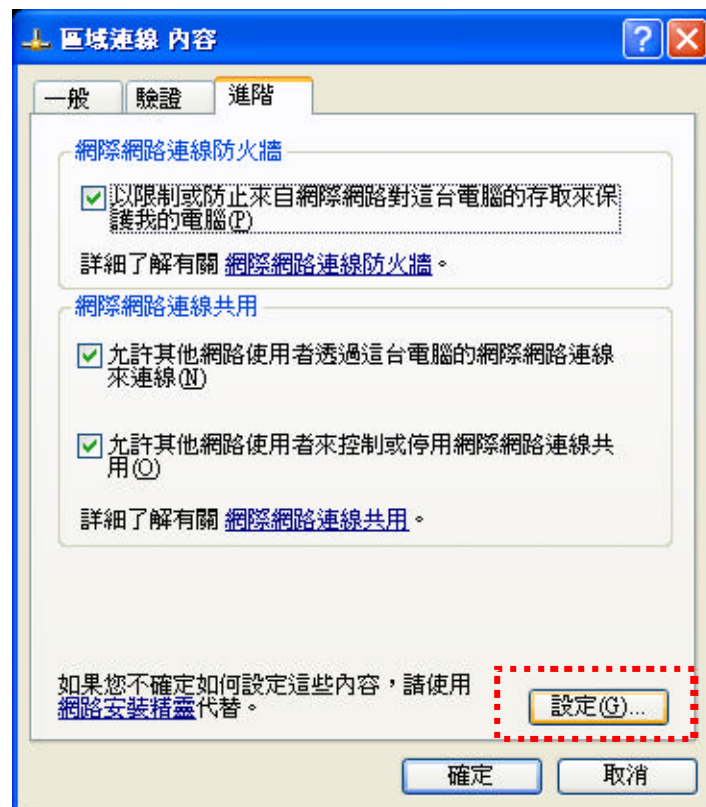


Static Mapping and Manual Configuration



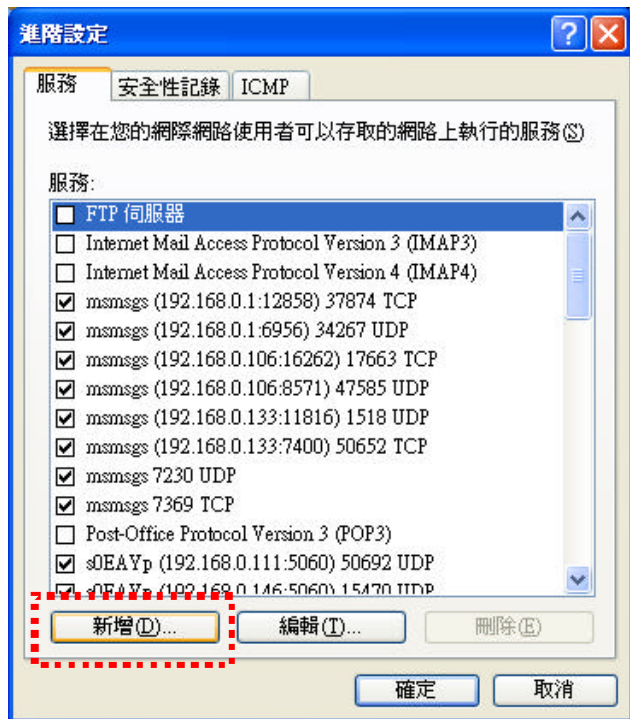
Windows XP NAT Setup (1)

- 開啟NAT對外的連線介面, 於firewall上設定將NAT內部的port指定到特定NAT對外連線介面的port

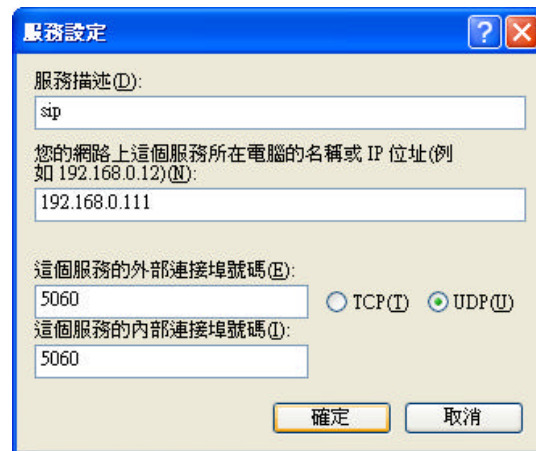
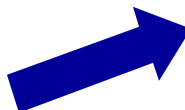




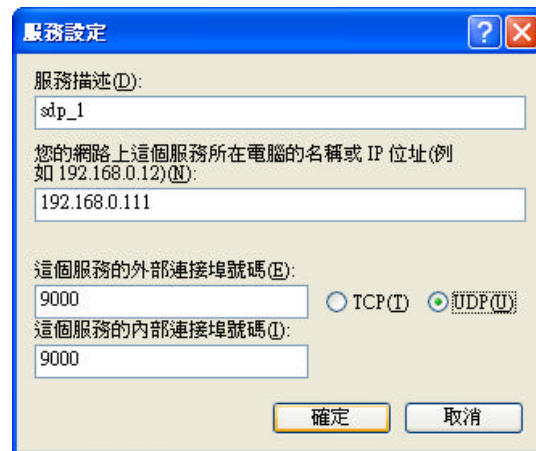
Windows XP NAT Setup (2)



For SIP



For RTP





SIP UA Setup for Static Mapping (1)

snom 200 VoIP Phone :: Home - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://192.168.0.111/index_en.htm 移至 連結 >>

snom

The SIP Experts

Phone Settings

- Redirection
- Base
- SIP
- H323
- Codecs
- Network
- Miscellaneous
- Key Mapping
- Updates

Home

Stack

Authentication

your phone!

On these pages you can work with your VoIP phone.

Outgoing line:

944021375@ Set

Dialed, Missed, Received

Dialed Numbers

Date	Number
7/8/2004 11:20AM	944021371

Missed Calls

Date	Number
------	--------

Received Calls

english





SIP UA Setup for Static Mapping (2)

snom 200 VoIP Phone :: Settings :: SIP :: Stack - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜索 我的最愛 媒體

網址(D) http://192.168.0.111/set_sip_stack_en.htm 移至 連結 >>

Settings

Stack

Here you may specify the behavior of the SIP stack. If you are behind NAT, you may statically assign a network identity and the RTP ports here. Please contact your operator for details.

Register Postfix

Outbound Proxy:
Registrar is outbound proxy ☒ Yes ☐ Use Path
Path

Treat as initial route ☐ Route ☒ Address

NAT:
NAT detection Static

STUN server (IP-addr:port)

STUN binding interval (seconds)

Dynamic RTP port start

Dynamic RTP port end

Network identity (hostname)

Network identity (port)

Local SIP port ☐ Network port ☒ Default SIP port

SIP timers:
Retry T1 (ms)



REGISTER Message

(Untitled) - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

12	52.805868	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7
13	52.810160	140.113.131.7	192.168.0.111	SIP	Status: 200 OK (5 bindings)

Frame 12 (526 bytes on wire (526 bytes captured))

Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb

Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Request-Line: REGISTER sip:140.113.131.7 SIP/2.0

Message Header

Via: SIP/2.0/UDP 140.113.131.89:5060;branch=z9hG4bK-fzw1kc7rhauw:rport

From: "Ya-Lin" <sip:944021375@140.113.131.7>;tag=upq7h13pek

To: "Ya-Lin" <sip:944021375@140.113.131.7>

Call-ID: 3c267004af57-j3fdv4s39oz7@140-113-131-89

CSeq: 1 REGISTER

Max-Forwards: 70

Contact: <sip:944021375@140.113.131.89:5060;transport=udp;line=1hynyb3y;q=1.0;description="Available">

User-Agent: snom200-2.03c

Supported: gruu

Expires: 3600

Content-Length: 0

0000 00 04 75 e4 66 eb 00 04 11 10 11 28 08 00 45 00 ...U.T... (...E.

0010 02 00 00 00 40 00 40 11 68 5d c0 a8 00 6f 8c 71 ...0.0.0. h]...o.g

0020 83 07 13 c4 13 c4 01 ec c1 3d 52 45 47 49 53 54=REGIST

0030 45 52 20 73 69 70 3a 31 34 30 2e 31 31 33 2e 31 ER sip:140.113.1

0040 33 31 2e 37 20 53 49 50 2f 32 2e 30 0d 0a 56 69 31.7 SIP /2.0..Vi

Filter sip

Expression Clear Apply

File: (Untitled) 54 KB P: 314 D: 38 M: 0



INVITE Message (SIP)

(Untitled) - Ethernet

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
81	92.476762	192.168.0.111	140.113.131.7	SIP/SDP	Request: INVITE sip:944021371@140.113.131.7;user=phone
82	92.483497	140.113.131.7	192.168.0.111	SIP	Status: 100 trying -- your call is important to us

Frame 81 (1038 bytes on wire (1038 bytes captured))

- Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb
- Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
 - Request-Line: INVITE sip:944021371@140.113.131.7;user=phone SIP/2.0
 - Message Header
 - Via: SIP/2.0/UDP-140.113.131.89:5060;branch=z9hG4bK-woruoqtoarw
 - From: "Ya-Lin" <sip:944021375@140.113.131.7>;tag=22522c2hlr
 - To: <sip:944021371@140.113.131.7;user=phone>
 - Call-ID: 3c26702c5ba6-hegcoky1hezq@140-113-131-89
 - CSeq: 1 INVITE
 - Max-Forwards: 70
 - Contact: <sip:944021375@140.113.131.89:5060;transport=udp;line=1hnyb3yx>
 - User-Agent: snom200-2.03o
 - Accept-Language: en
 - Accept: application/sdp
 - Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
 - Supported: timer, 100rel, replaces
 - Session-Expires: 7200
 - Content-Type: application/sdp
 - Content-Length: 333
 - Message body

Filter: sip

Expression: Clear Apply

Frame (frame), 1038 B P: 314 D: 38 M: 0



INVITE Message (SDP)

Wireshark packet capture analysis of an INVITE message (SDP).

No.	Time	Source	Destination	Protocol	Info
81	92.476762	192.168.0.111	140.113.131.7	SIP/SOP	Request: INVITE sip:944021371@140.113.131.7;user=phone
82	92.483497	140.113.131.7	192.168.0.111	SIP	Status: 100 trying -- your call is important to us

Frame 81 (1038 bytes on wire, 1038 bytes captured)

- Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb
- Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
 - Request-Line: INVITE sip:944021371@140.113.131.7;user=phone SIP/2.0
 - Message Header
 - Message body
 - Session Description Protocol
 - Session Description Protocol Version (v): 0
 - Owner/Creator, Session Id (o): root 1389867269 1389867269 IN IP4 140.113.131.89
 - Session Name (s): call
 - Connection Information (c): IN IP4:140.113.131.89
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio:9000 RTP/AVP 18 3 0 8 101
 - Media Attribute (a): rtpmap:18 g729/8000
 - Media Attribute (a): rtpmap:3 gsm/8000
 - Media Attribute (a): rtpmap:0 pcmu/8000
 - Media Attribute (a): rtpmap:8 pcma/8000
 - Media Attribute (a): rtpmap:101 telephone-event/8000
 - Media Attribute (a): fmtp:101 0-15
 - Media Attribute (a): sendrecv
 - Media Attribute (a): srccdr:192.168.0.111:9000 140.113.131.89:9000

Hex dump and ASCII view of the SDP body:

```

0000  00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00  ..U.T... (...E.
0010  04 00 00 00 00 40 00 11 66 5d c0 a8 00 6f 8c 71  ...B.B. f]...o.g
0020  83 07 13 c4 13 c4 03 ec 53 42 49 4e 56 49 54 45  .... SBINVITE
0030  20 73 69 70 3a 39 34 34 30 32 31 33 37 31 40 31  sip:944 021371@1
0040  34 30 2e 31 31 33 2e 31 33 31 2e 37 3b 75 73 65  40.113.1 31.7;use
    
```

Filter: sip



交通大學

National Chiao Tung University

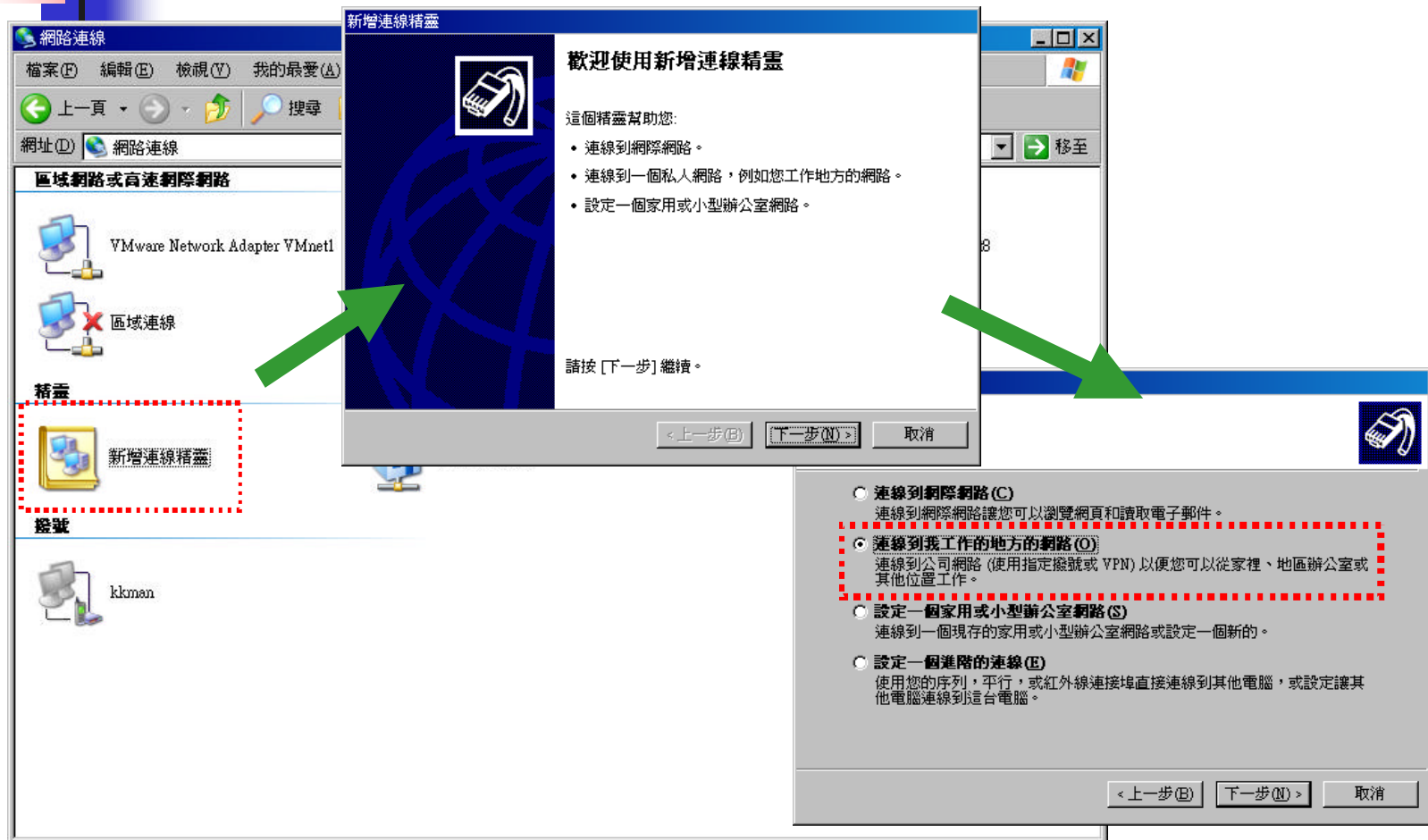
LAB 117
&
VoIP LAB



Virtual Private Network (VPN)

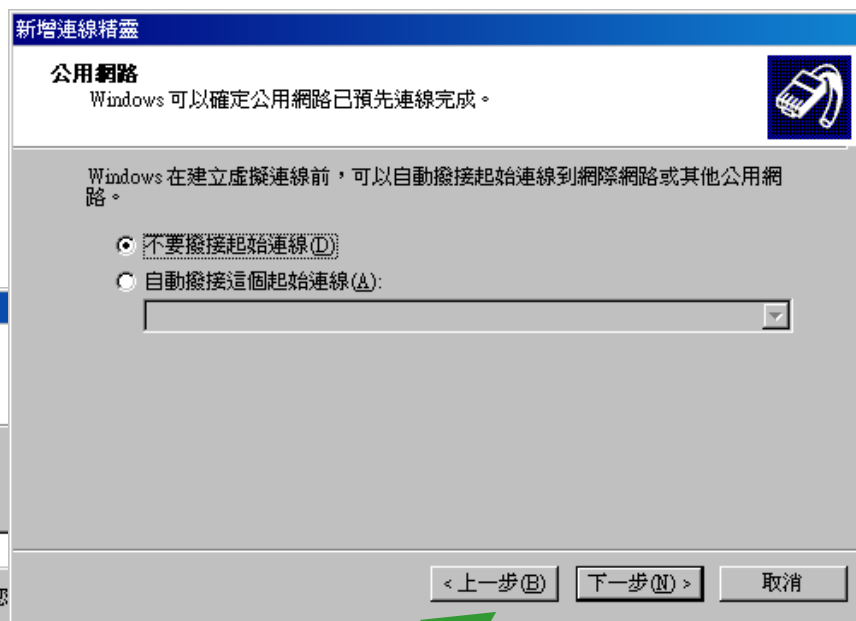
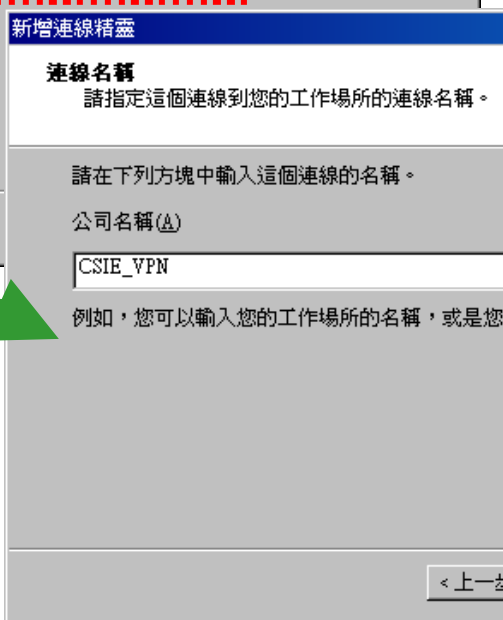
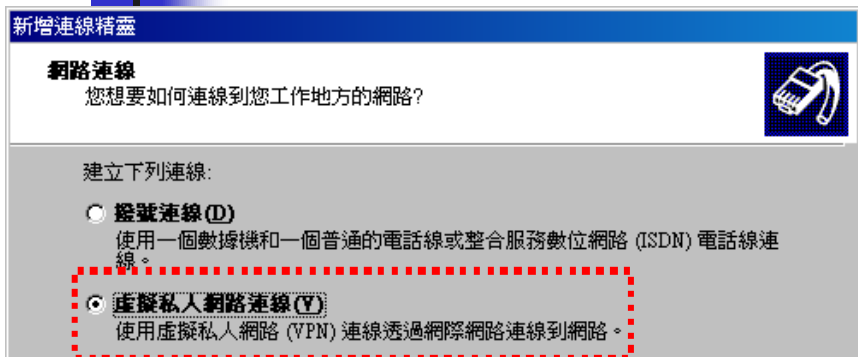


VPN Setup on Windows XP (1)





VPN Setup on Windows XP (2)





VPN Setup on Windows XP (3)

新增連線精靈

選取 VPN 伺服器

VPN 伺服器的名稱或位址為？

請輸入您正要連線的電腦主機名稱或 IP 位址。

主機名稱或 IP 位址 (例如 microsoft.com 或 157.54.0.1)(H):

vpn.csie.nctu.edu.tw

新增連線精靈

完成新增連線精靈

您已成功地完成了建立下列連線所需要的步驟：

CSIE VPN

- 跟這台電腦上所有的使用者共用

這個連線將儲存於 [網路連線] 資料夾中。

☐ 將這個連線的捷徑加到我的桌面上(S)

要建立這個連線和關閉這個精靈，請按 [完成]。

< 上一步(B) 完成 取消

連線到 CSIE_VPN

使用者名稱(U): huangyl

密碼(P): *****

☐ 儲存這個使用者名稱及密碼供下列使用者使用(S)

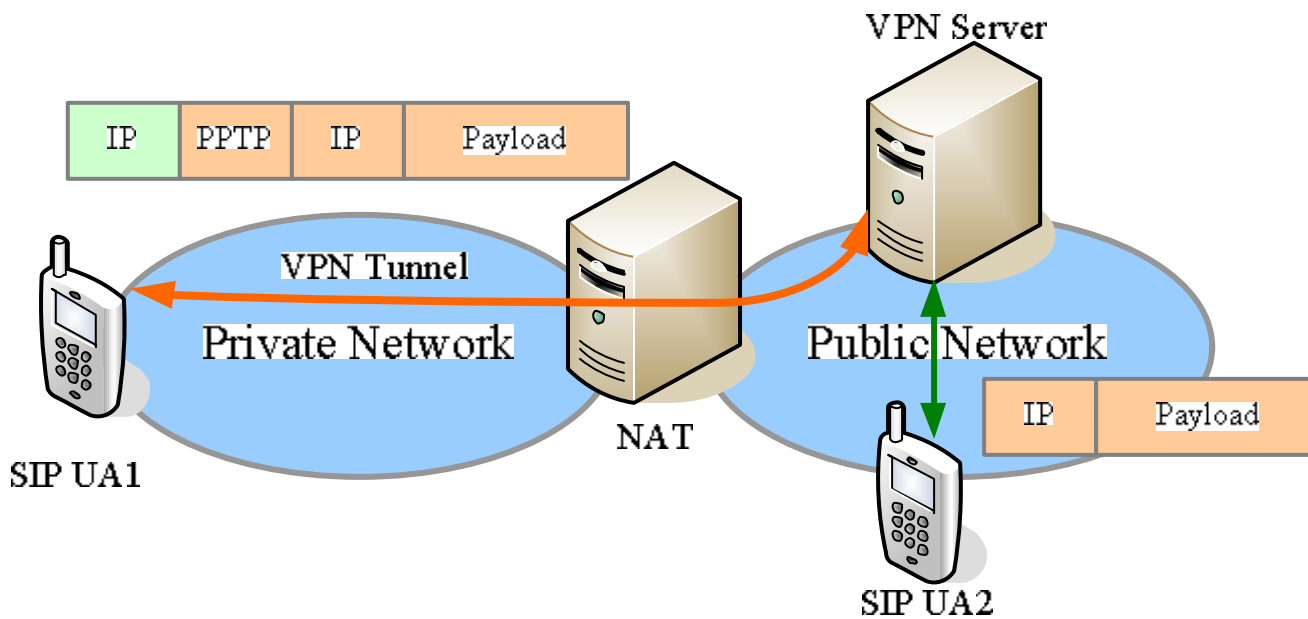
☒ 只有我自己(O)

☐ 所有使用這台電腦的使用者(A)

連線(C) 取消 內容(O) 說明(H)



VPN





Before Setup VPN Connection

Default Route

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.111	20
127.0.0.0	255.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.255.0	255.255.255.0	192.168.0.111	192.168.0.111	20
192.168.0.111	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.0.255	255.255.255.255	255.255.255.255	192.168.0.111	192.168.0.111	20
192.168.5.0	255.255.255.0	255.255.255.0	192.168.5.1	192.168.5.1	20
192.168.5.1	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.5.255	255.255.255.255	255.255.255.255	192.168.5.1	192.168.5.1	20
192.168.153.0	255.255.255.0	255.255.255.0	192.168.153.1	192.168.153.1	20
192.168.153.1	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.153.255	255.255.255.255	255.255.255.255	192.168.153.1	192.168.153.1	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.0.111	192.168.0.111	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.5.1	192.168.5.1	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.153.1	192.168.153.1	20
255.255.255.255	255.255.255.255	255.255.255.255	192.168.0.111	192.168.0.111	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.5.1	192.168.5.1	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.153.1	192.168.153.1	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.153.1	5	1

Default Gateway: 192.168.0.1

Persistent Routes:

None



After Setup VPN Connection

Default Route

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	140.113.235.164	140.113.235.164	1
0.0.0.0	0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.111	21
127.0.0.0	255.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
140.113.235.164	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	50
140.113.235.249	255.255.255.255	255.255.255.255	192.168.0.1	192.168.0.111	20
140.113.255.255	255.255.255.255	255.255.255.255	140.113.235.164	140.113.235.164	50
192.168.0.0	255.255.255.0	255.255.255.0	192.168.0.111	192.168.0.111	20
192.168.0.111	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.0.255	255.255.255.255	255.255.255.255	192.168.0.111	192.168.0.111	20
192.168.5.0	255.255.255.0	255.255.255.0	192.168.5.1	192.168.5.1	20
192.168.5.1	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.5.255	255.255.255.255	255.255.255.255	192.168.5.1	192.168.5.1	20
192.168.153.0	255.255.255.0	255.255.255.0	192.168.153.1	192.168.153.1	20
192.168.153.1	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.153.255	255.255.255.255	255.255.255.255	192.168.153.1	192.168.153.1	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.0.111	192.168.0.111	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.5.1	192.168.5.1	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.153.1	192.168.153.1	20
224.0.0.0	240.0.0.0	240.0.0.0	140.113.235.164	140.113.235.164	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.0.111	192.168.0.111	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.5.1	192.168.5.1	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.153.1	192.168.153.1	1
255.255.255.255	255.255.255.255	255.255.255.255	192.168.153.1	5	1

Default Gateway: 140.113.235.164

Persistent Routes:

None



交通大學

National Chiao Tung University

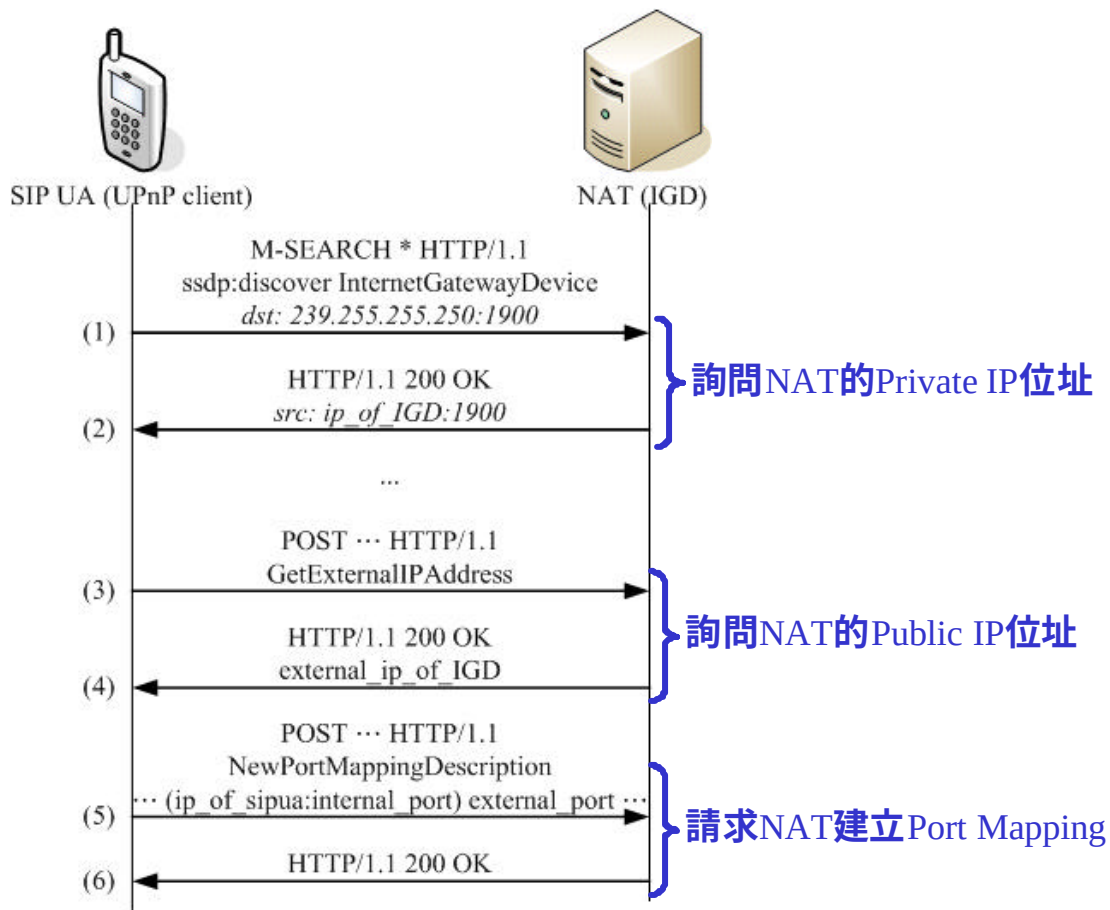
LAB 117
&
VoIP LAB



UPnP – Universal Plug-and-Play



UPnP 運作流程





SSDP Discover Message (1)

Wireshark packet capture analysis of an SSDP Discover message.

No.	Time	Source	Destination	Protocol	Info
41	58.377436	192.168.0.111	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
42	58.384919	192.168.0.111	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
43	58.391366	192.168.0.111	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
44	58.507460	192.67.198.4	192.168.0.111	TCP	http > 2049 [SYN, ACK] Seq=1293375672 Ack=2200752468 Win=584
45	58.508150	192.168.0.111	192.67.198.4	TCP	2049 > http [ACK] Seq=2200752468 Ack=1293375673 Win=584
46	58.511065	192.168.0.111	192.67.198.4	HTTP	GET /snom200/snom200-updates.xml HTTP/1.1
47	58.532094	192.168.0.1	192.168.0.111	SSDP	HTTP/1.1 200 OK
48	58.568111	192.168.0.1	192.168.0.111	TCP	2869 > 2056 [FIN, ACK] Seq=2869254471 Ack=2869254471 Win=0 Len=0
49	58.569855	192.168.0.111	192.168.0.1	TCP	2056 > 2869 [RST] Seq=2869254471 Ack=0 Win=0 Len=0
50	58.577719	192.168.0.111	192.168.0.1	TCP	2050 > 2869 [SYN] Seq=2200752468 Ack=0 Win=5840 Len=0

Frame 41 (179 bytes on wire, 179 bytes captured)

- Ethernet II, Src: 00:04:13:10:11:28, Dst: 01:00:5e:7f:ff:fa
- Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 239.255.255.250 (239.255.255.250)
- User Datagram Protocol, Src Port: 1901 (1901), Dst Port: 1900 (1900)
- Hypertext Transfer Protocol
 - M-SEARCH * HTTP/1.1\r\n
 - Request Method: M-SEARCH
 - Host: 239.255.255.250:1900\r\n
 - ST: urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
 - MAN: "ssdp:discover"\r\n
 - MX: 3\r\n
 - \r\n

Hex dump and ASCII view:

```

0000  01 00 5e 7f ff fa 00 04 13 10 11 28 08 00 45 00  ..A.....E.
0010  00 a5 00 00 40 00 01 11 c8 36 c0 a8 00 6f ef ff  ...Q...6...o.
0020  ff fa 07 6d 07 6c 00 91 6c e3 4d 2d 53 45 41 52  ...n.l...1,M-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1.H
0040  6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  ost: 239.255.255
    
```



SSDP Discover Message (2)

Wireshark packet capture window titled "upnp_ethereal - Ethernet". The packet list shows several SSDP M-SEARCH messages and one HTTP GET message. The selected packet (47) is an HTTP 200 OK response from 192.168.0.1 to 192.168.0.111.

No.	Time	Source	Destination	Protocol	Info
41	58.377436	192.168.0.111	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
42	58.384919	192.168.0.111	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
43	58.391366	192.168.0.111	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
44	58.507460	192.67.198.4	192.168.0.111	TCP	http > 2049 [SYN, ACK] Seq=1293375672 Ack=2200752468 Win=584
45	58.508150	192.168.0.111	192.67.198.4	TCP	2049 > http [ACK] Seq=2200752468 Ack=1293375673 Win=584
46	58.511065	192.168.0.111	192.67.198.4	HTTP	GET /snow200/snow200-updates.xml HTTP/1.1
47	58.532094	192.168.0.1	192.168.0.111	SSDP	HTTP/1.1 200 OK
48	58.568111	192.168.0.1	192.168.0.111	TCP	2869 > 2056 [FIN, ACK] Seq=2956581336 Ack=2869254471 Win=0
49	58.569855	192.168.0.111	192.168.0.1	TCP	2056 > 2869 [RST] Seq=2869254471 Ack=0 Win=0 Len=0
50	58.572219	192.168.0.111	192.168.0.1	TCP	2050 > 2869 [SYN] Seq=2206752664 Ack=0 Win=5840 Len=0

Frame 47 (420 bytes on wire, 420 bytes captured)

- Ethernet II, Src: 00:04:75:e4:66:eb, Dst: 00:04:13:10:11:28
- Internet Protocol, Src Addr: 192.168.0.1 (192.168.0.1), Dst Addr: 192.168.0.111 (192.168.0.111)
- User Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1901 (1901)
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Response Code: 200
 - ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
 - USN:uuid:4a913003-f0f4-4e5c-adfd-178a3e6e72d8::urn:schemas-upnp-org:device:InternetGatewayDevice:1\r\n
 - Location:http://192.168.0.1:2869/upnp/udhisapi.dll?content=uuid:4a913003-f0f4-4e5c-adfd-178a3e6e72d8\r\n
 - Cache-Control:max-age=1800\r\n
 - Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0\r\n
 - Ext:\r\n
 - \r\n

Packet bytes on wire (0x0000-0x0040): 00 04 13 10 11 28 00 04 75 e4 66 eb 08 00 45 00C...u.f...E.
 0010 01 96 6c 44 00 00 01 11 ca 52 c0 a8 00 01 c0 a8 ...D....R.....
 0020 00 6f 07 6c 07 6d 01 82 b5 79 48 54 54 50 2f 31 ...o.l.m...yHTTP/1
 0030 2e 31 20 32 30 30 20 4f 4b 0d 0a 53 54 3a 75 72 ...l 200 O K..ST:ur
 0040 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f n:schema s-upnp-o

Filter: Expression: Clear Apply File: upnp_ethereal 1 P: 580 D: 580 M: 0



IGD Control Message (1)

```
POST /upnphost/udhisapi.dll?control=uuid:323c1e53-7be5-438a-9004-e3b4189e45d5+urn:upnp-org:serviceId:WANIPConn1 HTTP/1.1
Host: 192.168.0.1:2869
Content-Length: 336
Content-Type: text/xml; charset="utf-8"
SOAPAction: "urn:schemas-upnp-org:service:WANIPConnection:1#GetExternalIPAddress"
```

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <u:GetExternalIPAddress xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
      </u:GetExternalIPAddress>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

```
HTTP/1.0 200 OK
Date: Wed, 07 Jul 2004 08:15:39 GMT
Connection: close
Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
Content-Length: 464
Content-Type: text/xml; charset="utf-8"
EXT:
```

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-
  ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><m:GetExternalIPAddressResponse
  xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1"><NewExternalIPAddress xmlns:dt="urn:schemas-microsoft-
  com:datatypes" dt:dt="string">140.113.131.89</NewExternalIPAddress></m:GetExternalIPAddressResponse></SOAP-
  ENV:Body></SOAP-ENV:Envelope>
```



IGD Control Message (2)

```
POST /upnphost/udhisapi.dll?control=uuid:323c1e53-7be5-438a-9004-e3b4189e45d5+urn:upnp-org:serviceId:WANIPConn1 HTTP/1.1
```

```
Host: 192.168.0.1:2869
```

```
Content-Length: 732
```

```
Content-Type: text/xml; charset="utf-8"
```

```
SOAPAction: "urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"
```

```
<SOAP-ENV:Envelope
```

```
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
```

```
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
```

```
<SOAP-ENV:Body>
```

```
<u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
```

```
<NewRemoteHost></NewRemoteHost>
```

```
<NewExternalPort>53404</NewExternalPort>
```

```
<NewProtocol>UDP</NewProtocol>
```

```
<NewInternalPort>5060</NewInternalPort>
```

```
<NewInternalClient>192.168.0.111</NewInternalClient>
```

```
<NewEnabled>1</NewEnabled>
```

```
<NewPortMappingDescription>s0EBEo (192.168.0.111:5060) 53404 UDP</NewPortMappingDescription>
```

```
<NewLeaseDuration>0</NewLeaseDuration>
```

```
</u:AddPortMapping>
```

```
</SOAP-ENV:Body>
```

```
</SOAP-ENV:Envelope>
```

```
HTTP/1.0 200 OK
```

```
Date: Wed, 07 Jul 2004 08:15:39 GMT
```

```
Connection: close
```

```
Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
```

```
Content-Length: 305
```

```
Content-Type: text/xml; charset="utf-8"
```

```
EXT:
```

```
<?xml version="1.0"?>
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-
```

```
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><m:AddPortMappingResponse xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1"/></SOAP-ENV:Body></SOAP-ENV:Envelope>
```



IGD Control Message (3)

```
POST /upnphost/udhisapi.dll?control=uuid:323c1e53-7be5-438a-9004-e3b4189e45d5+urn:upnp-org:serviceId:WANIPConn1 HTTP/1.1
```

```
Host: 192.168.0.1:2869
```

```
Content-Length: 734
```

```
Content-Type: text/xml; charset="utf-8"
```

```
SOAPAction: "urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"
```

```
<SOAP-ENV:Envelope
```

```
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
```

```
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
```

```
<SOAP-ENV:Body>
```

```
<u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
```

```
<NewRemoteHost></NewRemoteHost>
```

```
<NewExternalPort>13016</NewExternalPort>
```

```
<NewProtocol>UDP</NewProtocol>
```

```
<NewInternalPort>10002</NewInternalPort>
```

```
<NewInternalClient>192.168.0.111</NewInternalClient>
```

```
<NewEnabled>1</NewEnabled>
```

```
<NewPortMappingDescription>s3EBEo (192.168.0.111:10002) 13016 UDP</NewPortMappingDescription>
```

```
<NewLeaseDuration>0</NewLeaseDuration>
```

```
</u:AddPortMapping>
```

```
</SOAP-ENV:Body>
```

```
</SOAP-ENV:Envelope>
```

```
HTTP/1.0 200 OK
```

```
Date: Wed, 07 Jul 2004 08:15:40 GMT
```

```
Connection: close
```

```
Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
```

```
Content-Length: 305
```

```
Content-Type: text/xml; charset="utf-8"
```

```
EXT:
```

```
<?xml version="1.0"?>
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-
```

```
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><m:AddPortMappingResponse xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1"/></SOAP-ENV:Body></SOAP-ENV:Envelope>
```




Current Defects of UPnP

- 目前尚未解決的問題
 - Aging 問題
 - 程式需自行清除 port mapping
 - 安全性問題
 - UPnP 尚未提供認證機制
 - Multi-level NAT
 - NAT 內的裝置只能存取前一層的 IP 位址



REGISTER Message

Wireshark packet capture of a SIP REGISTER message. The packet list shows a SIP Request (REGISTER) from 192.168.0.111 to 140.113.131.7. The packet details show the SIP message structure, including the Request-Line, Message Header, and various fields like Via, From, To, Call-ID, CSeq, Max-Forwards, Contact, User-Agent, Supported, Expires, and Content-Length. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
133	60.745276	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7
134	60.749142	140.113.131.7	192.168.0.111	SIP	Status: 200 OK (3 bindings)

Frame 133 (518 bytes on wire, 518 bytes captured)

- Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb
- Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
 - Request-Line: REGISTER sip:140.113.131.7 SIP/2.0
 - Method: REGISTER
 - Message Header
 - Via: SIP/2.0/UDP;140.113.131.89:53404;branch=z9hG4bK-lhezqiih2eoi
 - From: "Ya-Lin" <sip:944021375@140.113.131.7>;tag=m58p6kg08q
 - To: "Ya-Lin" <sip:944021375@140.113.131.7>
 - Call-ID: 3c267004a41e-j3fdv4sj9oz7@192-168-0-111
 - CSeq: 2 REGISTER
 - Max-Forwards: 70
 - Contact: <sip:944021375@140.113.131.89:53404>;transport=udp;line=1hvmv3vy;q=1.0;description="Available"
 - User-Agent: snom200-2.03o
 - Supported: gruu
 - Expires: 0
 - Content-Length: 0

Filter: sip



INVITE Message (SIP)

(Untitled) - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

210	112.322195	192.168.0.111	140.113.131.7	SIP/SIP	Request: INVITE sip:944021371@140.113.131.7;user=phone.
211	112.328949	140.113.131.7	192.168.0.111	SIP	Status: 100 trying -- your call is important to us

Frame 210 (1043 bytes on wire, 1043 bytes captured)

Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb

Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Request-Line: INVITE sip:944021371@140.113.131.7;user=phone SIP/2.0

Message Header

Via: SIP/2.0/UDP 140.113.131.89:53404;branch=z9hG4bK-n9izn36589ev

From: "Ya-Lin" <sip:944021375@140.113.131.7>;tag=3nmkgitfIk

To: <sip:944021371@140.113.131.7;user=phone>

Call-ID: 3c26703bd3de-jppsssnjjdg7@140-113-131-89

CSeq: 1 INVITE

Max-Forwards: 70

Contact: <sip:944021375@140.113.131.89:53404;transport=udp;line=1hymh3>

User-Agent: snom200-2.03o

Accept-Language: en

Accept: application/sdp

Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO

Supported: timer, 100rel, replaces

Session-Expires: 7200

Content-Type: application/sdp

Content-Length: 336

Message body

```

0000 00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00  ...u.f... (...E.
0010 04 05 00 00 40 00 40 11 66 58 c0 a8 00 6f 8c 71  ...0.0. +X...o.g
0020 83 07 13 c4 13 c4 03 f1 8d 07 49 4e 56 49 54 45  .... INVITE
0030 20 73 69 70 3a 39 34 34 30 32 31 33 37 31 40 31  sip:944 021371@1
0040 34 30 2e 31 31 33 2e 31 33 31 2e 37 3b 75 73 65  40.113.1 31.7;use
  
```

Filter sip

Expression...

Clear

Apply

File: (Untitled) 112 KB P: 580 D: 68 M: 0



INVITE Message (SDP)

(Untitled) - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

210	112.322195	192.168.0.111	140.113.131.7	SIP/SOF	Request: INVITE sip:944021371@140.113.131.7;user=phone.
211	112.328949	140.113.131.7	192.168.0.111	SIP	Status: 100 trying -- your call is important to us

Frame 210 (1043 bytes on wire (8344 bytes captured) on interface 0)

Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb

Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Request-Line: INVITE sip:944021371@140.113.131.7;user=phone SIP/2.0

Message Header

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): root:1605539862 1605539862 IN IP4:140.113.131.89

Session Name (s): call

Connection Information (c): IN IP4 140.113.131.89

Time Description, active time (t): 0 0

Media Description, name and address (m): audio/13016 RTP/AVP 18 3 0 8 101

Media Attribute (a): rtpmap:18 g729/8000

Media Attribute (a): rtpmap:3 gsm/8000

Media Attribute (a): rtpmap:0 pcma/8000

Media Attribute (a): rtpmap:8 pcma/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): fmtp:101 0-15

Media Attribute (a): sendrecv

Media Attribute (a): srccidr:192.168.0.111:10002 140.113.131.89:13016

0000 00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00 ...u.f... (...E.

0010 04 05 00 00 40 00 40 11 66 58 c0 a8 00 6f 8c 71 ...0.0. fx...o.g

0020 83 07 13 c4 13 c4 03 f1 8d 07 49 4e 56 49 54 45 INVITE

0030 20 73 69 70 3a 39 34 34 30 32 31 33 37 31 40 31 sip:944 021371@1

0040 34 30 2e 31 31 33 2e 31 33 31 2e 37 3b 75 73 65 40.113.1 31.7;use

Filter: sip

Expression: Clear Apply

File: (Untitled) 112 KB P: 580 D: 68 M: 0

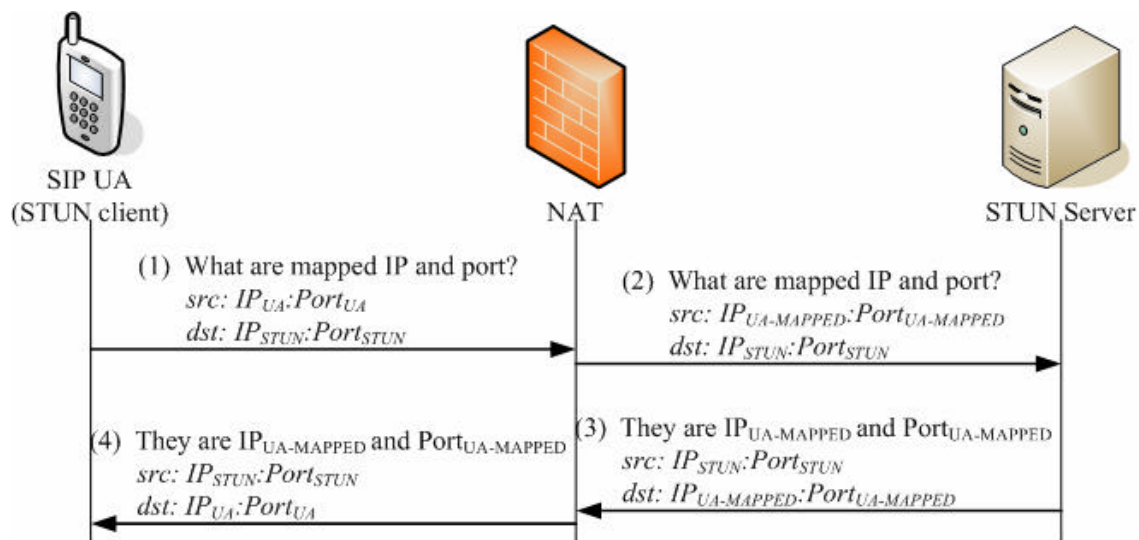


Simple Traversal of UDP through NAT (STUN)



STUN (RFC 3489)

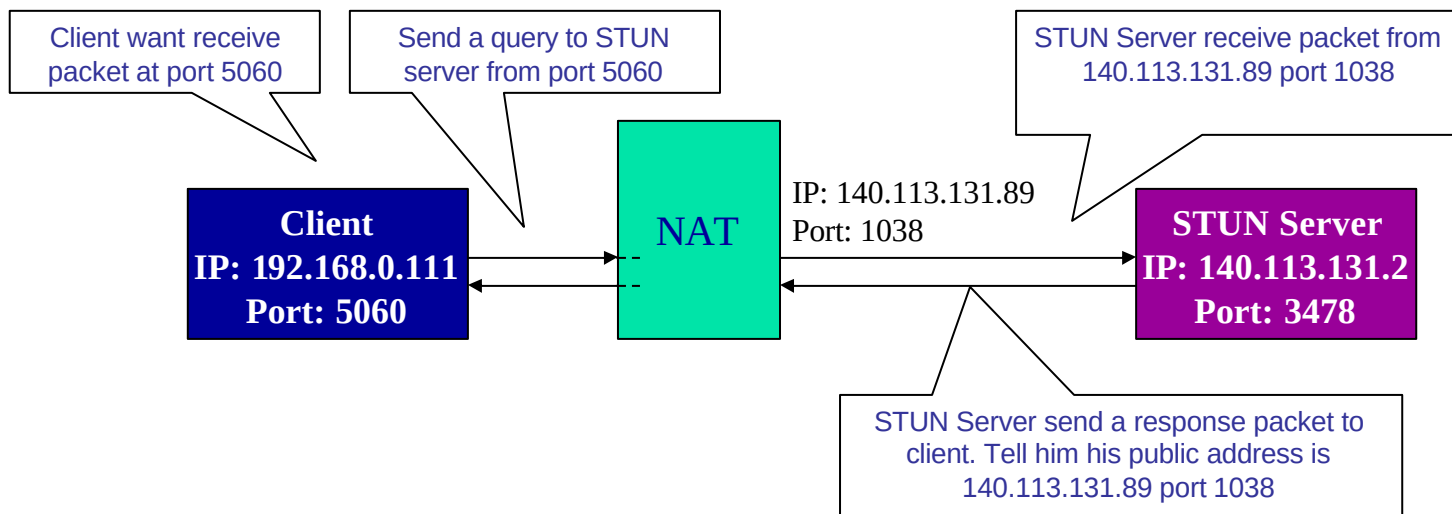
- A mechanism for a socket behind NAT(s) to get its mapped (IP,port) on Internet.
- Check whether UA is behind NAT.
 - If not true, the STUN mechanism is not applied.
- When new socket is created, use this socket to request its mapped (IP,port) from STUN server.
 - The response IP is stored in a string buffer.
 - The response port is saved in a table, using source port as key.
- When UA wants to stuff local IP or port in a message, it will first look up mapped IP or port in the table.





STUN Server

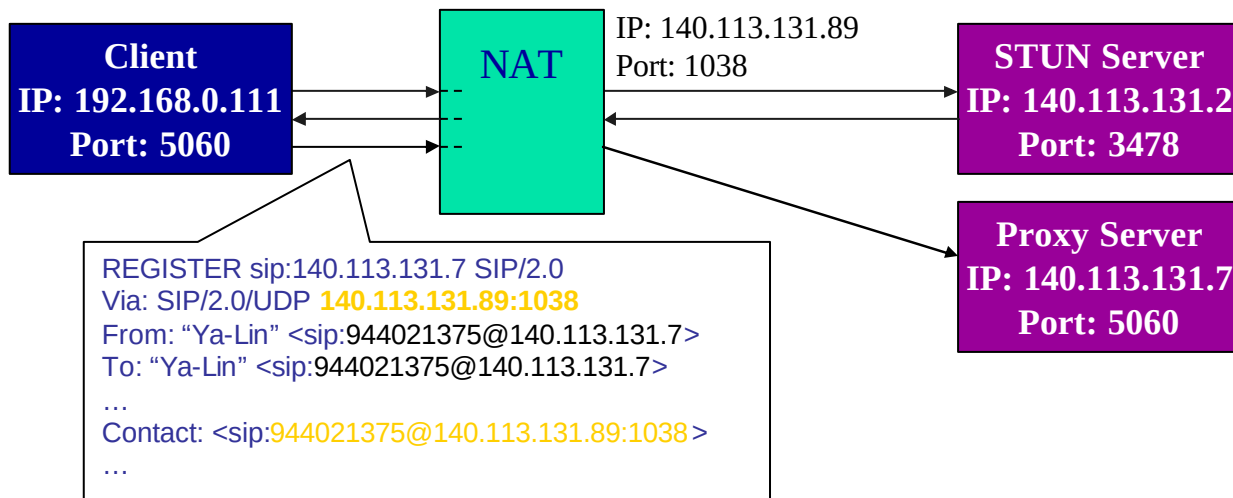
- Allow clients to discover if it is behind a NAT, what type of NAT it is, and the public address & port NAT will use.
- Very Simple Protocol, Easy to implement, Little load





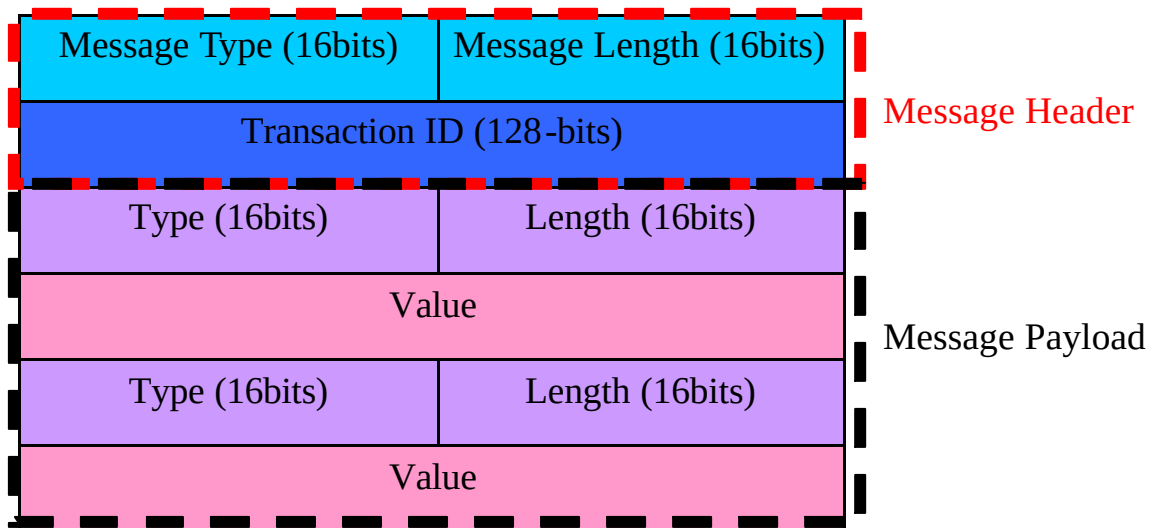
Use STUN for SIP Registration

- Use port 5060 to send a packet to STUN Server
- Receive public address & port mapped to client:5060 from STUN Server
- Fill the SIP register message with client's public address & port, send to proxy server





STUN訊息格式





STUN Message (Register)

stun_ethereal - Ethereal

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
25	1.858133	192.168.0.111	140.113.131.2	STUN	Message : Binding Request
26	1.858800	140.113.131.2	192.168.0.111	STUN	Message : Binding Response

▶ Frame 26 (98 bytes on wire, 98 bytes captured)

- ▶ Ethernet II, Src: 00:04:75:e4:66:eb, Dst: 00:04:13:10:11:28
- ▶ Internet Protocol, Src Addr: 140.113.131.2 (140.113.131.2), Dst Addr: 192.168.0.111 (192.168.0.111)
- ▶ User Datagram Protocol, Src Port: 3478 (3478), Dst Port: 5060 (5060)
- ▼ Simple Traversal of LDP Through NAT
 - Message Type: Binding Response (0x0101)
 - Message Length: 0x0024
 - Message Transaction ID: 0EC4821D74F8418621F53D8DDC8D87F0
 - ▼ Attributes
 - Attribute Type: MAPPED-ADDRESS (0x0001)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 1038
 - IP: 140.113.131.89 (140.113.131.89)
 - Attribute Type: SOURCE-ADDRESS (0x0004)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 3478
 - IP: 140.113.131.2 (140.113.131.2)
 - Attribute Type: CHANGED-ADDRESS (0x0005)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 3479

0000 00 04 13 10 11 28 00 04 75 e4 66 eb 08 00 45 00u.f...E.
 0010 00 54 00 00 40 00 3f 11 6b 0e 8c 71 83 02 c0 a8 .T..G..f..k..q...
 0020 00 6f 0d 96 13 c4 00 40 b2 be 01 01 00 24 0a c4 .o.....G.....\$.
 0030 82 1d 74 f8 41 86 21 f5 3d bd dc 8d 87 f0 00 01 ..t.A.!..=.....
 0040 00 08 00 01 04 0e 8c 71 83 59 00 04 00 08 00 01q..Y.....

Filter: stun Expression: Clear Apply File: stun_ethereal9 P: 412 D: 30 M: 0



Correct SIP REGISTER Message

stun_ethereal - Ethereal

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
35	1.975435	192.168.0.111	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7
36	1.979433	140.113.131.7	192.168.0.111	SIP	Status: 200 OK (3 bindings)

Frame 35 (526 bytes on wire (526 bytes captured))

- Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb
- Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
 - Request-Line: REGISTER sip:140.113.131.7 SIP/2.0
 - Method: REGISTER
 - Message Header
 - Via: SIP/2.0/UDP;140.113.131.89:1038;branch=z9hG4bK-kh12in066asp;rport
 - From: "Ya-Lin" <sip:944021375@140.113.131.7>;tag=6jsmzgdd5v
 - To: "Ya-Lin" <sip:944021375@140.113.131.7>
 - Call-ID: 3c2670064aaf-91zworugrttg@140-113-131-89
 - CSeq: 1 REGISTER
 - Max-Forwards: 70
 - Contact: <sip:944021375@140.113.131.89:1038;transport=udp;line=1hvmvb3>;q=1.0;description="Available"
 - User-Agent: snom200-2.03a
 - Supported: gruu
 - Expires: 3600
 - Content-Length: 0

0000 00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00 ...u.f... (...E.
 0010 02 00 00 00 40 00 40 11 68 5d c0 a8 00 6f 8c 71 ...0.0. h]...o.g
 0020 83 07 13 c4 13 c4 01 ec 1e ad 52 45 47 49 53 54REGIST
 0030 45 52 20 73 69 70 3a 31 34 30 2e 31 31 33 2e 31 ER sip:1 40.113.1
 0040 33 31 2e 37 20 53 49 50 2f 32 2e 30 0d 0a 56 69 31.7 SIP /2.0..V

Filter: sip

Expression: Clear Apply

File: stun_ethereal9 P: 412 D: 83 M: 0



STUN Message (SIP Port)

stun_ethereal - Ethereal

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
139	63.958744	192.168.0.111	140.113.131.2	STUN	Message : Binding Request
140	63.959429	140.113.131.2	192.168.0.111	STUN	Message : Binding Response

Frame 140 (98 bytes on wire, 98 bytes captured)

- Ethernet II, Src: 00:04:75:e4:66:eb, Dst: 00:04:13:10:11:28
- Internet Protocol, Src Addr: 140.113.131.2 (140.113.131.2), Dst Addr: 192.168.0.111 (192.168.0.111)
- User Datagram Protocol, Src Port: 3478 (3478), Dst Port: 5060 (5060)
- Simple Traversal of UDP Through NAT
 - Message Type: Binding Response (0x0101)
 - Message Length: 0x0024
 - Message Transaction ID: 1A83281A21731897014307090D3DD841
 - Attributes
 - Attribute Type: MAPPED-ADDRESS (0x0001)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 1038
 - IP: 140.113.131.89 (140.113.131.89)
 - Attribute Type: SOURCE-ADDRESS (0x0004)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 3478
 - IP: 140.113.131.2 (140.113.131.2)
 - Attribute Type: CHANGED-ADDRESS (0x0005)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 3479

0000 00 04 13 10 11 28 00 04 75 e4 66 eb 08 00 45 00(..u.f...E.
 0010 00 54 00 00 40 00 3f 11 6b 0e 8c 71 83 02 c0 a8 .T..G..f..k..q...
 0020 00 6f 0d 96 13 c4 00 40 4d dd 01 01 00 24 1a 83 .o.....G M....S..
 0030 2b 1a 21 73 1b 97 01 43 07 09 0d 3d d8 41 00 01 +.!.S...C...=.A..
 0040 00 08 00 01 04 0e 8c 71 83 59 00 04 00 08 00 01Y.....

Filter: stun Expression: Clear Apply File: stun_ethereal97 P: 412 D: 30 M: 0



Correct INVITE Message (SIP)

stun_ethereal - Ethereal

File Edit View Capture Analyze Statistics Help

148 77.544782 192.168.0.111 140.113.131.7 SIP/SOP Request: INVITE sip:944021375@140.113.131.7;user=phone
149 77.541565 140.113.131.7 192.168.0.111 SIP Status: 100 trying -- your call is important to us

▶ Frame 148 (1039 bytes on wire, 1039 bytes captured)
▶ Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb
▶ Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)
▶ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
▼ Session Initiation Protocol
▶ Request-Line: INVITE sip:944021375@140.113.131.7;user=phone SIP/2.0
▼ Message Header
Via: SIP/2.0/UDP 140.113.131.89:1038;branch=z9hG4bK-pjq57vxe4zew
▶ From: "Ya-Lin" <sip:944021375@140.113.131.7>;tag=tnaltoeryw
▶ To: <sip:944021375@140.113.131.7;user=phone>
Call-ID: 3c267051cf45-igsuj186h6fg@140-113-131-89
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:944021375@140.113.131.89:1038;transport=udp;line=thynyb3y>
User-Agent: snom200-2.03o
Accept-Language: en
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO
Supported: timer, 100rel, replaces
Session-Expires: 7200
Content-Type: application/sdp
Content-Length: 334
▶ Message body

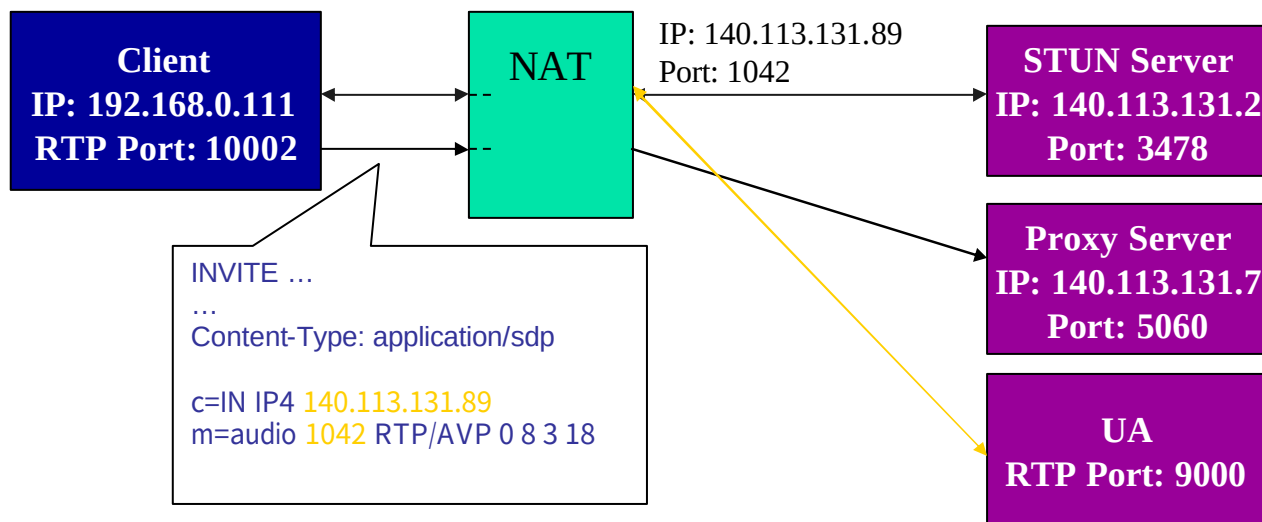
0000 00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00 ...u.f... (...E.
0010 04 01 00 00 40 00 40 11 66 5c c0 a8 00 6f 8c 71 ...0.0. f\...o.g
0020 83 07 13 c4 13 c4 03 ed e7 8e 49 4e 56 49 54 45 INVITE
0030 20 73 69 70 3a 39 34 34 30 32 31 33 37 31 40 31 sip:944 021371@1
0040 34 30 2e 31 31 33 2e 31 33 31 2e 37 3b 75 73 65 40.113.1 31.7;use

Filter: sip Expression: Clear Apply File: stun_ethereal.9 P: 412 D: 83 M: 0



Use STUN for RTP

- Send STUN queries from RTP port (10002) to STUN Server
- Use replied public address & port in SDP





STUN Message (SDP Port)

stun_ethereal - Ethereal

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
146	77.479361	192.168.0.111	140.113.131.2	STUN	Message : Binding Request
147	77.480041	140.113.131.2	192.168.0.111	STUN	Message : Binding Response

Frame 147 (98 bytes on wire, 98 bytes captured)

- Ethernet II, Src: 00:04:75:e4:66:eb, Dst: 00:04:13:10:11:28
- Internet Protocol, Src Addr: 140.113.131.2 (140.113.131.2), Dst Addr: 192.168.0.111 (192.168.0.111)
- User Datagram Protocol, Src Port: 3478 (3478), Dst Port: 10002 (10002)
- Simple Traversal of UDP Through NAT
 - Message Type: Binding Response (0x0101)
 - Message Length: 0x0024
 - Message Transaction ID: 58568CDC028DD8885A5DE533DC85294
 - Attributes
 - Attribute Type: MAPPED-ADDRESS (0x0001)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 1042
 - IP: 140.113.131.89 (140.113.131.89)
 - Attribute Type: SOURCE-ADDRESS (0x0004)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 3478
 - IP: 140.113.131.2 (140.113.131.2)
 - Attribute Type: CHANGED-ADDRESS (0x0005)
 - Attribute Length: 8
 - Protocol Family: IPv4 (0x0001)
 - Port: 3479

0000 00 04 13 10 11 28 00 04 75 e4 66 eb 08 00 45 00(..u.f...E.
 0010 00 54 00 00 40 00 3f 11 6b 0e 8c 71 83 02 c0 a8 .T...@.f. k..q...
 0020 00 6f 0d 96 27 12 00 40 90 58 01 01 00 24 5b 56 .o...f..@.X...\$[V
 0030 bc dc 02 8d db 8b b5 a5 de 53 3d cb 52 94 00 01S=.R...
 0040 00 08 00 01 04 12 8c 71 83 59 00 04 00 08 00 01q..Y.....

Filter: stun Expression: Clear Apply File: stun_ethereal97 P: 412 D: 30 M: 0



Correct INVITE Message (SDP)

stun_ethereal - Ethereal

File Edit View Capture Analyze Statistics Help

148 77.544782 192.168.0.111 140.113.131.7 SIP/SDP Request: INVITE sip:944021371@140.113.131.7;user=phone

149 77.541565 140.113.131.7 192.168.0.111 SIP Status: 100 trying -- your call is important to us

Frame 148 (1039 bytes on wire, 1039 bytes captured)

Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb

Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.7 (140.113.131.7)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Request-Line: INVITE sip:944021371@140.113.131.7;user=phone SIP/2.0

Message Header

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): root 1351538839 1351538839 IN IP4 140.113.131.89

Session Name (s): call

Connection Information (c): IN IP4:140.113.131.89

Time Description, active time (t): 0 0

Media Description, name and address (m): audio:1042 RTP/AVP 18 3 0 8 101

Media Attribute (a): rtpmap:18 g729/8000

Media Attribute (a): rtpmap:3 gsm/8000

Media Attribute (a): rtpmap:0 pcmu/8000

Media Attribute (a): rtpmap:8 poma/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): fmtp:101 0-15

Media Attribute (a): sendrecv

Media Attribute (a): srccidr:192.168.0.111:10002 140.113.131.89:1042

0000 00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00 ...f... (...E.

0010 04 01 00 00 40 00 40 11 66 5c c0 a8 00 6f 8c 71 ...0.0. f\...o.g

0020 83 07 13 c4 13 c4 03 ed e7 8e 49 4e 56 49 54 45 INVITE

0030 20 73 69 70 3a 39 34 34 30 32 31 33 37 31 40 31 sip:944 021371@1

0040 34 30 2e 31 31 33 2e 31 33 31 2e 37 3b 75 73 65 40.113.1 31.7;use

Filter: sip

Expression: Clear Apply

File: stun_ethereal9 P: 412 D: 83 M: 0



交通大學

National Chiao Tung University

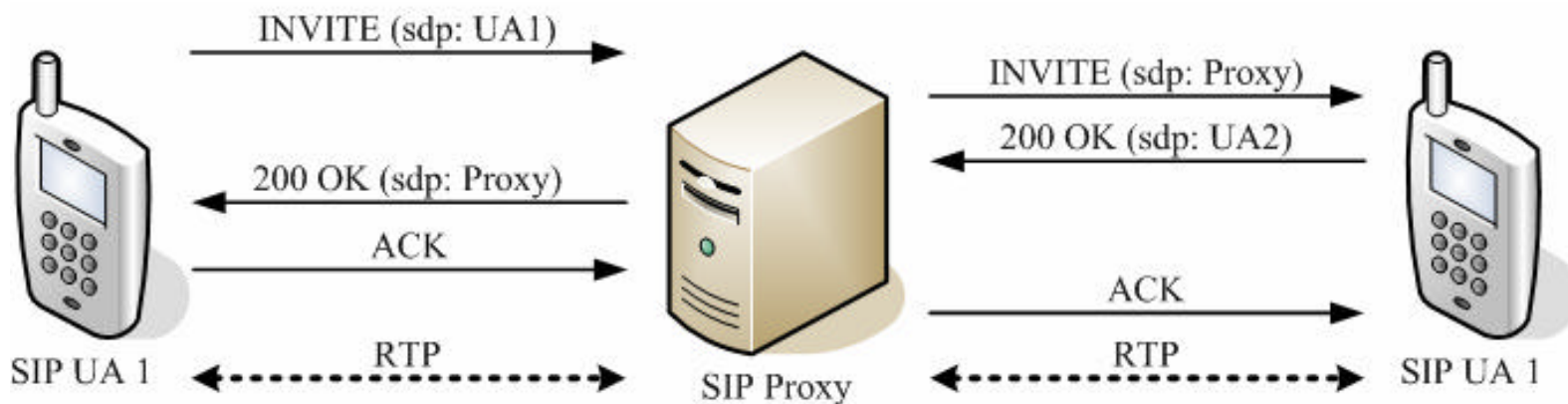
LAB 117
&
VoIP LAB



Session Controller

Session Controller 運作方法

- SIP
 - Add *Record-Route* header to enforce every SIP message inside this session passing through SIP Proxy for further modification
 - Modify *Contact* header for further routing
 - Add *rport* and *received* tag into *Via* for further routing
- SDP
 - Replace sdp of each UA into that of SIP Proxy for relaying RTP packages





SIP Server Configuration

```
01 record_route(); //add "Record-Route" header into SIP message
02 if( nat_uac_test() ){ //test if UA is behind 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 };
```



REGISTER Message

eth_proxy_caller - Ethernet

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
40	56.468281	192.168.0.111	140.113.131.17	SIP	Request: REGISTER sip:140.113.131.17
41	56.470166	140.113.131.17	192.168.0.111	SIP	Status: 200 OK (2 bindings)

Frame 40 (525 bytes on wire (525 bytes captured))

Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb

Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.17 (140.113.131.17)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Request-Line: REGISTER sip:140.113.131.17 SIP/2.0

Method: REGISTER

Message Header

Via: SIP/2.0/UDP 192.168.0.111:5060;branch=z9hG4bK-fzw1kc7rhaw;rport

From: "Ya-Lin" <sip:944021375@140.113.131.17>;tag=upq7h13pek

To: "Ya-Lin" <sip:944021375@140.113.131.17>

Call-ID: 3c267004cf40-j3fdv4sj9oz7@192-168-0-111

CSeq: 1 REGISTER

Max-Forwards: 70

Contact: <sip:944021375@192.168.0.111:5060;transport=udp;line=1hynb3y>;q=1.0;description="Available"

User-Agent: snom200-2.03s

Supported: gruu

Expires: 600

Content-Length: 0

0000 00 04 75 e4 66 eb 00 04 13 10 11 28 08 00 45 00 ...u.f...C...E.

0010 01 ff 00 00 40 00 40 11 68 54 c0 a8 00 6f 8c 71@.@.ht...o.g

0020 83 11 13 c4 13 c4 01 eb 81 b1 52 45 47 49 53 54REGIST

0030 45 52 20 73 69 70 3a 31 34 30 2e 31 31 33 2e 31 ER sip:1 40.113.1

0040 33 31 2e 31 37 20 53 49 50 2f 32 2e 30 0d 0a 56 31.17 SI P/2.0..V

Filter: sip

Expression: Clear Apply

File: eth_proxy_caller P: 901 D: 30 M: 0



200 OK Message of REGISTER

Packet #41: 56.470166 140.113.131.17 → 192.168.0.111 SIP Status: 200 OK (2 bindings)

Frame 41 (772 bytes on wire, 772 bytes captured)

Ethernet II, Src: 00:04:75:e4:66:eb, Dst: 00:04:13:10:11:28

Internet Protocol, Src Addr: 140.113.131.17 (140.113.131.17), Dst Addr: 192.168.0.111 (192.168.0.111)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol

Status-Line: SIP/2.0 200 OK

Status-Code: 200

Message Header

Via: SIP/2.0/UDP 192.168.0.111:5060;branch=z9hG4bK-fzw1kc7rhaw;rport=1407;received=140.113.131.89

From: "Ya-Lin" <sip:944021375@140.113.131.17>;tag=upq7h13pek

To: "Ya-Lin" <sip:944021375@140.113.131.17>;tag=b27e1ald33761e85846fc98f5f3a7e58.9100

Call-ID: 3c267004cf40-j3fdv4sj9oz7@192-168-0-111

CSeq: 1 REGISTER

Contact: <sip:944021375@140.113.131.89:1407;transport=udp;line=1hynyb3y>;q=1.00;expires=600

Contact: <sip:140.113.131.89:1065>;q=0.00;expires=1707

Server: Sip Express router (0.8.12 (i386/linux))

Content-Length: 0

Warning: 392 140.113.131.17:5060 "Noisy feedback tells: pid=21067 req_src_ip=140.113.131.89 req_src_port=1407 in_uri=sip:

Filter: sip



INVITE Message sent by caller (SDP)

Wireshark packet capture showing an INVITE message sent by the caller (SDP). The packet is captured on the Ethernet interface.

No.	Time	Source	Destination	Protocol	Info
64	65.773566	192.168.0.111	140.113.131.17	SIP/SIP	Request: INVITE sip:9440210900140.113.131.17;user=phone
65	65.775573	140.113.131.17	192.168.0.111	SIP	Status: 100 trying -- your call is important to us

Frame 64 (988 bytes on wire (988 bytes captured) on interface 0:00:04:13:10:11:28, 0:00:04:75:e4:66:eb)

- Ethernet II, Src: 00:04:13:10:11:28, Dst: 00:04:75:e4:66:eb
- Internet Protocol, Src Addr: 192.168.0.111 (192.168.0.111), Dst Addr: 140.113.131.17 (140.113.131.17)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
 - Request-Line: INVITE sip:9440210900140.113.131.17;user=phone SIP/2.0
 - Message Header
 - Message body
 - Session Description Protocol
 - Session Description Protocol Version (v): 0
 - Owner/Creator, Session Id (o): root 1823089412 1823089412 IN IP4 192.168.0.111
 - Session Name (s): call
 - Connection Information (c): IN IP4 192.168.0.111
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 10002 RTP/AVP 0 8 3 18 101
 - Media Attribute (a): rtpmap:0 pcmu/8000
 - Media Attribute (a): rtpmap:8 pcma/8000
 - Media Attribute (a): rtpmap:3 gsm/8000
 - Media Attribute (a): rtpmap:18 g729/8000
 - Media Attribute (a): rtpmap:101 telephone-event/8000
 - Media Attribute (a): fmtp:101 0-15
 - Media Attribute (a): sendrecv

Filter: sip



INVITE Message received by callee (SDP)

rtsp_proxy_callee - Ethereal

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

235	14.941736	140.113.131.17	140.113.131.82	SIP/SDP	Request: INVITE sip:140.113.131.82:4634, with session d
236	14.942547	140.113.131.82	140.113.131.17	SIP	Status: 100 Trying

Frame 235 (1139 bytes on wire (911 bytes captured) on interface 0)

Ethernet II, Src: 00:90:cc:6c:32:67, Dst: 00:0c:6e:49:1b:f9

Internet Protocol, Src Addr: 140.113.131.17 (140.113.131.17), Dst Addr: 140.113.131.82 (140.113.131.82)

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 4634 (4634)

Session Initiation Protocol

Request-Line: INVITE sip:140.113.131.82:4634 SIP/2.0

Message Header

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): root 1823089412 1823089412 IN IP4 192.168.0.111

Session Name (s): call

Connection Information (c): IN IP4 140.113.131.17

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 35056 RTP/AVP 0 8 3 18 101

Media Attribute (a): rtpmap:0 pcmu/8000

Media Attribute (a): rtpmap:8 pcma/8000

Media Attribute (a): rtpmap:3 gsm/8000

Media Attribute (a): rtpmap:18 g729/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): fmp:101 0-15

Media Attribute (a): sendrecv

0000 00 0c 6e 49 1b f9 00 90 cc 6c 32 67 08 00 45 10 ..nI... .12g..E.
 0010 04 65 00 00 40 00 40 11 17 32 8c 71 83 11 8c 71 ..e..&.. .2.q...q
 0020 83 52 13 c4 12 1a 04 51 64 b2 49 4e 56 49 54 45 .R.....Q d.INVITE
 0030 20 73 69 70 3a 31 34 30 2e 31 31 33 2e 31 33 31 sip:140 .113.131
 0040 2e 38 32 3a 34 36 33 34 20 53 49 50 2f 32 2e 30 .82:4634 SIP/2.0

Filter: sip

Expression... Clear Apply File: rtsp_proxy_callee P: 1071 D: 9 M: 0



200 OK Message of INVITE sent by callee (SDP)

rtsp_proxy_callee - Ethernet

File Edit View Capture Analyze Statistics Help

No. Time Source Destination Protocol Info

305	20.583876	140.113.131.82	140.113.131.17	SIP/SDP	Status: 200 OK, with session description
306	20.632671	140.113.131.17	140.113.131.82	SIP	Request: ACK sip:140.113.131.82:4634

Frame 305 (862 bytes on wire (862 bytes captured))

Ethernet II, Src: 00:0c:6e:49:1b:f9, Dst: 00:90:cc:6c:32:67

Internet Protocol, Src Addr: 140.113.131.82 (140.113.131.82), Dst Addr: 140.113.131.17 (140.113.131.17)

User Datagram Protocol, Src Port: 4634 (4634), Dst Port: 5060 (5060)

Session Initiation Protocol

Status-Line: SIP/2.0 200 OK

Message Header

Message body

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): PAN 0 0 IN IP4 140.113.131.82

Session Name (s): call

Connection Information (c): IN IP4 140.113.131.82

Bandwidth Information (b): CT:1000

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 60484 RTP/AVP 0 8 3 101

Media Attribute (a): rtpmap:0 pcmu/8000

Media Attribute (a): rtpmap:8 pcma/8000

Media Attribute (a): rtpmap:3 gsm/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Attribute (a): fmtp:101 0-16

0000 00 90 cc 6c 32 67 00 0c 6e 49 1b f9 08 00 45 00 ...120... nI...E.
 0010 03 50 72 21 00 00 80 11 a6 35 8c 71 83 52 8c 71 .Pr!.... .S.q.R.q
 0020 83 11 12 1a 13 c4 03 3c c8 10 53 49 50 2f 32 2e< ..SIP/2.
 0030 30 20 32 30 30 20 4f 4b 0d 0a 56 69 61 3a 20 53 0 200 OK ..Via: S
 0040 49 50 2f 32 2e 30 2f 55 44 50 20 31 34 30 2e 31 IP/2.0/U DP 140.1

Filter: sip

Expression... Clear Apply File: rtsp_proxy_callee P: 1071 D: 9 M: 0



200 OK Message of INVITE received by caller (SDP)

File Edit View Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
69	71.420414	140.113.131.17	192.168.0.111	SIP/SIP	Status: 200 OK, with session description
70	71.465669	192.168.0.111	140.113.131.17	SIP	Request: ACK sip:140.113.131.82:4634

Frame 69 (800 bytes on wire (800 bytes captured))

- Ethernet II, Src: 00:04:75:e4:66:eb, Dst: 00:04:13:10:11:28
- Internet Protocol, Src Addr: 140.113.131.17 (140.113.131.17), Dst Addr: 192.168.0.111 (192.168.0.111)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
 - Status-Line: SIP/2.0 200 OK
 - Message Header
 - Message body
 - Session Description Protocol
 - Session Description Protocol Version (v): 0
 - Owner/Creator, Session Id (o): PAN 0 0 IN IP4 140.113.131.82
 - Session Name (s): call
 - Connection Information (c): IN IP4 140.113.131.17
 - Bandwidth Information (b): CT:1000
 - Time Description, active time (t): 0 0
 - Media Description, name and address (m): audio 35056 RTP/AVP 0 B 3 101
 - Media Attribute (a): rtpmap:0 pcmu/8000
 - Media Attribute (a): rtpmap:8 pcma/8000
 - Media Attribute (a): rtpmap:3 gsm/8000
 - Media Attribute (a): rtpmap:101 telephone-event/8000
 - Media Attribute (a): fmtp:101 0-16

0000 00 04 13 10 11 28 00 04 75 e4 66 eb 08 00 45 10(..u.f...E.
 0010 03 12 00 00 40 00 3f 11 68 31 8c 71 83 11 c0 a84.?.hl.q....
 0020 00 6f 13 c4 13 c4 02 fe d6 ec 53 49 50 2f 32 2e .o.....:SIP/2.
 0030 30 20 32 30 30 20 4f 4b 0d 0a 56 69 61 3a 20 53 O 200 OK ..Via: S
 0040 49 50 2f 32 2e 30 2f 55 44 50 20 31 39 32 2e 31 IP/2.0/u DP 192.1

Filter: sip



Comparison

需要支援的設備

限制性比較

使用方便性比較

項目 機制	SIP UA是否 需要支援	NAT是否 需要支援	是否需要 額外設備	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	設定難易度	通訊延遲	IP改變是否 造成影響
VPN	是	否	是	是	是	是	否	較困難	最長	否
Static Assignment	是	否	否	是	是	否	否	最困難	最短	是
UPnP	是	是	否	是	否	否	否	最容易	次短	否
STUN	是	否	是	否	是	否	否	次容易	次短	否
Session Controller	否	否	是	是	是	否	是	最容易	較長	否



Summary

- [Static Mapping](#) is a simple mechanism, but users and network administrators should manually configure the IP and port for each IP phones. This work is tedious.
- [VPN](#) is a server-based solution. A user should have a VPN account and build VPN connection before communication. VPN will increase communication delay.
- [STUN](#) is a popular solution for [non-symmetric](#) NAT, but STUN cannot assist SIP to traverse symmetric NAT.
- A SIP UA obtains public IP & port information from NAT via [UPnP](#) and modifies the application-layer header. However, old NATs cannot provide UPnP without upgrade.
- [Session Controller](#) helps SIP and RTP traverse NAT without modifying SIP UA and NAT.
- [NTP VoIP Platform](#) provides all above NAT traversal mechanisms.



Reference (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”，TANET2004, 台東, Oct 2004。
- B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis, “A Framework for IP Based Virtual Private Networks”, IETF RFC-2764, February 2000.
- H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, IETF RFC-3550, July 2003.
- 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.
- 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.
- M. Handley, V. Jacobson, “SDP: Session Description Protocol”, IETF RFC-2327, April 1998.
- P. Srisuresh, M. Holdrege, “IP Network Address Translator (NAT) Terminology and Considerations”, IETF RFC-2663, August 1999.
- R. Droms, “Dynamic Host Configuration Protocol”, IETF RFC-1541, October 1993.



Reference (2)

- 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.
- Ethereal: A Network Protocol Analyzer, <http://www.ethereal.com/>
- iptel.org SIP Server: SIP Express Router, <http://www.iptel.org/ser/>
- Microsoft Corporation, <http://www.microsoft.com/>
- 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
- PortaOne nathelper RTP Proxy,
<http://www.portaone.com/resources/downloads/index.html>
- snom technology AG – Voice over IP (VoIP) SIP Phones,
http://www.snom.com/index1_en.php
- UPnP(TM) Forum, <http://www.upnp.org>
- voip-info.org: RTP Symmetric, <http://www.voip-info.org/wiki-RTP+Symmetric>
- Windows Messenger for Windows XP,
<http://www.microsoft.com/windows/messenger/>
- 黃雅琳、陳懷恩、吳坤熹、林一平. SIP Traversal over NAT Mechanisms on NTP VoIP Platform. TANET2004. 台東. Oct 2004.