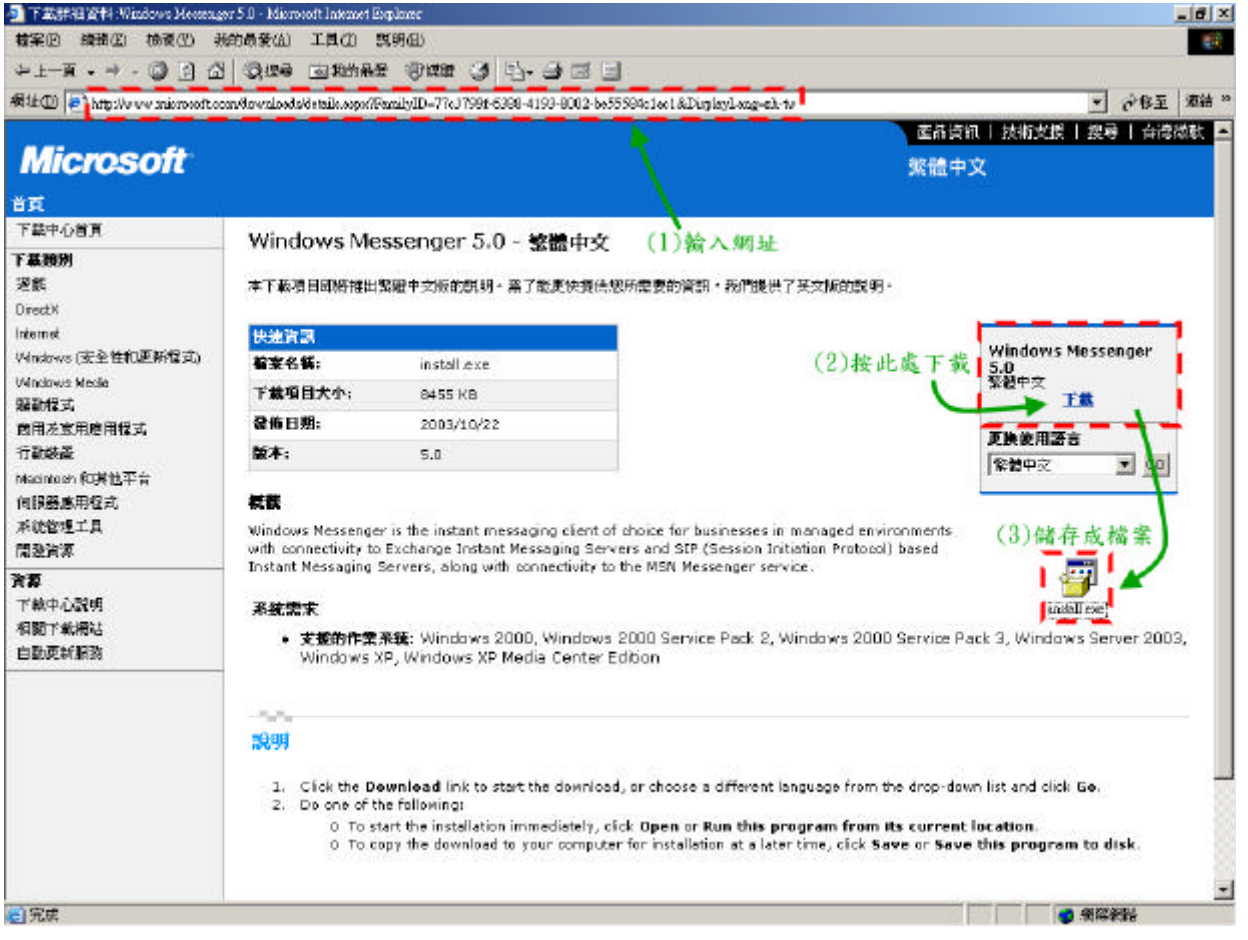
SIP Traversal over NAT Mechanisms on NTP VoIP Platform

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

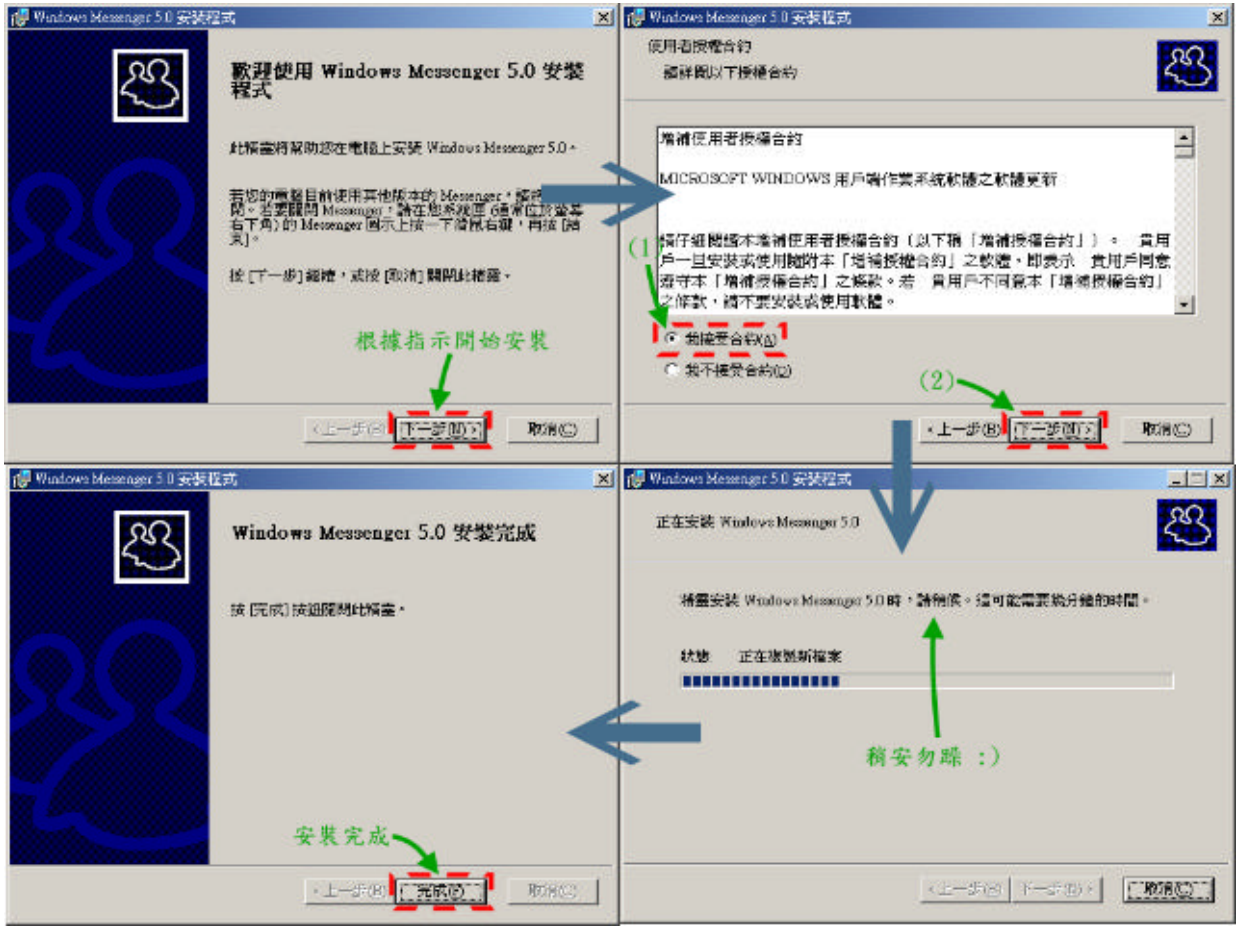
Outline

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

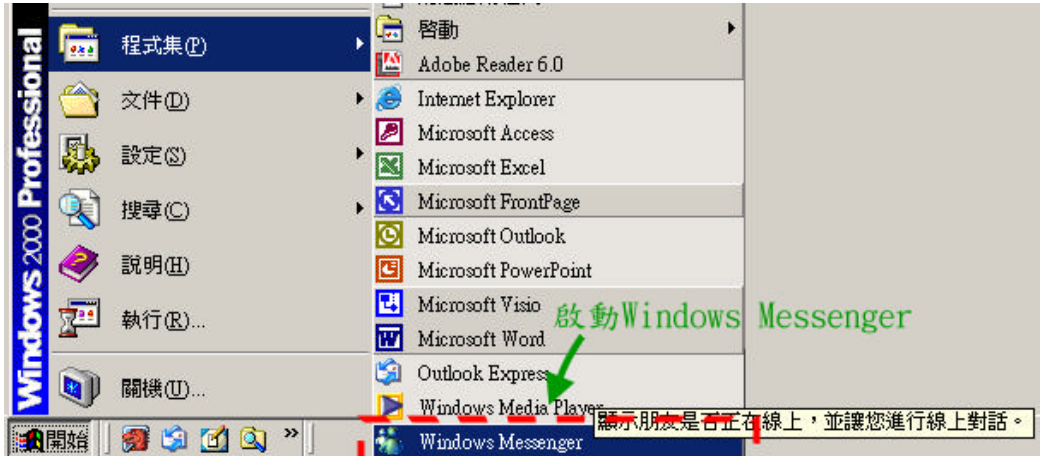
Windows Messenger Installation



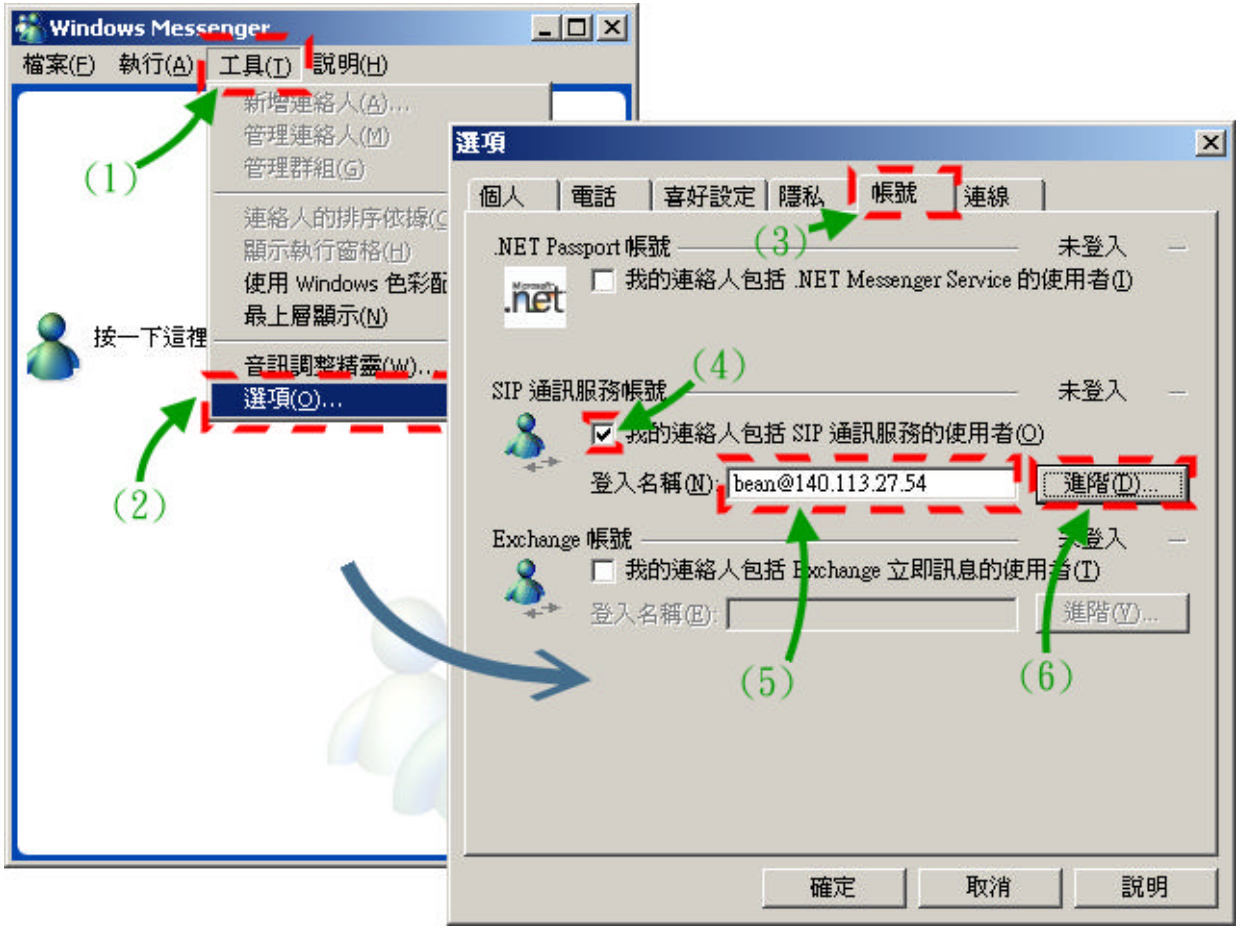
Step-by-step Installation



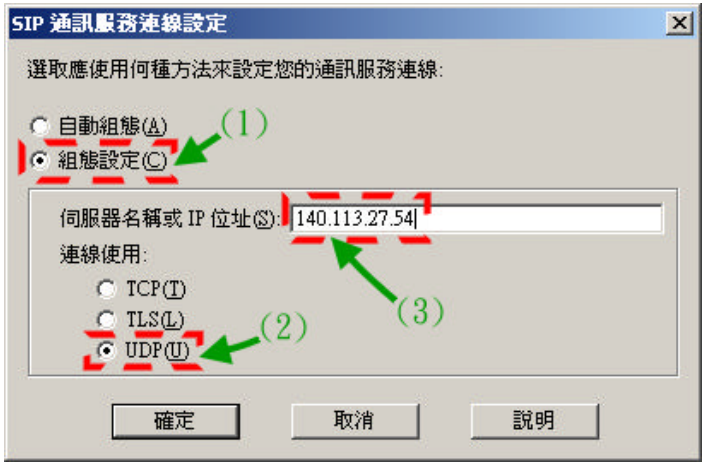
Windows Messenger Getting Start



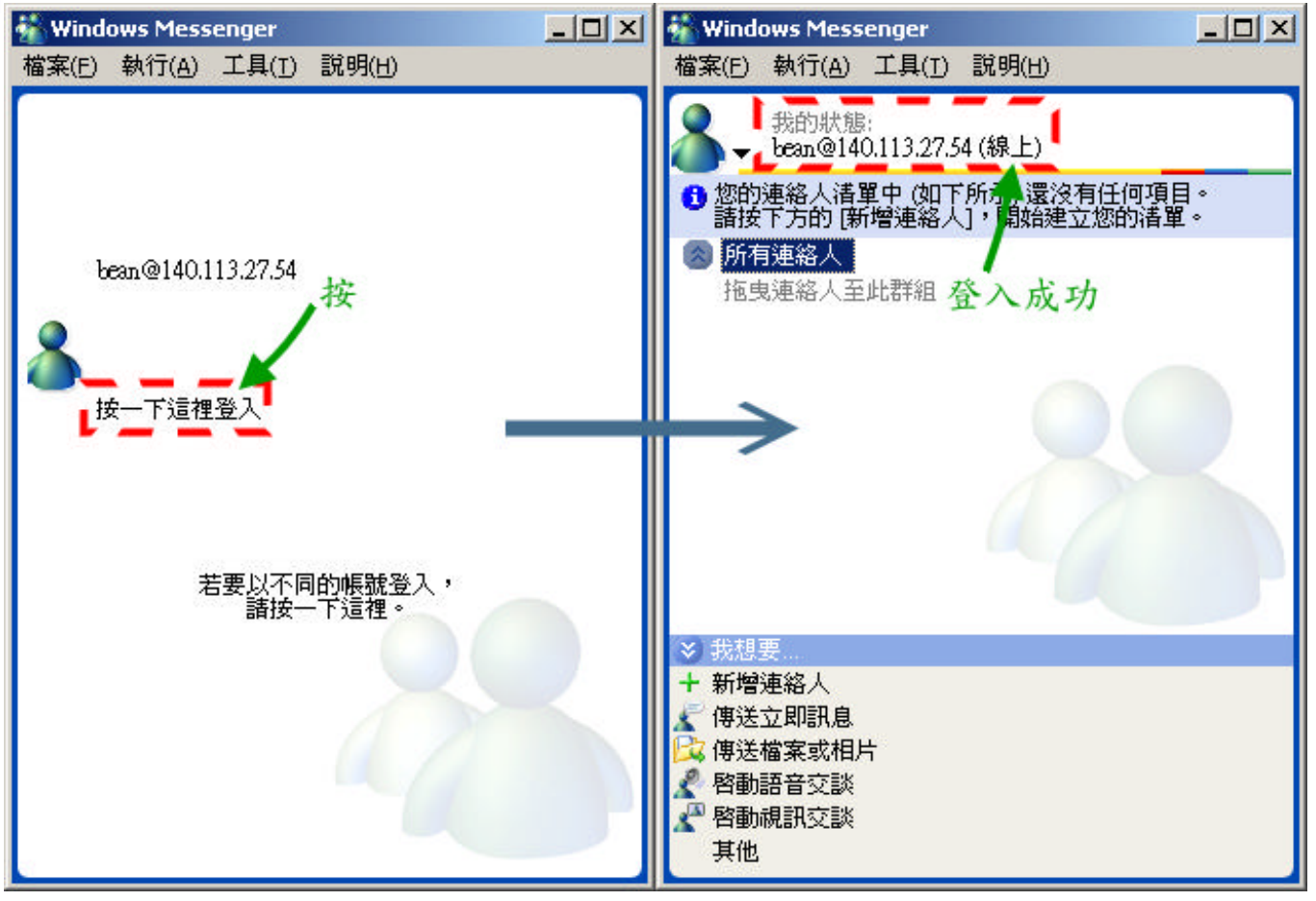
Windows Messenger Configuration



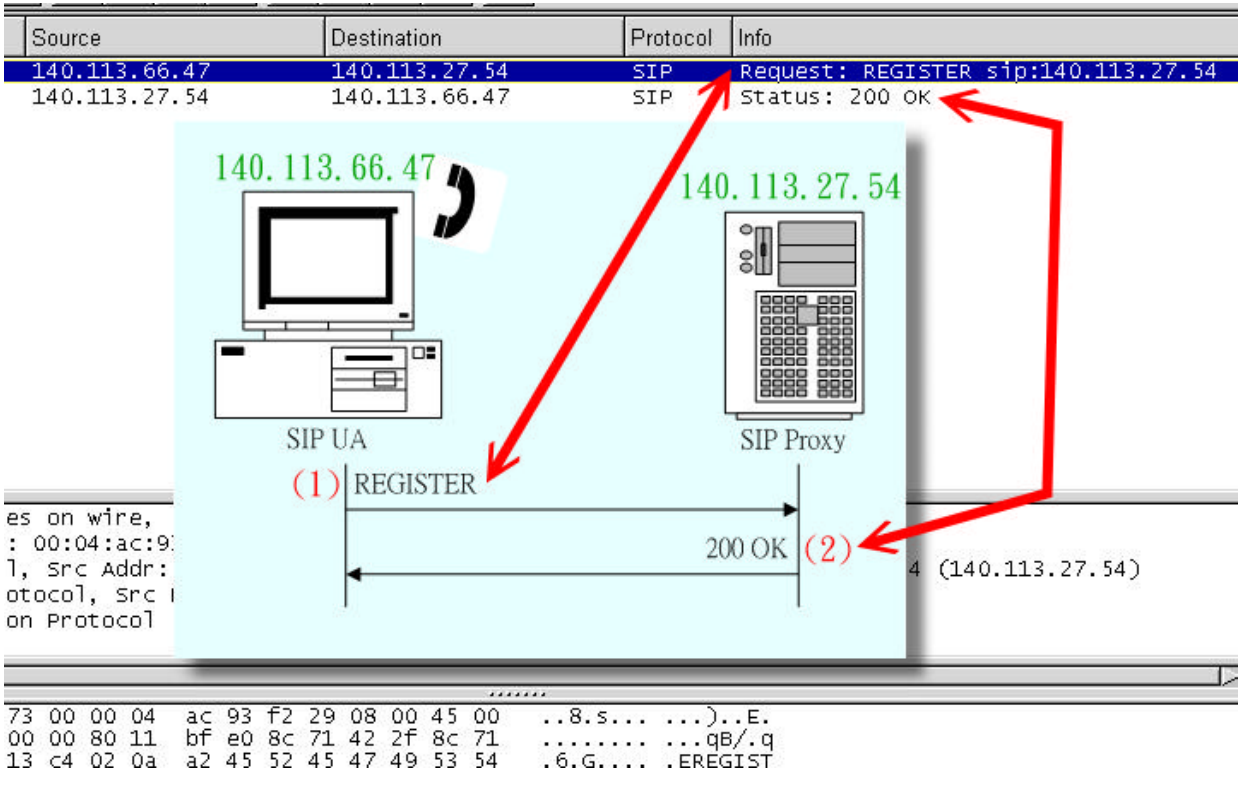
SIP Server Configuration



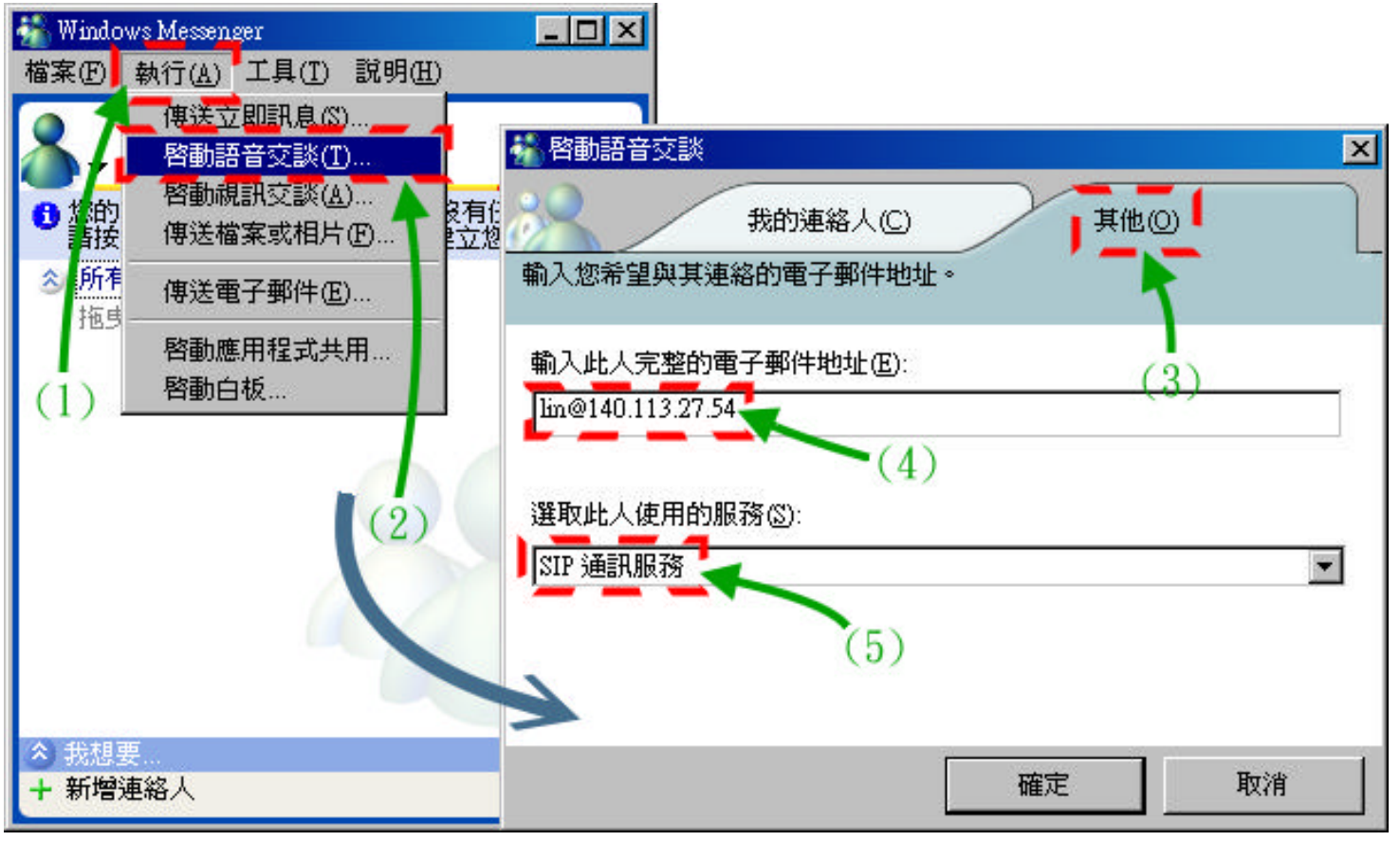
Login


Windows Messenger
檔案(F) 執行(A) 工具(T) 說明(H)
bean@140.113.27.54
按
按一下這裡登入
若要以不同的帳號登入，
請按一下這裡。
Windows Messenger
檔案(F) 執行(A) 工具(T) 說明(H)
我的狀態:
bean@140.113.27.54 (線上)
您的連絡人清單中 (如下所示) 還沒有任何項目。
請按下方的 [新增連絡人]，開始建立您的清單。
所有連絡人
拖曳連絡人至此群組
登入成功
我想要...
新增連絡人
傳送立即訊息
傳送檔案或相片
啓動語音交談
啓動視訊交談
其他

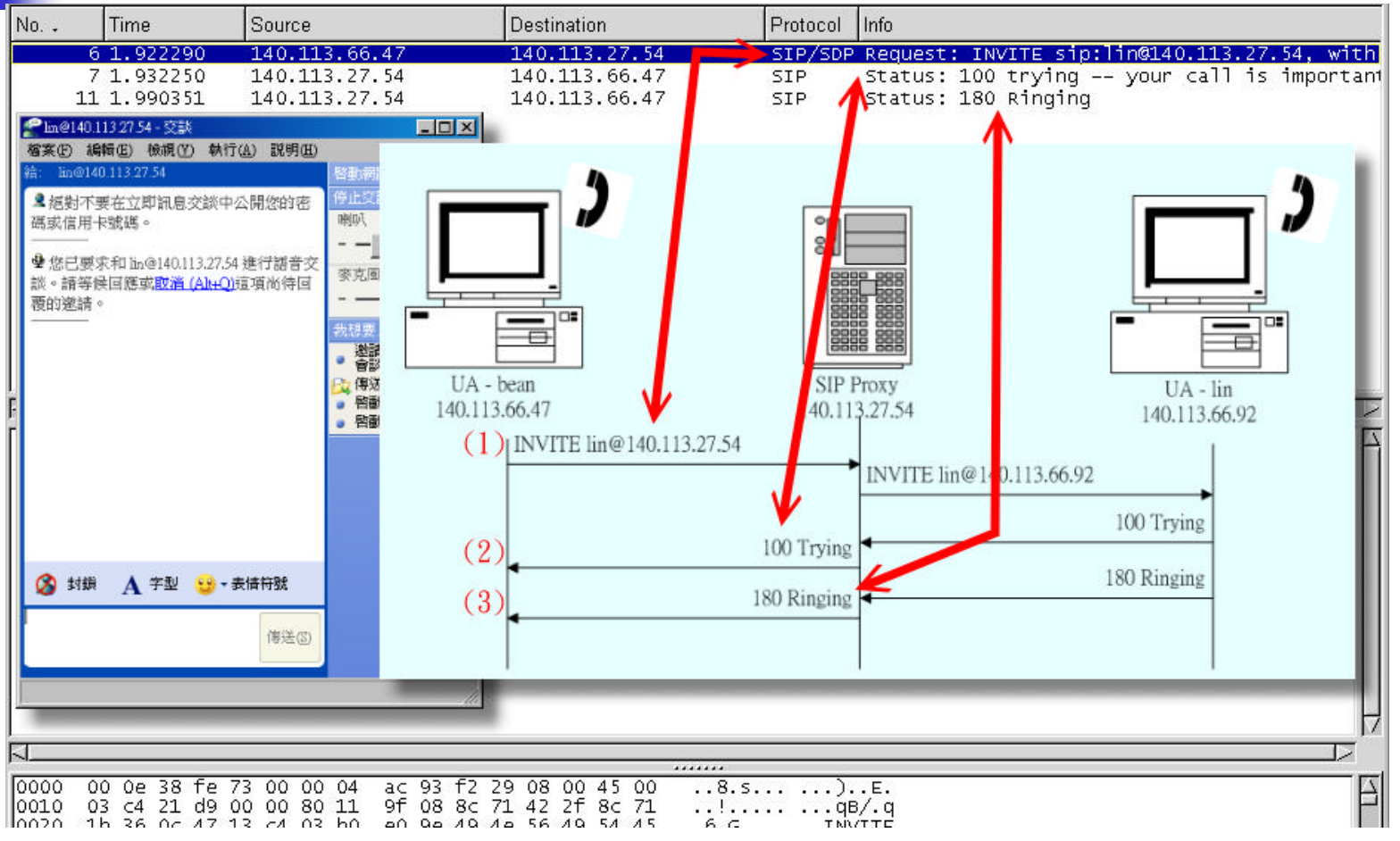
SIP Registration



Dialing

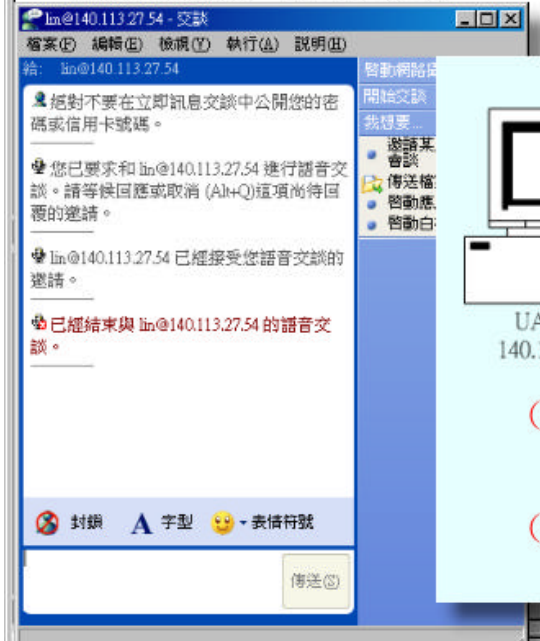

Windows Messenger
檔案(F)
執行(A)
工具(T)
說明(H)
傳送立即訊息(S)...
啓動語音交談(T)...
啓動視訊交談(A)...
傳送檔案或相片(F)...
傳送電子郵件(E)...
啓動應用程式共用...
啓動白板...
(1)
(2)
我想要...
新增連絡人
啓動語音交談
我的連絡人(C)
其他(O)
輸入您希望與其連絡的電子郵件地址。
輸入此人完整的電子郵件地址(E):
lin@140.113.27.54
(3)
(4)
選取此人使用的服務(S):
SIP 通訊服務
(5)
確定
取消

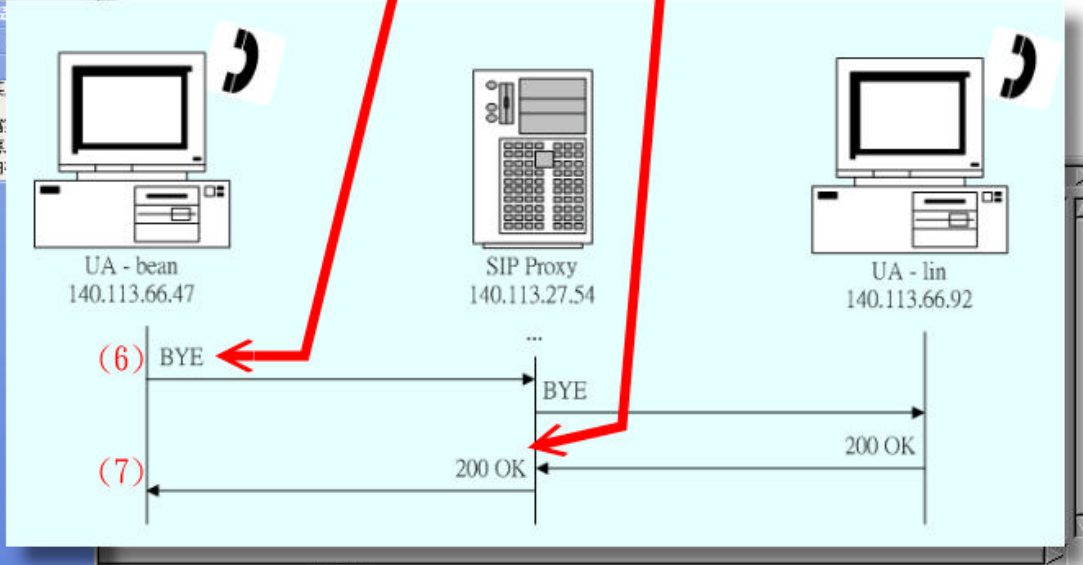
SIP INVITE Transaction



BYE Transaction

No.	Time	Source	Destination	Protocol	Info
6	1.922290	140.113.66.47	140.113.27.54	SIP/SDP	Request: INVITE sip:lin@140.113.27.54, with
7	1.932250	140.113.27.54	140.113.66.47	SIP	Status: 100 trying -- your call is important
11	1.990351	140.113.27.54	140.113.66.47	SIP	Status: 180 Ringing
64	24.634786	140.113.27.54	140.113.66.47	SIP/SDP	Status: 200 OK, with session description
65	24.759109	140.113.66.47	140.113.27.54	SIP	Request: ACK sip:lin@140.113.27.54;ftag=0f0
141	39.967548	140.113.66.47	140.113.27.54	SIP	Request: BYE sip:lin@140.113.27.54;ftag=0f0
144	40.172821	140.113.27.54	140.113.66.47	SIP	Status: 200 OK

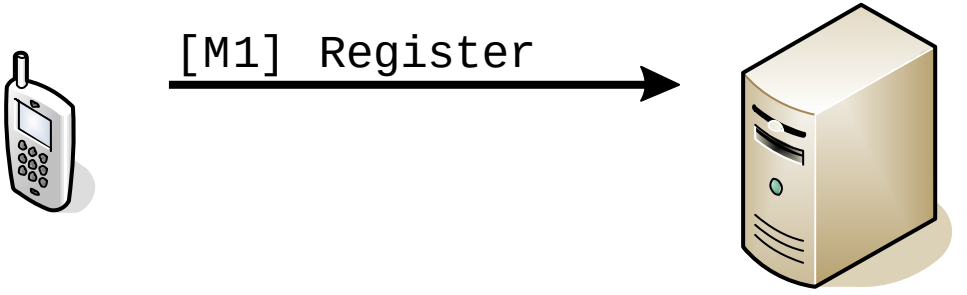





```
0010  03 c4 21 d9 00 00 80 11  9f 08 8c 71 42 2f 8c 71   ..!..... ...qB/.q
0020  1b 36 0c 47 13 c4 03 b0  e0 9e 49 4e 56 49 54 45   .6.G.... ..INVITE
```

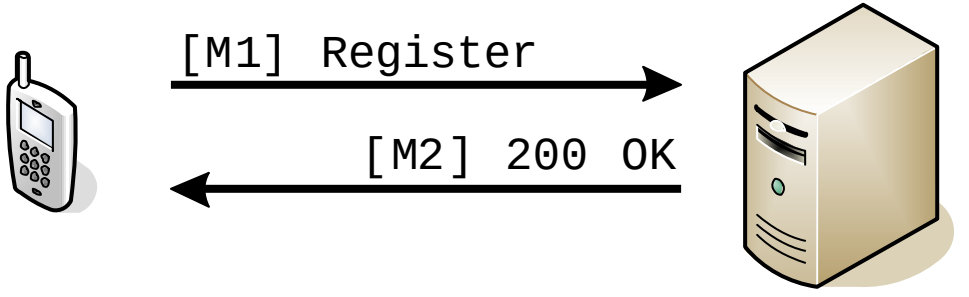
Accept a Call

Registration Message Flow [1/2]



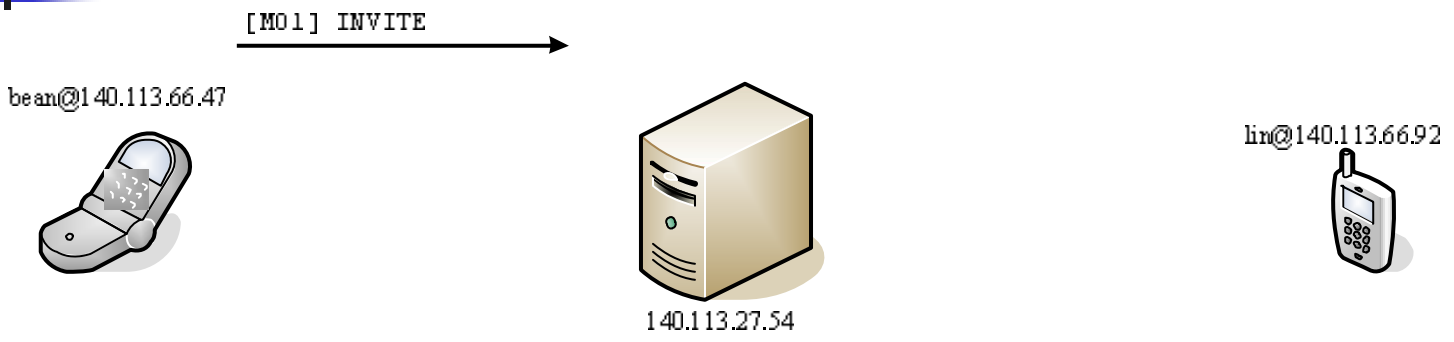

```
[M1]
REGISTER sip:140.113.27.54 SIP/2.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 70
From: <sip:bean@140.113.27.54>;tag=1209612b2a094c97b5473a6c8fca13a6;epid=04de356250
To: <sip:bean@140.113.27.54>
Call-ID: 8db46488bc4d4f6fb85476d9f3a68e62@140.113.66.47
CSeq: 1 REGISTER
Contact: <sip:140.113.66.47:12264>;methods="INVITE, 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]




```
[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"
```

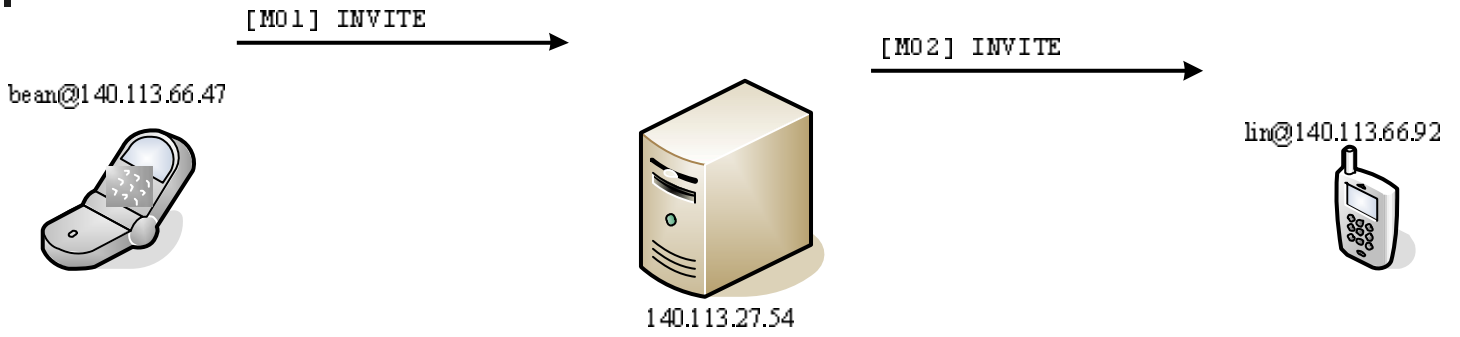
Call Message Flow [1/15]




```
[M01-1]
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:bear@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/1MLU2txhPZd3UfpksfafZeSwo
a=rtpmap:97 red/8000
...
```

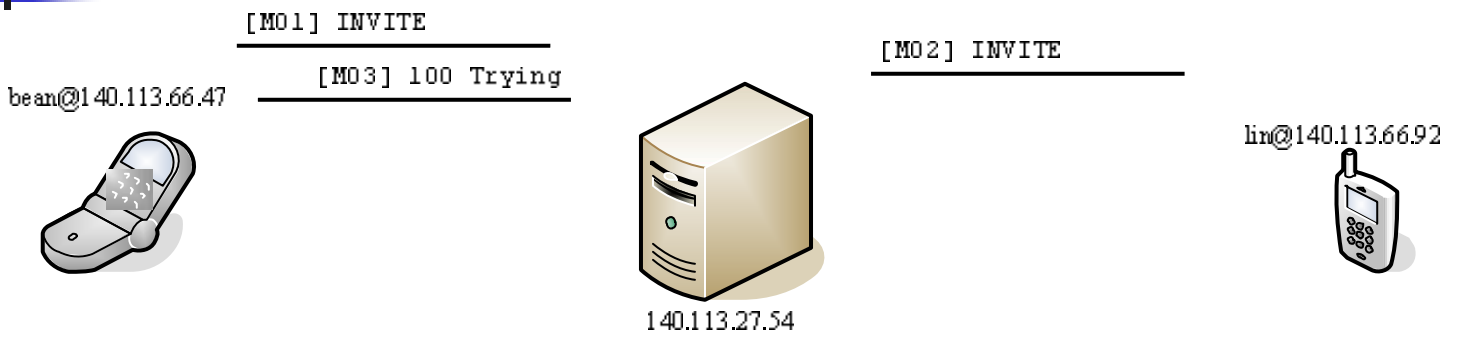
Call Message Flow [2/15]




```
[M02-1]
INVITE sip:140.113.66.92:15450 SIP/2.0
Record-Route: <sip:lir@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:lir@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
```

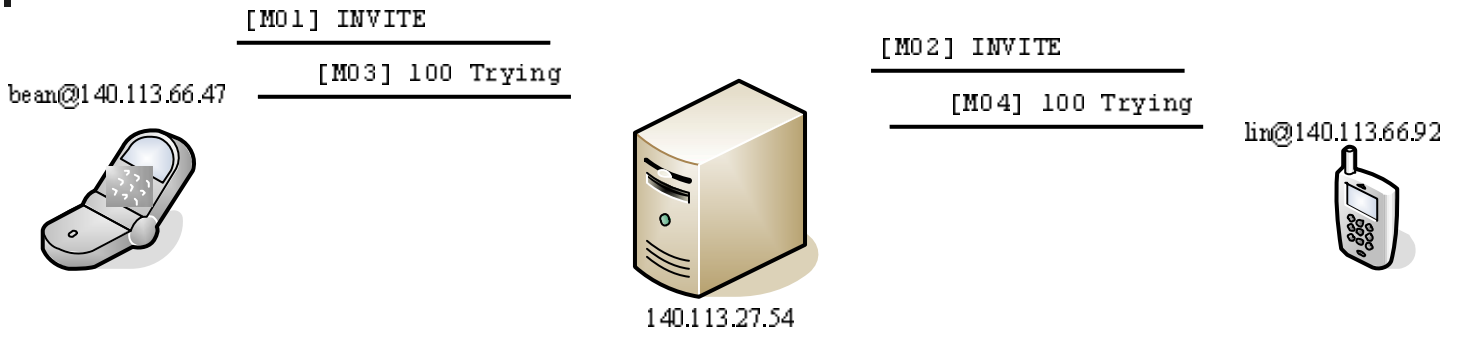
```
[M02-2]
v=0
o=- 0 0 IN IP4 140.113.66.47
s=session
c=IN IP4 140.113.66.47
b=CT:1000
t=0 0
m=audio 42522 RTP/AVP 97 111 112 6 0 8 4 5 3 101
k=base64:cReawB4kZs5su1tjK/1MLU2txhPZd3UfpksfafZeSwo
a=rtpmap:97 red/8000
...
```

Call Message Flow [3/15]



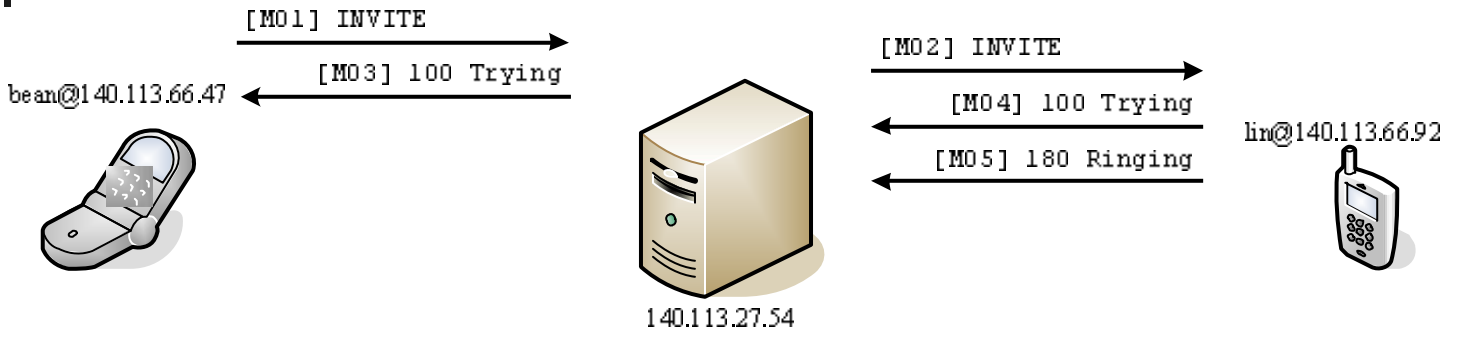

```
[M03]
SIP/2.0 100 trying -- your call is important to us
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 INVITE
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]



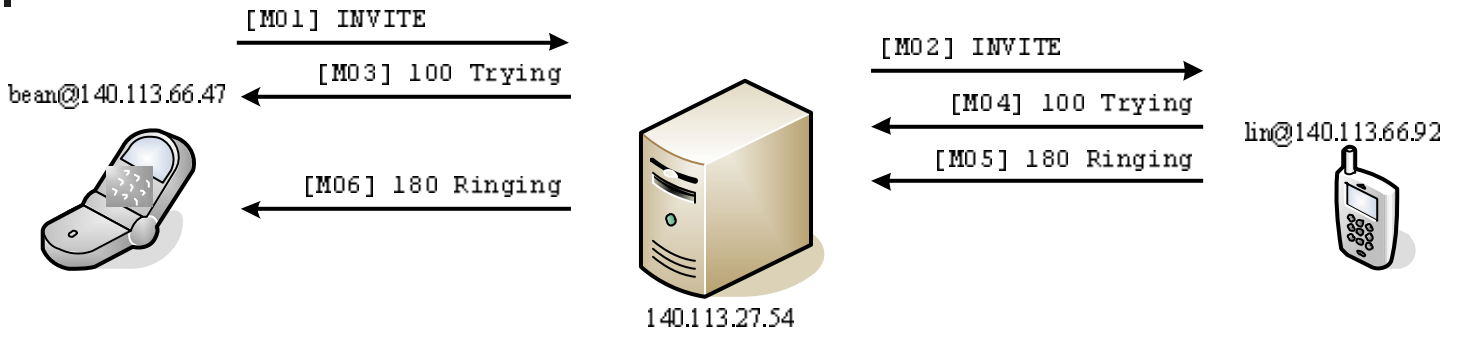

```
[M04]
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK944c.70b18621.0
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 1 INVITE
User-Agent: Windows RTC/1.0
Content-Length: 0
```

Call Message Flow [5/15]



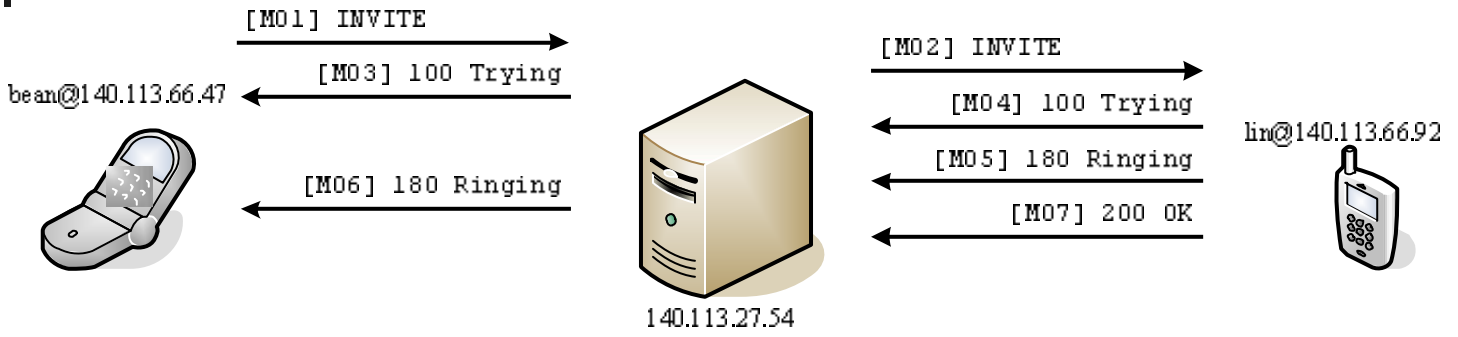

```
[M05]
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK944c.70b18621.0
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
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
```

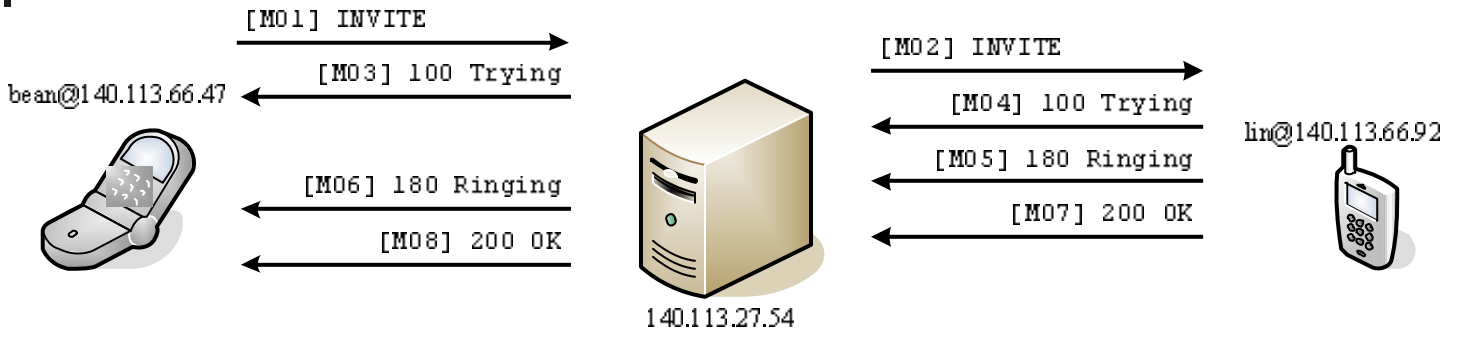
Call Message Flow [7/15]




```
[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
...
```

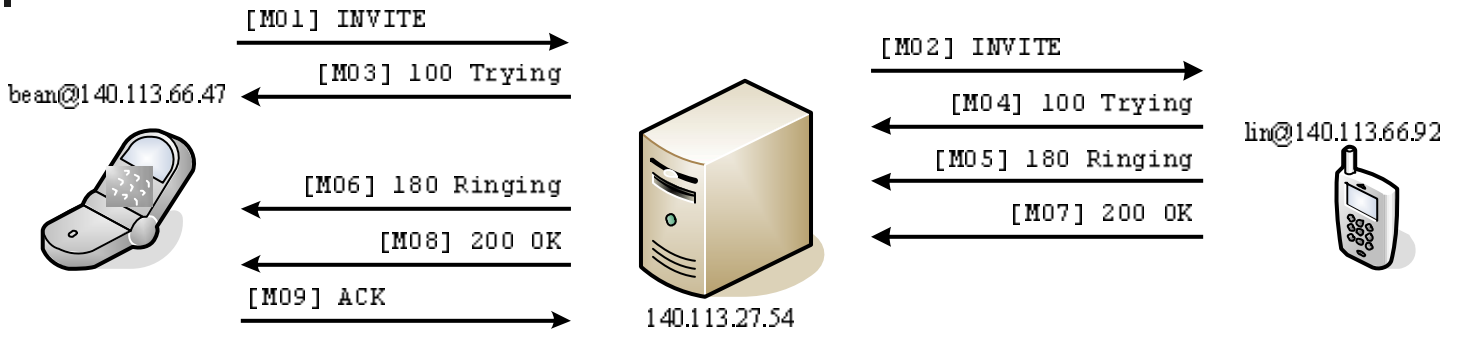
Call Message Flow [8/15]




```
[M08-1]
SIP/2.0 200 OK
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bear@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]

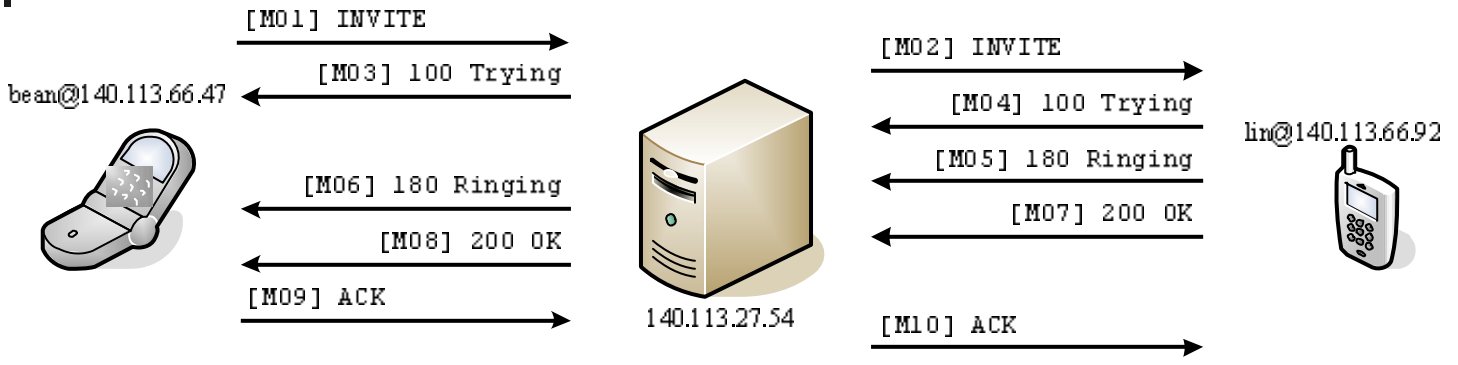



```
[M09]
ACK sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on SIP/2.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 70
From: "bean@140.113.27.54"<sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a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

140.113.66.92

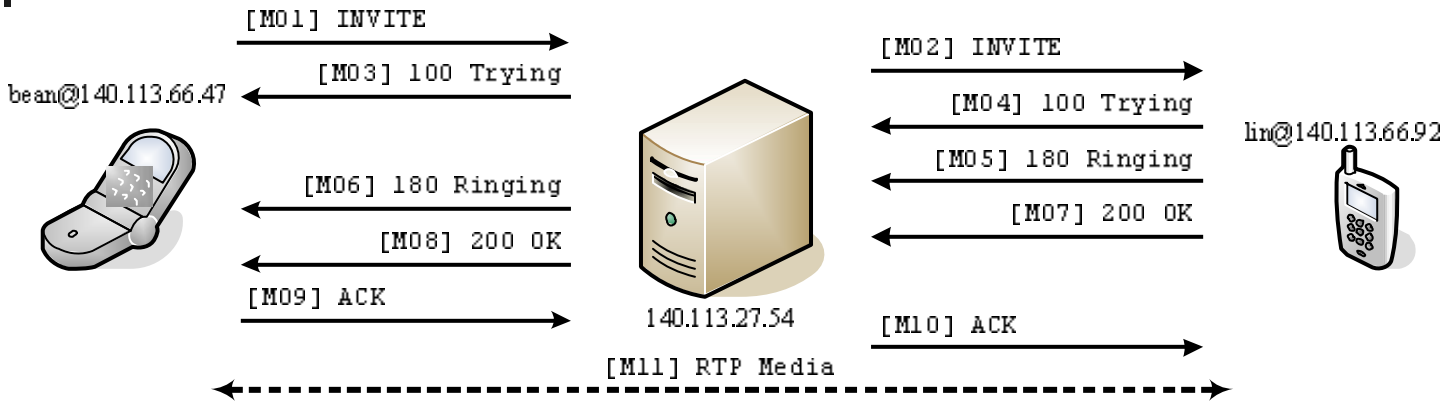
140.113.27.54

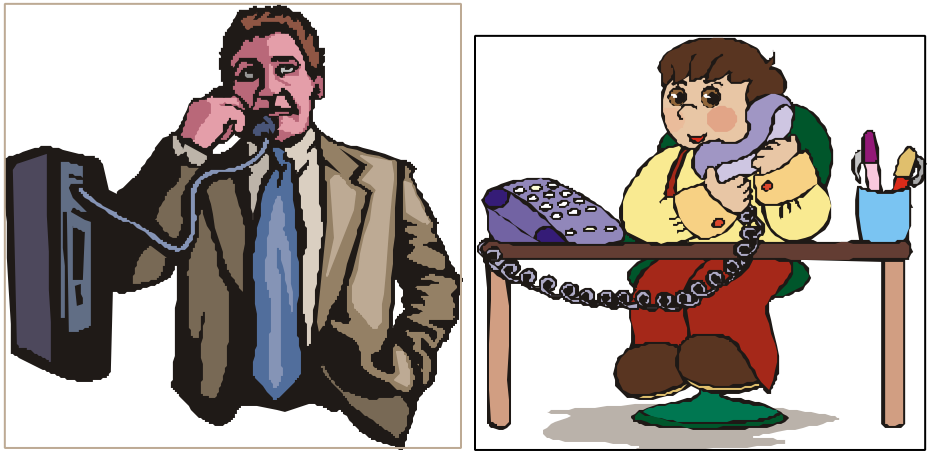
Call Message Flow [10/15]



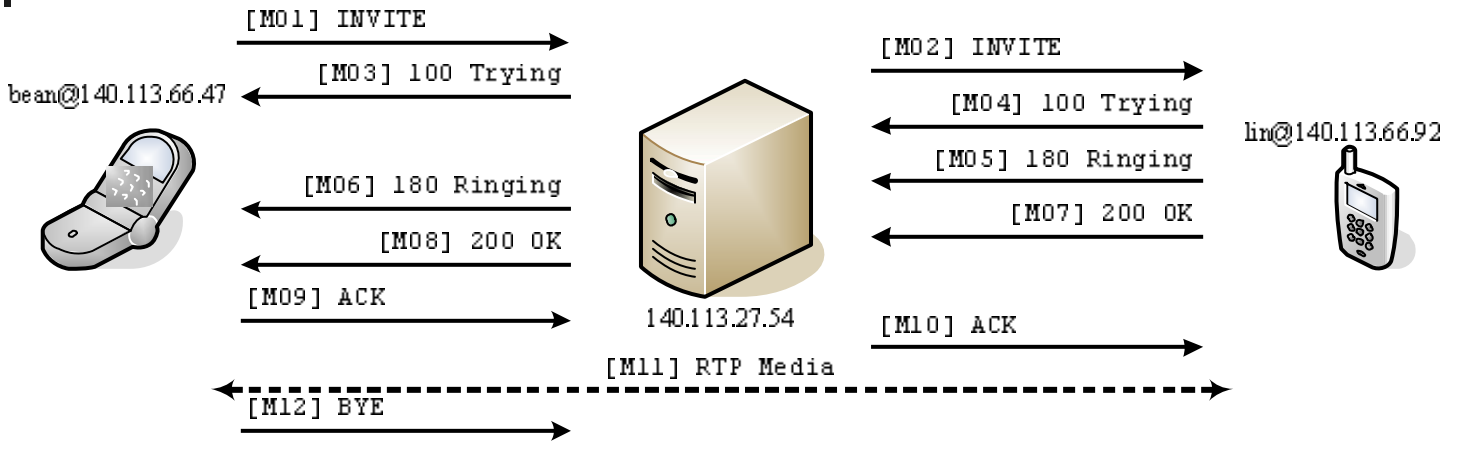

```
[M10]
ACK sip:140.113.66.92:15450 SIP/2.0
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Via: SIP/2.0/UDP 140.113.27.54;branch=0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 69
From: "bean@140.113.27.54"<sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
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]



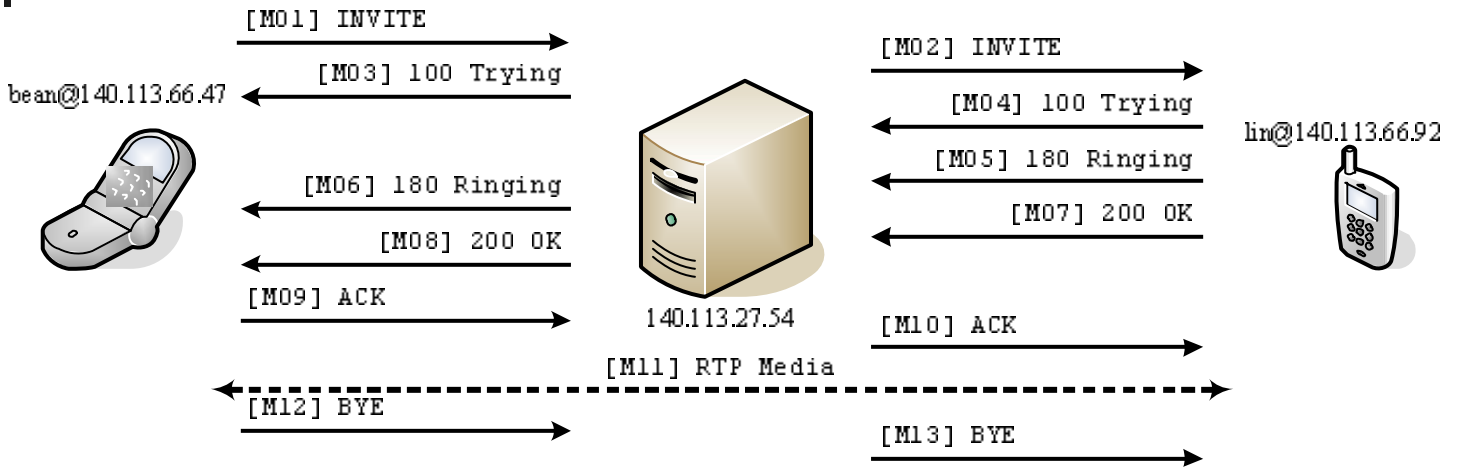


Call Message Flow [12/15]



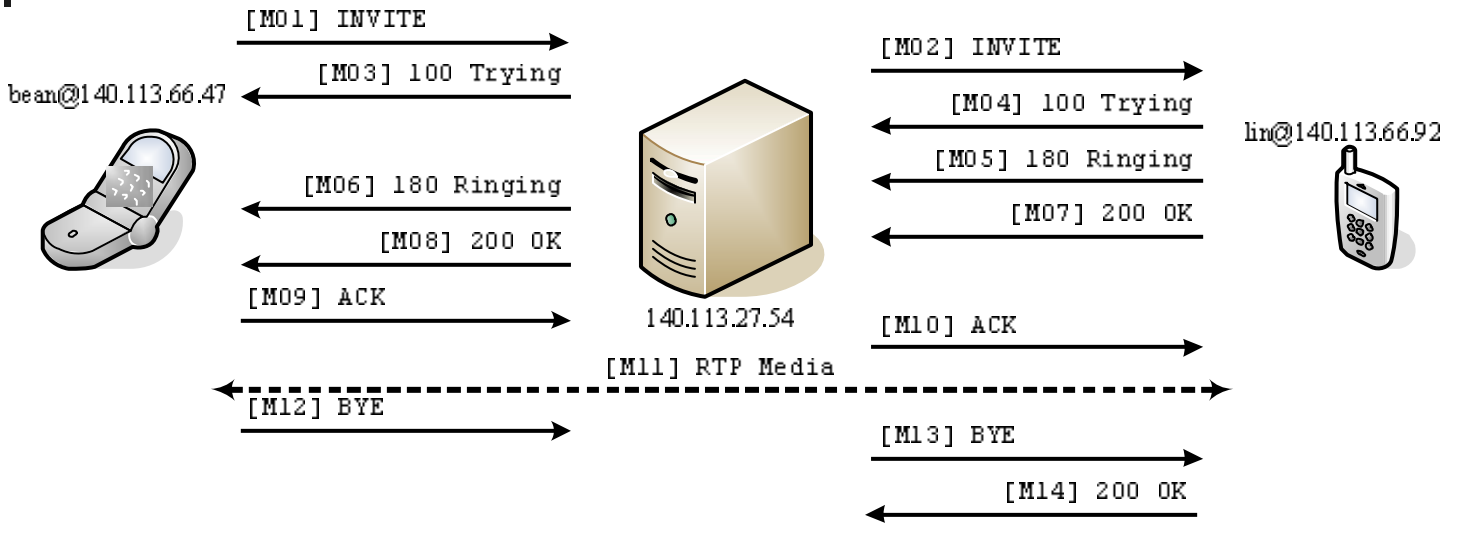

```
[M12]
BYE sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on SIP/2.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 70
From: "bear@140.113.27.54" <sip:bear@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
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]



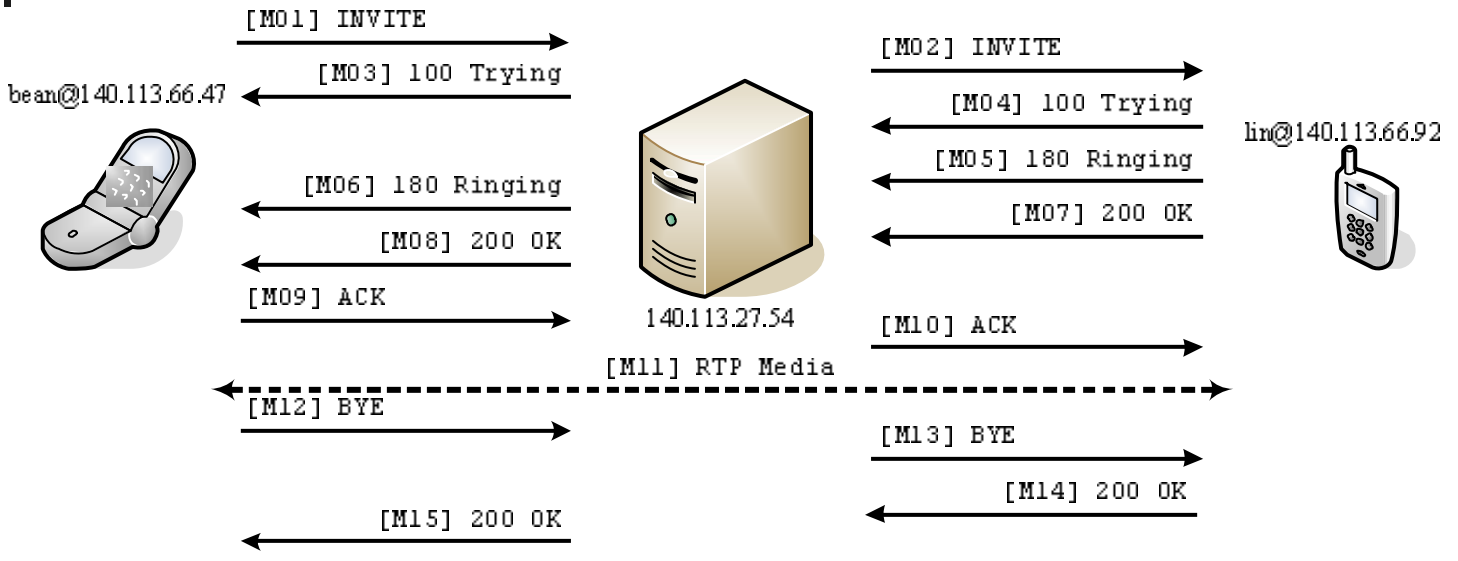

```
[M13]
BYE sip:140.113.66.92:15450 SIP/2.0
Record-Route: <sip:lin@140.113.27.54;ftag=4465847a8df4466ab7bf4cd21f4ef1f5;lr=on>
Via: SIP/2.0/UDP 140.113.27.54;branch=z9hG4bK644c.887cba62.0
Via: SIP/2.0/UDP 140.113.66.47:12264
Max-Forwards: 69
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
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]

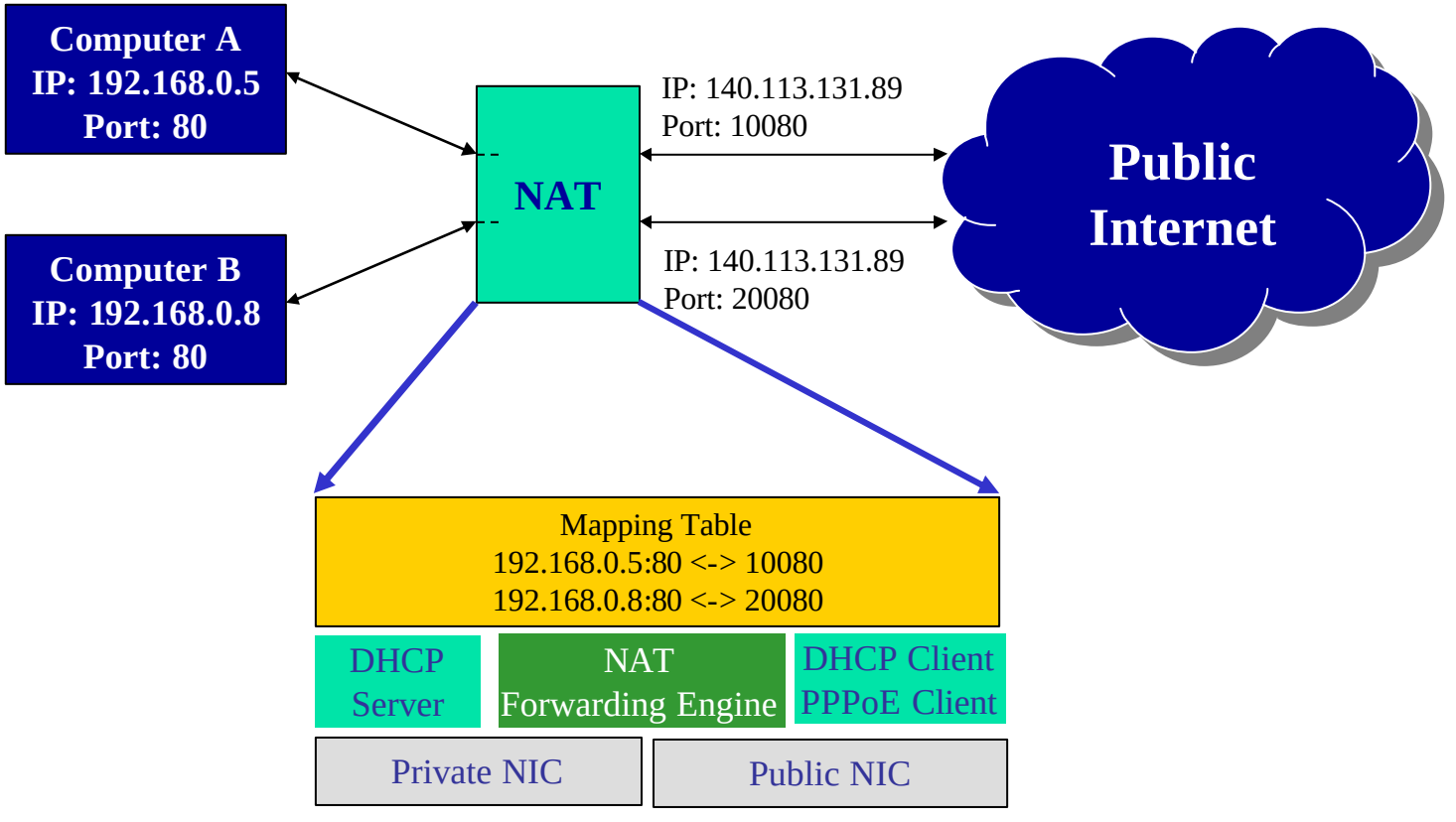



```
[M15]
SIP/2.0 200 OK
Via: SIP/2.0/UDP 140.113.66.47:12264
From: "bean@140.113.27.54" <sip:bean@140.113.27.54>;tag=4465847a8df4466ab7bf4cd21f4ef1f5;epid=04de356250
To: <sip:lin@140.113.27.54>;tag=adb6b6c3-bed2-4113-8cc0-2495ee252a5a
Call-ID: 383b5cdc4c784113b07e223f2f3a23c8@140.113.66.47
CSeq: 2 BYE
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

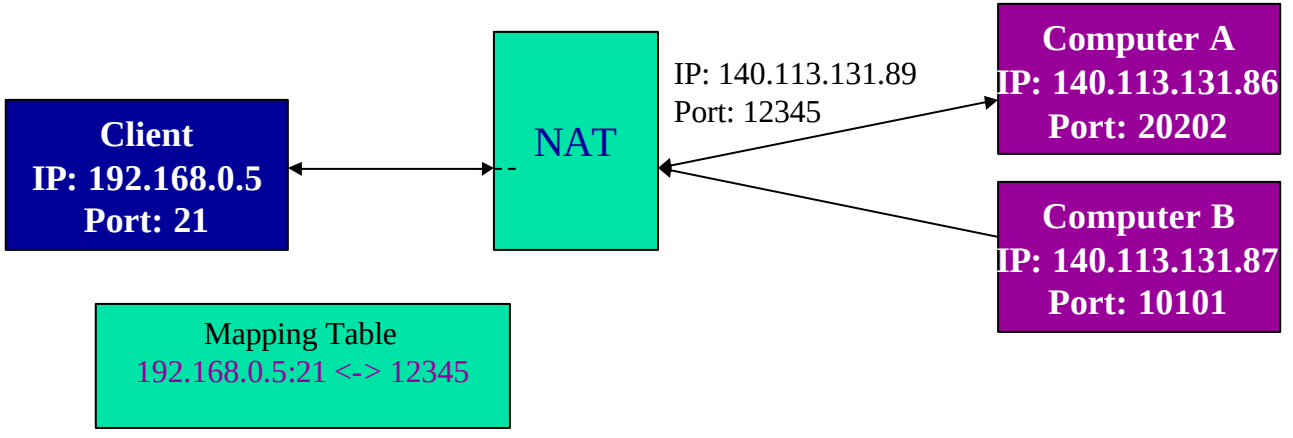


Types of NAT

- **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

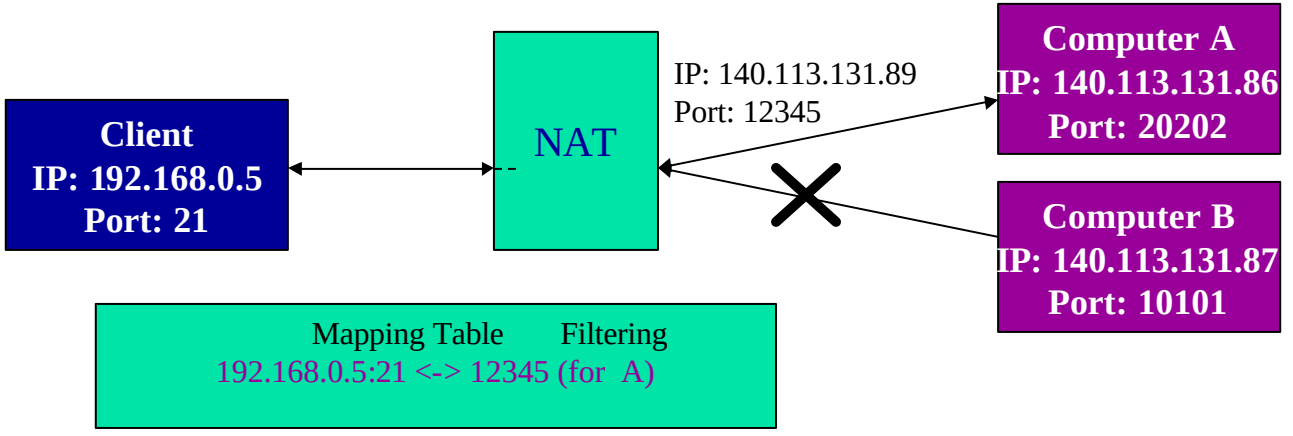
Fully Cone NAT

- 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.



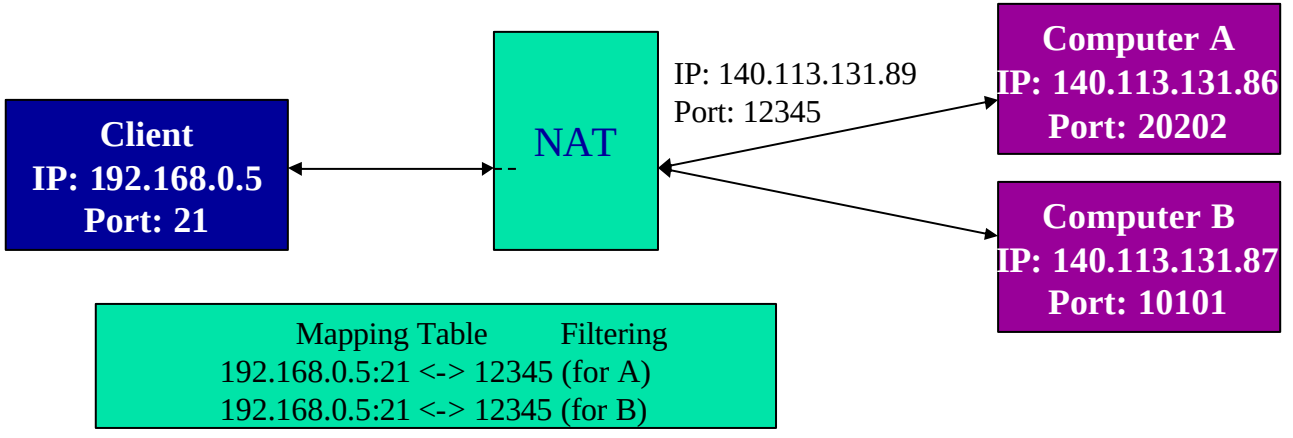
Restricted Cone NAT (1/2)

- 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.



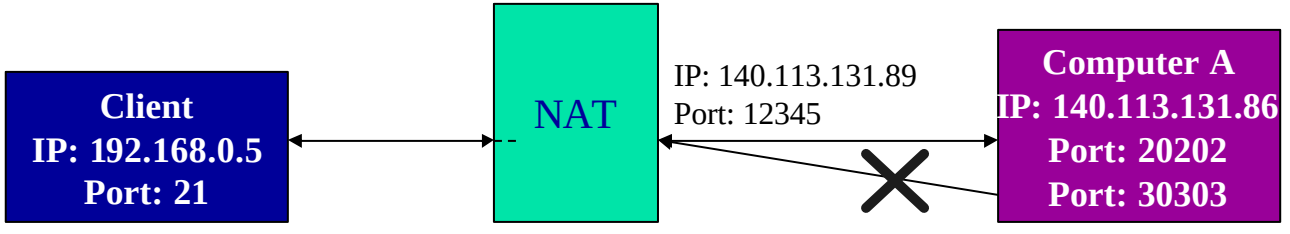
Restricted Cone NAT (2/2)

- 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

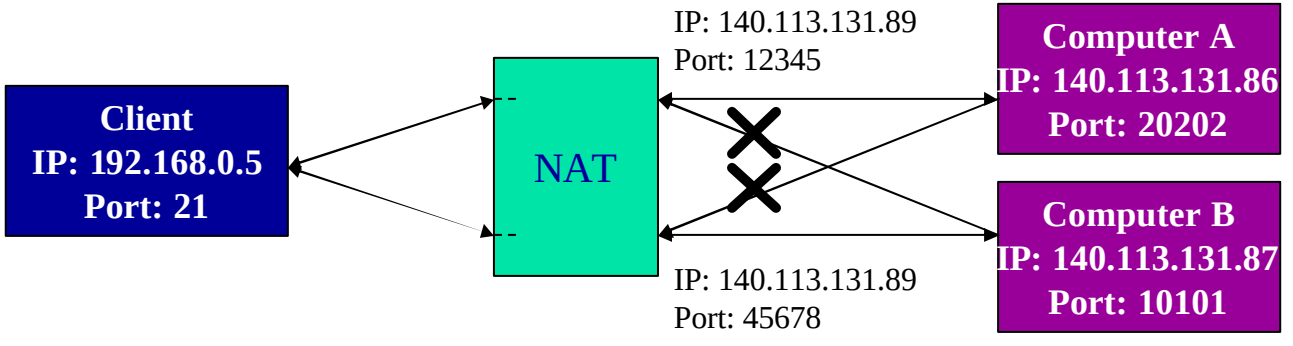
- Client sends a packet to public address A port 20202.
- NAT will allocate a public port (12345) for private port (21) on the client.
- Only incoming packet from address A and port 20202 to public port (12345) will be dispatched to private port (21) on the client.



Mapping Table	Filtering
192.168.0.5:21 <-> 12345 (for A : 20202)	
192.168.0.5:21 <-> 12345 (for A : 30303)	

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



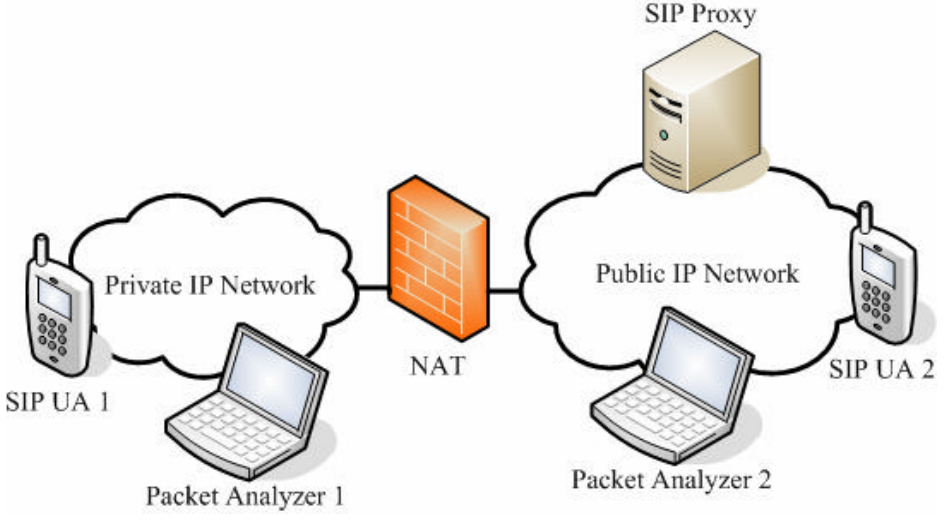
Mapping Table	Filtering
192.168.0.5:21 <-> 12345	(for A : 20202)
192.168.0.5:21 <-> 45678	(for B : 10101)

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

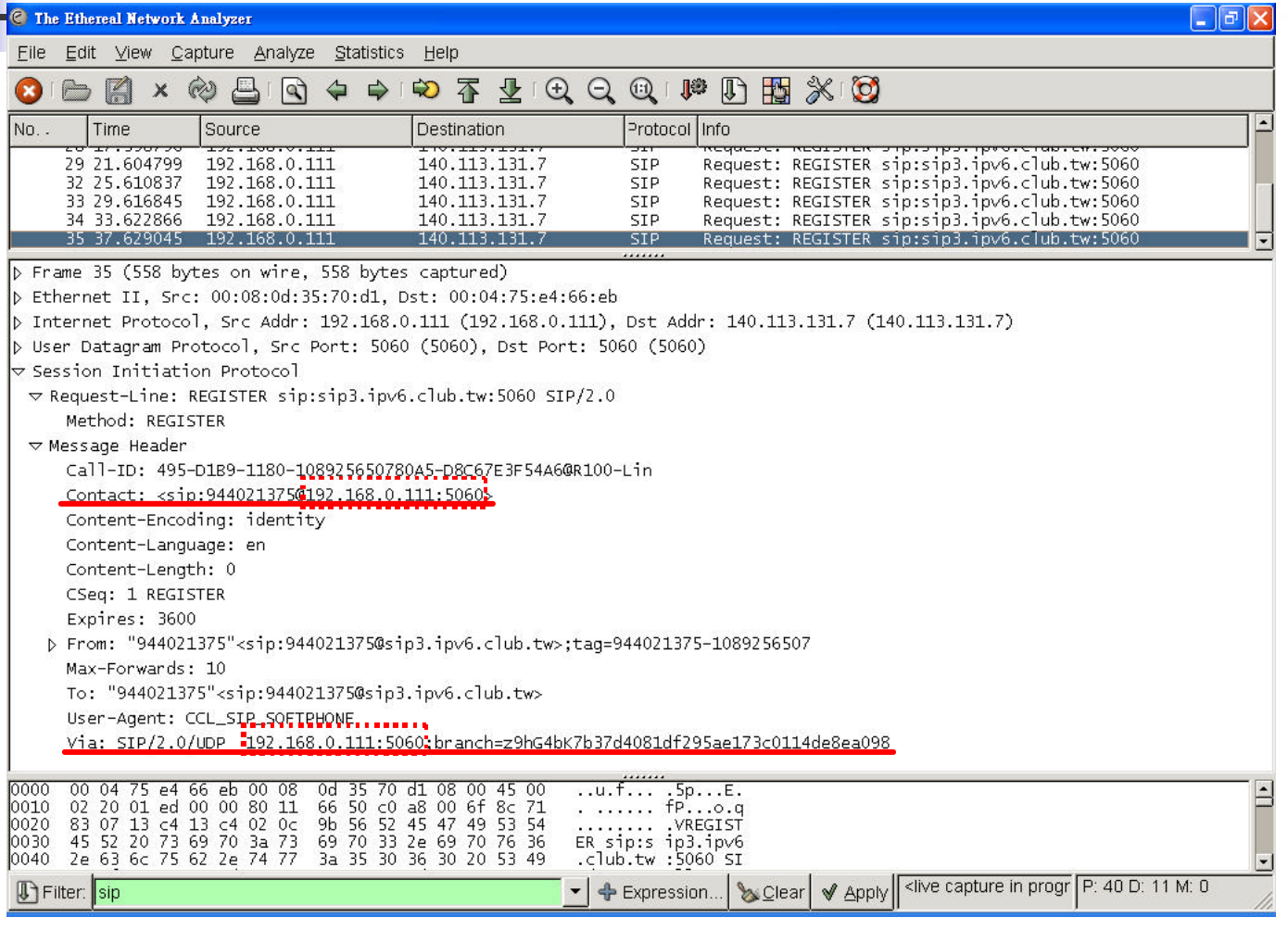
- SIP UA 1: User Agent behind NAT (Private Domain).
- SIP UA 2: SIP UA outside NAT (Public Domain).
- SIP Proxy: IPtel SIP Express Router (SER) v0.8.11.
- NAT: Windows XP with 2 NICs
- Packet Analyzer 1 & 2: Ethereal



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.

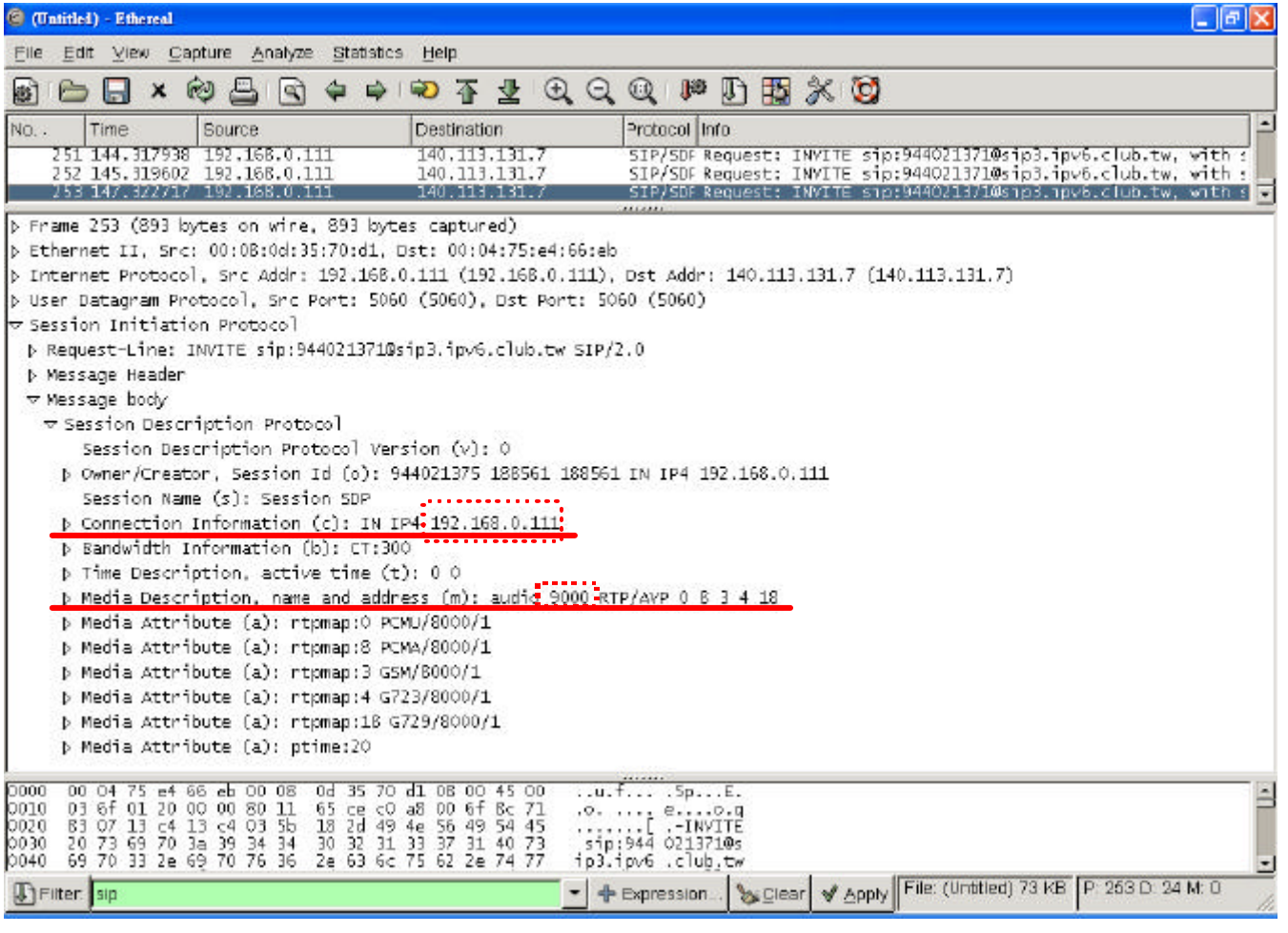
Incorrect REGISTER Message



The 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



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 addr ess & 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

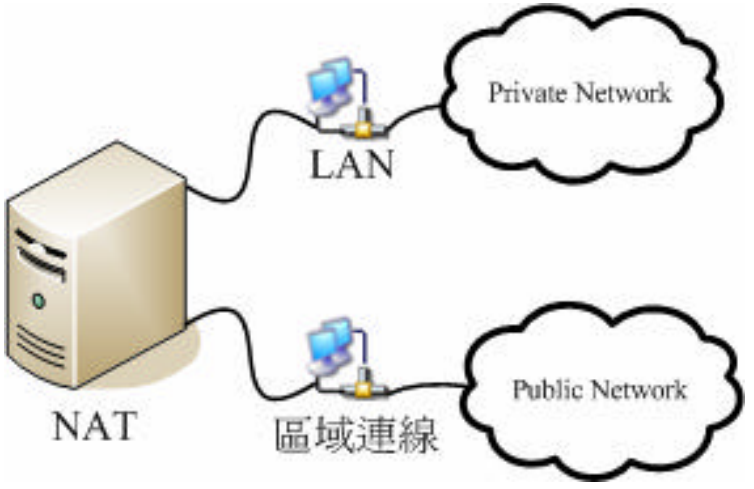
NAT Traversal Solutions

- 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

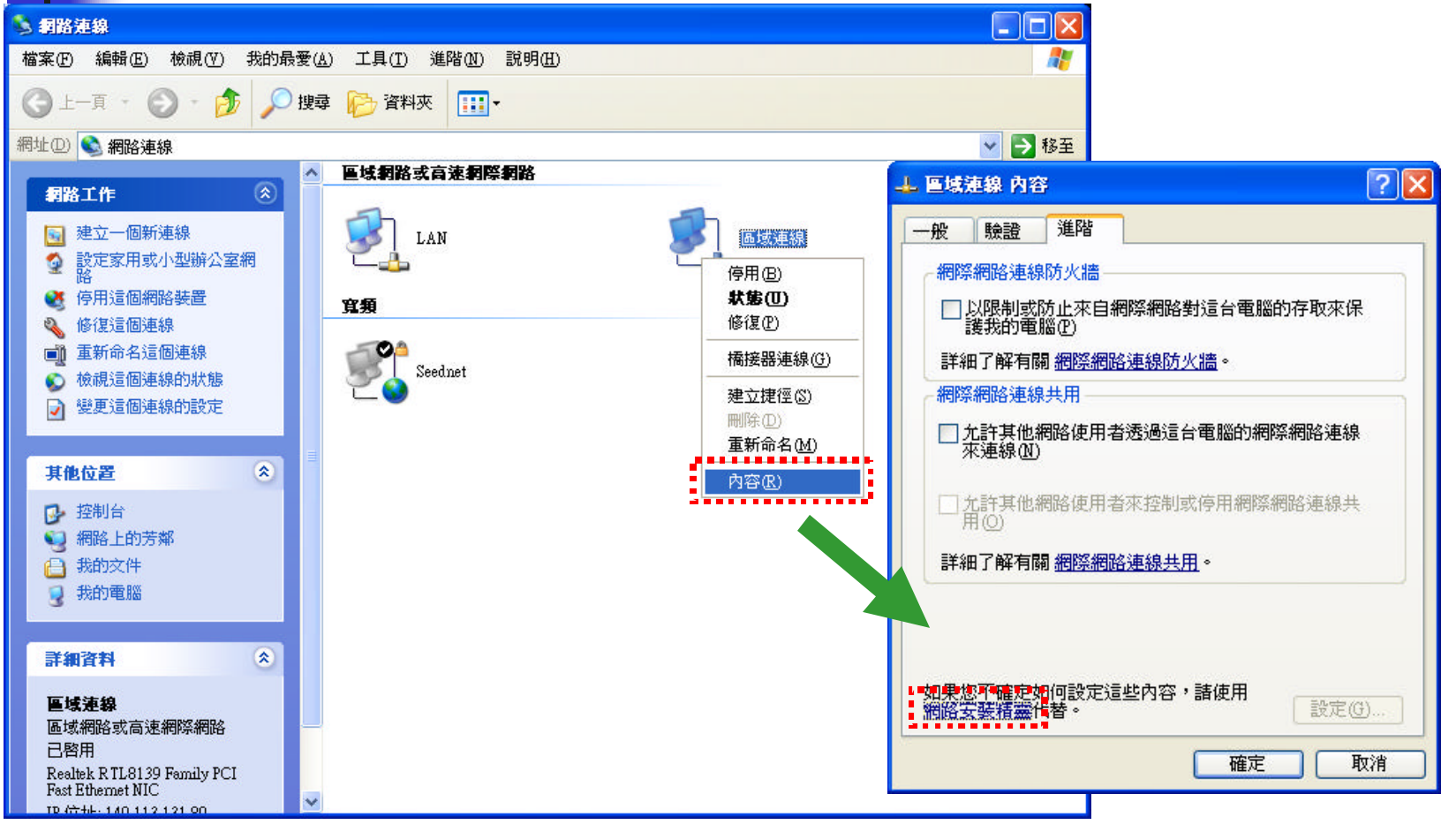
NAT Configuration-
Using Windows XP with 2 NICs

NAT of Windows XP with 2 NICs

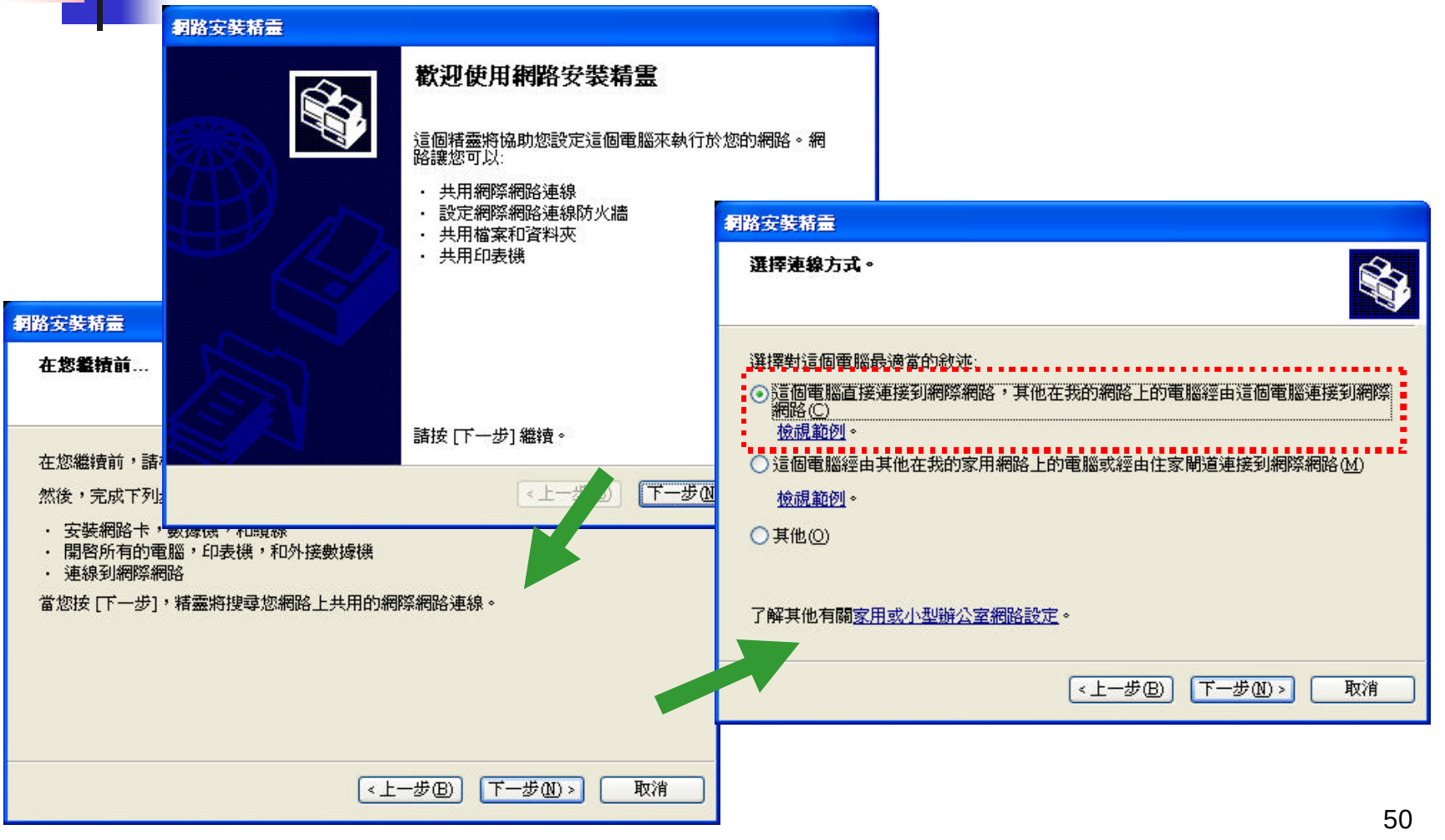
- **使用**Windows XP**架設**NAT**需要兩張網卡**
  - **區域連線**
  - **區域連線**2
- **將"區域連線"連接**NAT**內部網路**;**而"區域連線**2**"連接**NAT**外部網路**



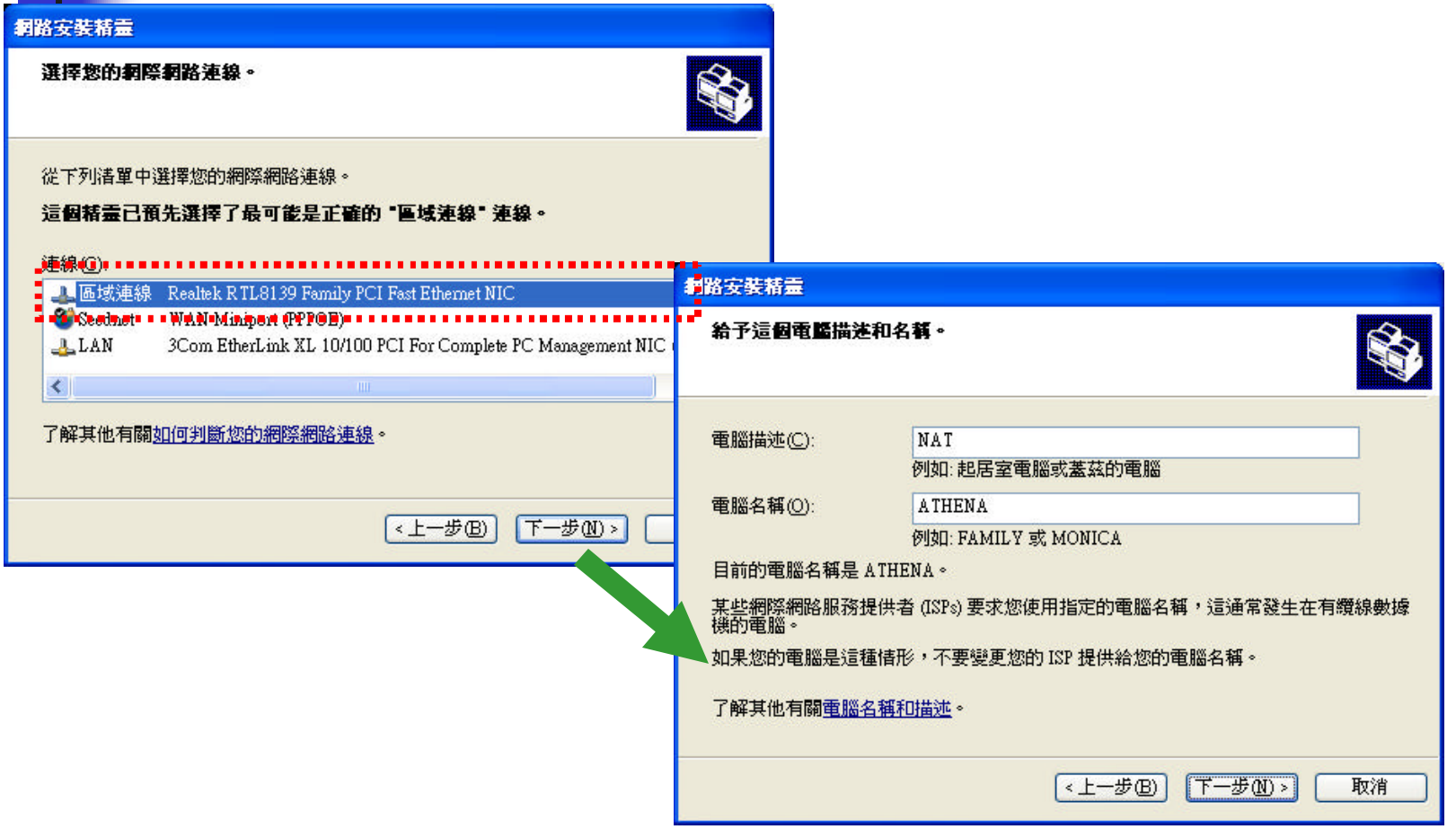
NAT of Windows XP Setup (1)



NAT of Windows XP Setup (2)



NAT of Windows XP Setup (3)



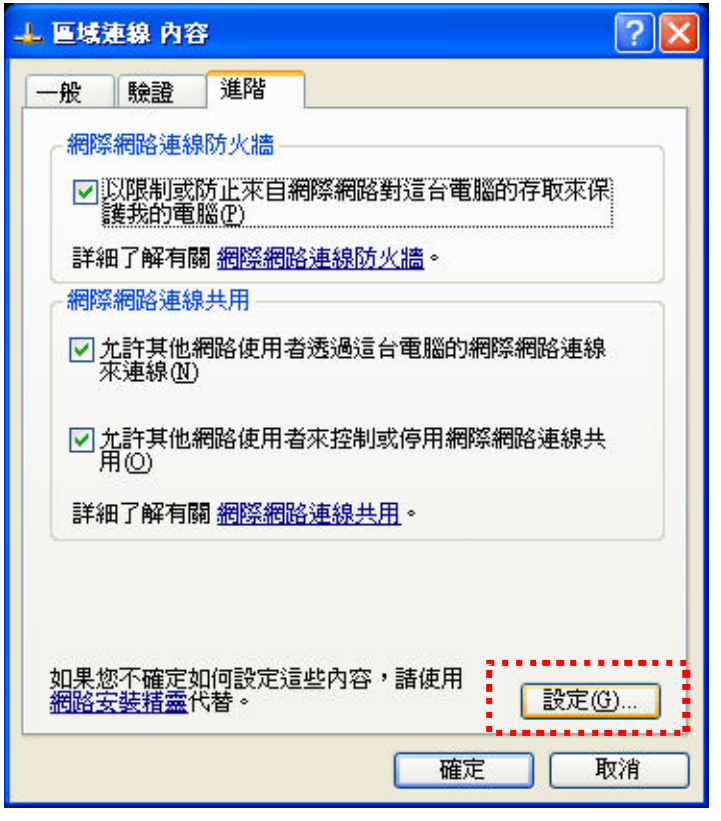
NAT of Windows XP Setup (4)

NAT of Windows XP Setup (5)

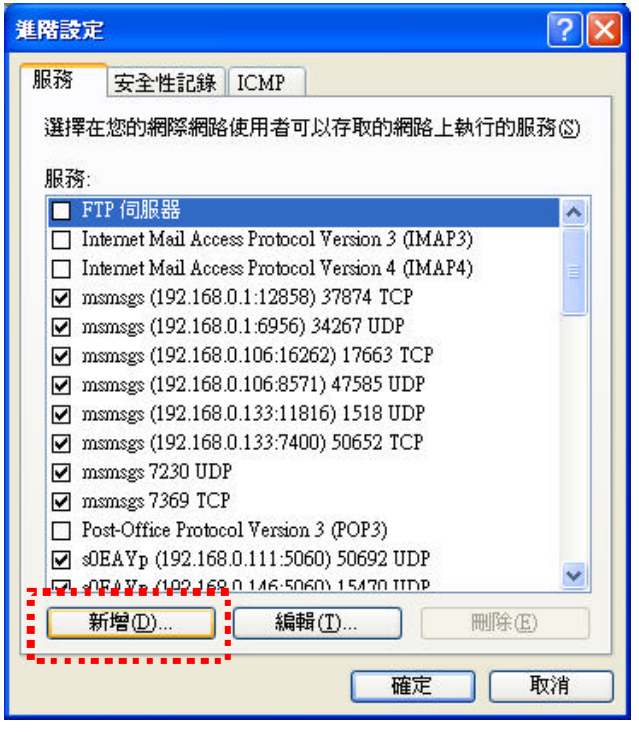
Static Mapping and Manual Configuration

Windows XP NAT Setup (1)

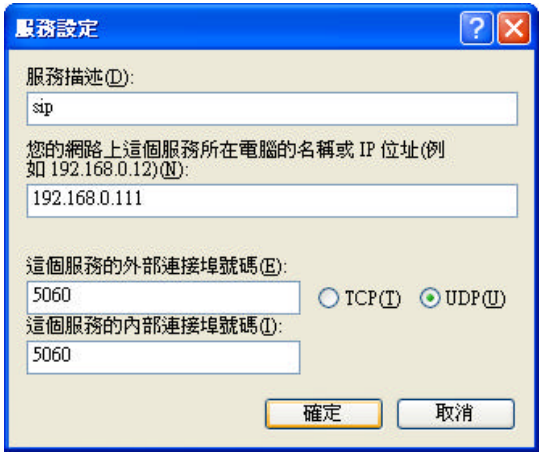
- **開啟NAT對外的連線介面, 於firewall上設定將NAT內部的port指定到特定NAT對外連線介面的port**



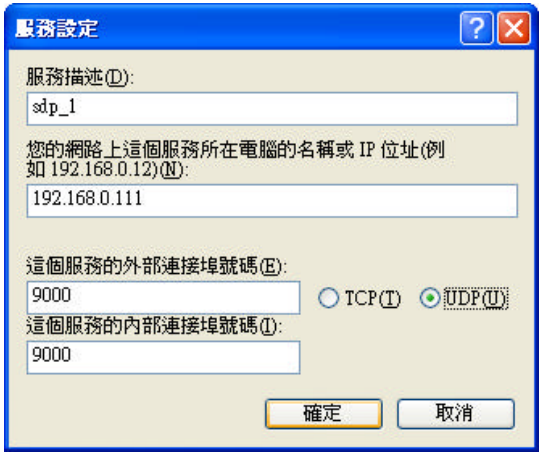
Windows XP NAT Setup (2)



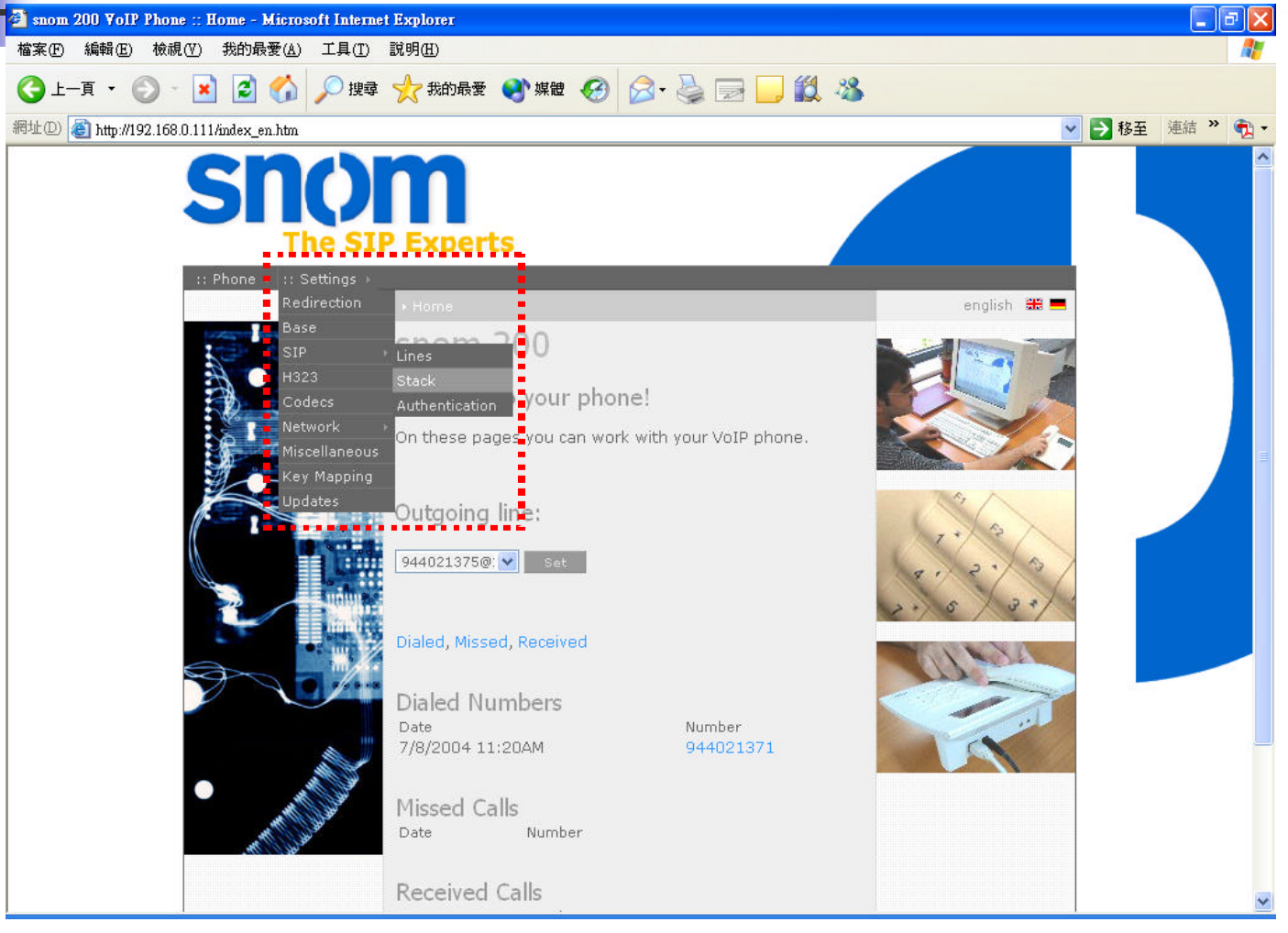
For SIP



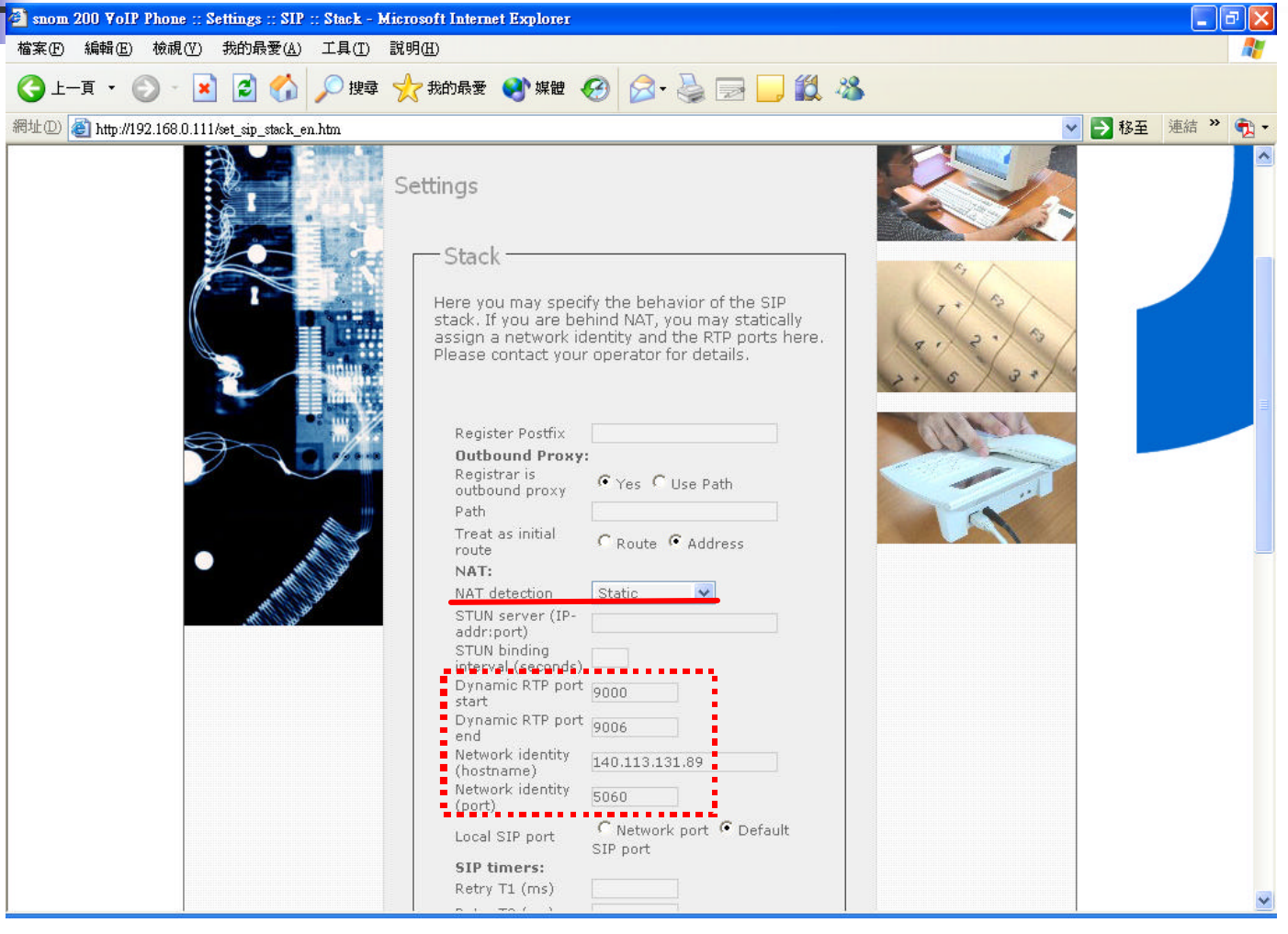
For RTP



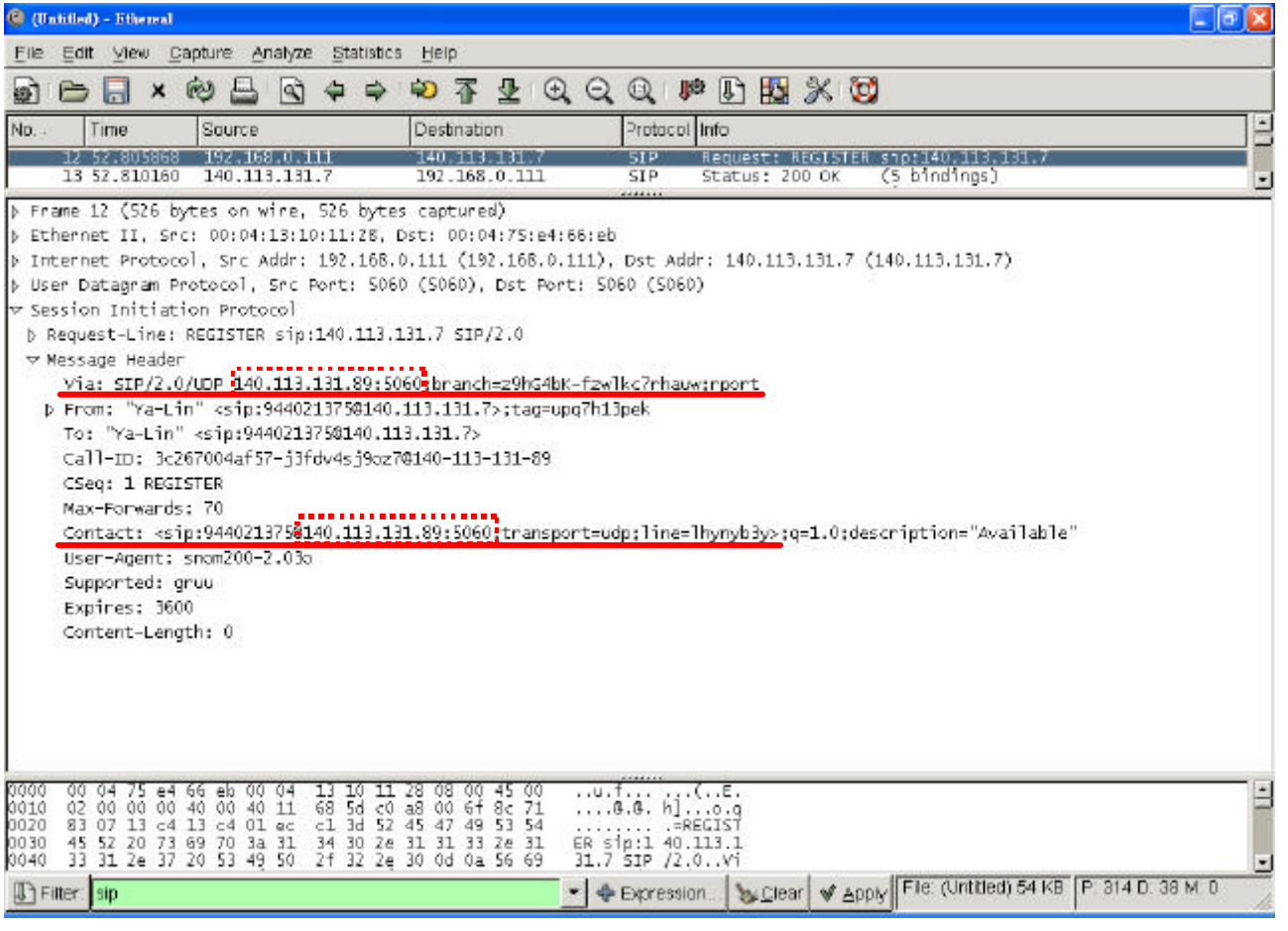
SIP UA Setup for Static Mapping (1)



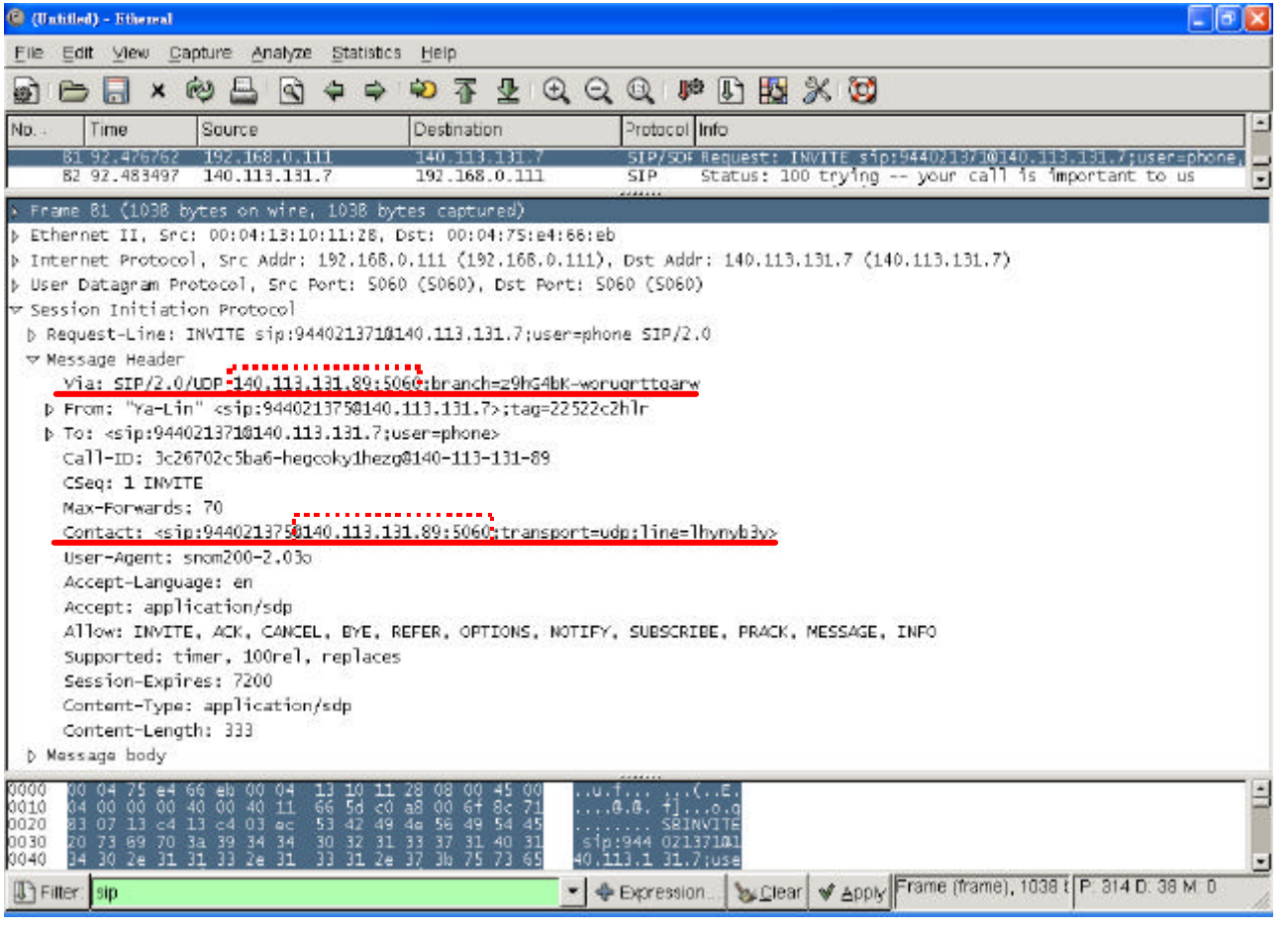
SIP UA Setup for Static Mapping (2)



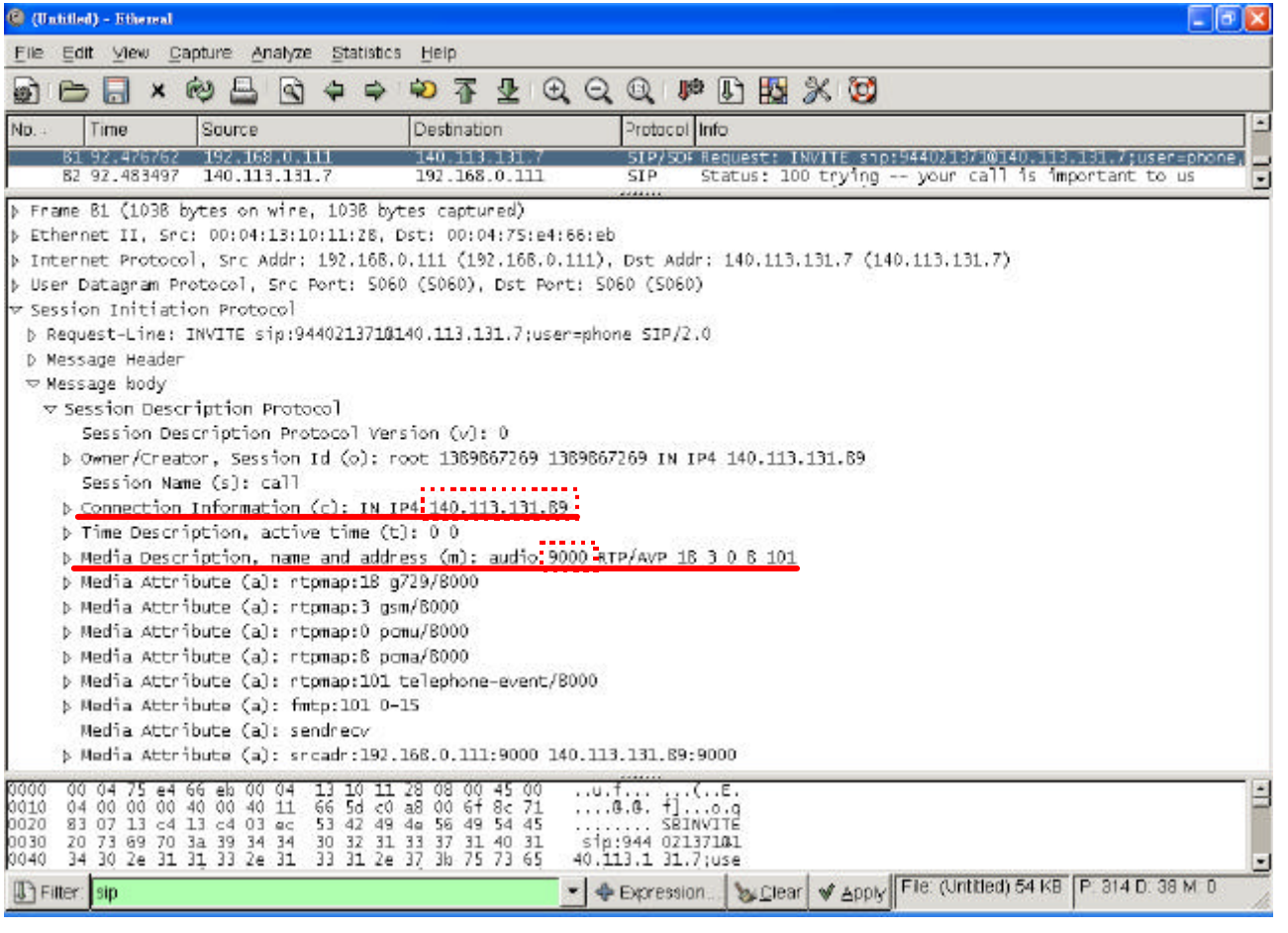
REGISTER Message



INVITE Message (SIP)

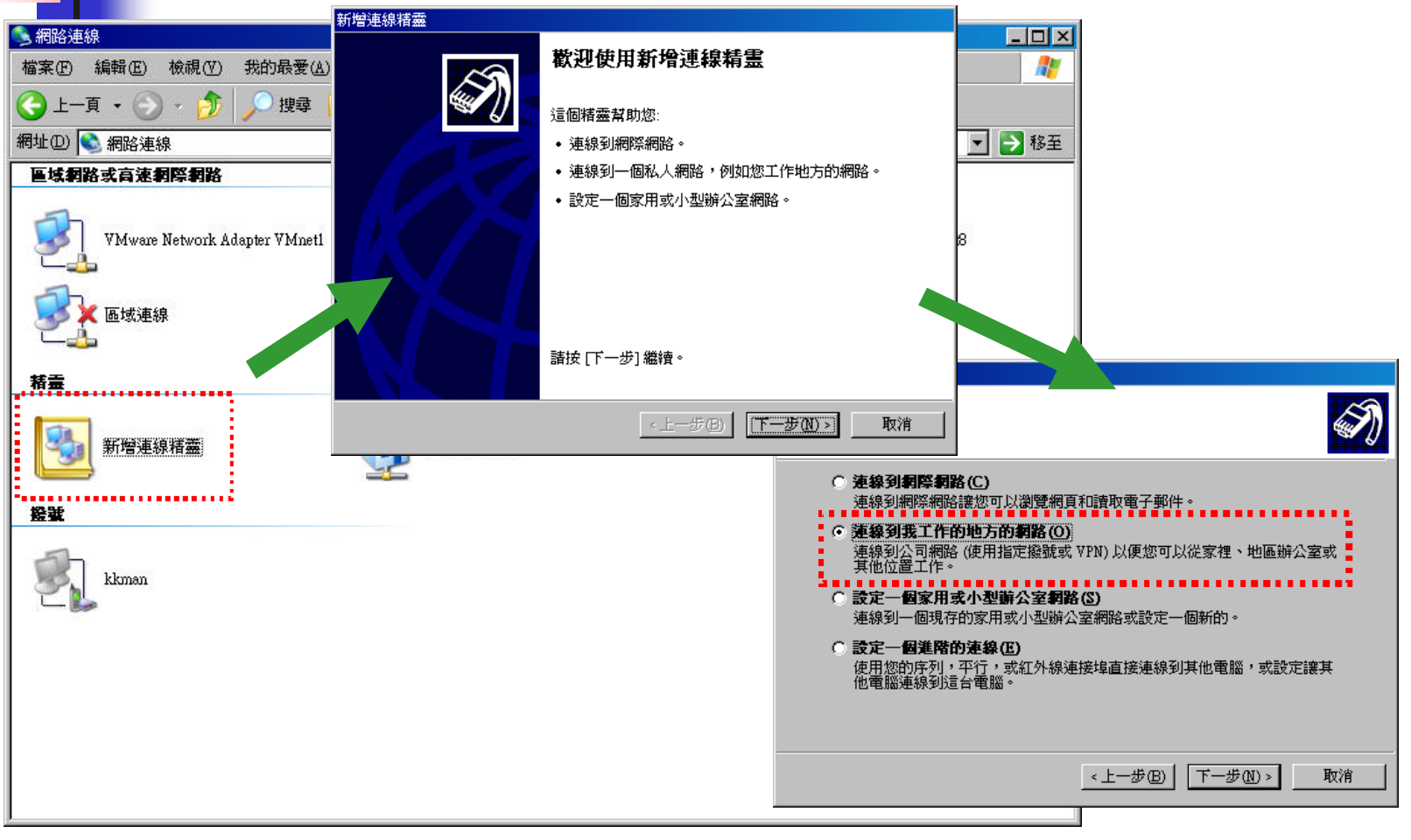


INVITE Message (SDP)

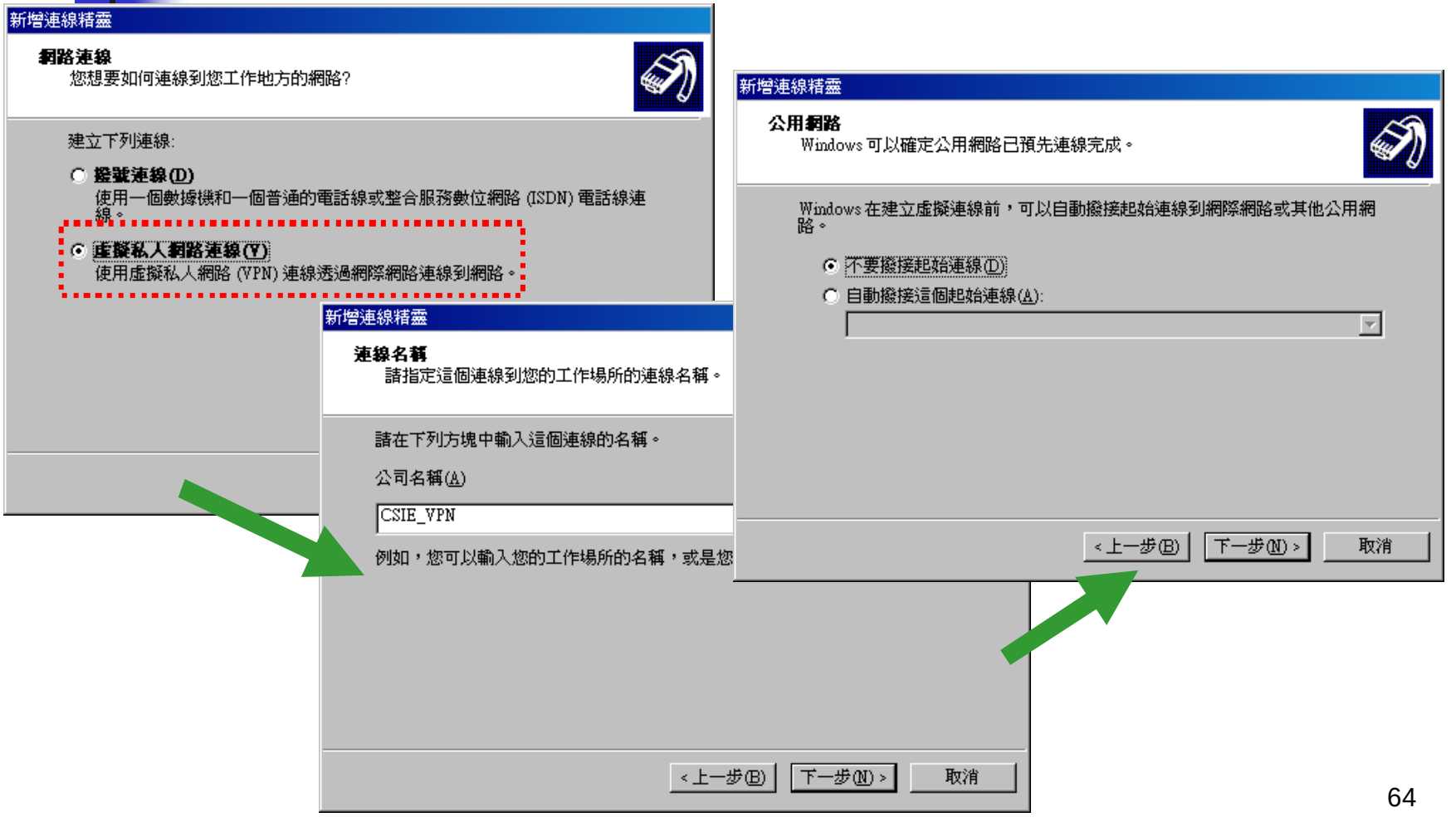


Virtual Private Network (VPN)

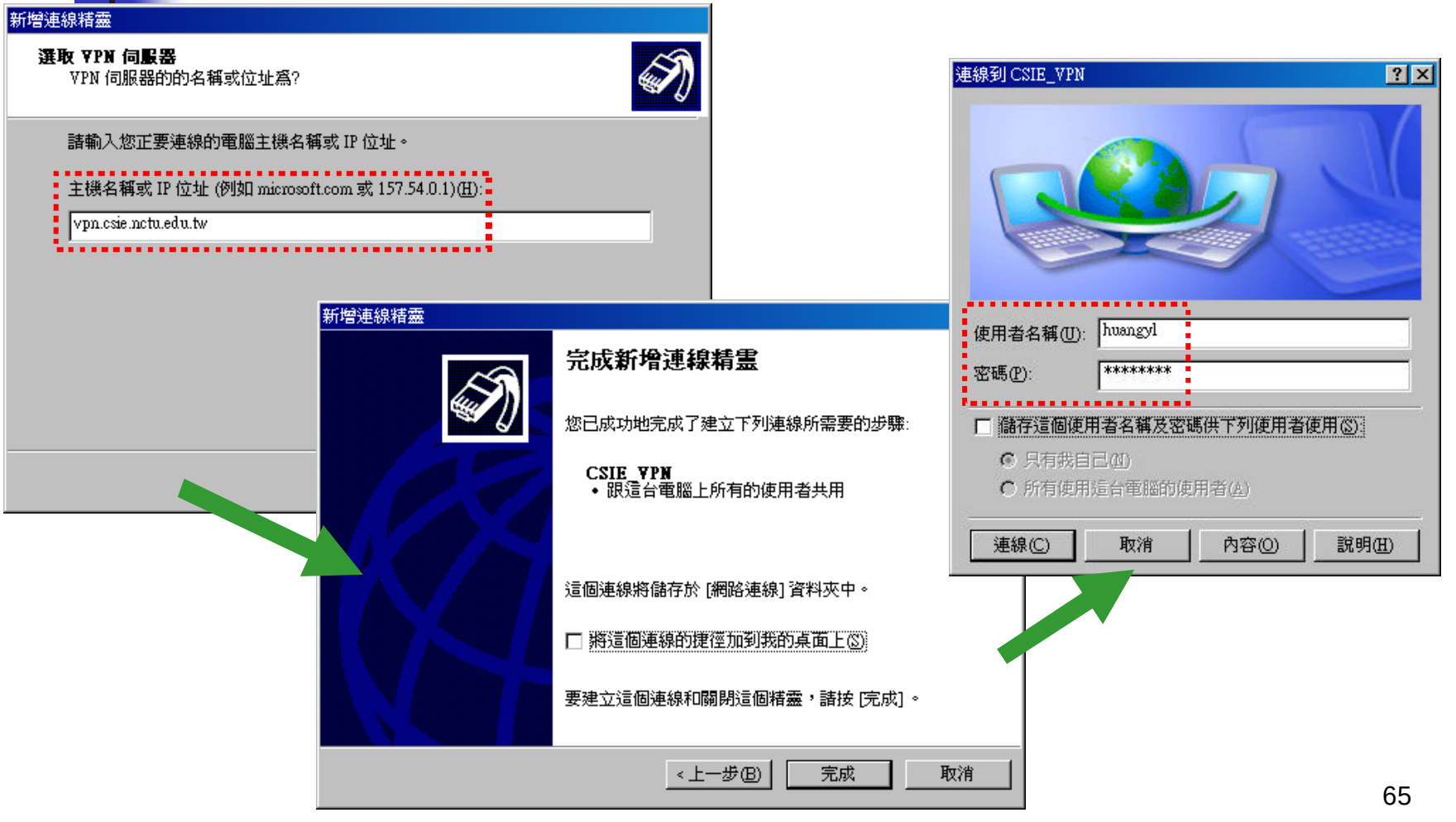
VPN Setup on Windows XP (1)



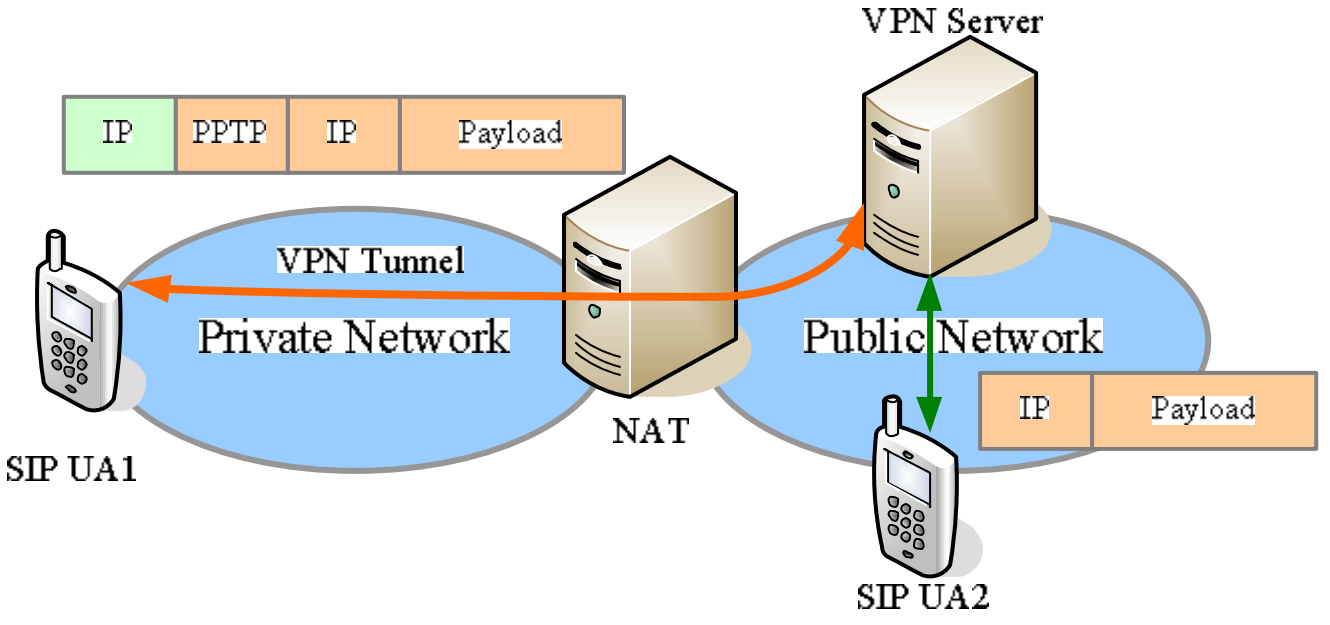
VPN Setup on Windows XP (2)



VPN Setup on Windows XP (3)



VPN


VPN Server
IP
PPTP
IP
Payload
VPN Tunnel
Private Network
Public Network
NAT
IP
Payload
SIP UA1
SIP UA2

Before Setup VPN Connection

Default Route

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          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        127.0.0.1       127.0.0.1       1
      192.168.0.0    255.255.255.0  192.168.0.111   192.168.0.111      20
    192.168.0.111  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.0.255  255.255.255.255  192.168.0.111   192.168.0.111      20
      192.168.5.0    255.255.255.0    192.168.5.1     192.168.5.1      20
      192.168.5.1  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.5.255  255.255.255.255    192.168.5.1     192.168.5.1      20
    192.168.153.0    255.255.255.0  192.168.153.1   192.168.153.1      20
    192.168.153.1  255.255.255.255        127.0.0.1       127.0.0.1      20
  192.168.153.255  255.255.255.255  192.168.153.1   192.168.153.1      20
        224.0.0.0        240.0.0.0  192.168.0.111   192.168.0.111      20
        224.0.0.0        240.0.0.0    192.168.5.1     192.168.5.1      20
        224.0.0.0        240.0.0.0  192.168.153.1   192.168.153.1      20
  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    192.168.5.1     192.168.5.1       1
  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  192.168.153.1               5       1
Default Gateway:       192.168.0.1
===========================================================================
Persistent Routes:
  None
```

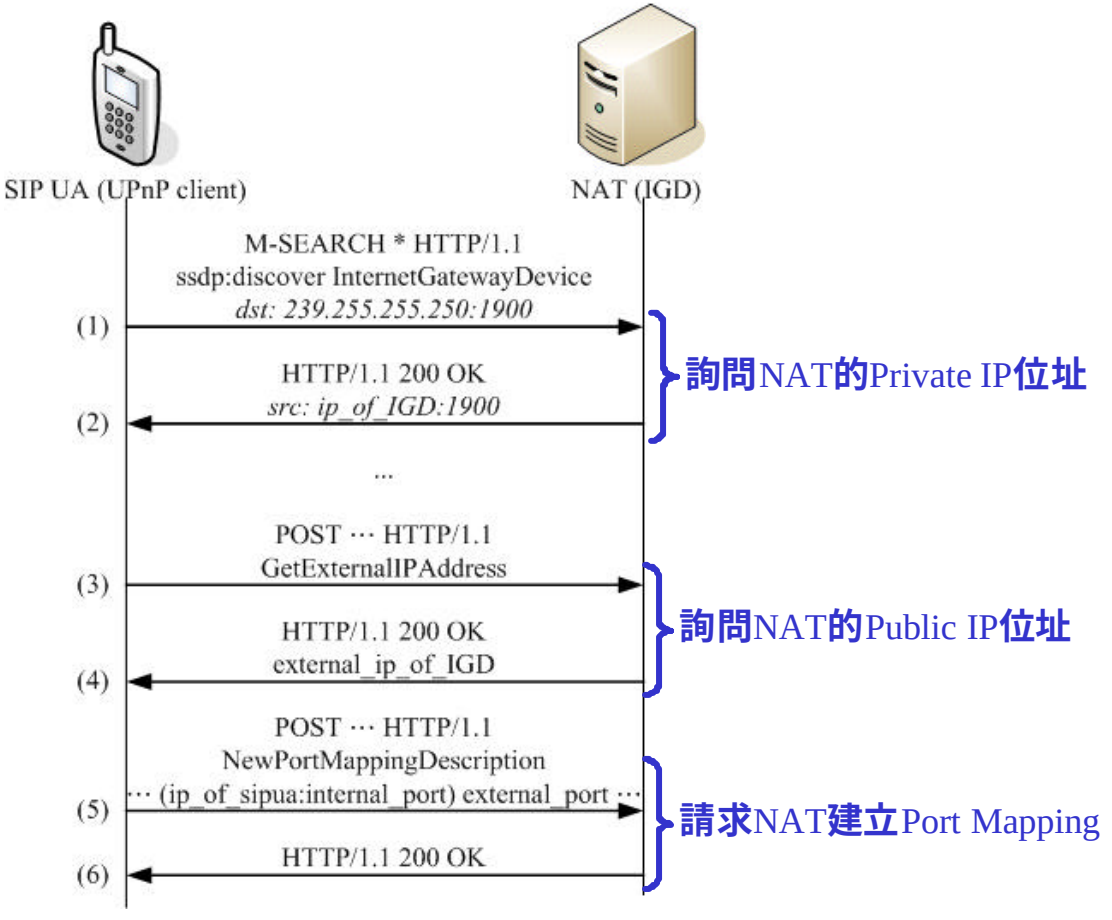
After Setup VPN Connection

Default Route

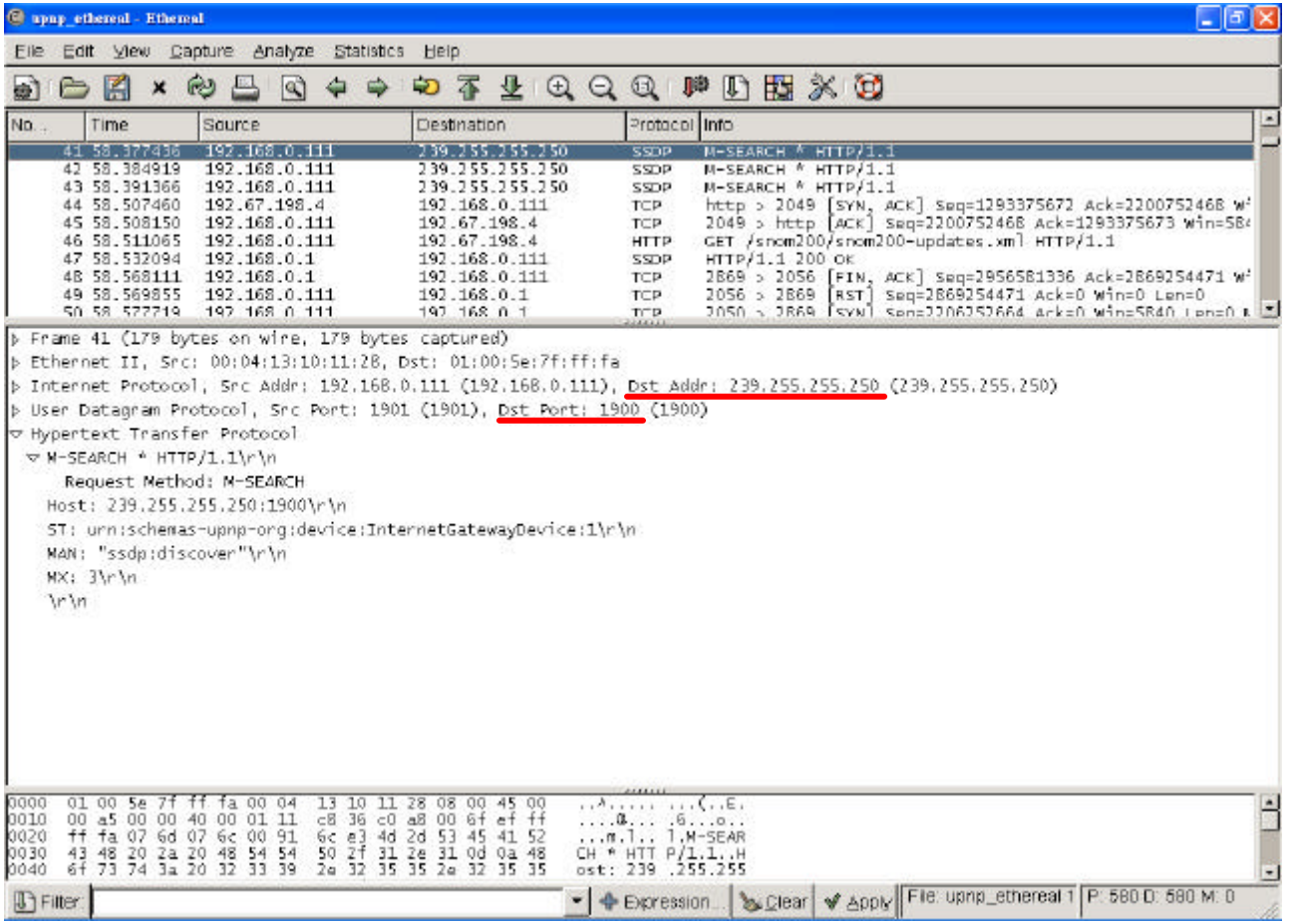
```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0  140.113.235.164  140.113.235.164      1
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.111     21
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
  140.113.235.164  255.255.255.255        127.0.0.1        127.0.0.1     50
  140.113.235.249  255.255.255.255      192.168.0.1    192.168.0.111     20
  140.113.255.255  255.255.255.255  140.113.235.164  140.113.235.164     50
      192.168.0.0    255.255.255.0    192.168.0.111    192.168.0.111     20
    192.168.0.111  255.255.255.255        127.0.0.1        127.0.0.1     20
    192.168.0.255  255.255.255.255    192.168.0.111    192.168.0.111     20
      192.168.5.0    255.255.255.0      192.168.5.1      192.168.5.1     20
      192.168.5.1  255.255.255.255        127.0.0.1        127.0.0.1     20
    192.168.5.255  255.255.255.255      192.168.5.1      192.168.5.1     20
    192.168.153.0    255.255.255.0    192.168.153.1    192.168.153.1     20
    192.168.153.1  255.255.255.255        127.0.0.1        127.0.0.1     20
  192.168.153.255  255.255.255.255    192.168.153.1    192.168.153.1     20
        224.0.0.0        240.0.0.0    192.168.0.111    192.168.0.111     20
        224.0.0.0        240.0.0.0      192.168.5.1      192.168.5.1     20
        224.0.0.0        240.0.0.0    192.168.153.1    192.168.153.1     20
        224.0.0.0        240.0.0.0  140.113.235.164  140.113.235.164      1
  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      192.168.5.1      192.168.5.1      1
  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    192.168.153.1                5      1
Default Gateway:   140.113.235.164
===========================================================================
Persistent Routes:
  None
```

UPnP – Universal Plug-and-Play

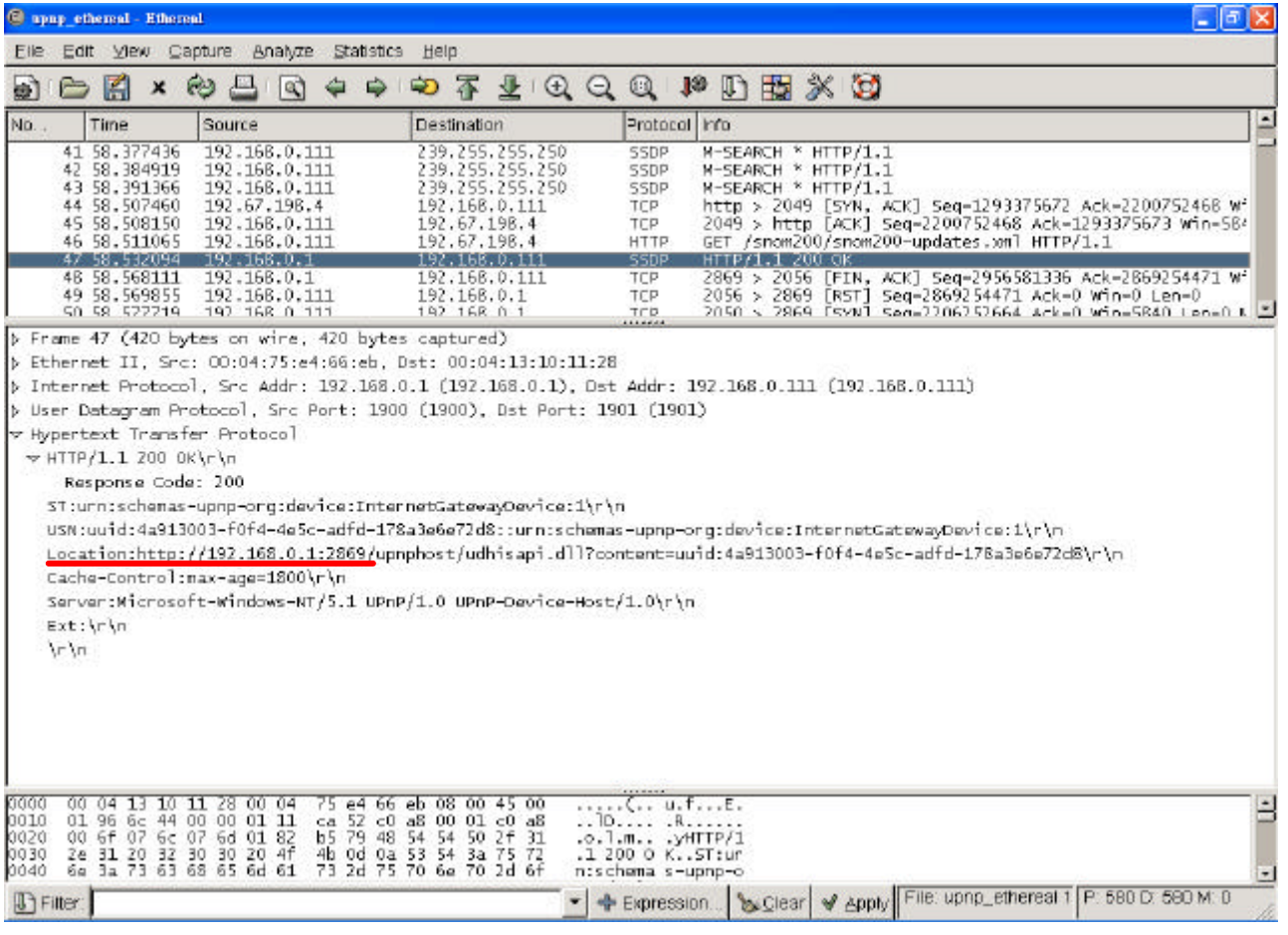
UPnP 運作流程


SIP UA (UPnP client)
NAT (IGD)
M-SEARCH * HTTP/1.1
ssdp:discover InternetGatewayDevice
dst: 239.255.255.250:1900
(1)
HTTP/1.1 200 OK
src: ip_of_IGD:1900
(2)
...
POST ··· HTTP/1.1
GetExternalIPAddress
(3)
HTTP/1.1 200 OK
external_ip_of_IGD
(4)
POST ··· HTTP/1.1
NewPortMappingDescription
··· (ip_of_sipua:internal_port) external_port ···
(5)
HTTP/1.1 200 OK
(6)
詢問NAT的Private IP位址
詢問NAT的Public IP位址
請求NAT建立Port Mapping

SSDP Discover Message (1)



SSDP Discover Message (2)



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>
```

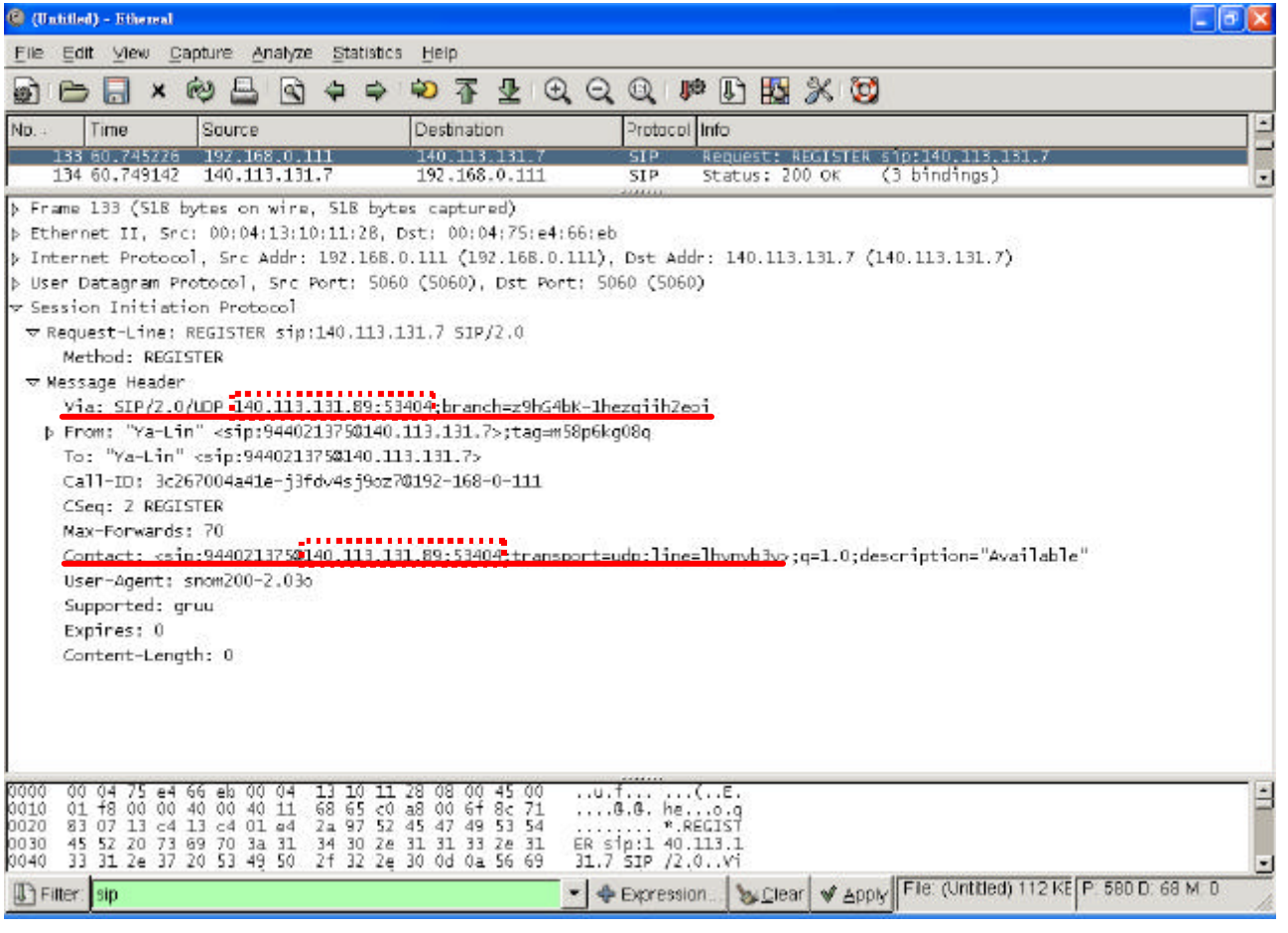
```
HTTP/1.0 200 OK
Date: Wed, 07 Jul 2004 08:15:40 GMT
Connection: close
Server: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
Content-Length: 305
Content-Type: text/xml; charset="utf-8"
EXT:

<?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>
```

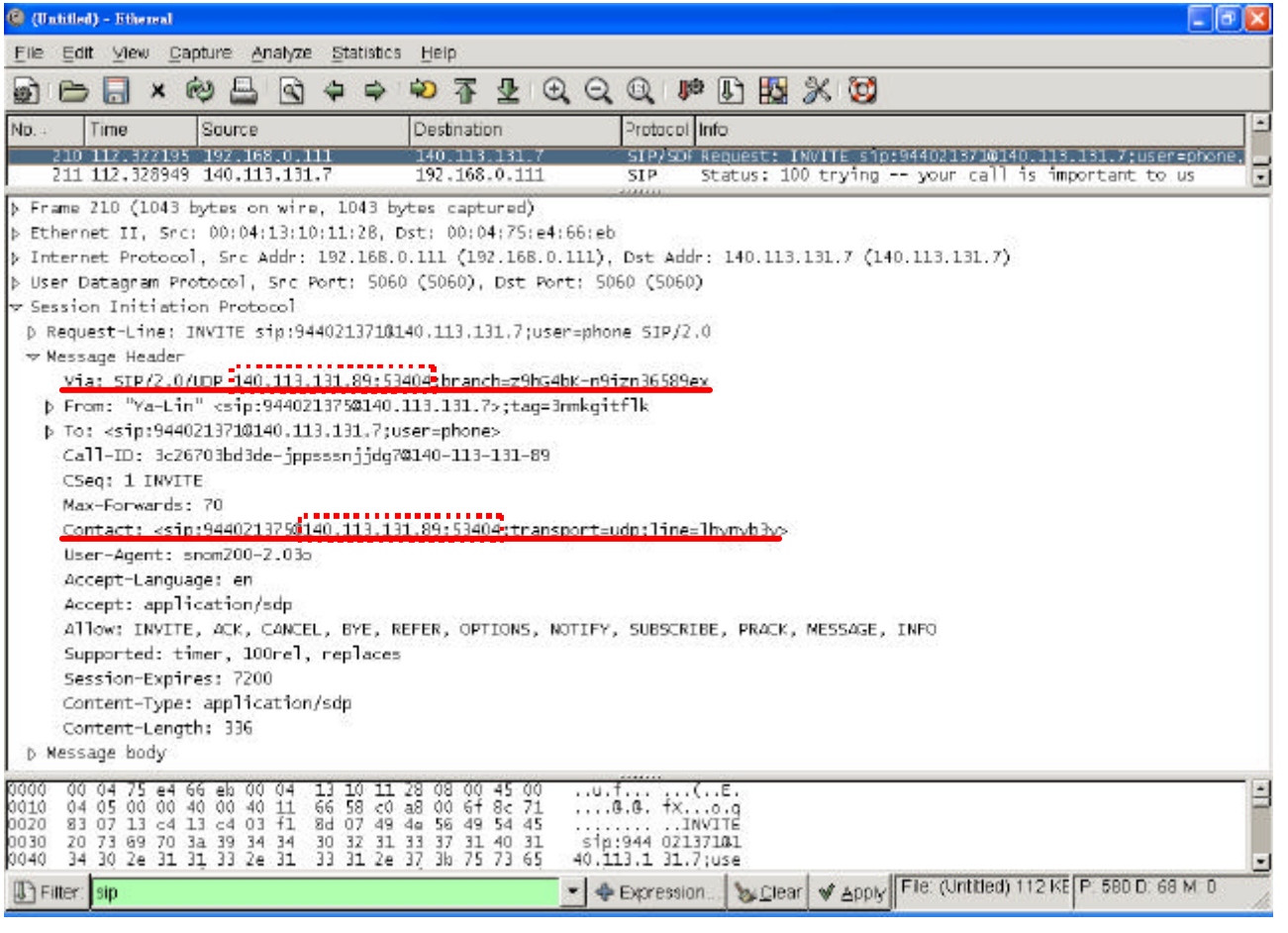
Current Defects of UPnP

- **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**

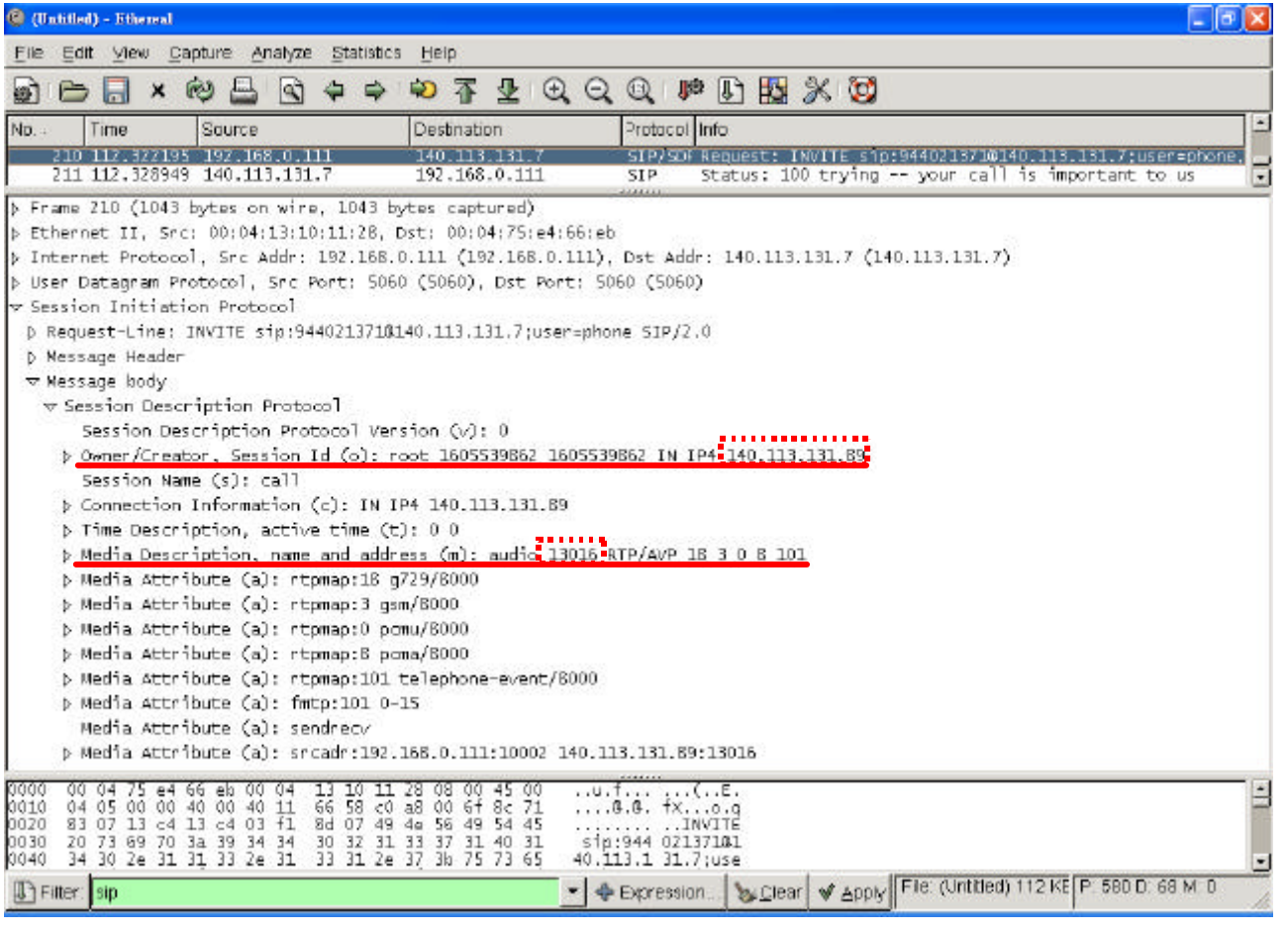
REGISTER Message



INVITE Message (SIP)



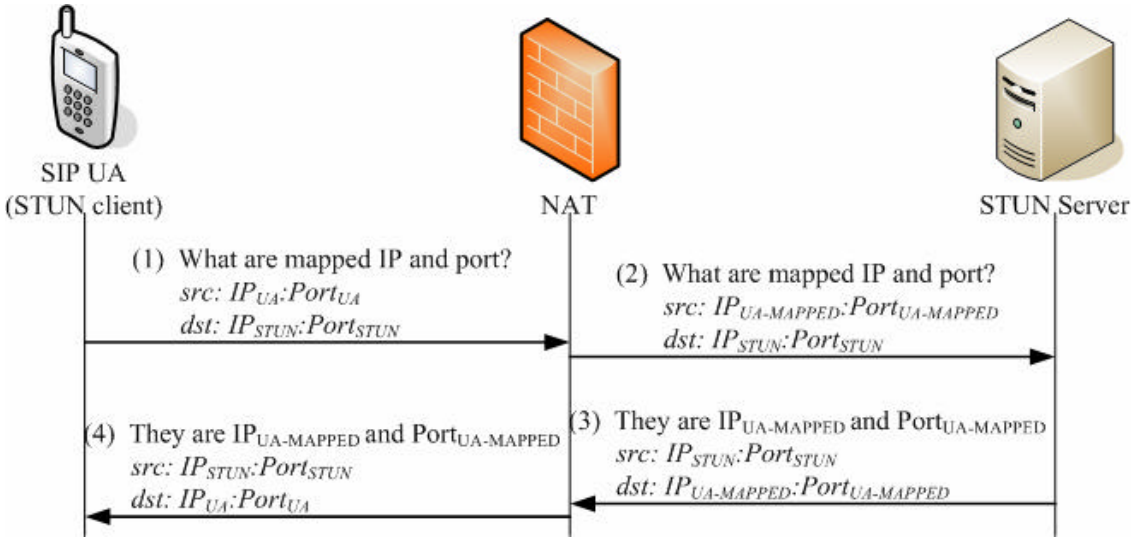
INVITE Message (SDP)



Simple Traversal of UDP through NAT (STUN)

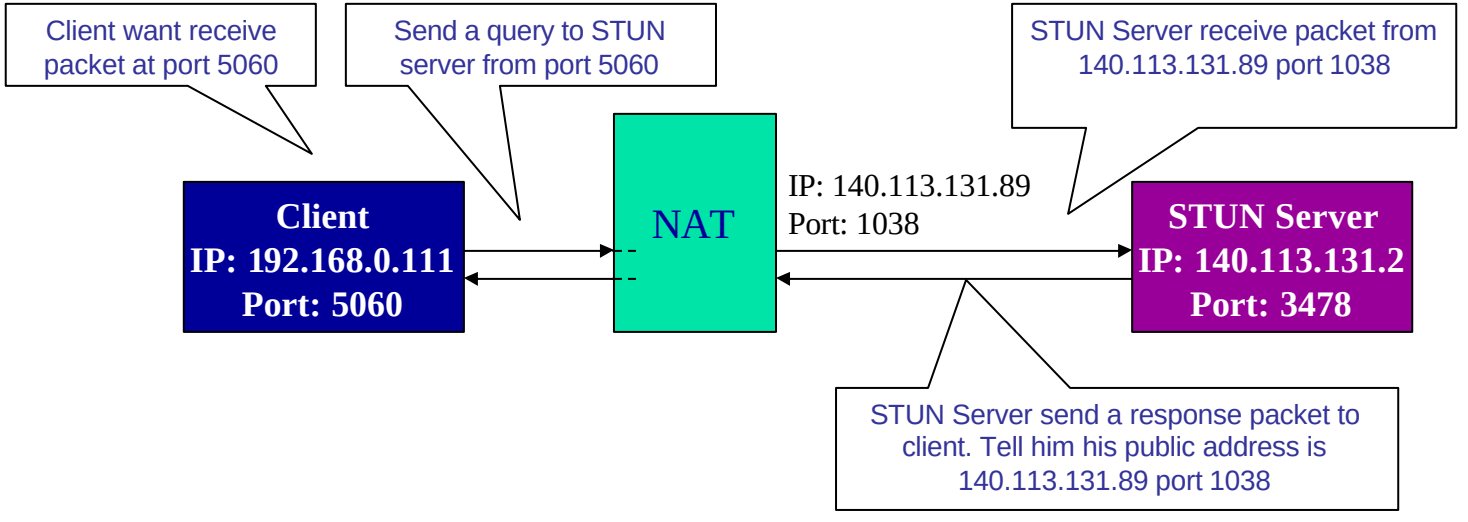
STUN (RFC 3489)

- 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.


SIP UA
(STUN client)
NAT
STUN Server
(1) What are mapped IP and port?
src: IP_UA:Port_UA
dst: IP_STUN:Port_STUN
(2) What are mapped IP and port?
src: IP_UA-MAPPED:Port_UA-MAPPED
dst: IP_STUN:Port_STUN
(3) They are IP_UA-MAPPED and Port_UA-MAPPED
src: IP_STUN:Port_STUN
dst: IP_UA-MAPPED:Port_UA-MAPPED
(4) They are IP_UA-MAPPED and Port_UA-MAPPED
src: IP_STUN:Port_STUN
dst: IP_UA:Port_UA

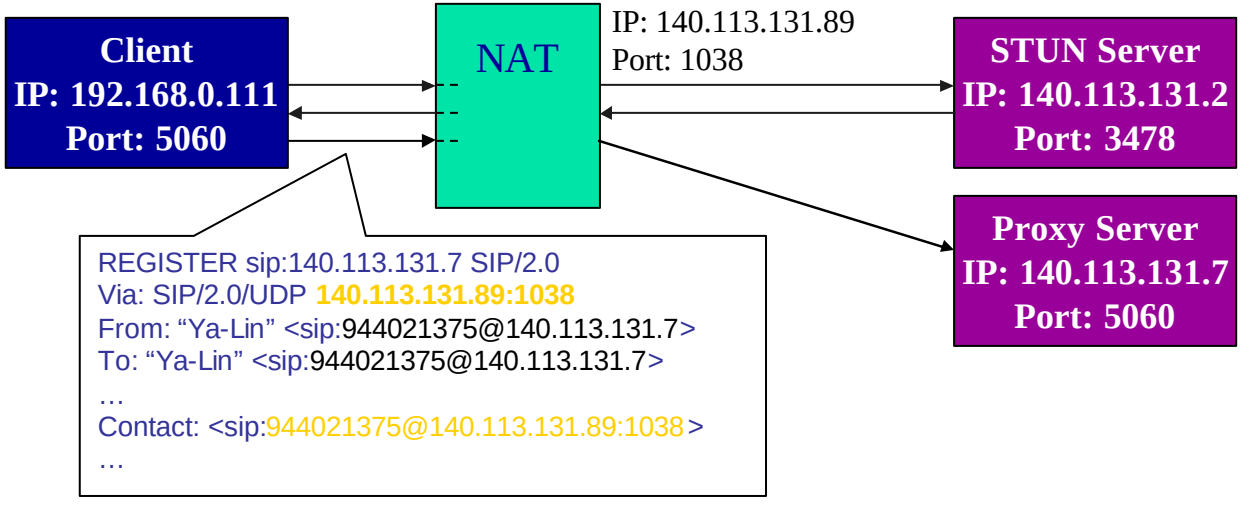
STUN Server

- 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

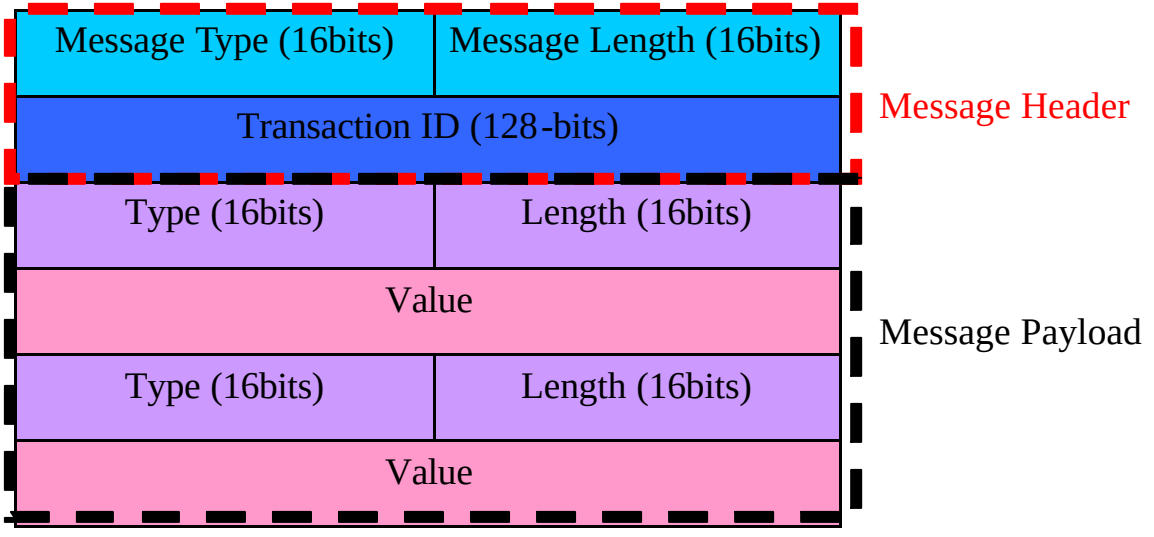


Use STUN for SIP Registration

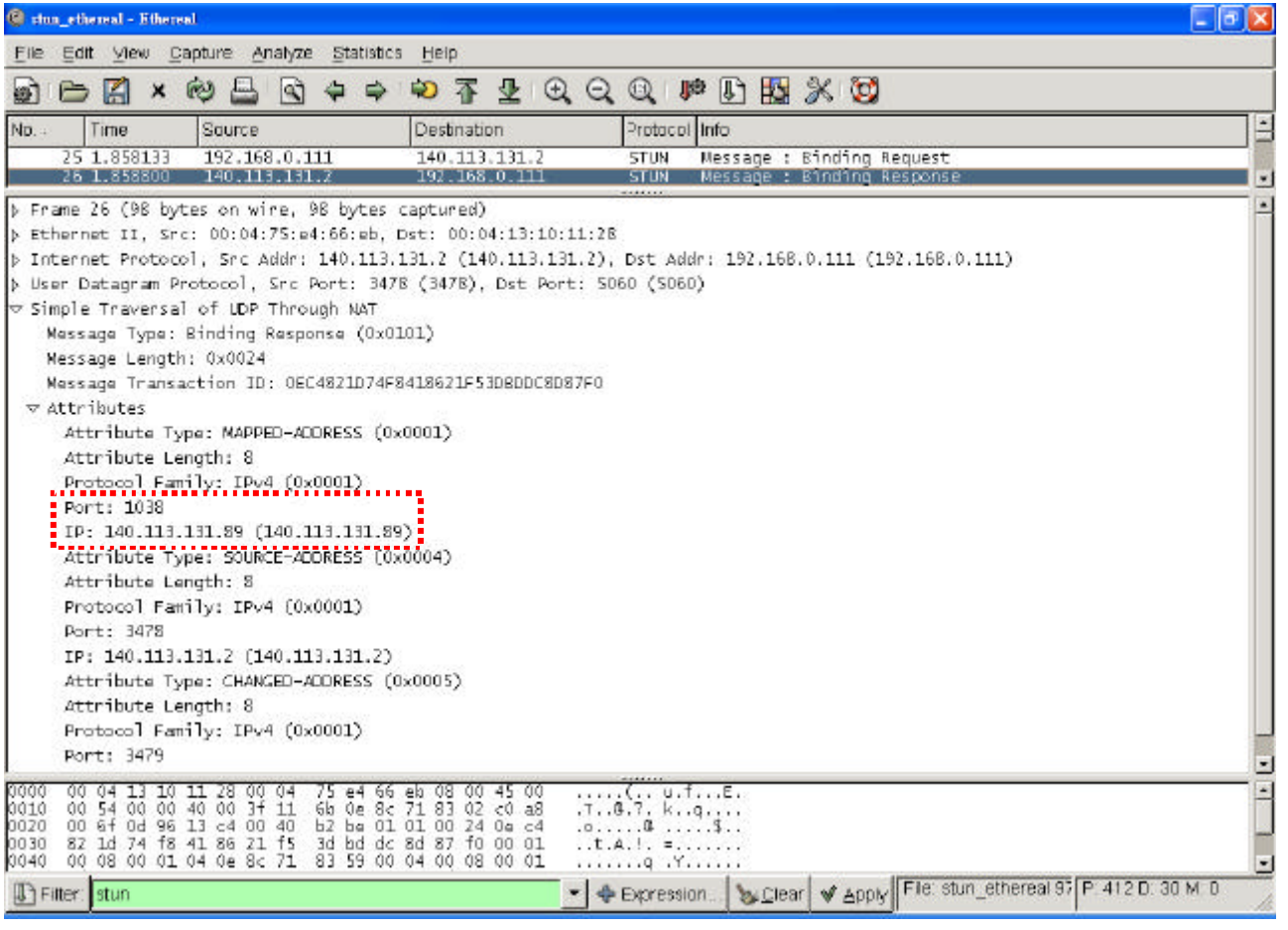
- Use port 5060 to send a packet to STUN Server
- Receive public address & port mapped to client:5060 from STUN Se rver
- Fill the SIP register message with client's public address & port, send to proxy server



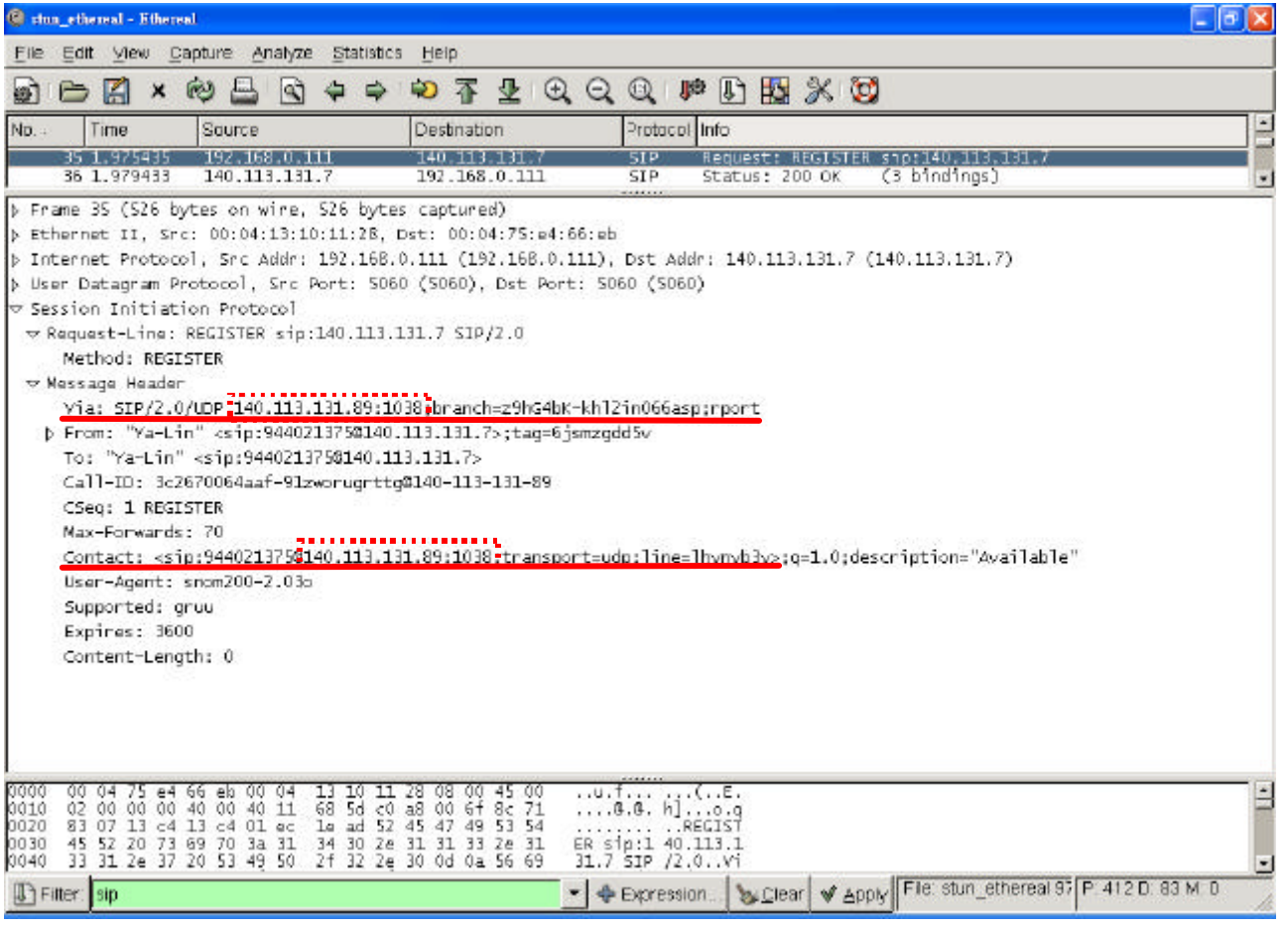
STUN訊息格式


Message Type (16bits)
Message Length (16bits)
Transaction ID (128-bits)
Message Header
Type (16bits)
Length (16bits)
Value
Message Payload
Type (16bits)
Length (16bits)
Value

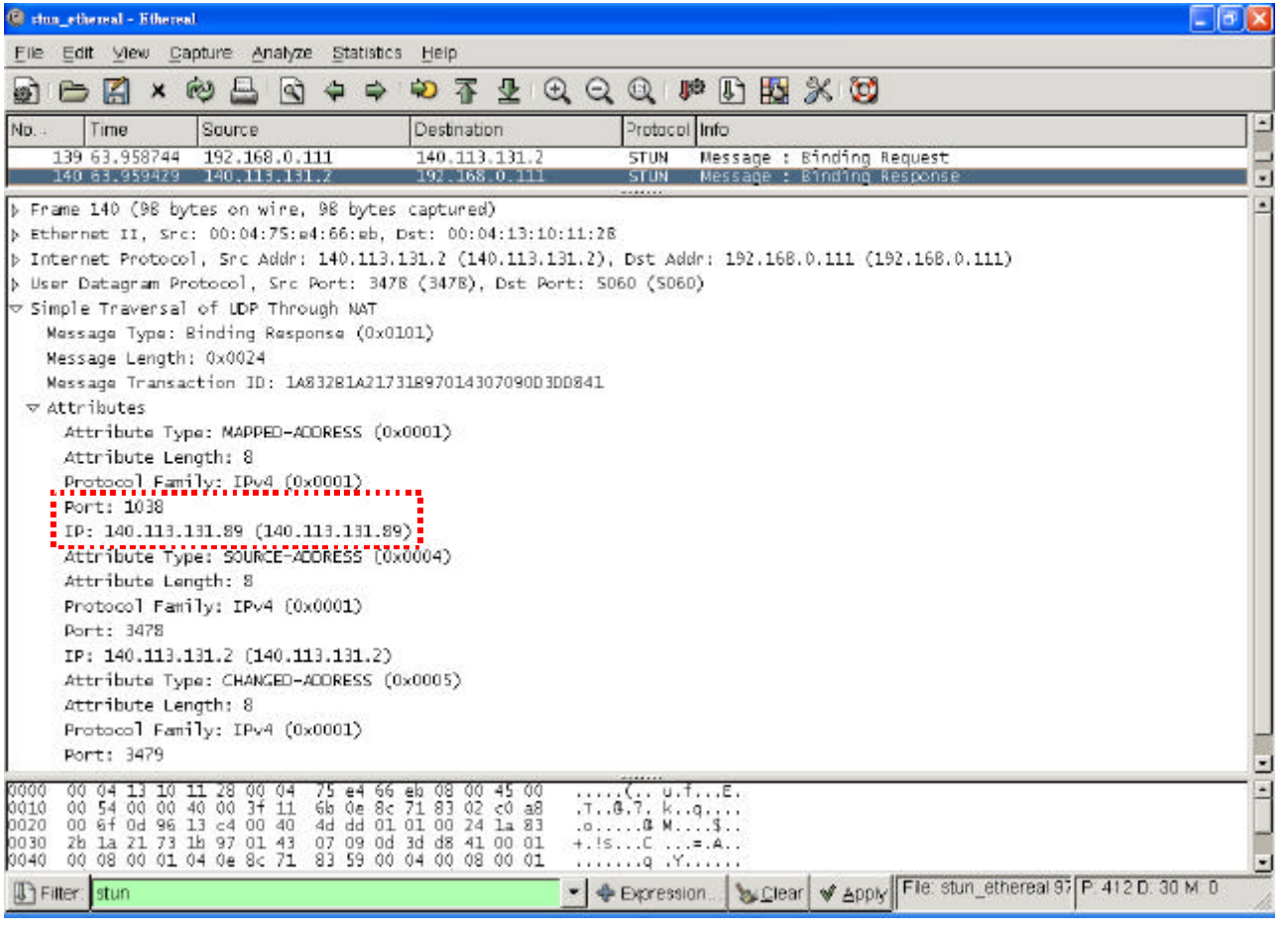
STUN Message (Register)



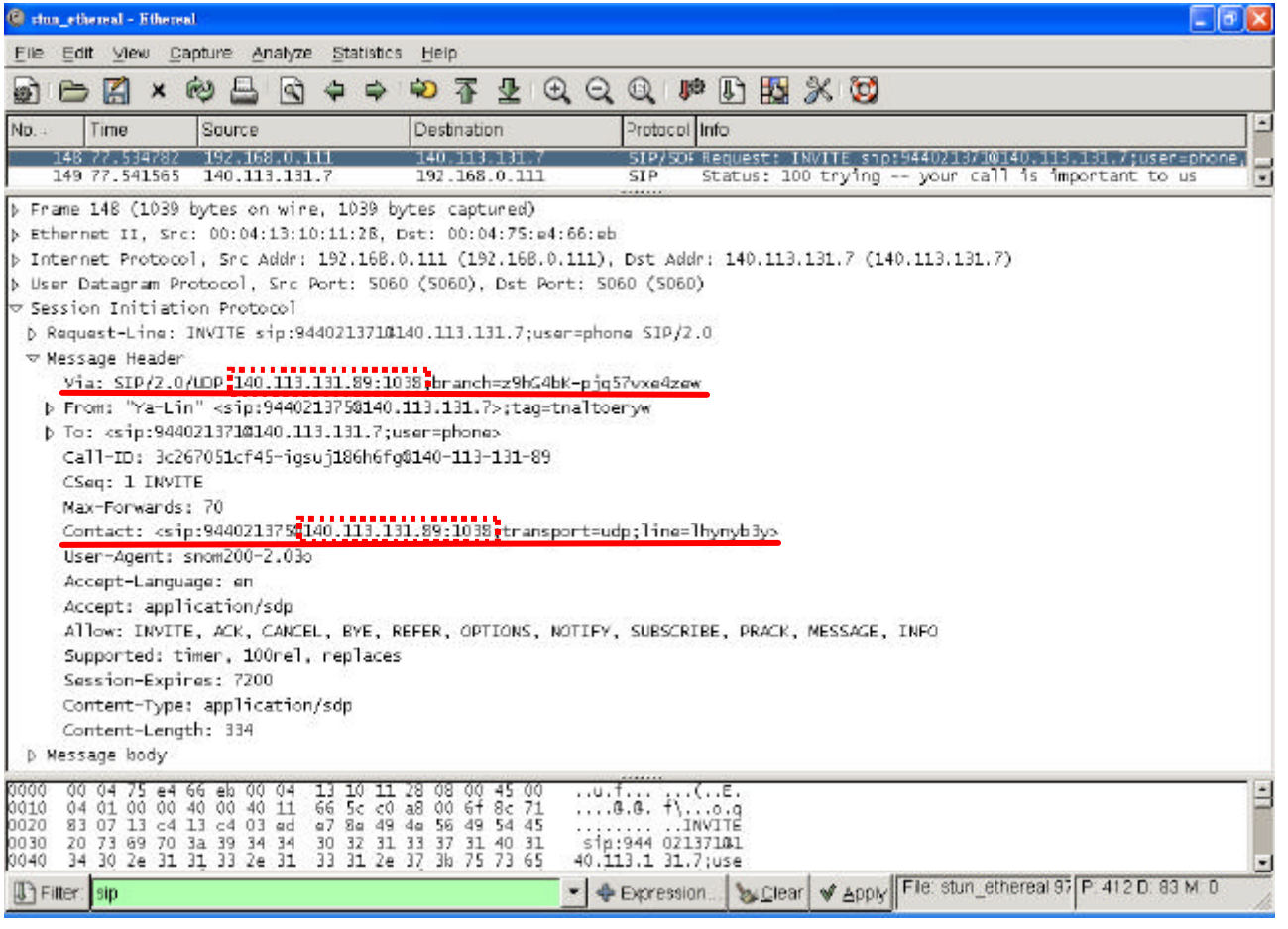
Correct SIP REGISTER Message



STUN Message (SIP Port)

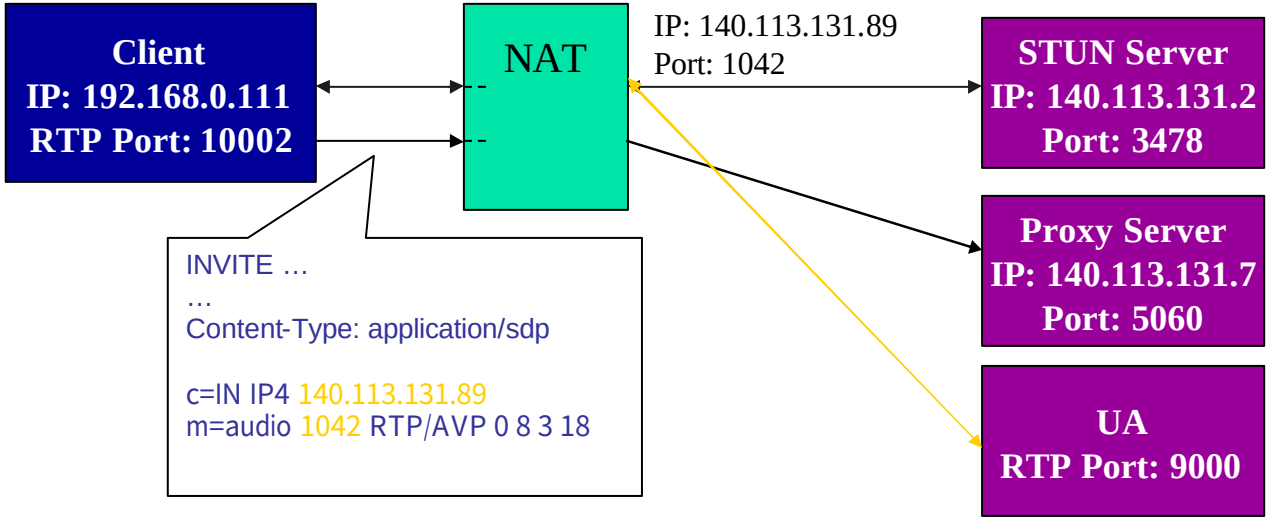


Correct INVITE Message (SIP)

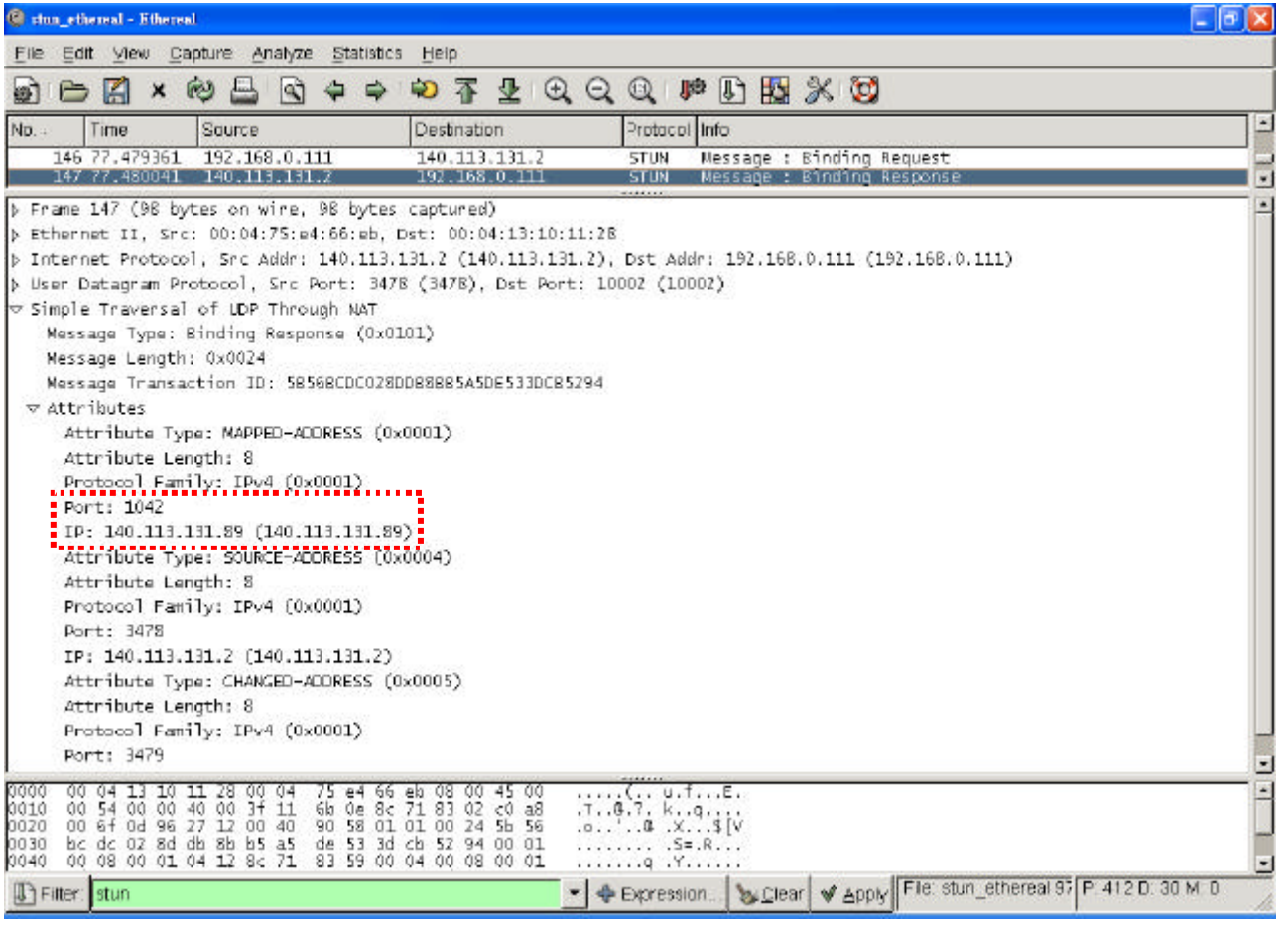


Use STUN for RTP

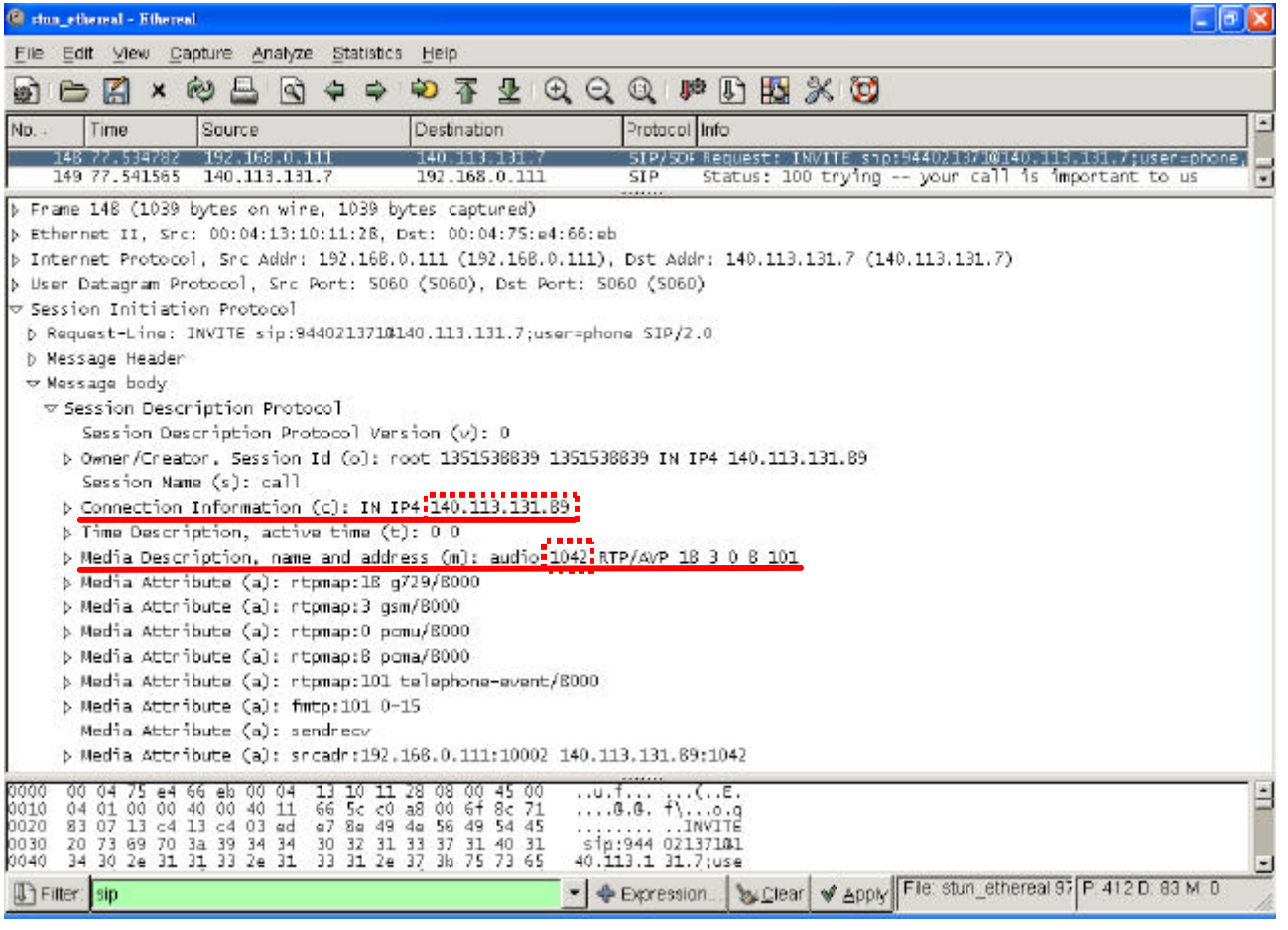
- Send STUN queries from RTP port (10002) to STUN Server
- Use replied public address & port in SDP



STUN Message (SDP Port)



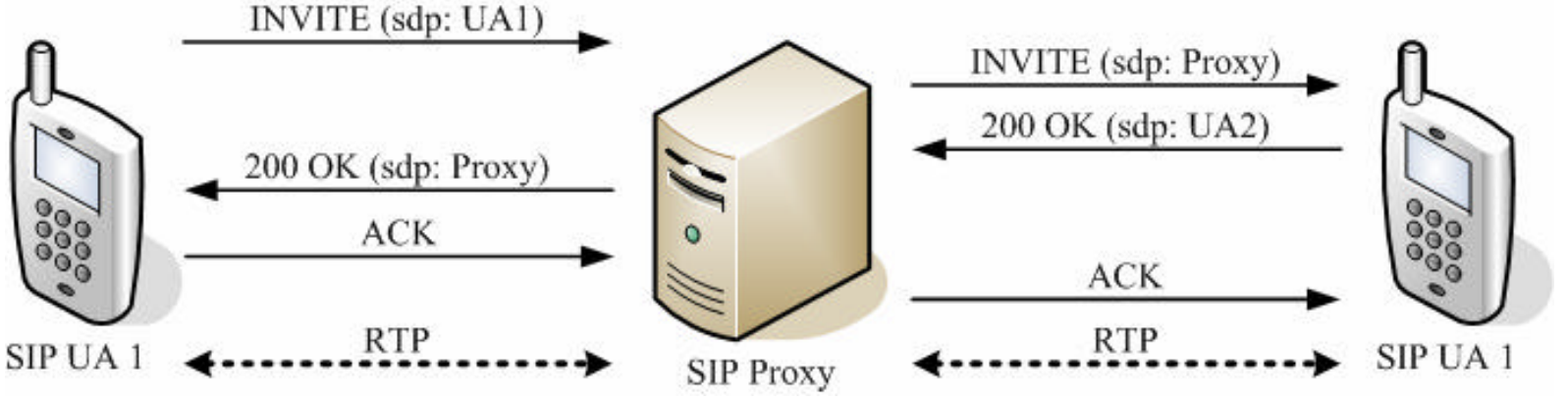
Correct INVITE Message (SDP)



Session Controller

Session Controller 運作方法

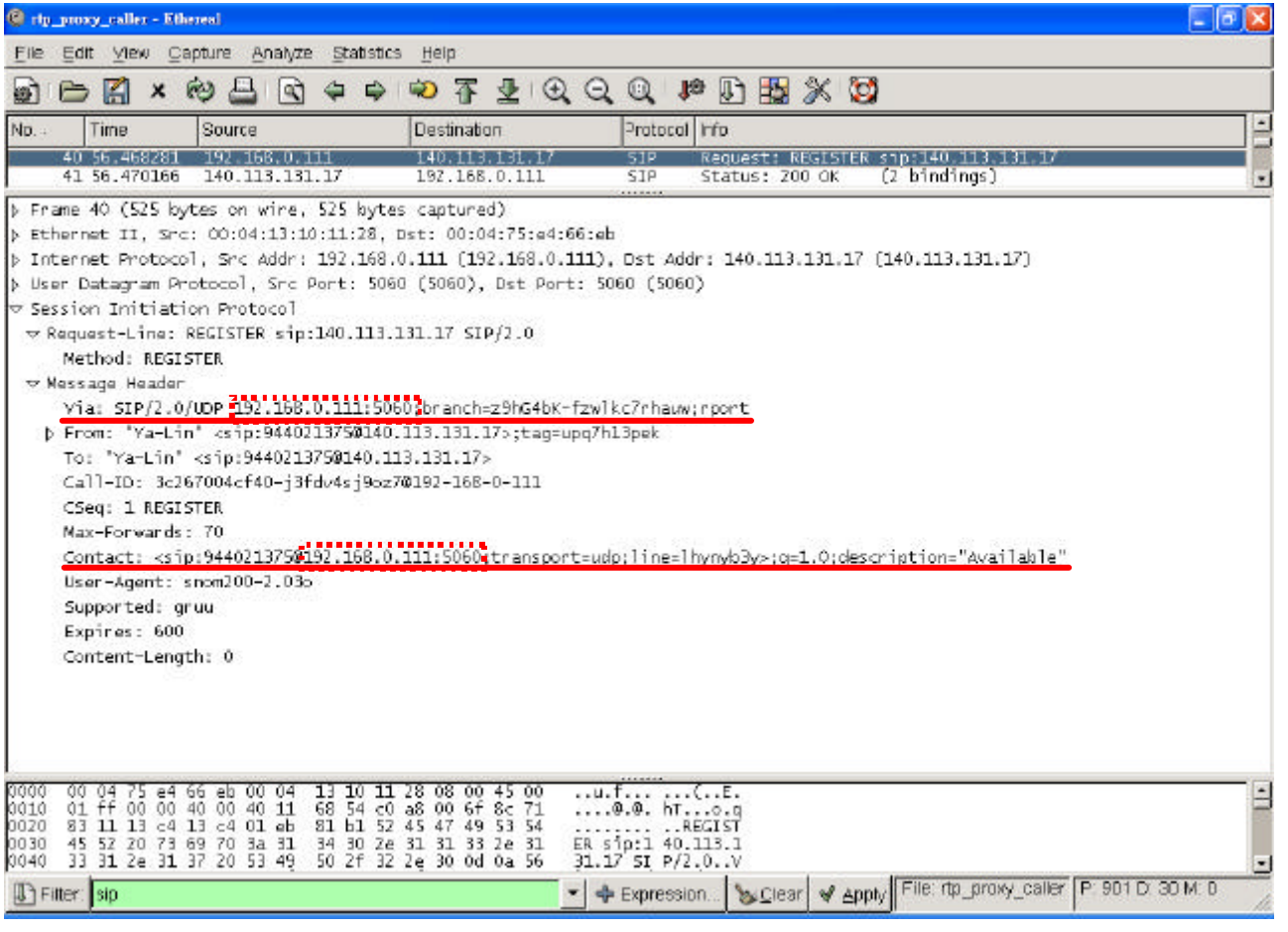
- SIP
  - Add *Record-Route* header to enforce every SIP message inside this session passing through SIP Proxy for further modification
  - Modify *Contact* header for further routing
  - Add *rport* and *received* tag into Via for further routing
- SDP
  - Replace sdp of each UA into that of SIP Proxy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



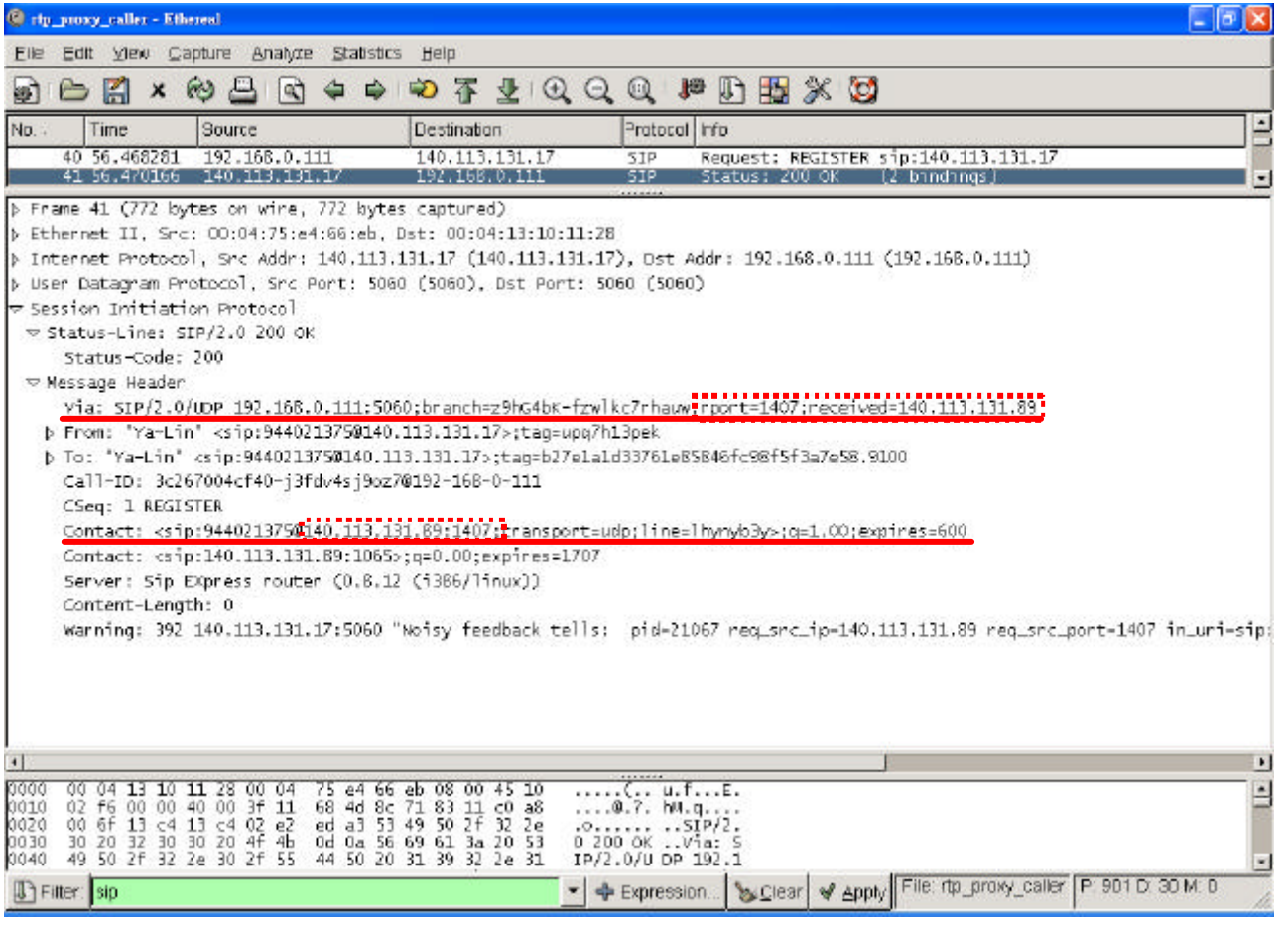
SIP Server Configuration

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

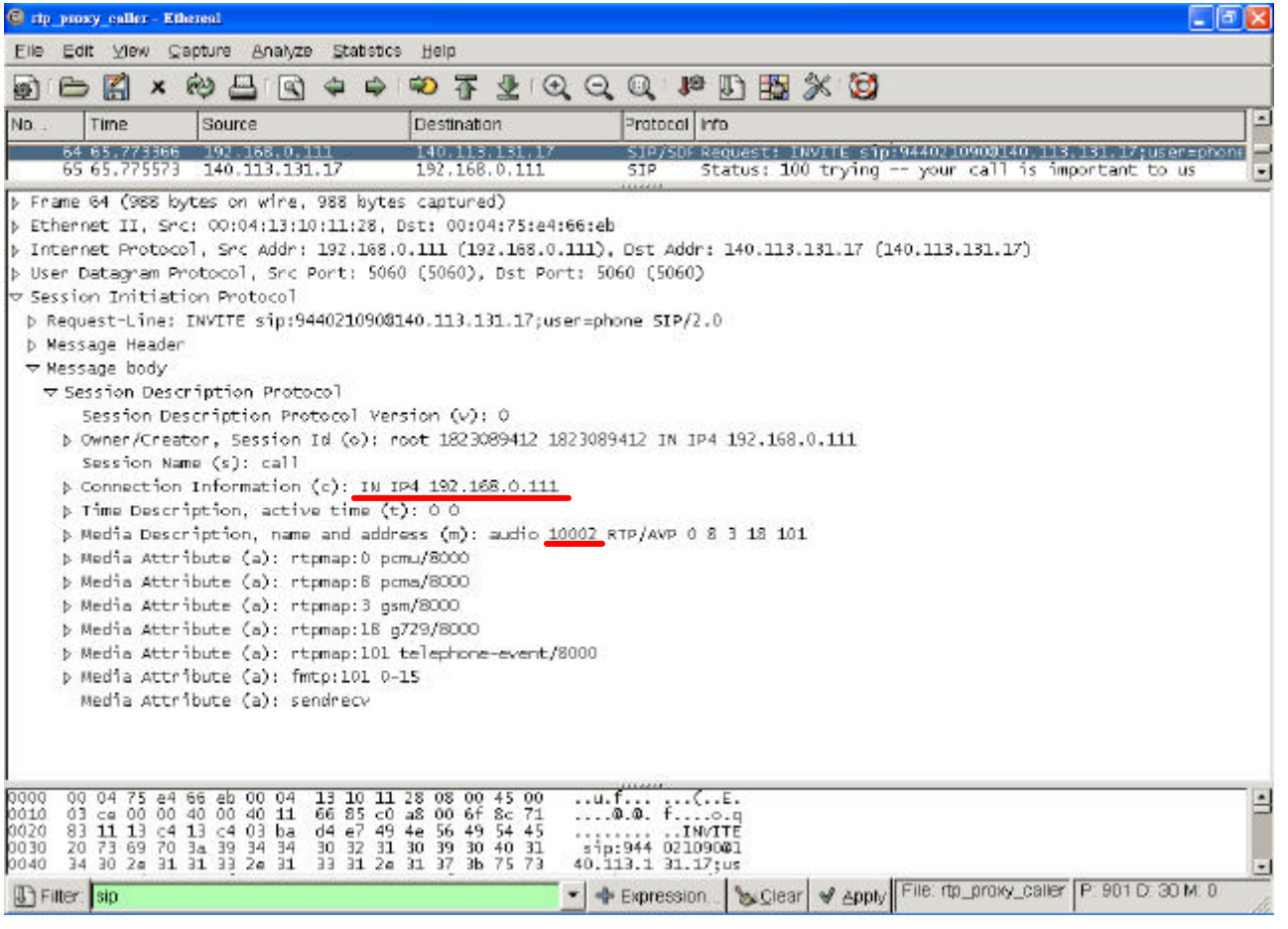
REGISTER Message



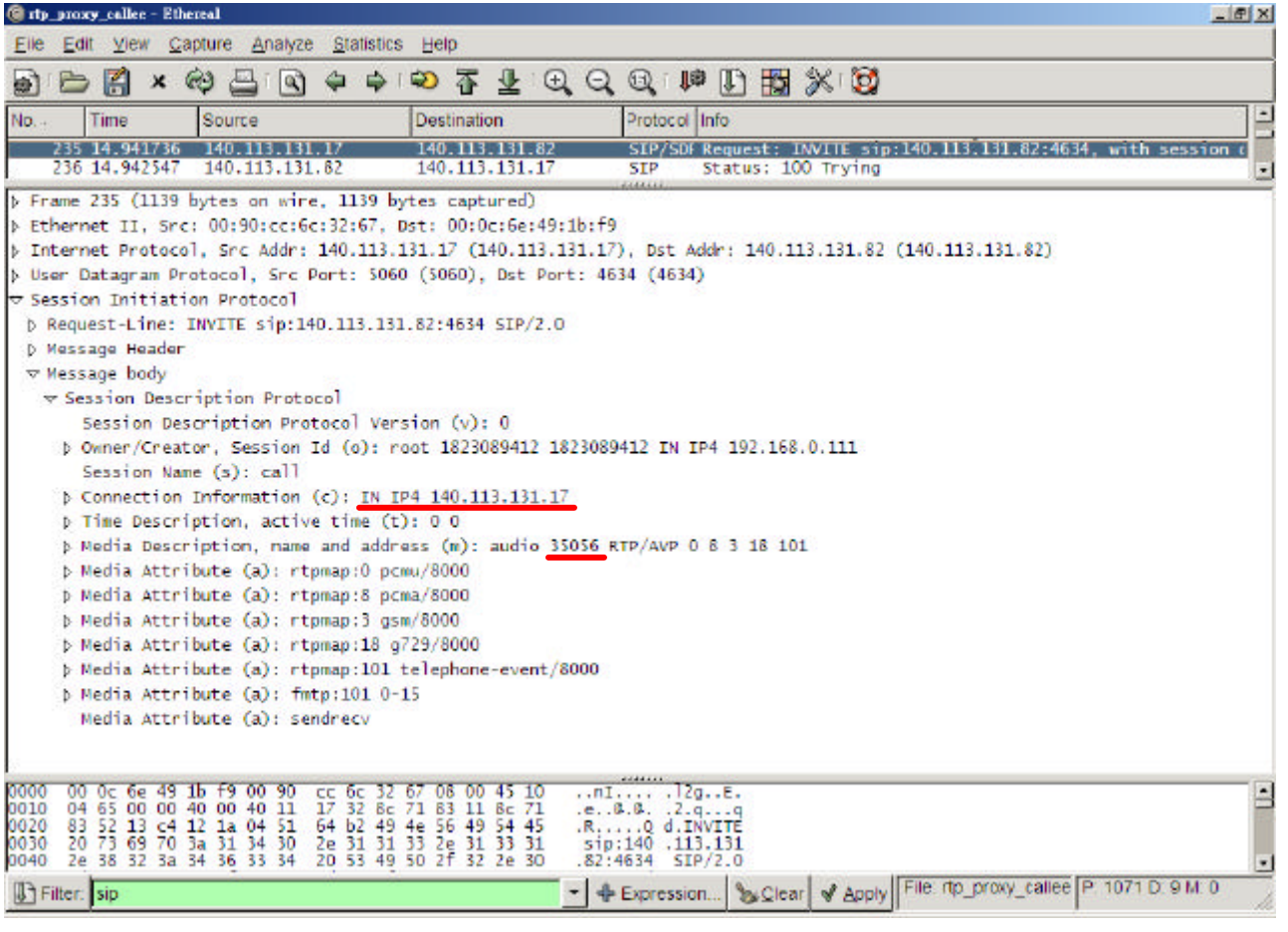
200 OK Message of REGISTER



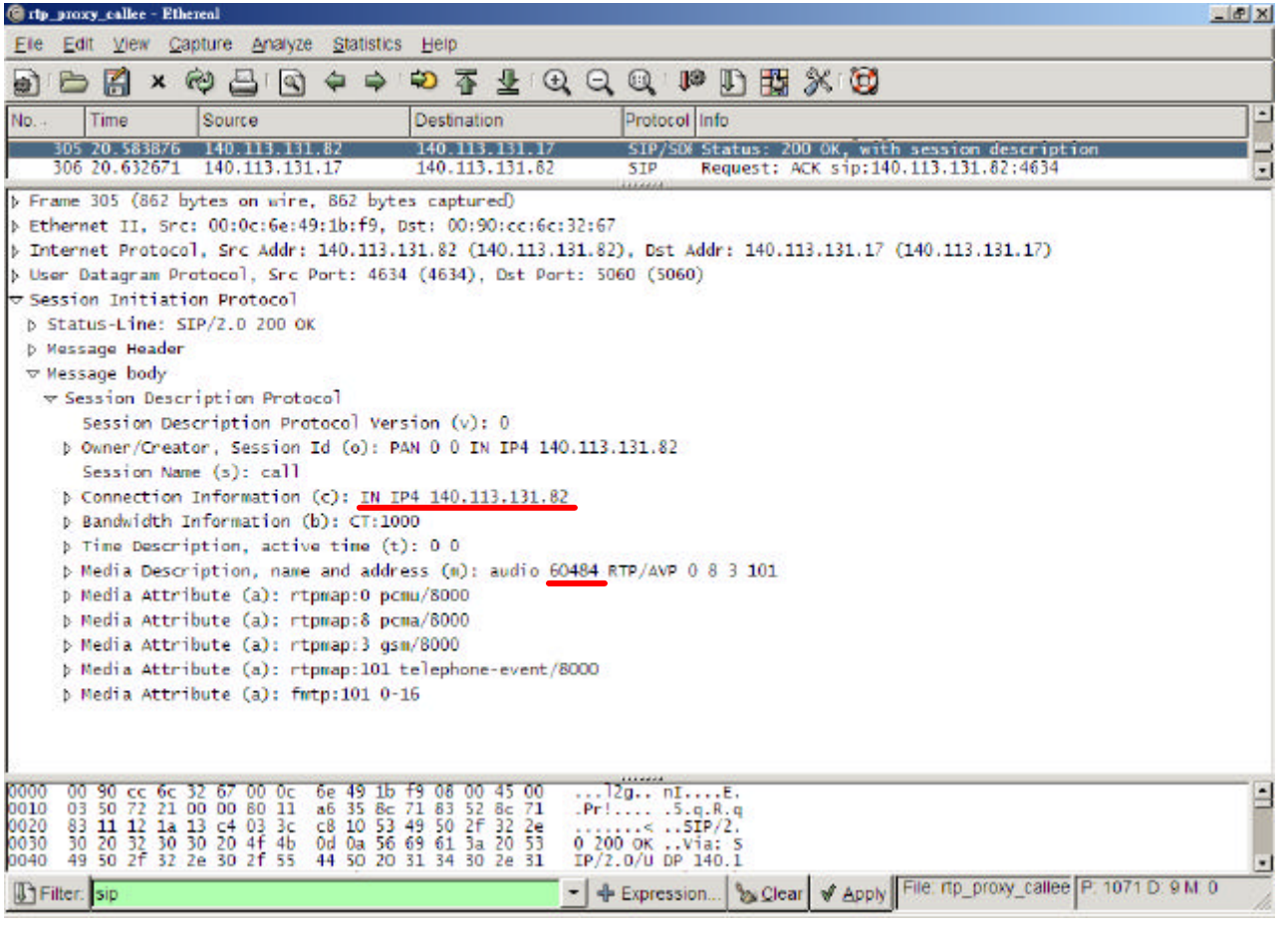
INVITE Message sent by caller (SDP)



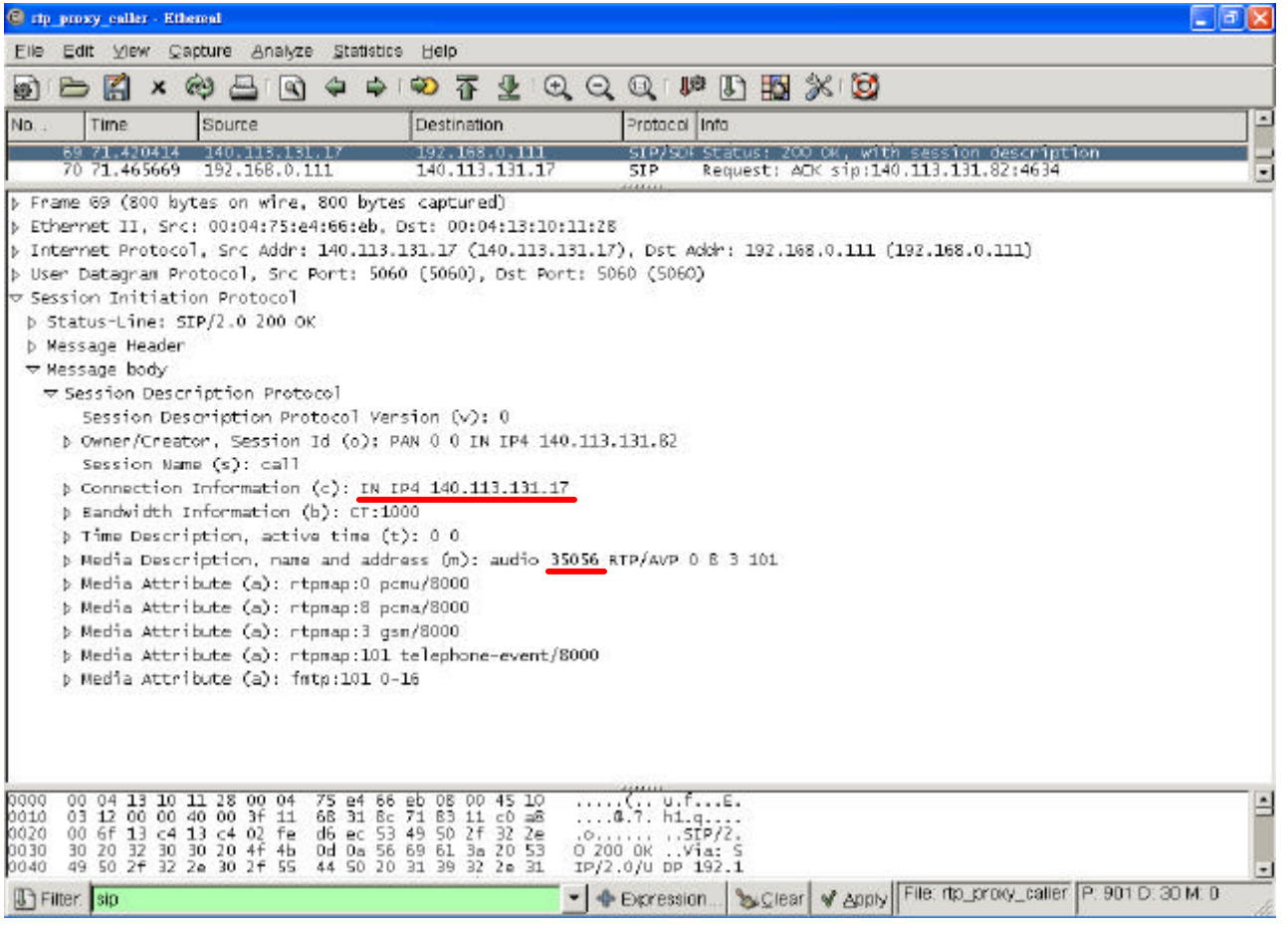
INVITE Message received by callee (SDP)



200 OK Message of INVITE sent by callee (SDP)



200 OK Message of INVITE received by caller (SDP)



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 Addres s 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.