



# NAT Traversal for VoIP

Dr. Quincy Wu

National Chi Nan University

Email: [solomon@ipv6.club.tw](mailto:solomon@ipv6.club.tw)

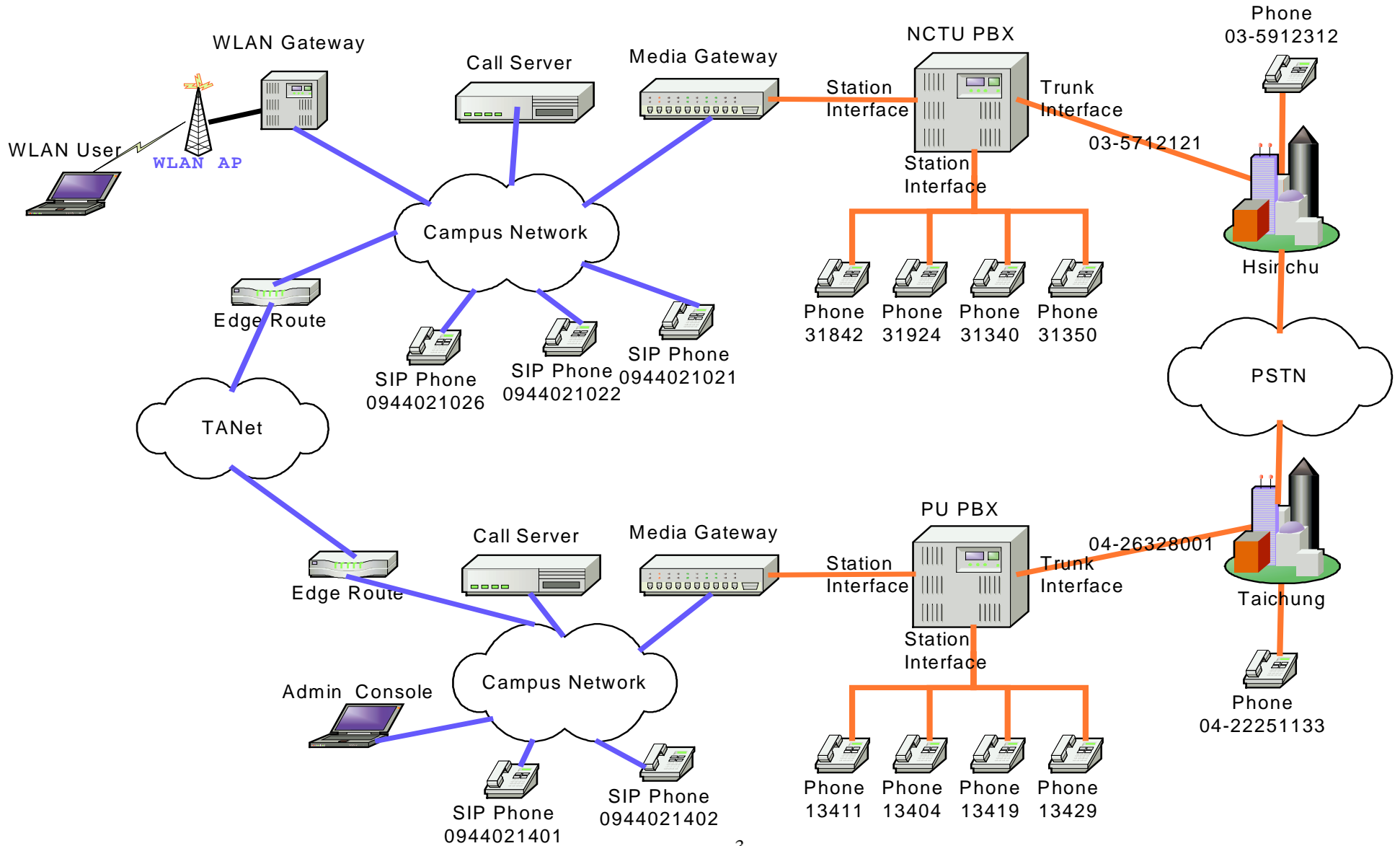


# NAT Traversal

- Where is NAT
- What is NAT
- Types of NAT
- NAT Problems
- NAT Solutions
- Program Download



# NTP VoIP Platform



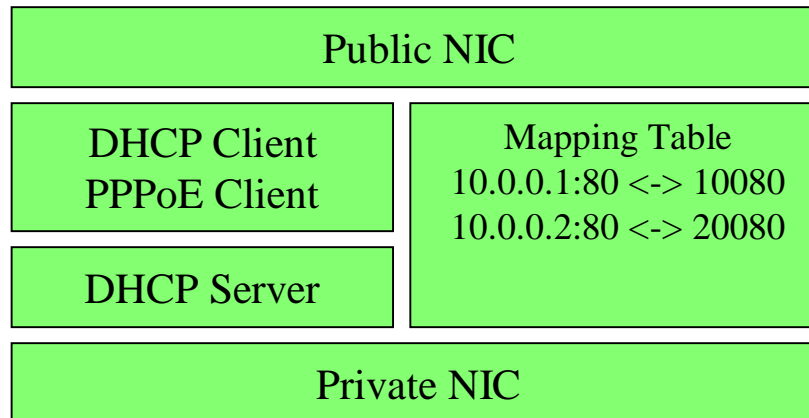
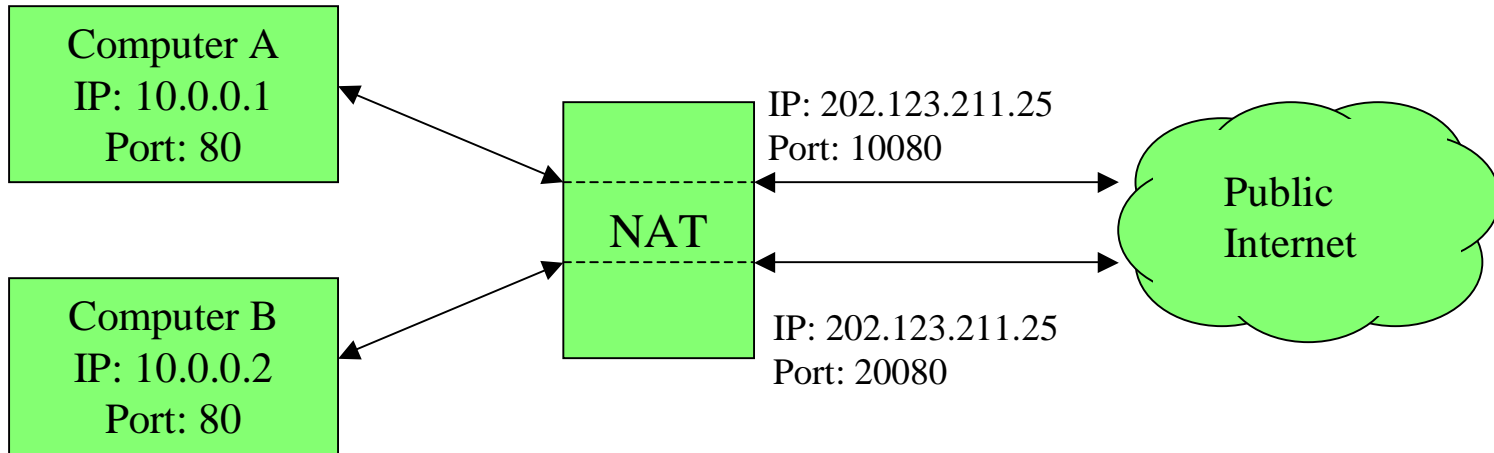


# What is NAT

- NAT - Network Address Translation
  - RFC 3022 - Traditional IP Network Address Translator (Traditional NAT)
  - 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 Network Address (and Port) between private and public realm
- Works on IP layer
- Transparent for Application



# NAT Schematic





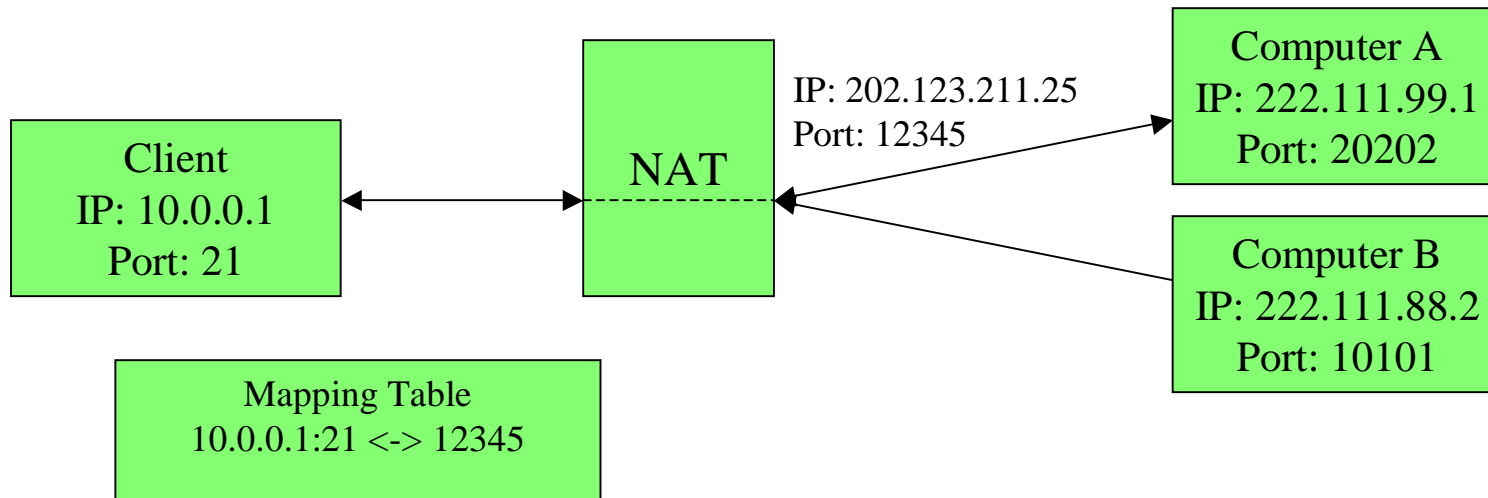
# Types of NAT

- Full Cone
- Restricted Cone
- Port Restricted Cone
- Symmetric



# Full Cone NAT

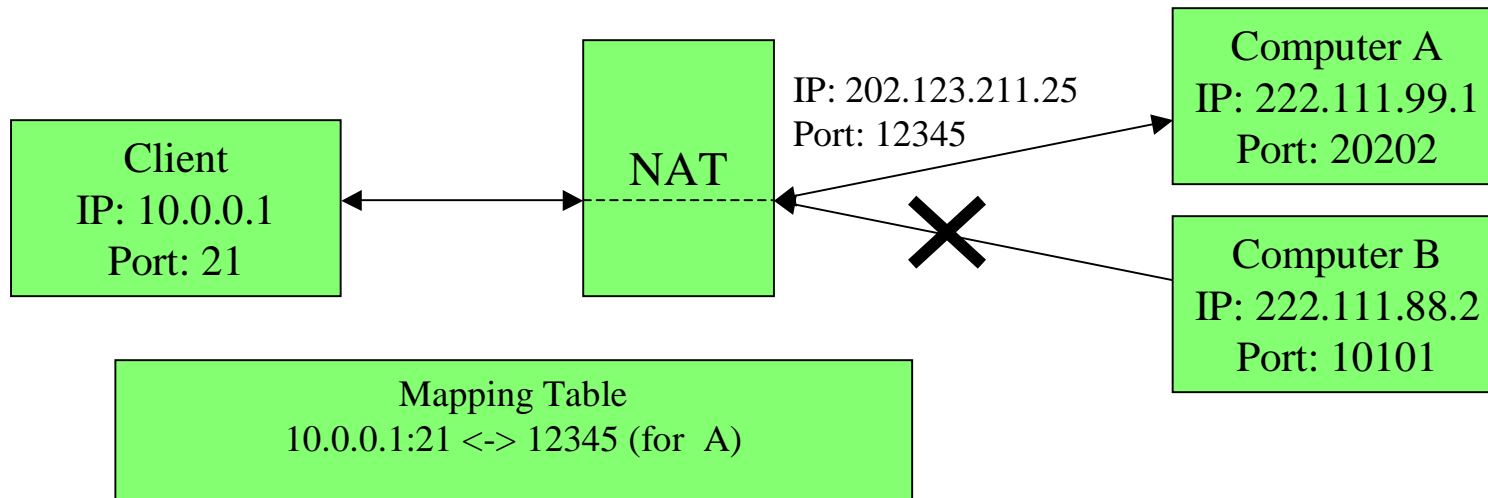
- Client send a packet to public address A.
- NAT allocate a public port (12345) for private port (21) on the client.
- Any incoming packet (from A or B) to public port (12345) will dispatch to private port (21) on the client.





# Restricted Cone NAT (1/2)

- Client send a packet to public address A.
- NAT allocate a public port (12345) for private port (21) on the client.
- Only incoming packet from A to public port (12345) will dispatch to private port (21) on the client.

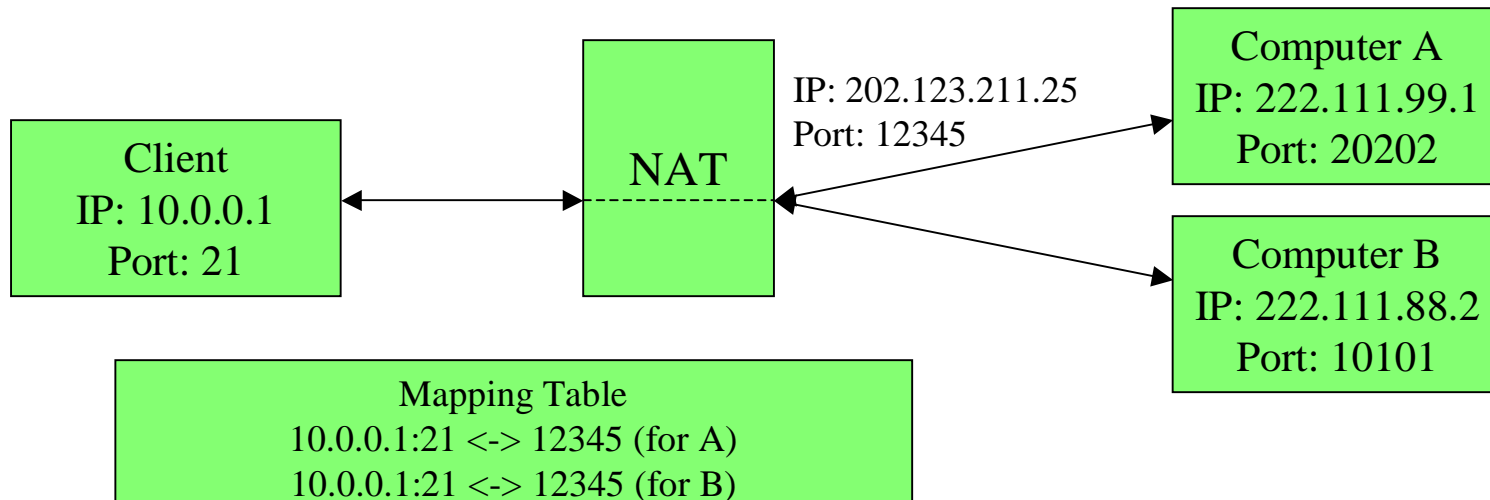






# Restricted Cone NAT (2/2)

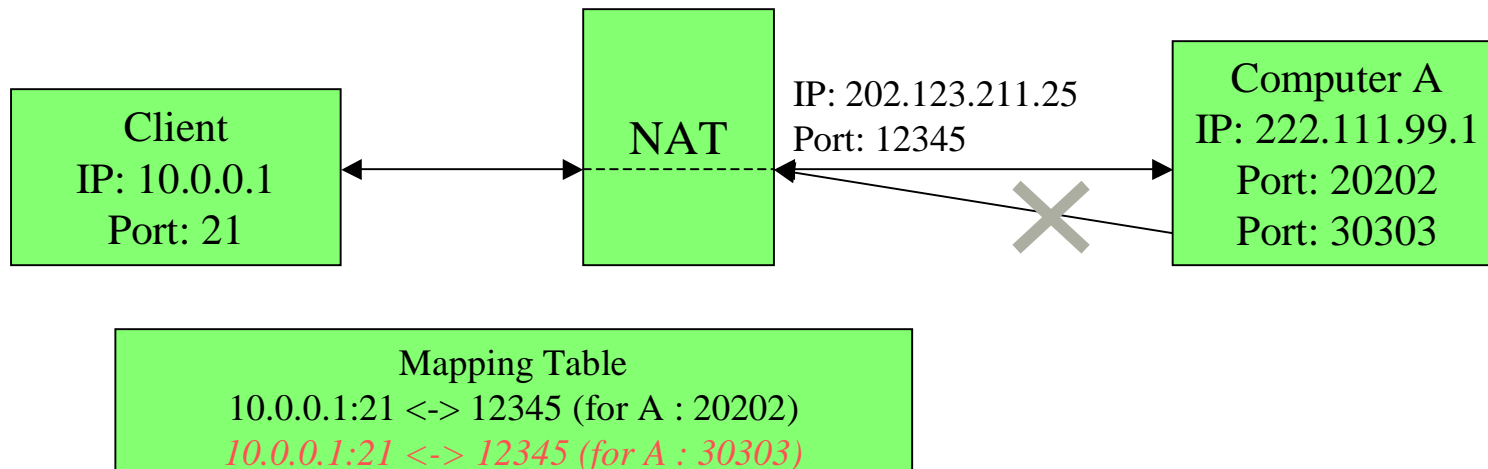
- Client send another packet to public address B.
- NAT will reuse allocated public port (12345) for private port (21) on the client.
- Incoming packet from B to public port (12345) will now dispatch to private port (21) on the client.





# Port Restricted Cone NAT

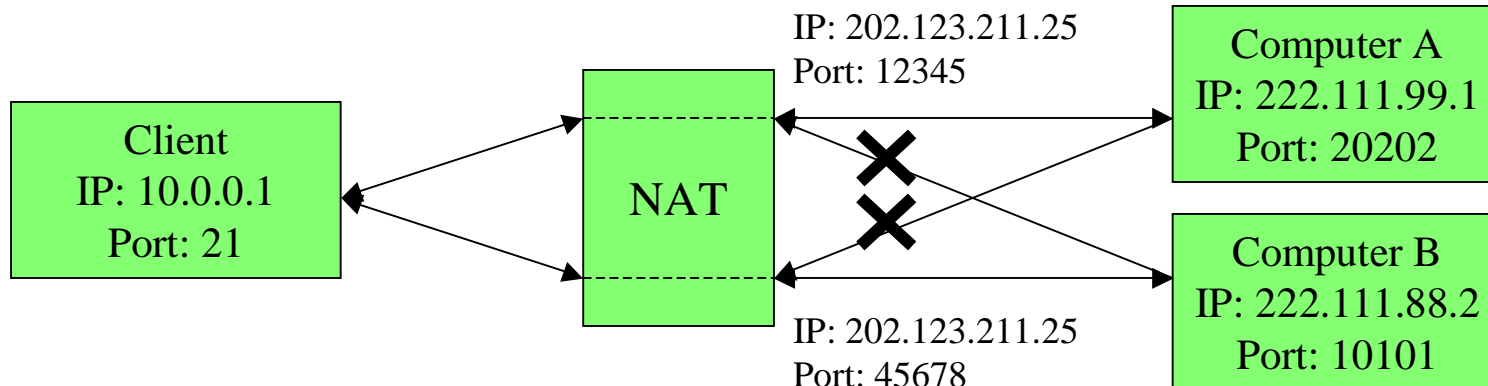
- Client send a packet to public address A port 20202.
- NAT will allocate a public port (12345) for private port (21) on the client.
- Only incoming packet from address A and port 20202 to public port (12345) will dispatch to private port (21) on the client.





# Symmetric NAT

- NAT allocate a public port each time the client send 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	
10.0.0.1:21	<-> 12345 (for A : 20202)
10.0.0.1:21	<-> 45678 ( for B : 10101)



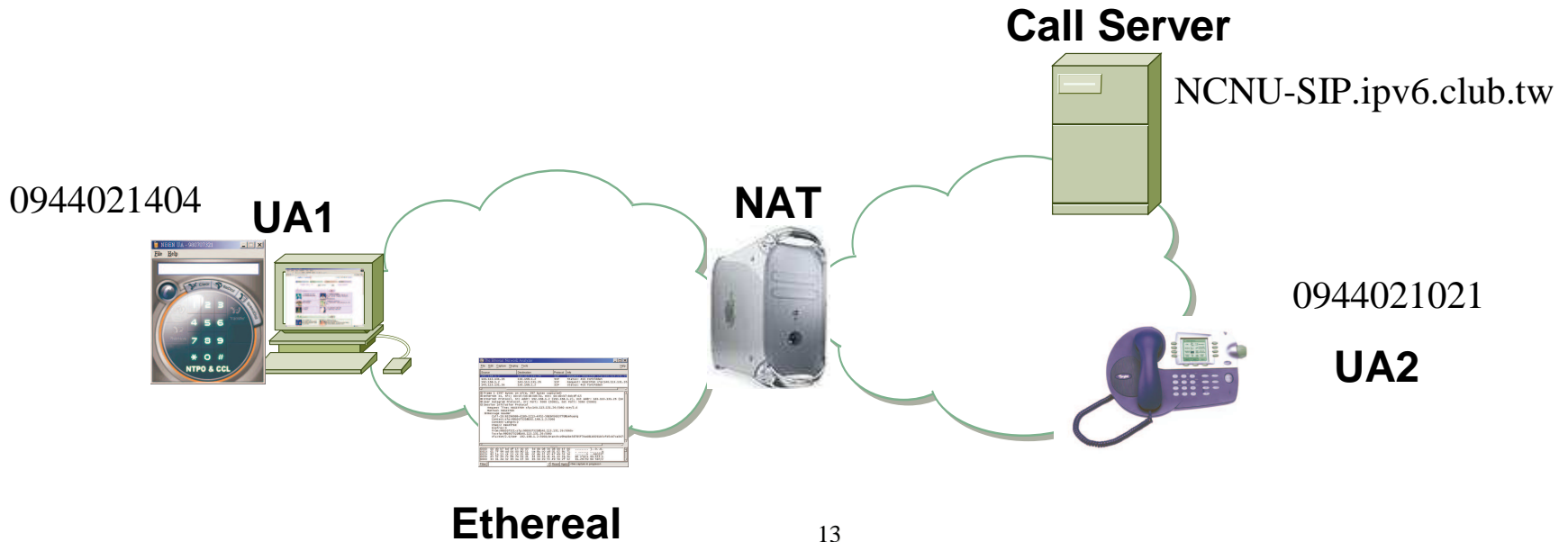
# VoIP Protocol and NAT

- NAT convert IP addresses on IP layer
- Problem 1:
  - SIP, H.323, Megaco and MGCP are application layer protocol but contain IP address/port info in messages, 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



# Lab Environment

- UA1: UA behind NAT.
- UA2: SIP device outside NAT.
- Call Server: SIP-express router 0.8.12.
- NAT: Linux Fedora Core 2.
- Packet Capturer: Ethereal-0.9.15.





# The Problem (1/2)

- Due to private address, the **Via header** and **Contact address** 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 Ethereal Network Analyzer

File Edit Capture Display Tools Help

Source	Destination	Protocol	Info
192.168.1.102	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7:5060
192.168.1.102	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7:5060
192.168.1.102	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7:5060
192.168.1.102	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7:5060
192.168.1.102	140.113.131.7	SIP	Request: REGISTER sip:140.113.131.7:5060

.....

Frame 1 (400 bytes on wire, 400 bytes captured)  
 Ethernet II, Src: 00:0c:6e:49:1b:4a, Dst: 00:90:cc:4f:d0:80  
 Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), 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:140.113.131.7:5060 SIP/2.0  
 Method: REGISTER  
 Message Header  
 Call-ID:63786888-d1b9-1277-f890-1eb37273c7e1@TRITON  
 Contact:sip:980707321@192.168.1.102:5060  
 Content-Length:0  
 CSeq:2 REGISTER  
 Expires:3600  
 From:980707321<sip:980707321@140.113.131.7:5060>  
 To:sip:980707321@140.113.131.7:5060  
 Via:SIP/2.0/UDP 192.168.1.102:5060;branch=z9hg4bk9a8c28f48e0e2319a877b8bbe15ceb15

.....

0020	83 07 13 c4 13 c4 01 6e 85 ec 52 45 47 49 53 54	.....n..REGIST
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 3a 35 30 36 30 20 53 49 50 2f 32 2e	31.7:506 0 SIP/2.
0050	30 0d 0a 43 61 6c 6c 2d 49 44 3a 36 33 37 38 36	0..Call- ID:63786
0060	38 38 38 2d 44 31 42 39 2d 31 32 37 37 2d 46 38	888-d1b9 -1277-f8

Filter: / Reset Apply <live capture in progress>



## The Problem (2/2)

- When UA1 initiate a call, the **connection information** 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

```
⊞ Frame 6 (900 bytes on wire, 900 bytes captured)
⊞ Ethernet II, Src: 00:0c:6e:49:1b:4a, Dst: 00:90:cc:4f:d0:80
⊞ Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 140.113.131.7
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol
⊞ Session Description Protocol
  session Description Protocol version (v): 0
  ⊞ Owner/Creator, Session Id (o): 980707321 1086859 1086859 IN IP4 192.168.1.102
    session Name (s): session SDP
  ⊞ Connection Information (c): IN IP4 192.168.1.102
  ⊞ 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): rtpmap:0 PCMU/8000/1
  ⊞ Media Attribute (a):ptime:20
  ⊞ Media Attribute (a): rtpmap:8 PCMA/8000/1
  ⊞ Media Attribute (a):ptime:20
  ⊞ Media Attribute (a): rtpmap:3 GSM/8000/1
  ⊞ Media Attribute (a):ptime:20
  ⊞ Media Attribute (a): rtpmap:4 G723/8000/1
  ⊞ Media Attribute (a):ptime:20
  ⊞ Media Attribute (a): rtpmap:18 G729/8000/1
  ⊞ Media Attribute (a):ptime:20
  ⊞ Media Description, name and address (m): video 9002 RTP/AVP 34 96
  ⊞ Media Attribute (a): rtpmap:34 H263/90000/2
  ⊞ Media Attribute (a):ptime:30
  ⊞ Media Attribute (a): rtpmap:96 MPEG4/90000/2
  ⊞ Media Attribute (a):ptime:30
```



# Solving NAT Traversal Problems

## ■ Target:

- 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 (45 sec ~ 5 min)
- Keep a TCP connection to target
- Send UDP packet to target every specified interval



# NAT Solutions

- IPv6 (Internet Protocol Version 6)
- UPnP (Universal Plug-and-Play)
  - UPnP Forum - <http://www.upnp.org/>
- VPN (Virtual Private Network)
- Proprietary protocol by NAT/Firewall
  - SIP ALG (Application Level Gateway)
  - No standard now. Not applicable for existing NATs.
- SIP extensions for NAT traversal
  - RFC 3581 - rport
  - Works for SIP only, can not help RTP to pass through NAT
- STUN (Simple Traversal of UDP Through Network Address Translators)
  - RFC 3489
  - Works except symmetric NAT
- TURN (Traversal Using Relay NAT)
  - draft-rosenberg-midcom-turn-08
  - for symmetric NAT



# UPnP – Universal Plug-and-Play



# NAT Traversal with UPnP

## ■ 目的

- 使 NAT 網路內的機器確切知道對外所用的 Public IP 位址資訊

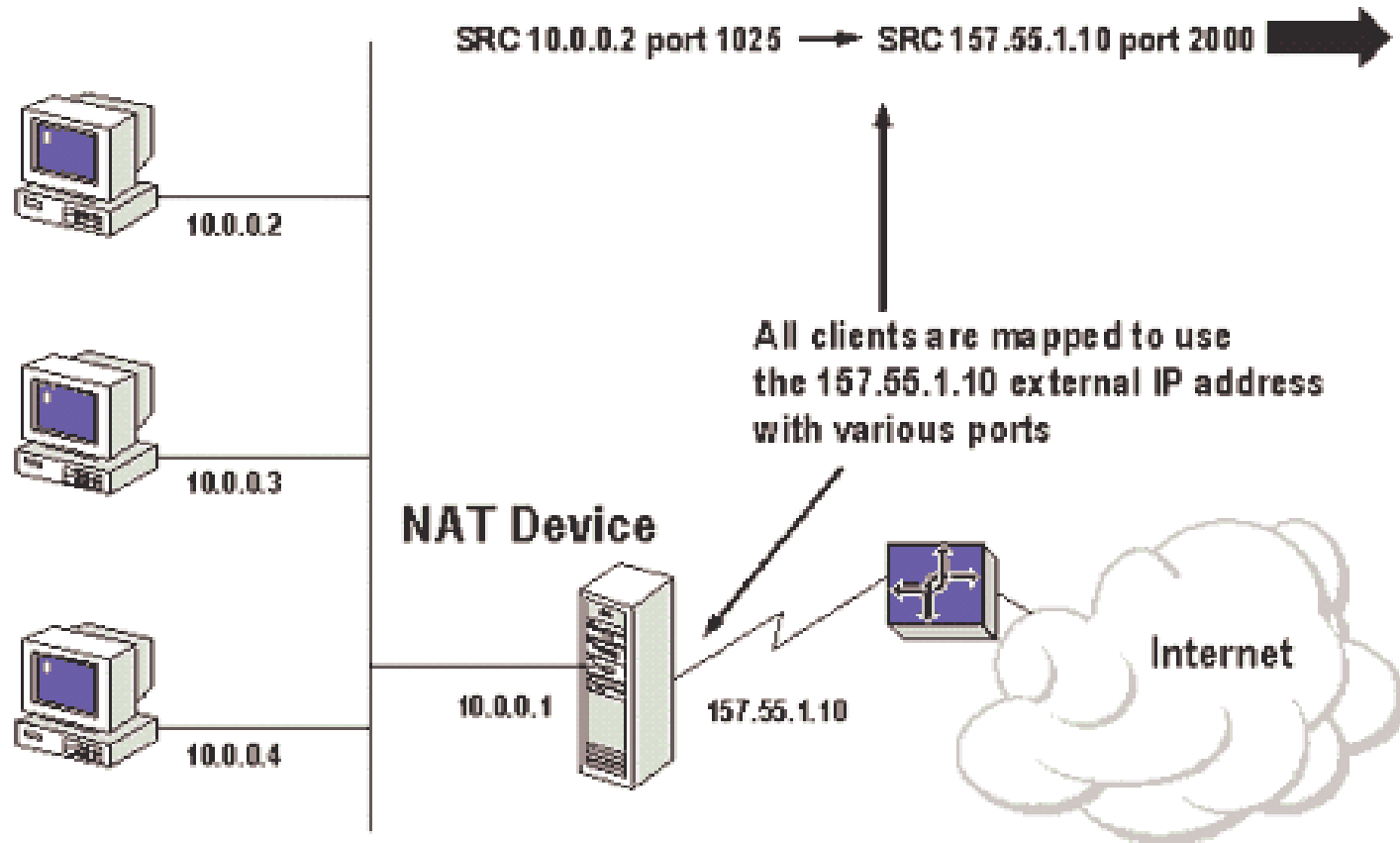
## ■ 解法

- 讓 NAT Device 可與 NAT 內的應用程式溝通, 交換位址資訊
- 定義 NAT Device 為一 UPnP Device (IGD)

☞ IGD -- Internet Gateway Device



# NAT 網路架構





# UPnP IGD

- 提供以下UPnP 功能
  - 取得 public IP 位址
  - 取得現有 port mapping
  - 新增/移除 port mapping
  - 指定 mapping 的存續時間



# 利用 UPnP 取得位址資訊

- NAT 內主機可利用 UPnP *Control Message* 通知 IGD 增加一 Port Mapping
- 範例:
  - 本機位址: 192.168.0.14
  - 正在本機 port 10001 上聽 UDP 封包
  - 希望能在 IGD 新增一 port mapping





# IGD Control Message

- POST /upnpghost/udhisapi.dll?control=uuid:c3038e95-ea88-4d5c-98ff-3ad68f7aaa32+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>17769</NewExternalPort>
- <NewProtocol>UDP</NewProtocol>
- <NewInternalPort>10001</NewInternalPort>
- <NewInternalClient>192.168.0.146</NewInternalClient>
- <NewEnabled>1</NewEnabled>
- <NewPortMappingDescription>s2EAYp (192.168.0.146:10001) 17769 UDP</NewPortMappingDescription>
- <NewLeaseDuration>0</NewLeaseDuration>
- </u:AddPortMapping>
- </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



# Simple Traversal of UDP Through Network Address Translators (STUN)



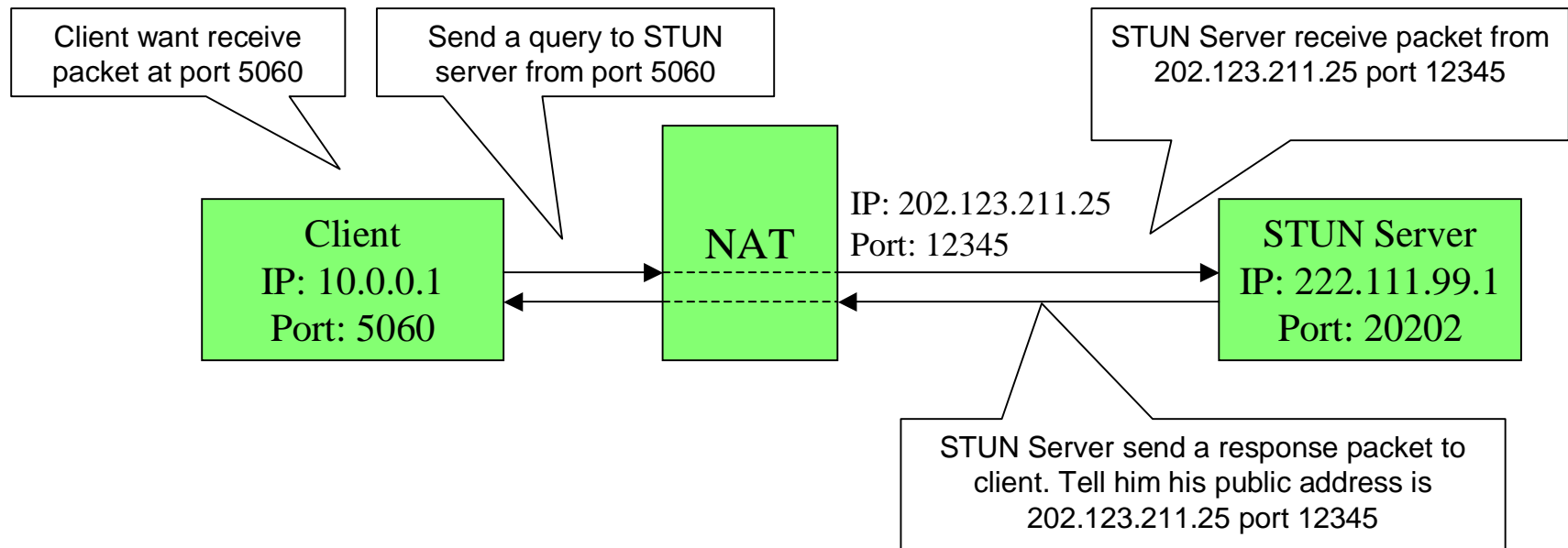
# STUN (RFC 3489)

- 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

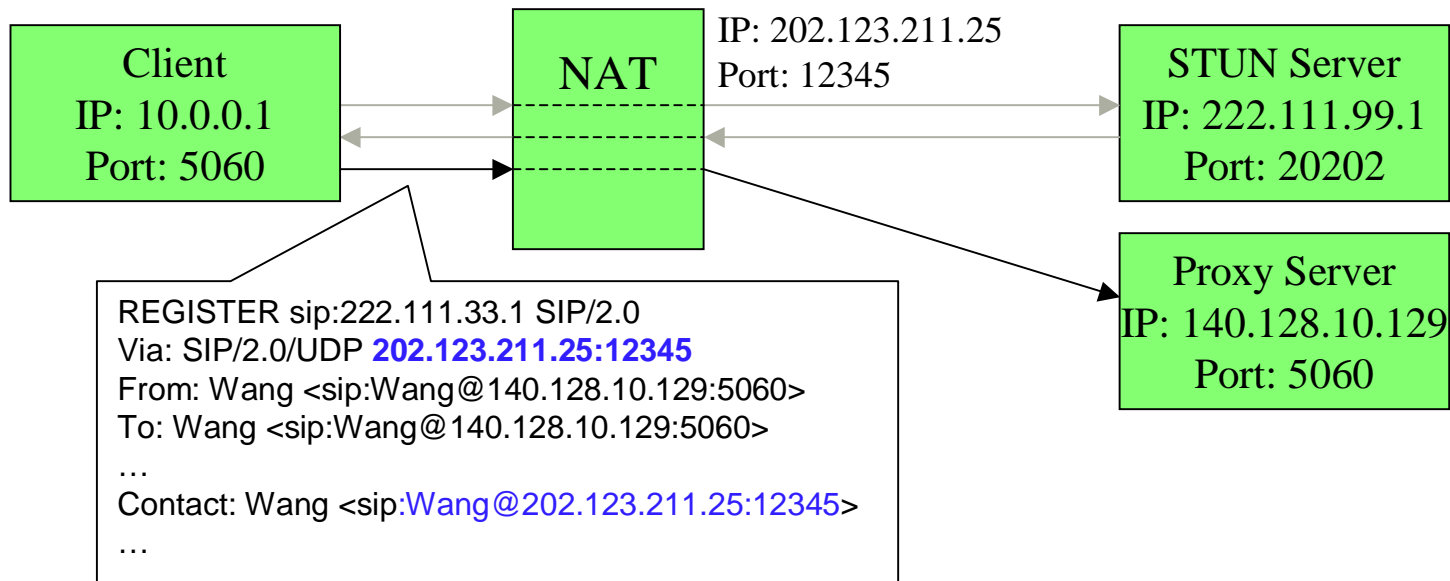
- Allow clients to discover if it is behind a NAT, what type of NAT it is, and the public address & port NAT will use.
- Very Simple Protocol, Easy to implement, Little load





# 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





# Corrected SIP Message

The Ethereal Network Analyzer

File Edit Capture Display Tools Help

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	140.113.131.7	SIP	Request: REGISTER sip
2	0.005094	140.113.131.7	192.168.1.102	SIP	Status: 200 OK

Frame 1 (434 bytes on wire, 434 bytes captured)

- Ethernet II, Src: 00:0c:6e:49:1b:4a, Dst: 00:90:cc:4f:d0:80
- Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), 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:140.113.131.7:5060 SIP/2.0
  - Method: REGISTER
  - Message Header
    - Call-ID:63787357-D1B9-1277-F890-1EB37273C7E1@TRITON
    - Contact:sip:980707321@140.113.131.72:56540
    - Content-Length:0
    - CSeq:4 REGISTER
    - Expires:3600
    - From:980707321<sip:980707321@140.113.131.7:5060>
    - To:sip:980707321@140.113.131.7:5060
    - User-Agent:CCL\_SIP\_SOFTPHONE
    - Via:SIP/2.0/UDP 140.113.131.72:56540;branch=z9hg4bked5ecd0be03e449d4648046ee5e31358

```

0000  00 90 cc 4f d0 80 00 0c 6e 49 1b 4a 08 00 45 00  ...O.... nI.J..E.
0010  01 a4 18 48 00 00 80 11 4f 7a c0 a8 01 66 8c 71  ...H.... OZ...f.q
0020  83 07 13 c4 13 c4 01 90 ce 8d 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:1 40.113.1
0040  33 31 2e 37 3a 35 30 36 30 20 53 49 50 2f 32 2e  31.7:506 0 SIP/2.

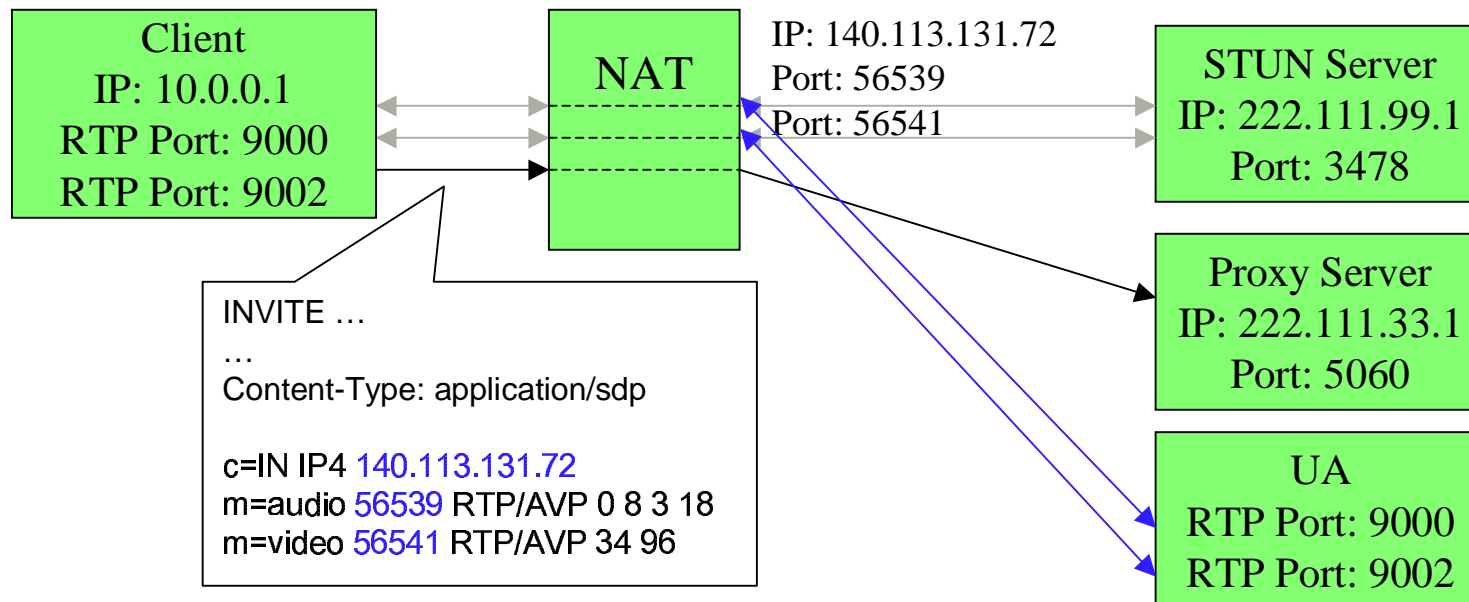
```

Filter: [ ] / Reset Apply <live capture in progress>



# Use STUN for RTP

- Send two STUN queries from RTP port (9000 & 9002) to STUN Server
- Use replied public address & port in SDP







# Corrected SDP



The Ethereal Network Analyzer

File Edit Capture Display Tools Help

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	140.113.131.2	STUN	Message : Binding Request
2	0.016250	140.113.131.2	192.168.1.102	STUN	Message : Binding Response
3	0.018516	192.168.1.102	140.113.131.2	STUN	Message : Binding Request
4	0.034725	140.113.131.2	192.168.1.102	STUN	Message : Binding Response
5	0.038840	192.168.1.102	140.113.131.7	SIP/SDP	Request: INVITE sip:980707325@140.113.131.7, with ses
6	0.045496	140.113.131.7	192.168.1.102	SIP	Status: 100 trying -- your call is important to us
7	0.057389	140.113.131.7	192.168.1.102	SIP	Status: 180 Ringing
8	14.746387	192.168.1.100	192.168.1.255	BROWSEI	Domain/workgroup Announcement VONTEL, NT Workstation,

.....

Frame 5 (961 bytes on wire, 961 bytes captured)

- Ethernet II, Src: 00:0c:6e:49:1b:4a, Dst: 00:90:cc:4f:d0:80
- Internet Protocol, Src Addr: 192.168.1.102 (192.168.1.102), Dst Addr: 140.113.131.7 (140.113.131.7)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
- Session Description Protocol
  - Session Description Protocol Version (v): 0
  - Owner/Creator, Session Id (o): 980707321 1694562 1694562 IN IP4 140.113.131.72
  - Session Name (s): session SDP
  - Connection Information (c): IN IP4 140.113.131.72
  - Bandwidth Information (b): CT:1000
  - Time Description, active time (t): 0 0
  - Media Description, name and address (m): audio 56539 RTP/AVP 0 8 3 4 18
  - Media Attribute (a): rtpmap:0 PCMU/8000/1
  - Media Attribute (a):ptime:20
  - Media Attribute (a): rtpmap:8 PCMA/8000/1
  - Media Attribute (a):ptime:20
  - Media Attribute (a): rtpmap:3 GSM/8000/1
  - Media Attribute (a):ptime:20
  - Media Attribute (a): rtpmap:4 G723/8000/1
  - Media Attribute (a):ptime:20
  - Media Attribute (a): rtpmap:18 G729/8000/1
  - Media Attribute (a):ptime:20
  - Media Description, name and address (m): video 56541 RTP/AVP 34 96
  - Media Attribute (a): rtpmap:34 H263/90000/2

.....

```

0000  00 90 cc 4f d0 80 00 0c 6e 49 1b 4a 08 00 45 00  ...O.... nI.J..E.
0010  03 b3 18 7f 00 00 80 11 4d 34 c0 a8 01 66 8c 71  ... .... M4...f.q
0020  83 07 13 c4 13 c4 03 9f 7c 69 49 4e 56 49 54 45  ..... |iINVITE
0030  20 73 69 70 3a 39 38 30 37 30 37 33 32 35 40 31  sip:980 707325@1
0040  34 30 2e 31 31 33 2e 31 33 31 2e 37 20 53 49 50  40.113.1 31.7 SIP
  
```

Filter: / Reset Apply <live capture in progress>



# Download

## ■ UACom.dll with STUN support

- Close your running SIP UA.
- Remove the UACom.dll file in your C:\WinApp\NBENUA directory.
- Download the new UACom.dll from <http://voip.ipv6.club.tw/Download/> and save it at C:\WinApp\NBENUA.
- Start SIP UA again. The registration and call setup will be successful.
- Our implementation supports incoming calls.

## ■ STUN Client

- A diagnosis tool which utilizes STUN mechanism to find out the type of NAT.
- Usage:
  - ☞ `stun-client STUN.ipv6.club.tw`
  - ☞ `stun-client -t STUN.ipv6.club.tw`
  - ☞ `stun-client -p 5060 STUN.ipv6.club.tw`
- Note: Be sure to close any running SIP UA before you run the STUN client.



# Running STUN Client on a PC

```
C:\WINDOWS\System32\cmd.exe

C:\WinApp\NBENUA>ipconfig

Windows IP Configuration

Ethernet adapter 區域連線:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 192.168.2.100
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.2.1

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : fe80::5efe:192.168.2.100%2
    Default Gateway . . . . .          : 

C:\WinApp\NBENUA>
```



# stun-client STUN.ipv6.club.tw

```
C:\WINDOWS\System32\cmd.exe
Encoding stun message:
Encoding ChangeRequest: 2

Encoding stun message:
Encoding ChangeRequest: 6

Encoding stun message:
Encoding ChangeRequest: 2

Encoding stun message:
Encoding ChangeRequest: 6

Encoding stun message:
Encoding ChangeRequest: 2

Encoding stun message:
Encoding ChangeRequest: 6

Encoding stun message:
Encoding ChangeRequest: 2

Cannot assign requested address
Internet connection is type: Port Restricted Nat

C:\WinApp\NBENUA>
```



# stun-client -t STUN.ipv6.club.tw

```
C:\WINDOWS\System32\cmd.exe
SourceAddress = 140.113.131.2:3478
ChangedAddress = 140.113.131.55:3479
    ok=1
    id=7:204:117:51:61:210:82:100:49:236:134:112:130:225:186:102
    mappedAddr=140.113.131.79:1533
    changedAddr=140.113.131.55:3479

Encoding stun message:
Encoding ResponseAddress: 140.113.131.79:1446
Encoding ChangeRequest: 0

About to send msg of len 40 to 140.113.131.2:3478
Encoding stun message:
Encoding ResponseAddress: 140.113.131.79:1446
Encoding ChangeRequest: 0

About to send msg of len 40 to 140.113.131.2:3478
Encoding stun message:
Encoding ResponseAddress: 140.113.131.79:1446
Encoding ChangeRequest: 0

About to send msg of len 40 to 140.113.131.2:3478
Refresh time is: 20 seconds

C:\WinApp\NBENUA>
```



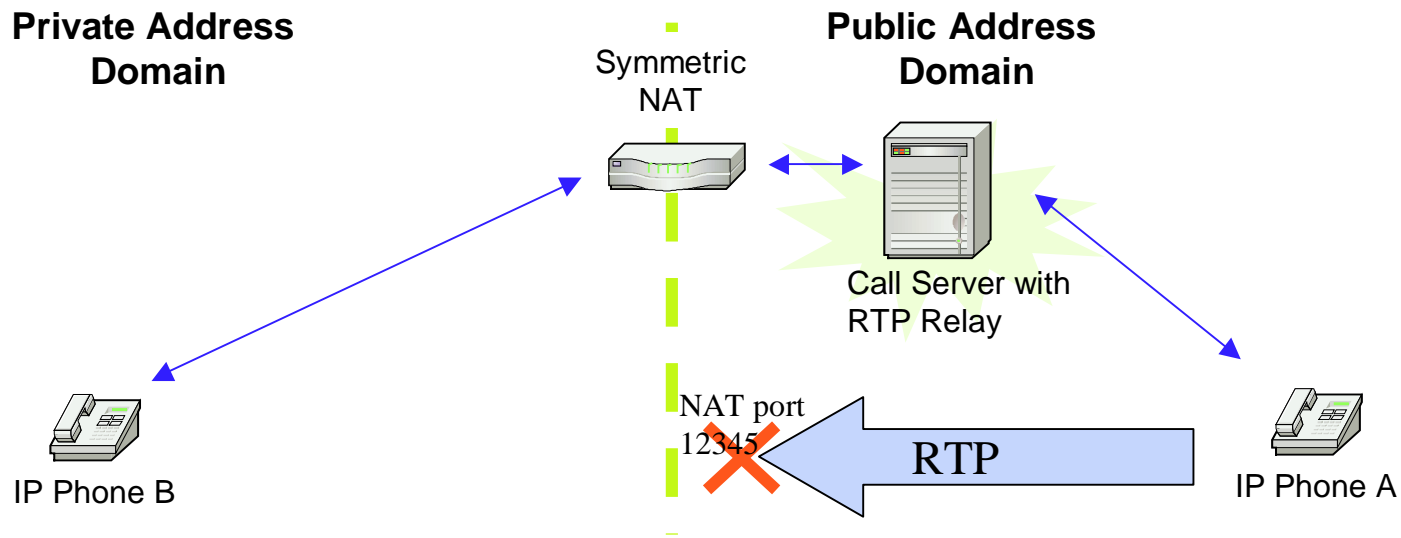
# Testing STUN & SIP UA

- Applying STUN mechanism in VoIP has been proved to be successful.
- More field trials must be conducted to make sure that it interoperates with most NAT devices.



# Clients Behind Symmetric NAT

- Provide a Call Server with RTP relay for non-upgradeable IP phone or Softphone
  - The loading for this server would be terribly heavy



Mapping Table	
192.168.10.1:5060	<-> 10120 (for Call Server : 5060)
192.168.10.1:9000	<-> 12345 (for Call Server : 9000)



# Summary

- STUN is a good solution for non-symmetric NAT
  - Suitable for small-scale solution
    - ☞ Client-side
    - ☞ Enterprise-server
  - Compatible with most NATs
  - STUN server is easy to implement and low-cost
- Call Server w/ RTP Relay may be needed, if the users cannot make sure whether they are behind a symmetric NAT
  - Capacity is limited
  - Centralized server is expensive
    - ☞ That's why Skype distributed the loading to individual users
- UPnP is a promising solution, but its nature is competing with IPv6.
  - Peer-to-Peer vs. Gateway/Device model