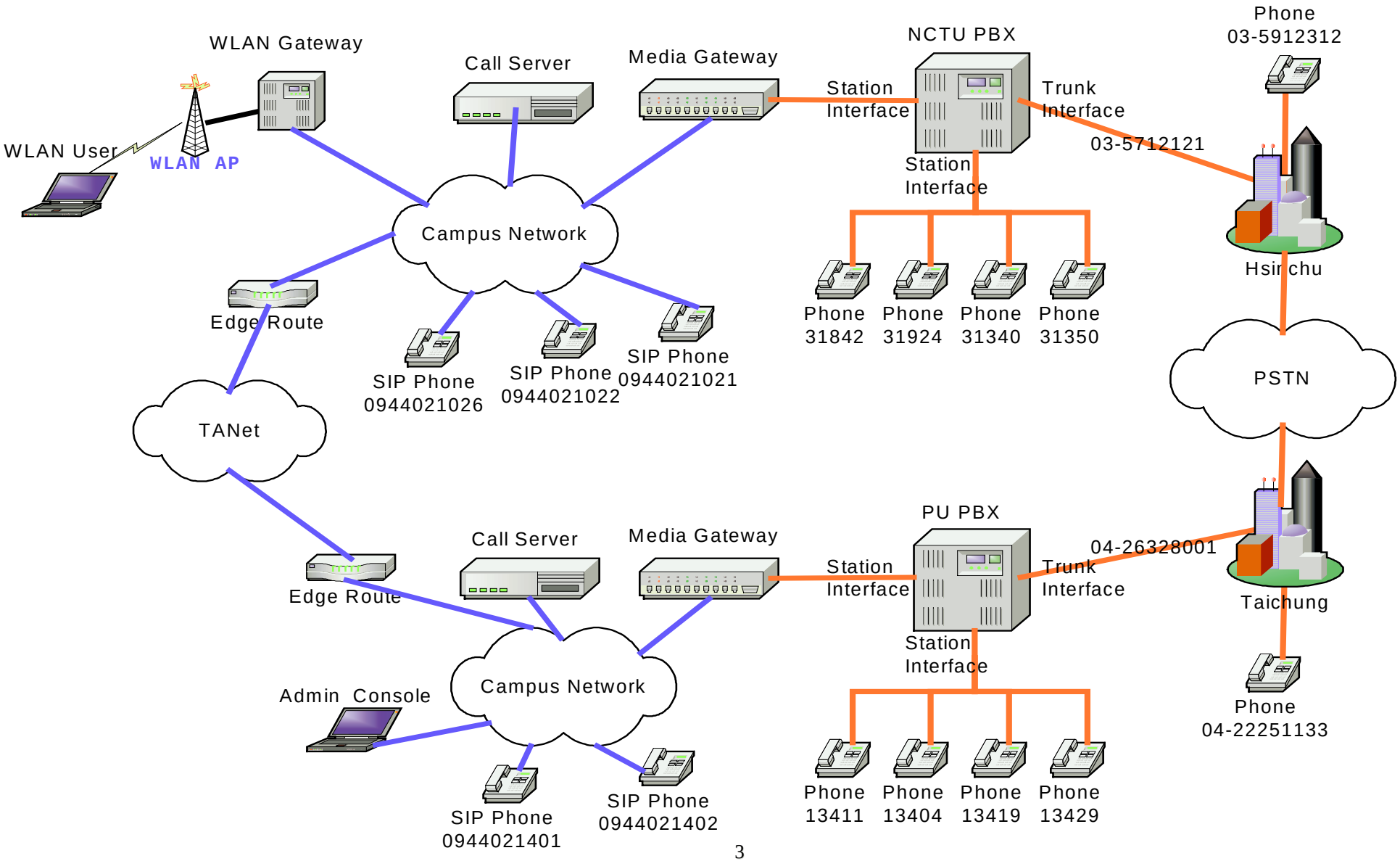
NAT Traversal for VoIP

Dr. Quincy Wu
National Chi Nan University
Email: solomon@ipv6.club.tw

NAT Traversal

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

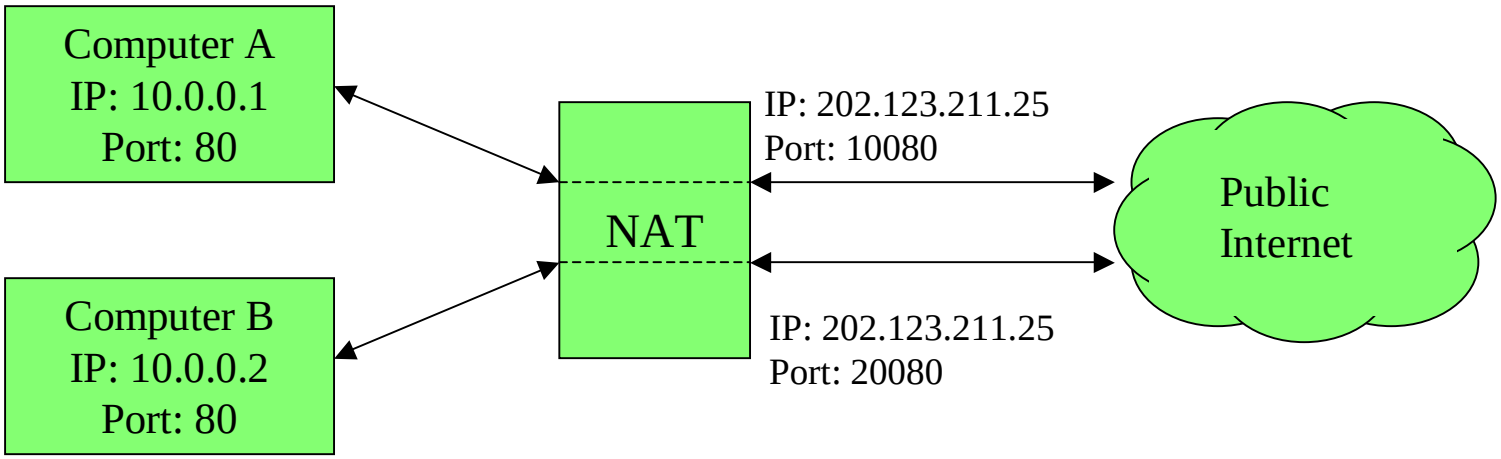
NTP VoIP Platform

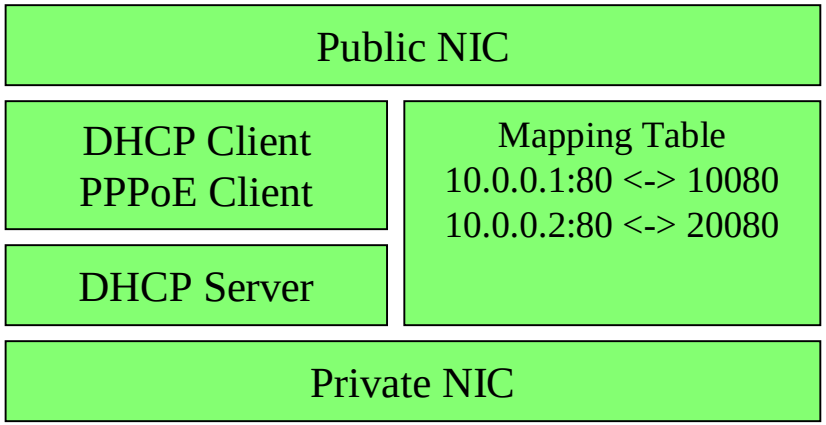


What is NAT

- 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



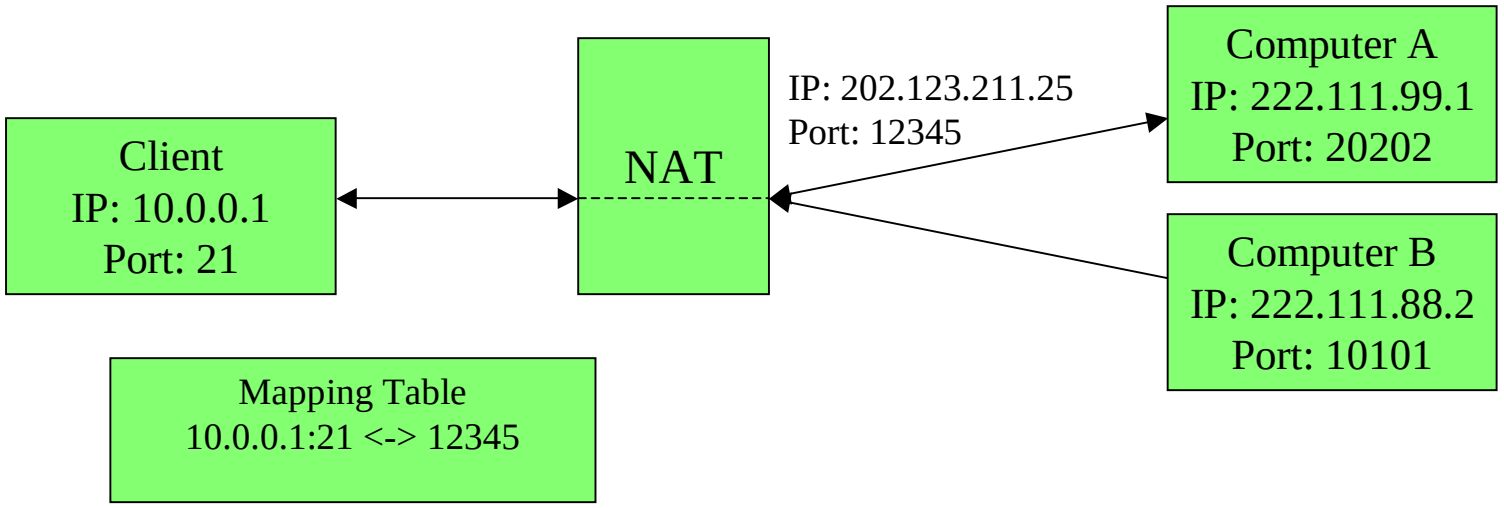


Types of NAT

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

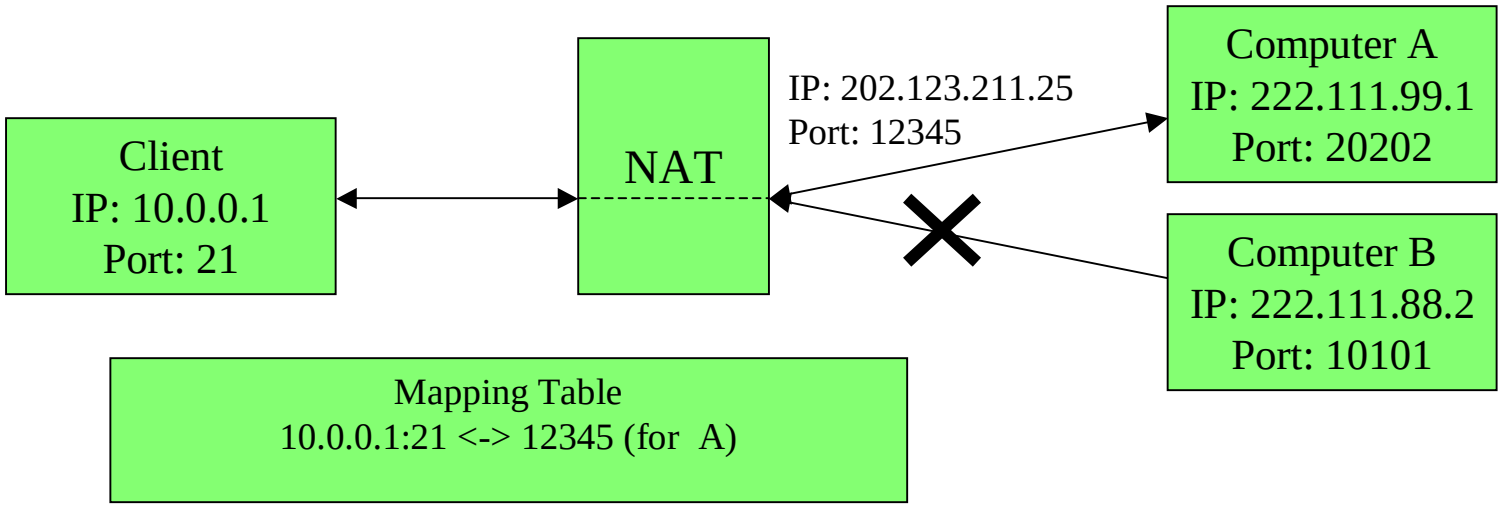
Full Cone NAT

- 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.



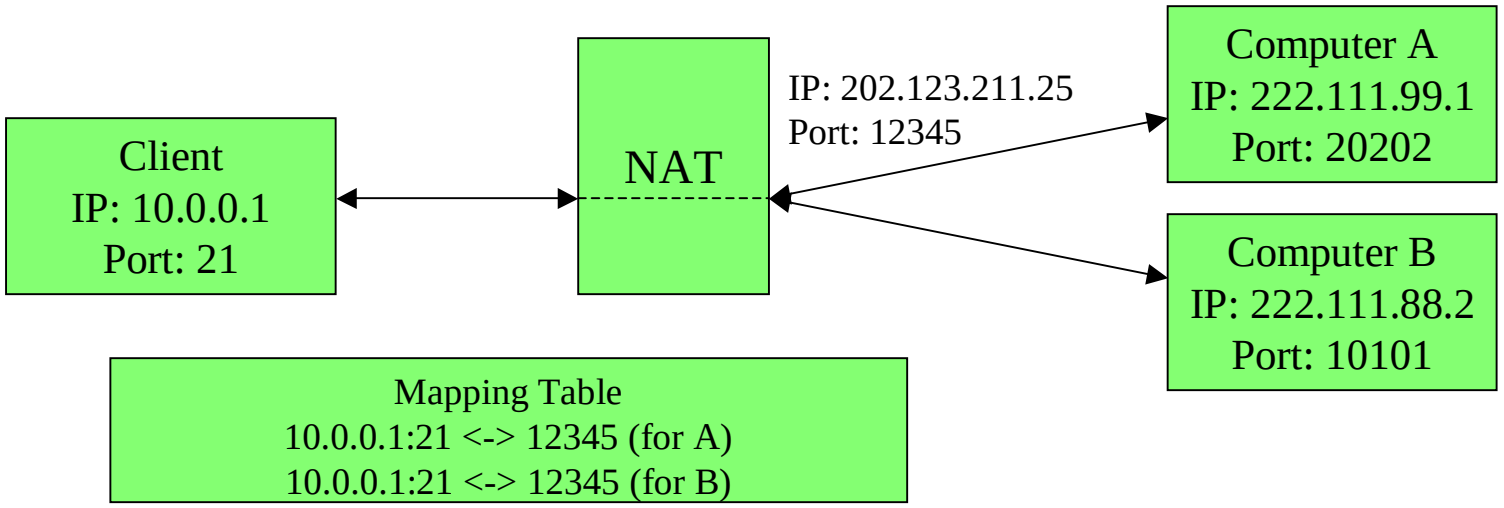
Restricted Cone NAT (1/2)

- 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.



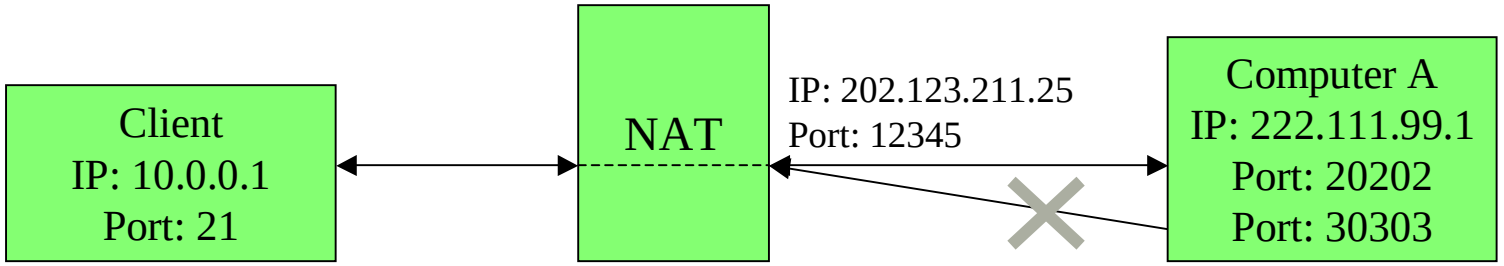
Restricted Cone NAT (2/2)

- 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

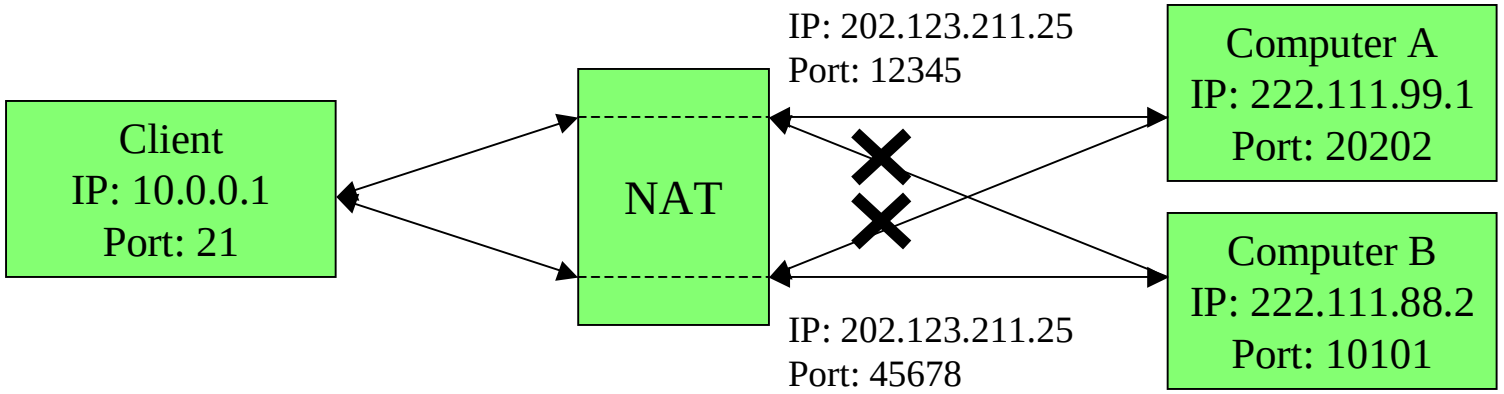
- Client send a packet to public address A port 20202.
- NAT will allocate a public port (12345) for private port (21) on the client.
- Only incoming packet from address A and port 20202 to public port (12345) will dispatch to private port (21) on the client.



Mapping Table
10.0.0.1:21 <-> 12345 (for A : 20202)
10.0.0.1:21 <-> 12345 (for A : 30303)

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



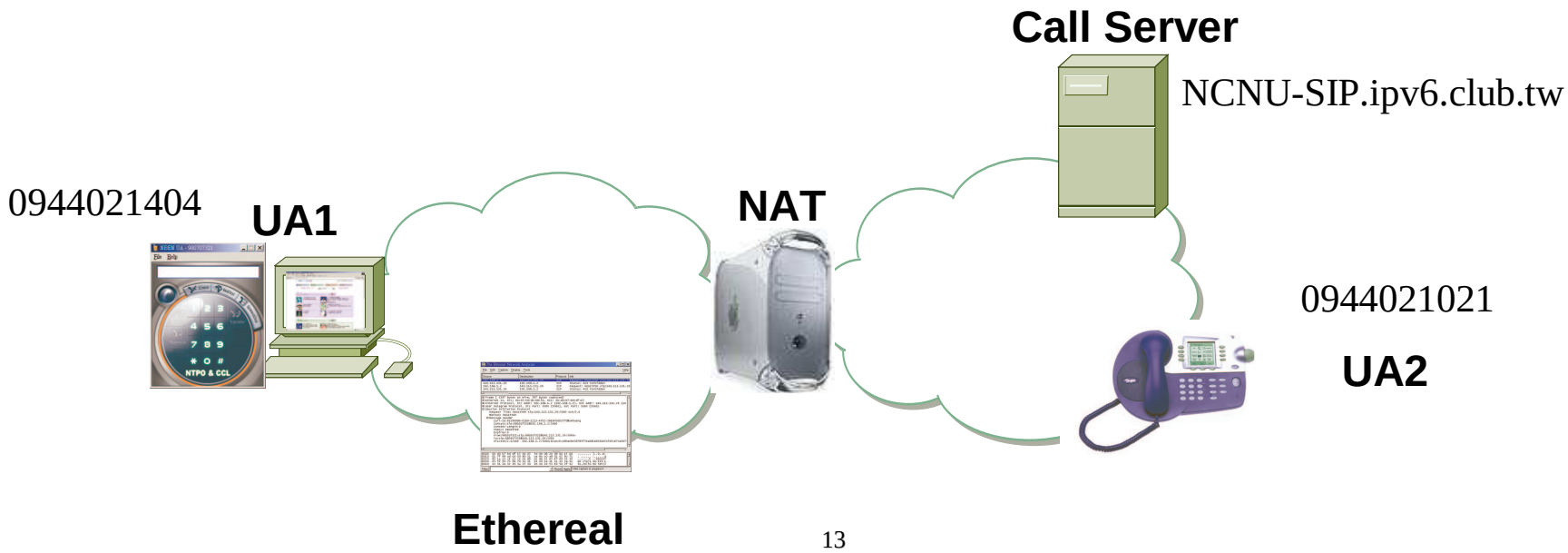
Mapping Table
10.0.0.1:21 <-> 12345 (for A : 20202)
10.0.0.1:21 <-> 45678 (for B : 10101)

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

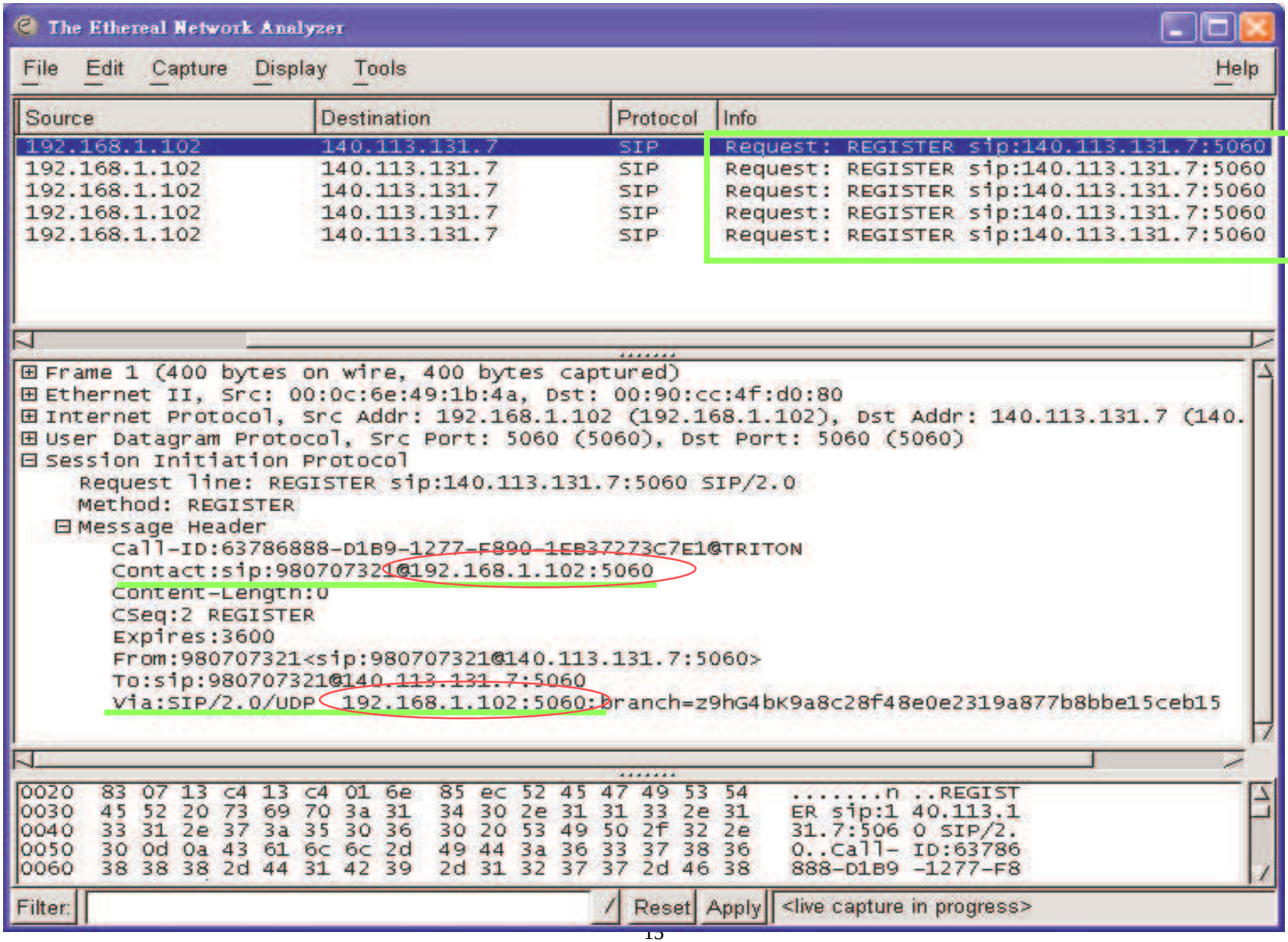
- UA1: UA behind NAT.
- UA2: SIP device outside NAT.
- Call Server: SIP-express router 0.8.12.
- NAT: Linux Fedora Core 2.
- Packet Capturer: Ethereal-0.9.15.



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 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

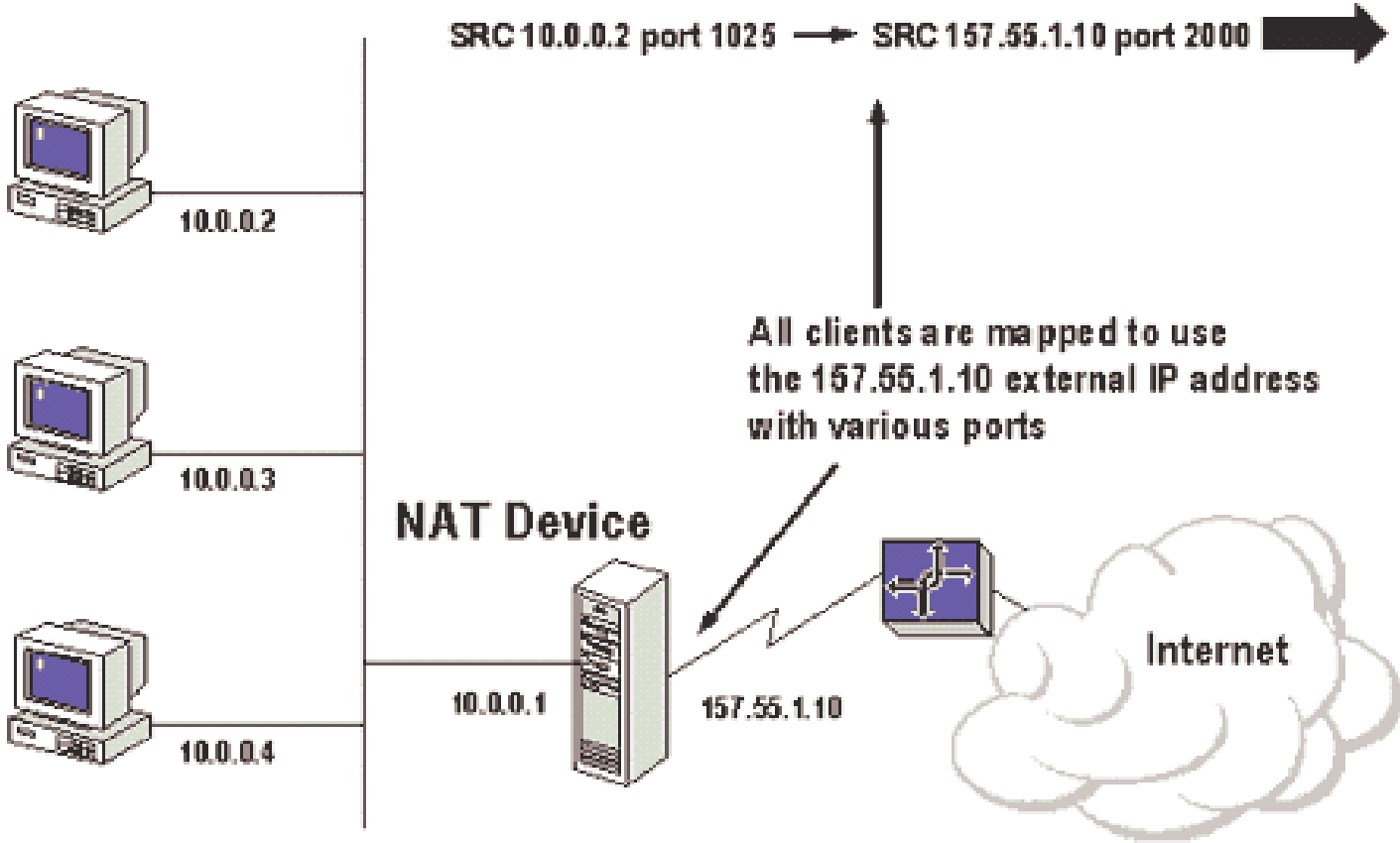
- IPv6 (Internet Protocol Version 6)
- UPnP (Universal Plug-and-Play)
  - UPnP Forum - http://www.upnp.org/
- VPN (Virtual Private Network)
- Proprietary protocol by NAT/Firewall
  - SIP ALG (Application Level Gateway)
  - No standard now. Not applicable for existing NATs.
- SIP extensions for NAT traversal
  - 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 爲一 UPnP Device (IGD)
    - ☞IGD -- Internet Gateway Device

NAT 網路架構


SRC 10.0.0.2 port 1025
SRC 157.55.1.10 port 2000
10.0.0.2
10.0.0.3
10.0.0.4
All clients are mapped to use
the 157.55.1.10 external IP address
with various ports
NAT Device
10.0.0.1
157.55.1.10
Internet

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 /upnphost/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

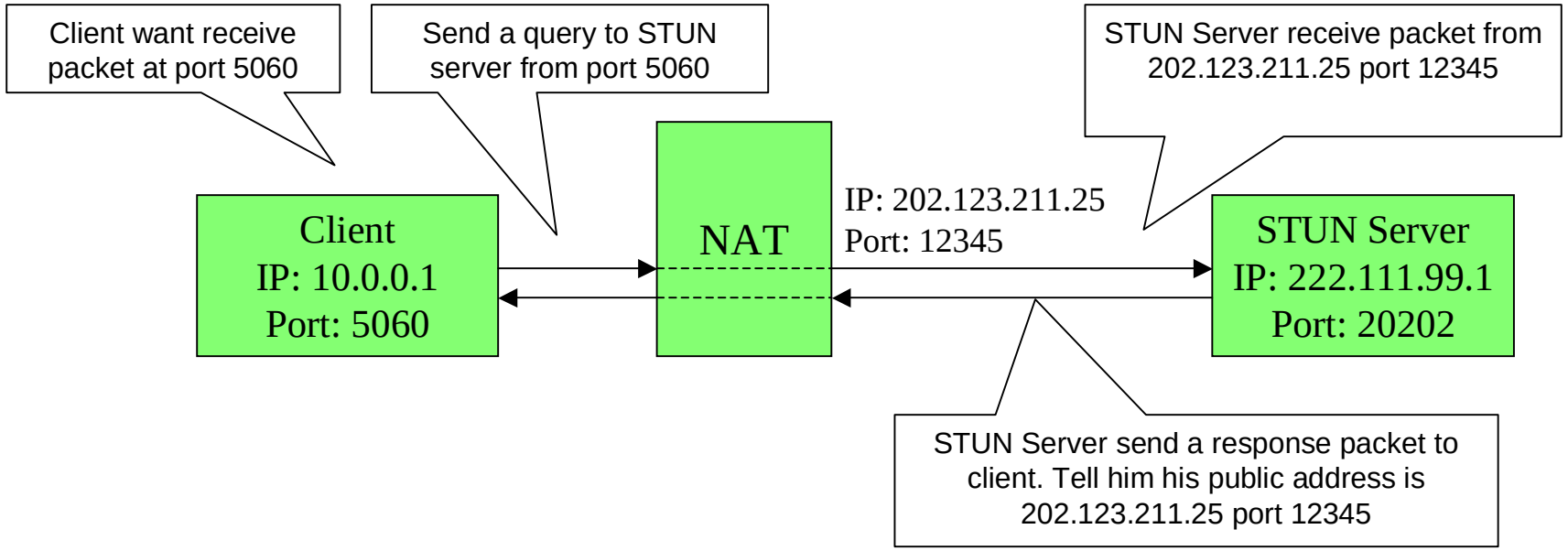
Simple Traversal of UDP Through Network Address Translators (STUN)

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.

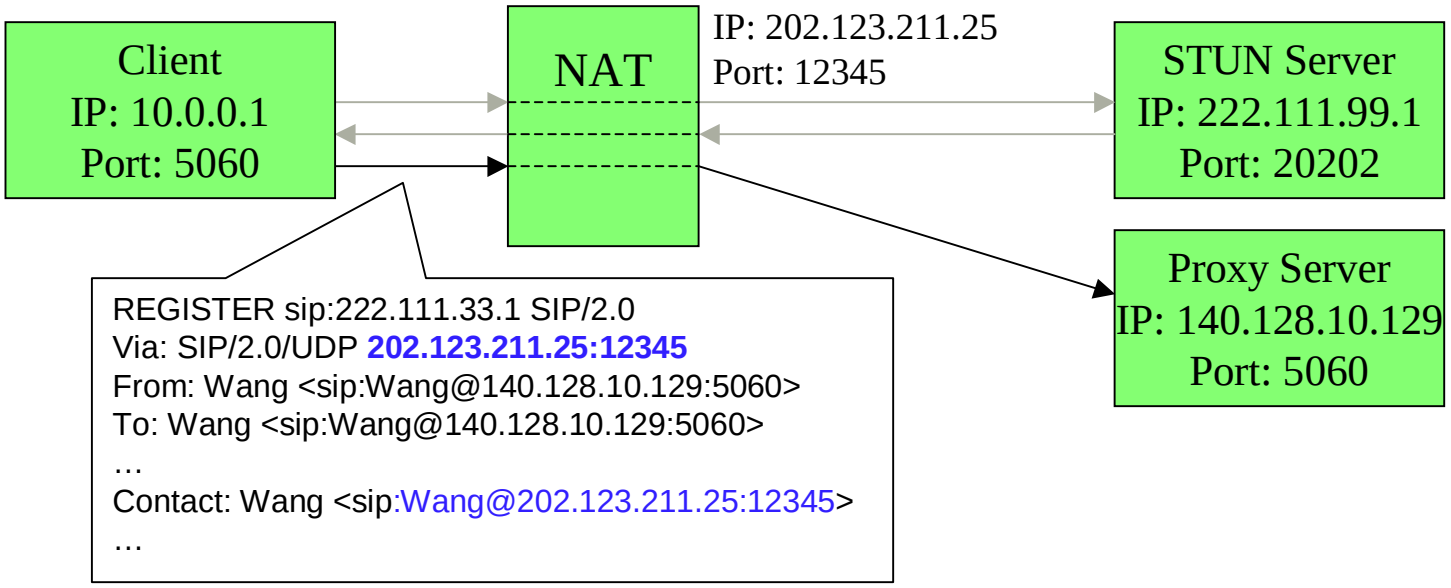
STUN Server

- 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

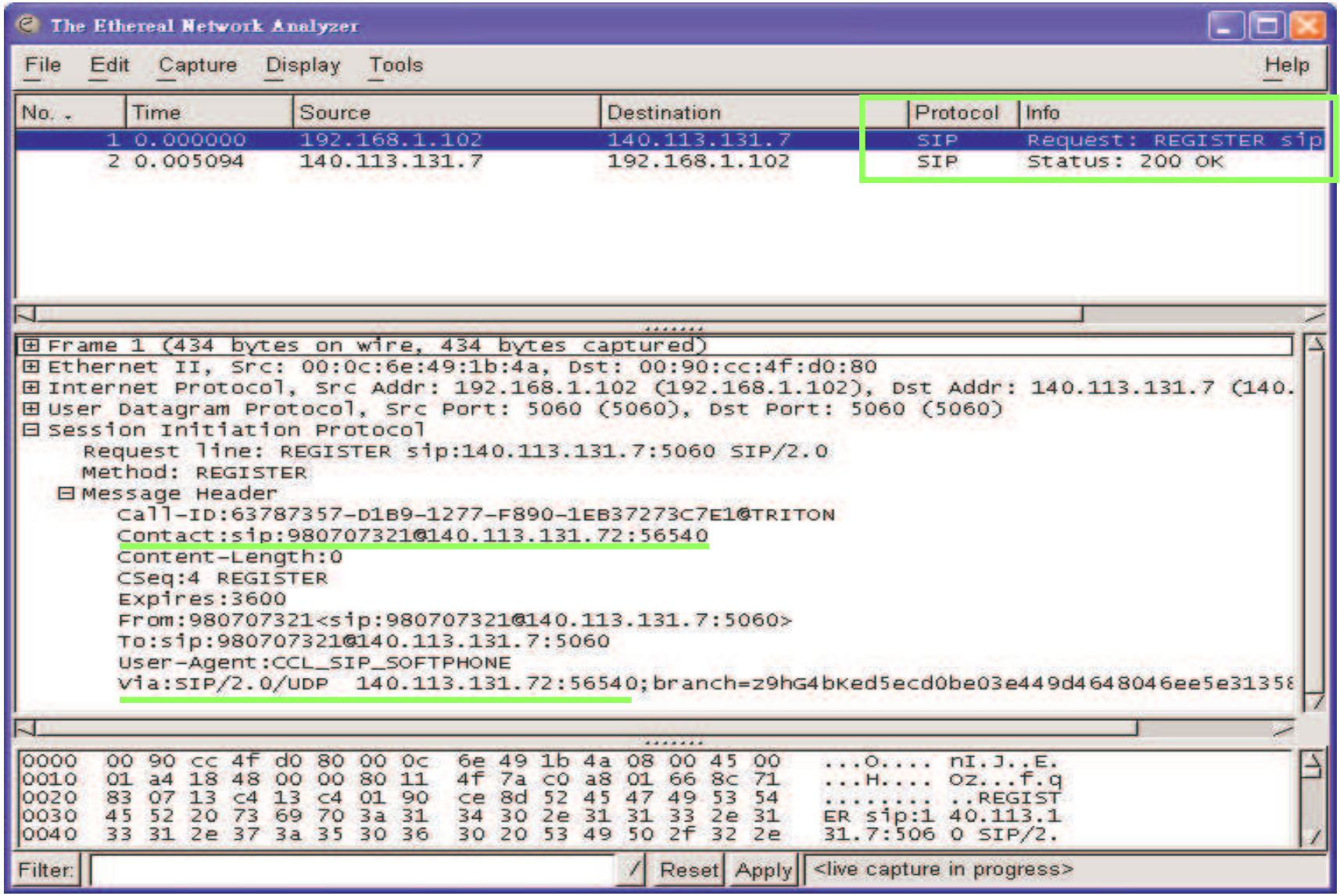


Use STUN for SIP Registration

- 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

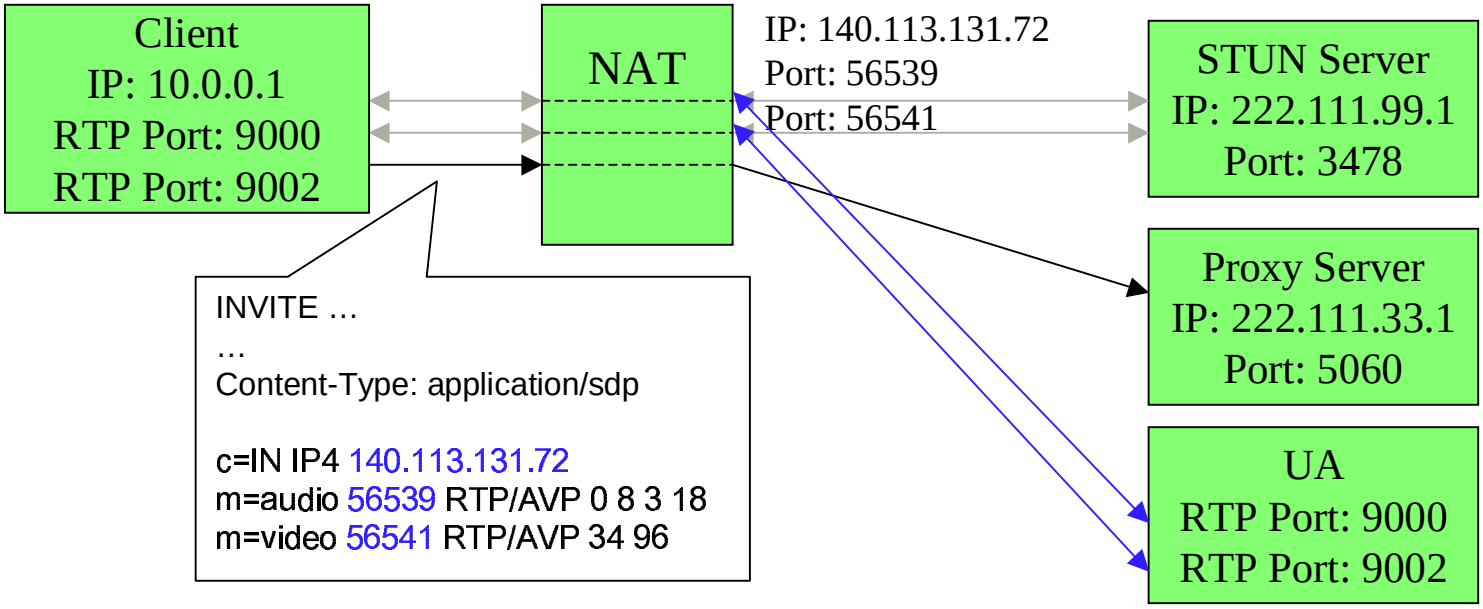


Corrected SIP Message

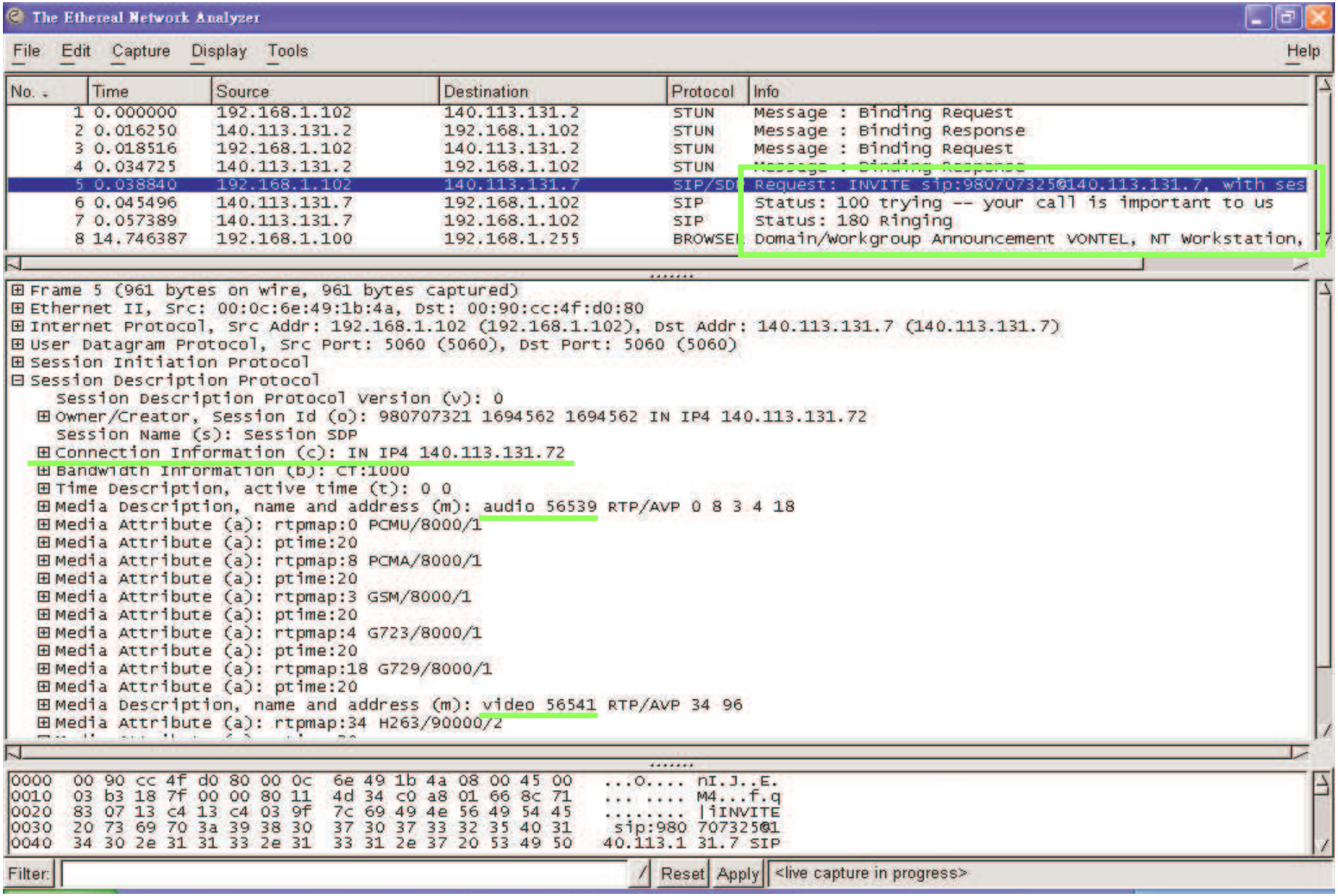


Use STUN for RTP

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



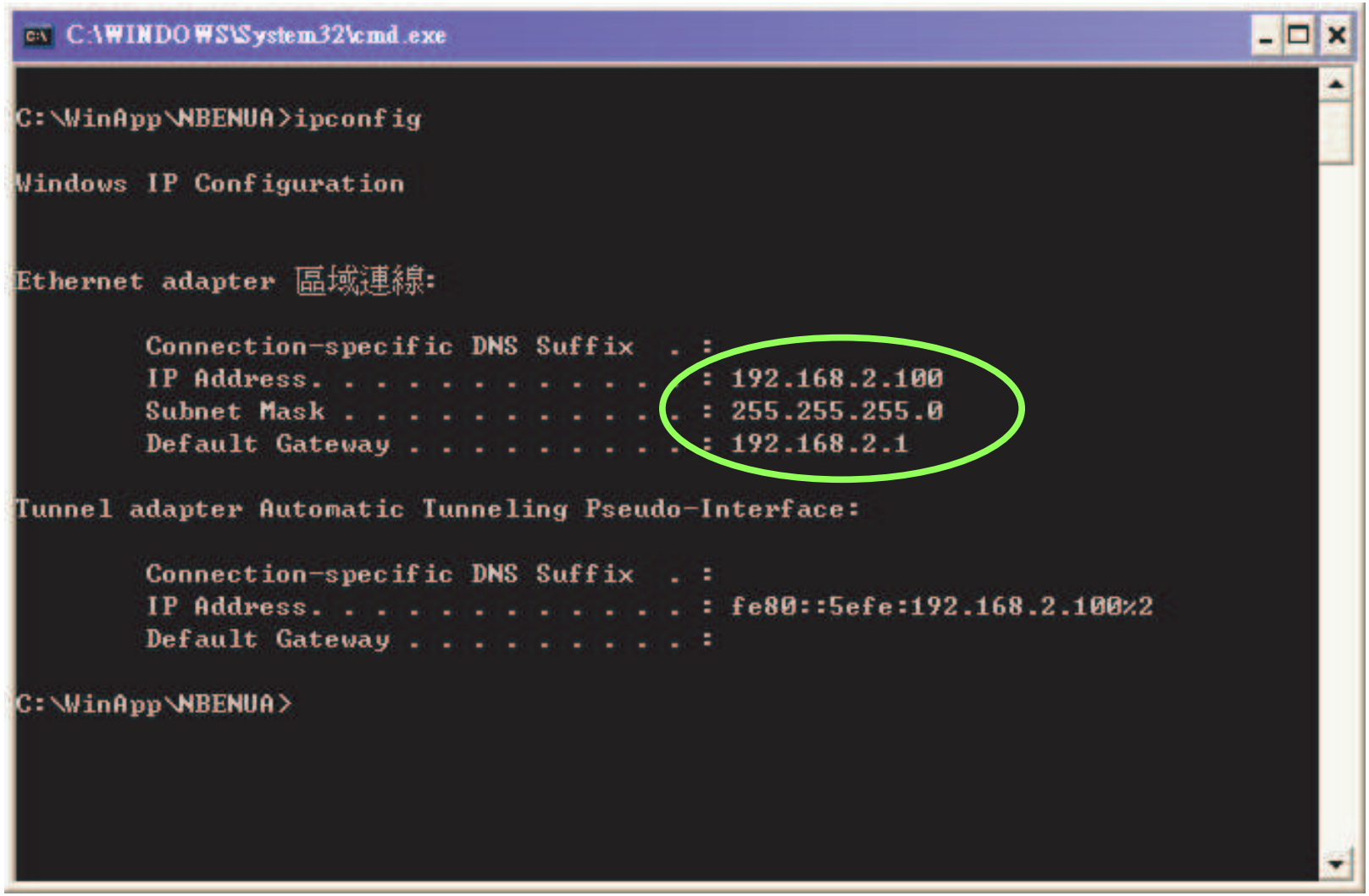
Corrected SDP



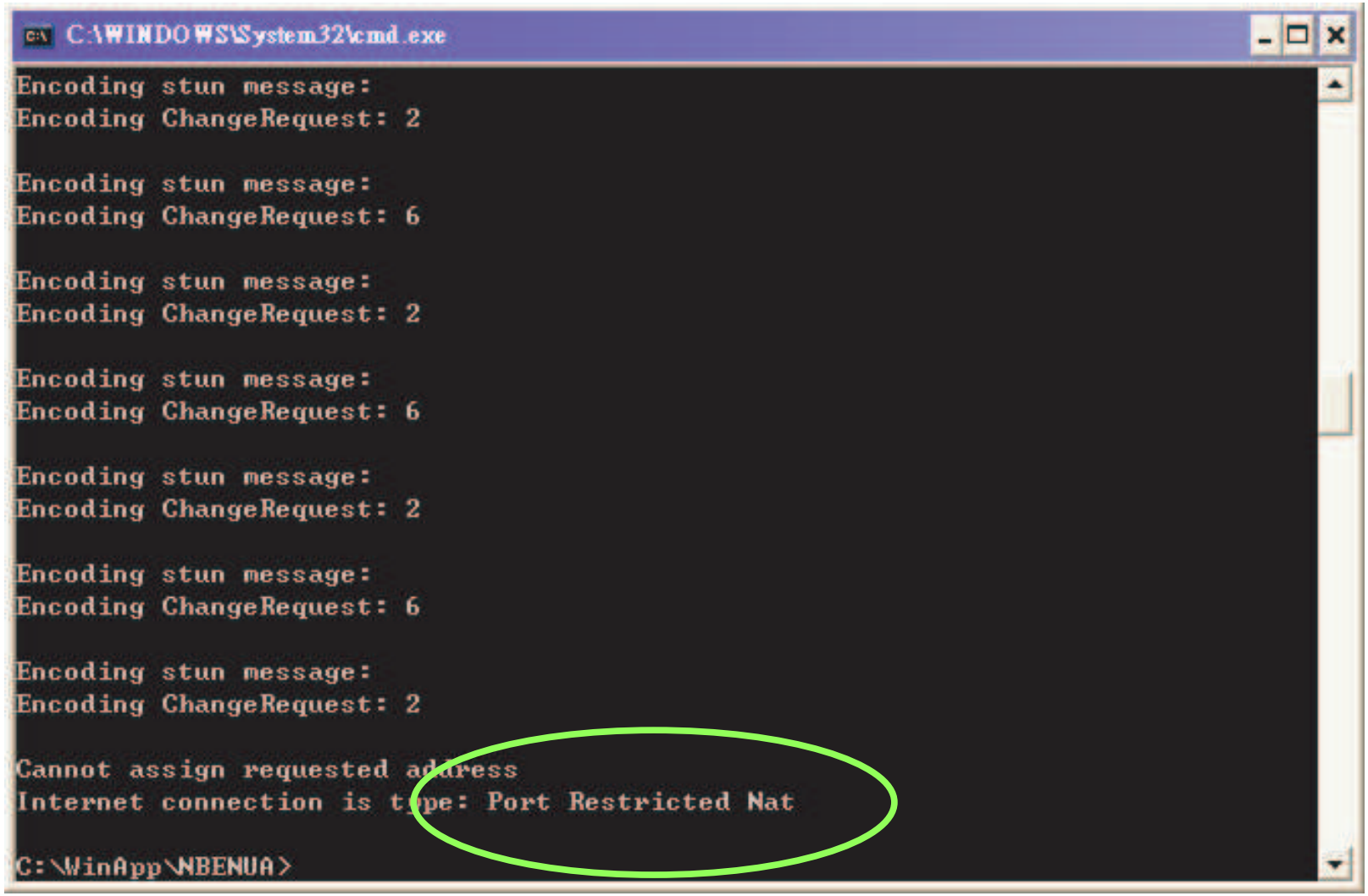
Download

- 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.

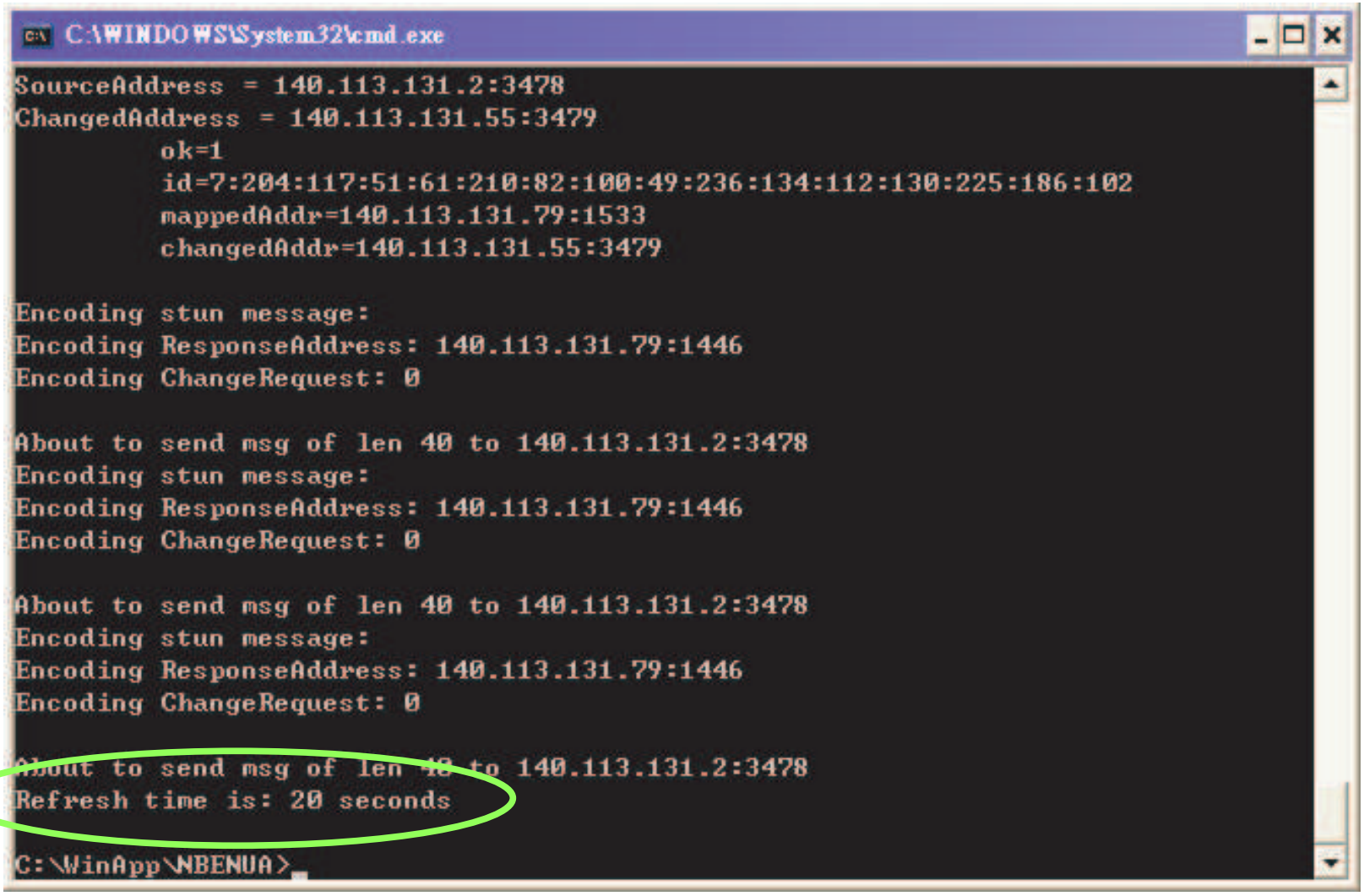
Running STUN Client on a PC



stun-client STUN.ipv6.club.tw



stun-client –t STUN.ipv6.club.tw

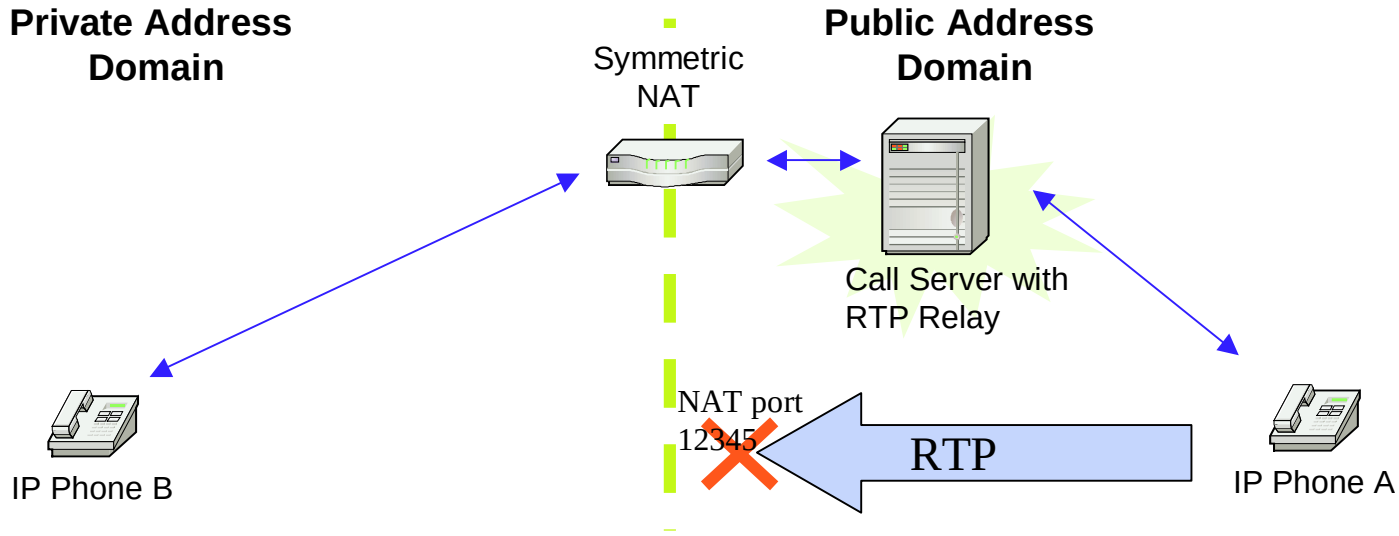


Testing STUN & SIP UA

- 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