

# Security in IP Telephony: selected topics

Saverio Niccolini, Ph. D.  
Research Staff Member @ Network Laboratories  
NEC Europe Ltd., Heidelberg, Germany

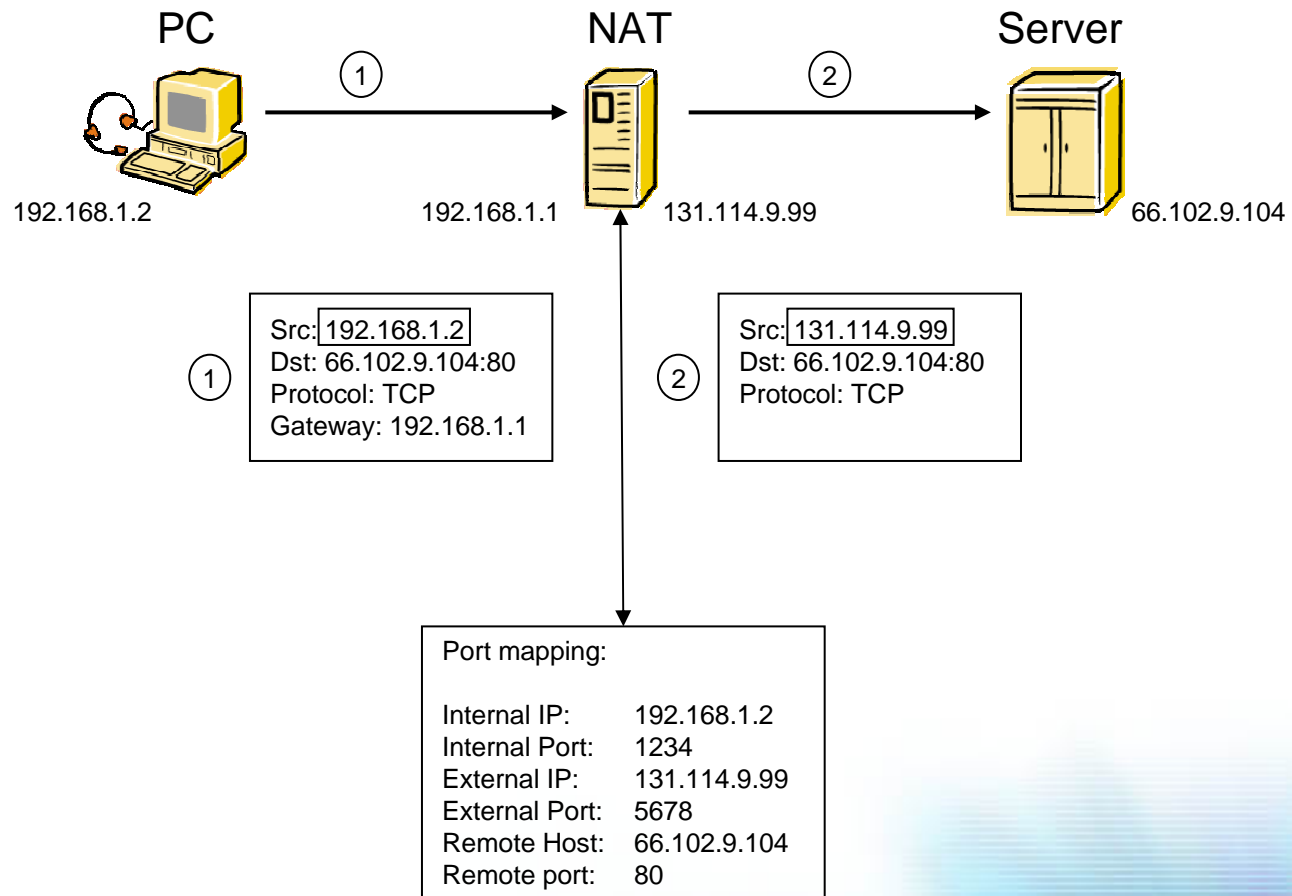
# SIP and Security

- Firewalls and NATs
- Security
  - Privacy
  - Encryption
  - Authentication
  - Denial of Service (DoS) attacks
  - Intrusion attacks
  - SPAM over Internet Telephony (SPIT)

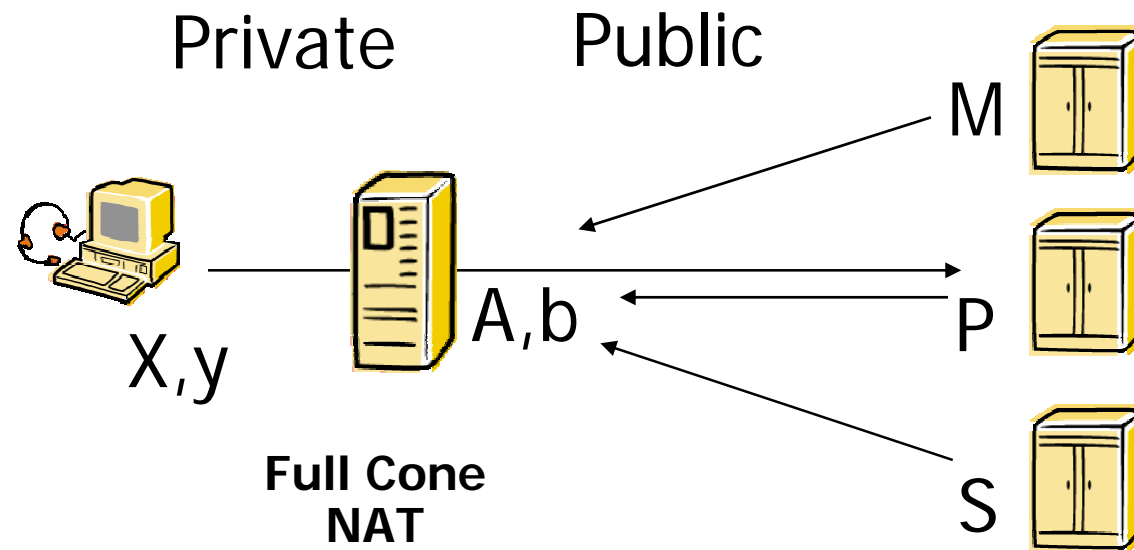
# SIP and Security: NATs and FWs

- NATs (Network Address Translators)
  - “light” security device
    - topology hiding
    - basic firewall functionality
  - number of NATs is growing (broadband at home, etc.)
    - reducing number of IP addresses
      - shortage of address in the IPv4 world
  - With IPv6 we would not need NATs anymore
    - even if it is probable that you will still be using NATs as light security mean
    - (I am still waiting for IPv6 to be commonly adopted)
- FWs (Firewalls)
  - security device
  - numbers of FWs is growing (including personal FWs)
  - FWs rules get more restrictive

# NATs: Basic Operation

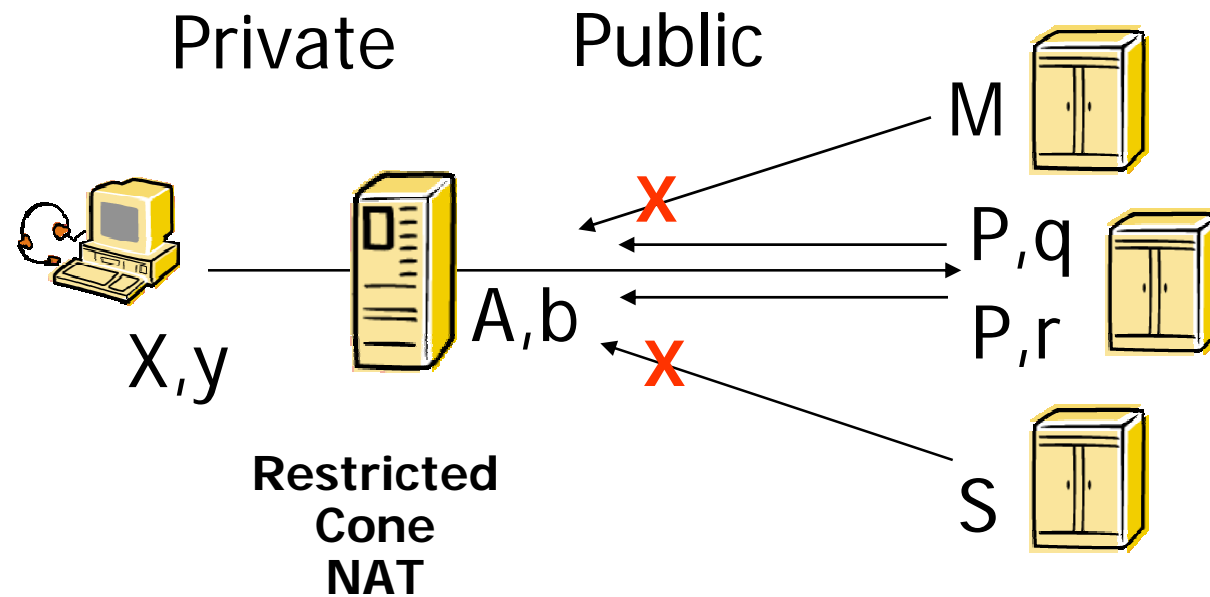


# Types of NATs: Full Cone NAT



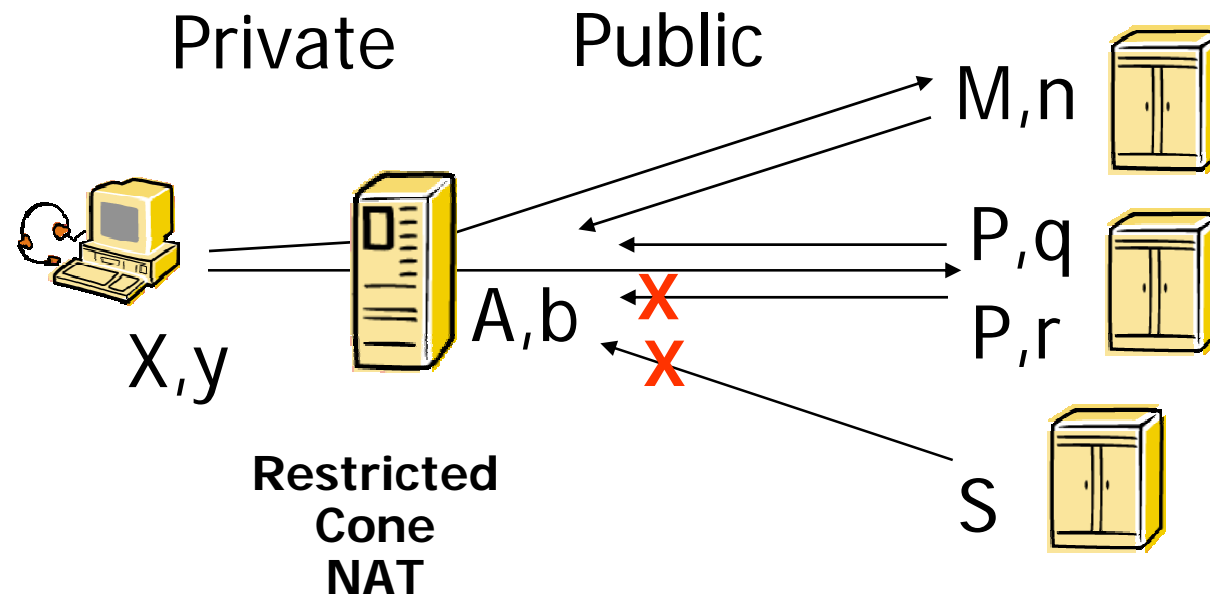
- No restrictions on IP traffic arriving at  $(A,b)$

# Types of NATs: Restricted Cone NAT



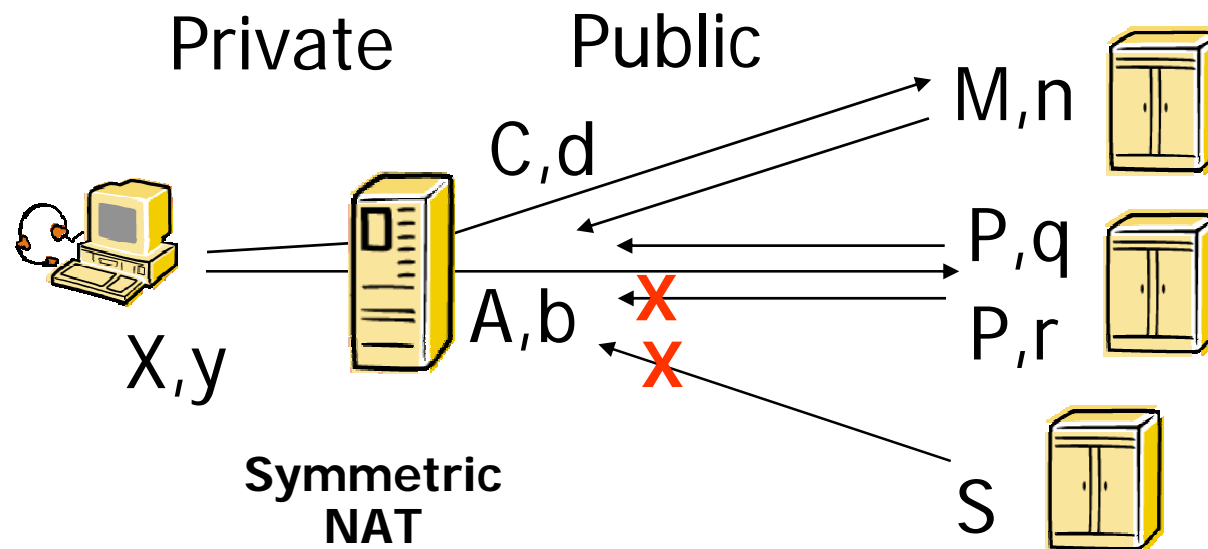
- Restricts at  $(A,b)$  only based on public IP address
  - not on public port
- If  $(X,y)$  sends to  $(P,q)$ 
  - $(P,r)$  can send back to  $(A,b)$

# Types of NATs: Port Restricted Cone NAT



- Restricts at  $(A,b)$  only based on public IP address and port number
- If  $(X,y)$  sends to  $(P,q)$ 
  - $(P,r)$  can not send back to  $(A,b)$

# Types of NATs: Symmetric NAT



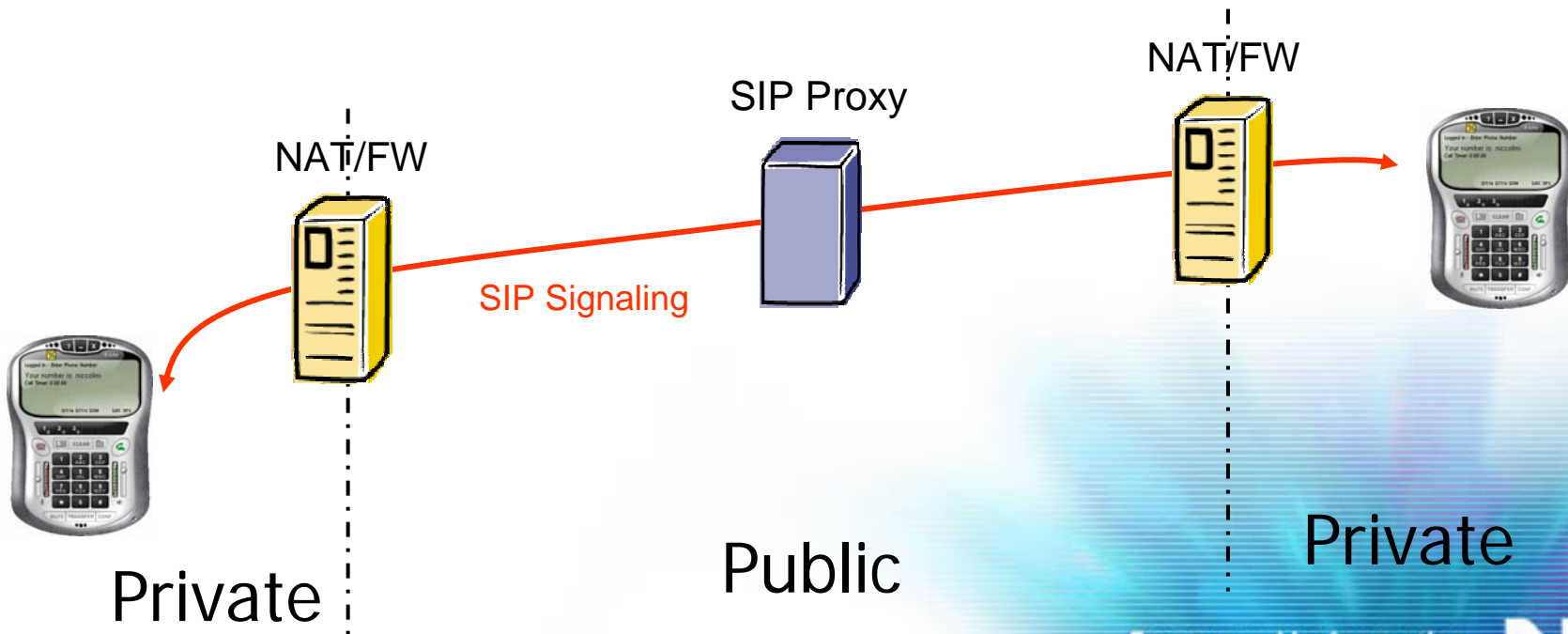
- Restricts at  $(A,b)$  only based on public IP address and port number
- If  $(X,y)$  sends to  $(P,q)$ 
  - $(P,r)$  can not send back to  $(A,b)$
- Creates a new instance  $(C,d)$  for each unique public IP address that it sends to

# SIP Problems with NATs/FWs

- Different issues with
  - SIP signaling
  - Media
- SIP signaling and media transport is done peer-to-peer
- Media ports are negotiated per call

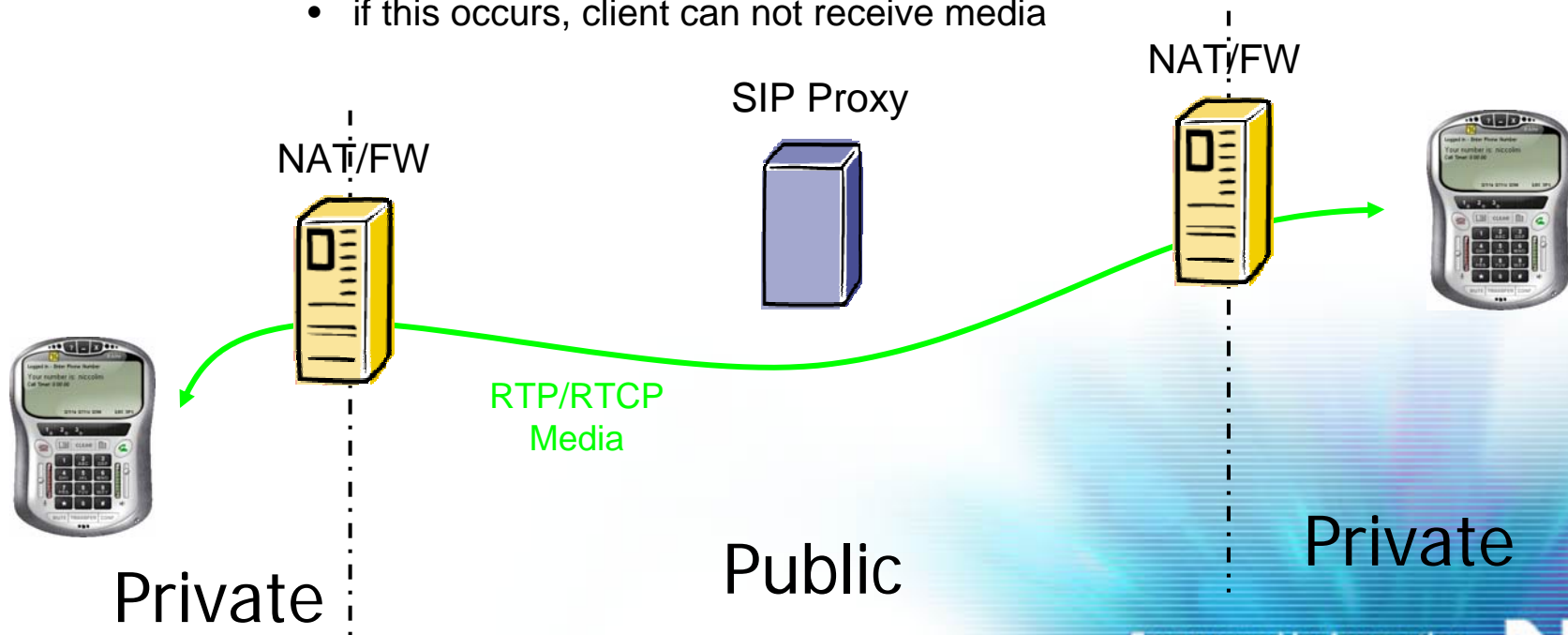
# SIP signaling Issues

- SIP proxy does not communicate back to SIP client on NAT'ed channel
- Pinhole in NAT/FW will timeout on inactivity
  - typically less than 1 minute
    - if this occurs, client can not receive incoming call



# Media Traversal Issues

- IP address and port sen in SIP INVITE / 200 OK (SDP) is private
  - not globally routable
- Media must be initiated in Private→Public direction
- RTCP (RTP port + 1) fails through firewall because of NAPT function (port translation)
- Pinhole in NAT/FW will timeout on inactivity (silence suppression)
  - typically less than 1 minute
    - if this occurs, client can not receive media

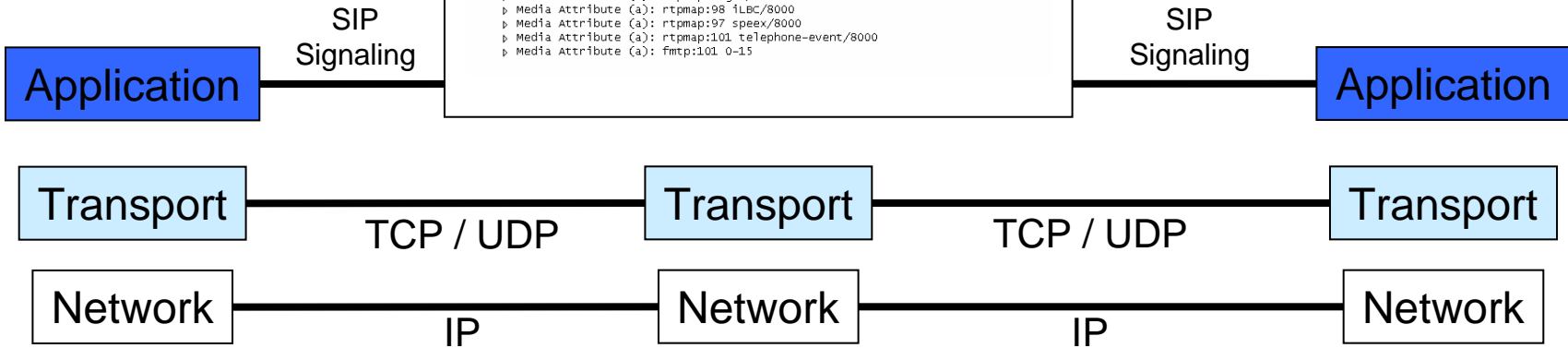


# Media Traversal Issues

SDP in SIP Signaling says:  
I receive RTP at 10.1.1.117:4567

```

    Message body
    - Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): niccolini 11990551 11990581 IN IP4 10.1.1.177
      Session Name (s): X-Lite
      Connection Information (c): IN IP4 10.1.1.177
      Time Description, active time (t): 0 0
      Media Description, name and address (m): audio 8000 RTP/AVP 0 8 3 98 97 101
      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:98 iLBC/8000
      Media Attribute (a): rtpmap:97 speex/8000
      Media Attribute (a): rtpmap:101 telephone-event/8000
      Media Attribute (a): fmtp:101 0-15
  
```



10.1.1.117

NAT



10.1.1.1

131.114.9.99

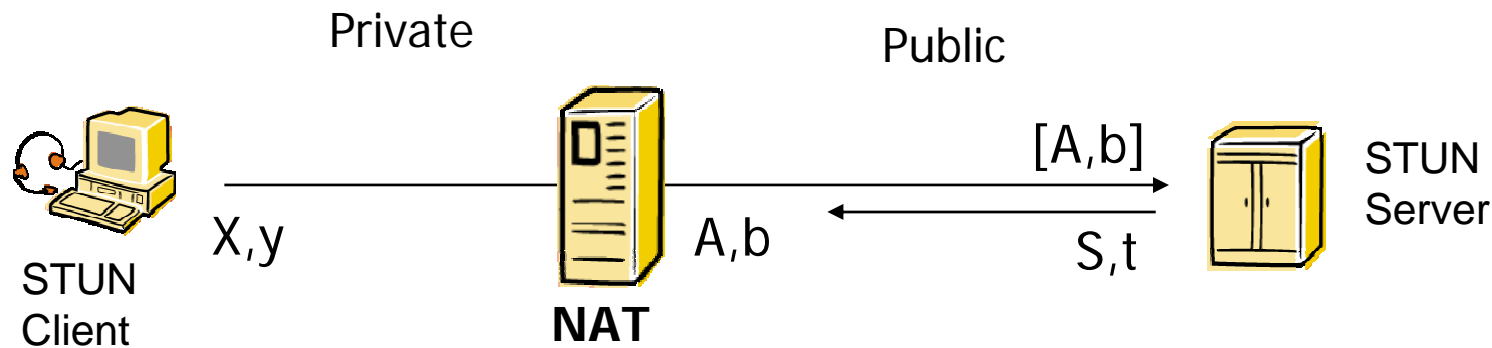


66.102.9.104

# Solutions to NAT Traversal

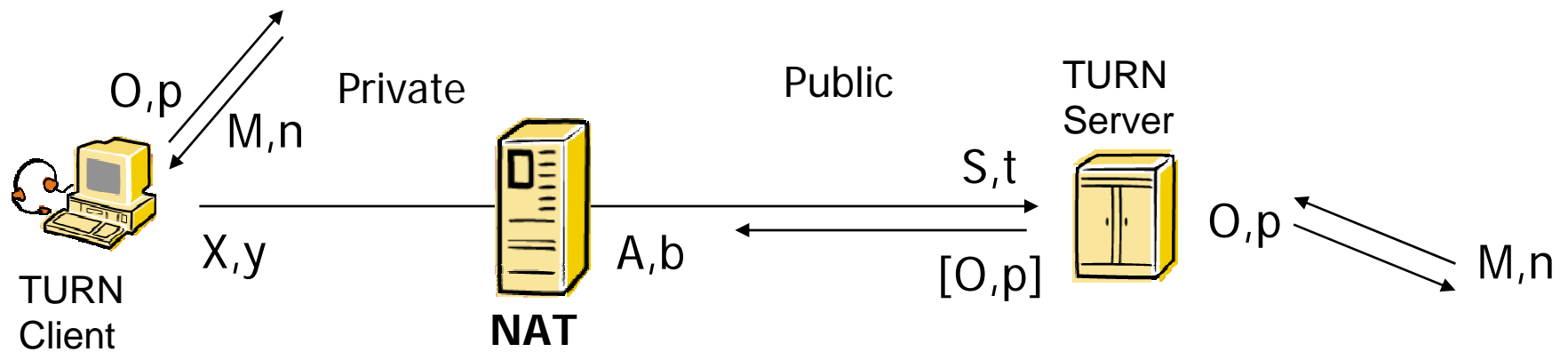
- STUN
  - TURN
  - ICE
  - B2BUA
- 
- All these solutions require UA to support symmetric signaling and media

# Solutions to NAT Traversal: STUN



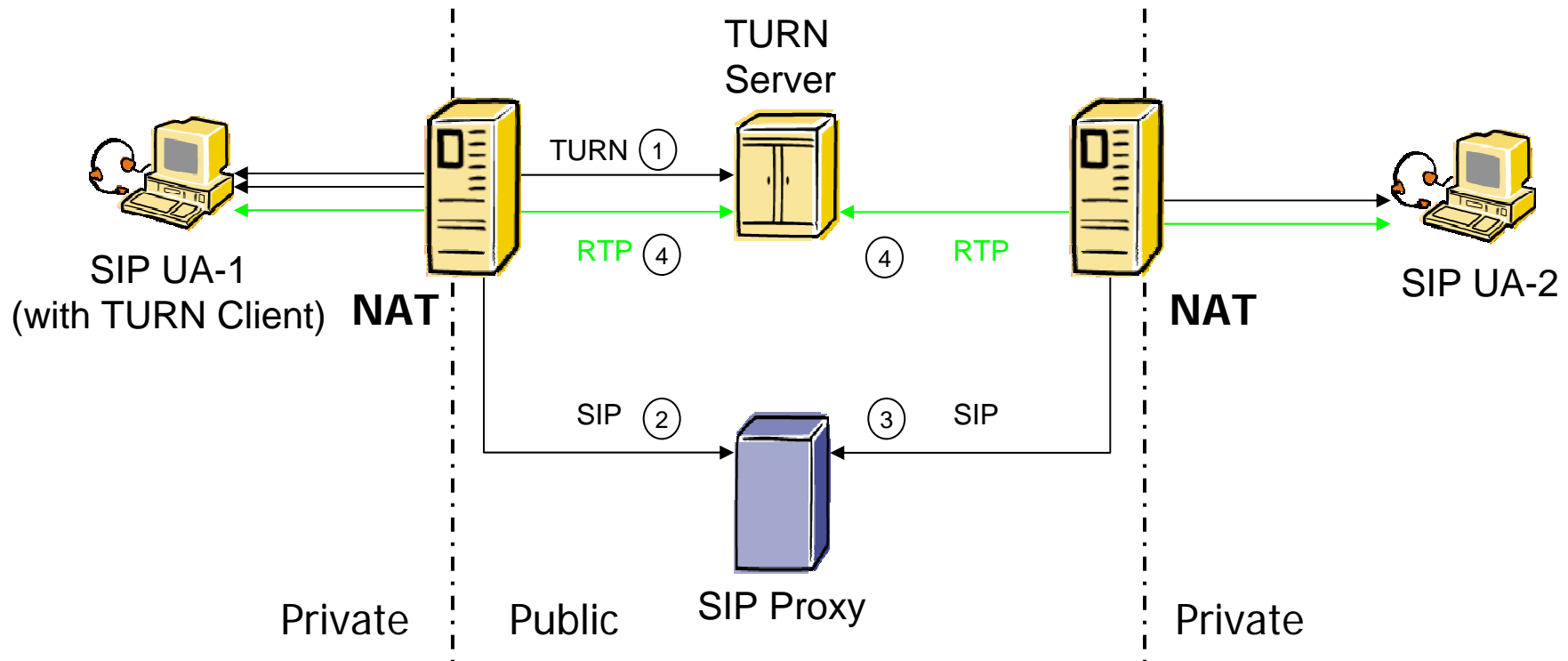
- IETF RFC 3489 “STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)”
  - discover public IP address (and port mapping rules) of NAT between client and Internet
  - does not work with Symmetric NATs used by most corporate environments
  - does not work if both clients are behind the same NAT
  - requires a STUN client in the SIP UA
    - best SIP UA have STUN support (Xten software, Zyxel WiFi phone)
  - requires additional deployment of a STUN server placed in the public space (normally co-located with the SIP Proxy server)
    - open-source stund server works perfectly with Xten products, Zyxel WiFi phone

# Solutions to NAT Traversal: TURN



- IETF MIDCOM draft “Traversal Using Relay NAT (TURN)”
  - draft-rosenberg-midcom-turn-07
  - protocol for allowing a client behind a NAT to receive incoming media over UDP
  - work with Symmetric NATs
  - it introduces a relay
    - single point of failure
    - need for server with high performance to avoid adding too much latency
  - few clients support TURN today (not yet a standard)
  - no free TURN server available (only commercial)

# Solutions to NAT Traversal: TURN

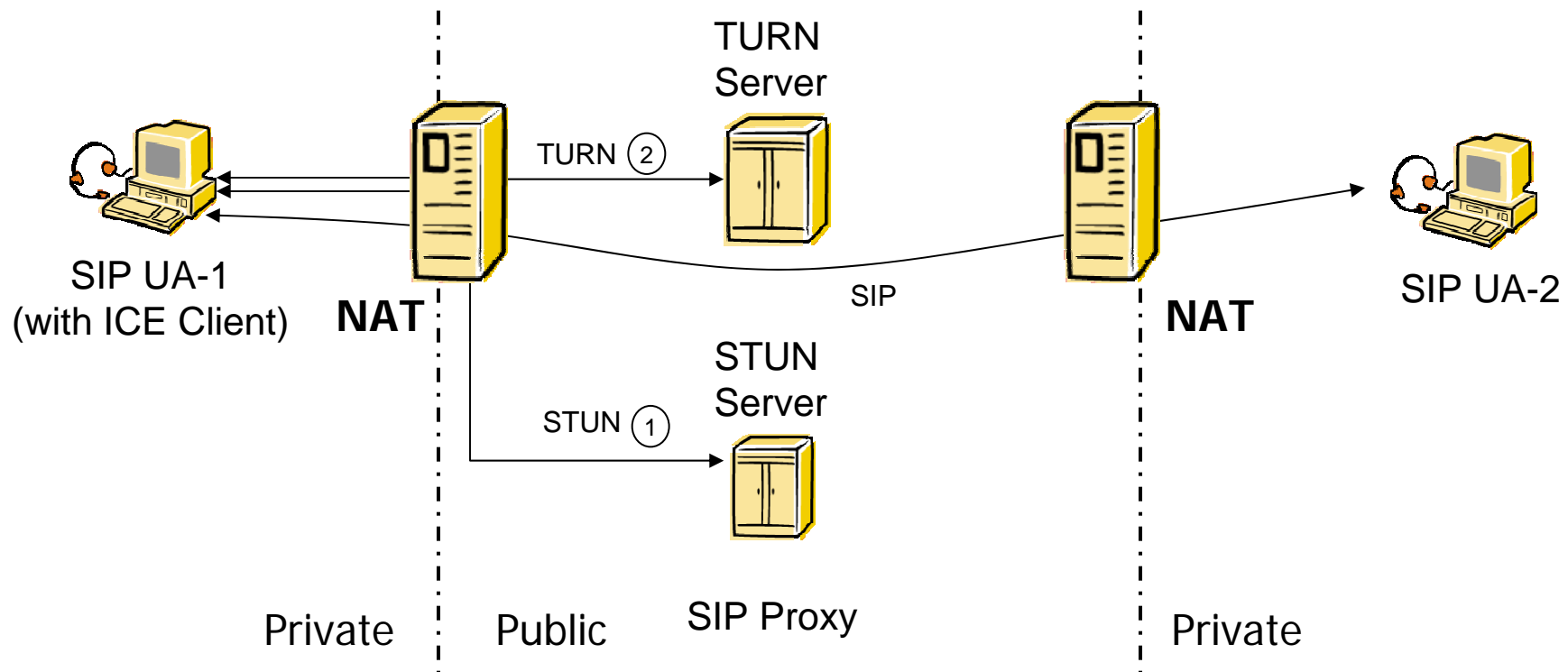


1. On request, the TURN server returns a globally reachable IP/Port pair
2. SIP invite using this IP/Port pair goes to SIP proxy
3. SIP invite goes to UA-2 (pinhole has been kept open by SIP proxy)
4. RTP is rerouted via TURN server (pinholes on both sides are opened by first RTP packet)

# Solutions to NAT Traversal: ICE

- IETF MMUSIC draft “Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Multimedia Session Establishment Protocols
  - draft-ietf-mmusic-ice-04
  - allows peers to discover NAT types and client capabilities
  - provide in SIP signaling many (ordered) alternatives, typically including STUN and TURN
  - few clients support TURN today (not yet a standard)
  - works with all types of NATs

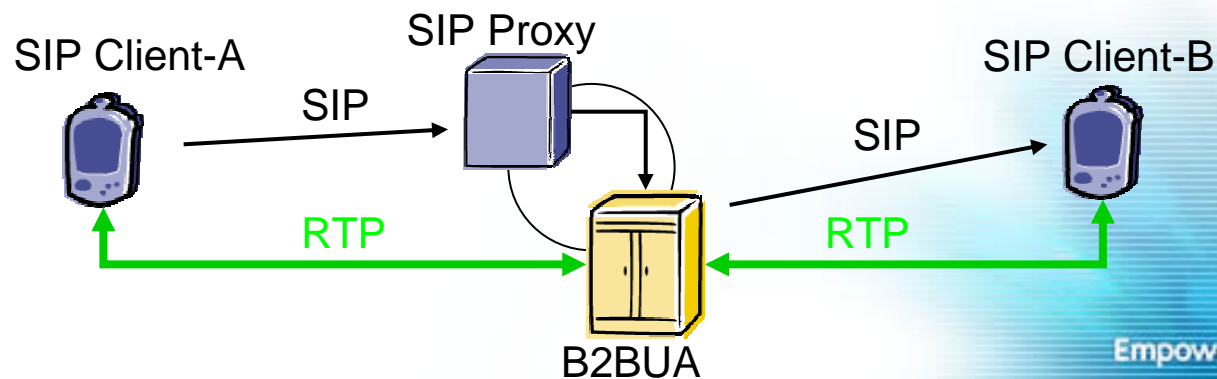
# Solutions to NAT Traversal: ICE



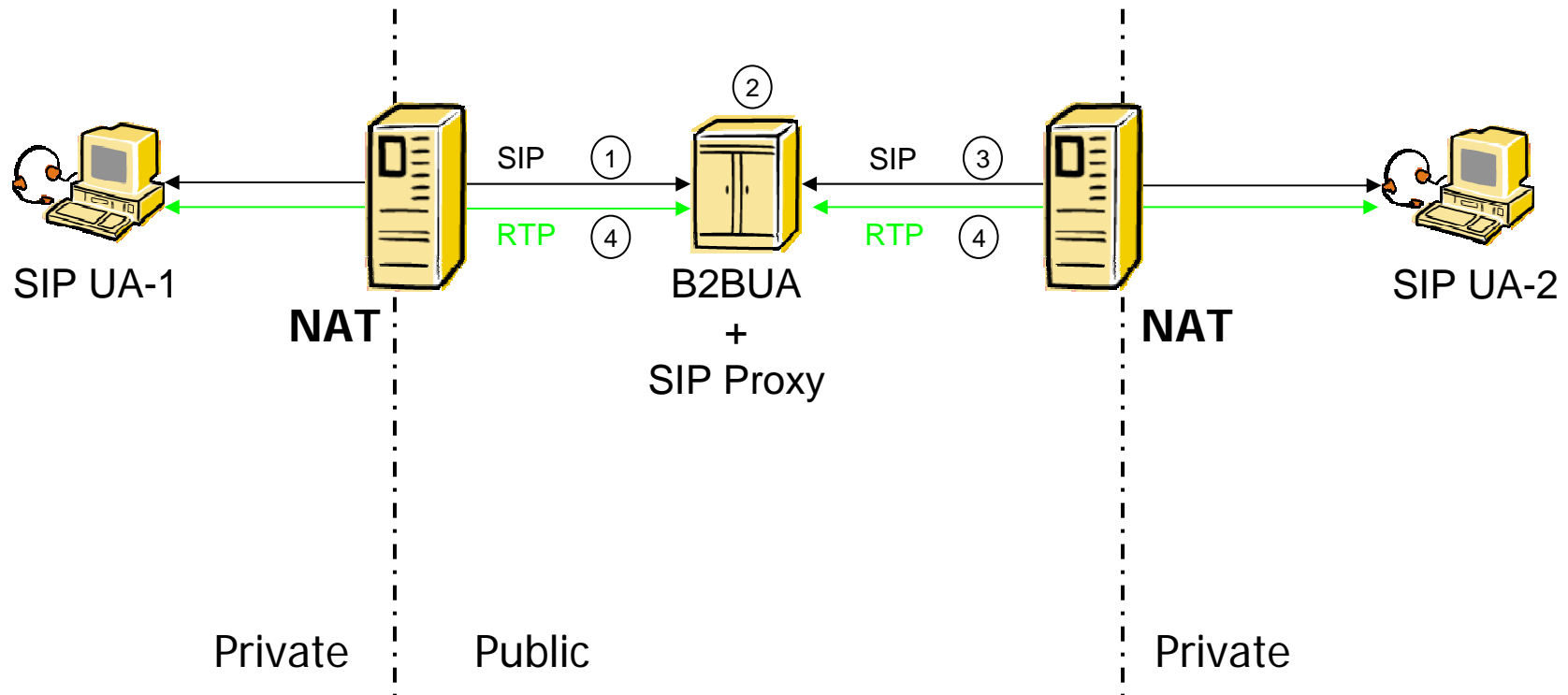
1. UA-1 discovers by STUN what kind of firewall or NAT it is behind and what public IP address (and port mapping rules) its NAT uses
2. As a backup plan it requests a public IP/Port pair from the TURN server
3. UA-1 send an INVITE containing any gained information on how it could be contacted as ordered alternatives
4. UA-2 uses these alternatives for “trial and error” until it has a successful connection (not shown here)

# Solutions to NAT Traversal: B2BUA

- Back-to-back User Agent (B2BUA)
  - it acts as a proxy for SIP signaling and media streams
    - media streams are no more end to end, signaling pass through it
  - used to assist SIP UA behind
    - NAT: if both UAs are behind NAT
    - Strong FWs: all RTP traffic is routed via public B2BUA
  - open source software available
    - Mediaproxy (available on SER, SIP Express Router as a module)
      - slow, performance issues
    - rtpproxy (available on SER, SIP Express Router as separate application, written in C)
      - fast, no released support for video so far (but already implemented by one of a project where I have worked in Switzerland, EIVD, Yverdon)
  - it breaks security
    - It performs a man-in-the-middle attack to SIP signaling (RTP is rerouted to B2BUA rewriting SIP messages)
      - integrity checks can fail on such messages



# Solutions to NAT Traversal: B2BUA



1. UA-1 sends SIP INVITE to B2BUA (default outbound proxy)
2. B2BUA modifies the SIP INVITE in order to be inserted in future messages related to this call (man-in-the-middle attack)
3. Modified SIP INVITE goes to SIP UA-2 (pinhole has been kept open by B2BUA or by SIP Proxy)  
On 200 OK, B2BUA applies the man-in-the-middle attack again
4. RTP is rerouted via B2BUA (pinholes on both sides are opened by first RTP packet)

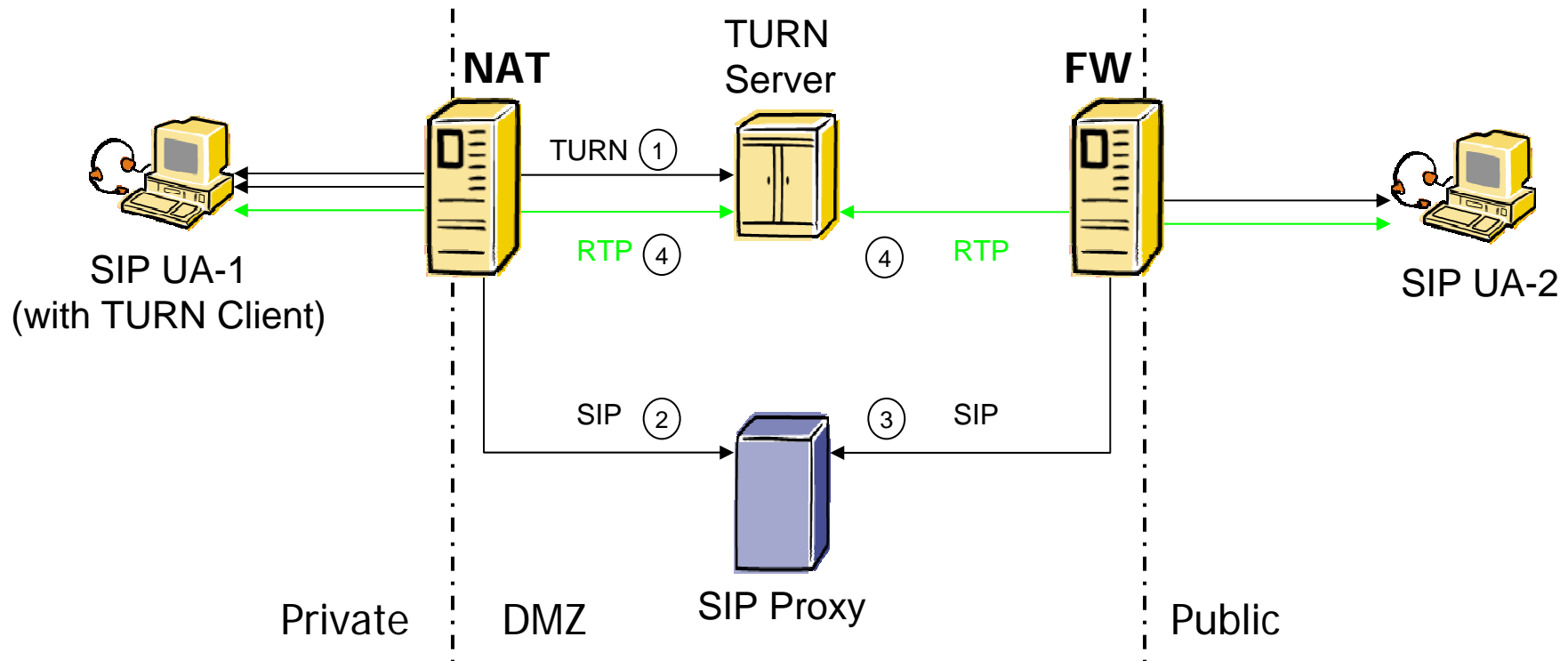
# Solutions to NAT/FW Traversal

- Additional NAT/FW Traversal solutions
  - Application Level Gateway (ALG)
    - SIP aware NAT/FW that modify SIP messages appropriately
    - more or less another way to call a B2BUA
  - IETF MIDCOM
    - splitting the middle box architecture
      - signaling functions
      - media functions
    - general framework for SIP, H.323, MGCP, RTP
  - UPnP
    - request NAT to open pinholes and return public IP/port pairs
    - used in home environments in combination with ATAs (Analog Telephone Adapter)
  - Port forwarding
    - statically configure NAT to keep certain pinholes and bindings open

# Solutions to FW Traversal

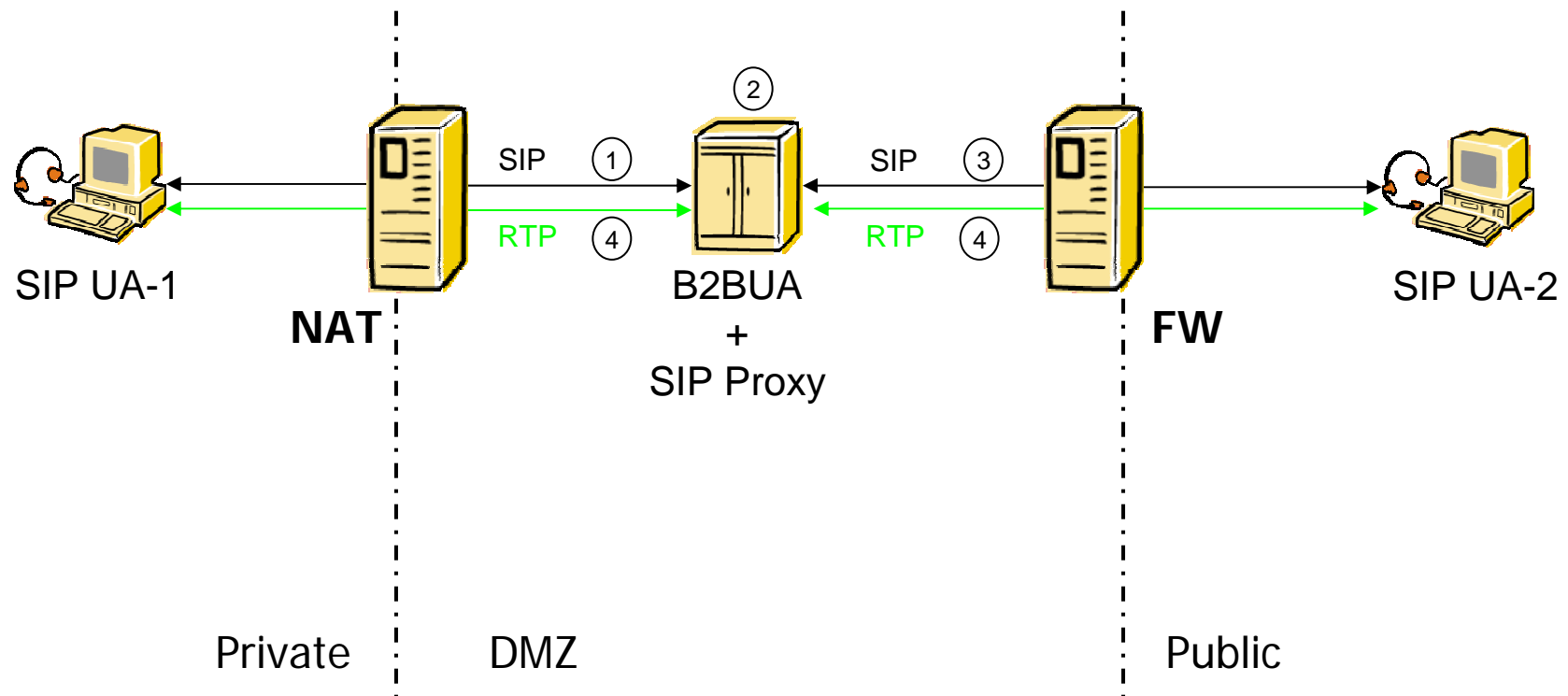
- Open pinholes (statically)
  - big security risk
  - difficult to configure since Internet Telephony protocols negotiate port on a call-by-call basis
- SIP aware FW
  - dynamically open pinholes per session
  - firewall just understands signaling and open pinholes consequently
- Stateful firewall
  - outgoing traffic open pinholes for corresponding incoming traffic
  - UA must support symmetric signaling and media
- Proxy solution
  - open pinholes just to dedicated host in a DMZ (De-Militarized Zone)
    - TURN server
    - B2BUA (already seen)

# Solutions to FW Traversal: TURN



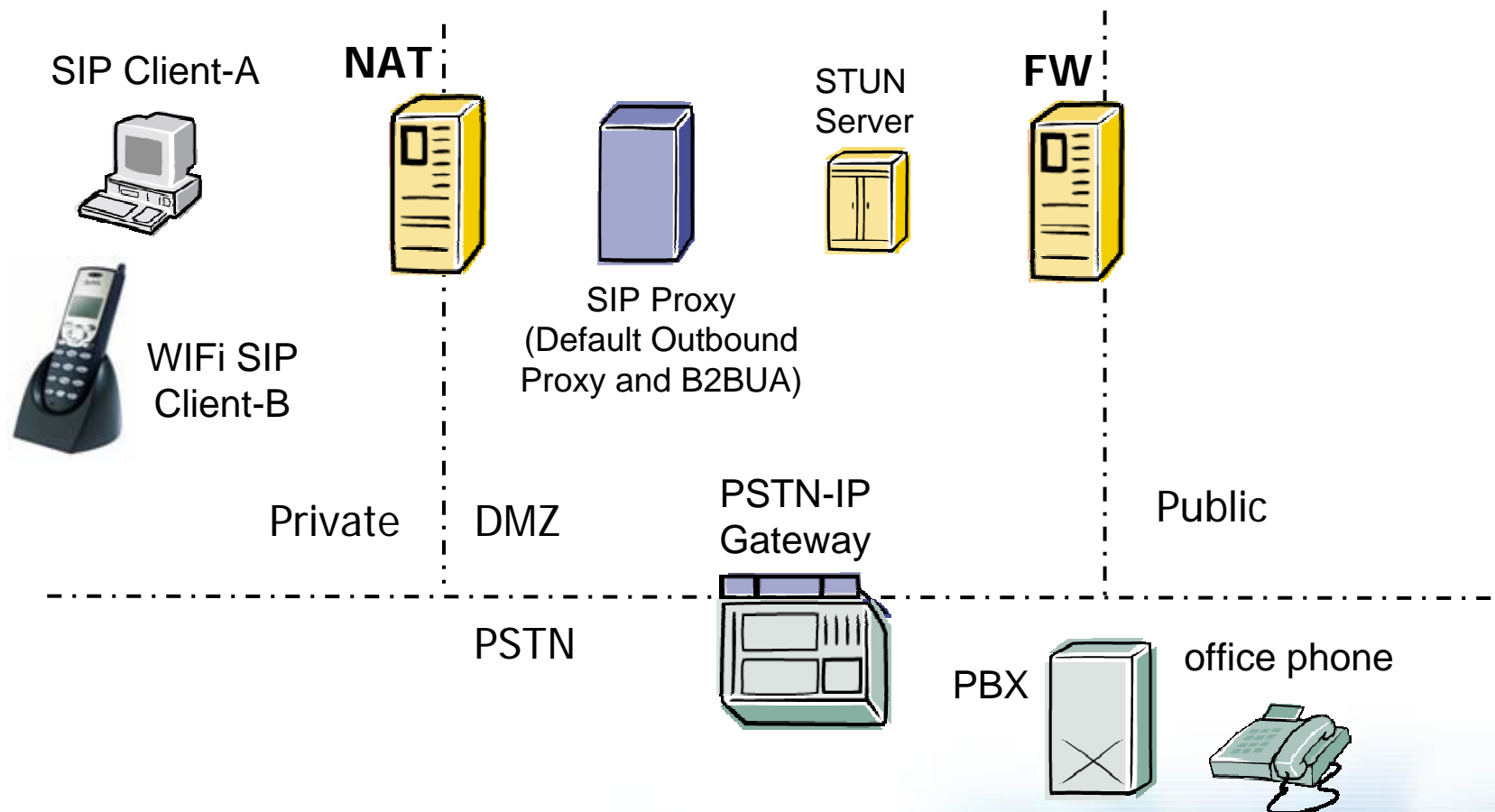
1. On request, the TURN server returns a globally reachable IP/Port pair
2. SIP goes via Default Outbound Proxy using this IP/Port pair
3. RTP is rerouted via TURN server

# Solutions to FW Traversal: B2BUA



1. UA-1 sends SIP INVITE to B2BUA (default outbound proxy)
2. B2BUA modifies the SIP INVITE in order to be inserted in future messages related to this call (man-in-the-middle attack)
3. Modified SIP INVITE goes to SIP UA-2 (pinhole has been kept open by B2BUA or by SIP Proxy)  
On 200 OK, B2BUA applies the man-in-the-middle attack again
4. RTP is rerouted via B2BUA (pinholes on both sides are opened by first RTP packet)

# SIP Deployment at NEC Europe Ltd.



- use STUN to pass the majority of NATs
- statically open pinholes just to dedicated servers in the DMZ (STUN server and SIP proxy)
- use B2BUA when clients are behind a “nasty” NAT/FW (like a symmetric NAT)
  - clients are flagged dynamically by SIP proxy (in cooperation with STUN server) on registration to understand how they should be treated (no changes in configuration of clients and server are needed)

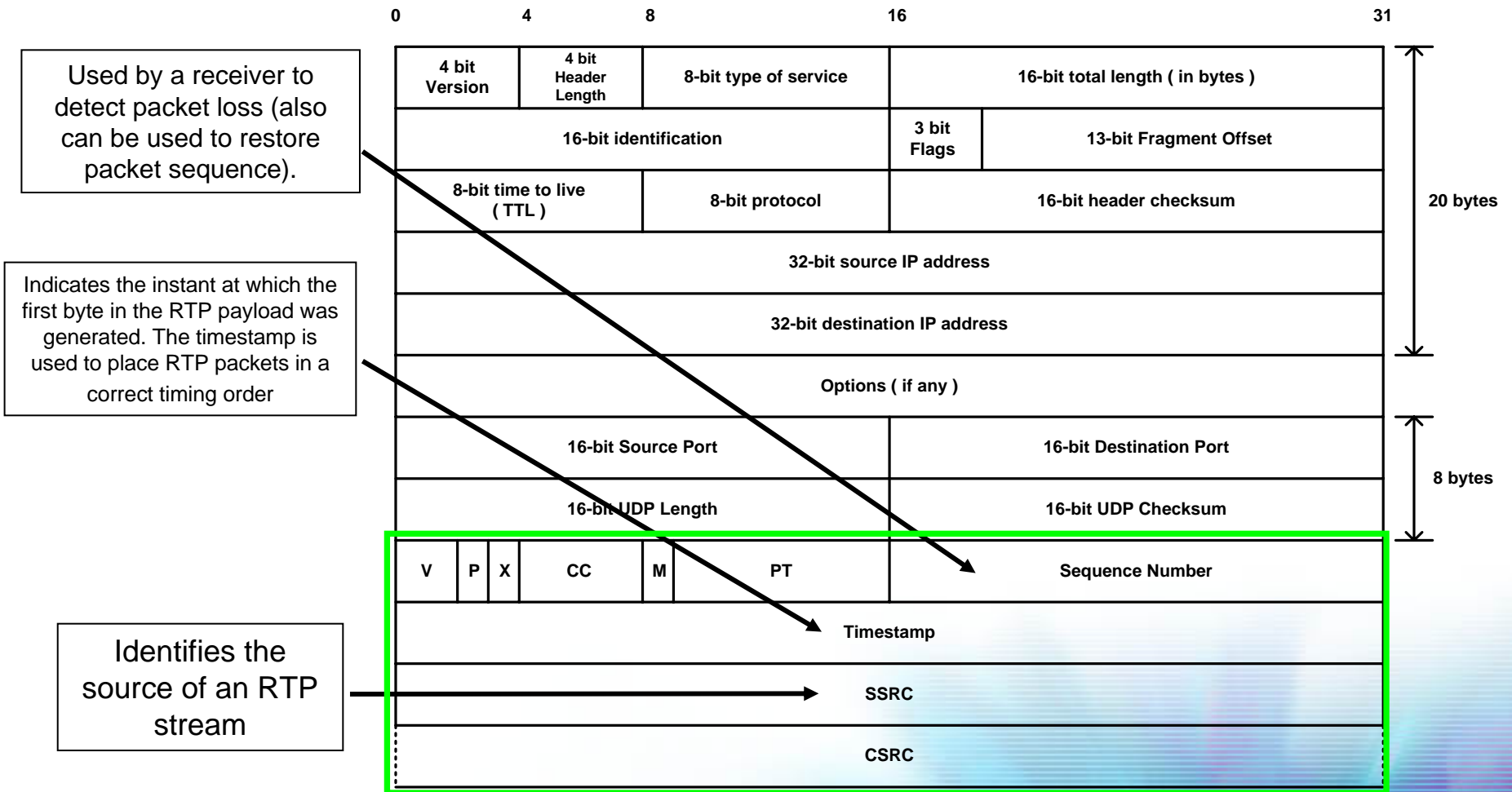
Empowered by Innovation

NEC

# Internet Telephony Security

- Biggest concern with Internet Telephony is now Security
  - “History has shown that advances and trends in information technology typically outpace the corresponding realistic security requirements. Such requirements are often tackled only after these technologies have been widely adopted and deployed” - Cable Datacom News
    - we are trying to solve the issues before Internet Telephony reaches unmanageable level
      - IDC forecasts that the total market for VoIP equipment will reach \$15.1 billion by 2007, with a compound annual growth rate of 44%
  - The first step is to secure existing TCP/IP networks
    - no 100% secure method of communication
    - this is out of the scope of this tutorial

# Media Transport: RTP



# Media Transport: RTP Security Issues

- RTP Denial of Service (DoS)
  - The way RTP handles SSRC Collisions
    - Sending command using SSRC of another participant of a session
      - Result: The ability to drop users from a certain session
    - Claiming SSRC of a user
      - Result: Transmission will stop, new selection of SSRC needs to take place and the transmission should resume
  - RTCP “BYE”, not in sync with the Signaling protocol
    - Result: The Signaling protocol is not aware that there is no exchange of voice samples any more
  - Forging Reception Reports
    - Reporting more Packet Loss
      - Result: usage of a poor quality codec with an adaptive system
    - Report more Jitter
      - Result: usage of a poor quality codec with an adaptive system

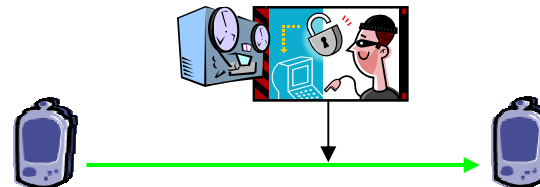
# Media Transport: RTP Security Issues

- RTP play-out



- Same SSRC, higher sequence number, higher timestamp
  - Result: The fake content will be played before the real one
    - This means that from now on we will be able to play what ever we wish to this side of the conversation since all the next transmissions of the other side will look “old” to the receiving party

- Call Eavesdropping



- Capturing RTP flows

- Since RTP identifies the codec being used (statically) or either using a “dynamic” identified codec it is easy to reconstruct the voice sampling (even in real time)
- Result: listen/record conversations
- Result: listen DTMF tones to steal passwords and PINs

# Internet Telephony Security

- Need to be in the middle to perform some attacks (it is not very difficult to get in the middle, and WLAN technology simplifies you the job)
  - DNS (modify entries to point all traffic to a hacker's machine)
  - DHCP (make all traffic go to hackers machine as default gateway, or change DNS entry to point at hacker's machine so all names resolve to hacker's IP address)
  - ARP (reply with hacker's MAC address, gratuitous ARPs or regular ARP replies)
  - Flood CAM tables in switches to destroy existing MAC addr/port associations so all traffic is broadcast out every port, and then use ARP attacks
  - Routing protocols (change routing such that traffic physically passes through a router/machine controlled by hacker)
  - Spanning tree attacks to change layer 2 forwarding topology
  - Physical insertion (e.g. PC with dual NIC cards, be it Ethernet-based or WLAN-based)

# Security solutions: Encryption

- Signaling
  - End-to-end
    - S/MIME (Secure/Multipurpose Internet Mail Extensions), IETF RFC 2633
      - provides a way to send and receive secure MIME data. Based on the MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption)
  - Hop-by-hop
    - Lower-Layer solutions (e.g. IPsec)
      - IPsec is actually a suite of protocols being developed by the IETF in the IPsec charter for authentication and encryption
    - SIPS (requires Transport Layer Security, TLS, on whole signaling path)
      - TLS version 1.0, detailed in IETF RFC 2246 but going to be updated to version 1.1, is a client/server protocol that allows peers to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery
- Media
  - Lower-Layer security (e.g. IPsec)
  - SRTP (Secure Real Time Protocol), IETF RFC 3711
    - provides confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP
    - key exchange done using MIKEY (Multimedia Internet KEYing), IETF RFC 3830
      - a key management scheme that can be used for real-time applications (both for peer-to-peer communication and group communication) supporting SRTP

# Security solutions: Encryption

- Data Encryption standard (DES)
  - if SIP is used the DES Key is sent in the clear with SDP “k” parameter...
  - actually introducing more delay and jitter, so who wants to use this anyway?
- Encryption as a Security solution
  - it is not a magic solution for everything
  - it consumes time, and introduce another delay
  - we already have been looking at the problems with NAT/FW traversal
    - adding encryption to the flows... ..

# Legal considerations on Encryption

- It may be mandatory for Internet Telephony Service Providers to provide Lawful Interception (LI)
  - U.S.A. and European laws:
    - U.S.A.: CALEA Interception of digital and other communications (<http://www.askcalea.com/calea.html>)
    - Switzerland: OFCOM draft tries to give Internet Telephony the standard telecommunication rules and restrictions (not yet released)
    - Germany, France: several activities on country and European level deciding on the regulation on Internet Telephony
  - Others:
    - In Singapore, the regulators favor a liberal approach
    - In Egypt and Thailand, only incumbent state phone companies will be allowed to provide telecom services
- The problems are coming when considering encryption (both of SIP signalling and RTP audio data)
  - End-to-end encrypted traffic can not be intercepted and decoded (then it is against the laws)

# Internet Telephony Security: Threats

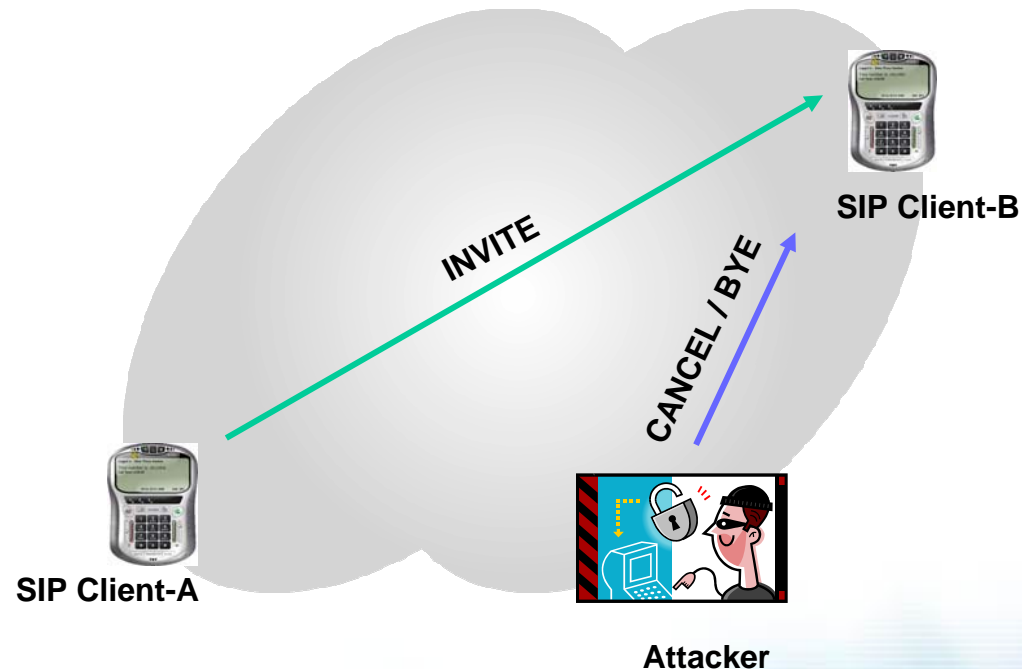
- Denial of Service (DoS) attacks
  - Novel, but simple, attacks directed at application layer
  - Effective at very low rates
  - Affecting even products classified as “Internet Telephony Security product”
  - Significant DoS vulnerabilities can result from liberal protocol parser behavior
  - Symptoms: Crashes, repeated reboot cycles, inability to process calls
- Examples (very simple)
  - To SIP Servers
    - big number of SIP messages would stop the SIP Proxy from working properly
    - buffer overflow
  - To End Clients
    - big numbers of SIP messages and/or RTP packets to open ports can stop the client from working properly
    - buffer overflow

# Internet Telephony Security: DoS attacks

- DoS against SIP (over UDP)
  - ICMP Error Message (such as Port Unreachable, Protocol Unreachable, Network Unreachable or even Host Unreachable) sent to the target where a caller is sending SIP (over UDP) messages
    - Result: it will terminate the signaling and the call in any state (UDP is asynchronous protocol)
- Using SIP CANCEL message
  - preventing UAs from making and receiving calls
  - making UAs drop the call
- Using SIP BYE message
  - making UAs drop the call

# Internet Telephony Security: DoS attacks

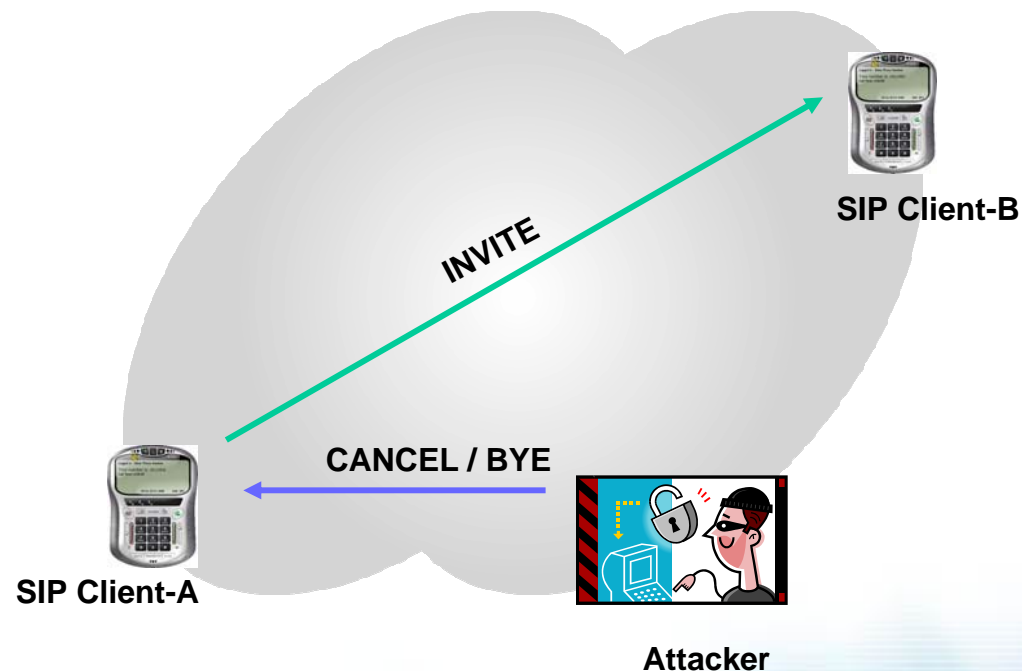
- Preventing SIP Client-A from making call



- The attacker messages cancel a pending request with the same Call-ID, TO, From, and Cseq fields

# Internet Telephony Security: DoS attacks

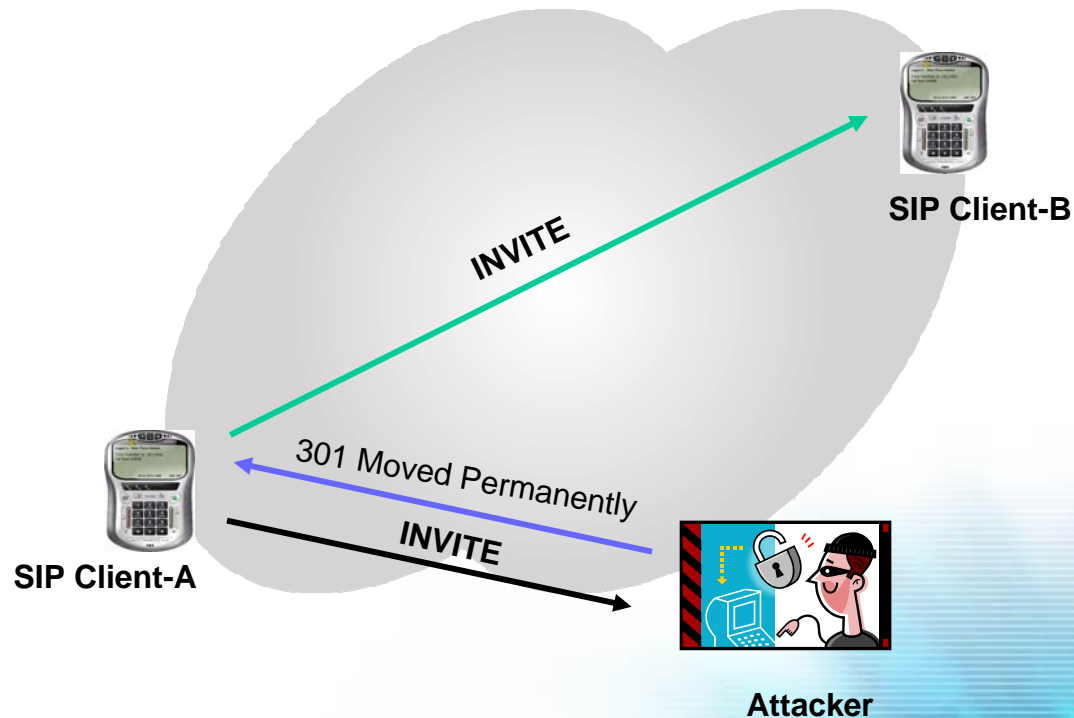
- SIP Client-A drops the call just initiated



- The attacker messages cancel a pending request with the same Call-ID, TO, From, and Cseq fields

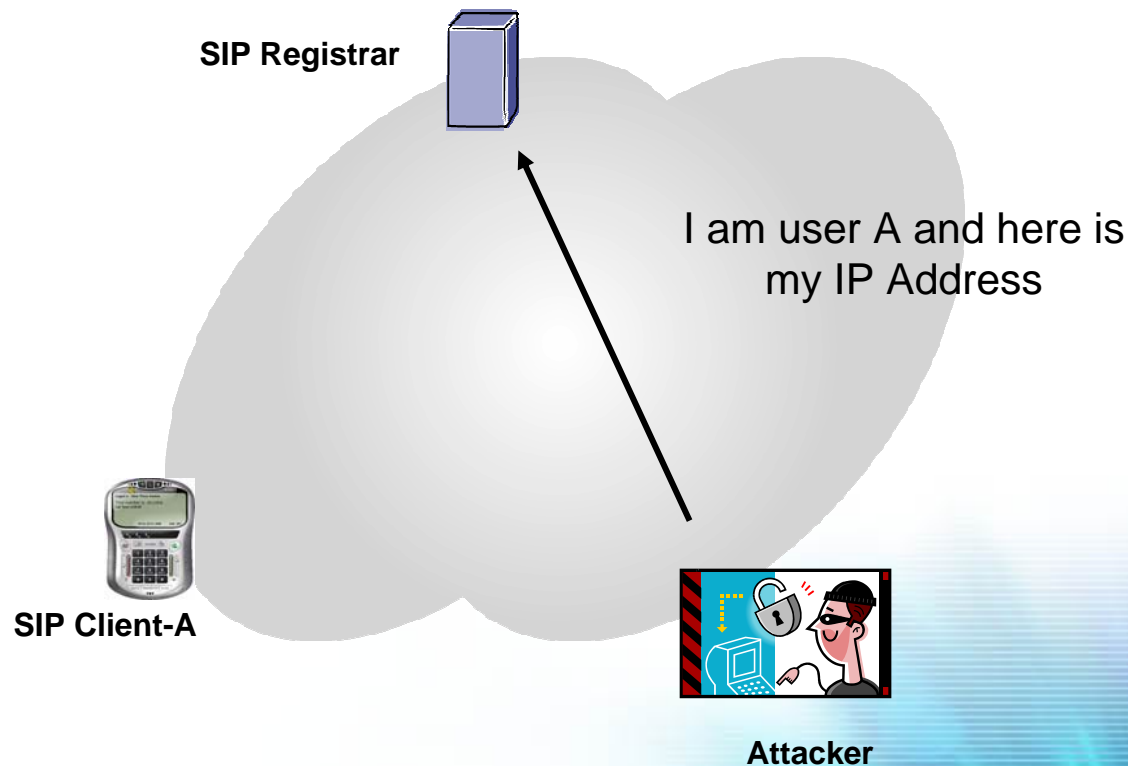
# Internet Telephony Security: Threats

- Call Hijacking
  - After INVITE message, a 301 “Moved Permanently” message would hijack the call towards whoever the attacker decides (himself or another client)



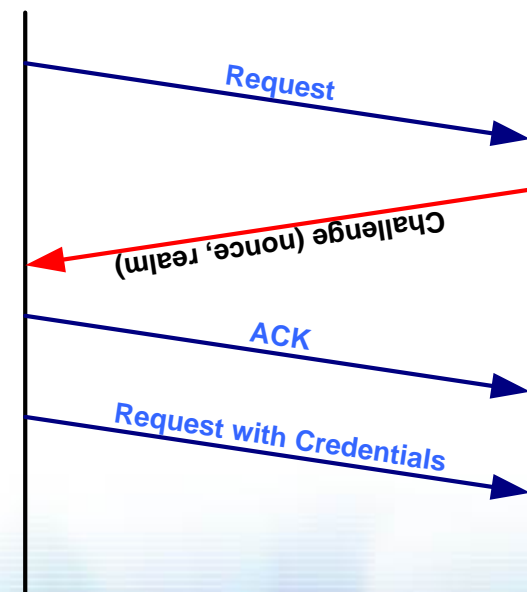
# Internet Telephony Security: Threats

- Identity Theft
  - Registering address instead of other (if requires authentication might use another type of attack)



# Security Solutions: Authentication

- Registration and call signaling/media should be authenticated
  - solving
    - Call Hijacking attack
    - Identity Theft attack
    - Man-in-the-middle attack
- Signaling (SIP)
  - End-to-end
    - Basic Authentication (deprecated)
    - Digest authentication (challenge - response)
    - S/MIME
  - Hop-by-hop
    - TLS, IPsec
    - SIPS
- Streams
  - SRTP
- All solutions require some kind of trust relationship
  - Shared secret
  - Certificate Authorities (CA)



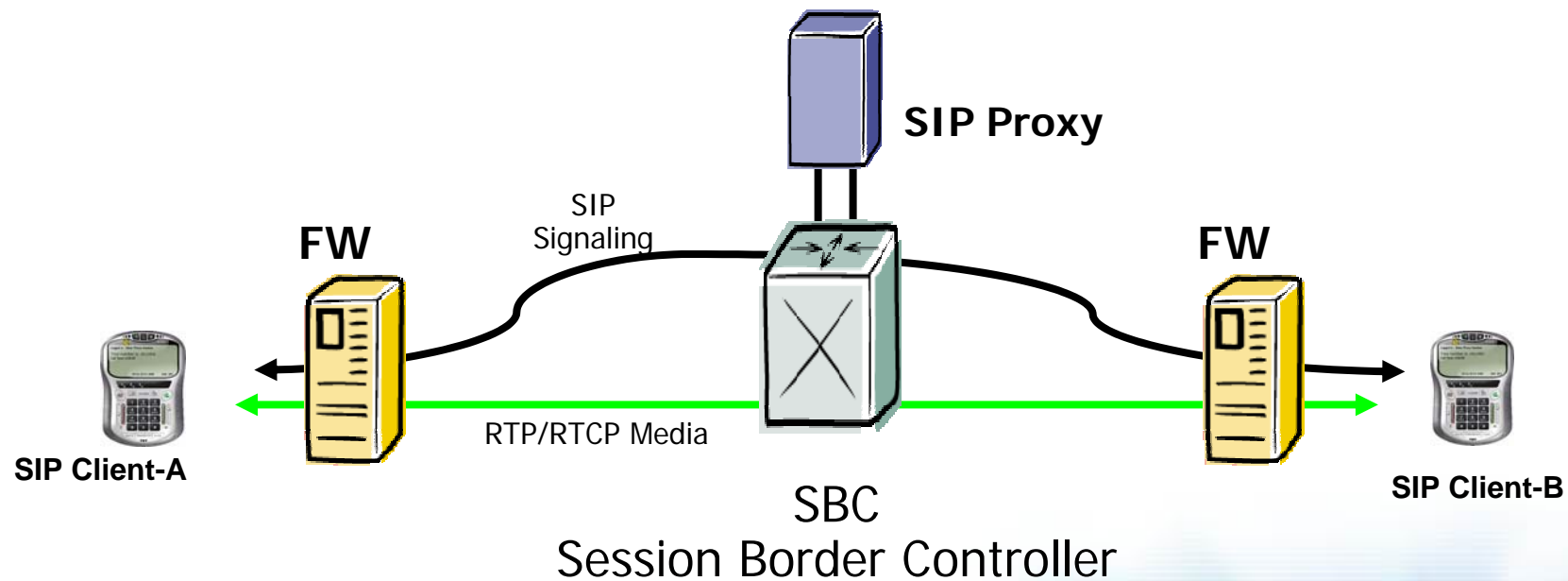
# SPAM over Internet Telephony (SPIT)

- Same thread as with email (hundreds of calls just with publicity messages, the phone is ringing all day, etc.)
- SIP allows field forging (like with email)
- Problem increase with respect to traditional telephony
  - Cheaper call rates than traditional telephony
  - Flexibility of receiving calls from anywhere from anybody in the world
- Consequences are worse than with email
  - SIP voice call interrupts user immediately
  - And SIP is not voice only, but applies to Instant Messaging, and Presence too
  - Mailboxes become full over night
    - less means to distinguish “spam” and “ham”

# SPIT: solutions

- Most E-mail filters rely on content analysis. But in voice calls, it is too late to analyze media for spamming
  - Voice Spam Detection – difficult
  - Headers for voice spam detection : “from” , “contact”. Are these enough ?
  - Detection in real time before the media arrives
- Investigated by IETF in the SIPPING working group
  - <<http://www.jdrosen.net/papers/draft-rosenberg-sipping-spam-01.txt>>
- Great variety of solution (a combination of more is foreseen)
  - Content filtering (see above)
  - Black lists
  - White lists
  - Consent-based communications (draft-ietf-sipping-consent-framework-01)
    - used to give consent to translation services in SIP servers
  - Reputation systems
  - Address obfuscation
  - Turing tests
    - Grey-listing
  - etc.

# NEC R&D in Internet Telephony Security



# NEC R&D in Internet Telephony Security

- Session Border Controller solution
  - Signaling Solution
    - SBC has ability to communicate to SIP client over NAT'ed address
    - SBC sets client re-register interval and handles SIP traffic
  - Media Traversal Solution
    - SBC allocation of IP address & port in public network
      - implementation of STUN, TURN servers
    - SBC handling of RTCP channel mapping
  - Security solution
    - local implementation of security
    - topology hiding
    - parsing checking
    - breaking the end-to-end security in two or more path
      - allowing Lawful Interception
    - it is not a magic solution for everything
      - single point of failure... :-)

# Special thanks

- SWITCH, The Swiss Education and Research Network (<http://www.switch.ch>)
  - provided ideas about this tutorial (and material)

Empowered by Innovation

**NEC**