IP Telephony: protocols, architectures and applications

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

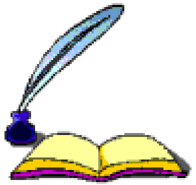
Empowered by Innovation NEC

Outline

- Introduction (what is IP Telephony)
- Protocols and architectures
- Integrating PSTN and IP Telephony using ENUM
- Applications and world-wide deployments
- Hot topics and open issues in research and development

What is IP Telephony?

- IP Telephony and VoIP (Voice over IP) are not the same!
- Although similar issues are faced by these technologies, they have some fundamental differences
- Definitions:



  - VoIP and Internet Telephony both refers to communications services carried over IP (Internet Protocol) rather than over the Public Switched Telephone Network (PSTN)
  - VoIP: turn the analog speech into a digital representation and then transport the signal in IP packets to the recipient
  - IP Telephony: telephony on top of IP (services, interoperability, scalability, availability, etc.)

© NEC Corporation 2005

Where is the difference?

- VoIP and IP Telephony are designed for different network sizes

- VoIP focuses on LANs (local address space) and has neither the intention of replacing the PSTN nor to be fully integrated with it

- IP Telephony is designed to scale over the whole Internet. It should offer an alternative to the PSTN, replicating the PSTN services and adding new ones

© NEC Corporation 2005

Towards IP Telephony

- Standardized protocols supporting interoperability among different devices/vendors
- Transparent integration with PSTN: seamless access to the PSTN (transition period with mixed IP Telephony – PSTN)
- Scalability: serving millions of users is mandatory (the classic TSPs, Telephony Service Providers, have millions of users)
- Availability: need to replicate the PSTN availability (>99.9%)

Empowered by Innovation NEC

© NEC Corporation 2005

What is not covered by IP Telephony

- Let’s destroy some myth:
  - Quality of Service (QoS) is definitely out of the scope of the core IP Telephony standards!

- If someone says: “the major concern for not adopting IP Telephony is the lack of QoS”
  - Please reply: “talk to the network guys for this!”
  - Voice codecs result in having a quality comparable to the PSTN one on a dedicated network
  - Network parameters like bandwidth, delay, jitter and loss make the difference among codecs and against PSTN (connection oriented paradigm)

- This tutorial is not going to address QoS for IP Telephony

© NEC Corporation 2005

Protocols

Standardized

H.323

SiP

H.248

Proprietary

skype™

YAHOO! MESSENGER

Asterisk™
(IAX, open source)

AOL. Instant Messenger™

CISCO SYSTEMS
(Skinny)

… and many many more…

Why going for standard protocols?

- Proprietary protocols
  - have restricted innovation (smaller users/developers community, narrowed vision, solving smaller issues)
  - restrict the set of available functionalities because of interoperability (developing gateways to every protocol take too long)

- Today’s Internet
  - offers diverse functionalities because of standardized communication protocols

© NEC Corporation 2005

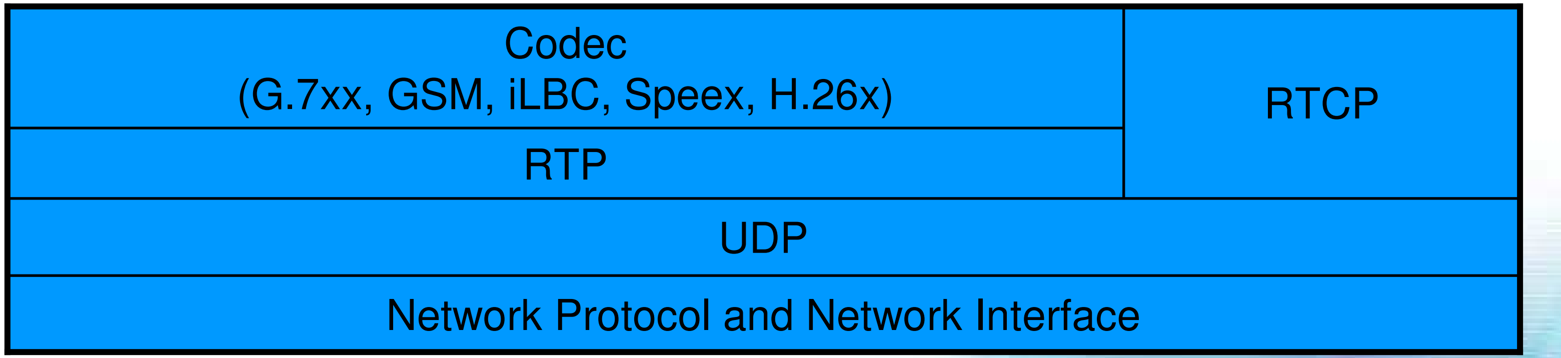
Standardized protocols

	Audio/Video transport	Signaling
ITU-T	RTP/RTCP	H.323 H.248
IETF	RTP/RTCP	SIP MGCP MEGACO

© NEC Corporation 2005

Standard protocols: media transport

- Protocols designed to deliver real time data to the remote entities:
  - RTP (Real Time Protocol: IETF RFC 3550, July 2003)
    - provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video
  - RTCP (Real Time Control Protocol: IETF RFC 3550, July 2003)
    - control protocol to allow monitoring of the data delivery, and to provide minimal control and identification functionalities
- RTP/RTCP are always sent on top of UDP (User Datagram Protocol) on IP-based networks



Codec
(G.7xx, GSM, iLBC, Speex, H.26x)

RTP

RTCP

UDP

Network Protocol and Network Interface

© NEC Corporation 2005

Standard protocols: call signaling

- Before audio or video media can flow using RTP/RTCP between two entities
  - need of finding the remote device and to negotiate the means by which media will flow between the two devices

- The protocols that are central to this process are referred to as call signaling protocols, the two standardized are
  - H.323 (ITU-T Study Group 16, version 5, 2003)
  - SIP (Session Initiation Protocol, original IETF RFC 2543, updated by IETF RFC 3261, June 2002)

© NEC Corporation 2005

Standard protocols: call signaling

- A little bit of story:
  - H.323 and SIP both have their origins in 1995
  - H.323 enjoyed the first commercial success due to the fact that ITU quickly published the first standard in early 1996
  - SIP progressed much more slowly in the IETF with the first recognized "standard" published later in 1999
  - SIP was revised over the years and re-published in 2002 as RFC 3261, which is the currently recognized standard for SIP
  - These delays in the standards process resulted in delays in market adoption of the SIP protocol
  - Today H.323 is still having the bigger commercial market share but the trend is toward SIP
    - SIP was chosen as the official protocol by the 3GPP partnership alliance for the UMTS IMS (IP Multimedia subsystem) (SIP is the official protocol for IP-based call signaling in UMTS
      - first application: Push To Talk (PTT)

Standard protocols: additional signaling

- MGCP (Media Gateway Control Protocol: IETF RFC 3661, was RFC 3435, was RFC 2705)
  – control protocol for controlling Media Gateways (MG) from external call control elements called Media Gateway Controllers (MGC)

- MEGACO (MEdia GAteway COntrol protocol)
  – This version of the protocol is the next generation of MGCP
  – Joint effort of the IETF MEGACO working group and the ITU Study Group 16
    - IETF refer to the protocol as "MEGACO" (RFC 3525, was RFC 3015, was RFC 2885)
    - ITU refers to it as H.248
  – Currently is under discussion the MEGACO/H.248 version 2

- Summarizing: they are not IP Telephony protocols of their own!
  – they are addressing complementary topics related to media control on gateways (only legacy voice features)
  – need to use them to achieve IP Telephony

© NEC Corporation 2005

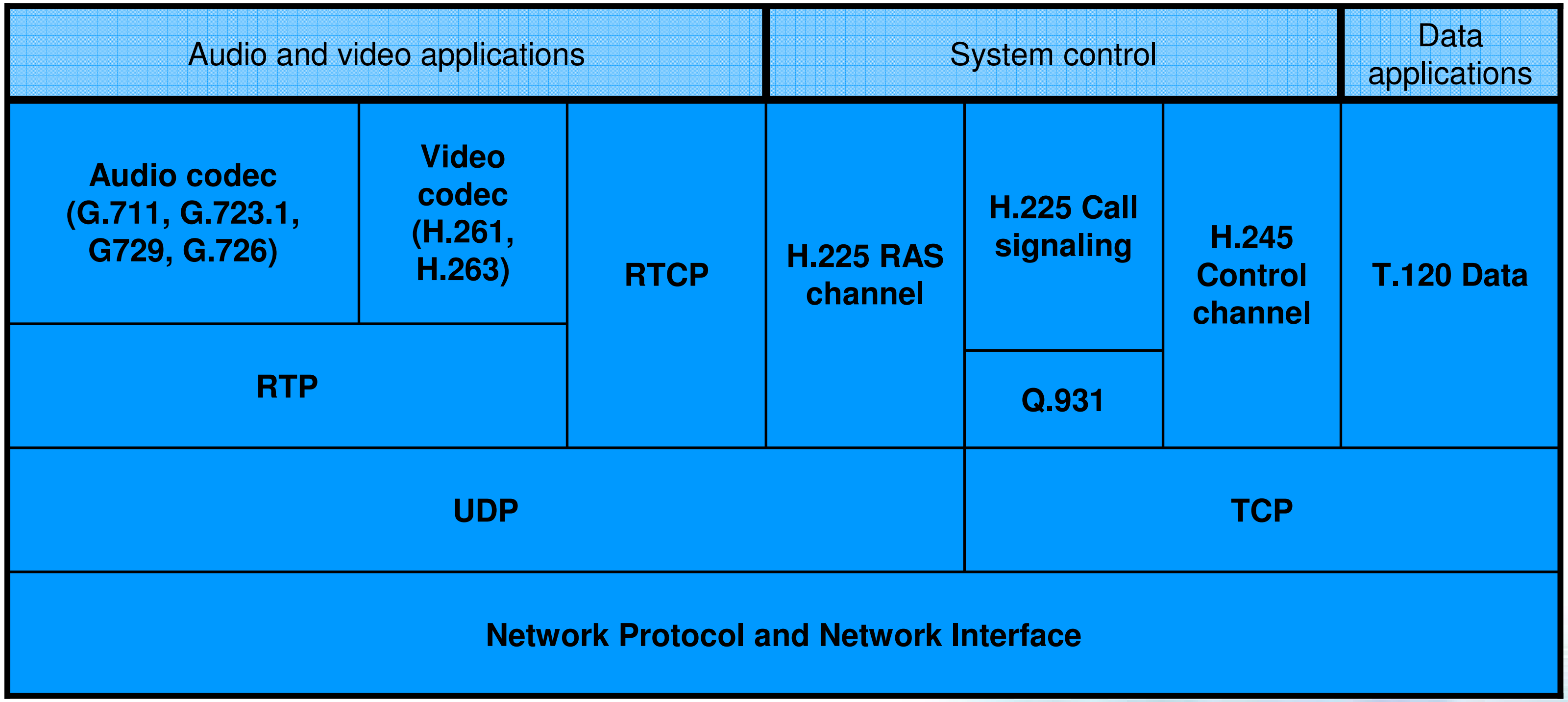
Standard protocols: H.323

What is H.323?

- H.323: “Packet-based multimedia communications systems” recommendation from ITU-T
  - vertically integrated protocol suite (“umbrella specification”)
  - it is composed of a series of protocol recommendations from ITU-T
    - H.225.0 – RAS, Q.931
    - H.245
    - RTP/RTCP
    - Audio/video codec
  - it is based on H.320 (ISDN Videoconferencing)
    - multistage signaling
    - good interoperability with PSTN

© NEC Corporation 2005

H.323: protocol stack



Audio and video applications

System control

Data applications

Audio codec (G.711, G.723.1, G729, G.726)

Video codec (H.261, H.263)

RTCP

H.225 RAS channel

H.225 Call signaling

H.245 Control channel

T.120 Data

RTP

Q.931

UDP

TCP

Network Protocol and Network Interface

© NEC Corporation 2005

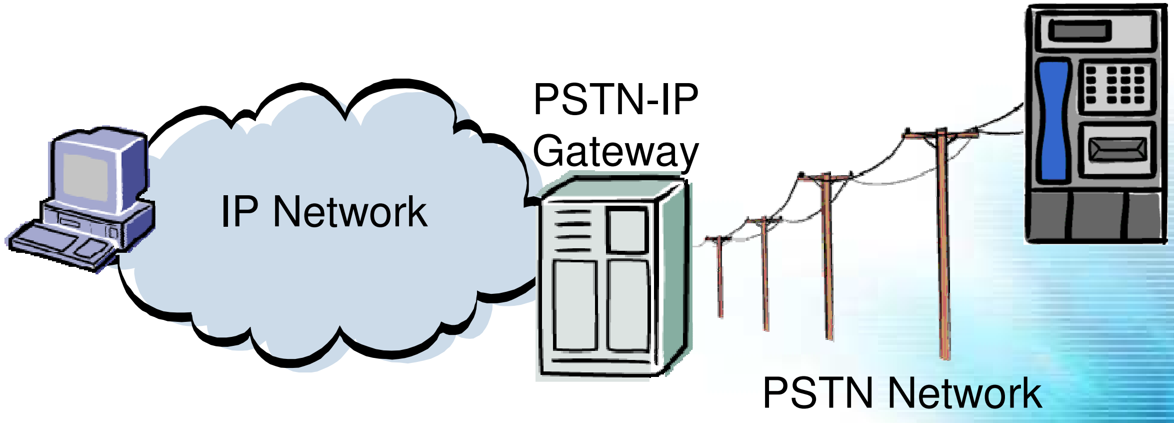
H.323: architectural elements

- Terminals (end-points)
  - hardware clients
  - software clients
  - they need to have
    - audio codec (at least G.711)
    - H.323 call signaling protocol suite
  - optional
    - video codec
    - data transmission

© NEC Corporation 2005

H.323: architectural elements

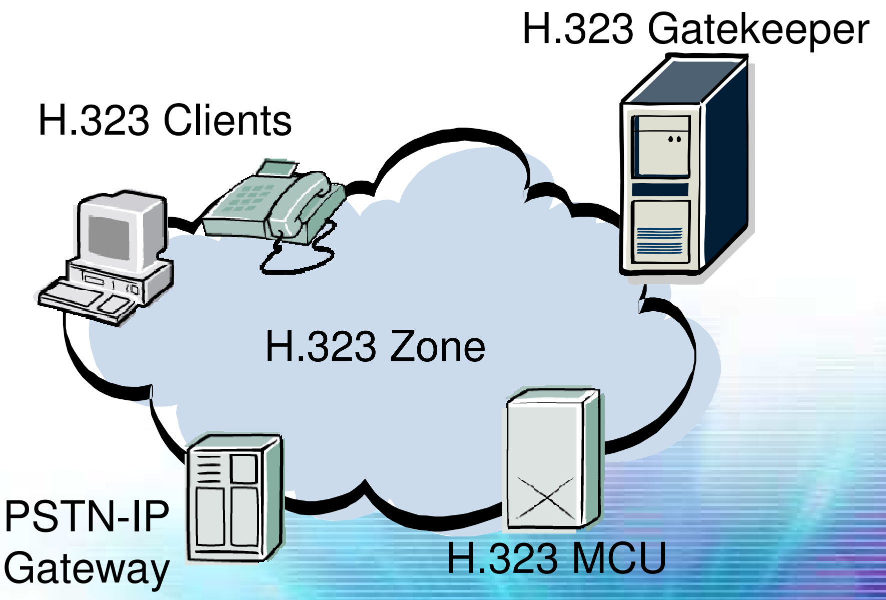
- Gateway
  - generic: an interface between two worlds
  - specific: interface between packet-based networks and circuit switched networks
  - translating the formats
    - information format (Media Gateway)
    - signaling format (Signaling Gateway)



© NEC Corporation 2005

H.323: architectural elements

- Gatekeeper
  - Optional entity (in the Recommendation, but it is worth using it)
  - Functionalities
    - Managing a zone (managing the H.323 entities in its domain)
      - Endpoint registration
    - Address translation (H323ID and E164ID to IP address and port)
      - Endpoint location
    - Call routing
      - Next hop location
    - Admission control
    - Bandwidth management
    - Authorization control
    - etc. etc. etc.

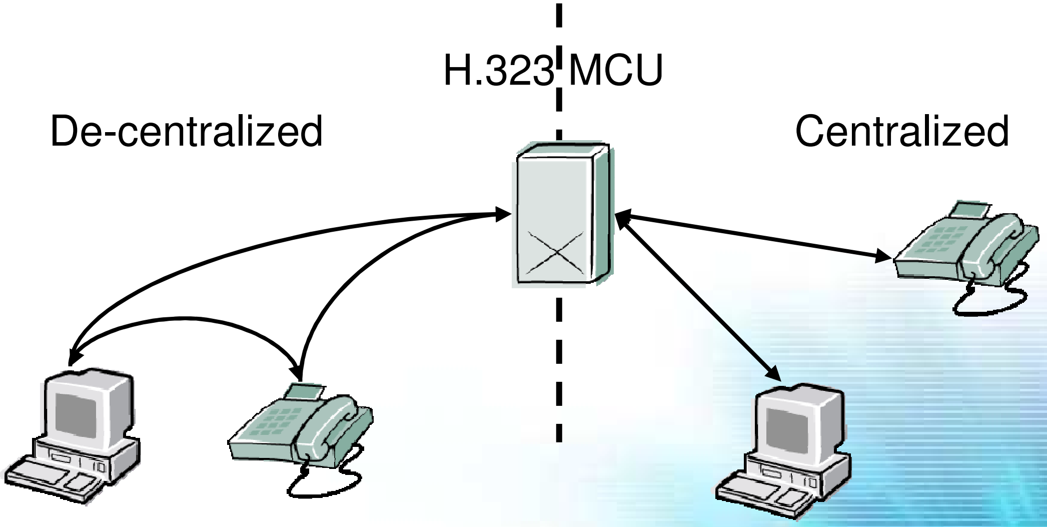


Empowered by Innovation NEC

© NEC Corporation 2005

H.323: architectural elements

- Multipoint Control Unit
  - Multipoint conferencing server
    - Centralized: manage the signaling and mixes the audio/video from terminals in one single flow
    - De-centralized: manage the signaling and let the terminals exchange audio/video using multicast
    - Mixed: some terminals are handled in centralized mode and others in de-centralized mode



Empowered by Innovation NEC

© NEC Corporation 2005

H.323: addresses

- Alias Address
  - Alias are easier to remember with respect to Network address and/or Transport Address in order to identify a terminal
  - Each alias has an unique Transport Address (IP address + Port)
  - One Transport address may correspond to multiple aliases
  - Aliases must be unique inside a zone

- Example
  - saverio.niccolini
  - myh323alias
  - whateveryoucanimagine

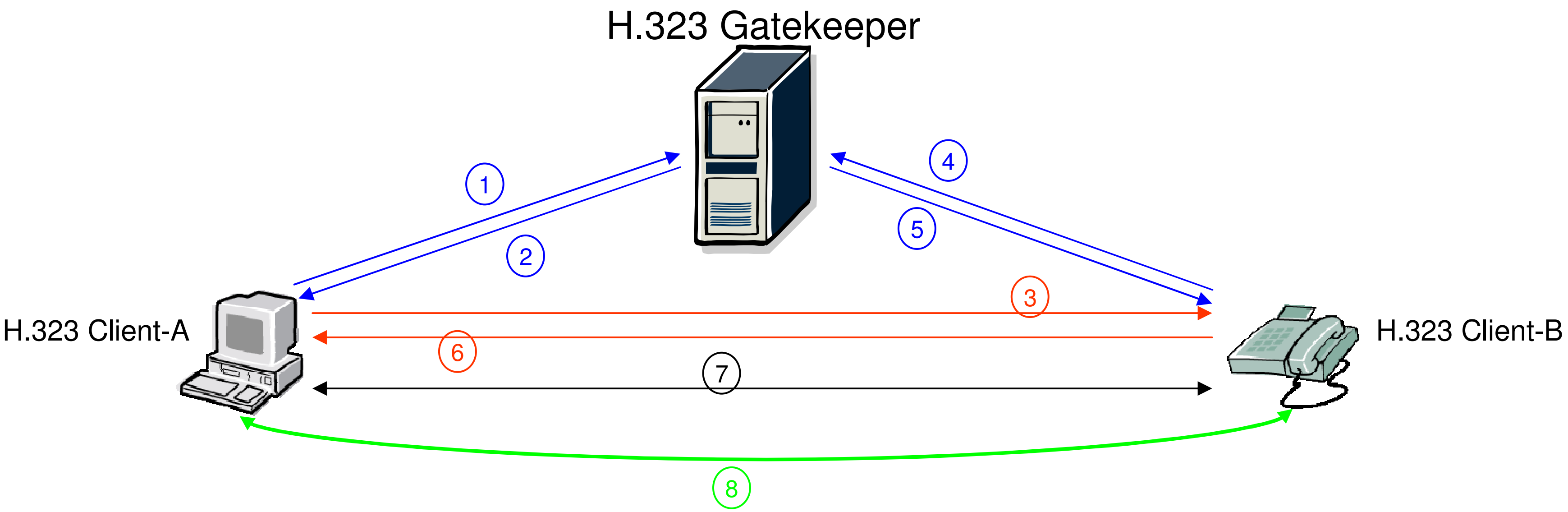
- As you can see there is no notion of global reachable address

- Either specific routes has to be set or neighboring/peering has to be properly configured

© NEC Corporation 2005

H.323: example of communication

1. Client-A sends ARQ (Admission ReQuest) to Gatekeeper: it asks to be connected to Client-B alias
2. Gatekeeper confirms or rejects the call (ACF, Admission ConFirm / ARJ, Admission ReJect): it returns the Client-B call signaling address (IP address and port of the call signaling address)
3. Client-A sends a SETUP to Client-B call signaling Address



4. Client-A sends ARQ (Admission ReQuest) to Gatekeeper: it asks to be connected to Client-A (he knows already Alias and call signaling address)
5. Gatekeeper confirms or rejects the call (ACF, Admission ConFirm / ARJ, Admission ReJect): it returns the Client-A call signaling address (IP address and port) if it was asked
6. Client-B sends a CONNECT to Client-A call signaling address
7. Capabilities about the call are exchanged among the terminals (on H.245 channel address different from call signaling channel address)
8. The media is sent end-to-end; i.e. to the IP addresses and ports negotiated during the signaling

Messages 3, 6, 7 may be exchanged with the H.323 Gatekeeper depending on the call model adopted
(Direct signaling, Gatekeeper-routed call signaling, Gatekeeper-routed H.245 control)

© NEC Corporation 2005

Standard protocols: SIP

Empowered by Innovation NEC

What is SIP?

- SIP (Session Initiation Protocol) is a protocol to initiate sessions
- It is an application layer protocol used to
  - establish
  - modify
  - terminate

  multimedia sessions (conferences)

  (Internet Telephony calls are basically multimedia session)

- It supports name mapping and redirection services transparently
  - personal mobility: one single externally visible identifier regardless of the network location

- Basic scope of SIP is to exchange
  - IP addresses
  - port numbers

  to which systems can receive data

- SIP is easily extensible

© NEC Corporation 2005

What SIP is not…

- SIP is NOT:
  - Transport protocol (like TCP, UDP)
  - QoS reservation protocol (like RSVP)
  - Gateway Control Protocol (like MEGACO)
  - Used to send session capabilities (instead it makes use of SDP, Session Description Protocol)
  - Designed for bulk transfer (like FTP)
  - Limited to Internet Telephony
    - it can be used by any application having a notion of session (e.g. Peer-to-peer applications, e.g. http://www.research.earthlink.net/p2p/)

© NEC Corporation 2005

How to address SIP entities

- SIP uses email-style addressing

- Each user has a globally reachable address (called SIP URI, Uniform Resource Indicator)
  - Users bind to this address using SIP REGISTER method (inform the server about the current location / host used)
  - This address is used to establish a session

- Examples for SIP URIs
  - sip:saverio.niccolini@sip-proxy.netlab.nec.de
  - sips:security@my-secure-proxy-server.org:5061

© NEC Corporation 2005

SIP methods

- SIP makes uses of different types of messages (methods) to communicate among parties
  - **INVITE**
    - initiate sessions (session description included in the message body encoded using SDP)
  - **ACK**
    - confirms session establishment
  - **BYE**
    - terminates sessions
  - **CANCEL**
    - cancels a pending INVITE
  - **REGISTER**
    - binds a permanent address to a current location
  - **OPTIONS**
    - capability inquiry
  - Other extensions have been standardized
    - e.g. INFO, UPDATE, MESSAGE, PRACK, REFER, etc.

© NEC Corporation 2005

SIP: architectural elements

- RFC 3261 defines some basic architectural elements:
  - User Agent Client (UAC)
    - a logical entity that creates a new request, and then uses the client transaction state machinery to send it
  - User Agent Server (UAS)
    - a logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request
  - Proxy Servers
    - a logical entity that routes SIP requests to UASs and SIP responses to UACs
      - Proxy Servers may reply directly to the UACs, when responding directly to a request, the element is playing the role of a UAS
    - they can operate (for each request)
      - in stateless mode (simply forwards requests and forgets about them afterwards)
      - in stateful mode (remembers information about requests, transaction state, it affects the processing of future messages associated with that request)

© NEC Corporation 2005

SIP: architectural elements

- Other elements are composed out of them (RFC 3261):
  - User Agent (UA)
    - A logical entity that can act as both a user agent client and user agent server (UA = UAC + UAS)
    - Software clients
      - X-Lite / X-pro / Eyebeam
      - Siemens SCS
      - Linphone, kphone
      - Etc.
    - Hardware clients
      - CISCO 7960, 7920, …
      - Snom 190, …
      - Zyxel Wi-Fi phone
      - Etc.

© NEC Corporation 2005

SIP: architectural elements

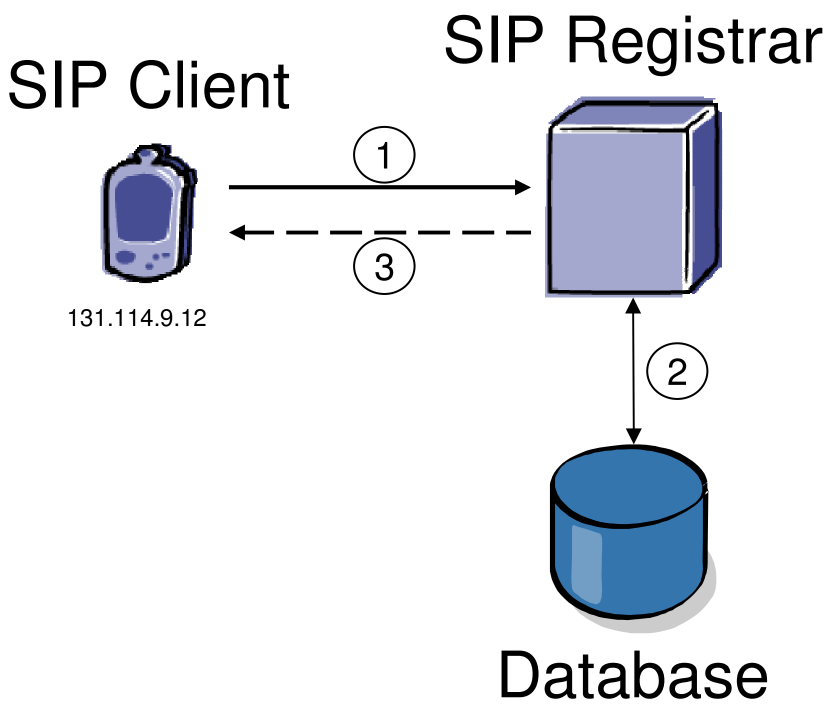
- Other elements are behaving like a combination of them (RFC 3261):
  - Back-to-Back User Agent (B2BUA):
    - A B2BUA is a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior
- Other elements are derived from them and assume other names (RFC 3261):
  - Registrar server
    - a special type of UAS where that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles

© NEC Corporation 2005

SIP: other architectural elements

- Other elements are derived from them and assume other names (but not defined as standard elements in RFC 3261):
  - Redirect Servers
    - a special type of UAS that redirects requests based on a location service (used to improve scalability)
  - Outbound proxy
    - a special type of proxy that receives requests from a client and relays call signaling (typically manually configured on UA and used to give assistance with firewalls and/or certain types of NATs)

SIP: registration example



1. SIP Client sends a SIP REGISTER message to the SIP proxy server, which acts as a SIP Registrar saying:
   - "I have this public SIP address and I am currently at this host"

```
REGISTER sip:registrar.atlanta.com SIP/2.0
To: sip:alice@atlanta.com
Contact: sip:alice@131.114.9.12:5060; expires=1800
[…]
```

2. The SIP Registrar save the user's current location in its database

3. The SIP Registrar informs SIP Client about the success of the registration (and any other currently active registration)

```
SIP/2.0 200 OK
To: sip:alice@atlanta.com
Contact: sip:alice@131.114.9.12:5060; expires=1800
Contact: sip:alice@131.114.53.1:5060; expires=1342
[…]
```

This message exchange was simplified, other messages may be exchanged (authorization messages, etc.)

© NEC Corporation 2005

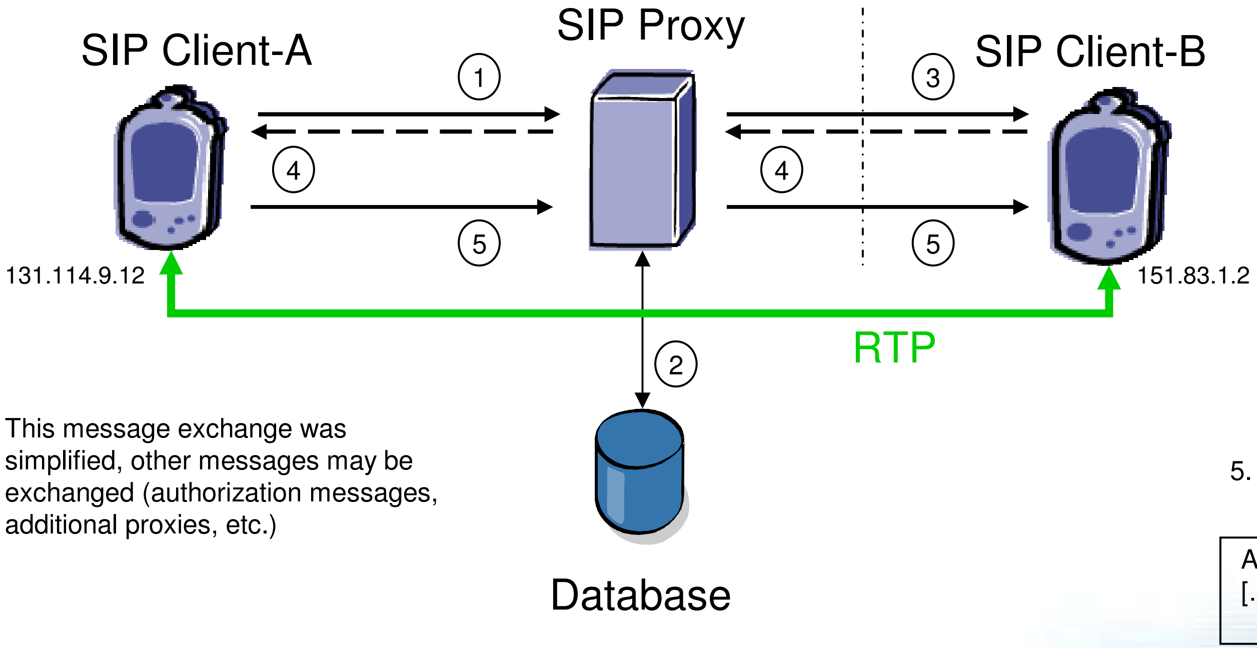
Empowered by Innovation NEC

SIP: session establishment example

1. Client-A (alice) sends SIP INVITE to the SIP proxy server

```
INVITE sip:bob@chicago.com SIP/2.0
To: sip:bob@chicago.com
From: sip:alice@atlanta.com
Contact: sip:alice@131.114.9.12:5060
[…]
```

2. SIP proxy server looks up user-B’s current location(s) in its database (if it is not in its database it resolves it using DNS entries and forwards the INVITE to the next proxy)



6. The media is sent end-to-end; i.e. to the IP addresses and ports negotiated during the signaling (SDP in INVITE/200 OK or in any other message)

This message exchange was simplified, other messages may be exchanged (authorization messages, additional proxies, etc.)

5. Client-A acknowledges the 200 OK by sending an ACK to client-B

```
ACK sip:bob@151.83.1.2:5060 SIP/2.0
[…]
```

3. SIP Proxy forwards the INVITE to user-B’s current location(s)

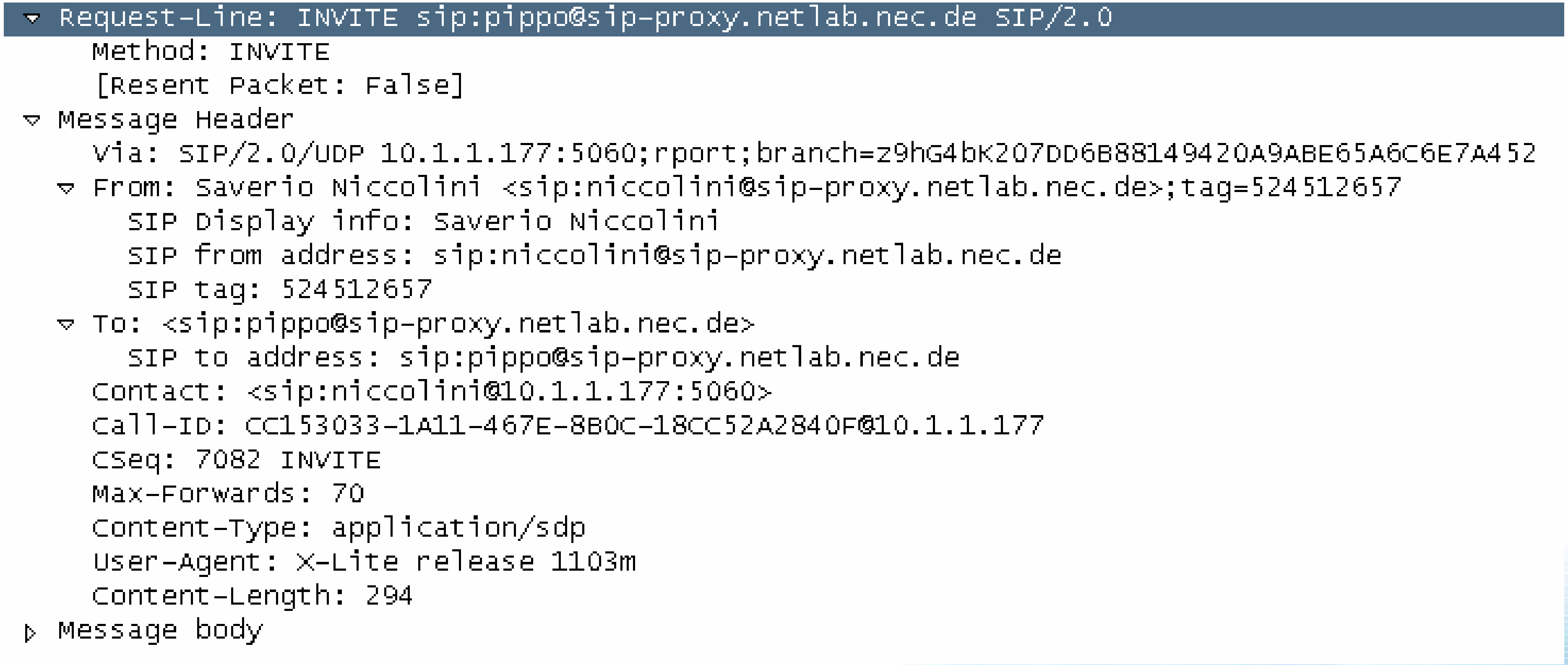
```
INVITE sip:bob@151.83.1.2:5060 SIP/2.0
To: sip:bob@chicago.com
From: sip:alice@atlanta.com
Contact: sip:alice@131.114.9.12:5060
[…]
```

4. After user-B answers his phone. it sends 200 OK message to client-A

```
SIP/2.0 200 OK
To: sip:alice@atlanta.com
From: sip:bob@chicago.com
Contact: sip:bob@151.83.1.2:5060
[…]
```

© NEC Corporation 2005

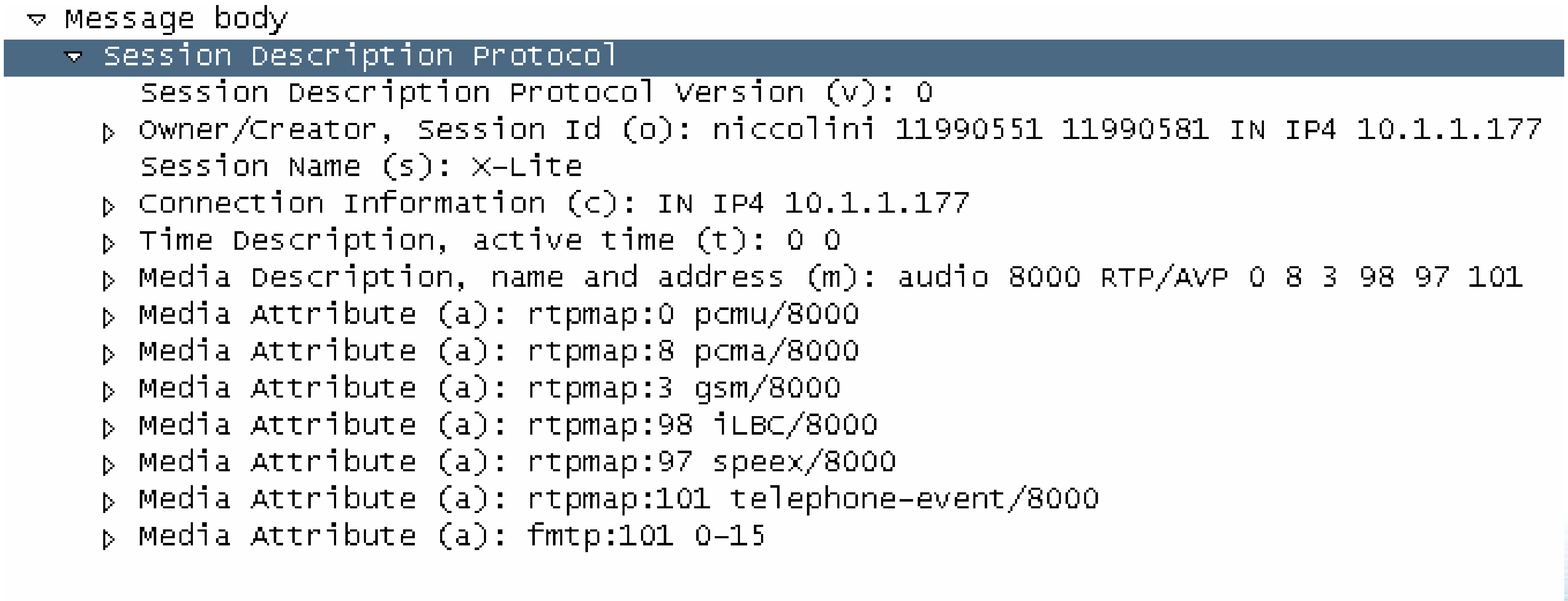
SIP: message example



```
▿ Request-Line: INVITE sip:pippo@sip-proxy.netlab.nec.de SIP/2.0
    Method: INVITE
    [Resent Packet: False]
▿ Message Header
    Via: SIP/2.0/UDP 10.1.1.177:5060;rport;branch=z9hG4bK207DD6B88149420A9ABE65A6C6E7A452
  ▿ From: Saverio Niccolini <sip:niccolini@sip-proxy.netlab.nec.de>;tag=524512657
      SIP Display info: Saverio Niccolini
      SIP from address: sip:niccolini@sip-proxy.netlab.nec.de
      SIP tag: 524512657
  ▿ To: <sip:pippo@sip-proxy.netlab.nec.de>
      SIP to address: sip:pippo@sip-proxy.netlab.nec.de
    Contact: <sip:niccolini@10.1.1.177:5060>
    Call-ID: CC153033-1A11-467E-8B0C-18CC52A2840F@10.1.1.177
    CSeq: 7082 INVITE
    Max-Forwards: 70
    Content-Type: application/sdp
    User-Agent: X-Lite release 1103m
    Content-Length: 294
▹ Message body
```

© NEC Corporation 2005

SIP: message example



```
▽ 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
```

© NEC Corporation 2005

Comparing H.323 and SIP

Empowered by Innovation NEC

Comparing H.323 and SIP

- From the beginning
  - H.323 was porting the legacy world to the Internet
    - ASN message format (binary format)
    - Local alias identifiers (h323:saverio.niccolini)
    - Domain organization leading to peering/hierarchies
  - SIP was designed for the Internet
    - HTTP-style message format (text format)
    - SIP URI (sip:niccolini@netlab.nec.de), global SIP address space using DNS
    - modular design
    - no need for peering/hierarchies
- H.323 has is introducing new options in the last versions that were part of SIP from the beginning
  - H.323 URL (h.323:niccolini@netlab.nec.de)
  - FastStart feature (no multistage signaling)
  - complexity grows (backward compatibility)
    - update of software/hardware takes more time

Comparing H.323 and SIP

- SIP is less complex than H.323
- SIP is better suited for the integration of presence, IM, and audio/video
  - SIP is more suited to mobile scenarios
- H.323 has more history right now (better interoperability)

- The trend indicates SIP as the winner (but on a long term scale)
  - If you start deploying IP Telephony now there is no reason why you should not deploy SIP instead of H.323

© NEC Corporation 2005

Integrating PSTN and Internet Telephony using ENUM

Empowered by Innovation NEC

ENUM protocol: what for?

- ENUM makes part of a more general framework on
  - “How to locate SIP Services”

- DNS is the preferred mechanism for determining IP address, port and transport of the host to which a SIP request is sent

- DNS provides two record types relevant to SIP requests:
  - SRV records
  - NAPTR records
  - both can be used in combination with ENUM to locate and differentiate SIP services

© NEC Corporation 2005

How to locate SIP services?

- Services need to be separated by the machine that provide that service

- If Alice is using servers like:
  - mailserver.atlanta.com (as mail server)
  - sip-proxy.atlanta.com (as SIP server)
- It is convenient to use one URI to address multiple services just changing the prefix
  - mailto:alice@atlanta.com
  - sip:alice@atlanta.com
- Instead of
  - mailto:alice@mailserver.atlanta.com
  - sip:alice@sip-proxy.atlanta.com

- Service location is achieved using SRV records (RFC 2782, February 2000)
  - one domain name is mapped to more services and to more machine
- SRV records are useful for
  - service differentiation
  - redundancy (multiple SIP proxies)
  - backup (failover SIP proxies)
  - transport protocol differentiation (UDP, TCP, TLS over TCP)

© NEC Corporation 2005

How to locate SIP services?

- SRV records are in the form of:

```
_Service._Proto.Name TTL Class SRV Priority Weight Port Target
```

- For example:

```
_sip._udp.bigu.edu 43200 IN SRV 10 10 5060 sipserver.bigu.edu.
```

- An example DNS implementation with redundant proxy servers might look like this:

```
_sip._udp.bigu.edu.   43200 IN SRV 0 0 5060  sipserver1.bigu.edu.
_sip._udp.bigu.edu.   43200 IN SRV 1 0 5060  sipserver2.bigu.edu.
_sip._tcp.bigu.edu.   43200 IN SRV 0 4 5060  sipserver1.bigu.edu.
_sip._tcp.bigu.edu.   43200 IN SRV 0 2 5060  sipserver2.bigu.edu.
_sips._tcp.bigu.edu.  43200 IN SRV 0 0 5060  sipserver1.bigu.edu.
_sips._tcp.bigu.edu.  43200 IN SRV 0 0 5060  sipserver2.bigu.edu.
```

© NEC Corporation 2005

ENUM protocol: what for?

- Internet URIs look like these:
  - mailto:saverio.niccolini@mymaildomain.org
  - sip:callme@mysipdomain.com

- Telephone systems use the E.164 numbering
  - +39 050 2217678
  - +49 6221 563423

- ENUM role is to map these address schemes one on the other
- ENUM (E.164 Number Mapping) has been standardized
  - E.164 numbers are mapped to Internet URIs
  - IETF RFC 3761, April 2004 (obsoletes RFC 2916, September 2000):
    - The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)

© NEC Corporation 2005

ENUM protocol: basics

- Remove all characters with the exception of the digits
  - +44-207-9460-148 becomes 442079460148

- Put dots (".") between each digit.
  - 442079460148 becomes 4.4.2.0.7.9.4.6.0.1.4.8

- Reverse the order of the digits
  - 4.4.2.0.7.9.4.6.0.1.4.8 becomes 8.4.1.0.6.4.9.7.0.2.4.4

- Append the string ".e164.arpa" to the end
  - 8.4.1.0.6.4.9.7.0.2.4.4 becomes 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa

- 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa is now the DNS zone (domain-name)

- The DNS zone is used to request NAPTR records which may contain the end result (or produce new keys in the form of domain-names from the DNS using SRV records)

© NEC Corporation 2005

Empowered by Innovation NEC

ENUM protocol: basics

- NAPTR records (specified in RFC 3403) are more of more general use than ENUM
  - they are used also in normal DNS queries
- NAPTR records are in the form of:

domain-name TTL class NAPTR order preference flags service regexp target

- For example:

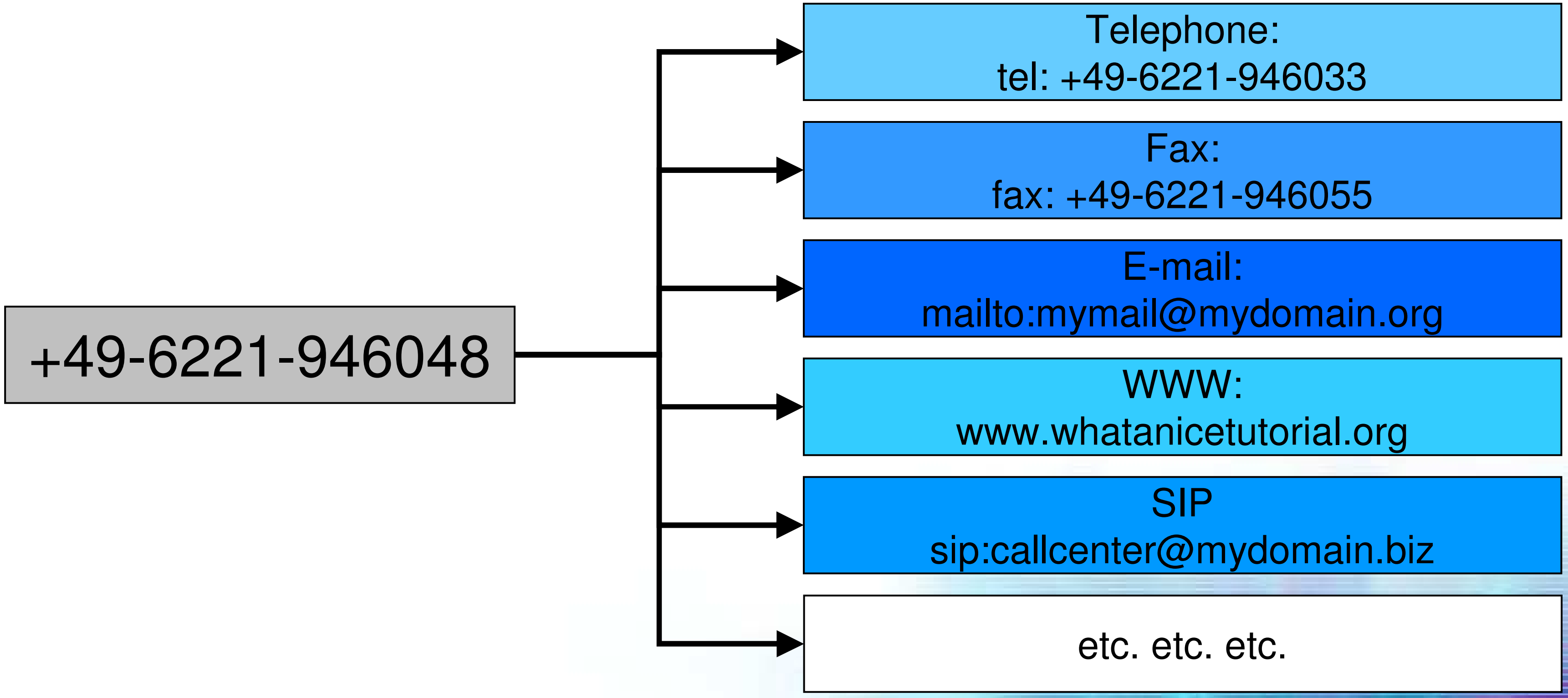
bigu.edu IN NAPTR 60 50 “s” “SIP+D2U” “” _sip._udp.bigu.edu

- The domain name is the one being queried
- The possible services are
  - SIP+D2U (SIP Protocol over UDP)
  - SIP+D2T (SIP Protocol over TCP)
  - SIP+D2S (SIP Protocol over SCTP)
  - SIPS+D2T (SIP Protocol over TLS over TCP)
- Regexp field may be used to change the domain name
- The target filed are static target where to send your message (with the indication of protocol included)

© NEC Corporation 2005

ENUM protocol: just one number

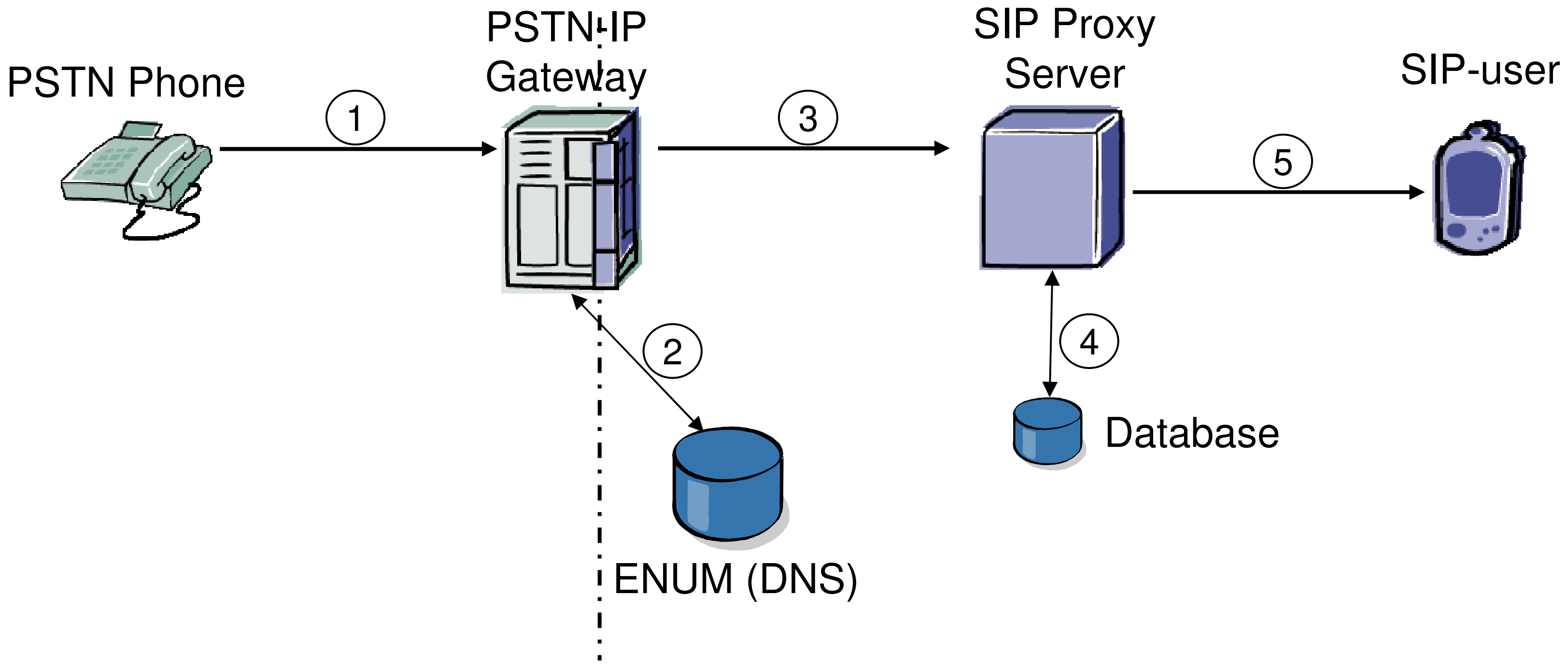
- ENUM is suitable to accommodate other applications



Empowered by Innovation NEC

© NEC Corporation 2005

Using ENUM protocol: PSTN to SIP



1. The call is directed to a PSTN-IP Gateway (GW)
2. GW looks up in ENUM (DNS) and gets SIP-user's SIP address as answer
3. GW routes call to SIP Proxy Server (SIP address in ENUM answer point to it)
4. SIP Proxy server consults its database for the current location(s) of SIP-user
5. Call is routed to SIP phone of SIP-user

Empowered by Innovation NEC

© NEC Corporation 2005

ENUM protocol: concerns

- ENUM protocol suffers from “legal” problems (Layer 9)
  - Who has to set-up the entries?
  - Who has the right to delegate the use of numbers for use in Internet Telephony?

- Can ENUM scale up to big numbers?
  - DNS entries are difficult to be populated and maintained when numbers are getting bigger and bigger
  - ENUM is maybe better applicable at the border of the network where numbers are small

- Some sort of hierarchy/peering is still needed among proxies to avoid queries
  - Extensions of Global Dialing Scheme (GDS) developed for H.323 Videoconferencing are currently being discussed in the TERENA Task Force – Voice Video and Collaboration (TF-VVC)
    - http://www.terena.nl/tech/task-forces/tf-vvc/

Applications and world-wide deployment

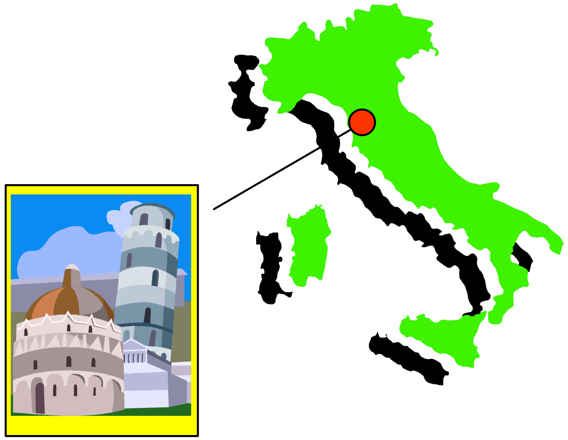
Empowered by Innovation NEC

What can be done with this?

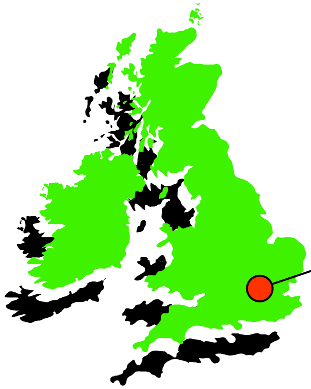
- Applications
  - The vision of a SIP mobile application
- World-wide deployments
  - SIP.edu
  - SIP.eu
  - Possible add-ons
  - NEC deployment

The vision of a SIP mobile application

- Alice and Barbara both work at GARR in Pisa



- Alice travels for a conference to Great Britain



© NEC Corporation 2005

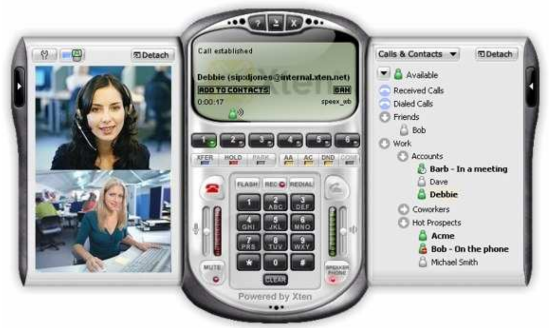
The vision of a SIP mobile application

- Barbara is working in the office and did not know that Alice is in Great Britain but she sees with her messaging client that Alice is online and initiate a mixed call/chat

Empowered by Innovation NEC

© NEC Corporation 2005

Scene 1



Barbara: Hi Alice, how are you?

Alice: I am fine, I am at a conference in London!

Barbara: Cool! I have called you because I need help in some technical matter. Do you know … ?

Alice: I have to think about. I'll call you later.

Barbara: Ok, thanks.

Barbara: Hi Alice, how are you?

Alice: I am fine, I am at a conference in London!

Barbara: Cool! I have called you because I need help in some technical matter. Do you know … ?

Alice: I have to think about. I'll call you later.

Barbara: Ok, thanks.

© NEC Corporation 2005

Scene 2

- Alice thinks about the question and has an idea and decides to call Barbara

- Barbara is not in the office, has joined some friends for a coffee
- She has her SIP WiFi phone with her

- When Alice calls Barbara’s number in Pisa
  - a Gateway converts the call
  - the SIP Proxy forks it to multiple locations making both her SIP client and her SIP WiFi ringing
  - Barbara picks up the call with the SIP WIFi phone and Alice can explain her the answer

© NEC Corporation 2005

What is behind all that?

- Scene 1
  - Mobility
    - Easy reachable when being abroad
  - Integration
    - Different Services (Presence, IM, Audio, Video)
- Scene 2
  - Mobility
    - Being reachable at multiple points at the same time
  - Integration
    - Open, non proprietary standards

- Protocols: SIP
- Services: ENUM
- Architectures: Gateway, Proxy, User Administration
- Security: NAT, FW
- Legal: TCL (Telecommunication Law)

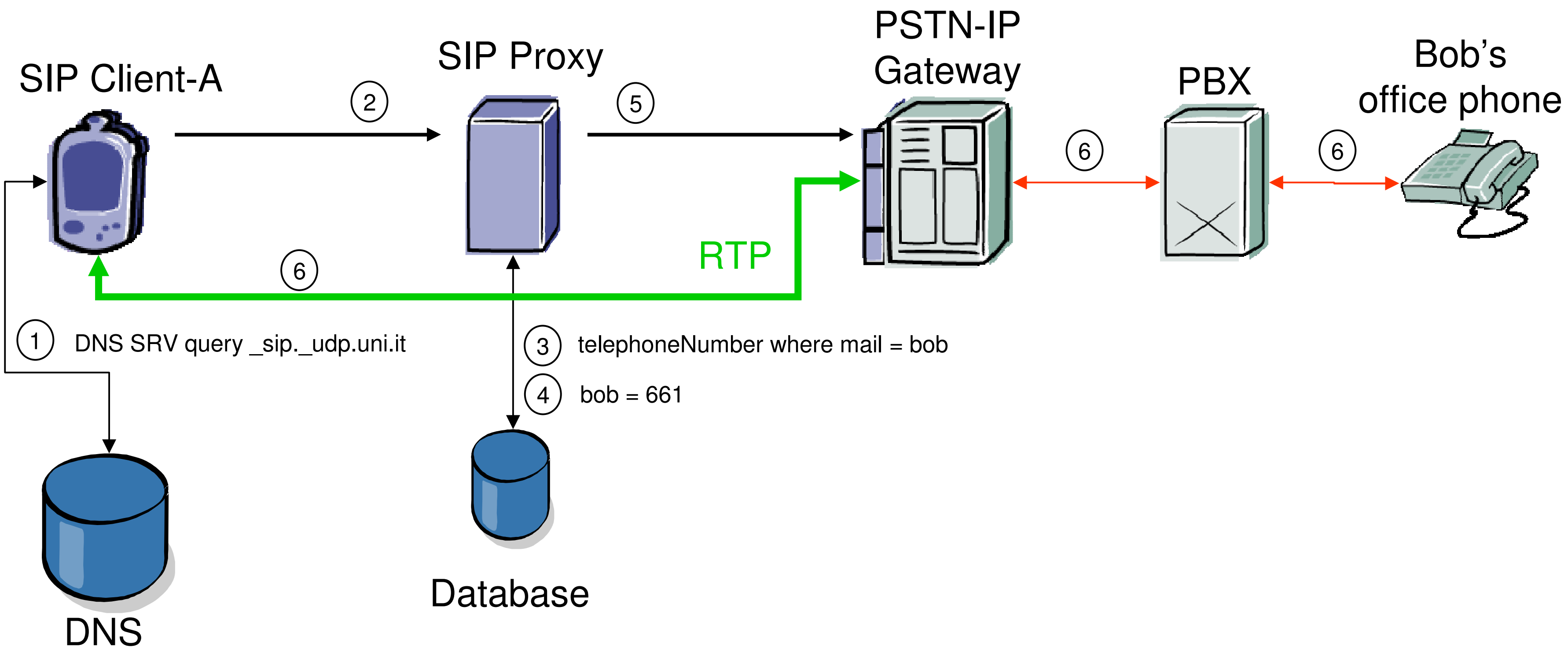
© NEC Corporation 2005

SIP world-wide deployments

- SIP.edu
  - Project of the Internet2 VoIP working group (http://voip.internet2.edu/)
- Aim:
  - Increase the number of SIP-reachable users (mainly in Internet2 but open to other academic institutions)
  - Extend email identities to voice services (promote convergence)
  - Build an academic community developing and deploying SIP services
    - with low cost entries
    - providing an useful service

© NEC Corporation 2005

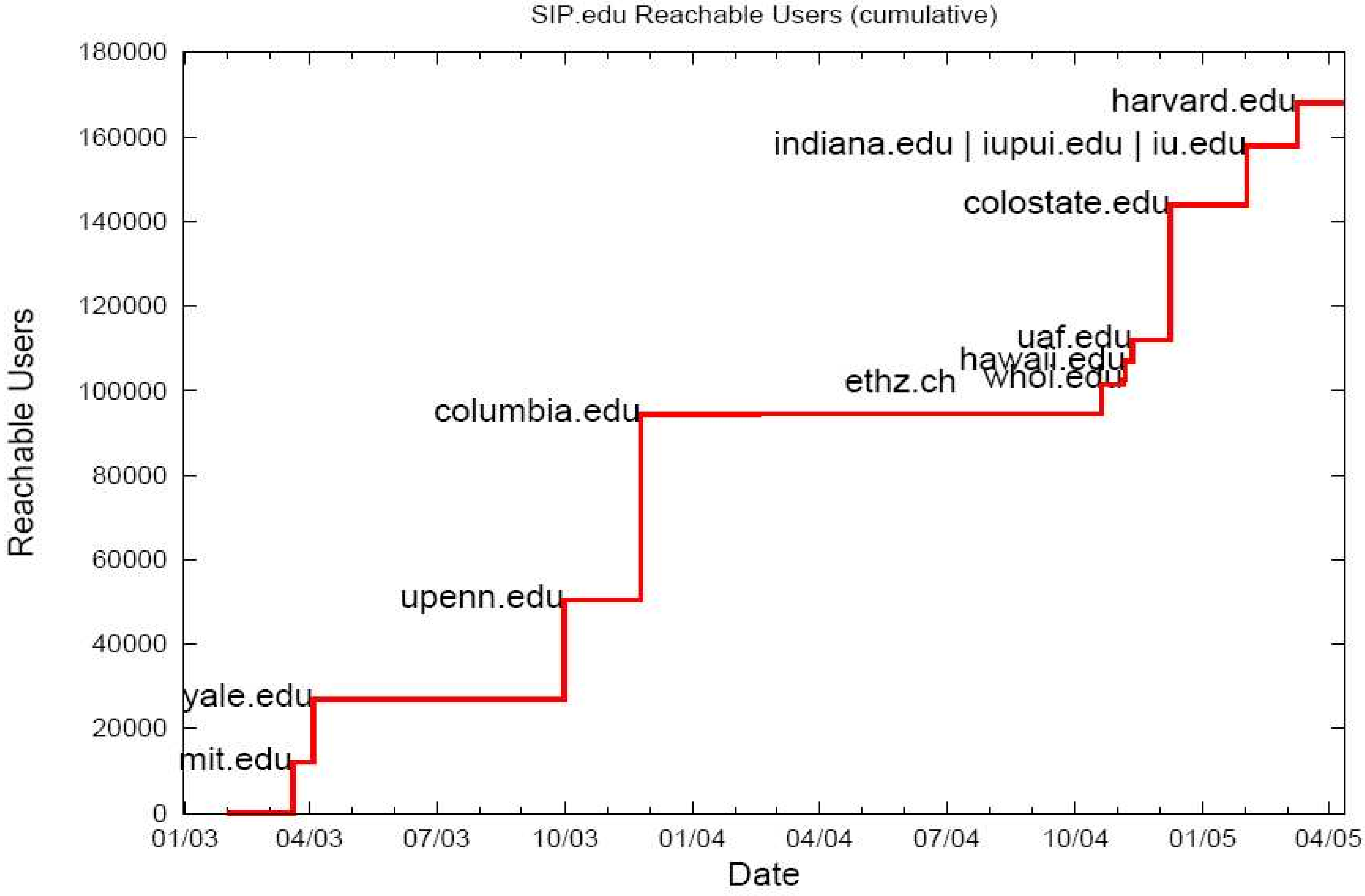
SIP.edu: How it works



0. Alice types bob@uni.it on her SIP Client
1. SIP Client of Alice finds via DNS resolution the SIP Server of Bob's university: proxy.uni.it
2. Alice's SIP Client sends an INVITE sip:bob@proxy.uni.it to the SIP server of the university
3. The proxy looks up Bob's phone number in the 'user directory'
4. 'user directory' tells SIP Proxy that Bob has extension number 661
5. The proxy rewrites the INVITE according the user directory and sends it to the gateway
6. The gateway initializes a connection to Bob's phone and joins Alice and Bob.

© NEC Corporation 2005

SIP.edu: how big it is



SIP.edu: Benefits and Open Issues

- Benefits:
  - Employees of an organization can be reached worldwide by a SIP client via their email-address
  - After the realization of SIP.edu, the organization is ready to build an organization-wide IP Telephony infrastructure (IM, Presence, Video) because the basic components are already available
  - ENUM can be easily integrated
  - SIP to SIP calls are open and always possible
- Open issues so far:
  - Call forking to multiple location should be implemented (office phone and registered SIP clients)
  - The claim that email addresses should converge to voice identities is not completely right
    - what about inbound integration with PSTN?
      - ENUM is there and I still have to remember an E.164 number as long as PSTN exists (for a long time) if I am calling from a PSTN phone (let's use ENUM for this)
  - It is a closed environment
    - what about people not employed in the organization that do not have a number (students for example)?
    - what about outbound calls to PSTN?

© NEC Corporation 2005

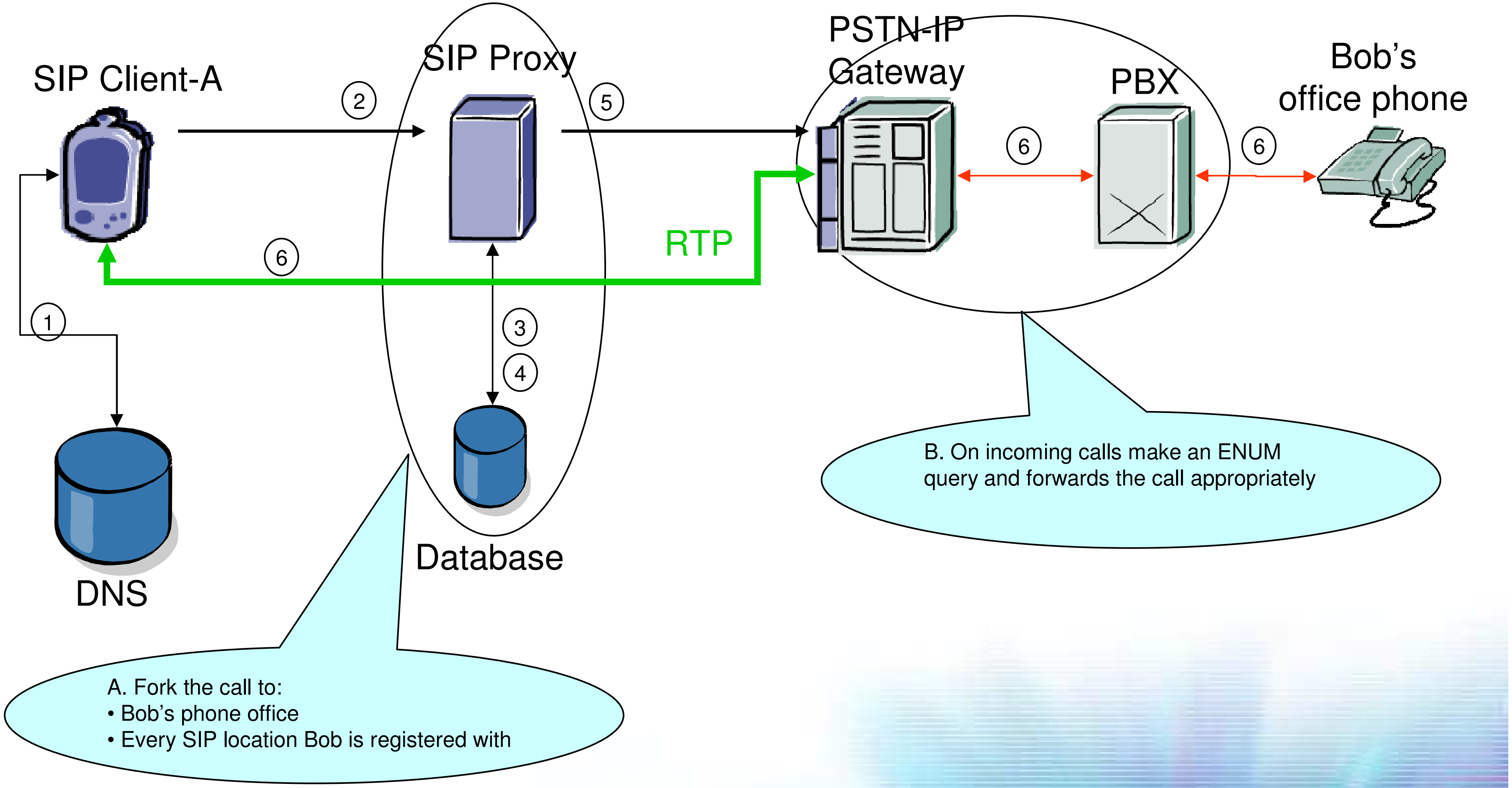
SIP.edu towards SIP.eu vision

- SIP.eu
  - SWITCH is “The Swiss Education and Research Network” (http://www.switch.ch)
  - They organized in January a SIP Infoday where they have promoted the adoption of an advanced vision of SIP.edu

- This should converge in a SIP.eu (European version of SIP.edu) currently being discussed
  - in Switzerland at national level
  - in the TERENA Task Force – Voice Video and Collaboration (TF-VVC) (http://www.terena.nl/tech/task-forces/tf-vvc/)

© NEC Corporation 2005

SIP.edu towards SIP.eu vision



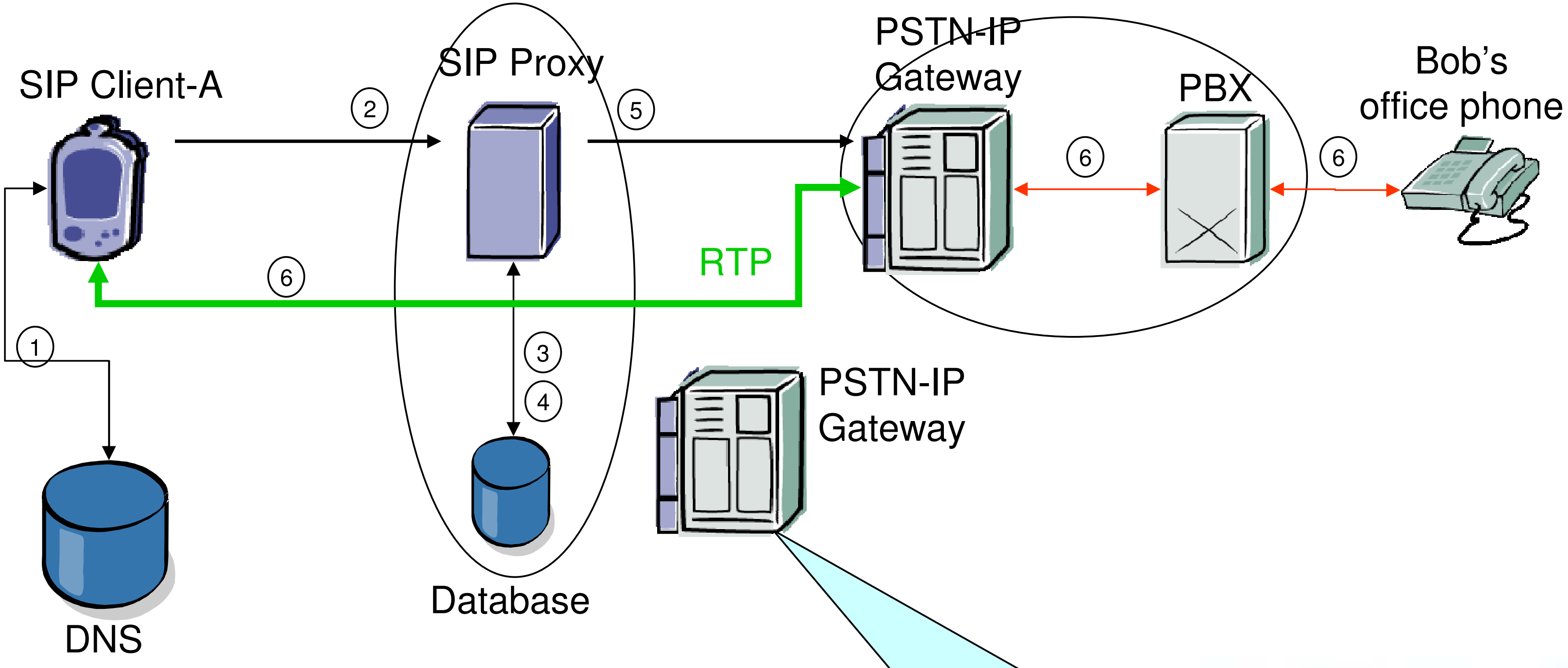
A. Fork the call to:

- Bob's phone office
- Every SIP location Bob is registered with

B. On incoming calls make an ENUM query and forwards the call appropriately

Empowered by Innovation NEC

SIP.eu: another add-on



C. Deploy additional gateways for outbound PSTN calls (charging on call-by-call may apply)

D. Have additional number space for students

© NEC Corporation 2005

Empowered by Innovation NEC

SIP.eu: another add-on

- Deploying additional gateways for outbound PSTN calls (charging on call-by-call may apply)
- Having additional number space for students

- This can not be handled at a global level
  - single organization have to deal with it and give services to their users (employees and/or students)

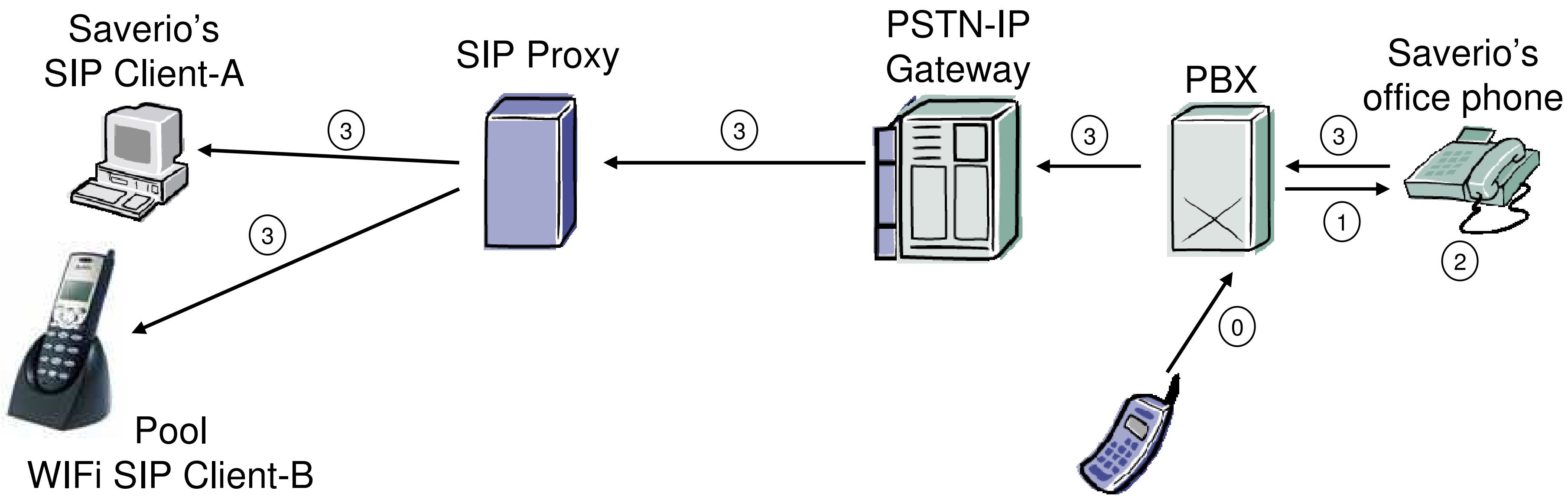
- There are already example of this
  - Internet Telephony and Polyphone project at ETH Zurich (only in German, sorry…)

Empowered by Innovation NEC

© NEC Corporation 2005

SIP Deployment at NEC Europe Ltd.

- Network Laboratories in Heidelberg (http://www.netlab.nec.de/)



Inbound call

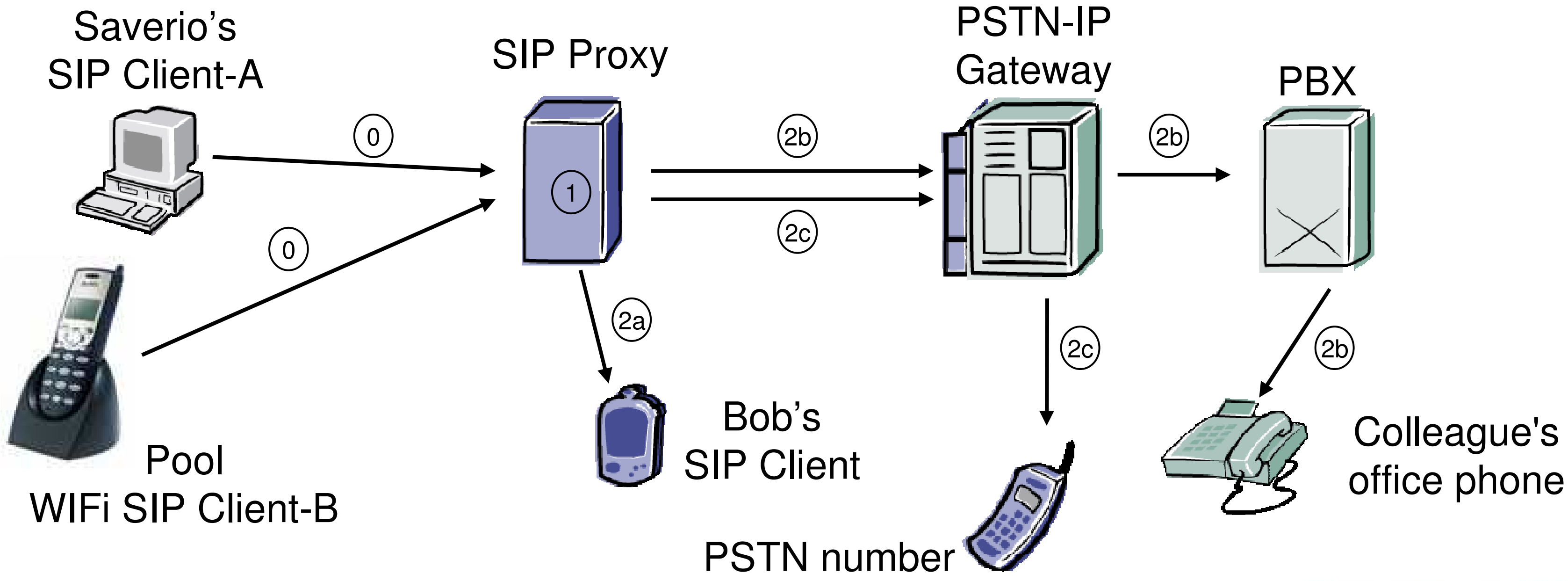
0. Someone decides to call me at my office number (0049-6221-9051118)
1. The call arrives at NEC PBX in Heidelberg and forwarded to my phone
2. I am away, I have configured an entry to forward the call to my SIP client (my phone does not ring)
3. The call is redirected to the SIP gateway (to the number associated to my SIP client (be it my software client or the WiFi pool phone)

We have not yet configured ENUM, thus no ENUM entry for such a number (gateway just configured statically to handle such redirected calls)

© NEC Corporation 2005

SIP Deployment at NEC Europe Ltd.

- Network Laboratories in Heidelberg (http://www.netlab.nec.de/)



Outbound calls

0. No matter where I am I register to my SIP proxy and I dial the numbers on my SIP clients as I was in the office (0 to exit, etc.)
1. I can call both SIP address, internal numbers and PSTN numbers (configuration of SIP proxy takes care of this)
2. The SIP proxy authorize me and routes my call
   - 2a. SIP-to-SIP: I am only using Internet connection
   - 2b. SIP-to-internal: I am calling my colleagues using internal numbers (65, 39, 32, etc.)
   - 2c. SIP-to-PSTN: I can call all the world as I was in my office (I make a local call in Germany thus my company is happy)

© NEC Corporation 2005

SIP Deployment at NEC Europe Ltd.

- Employees of NEC can be reached worldwide by a SIP client via their SIP address (convergence of SIP address and mail address requires configuration of SRV records, TBD by Network Administrators)
- The organization is ready to build an organization-wide IP Telephony infrastructure (IM, Presence, Video) because the basic components are already available
- ENUM can be easily integrated (TBD by Network Administrators)
- SIP to SIP calls are open and always possible
- Call forking to multiple location (TBD by Network Administrators)
- You can reach NEC employees using my office number or my SIP identity (which will be my email address as soon as Network Administrators configure it)
- I can make call from worldwide as I was in my office
  - Company savings in calls (roaming is 99% more expensive than office calls)

- We have implemented NAT traversal methods to counter one of the major problems of Internet Telephony
  - NAT and FW (this takes us to the next section of the tutorial)

© NEC Corporation 2005

Hot topics and Open Issues
in
Research and Development (R&D)

SIP and Security

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

© NEC Corporation 2005

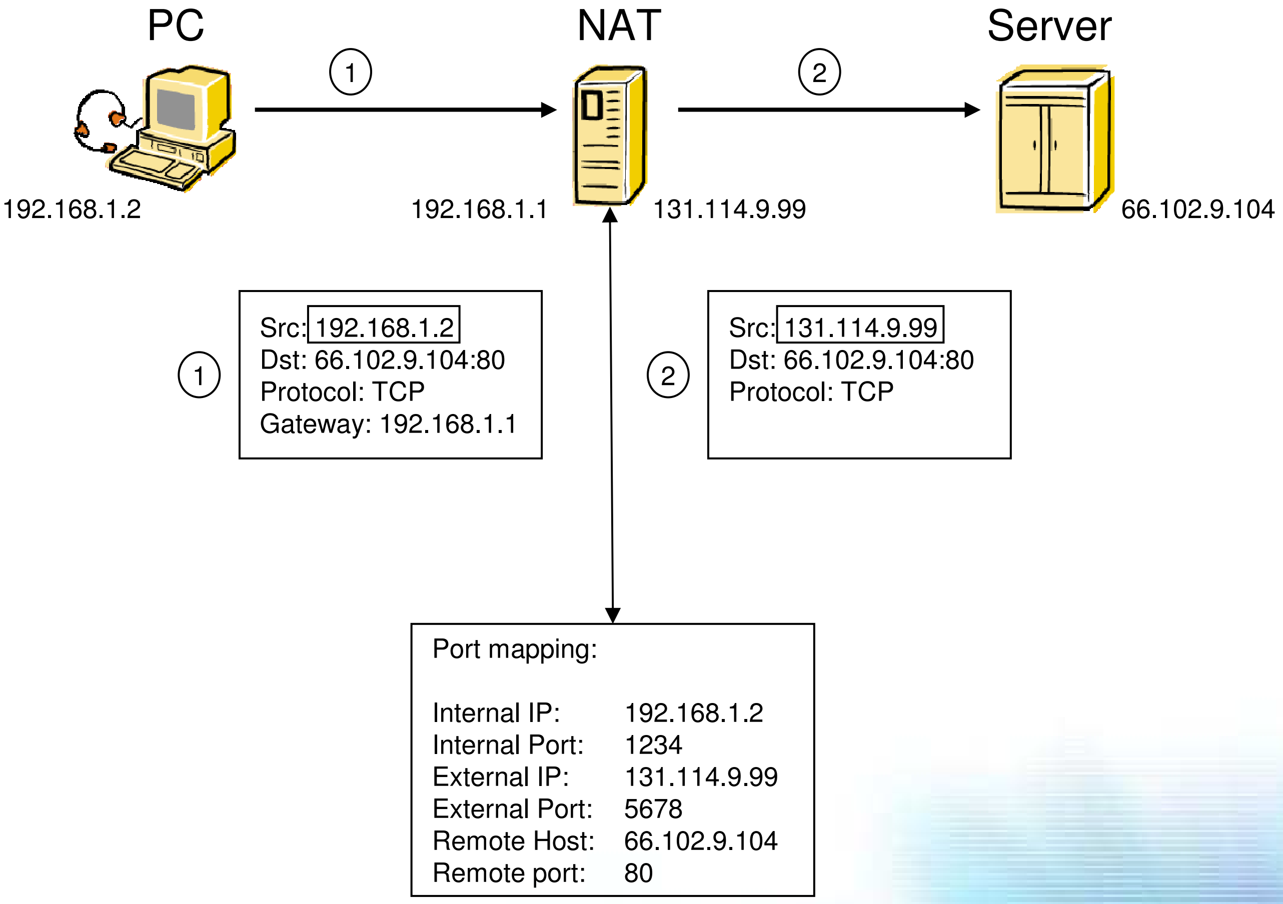
SIP and Security: NATs and FWs

- 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

© NEC Corporation 2005

NATs: Basic Operation



1

Src: 192.168.1.2
Dst: 66.102.9.104:80
Protocol: TCP
Gateway: 192.168.1.1

2

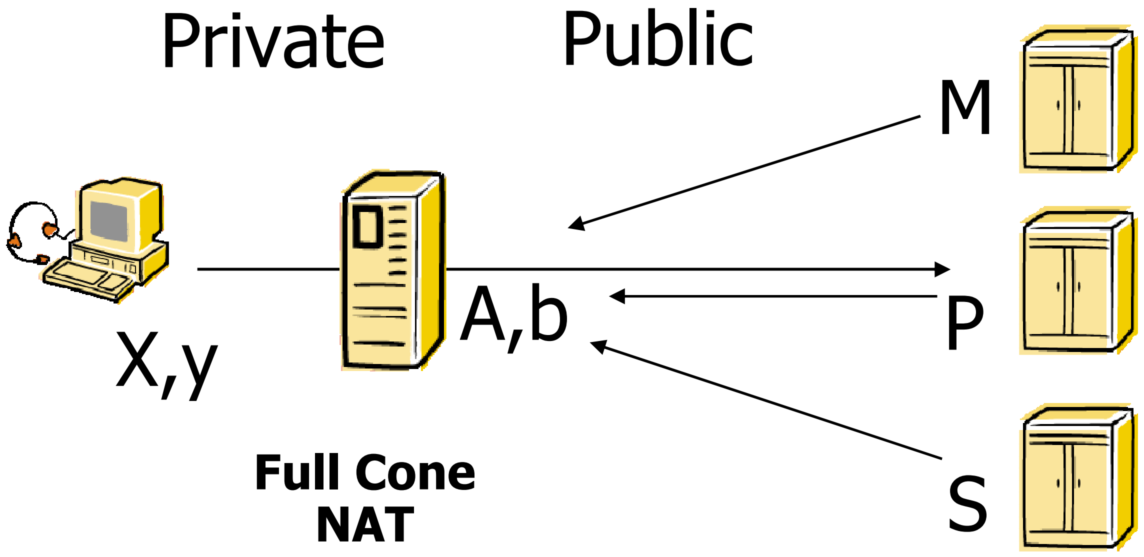
Src: 131.114.9.99
Dst: 66.102.9.104:80
Protocol: TCP

Port mapping:

Internal IP:	192.168.1.2
Internal Port:	1234
External IP:	131.114.9.99
External Port:	5678
Remote Host:	66.102.9.104
Remote port:	80

© NEC Corporation 2005

Types of NATs: Full Cone NAT

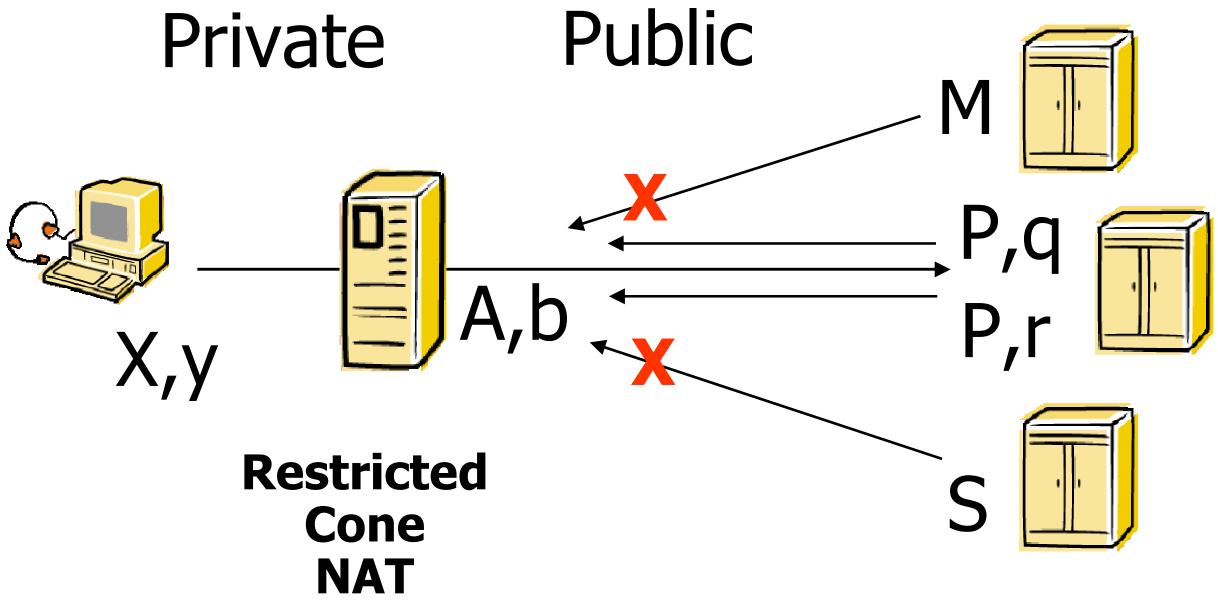


- No restrictions on IP traffic arriving at (A,b)

© NEC Corporation 2005

Empowered by Innovation NEC

Types of NATs: Restricted Cone NAT

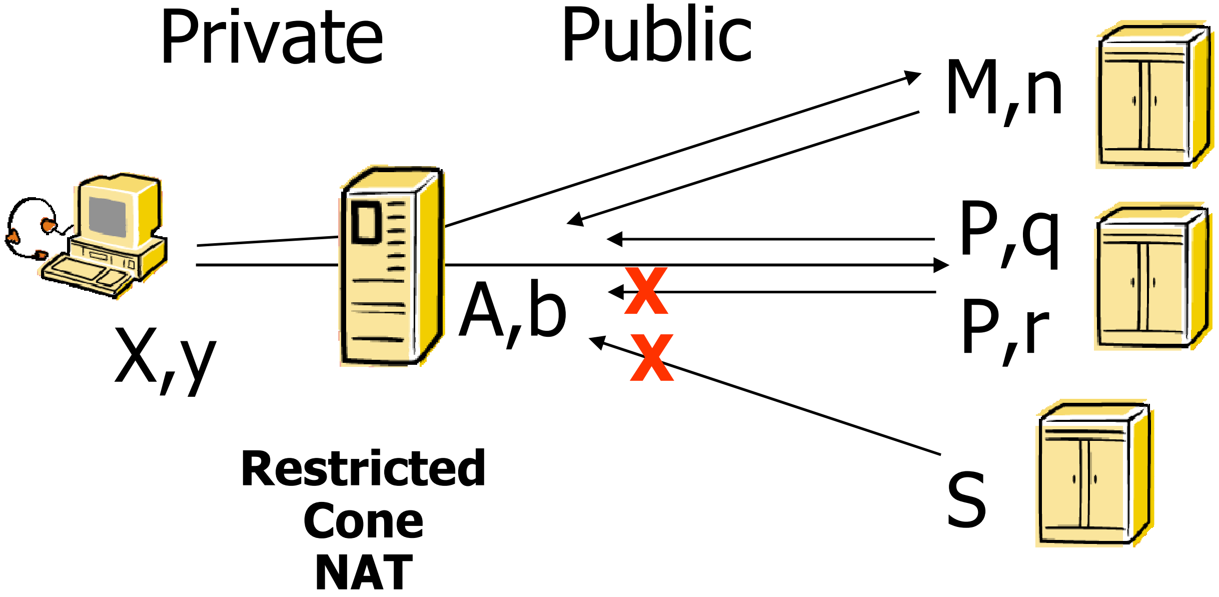


- Restricts at (A,b) only based on public IP address
  - not on public port
- If (X,y) sends to (P,q)
  - (P,r) can send back to (A,b)

Empowered by Innovation NEC

© NEC Corporation 2005

Types of NATs: Port Restricted Cone NAT

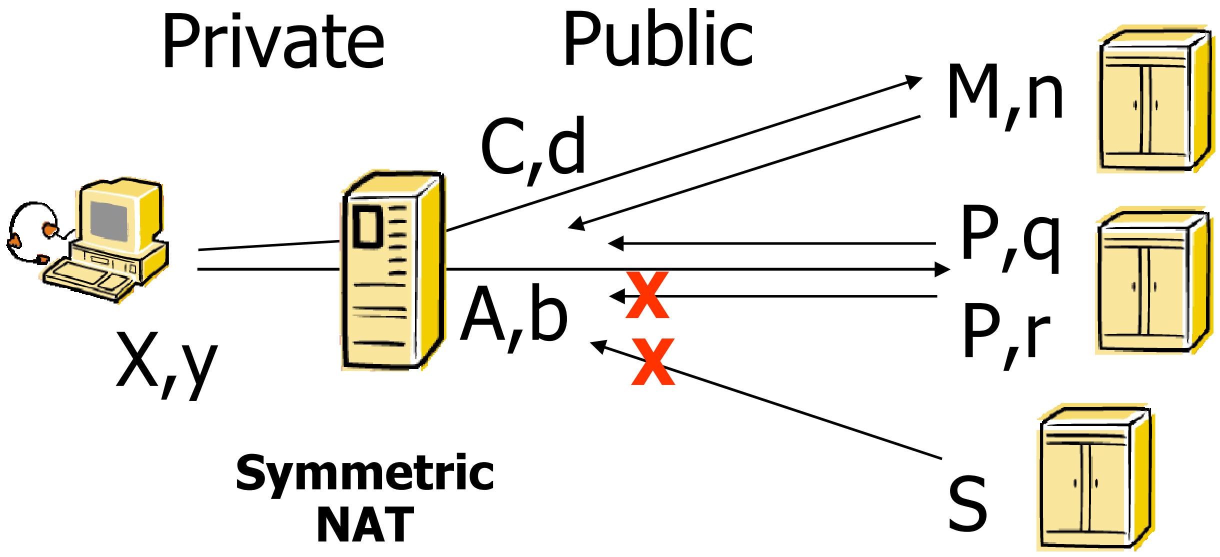


- Restricts at (A,b) only based on public IP address and port number
- If (X,y) sends to (P,q)
  - (P,r) can not send back to (A,b)

Empowered by Innovation NEC

© NEC Corporation 2005

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

© NEC Corporation 2005

Empowered by Innovation NEC

SIP Problems with NATs/FWs

- Different issues with
  - SIP signaling
  - Media

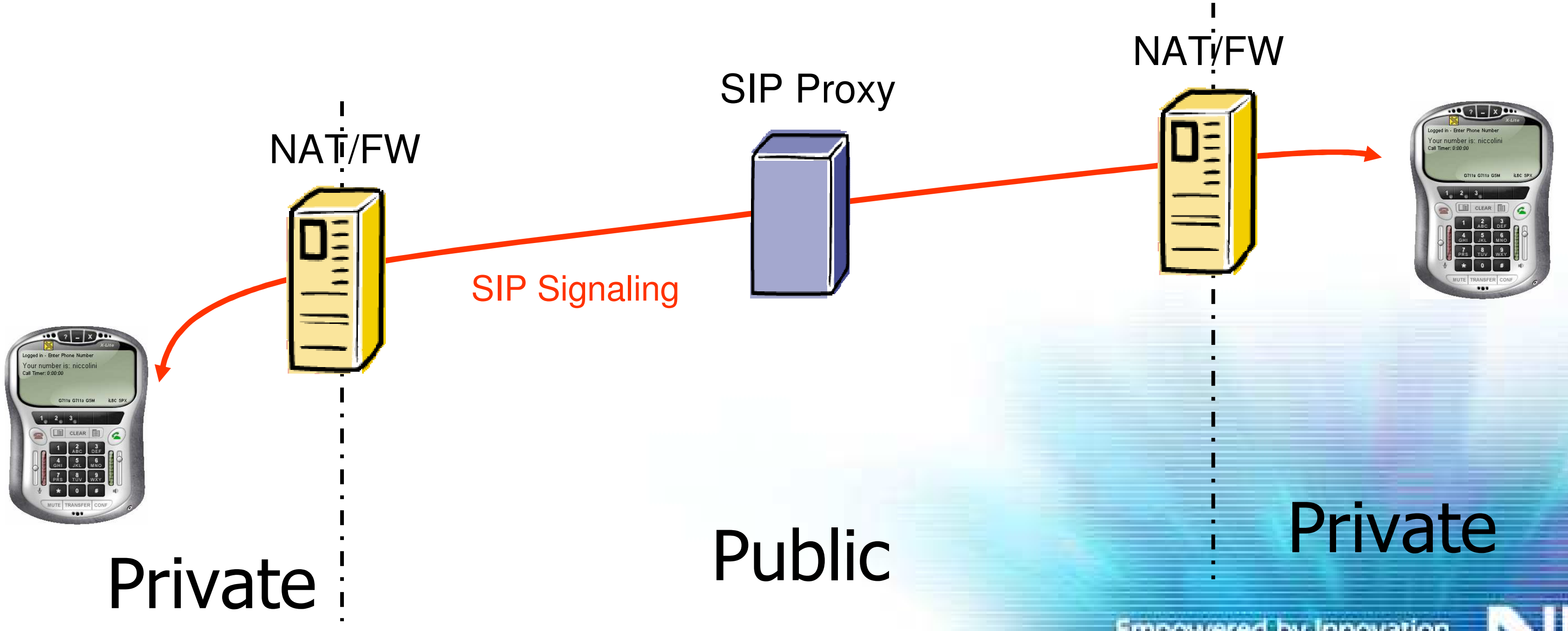
- SIP signaling and media transport is done peer-to-peer

- Media ports are negotiated per call

© NEC Corporation 2005

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

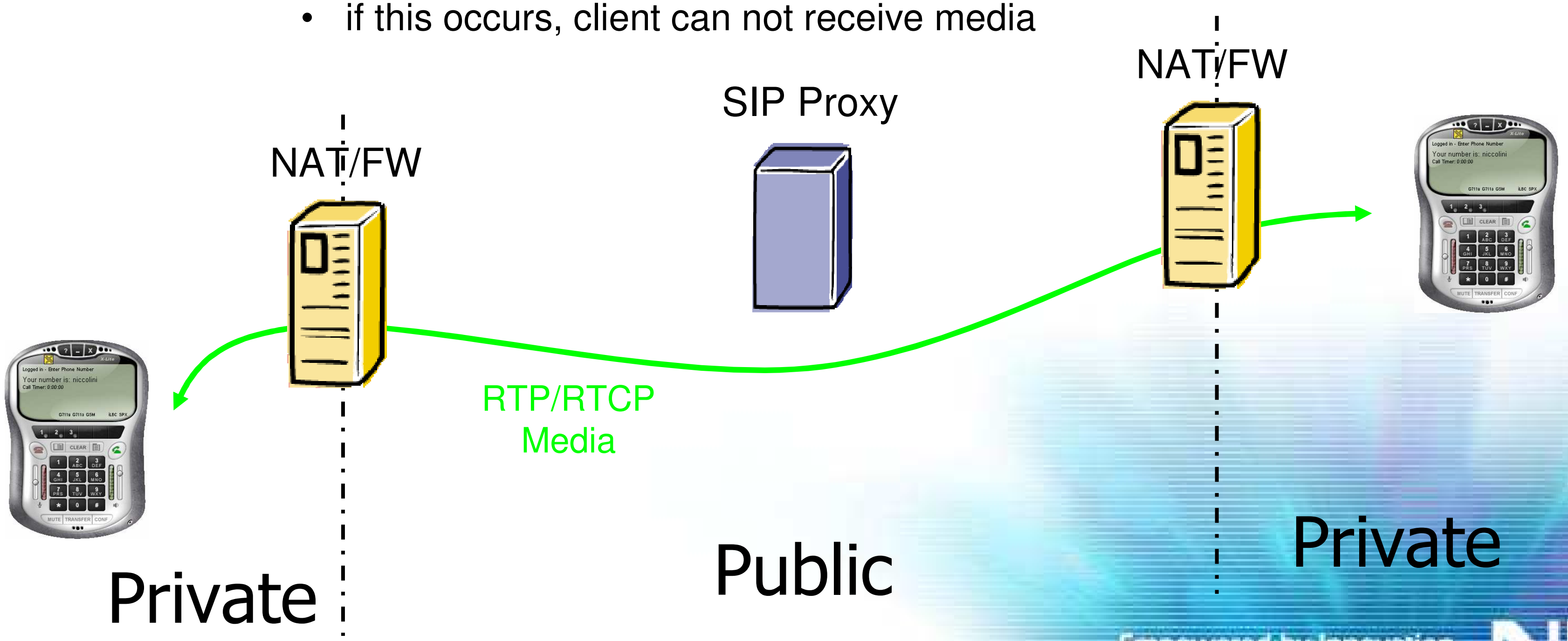


Empowered by Innovation NEC

© NEC Corporation 2005

Media Traversal Issues

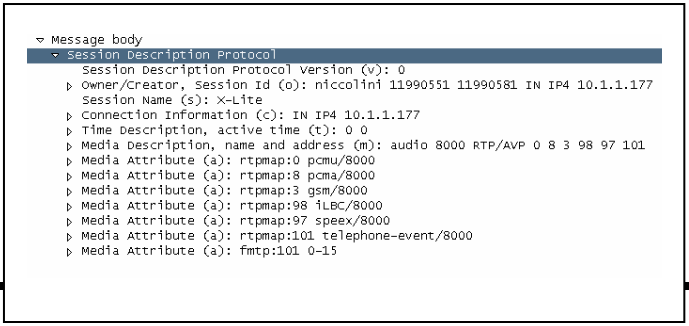
- IP address and port sen in SIP INVITE / 200 OK (SDP) is private
  - not globally routable
- Media must be initiated in Private→Public direction
- RTCP (RTP port + 1) fails through firewall because of NAPT function (port translation)
- Pinhole in NAT/FW will timeout on inactivity (silence suppression)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



© NEC Corporation 2005

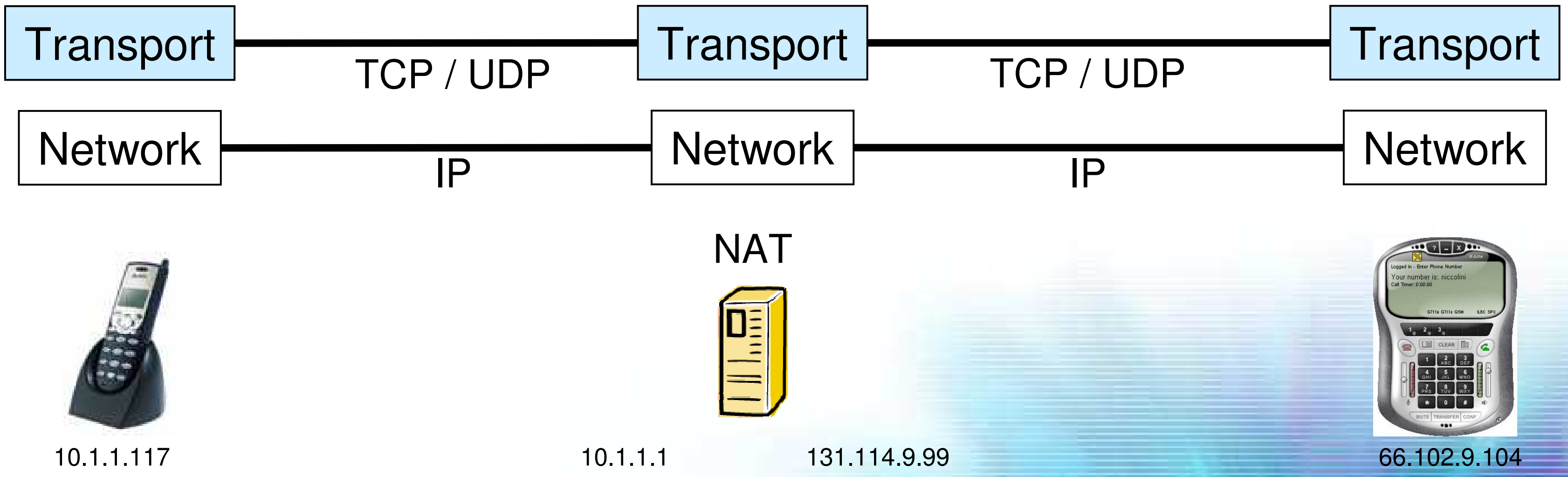
Media Traversal Issues

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
```

Application — SIP Signaling — SIP Signaling — Application



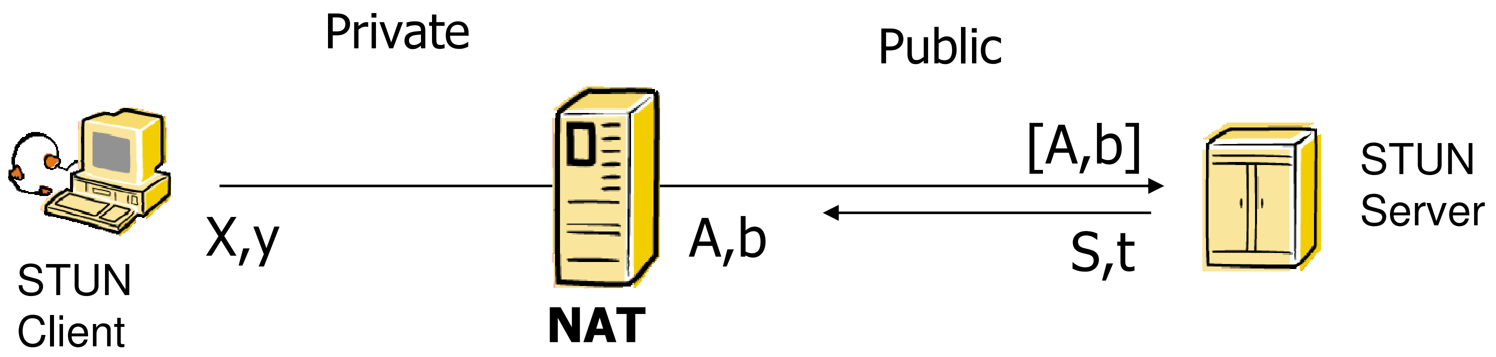
© NEC Corporation 2005

Solutions to NAT Traversal

- STUN
- TURN
- ICE
- B2BUA

- All these solutions require UA to support symmetric signaling and media

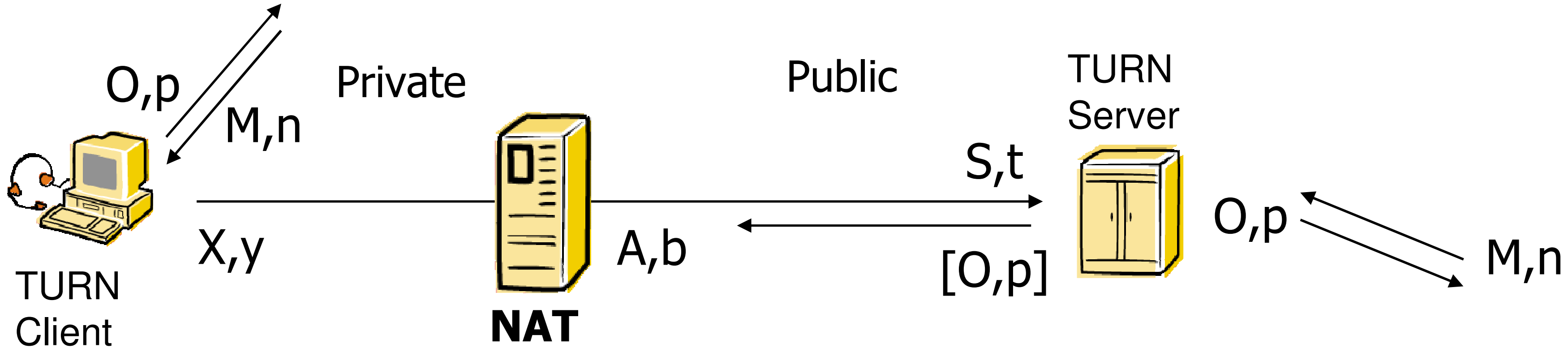
Solutions to NAT Traversal: STUN



- 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

© NEC Corporation 2005

Solutions to NAT Traversal: TURN

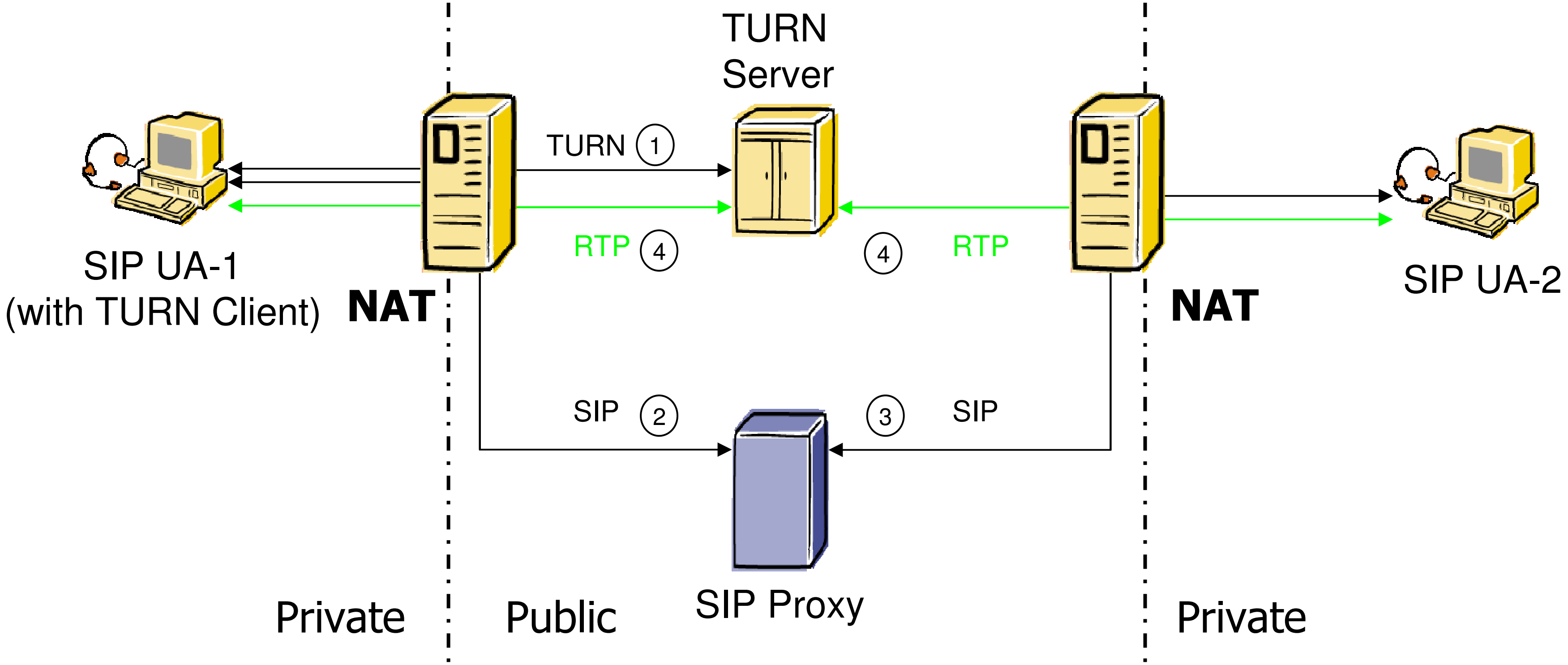


- IETF MIDCOM draft "Traversal Using Relay NAT (TURN)"
  - draft-rosenberg-midcom-turn-07
  - protocol for allowing a client behind a NAT to receive incoming media over UDP
  - work with Symmetric NATs
  - it introduces a relay
    - single point of failure
    - need for server with high performance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

© NEC Corporation 2005

Empowered by Innovation NEC

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)

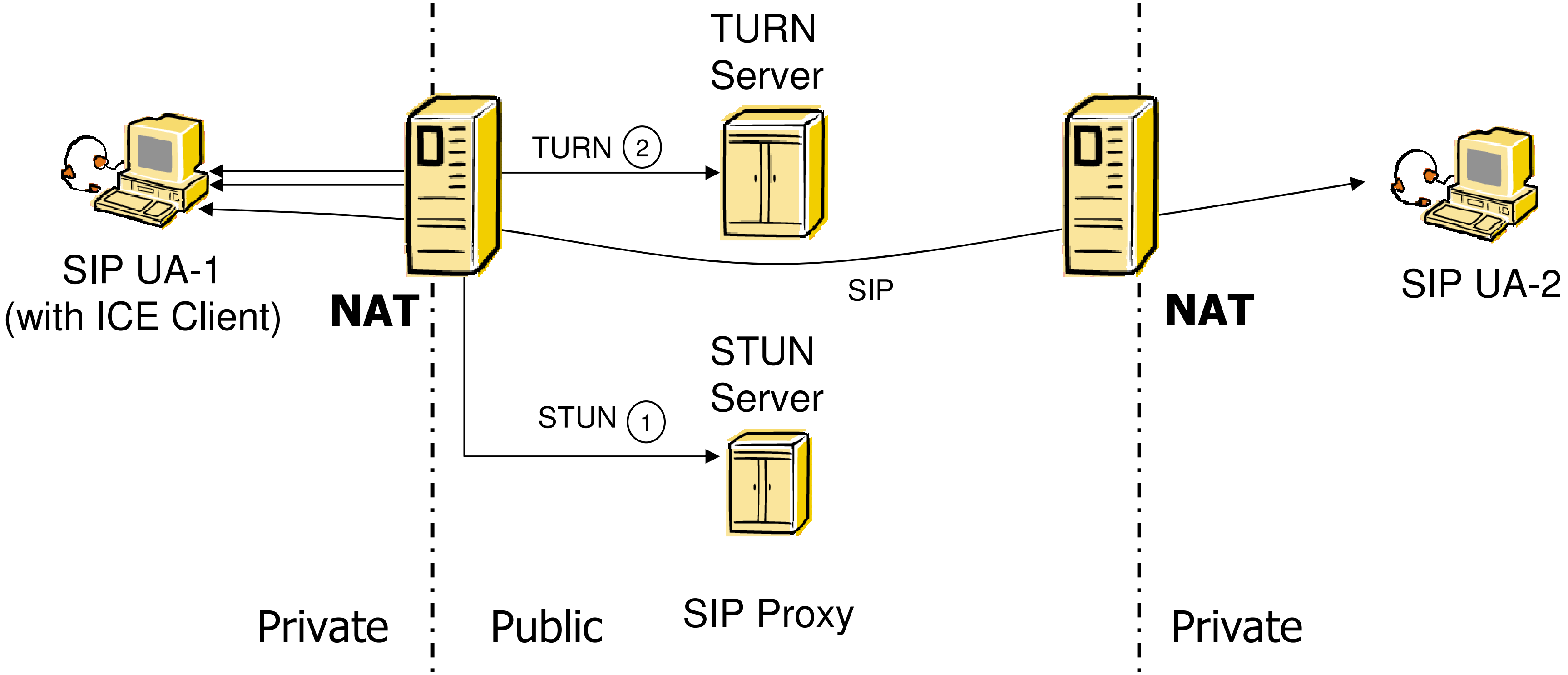
© NEC Corporation 2005

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

© NEC Corporation 2005

Solutions to NAT Traversal: ICE



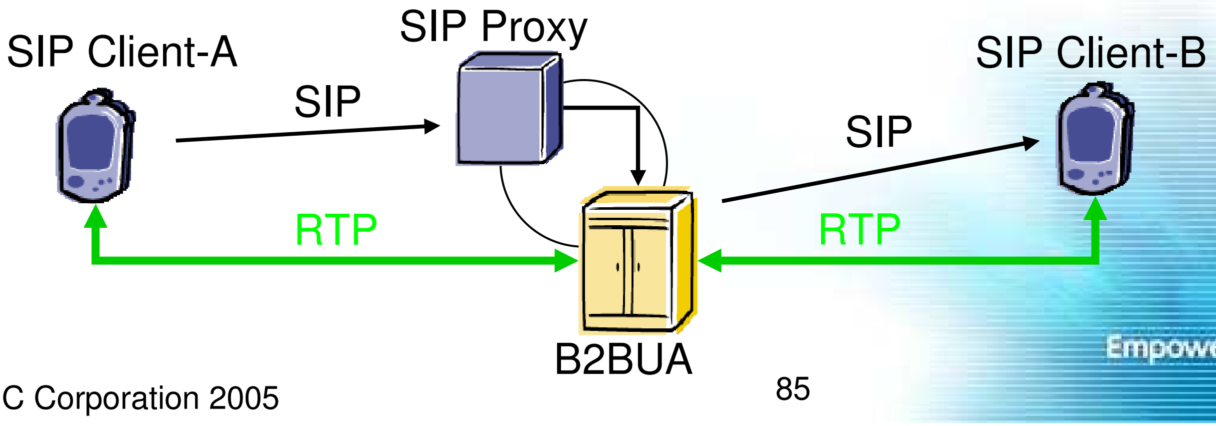
1. UA-1 discovers by STUN what kind of firewall or NAT it is behind and what public IP address (and port mapping rules) its NAT uses
2. As a backup plan it requests a public IP/Port pair from the TURN server
3. UA-1 send an INVITE containing any gained information on how it could be contacted as ordered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

Empowered by Innovation NEC

© NEC Corporation 2005

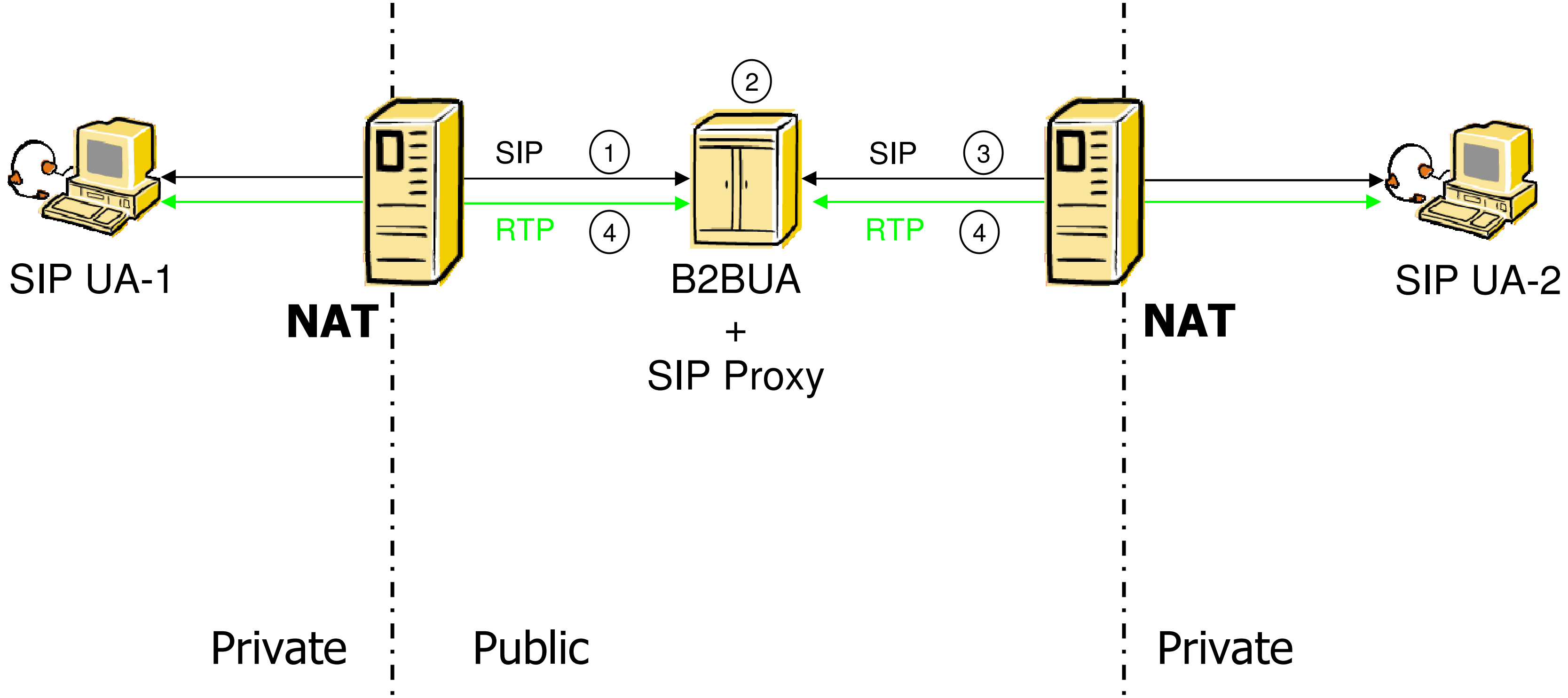
Solutions to NAT Traversal: B2BUA

- 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



© NEC Corporation 2005

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)

Empowered by Innovation NEC

© NEC Corporation 2005

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

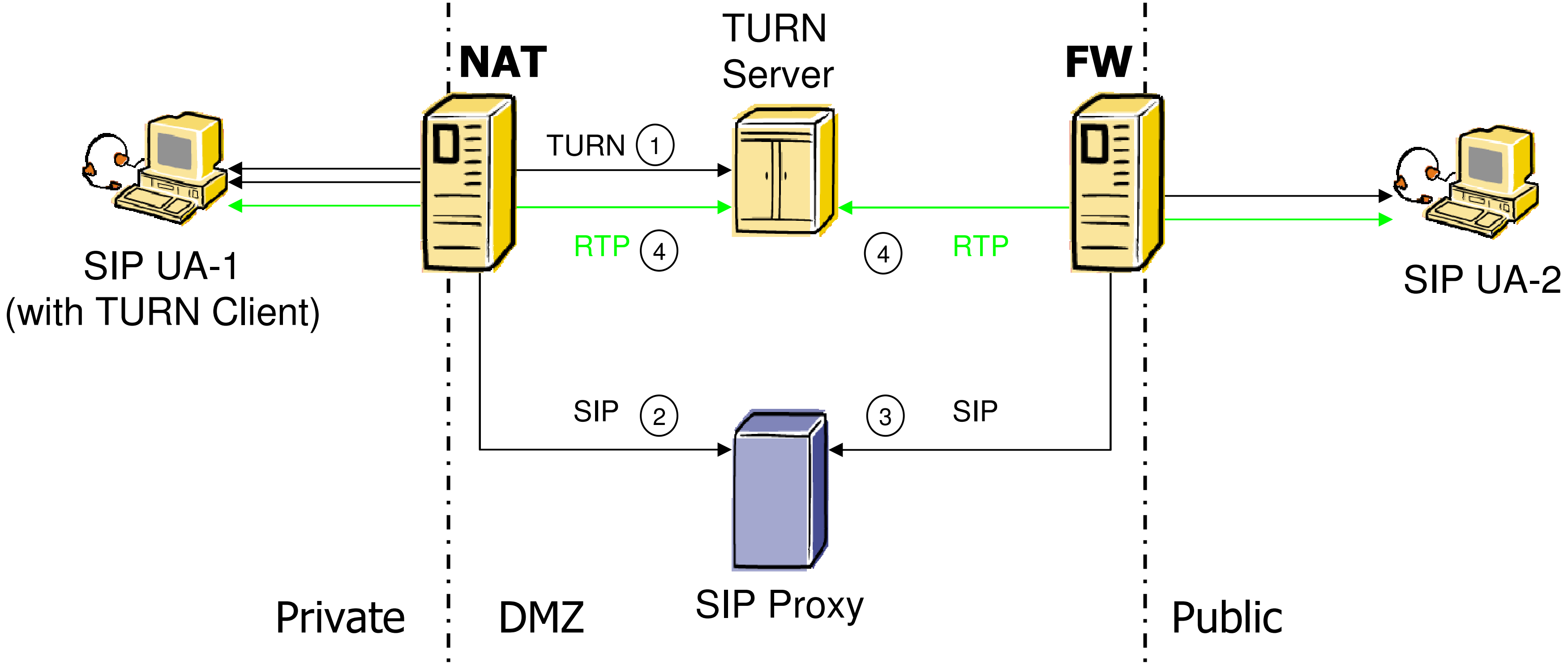
© NEC Corporation 2005

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)

© NEC Corporation 2005

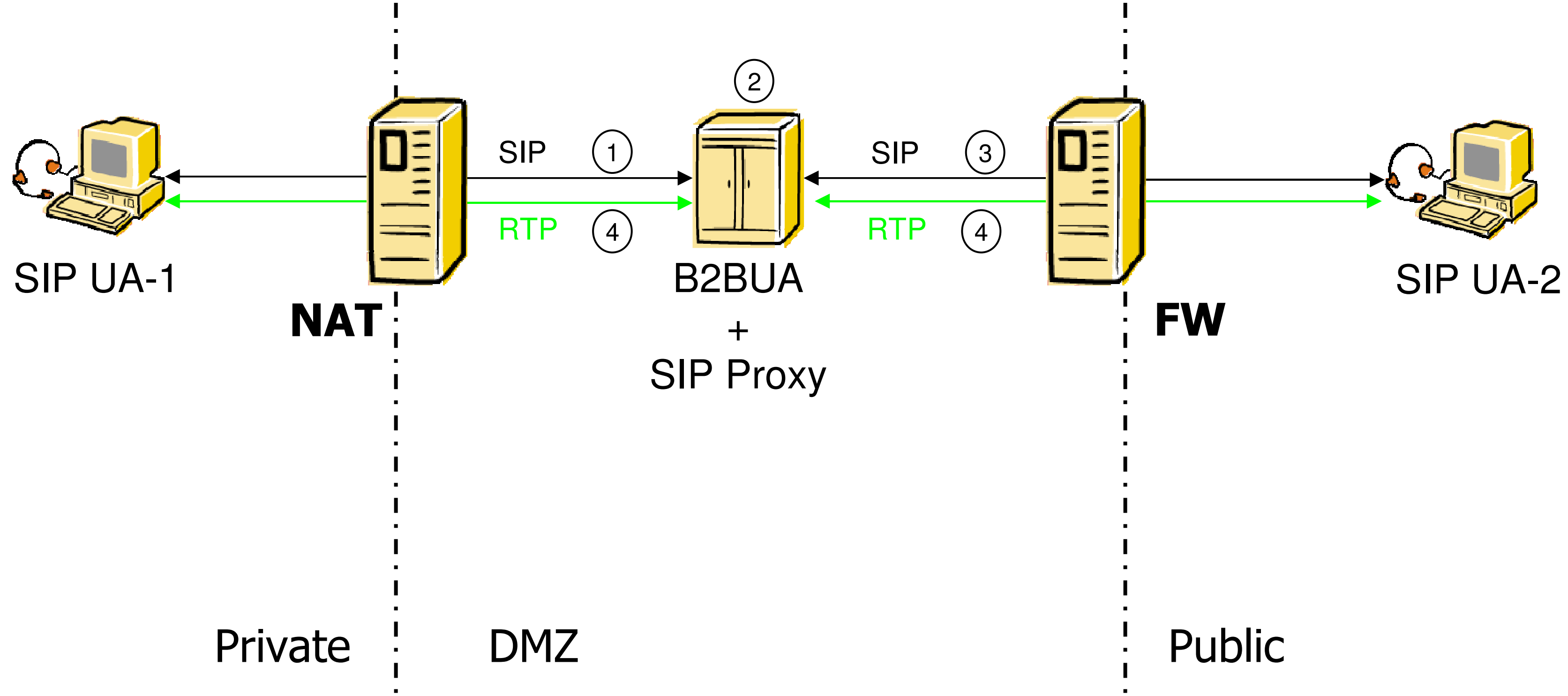
Solutions to FW Traversal: TURN



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

© NEC Corporation 2005

Solutions to FW Traversal: B2BUA

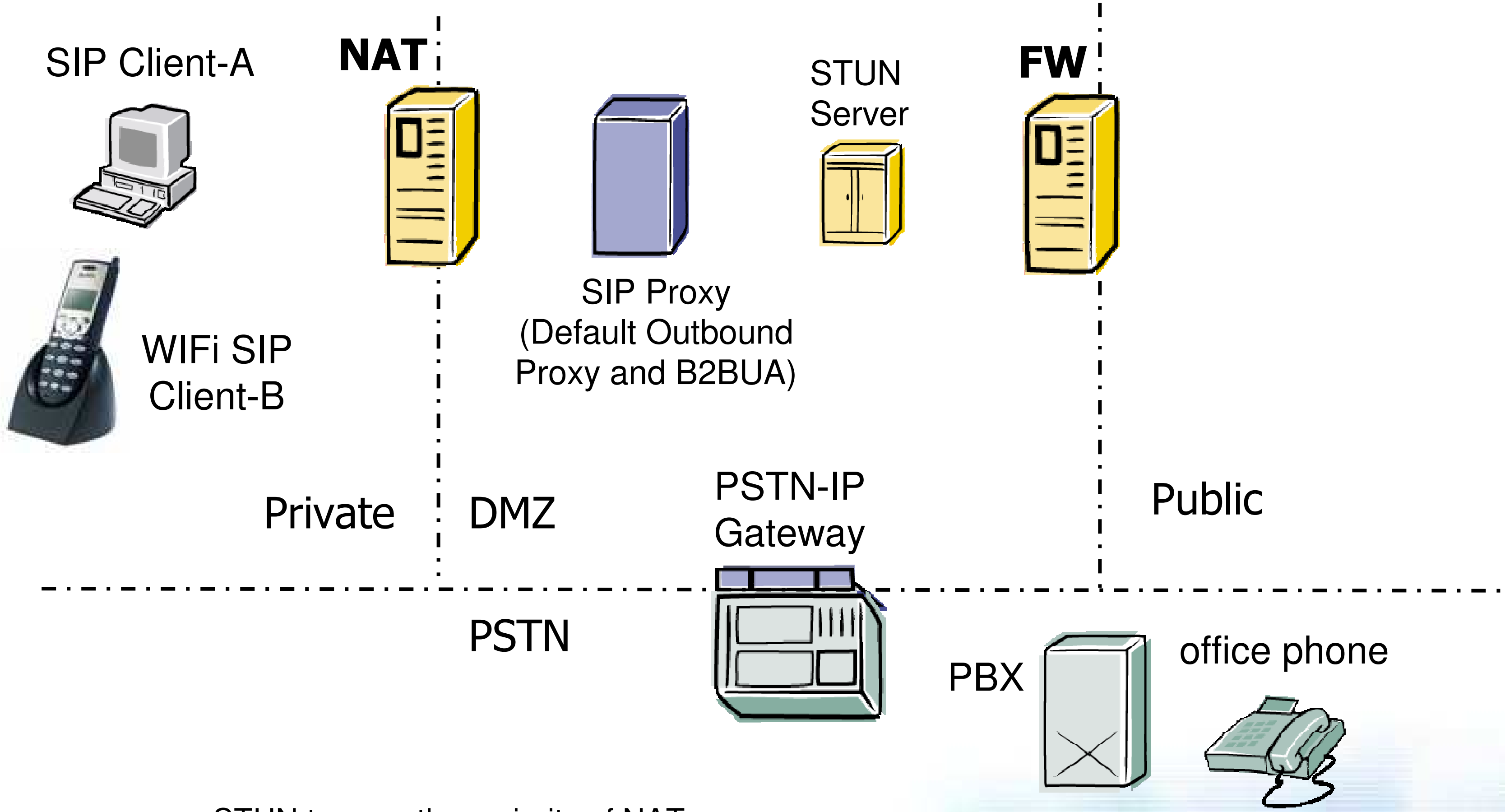


1. UA-1 sends SIP INVITE to B2BUA (default outbound proxy)
2. B2BUA modifies the SIP INVITE in order to be inserted in future messages related to this call (man-in-the-middle attack)
3. Modified SIP INVITE goes to SIP UA-2 (pinhole has been kept open by B2BUA or by SIP Proxy)
   On 200 OK, B2BUA applies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

Empowered by Innovation NEC

© NEC Corporation 2005

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)

© NEC Corporation 2005

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

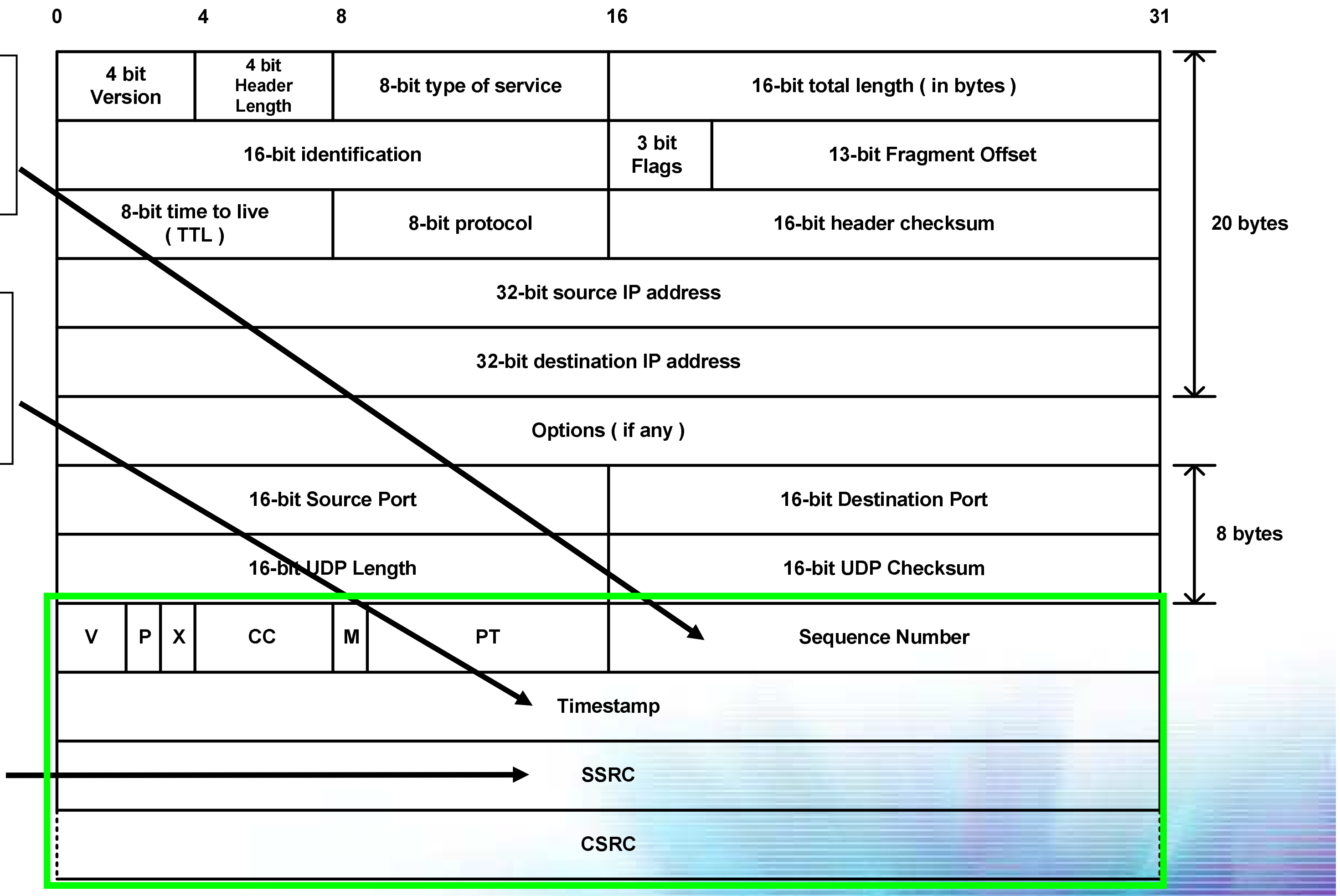
© NEC Corporation 2005

Media Transport: RTP

Used by a receiver to detect packet loss (also can be used to restore packet sequence).

Indicates the instant at which the first byte in the RTP payload was generated. The timestamp is used to place RTP packets in a correct timing order

Identifies the source of an RTP stream



Empowered by Innovation NEC

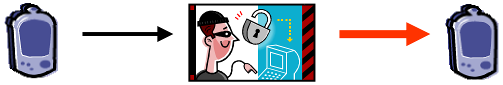
Media Transport: RTP Security Issues

- 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

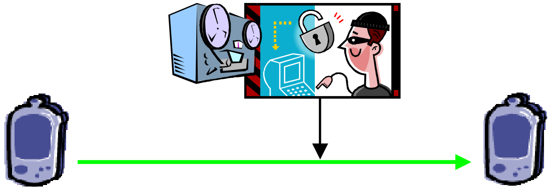
© NEC Corporation 2005

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

Empowered by Innovation NEC

© NEC Corporation 2005

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)

© NEC Corporation 2005

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

© NEC Corporation 2005

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)

© NEC Corporation 2005

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

Empowered by Innovation NEC

© NEC Corporation 2005

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)

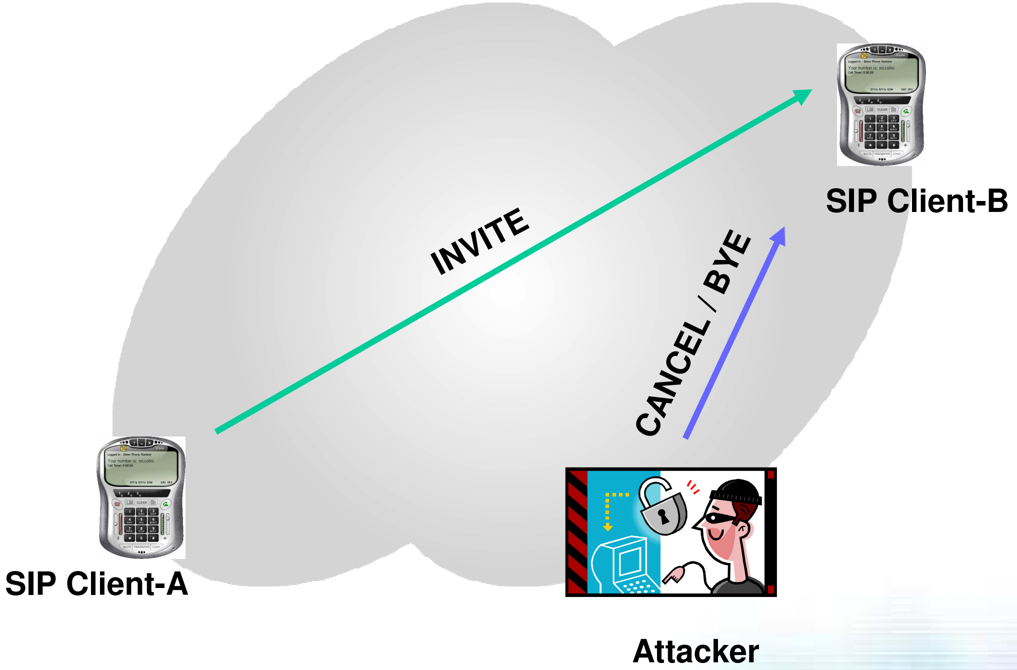
- Using SIP CANCEL message
  - preventing UAs from making and receiving calls
  - making UAs drop the call

- Using SIP BYE message
  - making UAs drop the call

© NEC Corporation 2005

Internet Telephony Security: DoS attacks

- Preventing SIP Client-A from making call



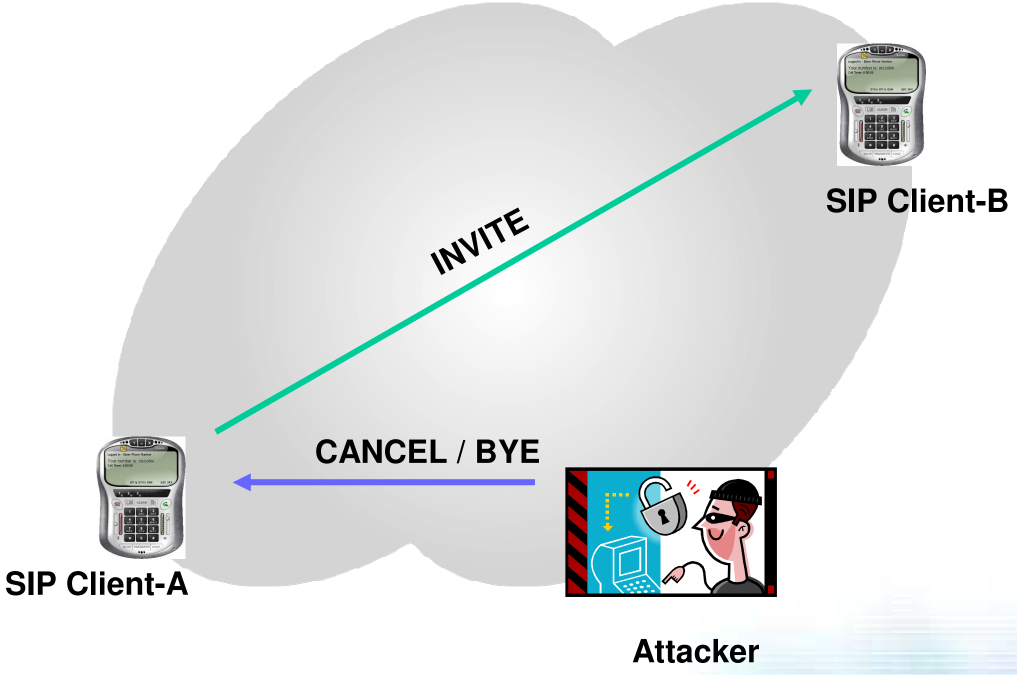
- The attacker messages cancel a pending request with the same Call-ID, TO, From, and Cseq fields

Empowered by Innovation NEC

© NEC Corporation 2005

Internet Telephony Security: DoS attacks

- SIP Client-A drops the call just initiated

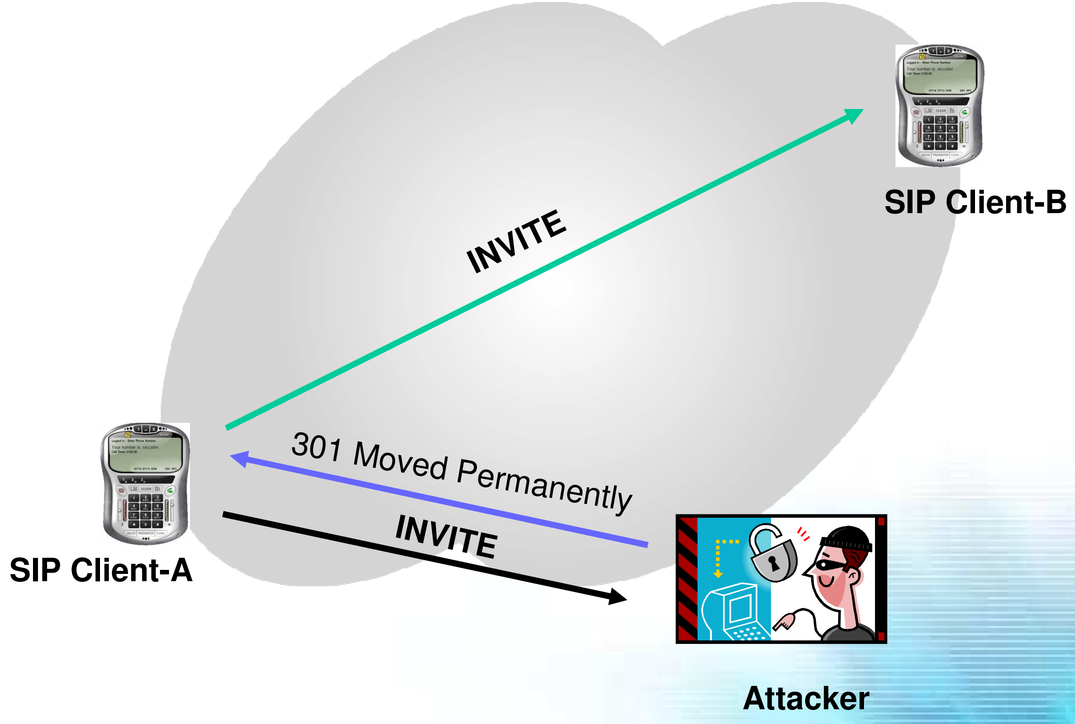


- The attacker messages cancel a pending request with the same Call-ID, TO, From, and Cseq fields

© NEC Corporation 2005

Internet Telephony Security: Threats

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

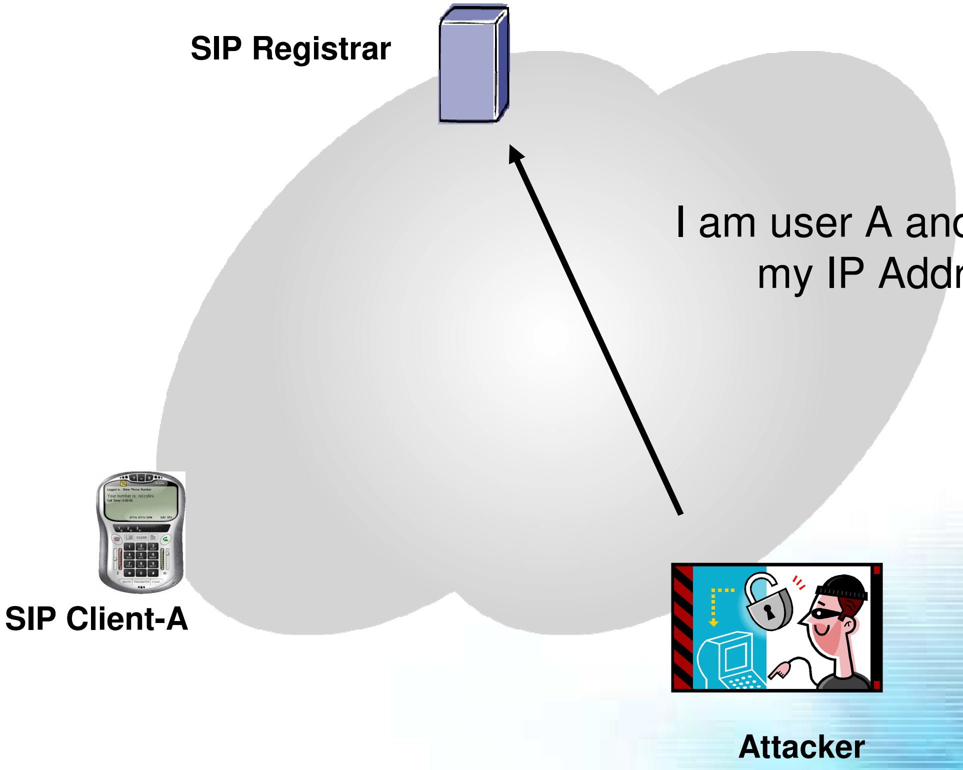


Empowered by Innovation NEC

© NEC Corporation 2005

Internet Telephony Security: Threats

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

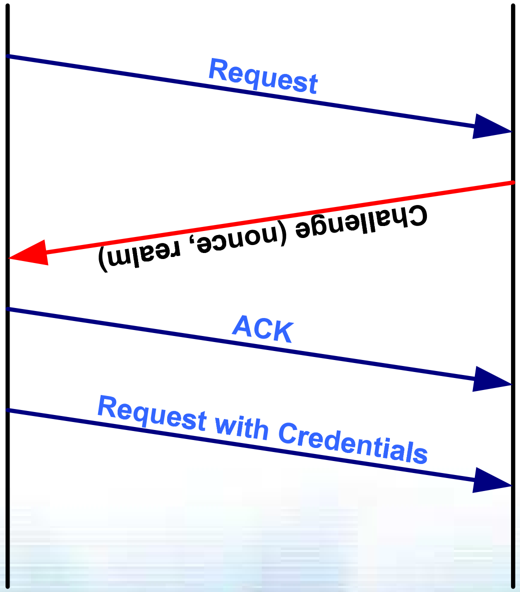


Empowered by Innovation NEC

© NEC Corporation 2005

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)



Empowered by Innovation NEC

© NEC Corporation 2005

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

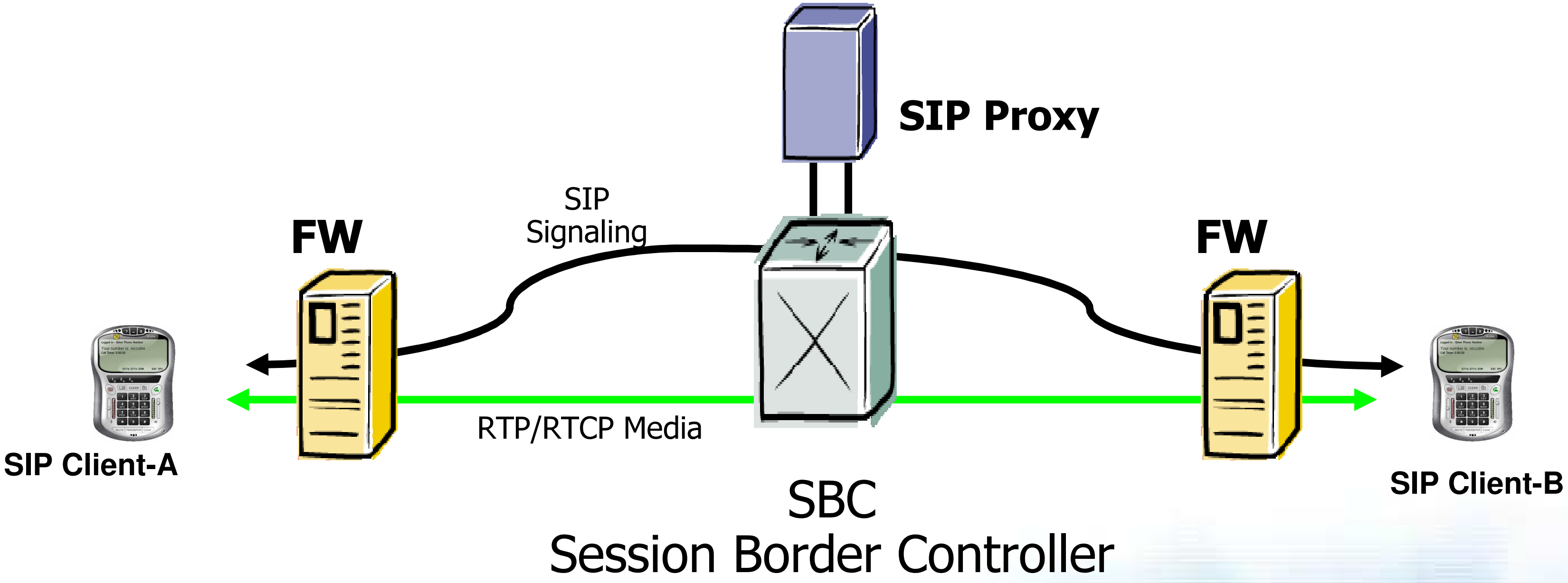
- Most E-mail filters rely on content analysis. But in voice calls, it is too late to analyze media for spamming
  - Voice Spam Detection – difficult
  - Headers for voice spam detection : “from” , “contact”. Are these enough ?
  - Detection in real time before the media arrives

- 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 Corporation 2005

NEC R&D in Internet Telephony Security



© NEC Corporation 2005

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… :-(

© NEC Corporation 2005

Special thanks

- SWITCH, The Swiss Education and Research Network (http://www.switch.ch)
  - provided some ideas about this tutorial (and material)
- GARR, The Italian Academic and Research Network (http://www.garr.it)
  - provided the infrastructure and local arrangements

© NEC Corporation 2005

Empowered by Innovation

NEC