Advanced Networking

ENUM: Migrating to VoIP

P2P Voice Applications

Renato Lo Cigno
Renato.LoCigno@disi.unitn.it

Credits for part of the original material to Saverio Niccolini NEC Heidelberg

Index

- ENUM
- P2P Basics
- Overlay & P2P
  - Does Voice Needs Servers?
  - Implications of P2P approaches
- H.323 → SIP → VoP2P (o SIP-peer?)
  - Can we have a standard P2P VoIP architecture?

What is the ENUM protocol?

- ENUM is part of a general framework whose goal is
  - **"How to find SIP services"**
- The preferred solution is DNS based: the answer tells the IP and ports associated to a SIP URI
- DNS supports two relevant records for this purpose:
  - SRV (Service) record
  - NAPTR (Naming Authority Pointer) record
- Both can be used in combination with ENUM to find SIP services

How to find SIP services?

- Services must be separated from supporting machines
- Alice uses:
  - mailserver.atlanta.com (come mail server)
  - sip-proxy.atlanta.com (come SIP server)
- Correct URIs will only change the prefix for the different services:
  - mailto:alice@atlanta.com
  - sip:alice@atlanta.com
- And not
  - mailto:alice@mailserver.atlanta.com
  - sip:alice@sip-proxy.atlanta.com
- Service loc. is given by SRV records (RFC 2782, Feb. 2000)
  - A domain name is mapped on more services and more machines
- SRV records are used to
  - Differentiate services
  - Replication/Redundancy (multiple SIP proxy)
  - backup (SIP proxy)
  - Transport protocol differentiation (UDP, TCP, TLS over TCP)

What is ENUM useful for?

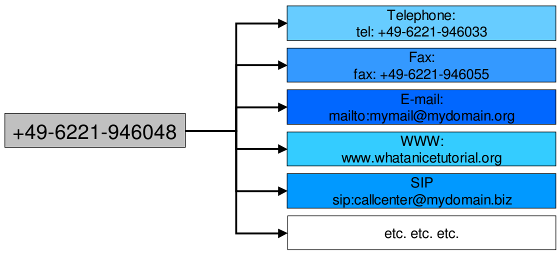
- Internet URIs:
  - mailto:saverio.niccolini@mymaildomain.org
  - sip:callme@mysipdomain.com
- E.164 telephone numbers:
  - +39 050 2217678
  - +49 6221 563423
- ENUM role is mapping the two addressing schemes
- ENUM (E.164 Number Mapping) is a standard
  - E.164 numbers are mapped on URI
  - IETF RFC 3761, Apr. 2004
    - The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)

ENUM basics

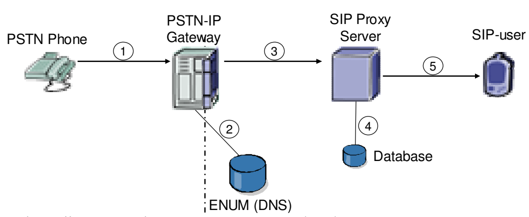
- Start from the plain number
  - +44-207-9460-148 → 442079460148
- Dot-separate numbers
  - 442079460148 → 4.4.2.0.7.9.4.6.0.1.4.8
- Reverse the order
  - 4.4.2.0.7.9.4.6.0.1.4.8 → 8.4.1.0.6.4.9.7.0.2.4.4
- Add ".e164.arpa"
  - 8.4.1.0.6.4.9.7.0.2.4.4 → 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa
- 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa is now the DNS entry of the original number
- The DNS entry is used to ask the NAPTR record and SRV records to the DNS service and realize the proper final mapping

ENUM: from a number to a set of services

- ENUM can associate to a single number multiple URI based on the actual service required



ENUM example: from PSTN toa SIP



1. The call wueries the PSTN-IP Gateway (GW)
2. GW searches the ENUM records on DNS and gets the SIP URI of the callee
3. GW forwarde the call to the SIP Proxy Server
4. The SIP Proxy server find the actual location of the callee
5. The call is forwarded to the user

Advanced Networking

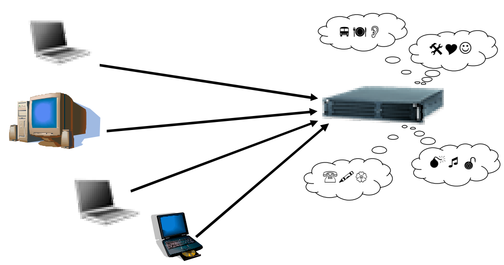
P2P VoIP

What is Peer-to-Peer (not specific to VoIP)?

- Peer-to-Peer (P2P) paradigm
  - Fundamentally different than client server
  - Nodes cooperate with each other
    - to provide (collectively) the functionality a central server would provide
  - Not all nodes provide all services/know everything, but as a group they do

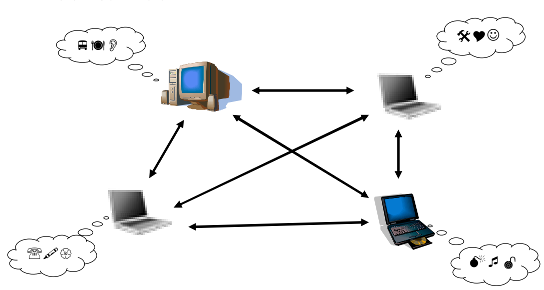
What is Peer-to-Peer (not specific to VoIP)?

Client-Server

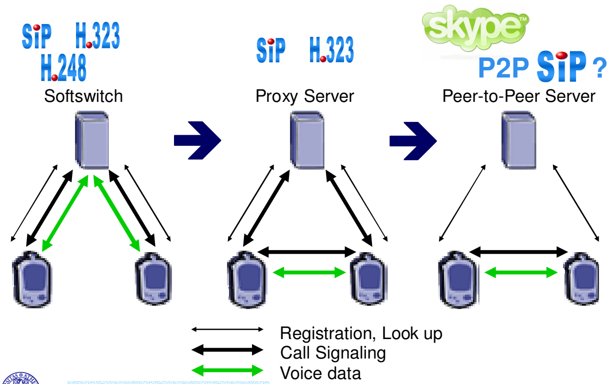


What is Peer-to-Peer (not specific to VoIP)?

Peer-to-Peer



Towards VoIP P2P: Evolution



Why P2P?

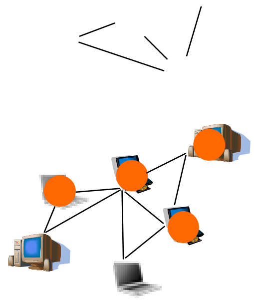
- **Infrastructure independence**
  - **No central servers (up to a a certain limit)**
  - **Don't need direct connectivity (up to a certain limit)**
- **Simple discovery and setup**
- **Privacy**
- **Highly scalable**
- **Lack of central control**
- **Dynamic DNS doesn't offer all of this**

P2P Basics

- Most ~~famous~~ infamous use of P2P is file sharing
  - Each user stores some number of files on the network, ask peers for the file
- Can also share other resources or services, no need to be files
- Connected to each other in a logical network called an overlay

Overlay Network

- Collection of nodes, connected logically in some way
- The connections in the overlay are frequently not related to those in the physical network



Renato.LoCigno@disi.unitn.it

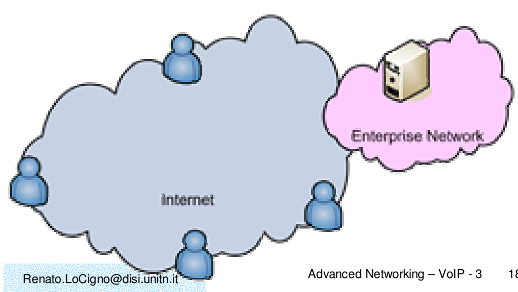
Motivating Cases

- Small deployments
  - Distributed remote office solutions
    - different from centralized VPN
  - Better enforcement of security
  - Lack of resources
- Limited/No Internet connectivity
- Ad-Hoc groups
- Censorship or impeded access
- Large scale decentralized communications
  - Skype (sort of)

Renato.LoCigno@disi.unitn.it

Distributed remote office solutions

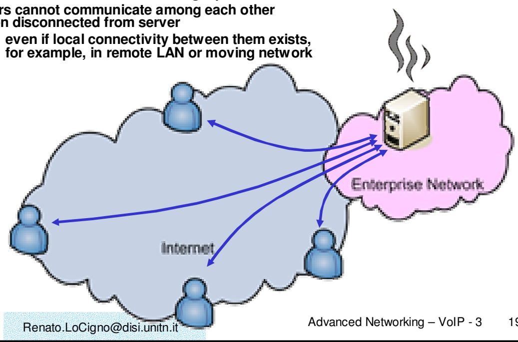
- Road warriors need virtual office network
- Collaborative network between employees
- Employees need access to company data as well



Renato.LoCigno@disi.unitn.it

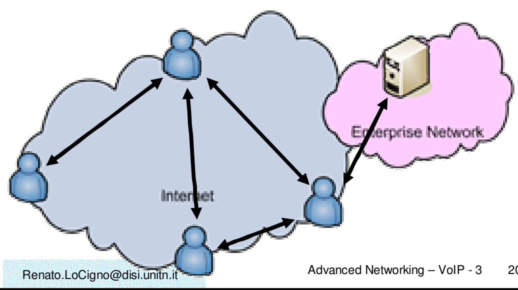
Background: Conventional VPN

- Provides private and secure connections over the public network.
- All users connect to this server: server is data hub.
- Server is bottleneck, server is single point of failure.
- Users cannot communicate among each other when disconnected from server
  - even if local connectivity between them exists, for example, in remote LAN or moving network

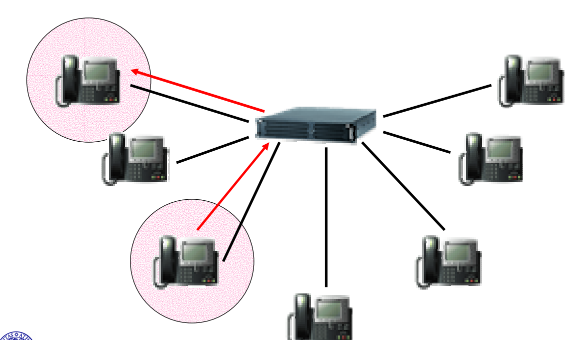


Background: Peer-To-Peer Networks

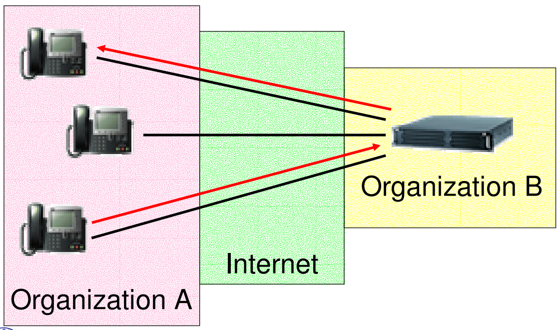
- flexible network
- no data hub



Client-Server Session



Problem with Remote Server



VoP2P Standardization

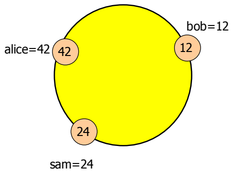
- SIP is already compatible with the P2P paradigm
  - need to substitute the register and proxy servers with distributed functions and data bases
- There are several proposals
  - If the idea is a winner … some of them will survive

SIPeer

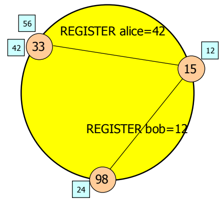
- Goals
  - Progetto P2P basato sulle primitive SIP
  - Nessuna necessità di configurazione
  - Audio conferenza e messaggistica
  - Interoperabile con i sistemi SIP esistenti
- In qualche modo si può dire ispirato a Skype
- Uso di sistemi di ricerca distribuita esistenti DHT (Distributed Hash Tables)
  - Key=hash(user@domain)

User Search: Examples

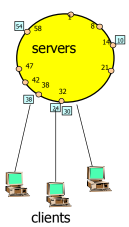
- No "REGISTER"
  - Compute a key based on the user ID
  - Nodes are connected to the P2P overlay based on the User ID
  - One node ⇔ One user



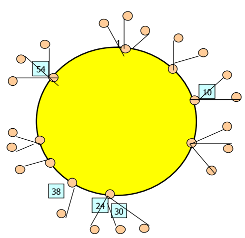
With "REGISTER"
- The user REGISTERs with nodes that handles his key
- Need periodic refreshing
- Enable off-line services (voice-mail, messaging, …)



Several design alternatives



Mixed models with servers handling DHTs



Hierarchical supernodes a-la-skype

P2P real-time: Users perspective

- **Ease of usage**
- **No user configuration required**
- **Working across all networking environments**
  - **Network Address Translators (NATs)**
  - **Firewalls (FWs)**
- **P2P real-time applications are not standard-based but they "just work"**
- **Different user experience with respect to standard-based real-time applications**
  - **e.g. H.323-based or SIP-based**

Identification of issues with P2P SIP

- Goal
  - Identify potential issues of SIP-based P2P communication related to Middleboxes (NAT and firewall) traversal
    - to be considered when designing standards for a SIP-based P2P infrastructure
- Non-Goals
  - Constrain a future P2P SIP architecture in any way
  - Still we need to list potential communication steps that might raise issues
  - Those steps are not necessary part of the final SIP-based P2P solution
  - Suggest NAT traversal methods to be selected for P2P solution

Potential Communication Steps

- Steps considered
  - middlebox detection
  - registration
  - search for relays
  - address lookup
  - call setup
  - call termination
- Not all steps might be necessary
- Several steps may be combined into one

Middlebox Detection

- Detect Middleboxes
  - on the signaling path
  - on the data path
- Communication means detection for
  - registration
  - incoming / outgoing signaling
  - data streaming to and from other terminals or relays
- Checks to be performed
  - sending and receiving UDP packets
  - opening incoming and outgoing TCP connections
  - use of certain fixed port numbers
  - the option to relay or tunnel signaling messages and streamed data
- NAT parameter detection
  - full cone, half cone, etc…

Registration

- Authentication of the user
- Notification of communication capability and willingness
- Registration of contact parameters
- Notification of service provisioning capability and willingness

Further Steps

- Search and Connect Relay
  - Candidate relays may be suggested by infrastructure
- Address Lookup
  - Per-call lookup
  - Buddy list lookup
- Connection Establishment and Termination

Middlebox Traversal Methods

- Tunneling
  - in highly restricted environments only
  - controversial:
    - HTTP and DNS tunneling are not legitimate
    - TURN could be OK
- Network-initiated Middlebox Signaling
  - not the right choice for P2P SIP
- Terminal-initiated Middlebox Signaling
  - several methods known

Terminal-initiated Middlebox Signaling

- Standards
  - STUN (IETF RFC3489)
  - UPnP (UPnP Forum)
  - SOCKS (IETF RFC 1928)
  - RSIP (IETF RFC 3103)
- Under development
  - STUN update (IETF behave WG)
  - ICE (IETF mmusic WG)
  - NSIS (IETF nsis WG)
- Middlebox traversal using relays
  - STUN relay (previously TURN) (IETF mmusic WG)

Open Issues for SIP-based P2P

- SIP-unrelated
  - middlebox detection beyond UDP
- SIP-related
  - terminal reachability
  - communication service requirements
  - communication service offers
- The relevance of these issues strongly depends on the choice of P2P architecture

Middlebox Detection Beyond UDP

- Limited or no middlebox detection for TCP and DCCP (Datagram Congestion Control Protocol) available
  - Middlebox signaling for TCP is covered by UPnP, SOCKS, RSIP, NSIS
- TCP considered for signaling and for data
  - Several SIP-signaled services use TCP
  - RTP over TCP used when UDP is blocked
- Might get solved partially by ICE TCP
  - still in early state

Terminal Reachability

- Relevance depends on registration and relay detection process
- Terminal might need to register first and then find and connect to a relay in order to be reachable
- In between these two steps it would be reachable for signaling but unreachable for data transmission and should be registered as such
- Currently, the SIP protocol does not provide explicit means for signaling such a state

Communication Service Requirement

- The terminal might need to express its needs for relaying
  - signaling messages
  - lookup requests
  - data streams
- Infrastructure nodes might need to suggest relays to be used by terminal
- For both, request and suggestion, signaling means are required
  - Extension Header Field for Service Route Discovery During Registration (RFC 3608) might offer means

Communication Service Offering

- A terminal in an unrestricted (or just slightly restricted) environment might be able (and the user willing) to offer services to other peers, such as relay services and lookup services
- Currently, the SIP protocol does not provide explicit means for signaling such offers

P2P SIP: how to locate peers?

- Basic idea is that what you are looking for has an identifier
  - Locate items in the overlay based on the identifier
  - Distributed Hash Table (DHT), Content Addressable Networks (CAN)
  - Since "everything has its place", eliminate false negatives
  - Since you can go (close to) directly to the item you want, more efficient

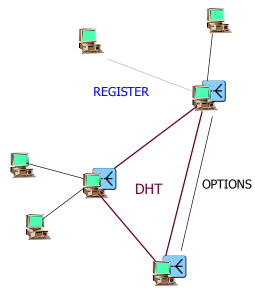
Applying this to SIP

- Use pure Distributed Hash Tables (DHT) to find the other UAs
  - Problems
    - currently no DHT standardized
    - some firewalls block DHT traffic as "file sharing"
- Use DHT for location, but implemented as SIP messages
  - Essentially, use DHT as another registration/location mechanism
- Use standard SIP to signal once resources are located

Problems with P2P SIP

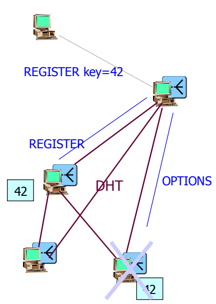
- Like most things SIP, NATs
  - Same problems, plus some new ones
  - Super nodes?
- Security
  - Sybil attacks
  - DoS (through traffic and true denial)
  - Encryption
  - Information "leakage"
  - Choosing node locations to divert/block

Node joining



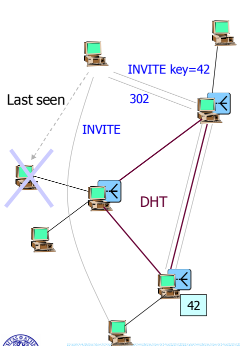
- Supernodes are registrar SIP
  ```
  REGISTER sip:node-address
  To: <sip:user@domain>
  ```
- Periodically control existing peers (as in any P2P system)
- Register imply insertion in the DHT for search
- Multiple state possible for users
- Simple multi-location management (as in skype)

Nodes leaving



- "Gentle" leave is useful:
  - Un-REGISTER
- Simple nodes do not pose problems
- A supernode leaving implies that
  - Connected nodes must re-REGISTER with another supernode
  - The new REGISTRAR must go to other supernodes (delete the leavign supernode from the DHT)
  - Supernodes must promptly update the DHT for presence and leaving

Call handling



- Valid for telephone, messaging, etc.
  ```
  INVITE sip:locigno@unitn.it
  MESSAGE sip:sergio.rossi@yahoo.com
  ```
- If the callee is in the buddy list communication can be direct
- Otherwise
  - lookup basato su SIP (DNS NAPTR, SRV,…)
  - lookup P2P
    - The caller send the INVITE to a supernode
    - Supernodes will use a DHT or similar distributed system to identify the callee position with high probability

Off-line services (messages, voice mails, …)

- The INVITE or MESSAGE fails
  - Supernodes memorize the message/call for later retrieval
  - Messagges/calls should be replicated to improve reliability
- Open Issues
  - Security and Trust + Privacy (is it worse than a centralized service?)
  - Guarantee that at least one copy of the information is maintained until the user has accessed it (cfr. Mail/SMS)