An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol

Matthias Wiech
Skype Network

Message exchange with the login server during login

- Ordinary host
- Super node
- Neighbour relationships in the Skype network
Key Components

• **Ports**: randomly selected port + port 80 (HTTP) + port 443 (HTTPS)
• **Host Cache**: list of supernode IP addresses and ports
• **Alternate Node Table**: list of nodes to connect to when supernode becomes unavailable
• **Codecs**: wideband codec at 32 kb/s
• **Buddy List**: encrypted list of contacts
• **Encryption**: AES 256 bit, RSA1536-2048 bit
• **NAT and Firewall**: ...
The NAT Problem

Host X cannot send packages to host Y because host Y's IP address is unknown to host X (and vice versa)!
The NAT Solution

LAN 1
192.168.0.0 192.168.0.1
192.168.0.2 192.168.0.3
Host X

NAT A
20.20.20.20
(supernode)

NAT B
30.30.30.30

LAN 2
192.168.0.0 192.168.0.1
192.168.0.2 192.168.0.3
Host Y

40.40.40.40

(supernode) acts as STUN-Server

http://www.skype.com/products/explained.html

“Non-firewalled clients and clients on publicly routable IP addresses are able to help NAT’ed nodes to communicate by routing calls.”
Login Process

1) establish TCP connection to **skype.com (Port 80)** //check for updates

2) for each node in **host cache** do:
   
   ```
   try: UPD connection on **user port**. if OK goto success.
   try: TCP connection on **user port**. if OK goto success.
   try: TCP connection on **port 80** (HTTP) if OK goto success.
   try: TCP connection on **port 443** (HTTPS) if OK goto success.
   ```

   success: ...

3) authenticate at **login server** //challenge-response
User Search

- distributed search
- guaranteed to find a user if it exists and has logged in during the last 72 hours.

http://www.skype.com/products/explained.html

The Global Index technology is a multi-tiered network where supernodes communicate in such a way that every node in the network has full knowledge of all available users and resources with minimal latency.