Skype

Une solution de VoIP à l'échelle mondiale
10 mars 2005

Didier Benza

INRIA
SOPHIA ANTIPOLIS

Skype - Plan

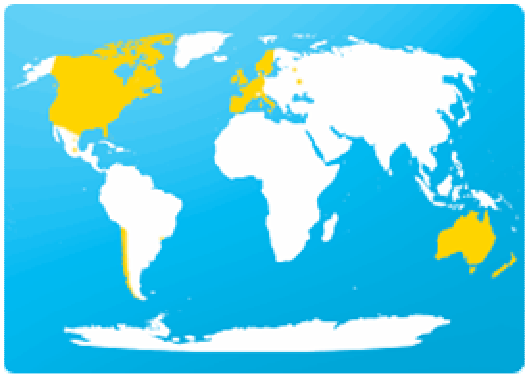
- Présentation de l'outil
- Fonctionnement technique
- Avantages
- Inconvénients
- Sécurité

Skype - Présentation

- Logiciel de téléphonie sur Internet
  - 68 Millions de téléchargement dans les 18 derniers mois
  - 25 millions d'utilisateurs dans le monde
  - Communication gratuite entre deux postes Skype
  - Communication payante entre un poste Skype et un abonné de téléphone
- Fonctionne en mode P2P
- Créé par les concepteurs de Kazaa[3]

Skype –SkypeOut

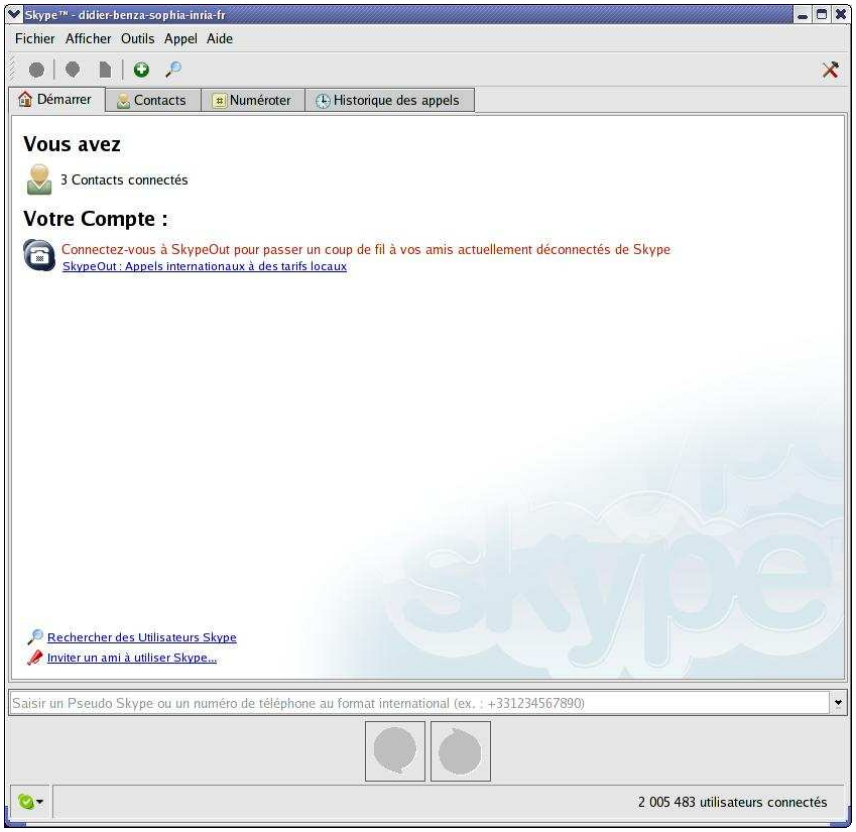
- Prix de 0,017 € HT/minute pour les destinations très fréquentes
- Prix allant jusqu'à 1,17 € HT/minute pour le Timor Oriental
- Exemple 0,022 € HT/minute pour Chine et Chine mobile



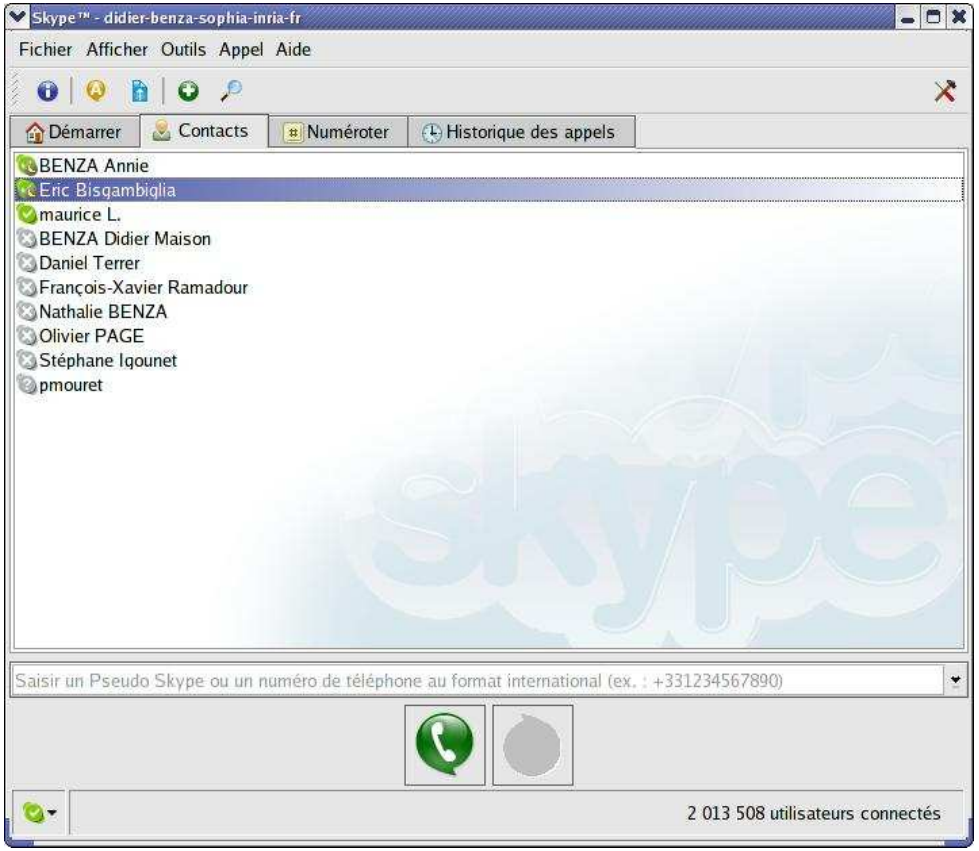
Skype - Présentation

- Communication cryptée de bout en bout
- Chat avec <= 50 personnes
- Conférence audio <= 5 personnes
- Transfert de fichier direct

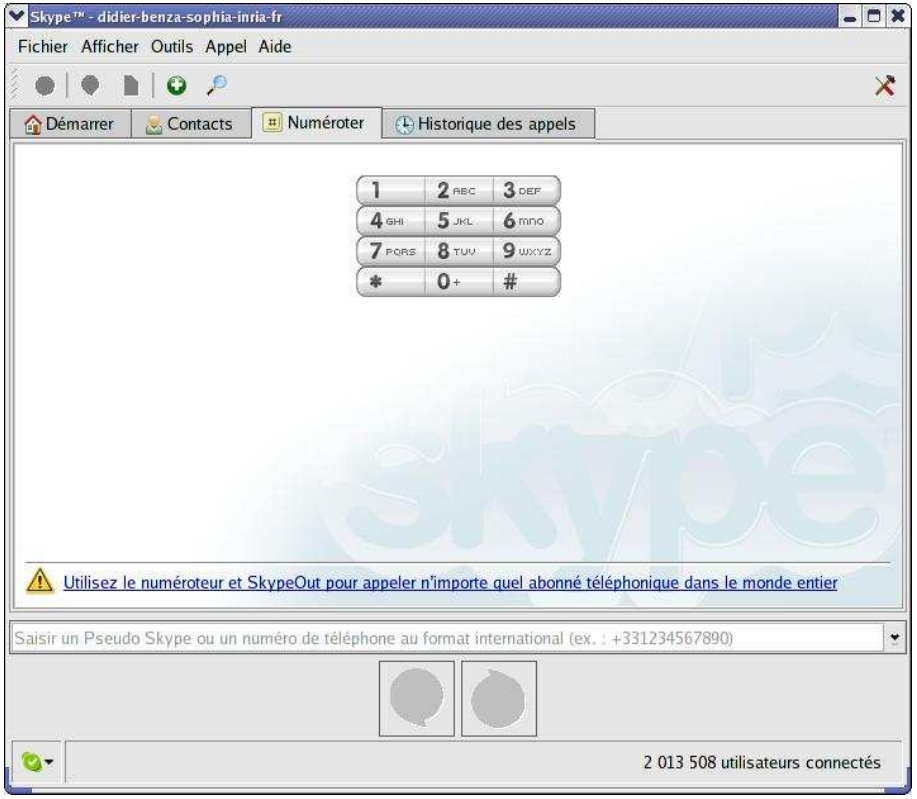
Skype - Présentation



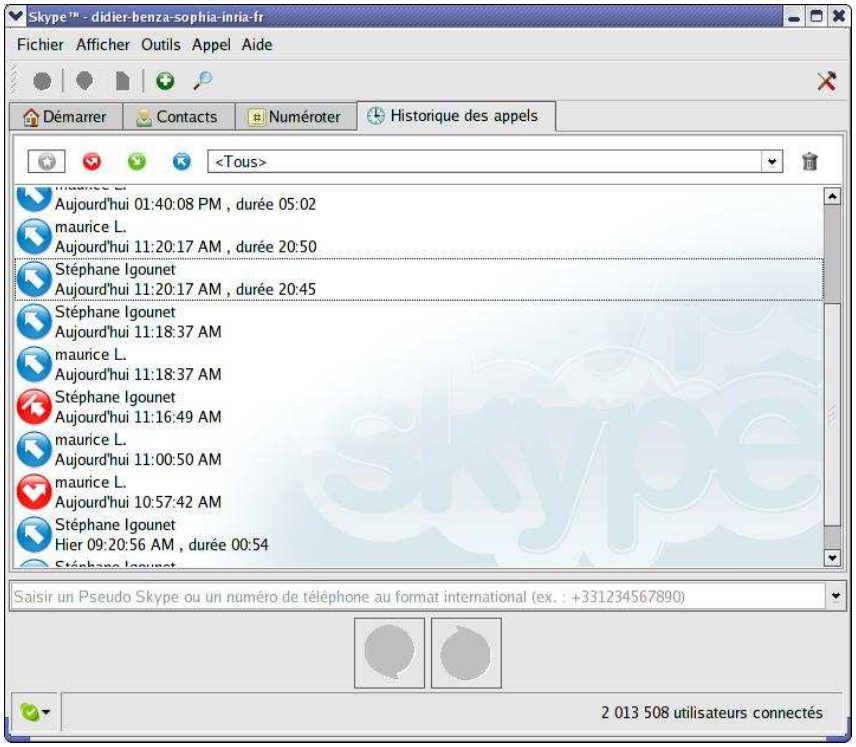
Skype - Présentation



Skype - Présentation

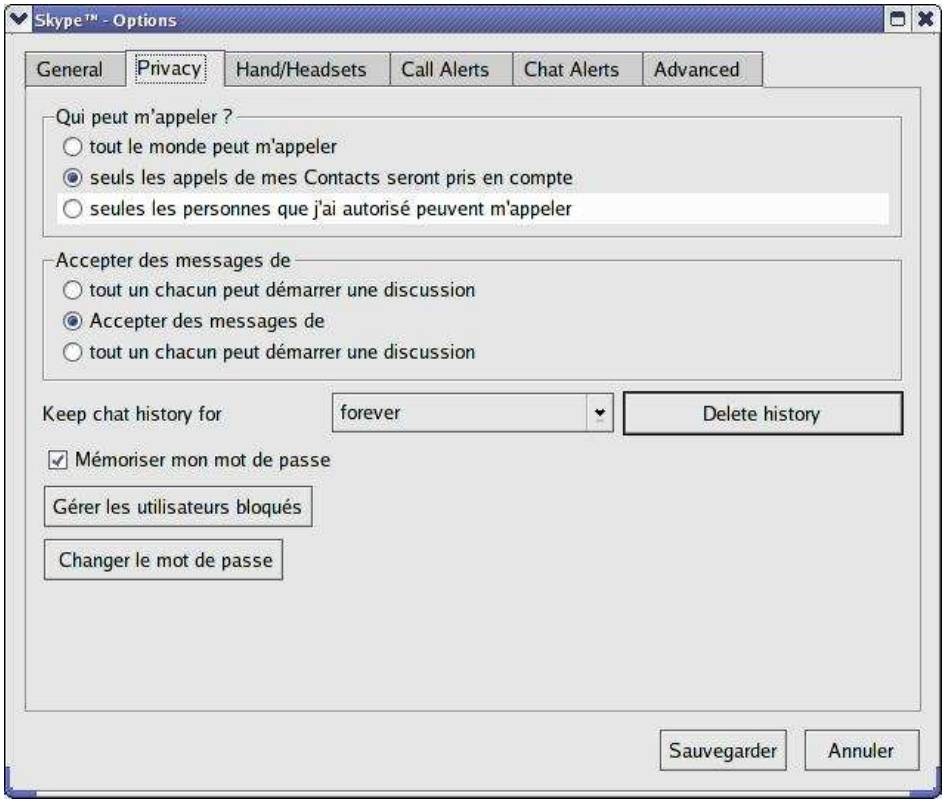


Skype - Présentation



INRIA
SOPHIA ANTIPOLIS

Skype - Présentation



Skype – Notion de contact

- Skype utilise la notion de *contact*
- On peut ajouter quelqu'un à sa liste de contact :
  - On sait quand il est connecté et s'il accepte d'être contacté
  - Il faut que la personne accepte d'être ajoutée à notre liste de contact (on connaît l'état connecté ou non de ses contacts)

Skype – Notion d'état

- On peut choisir d'apparaître à nos contacts dans un état donné

Skype - Conférence

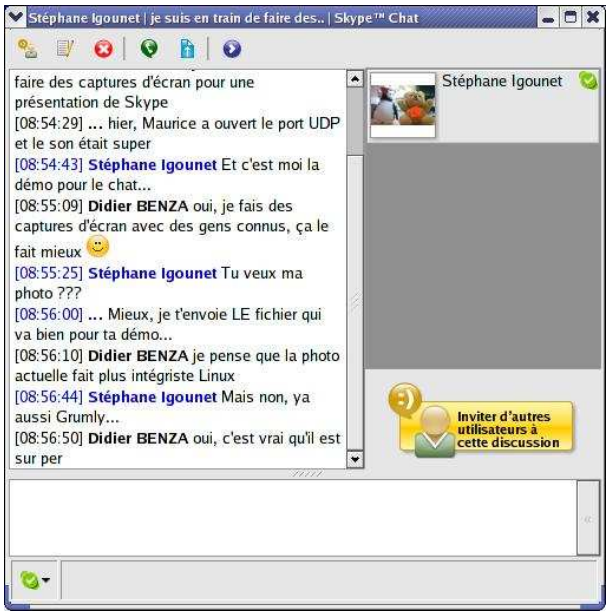
- Possibilité de créer une conférence <= 5 en quelques instants

Skype – Choix communication

- Le choix de communication avec un contact est le suivant :
  - Appel
  - Chat
  - Envoyer des contacts
  - Envoyer des fichiers

Skype - Chat

- Possible de faite du chat <= 50



Skype – Transfert de fichier

- Il est possible de transférer des fichiers de poste à poste :

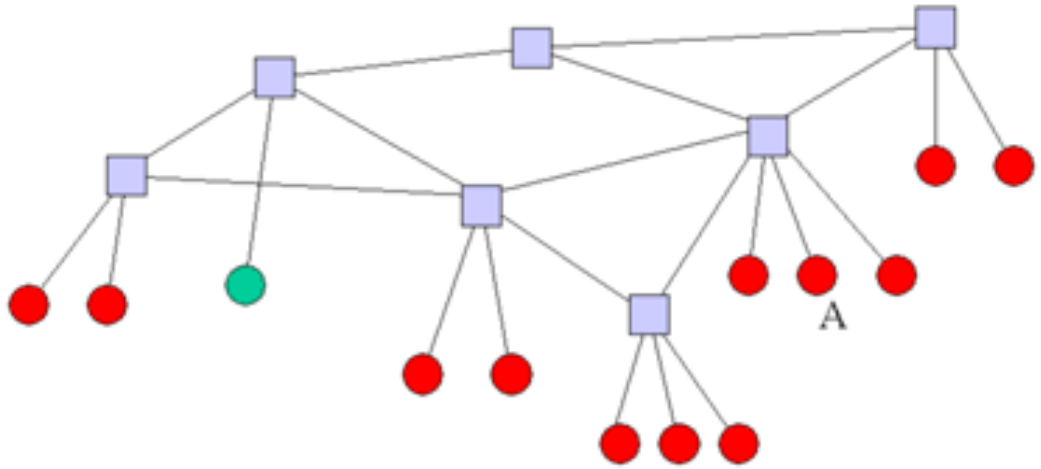
Skype - Technique

- Skype est une application fermée. Tout ce qui suit est déduit de l'observation du comportement réseau et des informations qui filtrent de la société
- Skype est une application P2P
- Chaque nœud Skype est classé dans l'une des deux catégories suivantes :
  - Node
  - Supernode (SN)
- Un SN est choisi pour des raisons d'accessibilité, de performance CPU, de bande passante

Skype - Technique

- On ne contrôle pas qui devient un SN
- Les bandes passantes disponibles sur nos sites nous rendent elligibles à devenir des SN
- Pas vrai en fonction des règles de sécurité (en fonction des ports bloqués)

Skype – Technique



[8]

Skype - Technique

- On pense que Skype implémente une variante de STUN[2] (Simple Traversal of User Datagram Protocol Through NAT, RFC 3489) et TURN (Traversal Using Relay NAT, draft-rosenberg-midcom-turn-03)
- Pas de serveur Firewall Traversal (pas de capture de trafic vers un serveur unique)
- Pour se connecter au réseau Skype un Client Skype (CS) doit se connecter sur un SN
- Le login+password est contrôlé par un serveur central (peut-être le point faible de la topologie Skype)

Skype - Technique

- Le CS attend des connexions entrantes sur un numéro choisi aléatoirement à l'installation, en TCP et UDP
- Il écoute aussi sur les ports 80 et 443
- Pas de port d'écoute par défaut
- A l'installation un CS connaît une liste de well-known hosts, des SNs. L'un d'eux au moins doit être up pour que le CS puisse se connecter. Après connexion, il construit au fur et à mesure une liste complémentaire de SN (limitée à 200)

Skype - Technique

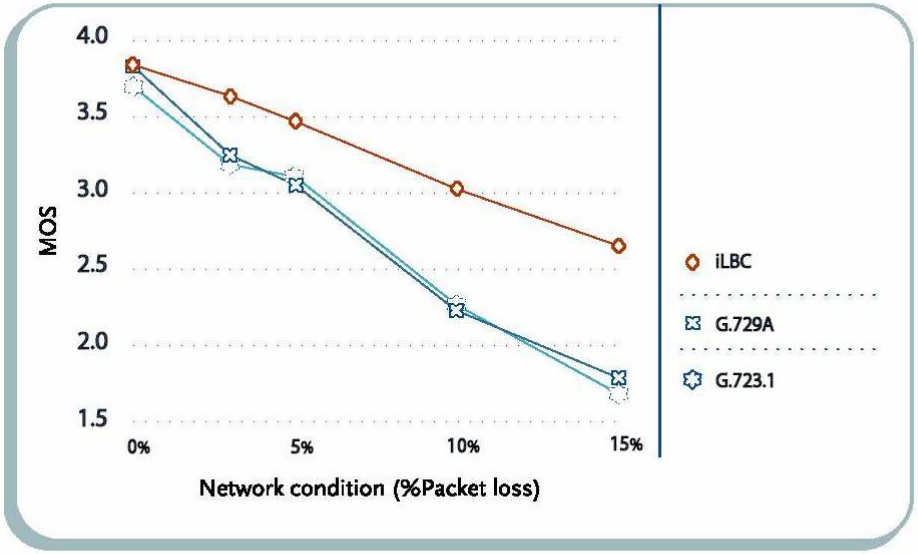
- Au démarrage un CS tente des connexions UDP sur des SN du Host Cache qu'il a construit ou hérité.
- S'il n'obtient pas de réponse au bout de 5 sec, il tente des connexions TCP sur le port 80
- S'il n'obtient pas de réponse au bout de 6 sec, il tente des connexions TCP sur le port 443
- Si ça ne fonctionne pas, il réessaie 4 fois
- Si un proxy est configuré (IE ou Opera ou http_proxy), Skype passe par le proxy
- Certains SN sont utilisés à la toute première connexion après installation et tentative de connexion : des bootstrap SN
- La connexion TCP avec le SN est maintenue pendant toute la durée d'exécution du CS

Skype – Technique Audio

- Skype utilise principalement deux codecs [4]
  - iLBC RFC3951 et RFC3952 (premier codec normalisé IETF)
    - Qualité meilleure que G.729 et G723.1(H324)
    - Robuste à la perte de paquets par rapport à G.729A, G.729E, G.723.1 et G.728
    - Qualité identique à G.729E, mais plus résistant
    - Fonctionne à 13.3 Kbits/s ou 15.2 Kbits/s
    - Libre de droits (code C téléchargeable sur serveur IETF)

Skype – Technique Audio

iLBC offers substantially better quality than G.729A and G.723.1.



Tests were performed by Dynastat, Inc., an independent test laboratory.
Score system range: 1 = bad, 2 = poor, 3 = fair, 4 = good, 5 = excellent.

Skype – Technique Audio

- Autre Codec :
  - iSAC
    - Débit entre 10 Kbits/s -> 32 Kbits/s
    - Robuste à la perte de paquets
    - Echantilonnage 16 KHz
    - Bande passante audio 8 KHz
    - Complexité comparable à G722.2, meilleure au même taux d'échantillonage

Skype – Technique Audio

- Des expérimentations [1][5] montrent que sans stress en BW la bande passante audio des codecs utilisés par Skype va de 50 Hz à 8 KHz
- Avec Net Peeker [6] la BW up/down est réduite à 1,5 Ko/s (12 Kbits/s), les fréquences audibles restent inchangées
- En dessous de 2 Ko/s (16 Kbits/s) up et down la qualité devient très dégradé. En dessous de 1,5 Ko/s la voix devient inintelligible

Skype – Technique Audio

- Pas de technique de suppression du silence
  - Evite les coupures désagréables à l'oreille
  - A des avantages réseau :
    - Maintient de la traduction active sur un routeur NAT
    - Laisse la fenêtre TCP a la taille qui a déjà été calculée afin d'éviter de prendre du RTT pour atteindre le maximum de nouveau
- En cas d'appel mis en attente, il y a quand même du trafic (faible) entre les CS (probablement pour les mêmes raisons que ci-dessus)

Skype – Technique - Recherche

- Skype annonce que la recherche est distribuée avec la technologie Gobal Index
- La recherche doit trouver quelqu'un qui s'est connecté dans les dernières 72 heures
- Le protocole étant propriétaire, on ne peut que s'appuyer sur des captures de paquets pour voir ce que le CS fait
  - Lorsqu'on lance la recherche, il y a un échange entre le CS et son SN qui lui communique 4 IP/Ports de SN à interroger, ce que fait le CS
  - Si c'est infructueux, le CS informe son SN qui lui donne 8 autres adresses de SN à interroger et ainsi de suite. On ne sait pas comment le CS détermine que le login ne peut être trouvé
  - Dans le cas d'un CS derrière un FW, c'est le SN qui fait la recherche
  - On a déterminé que le résultat de la recherche est mis dans un cache sur le SN

Skype – Technique - Appel

- La signalisation est toujours transmise sur TCP
- La durée de l'appel, si appel de quelqu'un qui n'est pas dans la liste des contacts = Recherche + Signalisation
- Appel entre deux machines avec IP publiques, sans FW = communication directe / UDP
- Appel entre deux machines dont l'une est derrière un FW / NAT => TCP ou mélange TCP et UDP avec un SN au milieu
- Le transfert de fichier obéit aux mêmes règles (UDP préféré, mais repli sur TCP possible avec un SN au milieu)
- Un utilisateur peut-être loggé sur plusieurs stations en même temps. La signalisation est transmise vers toutes les machines où il apparaît. Dès qu'il décroche sur l'une d'elle, l'appel est annulé vers les autres

Skype – Technique - Conférence

- Si les machines sont homogènes en CPU, BW et visibilité, la machine qui créée la conférence sert de *conference host* (concentration des connexions) et elle mixe et émet les flux qu'elle reçoit
- Sinon, c'est la machine la plus puissante qui est choisie comme conference host / mixer

Skype – Avantages usagers

- La prise en main par l'usager dure moins de 5 minutes, quasiment aucune configuration
- Communication Skype longue distance gratuite
- Communication téléphonique internationale à bas coût

Skype – Avantages usagers

- Qualité audio exceptionnelle
- Offre matérielle de périphériques croissante
- Accord Motorola – Skype[7] pour embarquer Skype dans les portables Motorola
- Disponible sous plusieurs OS :
  - Windows, Linux, Mac OS, Pocket PC

Skype – Avantages usagers

- VoIP longue distance qui fonctionne vraiment
- Traverse un grand nombre de FW et NAT
  - Des solutions existent avec les autres technologies (H323, SIP) mais nécessitent des investissements (GK, Pont) proches des coûts télécoms => sous-dimensionnement => mauvaise qualité
  - Avec Skype, les SNs aident les CS NATés à téléphoner

Skype – Avantages usagers

- Les communications sont cryptées
  - AES 256 bits (Rijndel), 1,1 x 10^{77} clefs possibles

Skype – Inconvénients usagers

- Pas de notion *corporate* permettant par exemple d'accepter les appels INRIA en refusant les appels provenant de contacts non identifiés
- La liste des contacts est locale pour un couple (PC, utilisateur) donné
- Nécessite des périphériques audio adaptés (casques, micro)

Skype Avantages - INRIA

- **Prix** : Skype = Voix sur IP… sur IP
  - Y compris pour les appels longue distance
  - Client gratuit
- Facilité d'installation (faible impact / services informatiques)
- Audioconférences faciles à organiser
- Pas de coût humain dans la gestion d'une infrastructure ou de serveurs
- Faible impact d'un CS sur le réseau

Skype – Inconvénients INRIA

- Pas un produit Open Source, on doit faire confiance à Skype (AES, Informations, etc…)
  - Toutes les captures effectuées concordent avec ce que Skype affirme.
  - La plupart des produits H323 ne sont pas Open Source non plus, mais norme = relative stabilité
- On ne sait pas garantir le service à l'utilisateur (pas de serveurs sous notre charge)
- Pas de visibilité vers une évolution multicast du produit

Inconvénients - INRIA

- Difficulté probable administrative / financière de gérer les crédits Skype Out
- Pas d'intervention possible en cas de panne (pas de serveurs)
- L'impact réseau en cas d'hébergement d'un SN peut être non négligeable
- On ne connaît pas l'évolution du modèle économique (gratuit… pour combien de temps ?)

Impact INRIA

- Obligation de mettre en place une règle de nommage des login, ex :
  - didier-benza-sophia-inria-fr
- Modification de l'annuaire pour ajouter des liens callto

Skype – Considération de sécurité

- La génération aléatoire du port utilisé par le CS pour les connexions entrantes (UDP/TCP) hors 80 et 443 est due à la volonté de franchir un NAT
  - Sur un site non NATé ce choix est inutile et peut être difficile à mettre en œuvre si tout UDP est filtré en entrée, par exemple
- Sur un site non NATé, on peut imposer aux CS une normalisation du port utilisé de façon à n'ouvrir qu'un port TCP/UDP au monde extérieur
  - Complexification légère de la procédure d'installation
- Sur un site IP public ou NATé la connexion du CS au réseau prend entre 3 et 7 secondes
- Sur un site UDP-filtré, la connexion prend plus de 30 sec.

Skype – Considération de sécurité

- Effet pervers : quand on filtre trop, on oblige le CS à passer par un SN au lieu d'une connexion point à point
  - On diminue la sécurité alors qu'on voulait l'augmenter
  - Même dans ce cas, *difficile* d'écouter la conversation [10]

Skype - Références

- [1] Skype conferencing White paper by PowerModeling http://www.powermodeling.com/files/whitepapers/Conference%20Test%20feb%2009.pdf
- [2] Simple Traversal of User Datagram Protocol Through NAT (RFC3489) ftp://ftp.rfc-editor.org/in-notes/rfc3489.txt
- [3] Skype P2P Explained http://www.skype.com/products/explained.html
- [4] iLBC (RFC3951 et 3952) et iSAC Codecs http://www.globalipsound.com/solutions/solutions_Codecs.php

Skype - Références

- [5] An analysis of the Skype P2P Internet Telephony Protocol http://www1.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf
- [6] Net Peeker http://www.net-peeker.com/
- [7] Motorola and Skype Form Broad Seamless Mobility Alliance http://www.motorola.com/mediacenter/news/detail/0,,5174_5168_23,00.html
- [8] Les réseaux de pair à pair http://interstices.info/display.jsp?id=c_8622
- [9] Journées GERET – P2P 25/26 mars 2004 http://webcast.in2p3.fr/geretP2P/
- [10] Can they hear you now ? http://slate.msn.com/id/2095777