VoIP

L'avenir !

Principe de base

- En mettant la voix sur IP, on fait un meilleur usage de la bande passante (on ne transmet que quand il y a vraiment quelque chose à transmettre, EN THEORIE (parce qu'en pratique...))
- En pratique on transmet en permanence le flux voix (petits paquets à intervalle régulier)
- Problème: le jitter introduit par les réseaux IP est insupportable pour les flux voix
- Nécessite QoS (en théorie)
- C’est une application !

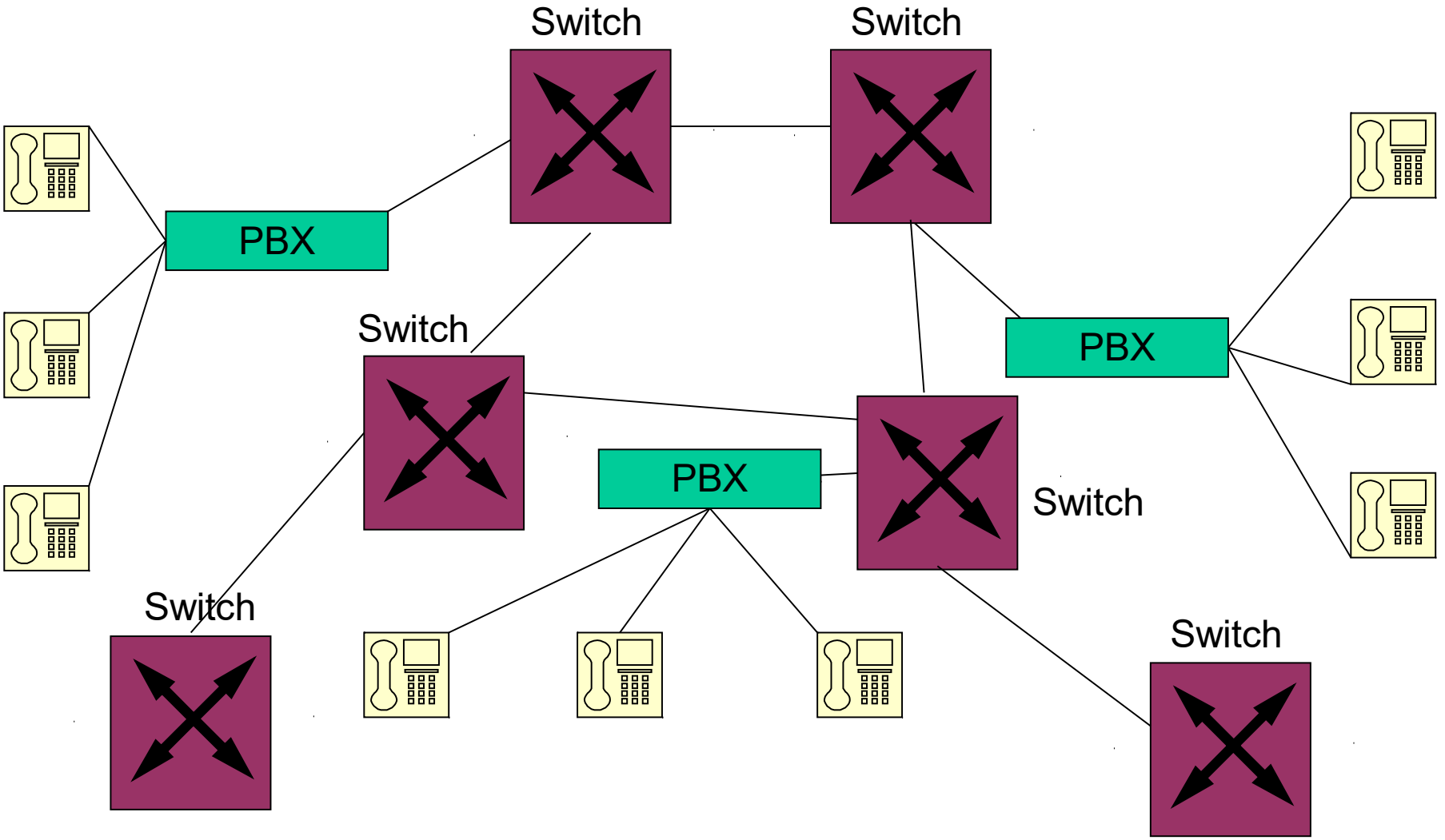
Architecture – 1

- Architecture générale basée sur:
  - Gateway (attention, il y a Gateway et Gateway !)
  - Gatekeeper (optionnel)
  - POTS (PSTN)
  - IP Phones ou ATA ou ‘Soft Phone’ ou téléphones (PSTN) ou terminaux...
  - Accès à l’Internet côté serveur (cloud) !
  - Accès à l’Internet côté client (centrale virtuelle) !

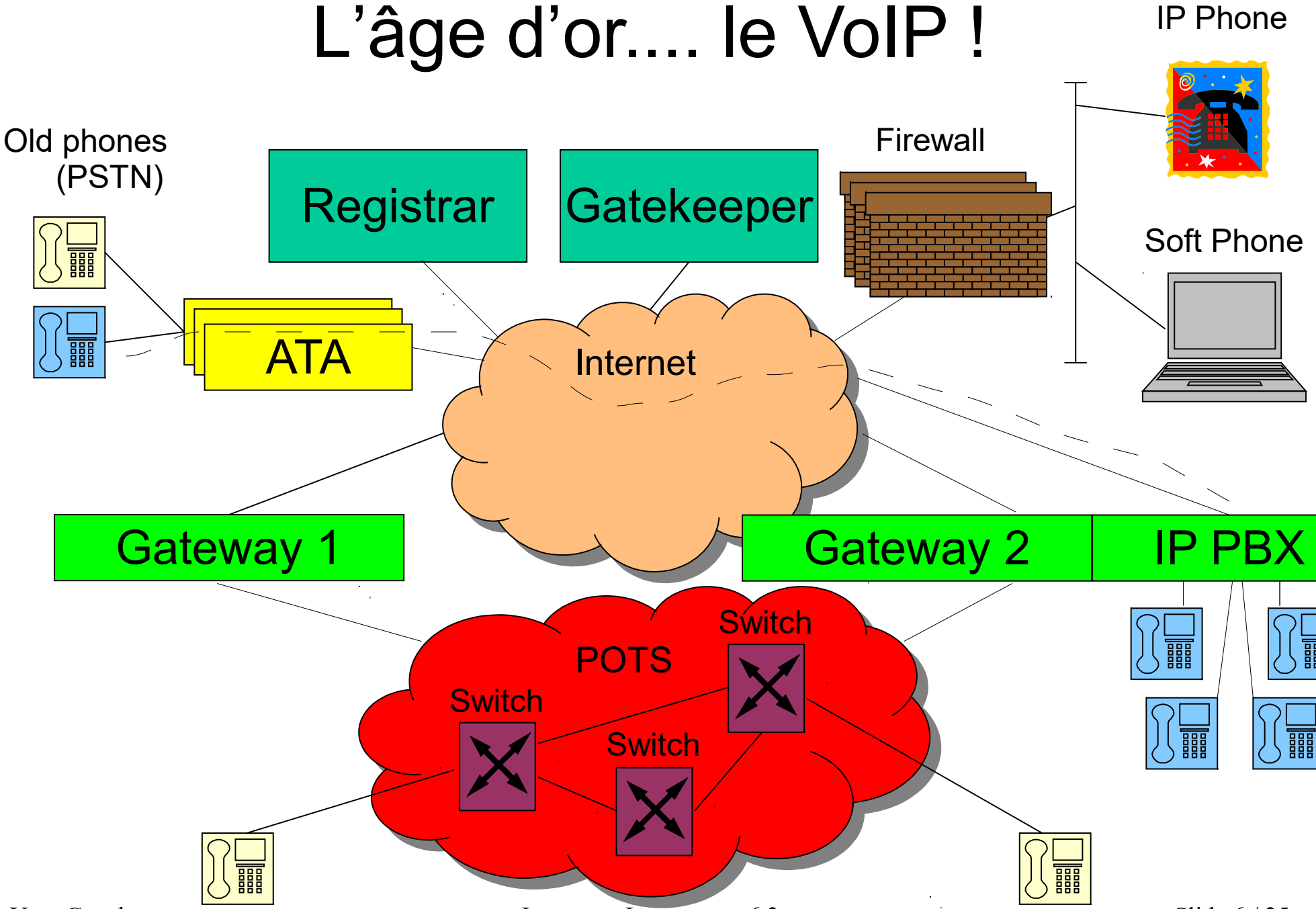
Architecture – 2

- Deux composantes essentielles:
  - Les protocoles de signaling (H323, SIP, MGCP...) à comparer avec SS7.
  - Le flux voix (RTP / RTCP) à comparer avec... la transmission de la voix (maintenant digitalisée).
- Ne pas oublier les aspects de facturation !
- Interconnexion obligatoire avec le PSTN (au moins en production) !!!

L’âge du bronze... le PSTN !



L’âge d’or.... le VoIP !

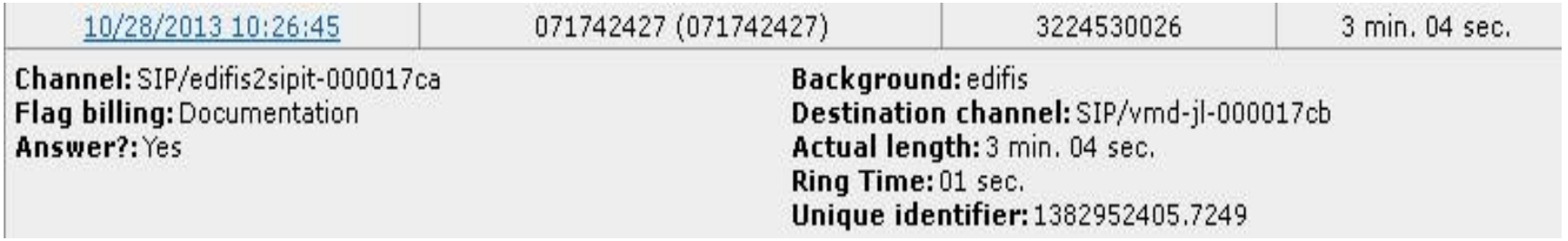


Gatekeeper – 1

- Les rôles essentiels du gatekeeper sont:
  - Accepter ou refuser les appels (admission control)
  - Router les appels (les flux voix) vers les bons gateways (LCR)
  - Gestion de la bande passante
  - Facturer les appels aux utilisateurs (prepaid / postpaid / forfaits / par minute / par seconde / pas de facturation / prix de setup / heures pleines / heures creuses ...)

Gatekeeper – 2

- Traces des appels: les CDRs (Call Detail Record)
- Exemple:
  - 1,17325551212,15,200002070628 12,21060207062815,200002070628 30,16,209.222.143.57 , 192.168.10.64,4,1,1,1,1,1,1, , ,0,0
  - Autres formats...
  - Interface graphique



10/28/2013 10:26:45	071742427 (071742427)	3224530026	3 min. 04 sec.

Channel: SIP/edifis2sipit-000017ca
Flag billing: Documentation
Answer?: Yes
Background: edifis
Destination channel: SIP/vmd-jl-000017cb
Actual length: 3 min. 04 sec.
Ring Time: 01 sec.
Unique identifier: 1382952405.7249

Codecs

- Pour coder et décoder efficacement (?) les flux voix et vidéos: les Codecs. Déterminent la compression et la performance utilisée...

Codec	Bit rate (kbps)	Remark
T38		Fax (!!! implémentation!!!)
G.711 µ Law	64	USA - Japan
G.711 A Law	64	Europe
G.721	32	
G.729	8	Pas libre de droits - Fréquent
G.723.1	6.3 / 5.3	

DTMF

- Dual Tone Multi Frequency
- Sert quand on doit guider un automate (IVR : banque, voice mail, carte prépayée etc...)
- 3 possibilités :
  - In audio
  - RFC 2833
  - SIP INFO

Principaux protocoles – SDP, RTP & RTCP.

- Session Description Protocol, Real time Transport Protocol & Real Time Control Protocol
- RFC 1889 & 1890
- Définis pour supporter la voix ET la vidéo !
- SDP pour négocier les capacités des participants (codecs, nombres, portes etc...)
- RTP sert à offrir le transport des paquets de données en temps réel. Paquets de taille fixe.
- RTCP sert à contrôler la QoS offert au sessions RTP.
- Tournent tous les trois sur UDP !

Les numéros de téléphone

- +883 est le code international pour la VoIP
- On peut rerouter (moyennant paiement) vers un numéro géographique. On devient alors indépendant de la situation géographique (cf GSM). C'est le portage. Les clients peuvent garder leur numéro s'ils le désirent.
- Attention aux numéros d'urgence ! Pas supporté en IP

Principaux protocoles – H323

- H323 disparaît petit à petit au profit de SIP
- H.225.0 (Call connexion signaling) basé sur les messages Q.931 (qui viennent du monde ISDN)
- H.245 (Media control and Transport)
- H.225 (Registration, Admission and Status)
- H.235 (Security)

Principaux protocoles – SIP – 1

- SIP (Session Initiation Protocol) sert à établir, à gérer et à terminer des sessions voix et vidéos sur des réseaux à commutation de paquets (comme l'internet).
- RFC 3261 (la plus grosse RFC, 648 KB de texte !)
- Fonctionne comme HTTP (y compris au niveau sécurité...).
- En pleine explosion ! Supposé être la plus grosse révolution depuis IP...
- Port 5060 sur UDP !

Principaux protocoles – SIP – 2

- Fonctionne (comme HTTP) sur un mode de requête – réponse.
- Basé (comme HTTP) sur une notion d'adresse (sip: yves@ipl.be) appelée SIP-URL.
- Utilise le record DNS SRV.
- S'appuie sur SDP (Session Description Protocol) pour établir les sessions. Les ports utilisés par SDP sont négociés lors de l'établissement de la session (donc problème de FW).
- SDP permet d'établir des sessions entre 2 ou plusieurs points...

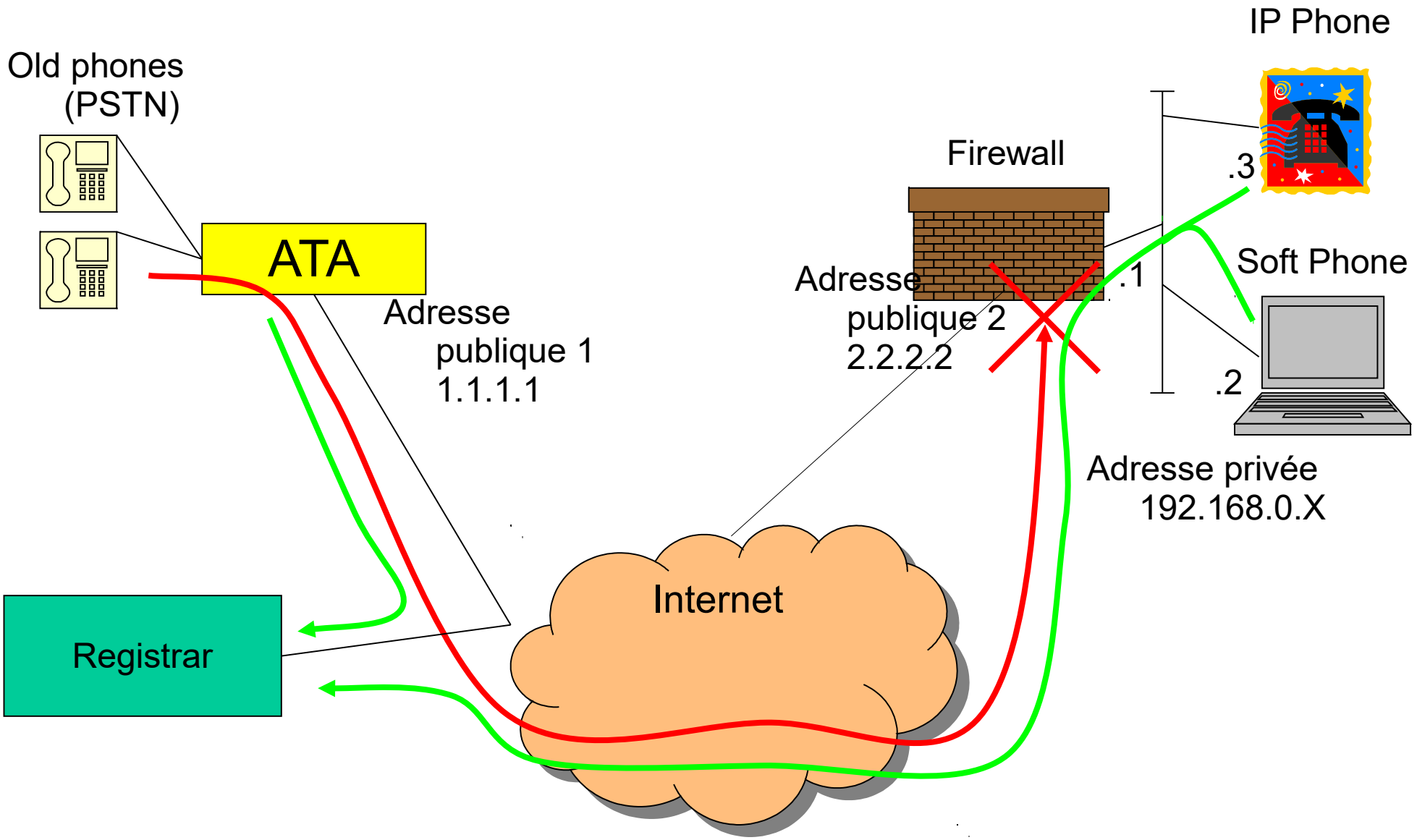
SIP – Les paquets

- Requêtes
  - INVITE
  - ACK
  - CANCEL
  - BYE
  - OPTIONS
  - REGISTER
  - INFO
- Réponses
  - 1XX : Provisionning
    - 100 – Trying
    - 180 – Ringing
  - 2XX : Succès
    - 200 – OK
  - 3XX : Redirection
  - 4XX : Erreur Client
    - 404 – Not found
    - 486 – Busy
  - 5XX : Erreur serveur
  - 6XX : Erreur globale

Le problème – 1

- Les appels entrants ne savent pas passer un FW / NAT (logique)
- Les appels sortant risquent de ne passer que dans un seul sens (depuis l'intérieur vers l'extérieur du FW).

Le problème – 2



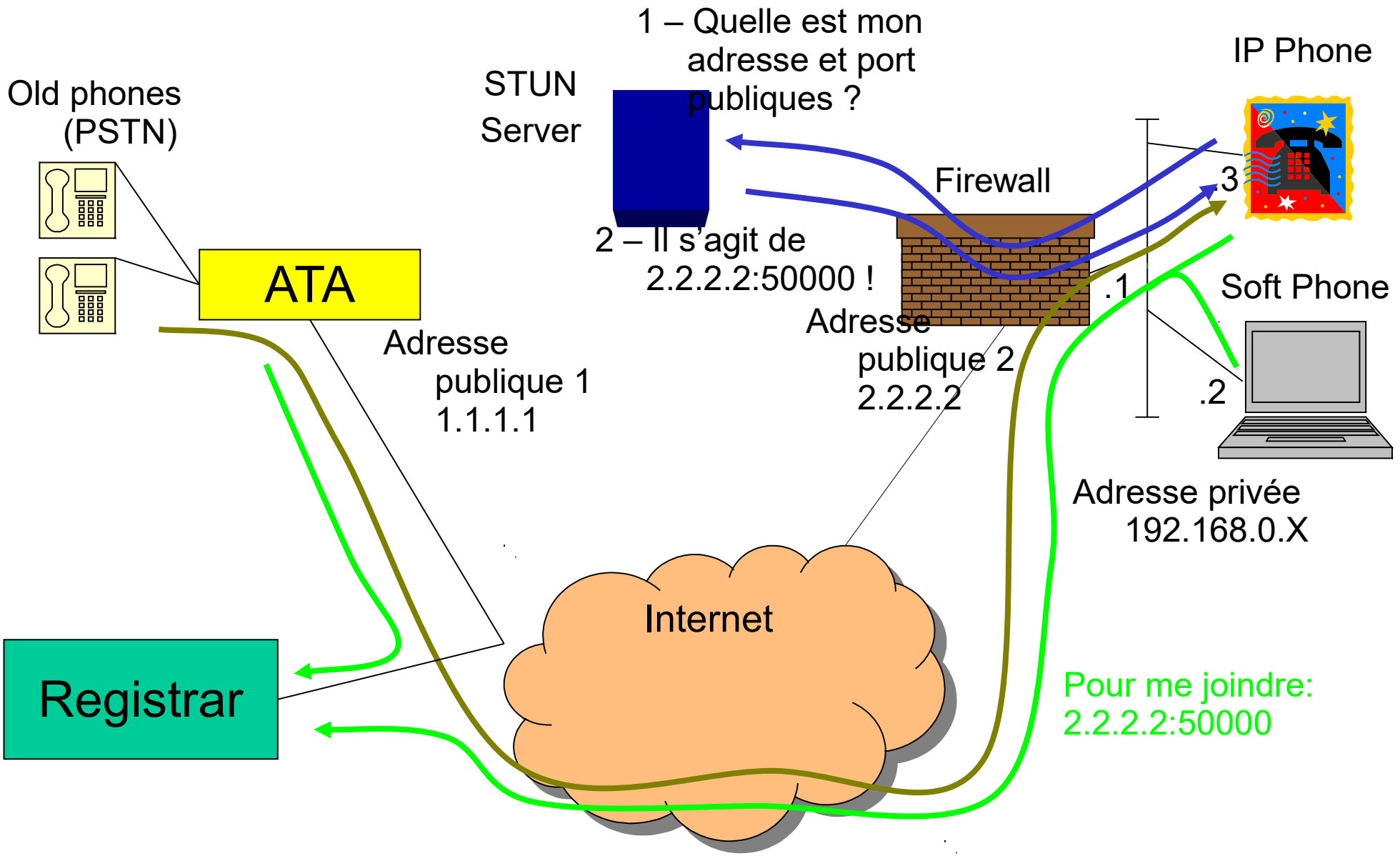
Solution – 1

- Entrée statique dans le FW / NAT
- Diminution de la sécurité
- Oblige à utiliser une adresse fixe (plus de DHCP, ou alors avec réservation).

Solution – 2

- Notion de STUN serveur.
- Le téléphone demande au STUN serveur avec quelle adresse il est vu de l'extérieur.
- Le STUN serveur répond au client (IP tel) l'adresse et le port public utilisé.
- Le client s'enregistre avec cette IP et ce port public
- Attention: ne fonctionne qu'avec des NAT symétriques (dont l'adresse et la porte publique ne dépendent pas de l'adresse et de la porte de destination)

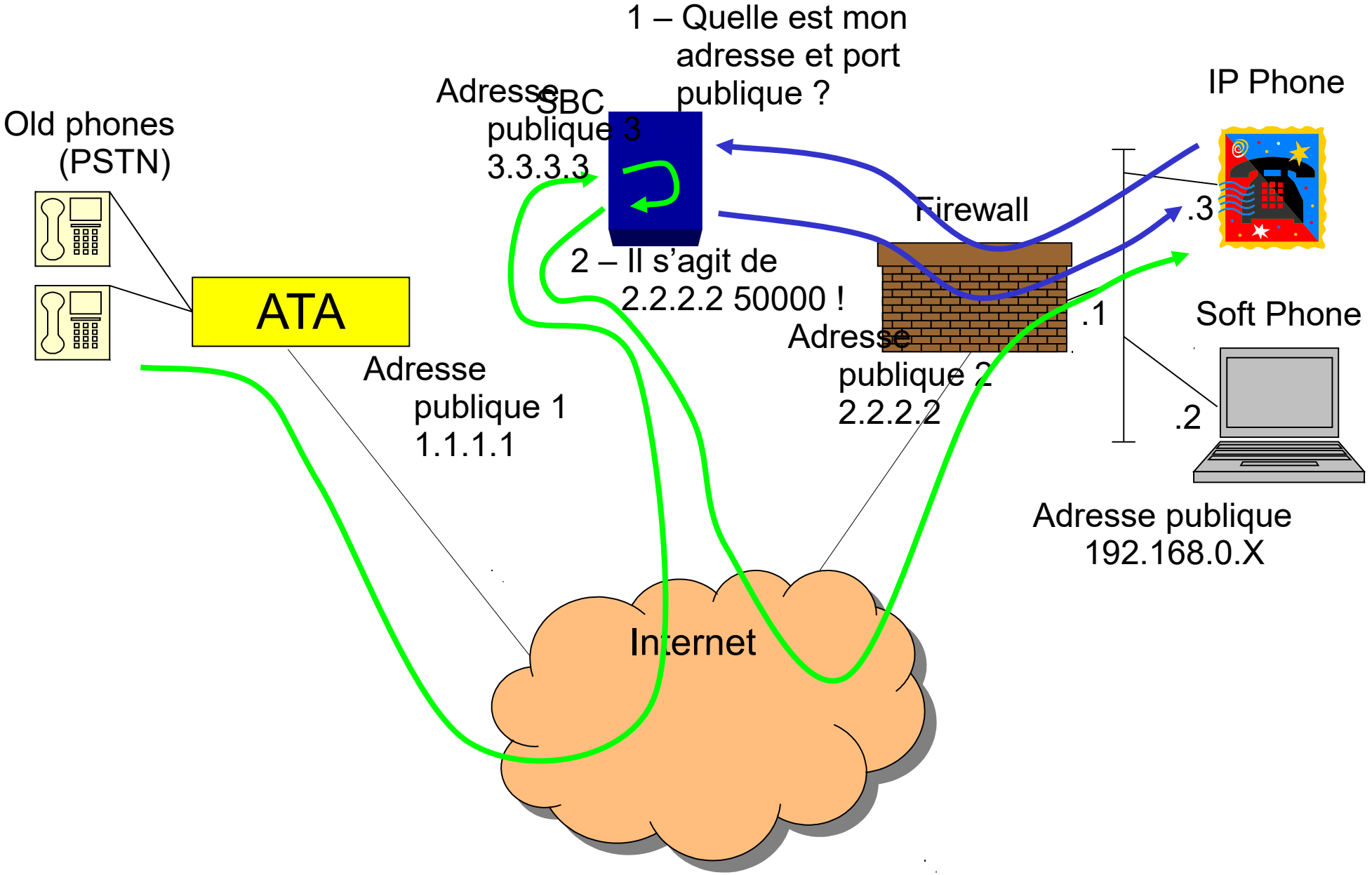
La solution – 2 – STUN



Solution – 3 – SBC

- Session Border Controler.
- Tout le trafic (signaling plus voix) passe par le SBC, qui a une adresse publique.
- Le client demande au SBC quel est son adresse et port publique (cf STUN).
- Tout le trafic passe par le SBC, qui maintient la session avec le client. Donc, le client est vu comme s'il était le SBC (adresse publique)...
- Le SBC agit comme s'il était un switch téléphonique.
- Performance améliorée, contrôle renforcé (par et dans le SBC).

La solution – 3 – SBC



Solution – 4 – Le Pinhole

- La solution la plus naturelle, pour contourner les FW, est que le téléphone, de l'intérieur du réseau (depuis le LAN) envoie régulièrement des paquets vers le GK ou vers le Registrar ; afin de maintenir un Pinhole ouvert dans le FW.
- C'est mieux, mais risque de timeout
- Le téléphone doit communiquer régulièrement avec le GK (ou Registrar) en fonction du timeout du FW.

La solution – 4 – Pinhole