Module M4205
Téléphonie sur IP
IUT de Villetaneuse
Département R&T
Année 2016–2017

http://www.lipn.univ-paris13.fr/~evangelista/cours/M4205

Plan

Contenu du module

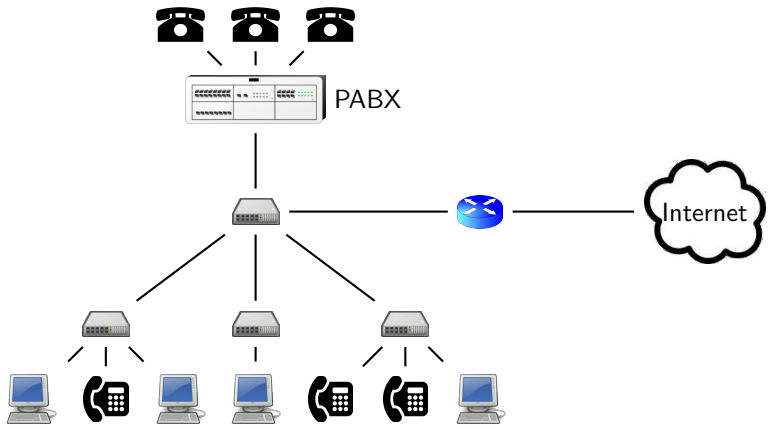
M4205 — Téléphonie sur IP
http://www.lipn.univ-paris13.fr/~evangelista/cours/M4205

- Objectif : étude des protocoles et mécanismes de qualité de service utilisés en téléphonie sur IP
- Organisation :
  - $2 \times$ 1h de cours
  - $6 \times$ 3h de TP
  - $1 \times$ 2h de Contrôle
- Évaluation : 4 TPs notés (1/3) + le contrôle (2/3)
- Enseignants : Benallouche, Feybesse, Evangelista

La ToIP

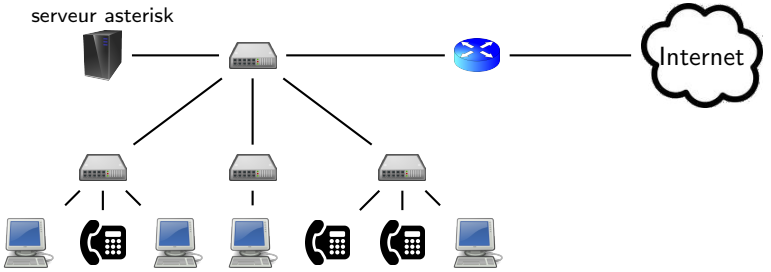
- ToIP = Telephony on IP
- Techniques de téléphonie qui utilisent uniquement le réseau IP (plus de réseau téléphonique).
- Équipements téléphoniques avec une pile TCP/IP.
- Avantages :
  - baisse des coûts (abonnements et communication)
  - simplification du câblage (un seul réseau avec un seul type de câble)
  - mobilité des utilisateurs (grâce aux registres, voir plus loin)
- Inconvénients :
  - pas de service pendant une coupure électrique
  - réseau IP moins fiable que le réseau téléphonique $\Rightarrow$ plus faible disponibilité
- Solution courante : presque tous les téléphones sur IP et on garde quelques téléphones analogiques de secours en cas de problème.

Exemple d'architecture hybride (TPs 1, 2 et 3)



- utilisation de téléphones analogiques (☎) et IP (📞)
- Tous les appels (entrants, sortants et en interne) transitent par le PABX.
- Rôles du PABX :
  - proxy et registrar SIP (voir plus loin)
  - passerelle VoIP (traduction flux analogiques ↔ flux numériques)

Exemple d'architecture 100% IP (TPs 4, 5 et 6)



- plus de téléphones analogiques
- asterisk = logiciel libre, serveur SIP sous Linux
- Le serveur asterisk remplace le PABX.

Plan

L'architecture SIP

Participants :

- **UAs** (User Agent) : logiciel ou équipement de téléphonie
- **Registrars** : les serveurs d'enregistrement des UAs
- **Proxys SIP** : intermédiaires entre les UAs
- **Serveurs DNS** : renseignent sur les proxys SIP de leur domaine

Les UAs et l'adressage SIP

- UA = n'importe quel logiciel (linphone, ekiga, ...) ou téléphone IP qui comprend le protocole SIP.
- Pas skype, par exemple, car il utilise un protocole propriétaire.
- Un UA est identifié par son **URI** (Uniform Ressource Identifier).
- forme générale d'une URI :

  `sip:identifiant[:motdepasse]@où[:port][?paramètres]`
- entre crochets : ce qui est optionnel
- Donc dans la forme la plus simple on a :

  `sip:identifiant@où`
- où peut être :
  - l'IP ou le nom de l'UA
  - l'IP ou le nom de son proxy SIP
  - le nom du domaine de l'UA

Les registrars (serveurs d'enregistrement)

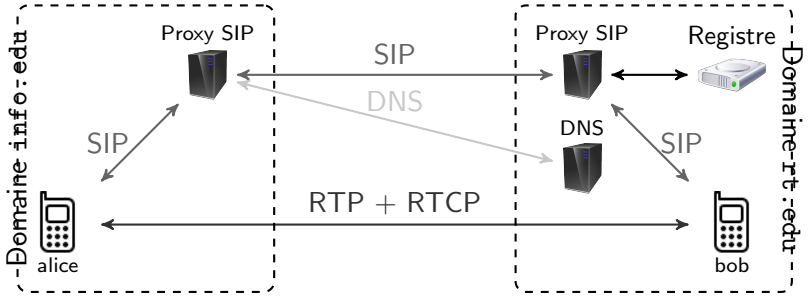
- Les utilisateurs peuvent se connecter avec leurs UAs sur différentes machines.
- Problème : comment retrouver son IP pour lui transmettre des appels ?
- La **registrar** maintient une base de données des localisations dans un **registre** sous forme de couples

  (identifiant, IP + port)
- registrar = n'importe quel serveur qui traite les requêtes SIP **REGISTER** des UAs
- À un identifiant peuvent être associées plusieurs IP.
  - Si on appelle cet identifiant toutes les IP seront contactées.
  - Le premier UA qui répond prend l'appel.
- Un registrar stocke uniquement les localisations de son domaine.

Les proxys SIP

- proxy SIP : intermédiaires entre deux UAs qui ne connaissent pas leurs localisations respectives
- Le proxy SIP consulte le registre de son domaine pour récuperer la localisation d'un UA appelé.
- Généralement, le proxy et le registrar sont une seule et même entité.
- Par exemple , les PABXs Aastra en R101 sont à la fois proxy et registrar.

Scénario d'appel entre deux UAs



`alice@info.edu` passe un appel à `bob@rt.edu`

1. Établissement de la session
   - utilisation de SIP entre les proxys et les UAs
   - Le proxy SIP de `info.edu` interroge le DNS de `rt.edu` pour avoir l'IP du proxy SIP de `rt.edu`.
   - Le proxy SIP de `rt.edu` interroge son registre pour connaître la(es) localisation(s) actuelle(s) de bob.
2. Lors de l'appel
   - transport du flux audio entre les deux UAs avec RTP+RTCP
3. Libération de la session
   - utilisation de SIP entre les proxys et les UAs

Utilisation de DNS pour localiser un proxy SIP

- Dans le scénario précédent, on a vu qu'un proxy interroge un serveur DNS quand il doit relayer un message SIP au proxy d'un domaine, disons `rt.edu`.
- Dans ce cas, le DNS du domaine `rt.edu` doit définir (au moins) un enregistrement SRV ayant la forme suivante :

  `_sip._prot SRV prio poids port nom-du-proxy-sip`

  avec :
  - `prot` = protocole de transport utilisé par le proxy
  - `prio` = classe de priorité du serveur
  - `poids` = poids relatif du serveur dans sa classe de priorité
  - `port` = numéro de port sur lequel il faut contacter le proxy sip
- Quand un proxy voudra communiquer en UDP avec un proxy de `rt.edu`, il demandera les enregistrements SRV concernant `_sip._udp.rt.edu`.

Utilisation de DNS pour localiser un proxy SIP : exemple

Fichier de la zone `rt.edu` :

```
;;              priorité  poids  port  nom-du-proxy
_sip._udp  SRV  1         2      5060  sip1
_sip._udp  SRV  1         1      5060  sip2
_sip._udp  SRV  2         1      6589  sip3

;;  adresses IP des trois serveurs
sip1  A  1.2.3.1
sip2  A  1.2.3.2
sip3  A  1.2.3.3
```

- Le domaine `rt.edu` a trois proxys SIP utilisant UDP : `sip1`, `sip2` sur le port 5060 et `sip3` sur le port 6589.
- `sip1` et `sip2` ont une priorité de 1 : c'est eux qu'il faut tenter de contacter en premier. Si aucun des deux ne répond, on contacte `sip3`.
- `sip1` et `sip2` ont la même priorité mais pas le même poids. Les poids relatifs indiquent que dans 2 cas sur 3 il faut contacter `sip1` et dans 1 cas sur 3 il faut contacter `sip2`.

Remarque sur les enregistrements DNS de type SRV

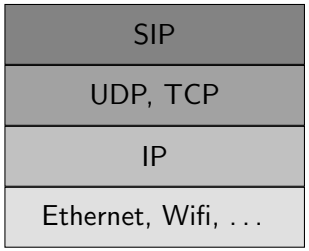
- Dans l'exemple précédent on a vu qu'un enregistrement SRV permet de découvrir l'identité d'un serveur SIP.
- Ce type d'enregistrement a été créé pour découvrir n'importe quel type de service proposé sur un domaine.
- Par exemple, si l'administrateur du domaine veut rendre visibles deux serveurs HTTP et FTP, il peut rajouter dans le fichier de zone :

```
;;              priorité  poids  port  nom de la machine
_http._tcp  SRV  1         1      80    www
_ftp._tcp   SRV  1         1      21    ftp
```

Plan

Présentation de SIP

- SIP = Session Initiation Protocol
- première version de SIP dans la RFC 3261 (juin 2002)
- protocole de signalisation pour l'établissement/libération de sessions interactives entre utilisateurs
- utilisé en téléphonie et plus généralement pour les communications multimédias
- port par défaut = 5060
  (utilisé par tous les équipements SIP : UAs, proxys, registrars)
- pile protocolaire :



- (En général c'est plutôt de l'UDP au niveau transport.)

Structure des messages SIP

- structure similaire aux messages HTTP
- Requêtes et réponses ont le même format :
  - 1 ligne avec
    - pour une requête : le type de la requête
    - pour une réponse : le code d'état
  - N ligne(s) d'en-tête avec différents champs
  - 1 ligne vide qui marque la fin de l'en-tête
  - un corps

Types de requête

Les types les plus utilisés :

- **INVITE** = demande d'initiation d'une session
- **ACK** = confirmation des paramètres d'une session
- **REGISTER** = enregistrement de sa localisation auprès d'un registrar
- **BYE** = fin d'une session ($\Leftrightarrow$ un des UAs raccroche pendant l'appel)
- **CANCEL** = annulation d'une session ($\Leftrightarrow$ l'appelant raccroche avant que l'appelé ne décroche)

Codes d'état des réponses

Les codes les plus utilisés :

- 1xx = Messages d'information
  - 100 = trying
  - 180 = ringing
- 200 = OK
- 3xx = Messages de redirection
  - 301 = moved permanently (identifiant demandé n'est plus dispo.)
  - 302 = moved temporarily
- 4xx = Erreur client
  - 401 = authorisation requise (p.ex., un registrar refuse l'enregistrement)
  - 404 = utilisateur inexistant
  - 486 = utilisateur occupé
- 5xx = Erreur serveur
  - 500 = erreur interne
  - 503 = service non disponible (p.ex., serveur surchargé)

Les champs d'en-tête

- Chaque champ de l'en-tête a la forme `Champ: Valeur`.
- Champs principaux pour les messages INVITE :
  - **From** — URI de l'appelant
  - **To** — URI de l'appelé
  - **Call-Id** — id. d'un appel
  - **User-Agent** — type de l'UA
  - **Via** — liste des UAs/Proxys par lequel le message est passé (IPs + ports)
    ⇒ **La réponse au message suivra ce même chemin.**
  - **Content-Type** — type MIME du contenu
  - **Max-Forwards** — nombre max. de proxys par lesquels un message peut transiter (⇒ permet d'éviter les boucles)

Le corps du message

- Le corps du message est optionnel.
- Il contient le descriptif des paramètres de la session :
  - **IP + port à utiliser pour le flux RTP**
  - medias souhaités pour la communication
  - codecs disponibles
  - paramètres des codecs

  ...
- On le trouve principalement dans
  - un message INVITE (param. fournis par l'appelant)
  - un message OK envoyé en réponse à un INVITE (param. fournis par l'appelé)
- Il peut être au format HTML ou SDP (Session Description Protocol).

Exemple de message INVITE


```
1  INVITE sip:411@ideasip.com SIP/2.0
2  CSeq: 1 INVITE
3  Via: SIP/2.0/UDP 194.254.173.6:5060
4  Via: SIP/2.0/UDP 157.12.54.87:5060
5  Via: SIP/2.0/UDP 54.21.4.7:5060
6  User-Agent: Ekiga/4.0.1
7  From: <sip:sami@194.254.173.6>
8  Call-ID: 54d5b754-cdbe-e611-885f
9  To: <sip:411@ideasip.com>
10 Content-Length: 458
11 Content-Type: application/sdp
12 Max-Forwards: 70
13
14 v=0
15 o=- 1481542778 1 IN IP4 194.254.173.6
16 s=Ekiga/4.0.1
17 c=IN IP4 194.254.173.6
18 t=0 0
19 m=audio 54678 RTP/AVP 116 0 8 101
20 a=sendrecv
21 a=rtpmap:116 Speex/16000/1
22 a=rtpmap:8 PCMA/8000/1
23 a=rtpmap:101 telephone-event/8000
24 a=fmtp:101 0-16,32,36
25 ...
```

En-tête (lignes 1 à 12)

ligne 1 — ligne de requête avec type de la requête, URI de l'appelé et num. de version SIP

lignes 3–5 — le INVITE a été émis par l'UA 194.254.173.6:5060. Il est ensuite passé par les proxys 157.12.54.87:5060 et 54.21.4.7:5060

lignes 7–9 — URIs de l'appelant et de l'appelé

ligne 11 — format du contenu du message = SDP

Corps (lignes 14 et suivantes)

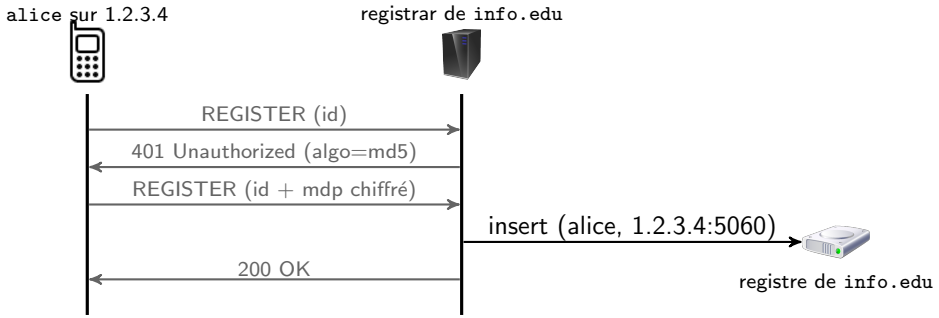
ligne 17 — IP à utiliser pour le flux RTP = 194.254.173.6

ligne 19 — port UDP à utiliser pour le flux RTP = 54678

ligne 20 et suivantes — autres info. RTP (media utilisés, codecs, ...)

Scénario SIP 1 — Enregistrement d'un UA

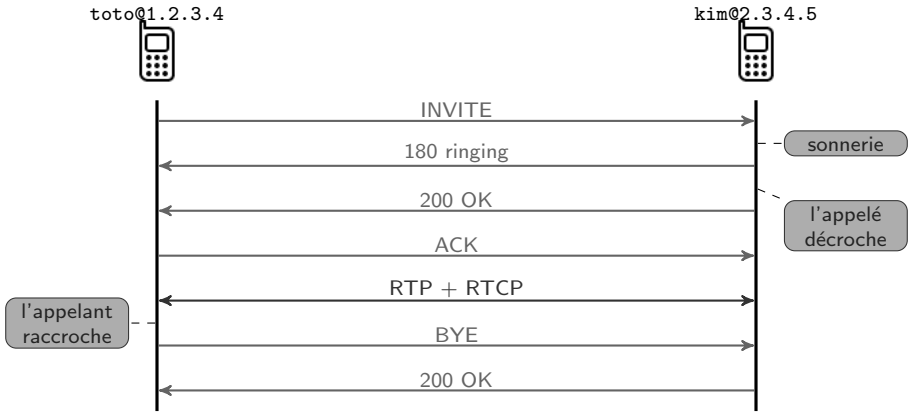
- `alice@info.edu` s'enregistre auprès de son registrar
- Quand a lieu l'enregistrement ? À l'ouverture du softphone, au branchement du téléphone IP, ...



- Un 1er message REGISTER contient l'identifiant.
- Le serveur refuse et envoie un algo de chiffrement (md5 ici).
- Un 2ème message REGISTER contient identifiant + mot de passe crypté.

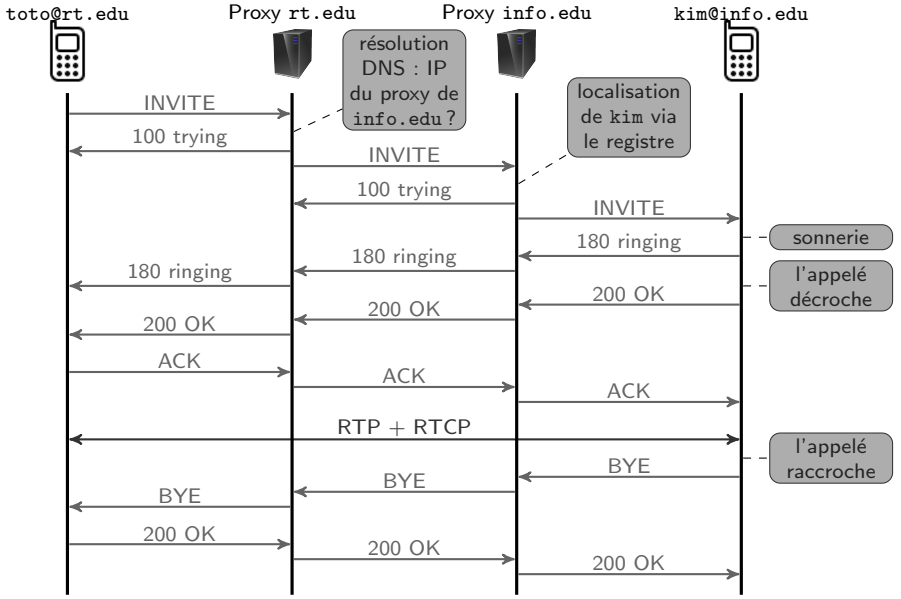
Scénario SIP 2 — Appel direct

- `toto@1.2.3.4` appelle `kim@2.3.4.5`
  (Pas nécessaire de passer par un proxy si on a l'IP de l'UA destinataire.)



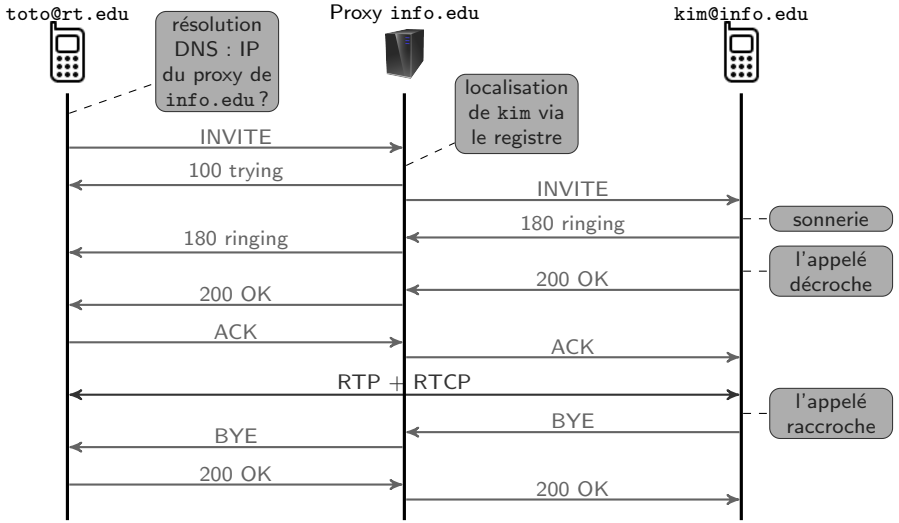
Scénario SIP 3 — Appel passant par deux proxys

- `toto@rt.edu` appelle `kim@info.edu` en passant par son proxy



Scénario SIP 4 — Appel passant par un proxy

- `toto@rt.edu` appelle `kim@info.edu` en contactant directement le proxy de `info.edu`



Plan

Rappels sur NAT

- NAT = Network Address Translation
- solution temporaire à la pénurie d'adresses IP
- Avec NAT : des réseaux privés (p.ex., à l'IUT) et le réseau public.
- sur un réseau privé : IP privées inutiles sur le réseau public
- Plages des adresses privées :
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Un réseau privé est derrière une passerelle NAT (généralement la passerelle par défaut du réseau) qui fait la translation entre les deux types d'adresse.
- L'interface de la passerelle qui la relie à l'extérieur a une IP publique.

Fonctionnement de la passerelle NAT (1/2)

1 Pour les paquets sortants, la passerelle :
  1.1 modifie l'IP et le port source (privés) par son IP publique et par un nouveau numéro de port qu'elle choisit (p.ex., aléatoirement dans une plage donnée) ;
  2.2 et mémorise l'association (IP + port privés, IP + port publics) dans une table de correspondance.

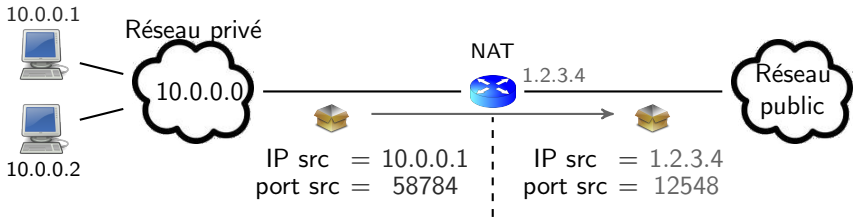


Table de correspondance

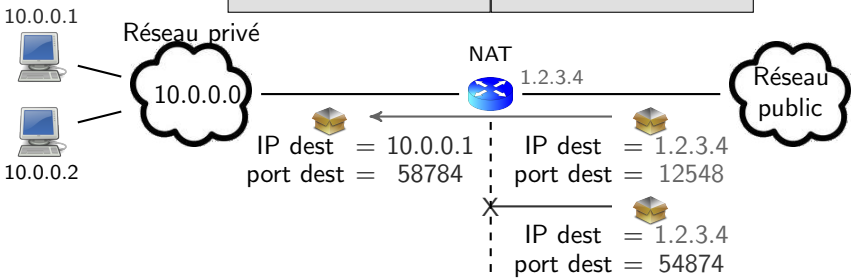
IP + port privés	IP + port publics
10.0.0.1:58784	1.2.3.4:12548

Fonctionnement de la passerelle NAT (2/2)

2 Pour les paquets entrants, la passerelle cherche dans sa table.
  2.1 si association trouvée : IP et port destination modifiés
  2.2 sinon : paquet jeté

Table de correspondance

IP + port privés	IP + port publics
10.0.0.1:58784	1.2.3.4:12548

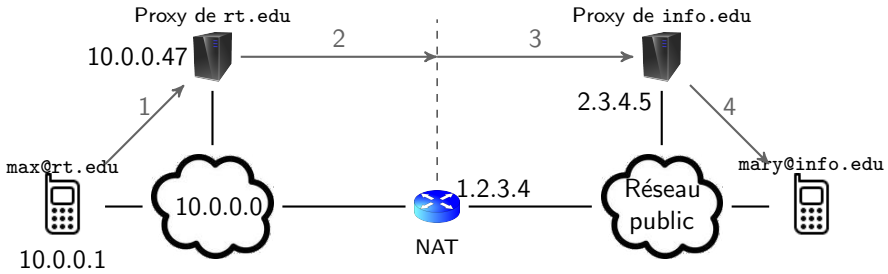


Remarques sur le fonctionnement de la passerelle NAT

- Certaines passerelles NAT ne font pas de translation de port : elles changent uniquement l'adresse IP.
- La sortie d'un paquet ouvre le port choisi par la passerelle.
- Les lignes de la table ont une durée de vie limitée (quelques minutes).
- La passerelle joue le rôle de filtre : elle
  - laisse entrer les paquets envoyés en réponse à des paquets sortis du réseau ;
  - et bloque les autres.
- Si un serveur se trouve sur le réseau privé et doit pouvoir être accessible depuis l'extérieur il faut rajouter statiquement une ligne dans la table.
  - Ex : l'administrateur ajoute (priv. = 10.0.0.2:80, pub. = 1.2.3.4:80) pour rendre le serveur web sur 10.0.0.2 accessible depuis l'extérieur.

Problème d'utilisation du NAT avec SIP (1/2)

`max.rt.edu` appelle `mary.info.edu`.



- La passerelle ne modifie pas l'en-tête et le contenu SIP !
- Dans le message SIP Invite 3 :
  - source IP et UDP = 1.2.3.4:48789 (port choisi par la passerelle NAT)
  - Dans l'en-tête SIP : `Via: 10.0.0.1:5060` et `Via: 10.0.0.47:5060`
  - Dans le corps SIP : IP + port pour le flux RTP = 10.0.0.1:8420

⇒ La réponse au INVITE ne pourra pas parvenir au proxy de `rt.edu`.

⇒ Même si la réponse au INVITE arrivait à max, le flux RTP envoyé par mary serait envoyé sur 10.0.0.1:8420

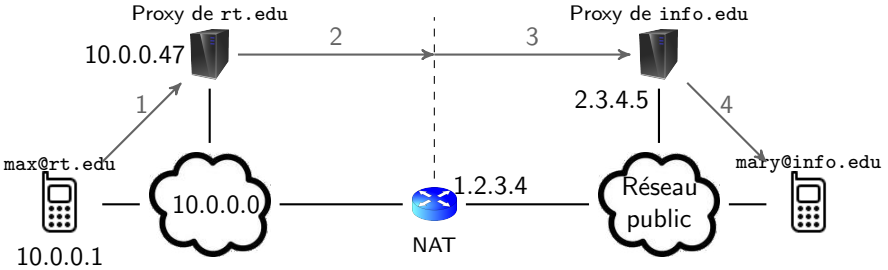
Problème d'utilisation du NAT avec SIP (2/2)

- L'exemple précédent montre qu'on doit résoudre deux problèmes :
  1. La réponse au INVITE doit arriver au proxy de `rt.edu`.
  2. Le flux RTP doit pouvoir arriver à max.
- Pour le problème 1 : utilisation de l'option received/rport.
- Pour le problème 2 : nombreuses solutions. Nous allons étudier STUN.

L'option received/rport

- Quand un proxy SIP va recevoir un INVITE, il :
  1. compare l'IP+port source à IP+port du dernier champ Via
  2. si ≠ alors il y a un NAT entre les 2 ⇒ il rajoute à ce dernier champ Via
     - l'option `received=<ip-source>`
     - l'option `rport=<port-source>`
- Ce sont les valeurs des options `received` et `rport` qui seront utilisées pour la réponse au INVITE.

L'option received/rport — Exemple

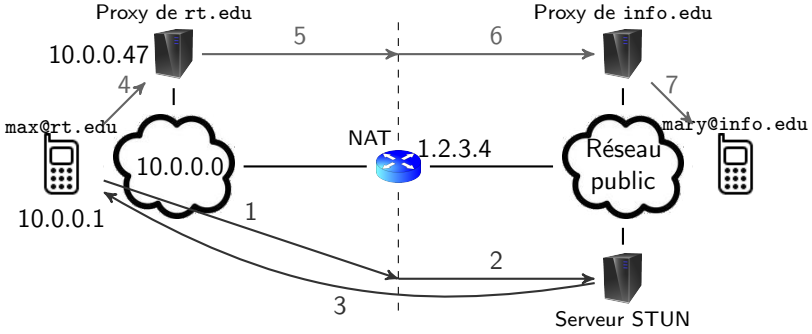


	IP + port sources	Champs Via (en-tête SIP)
1	10.0.0.1:5060	Via : 10.0.0.1:5060
2	10.0.0.47:5060	Via : 10.0.0.1:5060 Via : 10.0.0.47:5060
3	1.2.3.4:48789	Via : 10.0.0.1:5060 Via : 10.0.0.47:5060
4	2.3.4.5:5060	Via : 10.0.0.1:5060 Via : 10.0.0.47:5060 ;received=1.2.3.4 ;rport=48789 Via : 2.3.4.5:5060

Le proxy de `info.edu` pourra envoyer sa réponse à 1.2.3.4:48789.

- STUN = Simple Traversal of UDP through NATs
- Un serveur STUN permet au client de découvrir son IP et son port publics.
- On trouve plein de serveurs STUN libres d'utilisation sur Internet.
- Fonctionnement (simplifié) :
  1. Le client envoie un paquet UDP au serveur STUN.
  2. Le serveur STUN répond en plaçant dans sa réponse l'IP et le port du client.
- Remarques :
  - Le serveur STUN ne doit pas être sur le réseau privé du client.
  - L'IP et le port du client sont placés à l'intérieur du message STUN (⇒ non modifiés par le NAT lors du retour).
  - L'envoi du paquet STUN par le client permet d'ouvrir le port public alloué par le NAT.
  - STUN ne marche pas avec certains types de NATs : les NATs symétriques qui attribuent des ports publics en fonction de l'IP de destination.

- STUN va permettre à l'UA d'ouvrir un port UDP public pour le flux RTP.
- Le port et l'IP publics sont ensuite placés dans le corps du INVITE.



1 req. STUN — IP src = 10.0.0.1 et port src = 10000 (port RTP privé)
2 req. STUN — IP src = 1.2.3.4 et port src = 24045 (port RTP public)
3 rép. STUN — contenu : IP = 1.2.3.4 et port = 24045
4–7 INVITE — contenu SDP :

```
c=IN IP4 1.2.3.4
m=audio 24045 RTP/AVP 116 0 8 101
```