Réussir des liaisons AoIP avec les codecs AAS

1. Introduction : objet et généralités

Etablir une liaison via réseau IP entre codecs audio n'est pas (pas encore ?) aussi simple que via RNIS. Il y a plusieurs raisons à cela : nouveauté des techniques, diversité des environnements et organisations de réseaux, parfois aussi coordination insuffisante entre techniciens broadcast et réseaux…

La configuration des codecs et des équipements de réseau peut donc être assez délicate parfois, mais elle est souvent facilitée pour les codecs d'AETA AUDIO SYSTEMS grâce à l'utilisation du protocole SIP.

Ce document décrit les techniques à appliquer pour contourner les difficultés habituelles. Même sans prétendre à l'exhaustivité, les divers cas abordés devraient couvrir la grande majorité des situations. Les problèmes les plus classiques sont liés à :

- L'existence d'un routeur NAT sur le parcours réseau entre les codecs
- La présence de pare-feu sur ce parcours

Voir le glossaire en fin du document pour plus de détails sur certains acronymes utilisés.

Pour accès rapide, les informations essentielles sont repérées en rouge comme ce paragraphe.

Il est toujours important de disposer des informations sur l'organisation du réseau et de l'accès aux éléments qui nécessitent une configuration. Notre recommandation essentielle est donc l'implication de personnes habilitées pour cela.

2. Liaisons sur un réseau privé

2.1. Réseau local

Sur un réseau local, il n'y a aucun problème particulier de connectivité. La seule partie délicate est la configuration de l'adressage IP de chaque codec.

Le cas le plus simple est celui de la présence d'un serveur DHCP sur le réseau, où l'on parle souvent d'adressage « dynamique ». Dans le cas contraire dit d'adressage « statique », il faut donc configurer sur chaque codec, au strict minimum, l'adresse IP et le masque de sous-réseau. Selon l'organisation, il peut aussi être nécessaire de programmer l'adresse de passerelle par défaut et/ou l'adresse de DNS.

Une liaison peut être établie depuis un codec « appelant » vers l'autre codec :

- Choisir le codage souhaité
- Entrer l'adresse IP de l'autre codec, puis lancer l'appel. Si l'on utilise un serveur proxy SIP, au lieu d'une adresse IP on entrera l'identifiant (ou URI) SIP du destinataire.

Il n'est pas nécessaire de préparer l'autre codec, la procédure est analogue à un appel téléphonique.

Le fonctionnement est aussi possible avec les codecs d'autres constructeurs, lorsqu'ils sont conformes à la recommandation Tech3326 de l'UER (aussi connue comme recommandation « N/ACIP »). *Il faut cependant s'assurer dans ce cas des réglages ou préparations éventuellement nécessaires sur ces appareils.*

Ce document est propriété de AAS et ne peut être reproduit sans autorisation

2.2. *Réseau étendu*

Un réseau privé étendu va couvrir une grande étendue géographique, et la topologie du réseau impliquera que des routeurs peuvent se trouver sur le chemin entre les deux codecs à relier. Malgré cela, d'ordinaire il n'y a pas vraiment de différence en pratique avec un réseau local.

Remarque: l'utilisation d'une VPN ramène à ce cas de figure; la mise en œuvre est alors identique pour ce qui concerne les codecs.

3. Passage par un réseau public (Internet)

Si chacun des deux appareils concernés dispose d'un accès « direct » à Internet avec une adresse publique, on se retrouve dans un cas fonctionnellement identique au cas précédent (réseau privé étendu). L'adressage est normalement statique car DHCP est rarement utilisable en accès public. En fait, ce cas est très rarement rencontré en pratique !

Tout d'abord, l'accès à Internet est souvent protégé par un pare-feu, qui va, par principe même, empêcher *a priori* la connexion voulue. Il faut dans ce cas créer les exceptions (aux règles de sécurité du pare-feu) qui autorisent cette connexion ; l'opération est du ressort du responsable réseau qui gère ce pare-feu.

Le plus souvent, sur l'un des accès sinon les deux, le codec accède à Internet par l'intermédiaire d'un routeur NAT. Ce dernier partage un accès à Internet, avec une ou quelques adresses publiques, entre les équipements du réseau local. Sur ce dernier les appareils disposent d'adresses privées, et le routeur effectue au passage une *traduction d'adresse* IP. Il faut noter que :

- Par exemple, un modem-routeur d'accès ADSL grand public est quasiment toujours un routeur NAT, partageant une adresse publique IP unique entre les équipements reliés au routeur.
- Il en est de même d'un accès IP mobile 3G/3G+ ; les terminaux accèdent à Internet via un routage NAT.
- Le routage NAT est souvent inclus dans les fonctions du pare-feu lorsqu'il y en a un ; d'ailleurs le routage NAT participe à la protection contre les attaques directes de l'extérieur.

Le routage NAT est un obstacle a priori aux transmissions avec UDP, pour deux raisons principalement :

- Il ne permet pas l'entrée de données non sollicitées depuis l'extérieur. En d'autres termes, l'entrée de données est normalement acceptée sur un port en réponse à une demande depuis le réseau local, mais un agent externe ne peut pas prendre l'initiative de la transmission.
- Les terminaux sur le réseau local n'ont connaissance que de leur adresse privée sur ce dernier. Or le protocole SIP implique la communication entre les agents des adresses et ports utilisés pour les échanges de media. ; à cause du routage NAT, les agents ne disposent pas des véritables adresses, d'où l'échec des tentatives d'établissement de sessions.

Nous allons aborder diverses méthodes utilisées pour contourner ces obstacles.

Ce document est propriété de AAS et ne peut être reproduit sans autorisation janvier 2010 AN109fr - Réussir des liaisons AoIP.docx

3.1. NAT et utilisation d'un serveur STUN

Le protocole STUN est une méthode souvent efficace[1] pour que les agents découvrent leur adressage public même s'ils sont « masqués » derrière un routeur NAT. Principe de mise en œuvre :

- On utilise un serveur STUN accessible sur Internet ;
- L'adresse de ce serveur est programmée dans l'agent (dans le cas qui nous intéresse, le codec audio)
- L'agent interroge le serveur et découvre son adresse IP et numéro de port publics, tels qu'ils sont vus de l'extérieur du routeur NAT
- C'est ensuite cet adressage qu'il utilise pour la négociation de sessions media.

L'adresse du serveur STUN est programmable dans la page html d'un Scoop 4+ ou d'un Scoopy+. Par ailleurs, on trouve aussi dans le menu (clavier et afficheur en face avant de l'appareil) une possibilité d'activer/désactiver (on/off) l'utilisation de cette fonction, sans avoir à effacer l'adresse du serveur.

Il existe de nombreux serveurs STUN publics disponibles sur Internet ; voici quelques exemples valides à la date de rédaction de ce document :

Nom de domaine	Adresse numérique
stun.xten.com	75.101.138.128
stun.ekiga.net	75.101.138.128
stun.sipgate.net	217.10.79.2
stun.ippi.com	208.73.210.27
stun.sipphone.com	198.65.166.165

Exemples de serveurs STUN

Attention, il est conseillé de vérifier que le serveur est opérationnel. Une liste de serveurs est aussi affichée sur la page support de notre site web http://www.aeta-audio.com.

3.2. Routeur NAT standard

Cas considéré : codec A derrière un routeur NAT sans programmation particulière.
(un codec accédant à Internet par réseau mobile est quasiment toujours dans cette situation)
On suppose par ailleurs que l'autre codec (dit B) est accessible par une adresse publique.

Une fois que le codec A est configuré pour utiliser un serveur STUN :

- le codec A peut initier une liaison vers (appeler) le codec B
- le codec B ne peut pas appeler le codec A

Avantages	Inconvénients
Configuration relativement simple	B ne peut pas appeler A
Pas de modification à apporter au routeur	
Possibilité d'utiliser plusieurs codecs derrière le même routeur NAT	
Solution utilisable pour un accès réseau mobile	

[1] Cependant pas avec certains routeurs NAT dits « symétriques ».

Ce document est propriété de AAS et ne peut être reproduit sans autorisation

3.3. Routeur NAT avec DMZ

Cas considéré : codec A derrière un routeur NAT et placé en « DMZ ».
On supposera par ailleurs que l'autre codec (dit B) est accessible par une adresse publique.

Une fois que le codec A est configuré pour utiliser un serveur STUN :

- le codec A peut initier une liaison vers (appeler) le codec B
- le codec B peut appeler le codec A, en utilisant l'adresse publique du routeur NAT

Avantages	Inconvénients
Chaque codec peut initier une session	Nécessité de configurer le routeur
A est pratiquement équivalent à un codec avec accès public direct	Un seul codec peut être installé
	A est exposé aux attaques externes
	La DMZ peut être déjà réservée à un autre équipement du réseau
	Méthode inutilisable avec un accès réseau mobile

3.4. Routeur NAT avec redirection de ports

Cas considéré : codec A derrière un routeur NAT et configuration de ce dernier pour rediriger vers A les ports nécessaires.
On supposera par ailleurs que l'autre codec (dit B) est accessible par une adresse publique.

Redirections à effectuer sur le routeur :

- Port UDP 5060 (= port SIP)
- Ports UDP 5004 (port RTP) et 5005 (port RTCP)[1]

Une fois que le codec A est configuré pour utiliser un serveur STUN :

- le codec A peut initier une liaison vers (appeler) le codec B
- le codec B peut appeler le codec A, en utilisant l'adresse publique du routeur NAT

Avantages	Inconvénients
Chaque codec peut initier une session	Nécessité de configurer le routeur
A est pratiquement équivalent à un codec avec accès public direct	Un seul codec peut être installé
	Méthode inutilisable avec un accès réseau mobile

[1] Pour versions Scoop4+ antérieures à 1.32, ports 9000 et 9001 respectivement

Ce document est propriété de AAS et ne peut être reproduit sans autorisation janvier 2010 AN109fr - Réussir des liaisons AoIP.docx

3.5. Utilisation d'un serveur SIP

L'utilisation d'un serveur proxy SIP, mis à part les nombreux avantages fonctionnels qu'elle apporte, est une méthode très puissante pour résoudre les problèmes liés aux routeurs NAT, car la plupart des proxies SIP sont capables de détecter la présence de routeurs NAT sur le réseau et/ou de gérer leur traversée.

Si l'on dispose d'un serveur SIP, après enregistrement des codecs sur ce serveur :

- Tout codec enregistré peut appeler tout autre codec enregistré[1], qu'il y ait ou non un routeur NAT interposé sur la route
- L'identification (URI SIP) est stable et ne dépend pas de l'endroit où se trouve l'agent appelé (fonction de « mobilité »)

Il est possible soit d'utiliser un serveur public sur Internet, soit d'installer un serveur privé, accessible via Internet.

Avantages	Inconvénients
Chaque codec peut initier une session Chaque codec peut recevoir des appels	Installation éventuellement délicate (serveur privé)
Identification simple et stable selon lieu/date	Fiabilité du serveur non garantie (serveur public)
Sécurité : un proxy privé peut être associé à un pare-feu	
Fonctionne aussi avec les routeurs NAT symétriques	
Interfonctionnement avec téléphonie sur IP	
Solution utilisable pour un accès réseau mobile	

[1] Selon les contrôles d'accès, un serveur peut éventuellement accepter des appels « sortants » vers des domaines tiers, ou accepter des appels « entrants » venant d'agents non enregistrés.

Ce document est propriété de AAS et ne peut être reproduit sans autorisation janvier 2010 AN109fr - Réussir des liaisons AoIP.docx

AETA AUDIO SYSTEMS

4. Récapitulatif et rappel des règles essentielles

Le tableau ci-dessous résume les cas pour lesquels une liaison est possible (sans utilisation d'un serveur proxy SIP) et rappelle les réglages spécifiques nécessaires :

	Accès codec A	Appels possibles	Accès codec B	Notes
1	LAN	⇒ ⇐	LAN (identique)	
2	WAN privé	⇒ ⇐	WAN privé	
3	Internet direct	⇒ ⇐	Internet direct	
4	NAT	⇒	Internet direct	STUN nécessaire en A
5	NAT + DMZ	⇒ ⇐	Internet direct	STUN nécessaire en A
6	NAT + redirection ports	⇒ ⇐	Internet direct	STUN nécessaire en A Ports UDP 5004, 5005, 5060
7	NAT	⇒	NAT + DMZ	STUN nécessaire en A et B
8	NAT + DMZ	⇒ ⇐	NAT + DMZ	STUN nécessaire en A et B
9	NAT + redirection ports	⇒ ⇐	NAT + DMZ	STUN nécessaire en A et B Ports UDP 5004, 5005, 5060
10	NAT	⇒	NAT + redirection	STUN nécessaire en A et B
11	NAT + DMZ	⇒ ⇐	NAT + redirection	STUN nécessaire en A et B
12	NAT + redirection ports	⇒ ⇐	NAT + redirection	STUN nécessaire en A et B Ports UDP 5004, 5005, 5060

Règle de base : Codec derrière un routeur NAT => utiliser un serveur STUN.
Cela permet au codec d'initier des liaisons vers l'extérieur. Cela *ne suffit pas en soi* pour être accessible à une demande de connexion depuis l'extérieur.

Accès réseau mobile sans serveur SIP ni VPN => utiliser un serveur STUN

NAT + DMZ ou NAT + redirection => appels entrants possibles.
Les appels entrants ne sont pas possibles derrière un routeur NAT sans une telle modification et sans proxy SIP.

Serveur SIP => flexibilité maximale, contre un certain effort initial (d'installation).

Remarque importante : contrairement à une idée répandue mais fausse, le protocole SIP (toujours utilisé dans les codecs AAS) *n'impose nullement l'utilisation d'un* ***serveur*** *SIP*. Les codecs peuvent établir des liaisons point à point en utilisant ce protocole, dans les conditions décrites ci-dessus. En l'absence d'un *registrar* SIP, les identifiants sont tout simplement les adresses IP des codecs.

Ce document est propriété de AAS et ne peut être reproduit sans autorisation janvier 2010 AN109fr - Réussir des liaisons AoIP.docx

5. Glossaire

Terme ou abréviation	Signification
AoIP	*Audio over IP*, audio via un réseau au protocole IP
DMZ	Zone, sous-réseau ou adresse IP spécifique échappant aux règles du pare-feu et directement « visibles » de l'extérieur du réseau local.
DNS	*Domain Name Server,* serveur de noms de domaine. Assure la résolution des adresses symboliques en adresses numériques
NAT	*Network Address Translation,* traduction d'adresse réseau. Un routeur NAT sert typiquement à partager pour un sous-réseau privé une ou quelques adresses IP publiques.
SIP	*Session Initiation Protocol,* protocole utilisé pour la signalisation de sessions de communications multimedia (audio dans le contexte de ce document)
STUN	*Simple Traversal of UDP through NATs,* protocole permettant à un client derrière routeur(s) NAT de découvrir son adresse IP publique.
URI	*Uniform Resource Identifier,* identifiant d'un "agent" SIP (terminal mettant en œuvre le protocole SIP pour établir une session)

Ce document est propriété de AAS et ne peut être reproduit sans autorisation janvier 2010 AN109fr - Réussir des liaisons AoIP.docx