Groupe de travail Réseau
**Request for Comments : 3027**
Catégorie : Information
Traduction Claude Brière de L'Isle

M. Holdrege, ipVerse
P. Srisuresh, Jasmine Networks
janvier 2001

# Complications de protocole avec le traducteur d'adresse réseau IP

**Statut de ce mémoire**
Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.



**Résumé**
De nombreuses applications de l'Internet peuvent être affectées lorsque des nœuds d'extrémité ne sont pas dans le même domaine d'adresses et recherchent l'assistance d'un traducteur d'adresse réseau (NAT, *Network Address Translator*) IP sur le chemin pour raccorder les deux domaines. L'appareil NAT seul ne peut pas fournir la transparence nécessaire d'application/protocole dans tous les cas et recherche lorsque c'est possible l'assistance de passerelles de niveau application (ALG, *Application Level Gateway*) pour fournir la transparence. L'objet du présent document est d'identifier les protocoles et applications qui échouent en présence d'un NAT sur le chemin. Le document essaye aussi d'identifier tous les travaux connexes connus. Il n'est pas possible de saisir dans un seul document toutes les applications qui ne sont pas compatibles avec les NAT. Le présent document essaye de rassembler autant d'informations que possible, mais n'est en aucun cas exhaustif. On espère que celles qui sont rassemblées donnent des indices suffisants pour les applications qui ne sont pas couvertes.

## Table des matières

# 1. Introduction

Le présent document exige de la part du lecteur une certaine familiarité avec la terminologie et les fonctions des appareils de NAT décrites dans la [RFC2663]. Sous sa coquille, le NAT essaye de fournir une solution transparente d'acheminement aux hôtes d'extrémité qui ont besoin de communiquer avec des domaines d'adresses disparates. Le NAT modifie en chemin les adresses des nœuds d'extrémité (au sein de l'en-tête IP d'un paquet) et conserve l'état pour ces mises à jour de telle sorte que les datagrammes qui appartiennent à une session soient acheminés de façon transparente au bon nœud d'extrémité dans l'un ou l'autre domaine. Lorsque c'est possible, des ALG spécifiques de l'application peuvent être utilisées en conjonction avec le NAT pour fournir la transparence au niveau de l'application. À la différence du NAT, la fonction de l'ALG est spécifique de l'application et exigerait vraisemblablement un examen et une recomposition de la charge utile IP.

Les sections suivantes essayent de faire la liste des applications qui sont connues pour avoir été impactées par les appareils de NAT en chemin. Cependant, ce n'est en aucun cas une liste exhaustive de tous les protocoles et applications connus pour avoir des complications avec les NAT – c'est plutôt juste un sous-ensemble de la liste constituée par les auteurs. Il est aussi important de noter que ce document n'est pas destiné à être un plaidoyer en faveur des NAT, mais plutôt de souligner les complications avec les protocoles et applications lorsque des appareils de NAT sont sur leur chemin.

# 2. Caractéristiques communes des protocoles violés pas les NAT

Les [RFC2663] et [RFC3022] comportent des sections qui font la liste des problèmes et limitations de nature spécifique des appareils de NAT. Certaines de ces limitations sont répétées dans cette section pour résumer les caractéristiques des protocoles qui sont violés par les NAT.

## 2.1 Informations d'adresse IP spécifiques du domaine dans la charge utile

Une large gamme d'applications sont défaillantes quand il y a des NAT sur leur chemin lorsque des paquets IP contiennent une adresse IP spécifique d'un domaine ou des informations d'accès dans la charge utile. Une ALG peut être capable de contourner cela dans certains cas. Mais, si la charge utile du paquet est sécurisée par IPsec (ou sécurisée par un mécanisme de sécurité de niveau transport ou application) l'application est vouée à l'échec.

## 2.2 Applications de faisceaux de sessions

Les applications de sessions en faisceaux telles que FTP, H.323, SIP et RTSP, qui utilisent une connexion de contrôle pour établir un flux de données sont aussi cassées par les appareils de NAT sur leur chemin. Cela parce que ces applications échangent des paramètres d'adresse et d'accès au sein de la session de contrôle pour établir des sessions de données et des orientations de sessions. Les NAT ne peuvent pas connaître les interdépendances des faisceaux de sessions et vont traiter chaque session comme étant sans relation les unes avec les autres. Dans ce cas, les applications peuvent échouer pour diverses raisons. Les deux raisons d'échec les plus vraisemblables sont :

(a) que les informations d'adressage dans la charge utile de contrôle sont spécifiques du domaine et ne sont plus valides lorsque le paquet sort du domaine d'origine, et

(b) que la session de contrôle permet aux sessions de données d'être générées dans une direction que le NAT ne va pas permettre.

Lorsque les noms du DNS sont utilisés dans la charge utile de contrôle, l'appareil de NAT en conjonction avec une ALG DNS peut être capable d'offrir la transparence de niveau application nécessaire, si le NAT n'a pas de contre indication avec l'orientation de la session de données. Cependant, l'utilisation des noms du DNS au lieu d'adresses IP spécifiques d'un domaine peut n'être pas une option pour beaucoup de ces applications (par exemple, FTP).

Lorsque un adressage spécifique du domaine est spécifié dans la charge utile, et lorsque la charge utile n'est pas chiffrée, une ALG peut dans certains cas être capable de faire le contournement nécessaire pour faire fonctionner l'application en transparence à travers les domaines. La complexité de l'ALG dépend de la connaissance de niveau application exigée pour traiter la charge utile et conserver l'état.

## 2.3 Applications d'homologue à homologue

Les applications d'homologue à homologue vont plus vraisemblablement échouer lorsque un NAT se trouve sur le chemin que des applications fondées sur une relation client-serveur. À la différence des applications client-serveur, les applications

d'homologue à homologue peuvent être générées par l'un ou l'autre des homologues. Lorsque les homologues sont répartis dans des domaines privés et publics, une session générée à partir d'un domaine externe est très semblable à la session provenant d'un hôte dans un domaine privé. Les homologues externes ne seront capables de localiser leurs homologues dans un domaine privé que lorsque ils connaissent à l'avance l'adresse IP allouée en externe ou le FQDN *(fully-qualified domain name = nom de domaine complet)*. La transposition de nom FQDN en adresse allouée ne peut se faire que pour autant que l'appareil de NAT sur le chemin prenne en charge l'ALG DNS. Des exemples d'applications d'homologue à homologue incluent des jeux interactifs, la téléphonie Internet et les protocoles fondés sur l'événement (tels que la messagerie instantanée).

C'est particulièrement un problème avec le NAT traditionnel et peut poser moins de problèmes avec les NAT bidirectionnels, où les sessions sont permises dans les deux directions.

Un contournement possible de ce type de problème avec le NAT traditionnel est que les hôtes privés conservent une connexion sortante avec un serveur qui agit comme représentant vis-à-vis de l'Internet mondial.

### 2.4 Fragmentation IP avec NAPT en chemin

La fragmentation IP avec un NAPT en chemin ne pose pas de problème avec une application seule, mais se fait sentir un peu partout à travers les applications TCP/UDP. Le problème est décrit en détails dans la [RFC3022]. En bref, le problème se pose comme suit. Disons que deux hôtes privés ont généré des paquets TCP/UDP fragmentés chez le même hôte de destination. Et il se trouve qu'ils utilisent le même identifiant de fragmentation. Lorsque l'hôte cible reçoit les deux datagrammes qui n'ont pas de relation entre eux, qui portent le même identifiant de fragmentation, et provenant de la même adresse d'hôte, l'hôte cible est incapable de déterminer à laquelle des deux sessions appartiennent les datagrammes. Par conséquent, les deux sessions vont être lésées.

### 2.5 Applications qui exigent la rétention de la transposition d'adresse

Le NAT va très vraisemblablement casser les applications qui exigent que la transposition d'adresse soit conservée à travers des sessions contiguës. Ces applications exigent que la transposition d'adresse privée en adresse externe soit conservée entre les sessions afin que la même adresse externe puisse être réutilisée pour les interactions de session ultérieures. Le NAT ne peut pas connaître cette exigence et peut réallouer l'adresse externe à des hôtes différents entre les sessions.

Essayer d'empêcher un NAT d'éliminer une transposition d'adresse exigerait un protocole d'extension de NAT à l'application qui lui permettrait d'informer l'appareil de NAT de la nécessité de conserver les transpositions. Autrement, une ALG peut être nécessaire pour interagir avec le NAT pour empêcher que celui-ci élimine la transposition d'adresse.

### 2.6 Applications qui exigent plus d'adresses publiques que disponible

C'est un problème lorsque le nombre d'hôtes privés est supérieur à celui des adresses externes disponibles pour transposer les adresses privées. Prenons l'exemple du service rlogin initié à partir d'un hôte dans un domaine privé pris en charge par un NAPT. Les clients de service Rlogin utilisent l'accès rlogin bien connu 512 comme identifiant d'accès TCP. Un seul hôte dans le domaine privé peut initier le service. C'est un cas d'essai d'utilisation d'un service qui exige fondamentalement plus d'adresses publiques qu'il n'en est de disponibles. Les appareils de NAT peuvent conserver les adresses, mais ils ne peuvent pas créer plus d'adresses.

## 3. Protocoles qui ne peuvent pas fonctionner avec un NAT en chemin

### 3.1 IPsec et IKE

Les NAT fonctionnent fondamentalement en modifiant les adresses de nœud d'extrémité (au sein de l'en-tête IP) en chemin. D'un autre côté, la norme IPsec AH [RFC2402] est explicitement conçue pour détecter les altérations de l'en-tête du paquet IP. De sorte que lorsque le NAT altère les informations d'adresse en chemin dans un en-tête IP, l'hôte de destination qui reçoit le paquet altéré va invalider le paquet car le contenu des en-têtes a été altéré. Il en résulte que le paquet sécurisé par IPsec AH et qui traverse un NAT ne va tout simplement pas atteindre l'application cible.

Les paquets chiffrés avec IPsec ESP ([RFC2406]) ne peuvent être altérés par des appareils de NAT en chemin que dans un nombre de cas limité. Dans le cas de paquets TCP/UDP, le NAT va avoir besoin de mettre à jour la somme de contrôle dans les en-têtes TCP/UDP, lorsque une adresse a changé dans l'en-tête IP. Cependant, comme l'en-tête TCP/UDP est chiffré par l'ESP, le NAT ne sera pas capable de faire cette mise à jour de somme de contrôle. Il en résulte que les paquets TCP/UDP chiffrés dans le mode de transport ESP, qui traversent un appareil de NAT, vont échouer à la validation de

somme de contrôle TCP/UDP à l'extrémité de réception et ne vont tout simplement pas atteindre l'application cible.

Le protocole d'échange de clé Internet (IKE, *Internet Key Exchange*) peut éventuellement passer des adresses IP comme identifiants de nœud durant les modes Main, Aggressive et Quick. Pour qu'une négociation IKE passe correctement à travers un NAT, ces charges utiles devraient être modifiées. Cependant, ces charges utiles sont souvent protégées par un hachage ou obscurcies par le chiffrement. Même dans le cas où les adresses IP ne sont pas utilisées dans les charges utiles IKE et où une négociation IKE pourrait survenir sans interruption, il y a des difficultés à conserver la transposition d'adresse de privée en externe sur un NAT entre le moment où IKE a achevé la négociation et celui où IPsec utilise la clé sur une application. Finalement, l'utilisation de IPsec de bout en bout est de toutes façons sévèrement handicapée, comme on l'a décrit précédemment.

Pour toutes ces raisons pratiques, IPsec de bout en bout est impossible à réaliser avec un NAT sur le chemin.

### 3.2 Kerberos 4

Les tickets Kerberos 4 sont chiffrés. Donc, une ALG ne peut pas être écrite. Lorsque le centre de distribution de clés (KDC) reçoit une demande de ticket, il inclut l'adresse IP de source dans le ticket retourné. Tous les services Kerberos 4 ne vérifient pas en fait les adresses IP de source. AFS est un bon exemple d'un service Kerberos 4 qui ne le fait pas. Les services qui ne vérifient pas ne font pas les difficiles au sujet des appareils de NAT sur le chemin. Les tickets Kerberos sont liés à l'adresse IP qui a demandé le ticket et au service avec lequel le ticket sera utilisé.

Le ticket K4 (de réponse) contient une seule adresse IP qui décrit l'interface utilisée par le client pour restituer le ticket depuis le TGT du point de vue du KDC. Cela fonctionne bien si le KDC est au delà d'une passerelle de NAT et tant que les services Kerberos sont aussi derrière une passerelle de NAT. L'utilisateur final sur le réseau privé ne va pas remarquer de problème.

Il faut aussi faire attention que le NAT utilise la même transposition d'adresse pour l'hôte privé pour la connexion entre le client et le KDC que pour la connexion entre le client et le serveur d'application. Une façon de contourner ce problème serait de garder une connexion arbitraire ouverte pour le serveur distant durant la durée de vie du ticket, de façon à ne pas laisser le NAT abandonner le lien d'adresse. Autrement, une ALG devra être déployée pour s'assurer que le NAT ne va pas changer les liens d'adresse durant la durée de vie d'un ticket et entre le moment où un ticket est produit à l'hôte privé et le moment où le ticket est utilisé par l'hôte privé.

Mais le ticket sera valide à partir de tout hôte au sein du domaine privé du NAPT. Sans NAPT, un attaquant a besoin d'être capable d'usurper l'adresse IP de source d'une connexion qui est en cours d'établissement afin d'utiliser un ticket volé sur un hôte différent. Avec le NAPT, tout ce que l'attaquant a besoin de faire à partir du domaine privé du NAPT est simplement de s'assurer de la possession d'un ticket. Bien sûr, cela suppose que le domaine privé du NAPT ne soit pas un réseau de confiance – ce qui ne surprendra pas, car beaucoup d'attaques proviennent de l'intérieur d'une organisation.

### 3.3 Kerberos 5

Tout comme avec Kerberos 4, les tickets Kerberos 5 sont chiffrés. Donc, une ALG ne peut pas être écrite.

Dans Kerberos 5, le client spécifie une liste d'adresses IP pour lesquelles le ticket devrait être valide, ou il peut demander un ticket valide pour toutes les adresses IP. En demandant un ticket pour toutes les adresses IP ou un ticket contenant l'adresse de l'appareil NAPT, on peut obtenir que krb5 fonctionne avec un appareil NAPT, bien que cela ne soit pas très transparent (cela exige que les clients se comportent différemment de ce qu'ils feraient autrement). La mise en œuvre du MIT krb5 1.0 n'avait aucune possibilité de configuration pour les adresses IP que demandait le client (il demandait toujours l'ensemble de ses adresses d'interface) et n'interagissait pas bien avec le NAT. La mise en œuvre de MIT krb5 1.1 vous permet de mettre "noaddresses" quelque part dans krb5.conf pour demander des tickets valides sur toutes les adresses IP.

Le ticket K5 (de réponse) contient les adresses IP, telles que demandées par le nœud client, à partir desquelles le ticket sera considéré comme valide. Si les services auxquels on accède avec l'authentification Kerberos sont sur le côté public du NAT, l'authentification Kerberos va alors échouer parce que l'adresse IP utilisée par le NAT (NAT de base ou NAPT) n'est pas sur la liste des adresses acceptables.

Il y a dans Kerberos 5 deux astuces qui réduisent la sécurité des tickets. La première est de faire que les clients dans le domaine NAPT privé spécifient l'adresse IP publique du NAPT dans la liste IP du ticket. Mais cela conduit au même problème de sécurité qu'on a exposé pour K4. De plus, il n'est pas évident pour le client dans le domaine privé de trouver l'adresse IP publique du NAPT. Cela entraînerait un changement du comportement de l'application chez l'hôte d'extrémité.

La seconde méthode est de retirer toutes les adresses IP des tickets K5 mais cela rend alors le vol du ticket encore pire car

les tickets peuvent être utilisés à partir de n'importe où, et non plus seulement de l'intérieur du réseau privé.

### 3.4 Système X Windowing et X-term/Telnet

Le système X Windowing [RFC1198] se fonde sur TCP. Cependant, les relations client-serveur avec ces applications sont inversées par rapport à la plupart des autres applications. Le X serveur ou le serveur Open-windows est l'unité affichage/souris/clavier (c'est-à-dire, celle qui commande l'interface Windows réelle). Les clients sont les programmes d'application qui pilotent l'interface Windows.

Certaines machines font fonctionner plusieurs serveurs X Windows sur la même machine. Les premiers serveurs X Windows sont sur l'accès TCP 6000. Le premier serveur Open Windows peut être à l'accès 6000 ou à l'accès 2000 (plus souple). On se réfèrera principalement au système X windowing pour l'illustration de notre propos.

X-term transmet les adresses IP du client au serveur pour les besoins du réglage de la variable DISPLAY *(affichage)*. Lorsque elle est établie, la variable DISPLAY est utilisée pour les connexions ultérieures des clients X sur l'hôte avec un serveur X sur la station de travail. La variable DISPLAY est envoyée en ligne durant les négociations TELNET comme :

DISPLAY=<adresse_ip_locale>:<serveur>.<affichage>

Où <adresse_ip_locale> est restitué en cherchant l'adresse IP locale associée à la prise utilisée pour se connecter au <serveur>. Le <serveur> détermine quel accès (6000 + <serveur>) devrait être utilisé pour faire la connexion. <affichage> est utilisé pour indiquer quel moniteur rattaché au X serveur devrait être utilisé mais n'a pas d'importance dans cet exposé.

Le <adresse_ip_locale> utilisé n'est pas un nom DNS parce que :
- Il n'est pas possible à la machine locale de savoir son nom DNS sans effectuer une recherche DNS inversée sur l'adresse IP locale
- Il n'est pas garanti que le nom retourné par une recherche DNS inverse se retranspose en fait sur l'adresse IP locale.
- Enfin, sans DNSSEC, il peut n'être pas sûr d'utiliser les adresses DNS parce que elles peuvent être facilement usurpées. Le NAT et l'ALG DNS ne peuvent pas fonctionner si DNSSEC n'est pas désactivée.

Une utilisation courante de cette application est celle où des gens numérotent dans des bureaux d'entreprises à partir de leurs terminaux X à la maison. Disons que le client X fonctionne sur un hôte du côté public du NAT et le serveur X fonctionne sur un hôte qui est sur le côté privé du NAT. La variable DISPLAY est transmise en ligne à l'hôte sur lequel fonctionne le client X d'une certaine façon. Le processus qui transmet le contenu de la variable DISPLAY ne connaît pas l'adresse du NAT.

Si le canal qui transmet la variable DISPLAY n'est pas chiffré, l'appareil de NAT pourrait solliciter l'aide d'une ALG pour remplacer l'adresse IP et configurer un accès dans la gamme d'affichage valide (les accès 6000 et au-dessus) pour agir comme une passerelle. Autrement, le NAT peut être configuré pour écouter les connexions entrantes et fournir l'accès aux serveurs X, sans requérir une ALG. Mais cette approche augmente les risques pour la sécurité en donnant accès au serveur X qui ne serait autrement pas disponible. Lorsque l'ALG manipule les adresses IP, il ne sera pas non plus possible d'utiliser d'autre méthode d'autorisation X que MIT-MAGIC-COOKIE-1. MIT-MAGIC-COOKIE-1 est la moins sûre de toutes les méthodes d'autorisation X documentées.

Lorsque START_TLS est utilisé, il peut y avoir des problèmes de vérification du certificat de client causés par le fait que le NAT dépend des informations fournies dans le certificat.

### 3.5 RSH/RLOGIN

RSH utilise plusieurs sessions pour prendre en charge des flux séparés pour stdout et stderr. Un numéro d'accès aléatoire est transmis en ligne du client au serveur pour être utilisé comme accès stderr. La prise stderr est une connexion de retour du serveur au client. Et à la différence de FTP, il n'y a pas de mode équivalent à PASV. Pour le NAT traditionnel, c'est un problème car le NAT traditionnel ne permettrait pas de sessions entrantes.

RLOGIN n'utilise pas de sessions multiples. Mais les versions de RSH et de RLOGIN protégées par Kerberos ne vont pas fonctionner dans un environnement de NAT à cause des problèmes de ticket et de l'utilisation de plusieurs sessions.

# 4. Protocoles qui peuvent fonctionner avec l'aide d'une ALG

Le présent document s'adresse principalement aux problèmes associés aux NAT traditionnels, en particulier les NAPT.

## 4.1 FTP

FTP [RFC0959] est une application fondée sur TCP, utilisée pour transférer de façon fiable des fichiers entre deux hôtes. FTP utilise une approche de sessions en faisceaux pour réaliser cela.

FTP est initié par un client qui accède au numéro d'accès bien connu 21 sur le serveur FTP. C'est ce qu'on appelle la session de contrôle FTP. Souvent, une session de données supplémentaire accompagne la session de contrôle. Par défaut, la session de données sera de l'accès TCP 20 sur le serveur au client d'accès TCP utilisé pour initier la session de contrôle. Cependant, les accès de session de données peuvent être altérés au sein des sessions de contrôle FTP qui utilisent les commandes et réponses PORT et PASV codées en ASCII.

Disons qu'un client FTP est un réseau privé pris en charge par un NAT. Une ALG FTP sera nécessaire pour surveiller la session de contrôle FTP (pour les deux modes PORT et PASV) pour identifier les numéros d'accès de session de données FTP et modifier l'adresse et le numéro d'accès privés avec le numéro d'accès et l'adresse valides en externe. De plus, les numéros de séquence et d'accusé de réception, la somme de contrôle TCP, la longueur du paquet IP et sa somme de contrôle doivent être mis à jour. Par conséquent, les numéros de séquence dans tous les paquets suivants pour ce flux doivent être ajustés ainsi que les champs et somme de contrôle ACK de TCP.

Dans de rares cas, l'augmentation de la taille du paquet pourrait causer le dépassement de la MTU de la liaison de transport. Le paquet va alors devoir être fragmenté, ce qui pourrait affecter les performances. Ou, si le paquet a le bit DF établi, il sera rejeté par ICMP et l'hôte d'origine devra alors effectuer la découverte de la MTU du chemin. Cela peut avoir un effet néfaste sur les performances.

On notera cependant que si le canal de commandes de contrôle est sécurisé, il sera impossible à une ALG de mettre à jour les adresses IP dans l'échange de commandes.

Lorsque AUTH est utilisé avec Kerberos 4, Kerberos 5, et TLS, les mêmes problèmes surviennent avec FTP que ceux qui surviennent avec X-Term/Telnet.

Enfin, il est intéressant de noter que la section 4 de la RFC2428 (extensions à FTP pour IPv6 et les NAT) décrit comment utiliser la nouvelle commande d'accès FTP (EPSV ALL) pour permettre aux appareils de NAT de passer rapidement au protocole FTP, ce qui élimine tout autre traitement à travers une ALG, si le serveur distant accepte "EPSV ALL".

## 4.2 RSVP

RSVP [RFC2205] est positionné dans la pile de protocoles à la couche transport, et fonctionne par dessus IP (IPv4 ou IPv6). Cependant, à la différence des autres protocoles de transport, RSVP ne transporte pas de données d'application mais agit plutôt comme les autres protocoles de contrôle Internet (par exemple, ICMP, IGMP, protocoles d'acheminement). Les messages RSVP sont envoyés bond par bond entre les routeurs à capacité RSVP comme des datagrammes IP bruts qui utilisent le numéro de protocole 46. Il est prévu que les datagrammes IP bruts devraient être utilisés entre les systèmes d'extrémité et le routeur de premier bond (ou le dernier routeur). Cependant, cela peut n'être pas toujours possible car tous les systèmes ne peuvent pas faire de l'entrée/sortie de réseau brute. À cause de cela, il est possible d'encapsuler les messages RSVP au sein de datagrammes UDP pour la communication entre systèmes d'extrémité. Les messages RSVP encapsulés dans UDP sont envoyés à l'accès 1698 (si ils sont envoyés par un système d'extrémité) ou à l'accès 1699 (si ils sont envoyés par un routeur à capacité RSVP). Pour avoir plus d'informations en ce qui concerne l'encapsulation dans UDP des messages RSVP, consulter l'Appendice C de la [RFC2205].

Une session RSVP, qui est un flux de données avec une destination et un protocole de couche transport particuliers, se définit par :

Une adresse de destination – l'adresse IP de destination pour les paquets de données. Cela peut être une adresse d'envoi individuel ou une adresse de diffusion groupée.

Un identifiant de protocole – c'est l'identifiant de protocole IP (par exemple, UDP ou TCP).

Un accès de destination – un accès de destination généralisé qui est utilisé pour démultiplexer à la couche au-dessus de IP.

Les appareils de NAT présentent des problèmes particuliers lorsque ils se trouvent prendre en charge RSVP. Deux problèmes se posent :

1. Les objets de message RSVP peuvent contenir des adresses IP. Il en résulte qu'une ALG RSVP doit être capable de remplacer les adresses IP fondées sur la direction et le type du message. Par exemple, si un envoyeur externe se trouvait envoyer un message RSVP Path à un receveur interne, la session RSVP spécifiera l'adresse IP que l'envoyeur externe croit être l'adresse IP du receveur interne. Cependant, lorsque le message Path RSVP atteint l'appareil de NAT, la session RSVP doit être changée pour refléter l'adresse IP qui est utilisée en interne pour le receveur. Des actions similaires doivent être prises pour tous les objets de message qui contiennent des adresses IP.

2. RSVP donne un moyen, l'objet RSVP Integrity, pour garantir l'intégrité des messages RSVP. Le problème est que, à cause du point précédent, un appareil de NAT doit être capable de changer les adresses IP au sein des messages RSVP. Cependant, lorsque c'est fait, l'objet RSVP Integrity n'est plus valide car le message RSVP a été changé. Donc, une ALG RSVP ne va pas fonctionner lorsque l'objet RSVP Integrity est utilisé.

### 4.3 DNS

Le DNS est un protocole fondé sur TCP/UDP. Les noms de domaines sont un problème pour les hôtes qui utilisent des serveurs DNS locaux dans le domaine privé du NAT. La transposition du nom DNS en adresse pour les hôtes dans un domaine privé devrait être configurée sur un serveur de noms d'autorité au sein du domaine privé. On accèderait de la même façon à ce serveur par des hôtes externes et internes pour les résolutions de noms. Une ALG DNS serait nécessaire pour effectuer les conversions d'adresse en nom sur des interrogations et réponses du DNS. La [RFC2694] décrit en détails l'ALG DNS. Si les paquets DNS sont chiffrés/authentifiés selon DNSSEC, l'ALG DNS va alors échouer parce qu'elle ne sera pas capable d'effectuer les modifications de la charge utile.

Les applications qui utilisent un résolveur DNS pour résoudre un nom DNS en une adresse IP, supposent la disponibilité de l'allocation d'adresse pour réutilisation par la session spécifique de l'application. Il en résulte que l'ALG DNS sera obligée de garder l'adresse allouée (entre les adresses privées et externes) valide pour une durée préconfigurée, après l'interrogation du DNS.

Autrement, si il n'est pas besoin d'un serveur de noms au sein du domaine privé, les hôtes du domaine privé pourraient simplement pointer sur un serveur de noms externe pour une recherche de nom externe. Aucune ALG n'est requise lorsque le serveur de noms est situé dans un domaine externe.

### 4.4 SMTP

SMTP [RFC0822] est un protocole fondé sur TCP, utilisé par des programmes de messagerie électronique sur Internet tels que sendmail pour envoyer des messages électroniques fondés sur TCP à l'accès bien connu 25. Le serveur de messagerie peut être situé au sein d'un domaine privé ou en dehors. Mais, le serveur doit avoir un nom et une adresse mondiale alloués, accessibles par les hôtes externes. Lorsque le serveur de messagerie est situé au sein d'un domaine privé, les sessions SMTP entrantes doivent être redirigées sur l'hôte privé à partir de son adresse externe allouée. Aucune transposition particulière n'est requise lorsque le serveur de messagerie est situé dans le domaine externe.

Généralement parlant, les systèmes de messagerie sont configurés de telle façon que tous les usagers spécifient une seule adresse centralisée (telle que fooboo@compagnie.com) au lieu d'inclure des hôtes individuels (tels que fooboo@hôteA.compagnie.com). L'adresse centrale doit avoir un enregistrement MX spécifié dans le serveur de noms DNS accessible par les hôtes externes.

Dans la majorité des cas, les messages électroniques ne contiennent pas de référence aux adresses IP privées ou aux liaisons aux données de contenu via des noms qui ne sont pas visibles à l'extérieur. Cependant, certains messages électroniques contiennent des adresses IP des MTA *(Mail Transport Agent = agent de transport de messagerie)* qui relaient le message dans le champ "Received: ". Certains messages électroniques utilisent les adresses IP au lieu du FQDN pour des besoins de débogage ou à cause d'un manque d'enregistrement DNS, dans le champ "Mail From: ".

Si un ou plusieurs MTA se trouvent situés derrière un NAT dans un domaine privé, et si les messages ne sont pas sécurisés par signature ou clé de chiffrement, une ALG SMTP peut être utilisée pour traduire les informations d'adresse IP enregistrées par les MTA. Si les MTA ont une transposition d'adresse statique, la traduction sera valide à travers les domaines pendant longtemps.

La capacité à retracer le chemin des messages peut être altérée ou empêchée par un seul NAT, sans l'ALG. Cela peut causer des problèmes lors du débogage de problèmes de messagerie ou pour retrouver la trace d'utilisateurs indélicats de la messagerie.

### 4.5 SIP

SIP [RFC2553] peut fonctionner sur TCP ou sur UDP, mais par défaut sur le même accès 5060.

Lorsque elle est utilisée avec UDP, une réponse à une demande SIP ne va pas à l'accès de source dont venait la demande. Le message SIP contient plutôt le numéro d'accès où la réponse devrait être envoyée. SIP fait usage de l'erreur ICMP Accès injoignable dans la réponse pour demander les transmissions. Les messages de demande sont normalement envoyés sur la prise connectée. Si les réponses sont envoyées à l'accès de source qui figure dans la demande, chaque filière de demandes devrait écouter sur la prise d'où elle a envoyé la demande. Cependant, en permettant que les réponses ne viennent que sur un seul accès, une seule filière peut être utilisée pour écouter.

Un serveur peut préférer placer l'accès de source de chaque prise connectée dans le message. Chaque filière peut alors écouter séparément si il y a des réponses. Comme le numéro d'accès pour une réponse ne peut pas aller à l'accès de source de la demande, SIP ne va normalement pas traverser un NAT et va donc exiger une ALG SIP.

Les messages SIP portent des contenus arbitraires, qui sont définis par un type MIME. Pour les sessions multi supports, c'est normalement le protocole de description de session (SDP) [RFC2327]. SDP peut spécifier des adresses IP ou des accès à utiliser pour les échanges multi supports. Ceux-ci peuvent perdre toute signification lors de la traversée d'un NAT. Donc l'ALG SIP devra avoir l' intelligence pour déchiffrer et traduire les informations qui relèvent du domaine.

SIP porte des URL dans ses champs Contact, To et From qui spécifient des adresses de signalisation. Ces URL peuvent contenir des adresses IP ou des noms de domaines dans la portion accès d'hôte de l'URL. Ils peuvent n'être plus valides une fois qu'ils ont traversé un NAT.

Comme solution de remplacement à une ALG SIP, SIP accepte un serveur mandataire qui peut co-résider avec le NAT et fonctionne sur l'accès du NAT qui a une signification mondiale. Un tel mandataire va avoir une configuration spécifique localement.

### 4.6 RealAudio

En mode par défaut, les clients RealAudio (disons, dans un domaine privé) accèdent à TCP par l'accès 7070 pour initier une conversation avec un serveur RealAudio (disons qu'il est situé sur un domaine externe) et pour échanger des messages de contrôle durant l'exécution (par exemple, faire une pause dans le flux audio ou l'arrêter). Les paramètres de la session audio sont incorporés dans la session de contrôle TCP comme flux d'octets.

Le trafic audio réel est porté dans la direction opposée à celle des paquets entrants fondés sur UDP (générés par le serveur) dirigés sur des accès dans la gamme de 6970 à 7170.

Il en résulte que RealAudio est cassé par défaut sur un appareil de NAT traditionnel. On peut contourner cela en faisant examiner par l'ALG le trafic TCP pour déterminer les paramètres de la session audio et permettre de façon sélective les sessions UDP entrantes pour les accès admis dans la session de contrôle TCP. Autrement, l'ALG pourrait simplement rediriger toutes les sessions UDP entrantes dirigées sur les accès 6970 à 7170 sur l'adresse du client dans le domaine privé.

Pour un NAT bidirectionnel, il n'y a pas besoin d'une ALG. Le NAT bidirectionnel peut simplement traiter chacune des sessions TCP et UDP comme deux sessions sans relation entre elles et effectuer les traductions de niveau en-tête IP et TCP/UDP.

Le lecteur peut contacter RealNetworks pour avoir des lignes directrices détaillées sur la façon dont leurs applications peuvent fonctionner, en traversant des appareils de NAT et de pare-feu.

### 4.7 H.323

H.323 est complexe ; il utilise des accès dynamiques, et comporte plusieurs flux UDP. Voici un résumé des questions qui se posent :

Un appel H.323 est constitué de nombreuses connexions simultanées différentes. Au moins deux des connexions sont TCP. Pour une conférence en audio seul, il peut y avoir jusqu'à quatre "connexions" UDP différentes établies.

Toutes les connexions excepté une sont faites sur des accès éphémères (dynamiques).

Les appels peuvent être initiés à partir du domaine privé aussi bien qu'externe. Pour que le mode conférence soit utile, les utilisateurs externes doivent être capables d'établir les appels directement avec les systèmes portables des utilisateurs internes.

Les adresses et les numéros d'accès sont échangés au sein du flux des données de la connexion qui est l'avant dernière plus élevée. Par exemple, le numéro d'accès pour la connexion H.245 est établi au sein du flux de données Q.931. (Cela rend les choses particulièrement difficiles pour l'ALG, qui va devoir modifier les adresses au sein de ces flux de données.) Pour rendre les choses encore pires, il est possible en Q.931, par exemple, de spécifier que la connexion H.245 devrait être sécurisée (chiffrée). Si une session est chiffrée, il est impossible à l'ALG de déchiffrer le flux de données, à moins qu'elle n'ait accès à la clé partagée.

La plupart des informations de contrôle sont codées en ASN.1 (seules les informations d'utilisateur à utilisateur au sein des unités de données de protocole (PDU, *Protocol Data Unit*) de Q.931, sont codées en ASN.1 (les autres parties de chaque PDU Q.931 ne sont pas codées). Pour ceux qui ne sont pas familiers de l'ASN.1, il suffit de dire qu'il a un schéma de codage complexe, qui ne se termine pas avec des décalages d'octet fixes pour les informations d'adresse. En fait, la même version de la même application qui se connecte sur la même destination peut négocier d'inclure différentes options, ce qui change les décalages d'octet.

Ci-dessous figure l'échange de protocole pour un appel H.323 normal entre l'usager A et l'usager B. L'adresse IP de A est 88.88.88.88 et l'adresse IP de B est 99.99.99.99. Noter que les messages Q.931 et H.245 sont codés en ASN.1 dans la charge utile d'un paquet RTP. De sorte que pour accomplir une connexion à travers un appareil de NAT, une ALG H.323 sera obligée d'examiner le paquet, de décoder l'ASN.1, et de traduire les diverses adresses IP de contrôle H.323.

**Utilisateur A** **Utilisateur B**

A établit une connexion avec B sur l'accès Q.931 bien connu (1720)

---------->

Établissement Q.931 de l'adresse de l'appelant = 88.88.88.88
Accès appelant = 1120
Adresse de l'appelé = 99.99.99.99
Accès de l'appelé = 1720

<----------

Alerte Q.931

<----------

Q.931 connecte l'adresse H.245 = 99.99.99.99
Accès H.245 = 1092

L'usager A établit la connexion avec l'usager B à 99.99.99.99, accès 1092

<---------->

Plusieurs messages H.245 sont échangés (Ensemble de capacités du terminal, Détermination du maître et de l'esclave et leurs accusés de réception respectifs)

<----------

H.245 ouvre le canal logique, canal = 257
Adresse RTCP = 99.99.99.99
Accès RTCP = 1093

---------->

H.245 accuse réception de l'ouverture du canal logique, canal = 257
Adresse RTP = 88.88.88.88
Accès RTP = 2002
(C'est là que l'usager A voudrait que les données RTP soient envoyées à )
adresse RTCP = 88.88.88.88
accès RTCP = 2003

---------->

H.245 ouvre le canal logique, canal = 257
Adresse RTCP = 88.88.88.88
Accès RTCP = 2003

<----------

H.245 accuse réception de l'ouverture du canal logique, canal = 257
Adresse RTP = 99.99.99.99
Accès RTP = 1092
(C'est là que l'usager B voudrait que les données RTP soient envoyées à)
adresse RTCP = 99.99.99.99
accès RTP = 1093

Noter aussi que si une passerelle H.323 réside dans la limite d'un NAT, l'ALG devra connaître les divers schémas de découverte de passerelle et s'adapter aussi à ces schémas. Ou si juste l'hôte/terminal H.323 est dans les limites du NAT et essaye de s'enregistrer auprès d'un portier, les informations IP dans les messages d'enregistrement devront être traduits par le NAT.

### 4.8 SNMP

SNMP est un protocole de gestion de réseau fondé sur UDP. La charge utile SNMP peut contenir des adresses IP ou peut se référer à des adresses IP à travers un indice dans un tableau. Il en résulte que lorsque des appareils au sein d'un réseau privé sont gérés par un nœud extérieur, les paquets SNMP qui transitent par un appareil de NAT peuvent contenir des informations qui ne sont plus pertinentes dans le domaine externe. Dans certains cas, comme décrit dans la [RFC2962], une ALG SNMP peut être utilisée pour convertir de façon transparente les adresses spécifiques d'un domaine en adresses uniques au monde. Une telle ALG suppose une transposition statique d'adresse et un NAT bidirectionnel. Il ne peut fonctionner que pour l'ensemble de types de données (conventions textuelles) comprises par la mise en œuvre d'ALG SNMP et pour un ensemble donné de modules de MIB *(base de données d'informations de gestion)*. De plus, le remplacement des adresses dans la charge utile SNMP peut conduire à des échecs de communication dus aux changements de taille du message ou aux changements dans l'ordre lexicographique.

Rendre les ALG SNMP complètement transparentes à toutes les applications de gestion n'est pas une tâche réalisable. Les ALG vont avoir des problèmes avec les dispositifs de sécurité de SNMPv3, lorsque l'authentification (et en option la confidentialité) est activée, sauf si l'ALG a accès aux clés de sécurité. La [RFC2993] donne aussi des indications sur les problèmes potentiels avec la gestion SNMP via un NAT.

Autrement, les mandataires SNMP, tels que définis dans la [RFC2573], peuvent être utilisés en conjonction avec un NAT pour transmettre des messages SNMP à des moteurs SNMP externes (et vice versa). Les mandataires SNMP sont taillés sur mesure pour le contexte du domaine privé et peuvent donc fonctionner indépendamment des types d'objets gérés spécifiques auxquels ils ont accès. La solution du mandataire exige que l'application à gestion externe soit au courant de l'existence du mandataire de transmission et que les nœuds individuels gérés soient configurés pour diriger leur trafic SNMP (notifications et demandes) au mandataire de transmission.

## 5. Protocoles conçus explicitement pour fonctionner avec des NAT en chemin

### 5.1 Jeux Activision

Les jeux Activision ont été conçus pour être compatibles avec les NAT de façon à n'avoir pas besoin d'une ALG pour que les jeux fonctionnent de façon transparente à travers les appareils de NAT traditionnels. Les joueurs au sein d'un domaine privé peuvent jouer avec d'autres joueurs dans le même domaine ou dans un domaine externe. Le protocole des jeux Activision est breveté et se fonde sur UDP. Le serveur d'adresse utilise un numéro d'accès UDP de 21157 et il est supposé être situé sur le domaine d'adresse mondial.

Les joueurs se connectent d'abord au serveur d'adresse, et envoient leurs informations d'adresse IP privée (telles que l'adresse IP privée et le numéro d'accès UDP) dans le message de connexion initial. Le serveur note les informations d'adresse privée à partir du message de connexion et les informations d'adresse externe à partir des en-têtes IP et UDP. Le serveur envoie alors les informations d'adresse privée et externe du joueur à tous les autres joueurs homologues. À ce moment là, chaque joueur connaît les informations d'adresse privée et publique de tous ses homologues. Ensuite, chaque client ouvre une connexion symétrique directe avec chaque autre joueur et utilise la première adresse (privée ou externe) qui fonctionne.

Maintenant, les clients peuvent avoir une session directement avec les autres clients (ou ils peuvent avoir une session avec d'autres clients via le serveur de jeux). Le point clé est de permettre la réutilisation du même tuplet (adresse mondiale, accès UDP alloué) que celui utilisé pour la connexion initiale avec le serveur de jeux pour toutes les connexions suivantes avec le client. Un joueur est reconnu par le couple unique de (adresse privée, accès UDP) ou (adresse mondiale, numéro UDP alloué) par tous les autres joueurs. Ainsi, la liaison entre les tuplets devrait rester inchangée sur le NAT, tant que le joueur est en session avec un ou plusieurs autres joueurs.

Ouvrir une connexion avec un serveur de jeux dans un domaine externe à partir d'un hôte privé ne pose pas de problème. Tout ce que les NAT vont avoir à faire est d'assurer la transparence de l'acheminement et de conserver la même liaison entre adresse privée et adresse externe tant qu'il y a un minimum d'une session de jeu avec un nœud externe. Mais, une configuration de NAPT doit permettre plusieurs connexions UDP simultanées sur la même adresse mondiale allouée /accès.

L'approche ci-dessus pose quelques problèmes. Par exemple, un client pourrait essayer de contacter une adresse privée, mais cette adresse privée pourrait être utilisée en local, alors que c'est l'adresse privée sur quelque autre domaine qu'on voulait. Si le nœud contacté à tort a quelque autre service ou aucun service enregistré pour l'accès UDP, les messages Activision de connexion sont supposés être tout simplement abandonnés. Dans le cas peu vraisemblable ou une application enregistrée choisirait d' interpréter le message, les résultats peuvent être imprévisibles.

Le lecteur peut se référer à Activision pour les informations détaillées brevetées sur la fonction et le concept de ce protocole.

## 6. Remerciements

Les auteurs tiennent à exprimer leurs sincères remerciements à Bernard Aboba, Bill Sommerfield, Dave Cridland, Greg Hudson, Henning Schulzrine, Jeffrey Altman, Keith Moore, Thomas Narten, Vernon Shryver et aux autres qui ont fourni des apports précieux à la préparation du présent document. Des remerciements tout particuliers à Dan Kegel pour son explication de la méthodologie de conception des jeux Activision.

## 7. Considérations pour la sécurité

Les considérations pour la sécurité soulignées dans [NAT-TERM] sont pertinentes pour tous les appareils de NAT. Le présent document n'ajoute pas de considérations supplémentaires pour la sécurité.

## 8. Références

[H.323] UIT-T GT16 H.323, contribution Intel, "H.323 and Firewalls", Dave Chouinard, John Richardson, Milind Khare (avec l'assistance de Jamie Jason).

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC0959] J. Postel et J. Reynolds, "Protocole de transfert de fichiers (FTP)", STD 9, octobre 1985.

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", , STD 13, novembre 1987.

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", RFC1035, STD 13, novembre 1987.

[RFC1198] R. Scheifler, "FAQ sur le système X Window", FYI0006, novembre 1990. *(Info)*

[RFC1918] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. de Groot, et E. Lear, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2101] B. Carpenter, J. Crowcroft, Y. Rekhter, "Comportement actuel des adresses IPv4", février 1997. *(Information)*

[RFC2205] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495) *(P.S.)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir RFC4303)*

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Information)*

[RFC2553] R. Gilligan, S. Thomson, J. Bound, W. Stevens, "Extensions de base d'interface de prise pour IPv6", mars 1999. (*Obsolète, voir* RFC3493) (*MàJ par* RFC3152) *(Information)*

[RFC2573] D. Levi, P. Meyer, B. Stewart, "Applications SNMP", avril 1999. (*Obsolète, voir* RFC3413) *(D.S.)*

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", , août 1999. *(Information)*

[RFC2694] P. Srisuresh, G. Tsirtsis, P. Akkiraju, A. Heffernan, "Extensions du DNS aux traducteurs d'adresse réseau (DNS_ALG)", septembre 1999. *(Information)*

[RFC2709] P. Srisuresh, "Modèle de sécurité avec IPsec en mode tunnel pour les domaines de NAT", octobre 1999. *(Information)*

[RFC2962] D. Raz, J. Schoenwaelder, B. Sugla, "Passerelle de niveau application pour la traduction d'adresse de charge utile dans SNMP", octobre 2000. *(Information)*

[RFC2993] T. Hain, "Implications architecturales des traducteurs d'adresse réseau (NAT)", novembre 2000. *(Information)*

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

## Adresse des auteurs

Matt Holdrege
ipVerse
223 Ximeno Ave.
Long Beach, CA 90803
USA
mél : matt@ipverse.com

Pyda Srisuresh
Jasmine Networks, Inc.
3061 Zanker Road, Suite B
San Jose, CA 95134
téléphone : (408) 895-5032
mél : srisuresh@yahoo.com

## Déclaration de droits de reproduction



## Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.