Groupe de travail Réseau
Request for Comments : 3022
RFC rendue obsolète : 1631
Catégorie : Information

P. Srisuresh, Jasmine Networks
K. Egevang, Intel Corporation
janvier 2001
Traduction Claude Brière de L'Isle

Traduction d'adresse réseau IP traditionnelle (NAT traditionnelle)

Préface
Le fonctionnement de NAT décrit dans le présent document étend la traduction d'adresse introduite dans la RFC1631 et inclut un nouveau type de traduction d'adresse réseau et d'accès TCP/UDP. De plus, le présent document corrige l'algorithme d'ajustement de somme de contrôle publié dans la RFC1631 et tente de discuter en détails du fonctionnement et des limitations de la NAT.

Résumé
La traduction d'adresse réseau de base ou NAT de base est une méthode par laquelle les adresses IP sont transposées d'un groupe à un autre, de façon transparente pour l'utilisateur final. La traduction d'accès d'adresse réseau, ou NAPT, est une méthode par laquelle de nombreuses adresses réseau et leurs accès TCP/UDP (protocole de contrôle de transmission/protocole de datagramme d'utilisateur, TU) sont traduits en une seule adresse réseau et ses accès TCP/UDP. Ensemble, ces deux opérations, qu'on appelle NAT traditionnelle, fournissent un mécanisme pour connecter un domaine avec des adresses privées en un domaine externe avec des adresses enregistrées uniques au monde.

1. Introduction

Le besoin de traduction d'adresse IP survient lorsque les adresses IP internes d'un réseau ne peuvent pas être utilisées en dehors de ce réseau pour des raisons de confidentialité ou parce qu'elles sont invalides à l'extérieur du réseau.

La topologie du réseau en dehors d'un domaine local peut différer de nombreuses façons. Les consommateurs peuvent changer de fournisseur, les cœurs de réseau des compagnies peuvent être réorganisés, ou des fournisseurs peuvent fusionner ou se partager. Chaque fois que change dans le temps la topologie externe, les affectations d'adresse aux nœuds qui sont au sein du domaine local doivent aussi changer pour refléter les changements externes. Les changements de ce type peuvent être cachés aux usagers de l'intérieur du domaine en centralisant les changements sur un seul routeur de traduction d'adresse.

La traduction d'adresse de base va permettre (dans beaucoup de cas, sauf comme noté dans [NAT-TERM] et à la section 6 du présent document) aux hôtes dans un réseau privé d'accéder en toute transparence au réseau externe et permettre l'accès de l'extérieur à des hôtes locaux choisis. Les organisations qui ont établi un réseau pour une utilisation interne prédominante, avec un besoin occasionnel d'accès externe, sont de bonnes candidates pour ce schéma.

Beaucoup d'utilisateurs des professions libérales et travailleurs à domicile (SOHO, *Small Office, Home Office*) et d'employés télécommunicants ont plusieurs nœuds réseau dans leur bureau, avec des applications TCP/UDP, mais une seule adresse IP allouée à leur routeur d'accès distant par leur fournisseur de service pour accéder aux réseaux distants. Cette communauté toujours croissante d'utilisateurs d'accès distant bénéficie de NAPT, qui permet à plusieurs nœuds dans n réseau local d'accéder simultanément à des réseaux distants en utilisant la seule adresse IP allouée à leur routeur.

Il y a des limitations à l'utilisation de la méthode de traduction. Il est obligatoire que toutes les demandes et les réponses appartenant à une session soient acheminées via le même routeur NAT. Une façon de s'en assurer serait d'avoir le NAT situé sur un routeur frontière qui soit unique à un domaine de bout, où tous les paquets IP sont soit générés dans le domaine soit destinés au domaine. Il y a d'autres façons de s'assurer de cela avec plusieurs appareils de NAT. Par exemple, un domaine privé pourrait avoir deux points de sortie distincts pour des fournisseurs différents et le flux de session provenant

des hôtes dans un réseau privé pourrait traverser par l'appareil de NAT qui a la meilleure métrique pour un hôte externe. Quand un des routeurs de NAT a une défaillance, les autres pourraient acheminer le trafic pour toutes leurs connexions. Il faut cependant faire très attention avec cette approche, parce que les flux réacheminés pourraient échouer au moment du transfert au nouveau routeur de NAT. Une façon de surmonter ce problème potentiel est que les routeurs partagent la même configuration de NAT et échangent des informations d'état pour s'assurer mutuellement d'une sauvegarde libre de défaillance.

La traduction d'adresse est indépendante de l'application et est souvent accompagnés de passerelles spécifiques d'application (ALG) pour effectuer la surveillance et les altérations de charge utile. FTP est l'ALG résidente la plus populaire sur les appareils de NAT. Les applications qui requièrent l'intervention d'une ALG ne doivent pas avoir une charge utile codée, car cela empêcherait effectivement l'ALG de jouer son rôle, sauf à ce que l'ALG ait la clé pour déchiffrer la charge utile.

Cette solution présente l'inconvénient d'abandonner la signification de bout en bout de l'adresse IP et de la maquiller avec une augmentation d'état dans le réseau. Par suite, le niveau de sécurité de bout en bout du réseau IP assuré par IPSec ne peut pas être garanti pour les hôtes d'extrémité, lorsque un appareil de NAT se trouve sur le chemin. L'avantage de cette approche est cependant que cela peut être installé sans changement aux hôtes ou aux routeurs.

La définition de termes comme "domaine d'adresses", "acheminement transparent ", "accès TU ", "ALG" et autres, utilisés tout au long de ce document, se trouvent dans [NAT-TERM].

2. Survol de la NAT traditionnelle

L'opération de traduction d'adresse présentée dans ce document est appelée "NAT traditionnelle". Il y a d'autres variantes de NAT qui ne seront pas explorées dans ce document. La NAT traditionnelle permet aux hôtes au sein d'un réseau privé d'accéder de façon transparente aux hôtes dans le réseau externe, dans la plupart des cas. Dans une NAT traditionnelle, les sessions sont unidirectionnelles, en sortie du réseau privé. Les sessions dans la direction opposée peuvent être admises de façon exceptionnelle en utilisant des transpositions d'adresse statiques pour des hôtes pré sélectionnés. La NAT de base et NAPT sont deux variantes de la NAT traditionnelle, en ce que la traduction dans la NAT de base est limitée aux seules adresses IP, alors que la traduction dans NAPT est étendue pour inclure l'adresse IP et l'identifiant de transport (comme l'accès TCP/UDP ou l'identifiant d'interrogation ICMP).

Sauf mention contraire, tout au long de ce document, traduction d'adresse ou NAT se réfèrent à la NAT traditionnelle, à savoir la NAT de base aussi bien que NAPT. Seuls les routeurs frontière de bout qui sont décrits dans la figure 1 ci-dessous peuvent être configurés pour effecteur la traduction d'adresse.

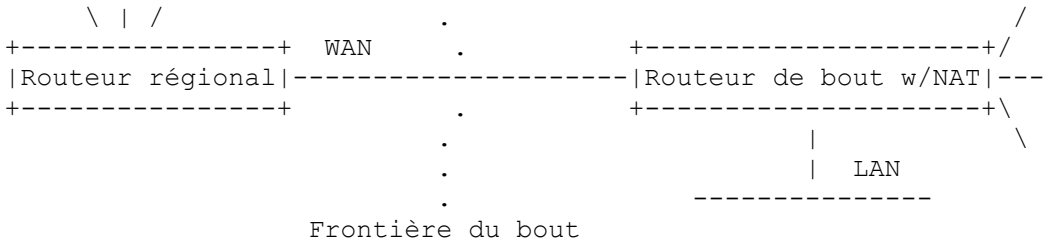

Figure 1 : Configuration de NAT traditionnelle

2.1 Vue d'ensemble de la NAT de base

La NAT de base fonctionne de la façon suivante. Un domaine de bout avec un ensemble d'adresses réseau privées pourrait être capable de communiquer avec le réseau externe en transposant de façon dynamique l'ensemble des adresses privées en un ensemble d'adresses réseau à validité mondiale. Si le nombre des nœuds locaux est inférieur ou égal à celui des adresses dans l'ensemble mondial, chaque adresse locale a la garantie d'être transposée en une adresse mondiale. Autrement, les nœuds à qui il est permis d'avoir un accès simultané au réseau externe sont limités par le nombre des adresses dans l'ensemble mondial. Les adresses locales individuelles peuvent être transposées de façon statique en adresses mondiales spécifiques pour assurer un accès garanti à l'extérieur ou pour permettre l'accès à l'hôte local à partir d'hôtes externes via une adresse publique fixe. Plusieurs sessions simultanées peuvent être initiées à partir d'un nœud local, en utilisant la même transposition d'adresse.

Les adresses à l'intérieur d'un domaine de bout sont locales pour ce domaine et ne sont pas valides en dehors du domaine. Donc, les adresses à l'intérieur d'un domaine de bout peuvent être réutilisées par tout autre domaine de bout. Par exemple,

une seule adresse de classe A pourrait être utilisée par de nombreux domaines de bout. À chaque point de sortie entre un domaine de bout et le cœur de réseau, la NAT est installée. Si il y a plus d'un point de sortie, il n'est pas très important que chaque NAT ait le même tableau de traduction.

Par exemple, dans le cas de la figure 2, deux bouts A et B utilisent en interne le bloc d'adresses privées de classe A 10.0.0.0/8 [RFC1918]. Au NAT du bout A est alloué le bloc d'adresses de classe C 198.76.29.0/24, et au NAT du bout B est alloué le bloc d'adresse de classe C 198.76.28.0/24. Les adresses de classe C sont uniques au monde et aucune autre boîte de NAT ne peut les utiliser.

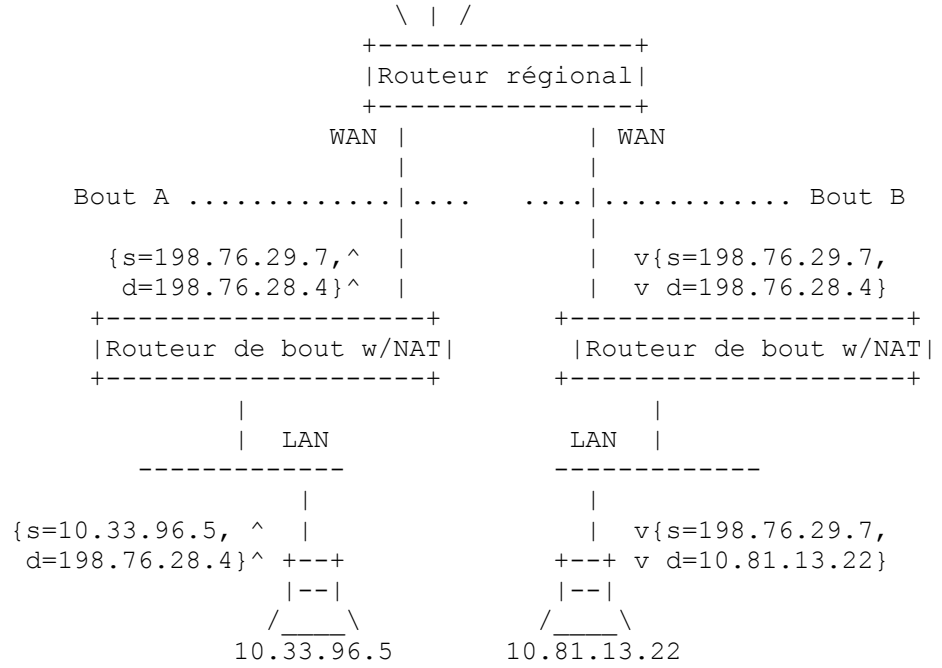

Figure 2 : Fonctionnement de NAT de base

Lorsque l'hôte 10.33.96.5 du bout A souhaite envoyer un paquet à l'hôte 10.81.13.22 du bout B, il utilise l'adresse unique au monde 198.76.28.4 comme destination, et envoie le paquet à son routeur principal. Le routeur de bout a un chemin statique pour le réseau 198.76.0.0 de sorte que le paquet est transmis à la liaison WAN. Cependant, la NAT traduit l'adresse de source 10.33.96.5 de l'en-tête IP en l'adresse unique au monde 198.76.29.7 avant que le paquet ne soit transmis. De même, les paquets IP sur le chemin de retour passent par des traductions d'adresse similaires.

Remarquez que cela n'exige aucun changement des hôtes ou des routeurs. Par exemple, pour autant que les hôtes du bout A soient concernés, 198.76.28.4 est l'adresse utilisée par l'hôte dans le bout B. Les traductions d'adresse sont transparentes pour les hôtes d'extrémité dans la plupart des cas. Bien sûr, ceci n'est qu'un simple exemple. Il y a de nombreuses questions à examiner.

2.2 Vue d'ensemble de NAPT

Disons qu'une organisation a un réseau IP privé et une liaison WAN avec un fournisseur de service. Le routeur de bout du réseau privé a reçu une adresse valide dans le monde entier sur la liaison de WAN et les nœuds restants dans l'organisation ont des adresses IP qui n'ont qu'une signification locale. Dans un tel cas, les nœuds sur le réseau privé pourraient avoir un accès simultané au réseau externe en utilisant la seule adresse IP enregistrée avec l'aide de NAPT. NAPT permettrait la transposition des tuplets du type (adresses IP locales, numéro d'accès TU local) en tuplets du type (adresse IP enregistrée, numéro d'accès TU alloué).

Ce modèle satisfait aux exigences de la plupart des groupes de professions libérales et travailleurs à domicile (SOHO) pour accéder au réseau externe en utilisant une seule adresse IP allouée par le fournisseur de service. Ce modèle pourrait être étendu de façon à permettre l'accès sortant par une transposition statique d'un nœud local pour chaque accès TU de service de l'adresse IP enregistrée.

Dans l'exemple de la figure 3 ci-dessous, le bout A utilise en interne le bloc d'adresses de classe A 10.0.0.0/8. L'interface WAN du routeur de bout a reçu une adresse IP de 138.76.28.4 de la part du fournisseur de service.

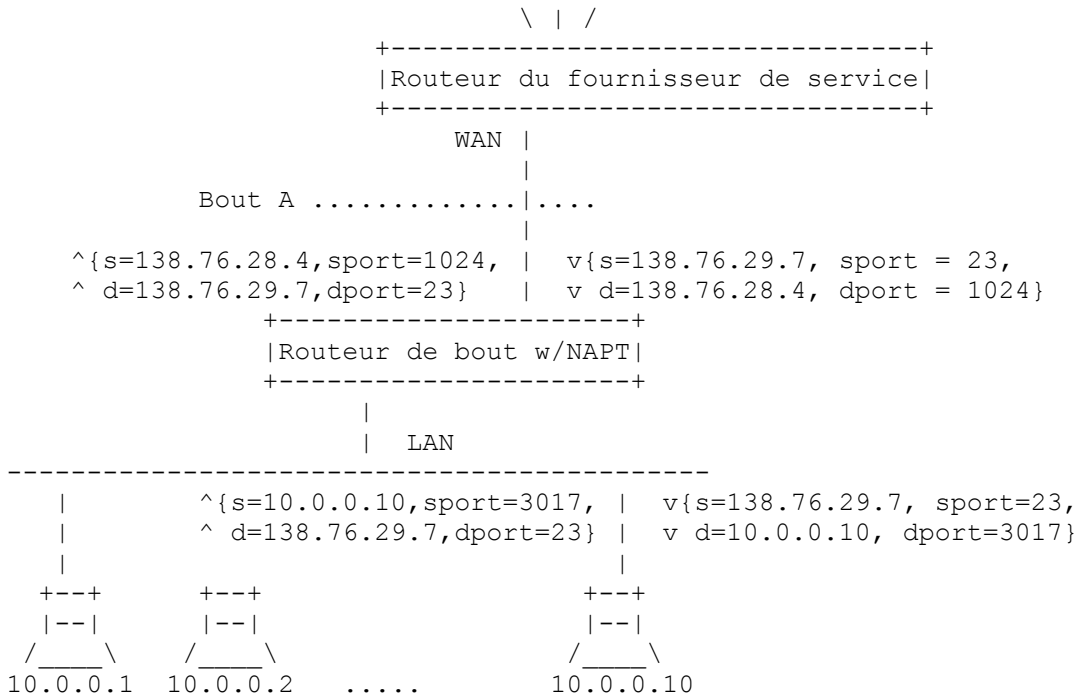

Figure 3 : Fonctionnement de la traduction de l'accès d'adresse réseau (NAPT)

Lorsque l'hôte 10.0.0.10 du bout A envoie un paquet telnet à l'hôte 138.76.29.7, il utilise l'adresse unique au monde 138.76.29.7 comme destination, et envoie le paquet à son routeur principal. Le routeur de bout a un chemin statique pour le sous réseau 138.76.0.0/16 de sorte que le paquet est transmis sur la liaison WAN. Cependant, NAPT traduit le tuplet de l'adresse de source 10.0.0.10 et de l'accès TCP de source 3017 dans les en-têtes IP et TCP en l'adresse unique au monde 138.76.28.4 et en l'accès TCP alloué de façon univoque, disons 1024, avant que le paquet ne soit transmis. Les paquets sur le chemin de retour passent par des traductions similaires d'adresse et d'accès TCP pour l'adresse IP et l'accès TCP cibles. Là encore, remarquer que cela n'exige pas de changement chez les hôtes et les routeurs. La traduction est complètement transparente.

Dans cette disposition, seules les sessions TCP/UDP sont permises et doivent être générées à partie du réseau local. Cependant, il y a des services comme le DNS qui demandent un accès entrant. Il peut y avoir d'autres services pour lesquels une organisation souhaite permettre l'accès de sessions entrantes. Il est possible de configurer de façon statique un service d'accès TU bien connu [RFC1700] sur le routeur de bout pour être dirigé sur un nœud spécifique dans le réseau privé.

En plus des sessions TCP/UDP, les messages ICMP, à l'exception des messages de type REDIRECT, peuvent aussi être surveillés par le routeur NAPT. Les paquets de type interrogation ICMP sont traduits de façon similaire à celles des paquets TCP/UDP, en ce que le champ identifiant dans l'en-tête de message ICMP va être transposé de façon univoque en un identifiant d'interrogation de l'adresse IP enregistrée. Le champ identifiant dans les messages d'interrogation ICMP est établi par l'envoyeur de l'interrogation et retourné inchangé dans le message de réponse par celui qui répond à l'interrogation. Ainsi, le tuplet de (adresse IP locale, identifiant local d'interrogation ICMP) est transposé en un tuplet de (adresse IP enregistrée, identifiant alloué d'interrogation ICMP) par le routeur NAPT pour identifier de façon univoque les interrogations ICMP de tous les types provenant de tout hôte local. Les modifications aux messages d'erreur ICMP sont discutées dans une autre section, car elles impliquent des modifications à la charge utile ICMP ainsi qu'aux en-têtes IP et ICMP.

Dans la disposition NAPT, où l'adresse IP enregistrée est la même que l'adresse IP de l'interface de WAN du routeur de bout, le routeur doit être sûr de faire la distinction entre les sessions TCP, UDP ou d'interrogation ICMP générées de lui-même plutôt que celles générées par les nœuds sur le réseau local. Toutes les sessions entrantes (y compris de TCP, UDP et de session d'interrogation ICMP) sont supposées être dirigées sur le routeur de NAT comme nœud d'extrémité, sauf si l'accès du service cible est transposé de façon statique sur un nœud différent dans le réseau local.

Les sessions autres que de type TCP, UDP et d'interrogation ICMP ne sont tous simplement pas permises à partir des nœuds locaux, desservis par un routeur NAPT.

3. Phases de traduction d'une session.

Les phases de traduction sont les mêmes avec la NAT traditionnelle que celles décrites dans [NAT-TERM]. Les paragraphes qui suivent identifient les éléments qui sont spécifiques du NAT traditionnel.

3.1 Lien d'adresse

Avec la NAT de base, une adresse privée est liée à une adresse externe, lorsque la première session sortante est initiée à partir de l'hôte privé. Ensuite de cela, toutes les autres sessions sortantes générées à partir de la même adresse privée vont utiliser le même lien d'adresse pour la traduction des paquets.

Dans le cas de NAPT, où de nombreuses adresses privées sont transposées en une seule adresse unique au monde, le lien serait du tuplet (adresse privée, accès TU privé) au tuplet (adresse allouée, accès TU alloué). Comme avec le NAT de base, ce lien est déterminé lorsque la première session sortante est initiée par le tuplet (adresse privée, accès TU privé) sur l'hôte privé. Bien que ce ne soit pas une pratique courante, il est possible qu'on ait sur l'hôte privé une application qui établisse plusieurs sessions simultanées originaires du même tuplet de (adresse privée, accès TU privé). Dans un tel cas, un seul lien pour le tuplet (adresse privée, accès TU privé) peut être utilisé pour la traduction des paquets qui relèvent de toutes les sessions générées à partir du même tuplet sur un hôte.

3.2 Recherche d'adresse et traduction

Après l'établissement d'un lien d'adresse ou d'un lien du tuplet (adresse, accès TU) dans le cas de NAPT, un état conditionnel peut être conservé pour chacune des connexions qui utilisé le lien. Les paquets qui appartiennent à la même session seront soumis à la recherche de session pour les besoins de la traduction. La nature exacte de la traduction est exposée dans la section suivante.

3.3 Défaire un lien d'adresse

Lorsque la dernière session fondée sur un lien d'adresse ou de tuplet (adresse, accès TU) est terminée, le lien lui-même peut être fermé.

4. Traductions de paquets

Les paquets qui relèvent de sessions gérées par la NAT subissent une traduction dans l'une et l'autre direction. Les questions de traduction de paquet individuel sont traitées en détail dans les paragraphes suivants.

4.1 Manipulations d'en-têtes IP, TCP, UDP et ICMP

Dans le modèle de NAT de base, l'en-tête IP de chaque paquet doit être modifié. Cette modification inclut l'adresse IP (adresse IP de source pour les paquets sortants et adresse IP de destination pour les paquets entrants) et la somme de contrôle IP.

Pour les sessions [TCP] et [UDP], les modifications doivent inclure la mise à jour de la somme de contrôle dans les en-têtes TCP/UDP. Cela parce que la somme de contrôle TCP/UDP couvre aussi un pseudo en-tête qui contient les adresses IP de source et de destination. Avec une exception, celle des en-têtes UDP avec une somme de contrôle de 0 qui ne devraient pas être modifiés. Comme pour les paquets d'interrogation [ICMP], aucun autre changement dans l'en-tête ICMP n'est nécessaire car la somme de contrôle dans l'en-tête ICMP ne couvre pas les adresses IP.

Dans le modèle NAPT, les modifications à l'en-tête IP sont similaires à celles du NAT de base. Pour les sessions TCP/UDP, les modifications doivent être étendues pour inclure la traduction de l'accès TU (accès TU de source pour les paquets sortants et accès TU de destination pour les paquets entrants) dans l'en-tête TCP/UDP. L'en-tête ICMP dans les paquets d'interrogation ICMP doit aussi être modifié pour remplacer la somme de contrôle de l'identifiant d'interrogation et de l'en-tête ICMP. L'identifiant d'interrogation d'hôte privé doit être traduit en identifiant alloué à la sortie et l'exact inverse à l'entrée. La somme de contrôle d'en-tête ICMP doit être corrigée pour tenir compte de la traduction de l'identifiant d'interrogation.

4.2 Ajustement de somme de contrôle

Les modifications de NAT sont par paquet et peuvent être très gourmandes en calcul, car elles impliquent une ou plusieurs

modifications de somme de contrôle en plus des simples traductions de champs. Heureusement, nous avons un algorithme qui rend les ajustement de sommes de contrôle très simple et efficace pour les en-têtes IP, TCP, UDP et ICMP. Comme tous ces en-têtes utilisent une somme de compléments à un, il est suffisant de calculer la différence arithmétique entre les adresses avant traduction et après traduction et d'ajouter cela à la somme de contrôle. L'algorithme ci-dessous n'est applicable qu'aux décalages pairs (c'est-à-dire que ci-dessous optr doit être un décalage pair par rapport au début de l'en-tête) et aux longueurs paires (c'est-à-dire que olen et nlen ci-dessous doivent être pairs). L'échantillon de code (en langage C) pour cela est le suivant :

```
void checksumadjust(unsigned char *chksum, unsigned char *optr, int olen, unsigned char *nptr, int nlen)
                                                    /* en supposant que : unsigned char est de 8 bits, long est 32 bits.
                                                       - chksum pointe sur la somme de contrôle dans le paquet
                                                       - optr pointe sur les anciennes données dans le paquet
                                                       - nptr pointe sur les nouvelles données dans le paquet */
{
 long x, old, new;
 x=chksum[0]*256+chksum[1];
 x=~x & 0xFFFF;
 while (olen)
 {
    old=optr[0]*256+optr[1]; optr+=2;
    x-=old & 0xffff;
    if (x<=0) { x--; x&=0xffff; }
    olen-=2;
 }
 while (nlen)
 {
    new=nptr[0]*256+nptr[1]; nptr+=2;
    x+=new & 0xffff;
    if (x & 0x10000) { x++; x&=0xffff; }
    nlen-=2;
 }
 x=~x & 0xFFFF;
 chksum[0]=x/256; chksum[1]=x & 0xff;
}
```

4.3 Modifications au paquet d'erreur ICMP

Les changements au message d'erreur [ICMP] vont inclure des changements aux en-têtes IP et ICMP sur la couche externe ainsi que des changements aux en-têtes de paquet incorporés au sein de la charge utile du message d'erreur ICMP.

Pour que la NAT soit transparente aux yeux de l'hôte d'extrémité, l'adresse de l'en-tête IP incorporée au sein de la charge utile du message d'erreur ICMP doit être modifiée, le champ Somme de contrôle de l'en-tête IP incorporé doit être modifié et normalement, la somme de contrôle de l'en-tête ICMP doit aussi être modifiée pour refléter les changements intervenus dans la charge utile.

Dans un dispositif NAPT, si le message IP incorporé au sein d'ICMP se trouve être un paquet TCP, UDP ou d'interrogation ICMP, on aura besoin de modifier le numéro d'accès TU approprié au sein de l'en-tête TCP/UDP ou le champ Identifiant d'interrogation dans l'en-tête d'interrogation ICMP.

Finalement l'en-tête IP du paquet ICMP doit aussi être modifié.

4.4 Prise en charge de FTP

Une des applications les plus répandues [FTP] exigerait une ALG pour surveiller la charge utile des sessions de contrôle pour déterminer les paramètres de session de données qui s'ensuivent. L'ALG de FTP fait partie intégrante de la plupart des mises en œuvre de NAT.

L'ALG de FTP exigerait un tableau spécial pour corriger les numéros de séquence et d'accusé de réception de TCP avec l'accès de source et de destination FTP. Les entrées du tableau devraient avoir l'adresse de source, l'adresse de destination, l'accès de source, l'accès de destination, la différence du numéro de séquence et un horodatage. De nouvelles entrées ne sont créées que lorsque sont vues les commandes FTP PORT ou les réponses PASV. Le différentiel du numéro de séquence peut être augmenté ou diminué pour chaque commande FTP PORT ou réponse PASV. Les numéros de séquence sont

incrémentés à la sortie et les numéros d'accusé de réception sont diminués à l'entrée de cette différence.

Les traductions de charge utile FTP sont limitées aux adresses privées et aux adresses externes qui leur sont allouées (codées en ASCII comme des octets individuels) pour la NAT de base. Pour un dispositif NAPT cependant, les traductions doivent être étendues pour inclure les octets de l'accès TCP (en ASCII) à la suite des octets de l'adresse.

4.5 Prise en charge du DNS

En considérant que dans un NAT traditionnel les sessions sont principalement en sortie d'un domaine privé, on peut éviter d'utiliser une ALG du DNS en conjonction avec un NAT traditionnel de la façon suivante : le ou les serveurs DNS internes au domaine privé conservent la transposition des noms en adresses IP pour les hôtes internes et éventuellement certains hôtes externes. Les serveurs DNS externes conservent la transposition de nom pour les seuls hôtes externes et pour aucun des hôtes internes. Si le réseau privé n'a pas de serveur DNS interne, toutes les demandes DNS peuvent être dirigées sur un serveur DNS externe pour trouver les transpositions d'adresse pour les hôtes externes.

4.6 Traitement d'option IP

Un datagramme IP qui a une des options IP Record Route, Strict Source Route ou Loose Source Route va exiger l'enregistrement ou l'utilisation des adresses IP des routeurs intermédiaires. Un routeur intermédiaire NAT peut choisir de ne pas prendre en charge ces options ou de laisser les adresses non traduites tout en traitant les options. Le résultat de la non traduction des adresses sera que les adresses privées seront exposées de bout en bout le long du chemin vers la source. Cela ne devrait pas en soi perturber le chemin de traversée du paquet, car chaque routeur est supposé ne regarder que le routeur du prochain bond.

5. Questions diverses

5.1 Partition des adresses locales et mondiales

Pour que la NAT fonctionne comme décrit dans le présent document, il est nécessaire de partager l'espace des adresses IP en deux parties – les adresses privées utilisées en interne au domaine de bout, et les adresses uniques au monde. Toute adresse doit être soit une adresse privée, soit une adresse mondiale. Il n'y a pas de chevauchement.

Le problème avec le chevauchement est le suivant : si on dit qu'un hôte dans le bout A souhaite envoyer des paquets à un hôte dans le bout B, mais si les adresses mondiales du bout B se chevauchent avec les adresses privées du bout A, les routeurs du bout A ne seront pas capables de distinguer l'adresse mondiale du bout B de ses propres adresses privées.

5.2 Recommandation pour l'espace d'adresses privé

La [RFC1918] a fait des recommandations sur l'allocation de l'espace d'adresses aux réseaux privés. L'Autorité d'allocation des numéros de l'Internet, IANA, *Internet Assigned Numbers Authority*) a trois blocs d'espace d'adresses IP, à savoir 10.0.0.0/8, 172.16.0.0/12, et 192.168.0.0/16 pour les internets privés. En notation pré CIDR, le premier bloc n'est rien d'autre qu'un seul numéro de réseau de classe A, alors que le second bloc est un ensemble de seize réseaux contigus de classe B, et le troisième bloc est un ensemble de 256 réseaux contigus de classe C.

Une organisation qui décide d'utiliser les adresses IP dans l'espace d'adresses défini ci-dessus peut le faire sans aucune coordination avec l'IANA ou un registraire de l'Internet. L'espace d'adresses peut donc être utilisé de façon privée par de nombreuses organisations indépendantes en même temps, avec le fonctionnement de la NAT activé sur leurs routeurs frontière.

5.3 Acheminement à travers un NAT

Le routeur qui effectue la NAT ne devrait pas annoncer les réseaux privés au cœur de réseau. Seuls les réseaux qui ont des adresses mondiales devraient être connus en dehors du bout. Cependant, les informations mondiales que le NAT reçoit du routeur frontière de bout peuvent être annoncées dans le bout de la façon habituelle.

Normalement, le routeur de bout qui fait la NAT va avoir un chemin statique configuré pour transmettre tout le trafic externe au routeur du fournisseur de service sur la liaison WAN, et le routeur du fournisseur de service va avoir un chemin statique configuré pour transmettre les paquets de NAT (c'est-à-dire, ceux dont l'adresse de destination IP tombe dans la gamme de la liste des adresses mondiales gérées par le NAT) au routeur NAT sur la liaison WAN.

5.4 Passage de la NAT de base à NAPT

Dans un dispositif de NAT de base, lorsque les nœuds du réseau privé sont plus nombreux que les adresses disponibles pour la transposition (disons un réseau privé de classe B transposé sur un bloc d'adresses mondiales de classe C) l'accès au réseau externe pour certains des nœuds locaux est abruptement interrompu après que la dernière adresse mondiales de la liste des adresses est utilisée. Ceci est très peu pratique et très contraignant. Un tel incident peut être évité en toute sécurité en permettant au routeur de NAT de base de passer facultativement sur le dispositif NAPT pour les dernières adresses mondiales de la liste d'adresses. Faire cela va assurer que les hôtes sur le réseau privé auront un accès ininterrompu aux nœuds et services externes pour la plupart des applications. Noter cependant, qu'il serait troublant que certaines des applications qui travaillaient avec la NAT de base se mettent soudain à s'interrompre à cause du passage sur NAPT.

6. Limitations des NAT

[NAT-TERM] traite des limitations de toutes les variantes de NAT, au sens large. Les paragraphes qui suivent identifient les limitations spécifiques de la NAT traditionnelle.

6.1 Confidentialité et sécurité

La NAT traditionnelle peut être vue comme fournissant un mécanisme de confidentialité car les sessions sont unidirectionnelles à partir des hôtes privés et les adresses réelles des hôtes privés ne sont pas visibles aux hôtes externes.

C'est la caractéristique même qui améliore la confidentialité qui rend potentiellement les problèmes de débogage (y compris les violations de la sécurité) plus difficiles. Si un hôte dans un réseau privé abuse de l'Internet d'une façon ou d'une autre (comme d'essayer d'attaquer une autre machine ou même d'envoyer une grosse quantité de pourriels) il est plus difficile de traquer la source réelle du problème parce que l'adresse IP de l'hôte est cachée dans un routeur de NAT.

6.2 Réponses de l'ARP aux adresses mondiales transposée par la NAT sur une interface de LAN

La NAT ne doit être activée que sur les routeurs frontière d'un domaine de bout. Les exemples fournis dans le document pour illustrer la NAT de base et NAPT ont conservé une liaison de WAN pour la connexion au routeur externe (c'est-à-dire, le routeur du fournisseur de service) à partir du routeur de NAT. Cependant, si la liaison de WAN devait être remplacée par une connexion de LAN et si une partie de, ou tout l'espace d'adresses mondial utilisé pour la transposition de NAT appartient au même sous-réseau IP que le segment de LAN, le routeur NAT serait supposé fournir la prise en charge de ARP *(protocole de résolution d'adresses)* pour la gamme d'adresses qui appartiennent au même sous-réseau. Répondre aux demandes ARP pour les adresses mondiales transposées par le NAT avec ses propres adresses MAC est une nécessité dans une telle situation avec le dispositif de NAT de base. Si le routeur NAT n'a pas répondu à ces demandes, il n'y a aucun autre nœud dans le réseau qui ait la propriété de ces adresses et elles resteront donc sans réponse.

Ce scénario est improbable avec un dispositif NAPT sauf lorsque la seule adresse utilisée dans la transposition NAPT n'est pas l'adresse d'interface du routeur NAT (comme dans le cas d'un passage de la NAT de base à NAPT expliqué au paragraphe 5.4 ci-dessus par exemple).

Utiliser une gamme d'adresses provenant d'un sous-réseau directement connecté pour la transposition d'adresse par la NAT empêcherait la configuration statique de chemin sur le routeur du fournisseur de service.

L'opinion des auteurs est qu'une liaison de LAN avec un routeur de fournisseur de service n'est pas très courante. Cependant, les fabricants pourraient être intéressés à prendre facultativement en charge un mandataire ARP pour le cas où...

6.3 Traduction de paquets TCP/UDP fragmentés sortants dans un dispositif NAPT

La traduction de fragments TCP/UDP sortants (c'est-à-dire, ceux générés d'hôtes privés) dans un dispositif NAPT est vouée à l'échec. La raison en est la suivante. Seul le premier fragment contient l'en-tête TCP/UDP qui serait nécessaire pour associer le paquet à une session pour les besoins de la traduction. Les fragments suivants ne contiennent pas les informations sur l'accès TCP/UDP, mais portent simplement le même identifiant de fragmentation que spécifié dans le premier fragment. Disons que deux hôtes privés ont généré des paquets TCP/UDP fragmentés pour 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 sans relation entre eux, qui portent le même identifiant de fragmentation et provenant de la même adresse d'hôte allouée, il sera incapable de déterminer à laquelle des deux sessions appartient le datagramme. Par conséquent, les deux sessions seront endommagées.

7. Mises en œuvre actuelles

De nombreuses mises en œuvre commerciales disponibles sur le marché adhèrent à la description de la NAT fournie dans le présent document. Le logiciel Linux du domaine public contient une NAT sous le nom de "IP masquerade". Le logiciel FreeBSD du domaine public a une mise en œuvre de NAPT fonctionnant comme un démon. Noter cependant que la source Linux est couverte par la licence GNU et le logiciel FreeBSD est couvert par une licence UC Berkeley.

Les logiciels Linux et FreeBSD sont libres, de sorte qu'on peut acheter les CD-ROM pour un peu plus que le coût de distribution. Ils sont aussi disponibles en ligne sur un certain nombre de sites FTP avec les dernières modifications.

8. Considérations pour la sécurité

Les considérations pour la sécurité décrites dans [NAT-TERM] pour toutes les variantes de NAT sont applicables au NAT traditionnel.

Références

(Les liens sur les numéros pointent sur la version anglaise, ceux du corps du titre sur la version française)

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

[ICMP] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", RFC0792, STD 5, septembre 1981.

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

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989.

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique)*

[RFC1818] J. Postel, T. Li, Y. Rekhter, "Bonnes pratiques actuelles", août 1995. *(Historique)*

[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)*

[TCP] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", RFC0793, (STD 7), septembre 1981.

[UDP] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", RFC0768, (STD 6), 28 août 1980.

Adresse des auteurs

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

Kjeld Borch Egevang
Intel Denmark ApS
téléphone : +45 44886556
Fax : +45 44886051
mél : kjeld.egevang@intel.com
http: //www.freeyellow.com/members/kbe

Déclaration de droits de reproduction

Remerciement

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