Groupe de travail Réseau
Request for Comments : 5508
BCP 48
Catégorie : Bonnes pratiques actuelles
Traduction Claude Brière de L'Isle

P. Srisuresh, Kazeon Systems
B. Ford, MPI-SWS
S. Sivakumar, Cisco Systems
S. Guha, Cornell U.
avril 2009

Exigences de comportement des NAT pour ICMP

Résumé
Le présent document spécifie les propriétés de comportement exigées des appareils de traduction d'adresse réseau (NAT, *Network Address Translator*) en conjonction avec le protocole de message de commande Internet (ICMP, *Internet Control Message Protocol*). L'objectif de ce mémoire est de rendre les appareils de NAT plus prévisibles et compatibles avec divers protocoles d'application qui traversent les appareils. Des documents d'accompagnement fournissent des recommandations de comportement spécifiques de TCP, UDP, et autres protocoles.

Table des matières

1. Introduction et domaine d'application

Comme le souligne la [RFC3424], les mises en œuvre de NAT varient largement dans la façon dont elles traitent les différents trafics. L'objet du présent document est de définir un ensemble spécifique d'exigences de comportement de NAT à l'égard des messages ICMP. L'objectif est de réduire l'imprévisibilité et la fragilité qu'introduisent les appareils de NAT. Le présent document s'ajoute aux [RFC4787], [RFC5382], et autres documents de comportement spécifiques de protocole qui définiront à l'avenir les exigences pour les NAT quand ils traitent du trafic spécifique de protocole.

Les exigences de la présente spécification s'appliquent aux NAT traditionnels comme décrit dans la [RFC3022]. Un NAT traditionnel a deux variantes, le NAT de base et le traducteur d'adresse/accès réseau (NAPT, *Network Address/Port Translator*). Parmi eux, le NAPT est de loin l'appareil de NAT le plus couramment déployé. Un NAPT permet à de multiples hôtes privés de partager simultanément une seule adresse publique IP.

Le présent document couvre seulement les aspects ICMP de la traversée de NAT, spécifiquement la traversée des messages ICMP Query et des messages d'erreur ICMP. Le NAT traditionnel rend par nature obligatoire le comportement de filtrage de style pare-feu [RFC4787]. Cependant, la fonction de pare-feu en général ou toute autre fonction de boîtier de médiation sort du domaine d'application du présent document.

Dans certains cas, le comportement de traversée du message ICMP sur un appareil de NAT peut être outrepassé par des politiques administratives locales. Des administrateurs peuvent choisir d'interdire entièrement la transmission des messages d'erreur ICMP à travers un appareil de NAT. Certains autres peuvent choisir d'interdire les applications fondées sur l'interrogation ICMP à travers un appareil de NAT. Ce sont des politiques locales et elles sortent du domaine de ce document. Pour cette raison, certaines des exigences ICMP mentionnées dans ce document sont précédées d'une contrainte de permission par la politique locale.

Le présent document se concentre strictement sur le comportement de l'appareil de NAT, et pas sur le comportement des applications qui traversent les NAT. Les concepteurs d'application peuvent se référer à [BEH-APP] et à la [RFC5245] pour des recommandations et lignes directrices sur la façon de faire travailler de manière plus robuste les applications sur les NAT qui suivent les exigences spécifiées ici et les documents de comportement spécifique du protocole qui s'y ajoutent.

Selon la [RFC1812], ICMP est un protocole de contrôle qui est considéré faire partie intégrante de IP, bien qu'il soit architecturalement mis en couche au dessus de IP -- il utilise IP pour porter ses données de bout en bout. À ce titre, de nombreuses exigences de comportement ICMP discutées dans ce document s'appliquent à tous les protocoles IP.

Au cas où une exigence du présent document entrerait en conflit avec des exigences de comportement spécifiques d'un protocole, ces dernières vont avoir la priorité. Les auteurs n'ont pas connaissance de conflits entre le présent document et d'autre document de l'IETF au moment de sa rédaction.

La Section 2 décrit la terminologie utilisée dans le document. La Section 3 se concentre sur les exigences concernant les applications fondées sur l'interrogation ICMP qui traversent un appareil de NAT. Les Sections 4 et 5 décrivent les exigences concernant les messages d'erreur ICMP traversant un appareil de NAT. La Section 6 décrit les exigences concernant les messages d'erreur ICMP générés par un appareil de NAT. La Section 7 revoit les exigences de conformité de la RFC 1812 et l'applicabilité aux NAT dans le traitement des messages ICMP. La Section 8 revoit une exigence que les messages ICMP ne soient ni des interrogations ICMP ni des erreurs ICMP. La Section 9 résume toutes les exigences en un seul lieu. La Section 10 discute les considérations sur la sécurité.

2. Terminologie

Les définitions de la majorité des termes de NAT utilisés dans ce document se trouvent dans les [RFC2663] et [RFC4787].

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119],.

Le terme de "domaine" est adapté de la [RFC2663] et est défini comme suit. "Domaine" est souvent utilisé de façon interchangeable pour "domaine réseau" ou simplement "réseau" à travers ce document.

Domaine d'adresses ou domaine - un domaine d'adresses est un domaine de réseau dans lequel les adresses de réseau sont allouées de façon univoque à des entités comme des datagrammes qui peuvent leur être acheminés. Les protocoles d'acheminement utilisés dans le domaine de réseau sont chargés de trouver des chemins pour les entités selon leurs adresses de réseau. Noter que ce document se limite à décrire les NAT dans l'environnement IPv4 et ne traite pas de l'utilisation de NAT dans d'autres types d'environnements (par exemple, l'environnement IPV6).

Le terme "session de NAT" est adapté de la [RFC4008] et est défini comme suit :

Session de NAT - une session de NAT est une association entre une session telle que vue dans le domaine privé et une session telle que vue dans le domaine public, en vertu de la traduction du NAT. Si une session dans le domaine privé devait être représentée comme (PrivateSrcAddr, PrivateDstAddr, TransportProtocol, PrivateSrcPort, PrivateDstPort) et si la même session dans le domaine public devait être représentée comme (PublicSrcAddr, PublicDstAddr, TransportProtocol, PublicSrcPort, PublicDstPort) la session de NAT fournirait le ciment de traduction entre les deux représentations de session. Les sessions de NAT dans ce document sont restreintes aux sessions fondées sur TCP, UDP, et ICMP. À l'avenir, les sessions de NAT pourront être étendues pour être fondées sur d'autres protocoles de transport comme le protocole de transmission de commandes de flux (SCTP, *Stream Control Transmission Protocol*), UDP-léger, et le protocole de contrôle d'encombrement de datagrammes (DCCP, *Datagram Congestion Control Protocol*).

Classification des messages ICMP - le paragraphe 3.2.2 de la [RFC1122] et le paragraphe 4.3.1 de la [RFC1812] groupent les messages ICMP en deux principales catégories, à savoir les messages "Interrogation ICMP" et les messages "Erreur ICMP". Tous les messages d'erreur ICMP mentionnés dans la RFC 1122 et la RFC 1812 contiennent une partie du datagramme Internet qui a provoqué l'erreur ICMP. Tous les messages Interrogation ICMP mentionnées dans les RFC 1122 et RFC 1812 contiennent un champ "Identifiant", qui est appelé dans le présent document un "identifiant d'interrogation". Il y a cependant des messages ICMP qui ne rentrent dans aucune de ces deux catégories. On les appelle des "messages ICMP non d'interrogation-erreur". Ces trois classes de message ICMP sont décrites comme suit :

- Messages Interrogation ICMP - les messages Interrogation ICMP sont caractérisés par un champ Identifiant dans l'en-tête ICMP. Le champ Identifiant utilisé par les messages Interrogation ICMP est aussi appelé un "identifiant d'interrogation" ou "Query Id", en abrégé dans le document. Un Query Id est utilisé par les envoyeurs et répondants aux interrogations comme équivalent d'un accès TCP/UDP pour identifier une session d'interrogation ICMP. Les messages Interrogation ICMP incluent des messages ICMP défini d'après la RFC 1122 ou la RFC 1812 (par exemple, les messages Interrogation ICMP Demande/réponse de nom de domaine définis dans la RFC 1788) car ils incluent des paires de demandes/réponses et contiennent un champ "Identifiant".

- Messages d'erreur ICMP - les messages d'erreur ICMP fournissent la signalisation pour IP. Tous les messages d'erreur ICMP sont caractérisés par le fait qu'ils incorporent le datagramme original qui a déclenché le message d'erreur ICMP. Le datagramme original incorporé dans la charge utile Erreur ICMP est aussi appelé le "paquet incorporé" dans ce document. À la différence des messages d'interrogation ICMP, les messages d'erreur ICMP n'ont pas d'identifiant d'interrogation dans l'en-tête ICMP.

- Messages ICMP non d'interrogation-erreur - les messages ICMP qui ne rentrent dans aucune des deux classes ci dessus sont appelés des "messages ICMP non d'interrogation-erreur" dans ce document. Par exemple, les messages ICMP de découverte de routeur [RFC1256] sont des message ICMPs de type "demande/réponse". Cependant, ils ne sont pas caractérisés comme des messages d'interrogation ICMP dans le présent document car il n'ont pas de champ "Identifiant" dans les messages. De même, il y a d'autres messages ICMP définis dans la [RFC4065] qui ne rentrent pas dans les catégories de message d'interrogation ICMP ou de message d'erreur ICMP, mais vont être appelés des messages ICMP non d'interrogation-erreur.

La raison de la catégorisation des messages ICMP pour les propriétés de comportement de NAT est que chaque catégorie a des caractéristiques différentes (c'est-à-dire, l'identifiant d'interrogation et le datagramme incorporé) utilisées pour transposer qui laissent les messages ICMP non interrogation-erreur dans un groupe distinctif séparé.

3. Traitement de l'interrogation ICMP

Cette section fait la liste des exigences de comportement pour un appareil de NAT quand il traite les paquets d'interrogation ICMP. Les paragraphes qui suivent discutent en détails les exigences spécifiques du traitement de l'interrogation ICMP.

3.1 Transposition d'interrogation ICMP

Sauf explicitement outrepassé par la politique locale, un appareil de NAT DOIT permettre les interrogations ICMP et leurs réponses associées, quand l'interrogation est initiée d'un hôte privé à des hôtes externes. La transposition de l'interrogation ICMP par les appareils de NAT est nécessaire pour que fonctionnent les applications actuelles fondées sur l'interrogation ICMP. Cela implique qu'un appareil de NAT transmette de façon transparente les paquets d'interrogation ICMP initiés à partir de nœuds derrière un NAT, et les réponses à ces paquets d'interrogation dans la direction opposée. Comme spécifié dans la [RFC3022], cela exige de traduire l'en-tête IP. Un appareil de NAPT traduit de plus l'identifiant d'interrogation ICMP et la somme de contrôle associée dans l'en-tête ICMP avant la transmission.

La transposition par le NAT des identifiants d'interrogation ICMP DEVRAIT être indépendante de l'hôte externe. Disons qu'un hôte interne envoie une interrogation ICMP à un hôte externe B en utilisant l'identifiant d'interrogation X. Et, disons que le NAT a alloué à cela une transposition externe d'identifiant d'interrogation X' sur l'adresse publique du NAT. Si l'hôte A a réutilisé l'identifiant d'interrogation X pour envoyer des interrogations ICMP au même hôte externe ou à un hôte différent, l'appareil de NAT DEVRAIT réutiliser la même transposition d'identifiant d'interrogation (c'est-à-dire, transposer l'identifiant d'interrogation X de l'hôte privé en identifiant d'interrogation X' sur l'adresse IP publique du NAT) au lieu de lui allouer une transposition différente. Ceci est similaire à l'exigence de "transposition indépendante du point d'extrémité" spécifiée dans les documents sur les exigences de TCP et UDP [RFC4787], [RFC5382].

Ci-dessous figure la justification de faire de la transposition indépendante du point d'extrémité de l'identifiant d'interrogation ICMP une exigence "DEVRAIT" [RFC2119]. Le Ping ICMP [RFC1470] et le traceroute ICMP [MS-TRCRT] sont deux applications traditionnelles très connues construites par dessus les messages d'interrogation ICMP. Aucune de ces applications n'exige que l'identifiant d'interrogation ICMP soit conservé à travers les différentes sessions avec des hôtes externes. Mais, ce peut n'être pas le cas avec des applications futures. À l'avenir, quand une application d'hôte d'extrémité réutilise le même identifiant d'interrogation dans des sessions avec des hôtes cibles différents, l'application d'hôte d'extrémité pourrait exiger que l'identité du point d'extrémité (c'est-à-dire, le couple adresse IP - identifiant d'interrogation) apparaisse identique à travers tous ses hôtes cibles. Dans un réseau IP sans exigences de NAT, une telle exigence va être valide.

Dans un monde avec des appareils de NAT, l'hypothèse ci-dessus va être valide quand les appareils de NAT appliquent une transposition de point d'extrémité qui est indépendante de l'hôte externe. Étant donnée la dichotomie entre applications traditionnelles qui n'exigent pas de transposition indépendante du point d'extrémité et les futures applications qui pourraient l'exiger, le niveau d'exigence reste à DEVRAIT [RFC2119].

REQ-1 : sauf explicitement outrepassé par la politique locale, un appareil de NAT DOIT permettre les interrogations ICMP et leurs réponses associées, quand l'interrogation est initiée d'un hôte privé aux hôtes externes.

a) la transposition par le NAT des identifiants d'interrogation ICMP DEVRAIT être indépendante de l'hôte externe.

3.2 Temporisations de session d'interrogation ICMP

Les NAT tiennent une temporisation de transposition pour les interrogations ICMP qui les traversent. La temporisation de transposition est le temps pendant lequel une transposition va rester active sans paquets traversant le NAT. Il y a une grande variété de valeurs utilisées par les différents NAT. L'exigence de temporisation de session d'interrogation ICMP est nécessaire pour que fonctionnent les applications courantes d'interrogation ICMP. Les temps de réponse aux interrogations peuvent varier. Les applications fondées sur l'interrogation ICMP sont principalement en mode demande/réponse.

Idéalement, la temporisation devrait être réglée au délai d'aller-retour maximum (RTT maximum, *Maximum Round Trip Time*). Pour donner une contrainte au RTT maximum, la durée de vie maximum de segment (MSL, *Maximum Segment Lifetime*) définie dans la [RFC0793], pourrait être considérée comme une directive pour régler la durée de vie du paquet. Selon la [RFC0793], MSL est la durée maximum d'un segment TCP dans un réseau avant d'être livré au receveur prévu. C'est la durée maximum qu'un paquet IP peut être supposé prendre pour atteindre le nœud de destination prévu avant de déclarer que le paquet ne va plus être livré. Pour une application qui initie un message Interrogation ICMP et attend une réponse à l'interrogation, le RTT maximum pourrait en pratique être contraint d'être la somme de la MSL pour le message d'interrogation et de la MSL pour le message de réponse. En d'autres termes, le RTT maximum pourrait être contraint de n'être pas plus que 2 x MSL. La valeur recommandée pour MSL dans la [RFC0793] est de 120 secondes, même si plusieurs mises en œuvre règlent cela à 60 secondes ou 30 secondes. Quand MSL est 120 secondes, le RTT maximum (2x MSL) va être de 240 secondes.

En pratique, le Ping ICMP [RFC1470] et le traceroute ICMP [MS-TRCRT], les deux applications traditionnelles les plus connues construites par dessus les messages Interrogation ICMP, prennent moins de 10 secondes pour achever un aller-retour quand le nœud cible est opérationnel sur le réseau.

Régler la temporisation de session de NAT ICMP à une très longue durée (disons, 240 secondes) pourrait potentiellement lier les précieuses ressources de NAT telles que les transpositions d'interrogation et les sessions de NAT pour toute la durée. Par ailleurs, régler la temporisation à une valeur très courte peut résulter en une libération prématurée des ressources du NAT et en ce que les applications échouent à se terminer en douceur. La temporisation de session d'interrogation ICMP doit tenir l'équilibre entre les deux extrêmes. Une temporisation de 60 secondes est un compromis entre les deux extrêmes. Un temporisateur de session d'interrogation ICMP NE DOIT PAS expirer en moins de 60 secondes. Il est RECOMMANDÉ que le temporisateur de session d'interrogation ICMP soit configurable.

REQ-2 : un temporisateur de session d'interrogation ICMP NE DOIT PAS expirer en moins de 60 secondes.

a) Il est RECOMMANDÉ que le temporisateur de session d'interrogation ICMP soit configurable.

4. Transmission d'erreur ICMP

De nombreuses applications utilisent des messages d'erreur ICMP provenant des hôtes d'extrémité et des appareils intermédiaires pour abréger les temporisations d'application. Certaines applications ne vont pas fonctionner correctement sans la réception de messages d'erreur ICMP. Les paragraphes qui suivent discutent les exigences auxquelles un appareil de NAT doit se conformer pour assurer une transmission fiable.

4.1 Validation de charge utile d'erreur ICMP

Une somme de contrôle de message d'erreur ICMP couvre le message ICMP entier, y compris la charge utile. Quand un paquet Erreur ICMP est reçu, si la somme de contrôle ICMP échoue à la validation, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. C'est parce que le NAT utilise les en-têtes IP incorporés et de transport pour la transmission et la traduction du message d'erreur ICMP (décrite au paragraphe 4.2). Quand la somme de contrôle ICMP est invalide, les en-têtes IP incorporés et de transport, qui sont couverts par la somme de contrôle ICMP, sont aussi suspects.

Les [RFC1812] et [RFC1122] exigent d'un routeur ou hôte d'extrémité qui reçoit un paquet IP avec une somme de contrôle d'en-tête IP invalide qu'il élimine en silence le paquet IP. À ce titre, les hôtes d'extrémité et routeurs ne génèrent pas de message d'erreur ICMP en réponse aux paquets IP avec une somme de contrôle d'en-tête IP invalide. Pour cette raison, si la somme de contrôle IP du paquet incorporé au sein d'un message d'erreur ICMP échoue à la validation, le NAT DEVRAIT éliminer en silence le paquet d'erreur.

Quand le paquet IP incorporé dans le message d'erreur ICMP inclut des options, l'appareil de NAT ne doit pas supposer que l'en-tête de transport du paquet incorporé est à un décalage fixe (comme ce serait le cas quand il n'y a pas d'option IP associée au paquet) depuis le début du paquet incorporé. Précisément, si le paquet incorporé inclut des options IP, l'appareil de NAT DOIT traverser jusqu'après les options IP pour localiser le début de l'en-tête de transport pour le paquet incorporé.

Il est possible de calculer la somme de contrôle de transport du paquet incorporé au sein d'un message d'erreur ICMP quand le message d'erreur ICMP contient le segment de transport entier. Cependant, souvent, les messages d'erreur ICMP ne contiennent pas le segment de transport entier. C'est parce que la [RFC0792] stipule qu'un message d'erreur ICMP devrait incorporer un en-tête IP et seulement un minimum de 64 bits de la charge utile IP. Même si le paragraphe 4.3.2.3 de la

[RFC1812] recommande à celui qui génère un Erreur ICMP d'inclure autant que possible du paquet original dans la charge utile, la longueur du datagramme ICMP résultant ne peut pas excéder 576 octets. Les générateurs d'erreur ICMP tronquent les paquets IP qui ne tiennent pas dans cette limite.

Un appareil de NAT NE DEVRAIT PAS valider la somme de contrôle de transport du paquet incorporé au sein d'un message d'erreur ICMP, même quand il est possible de le faire. C'est parce qu'un NAT qui élimine un message d'erreur ICMP à cause d'une somme de contrôle de transport invalide va rendre plus difficile aux hôtes d'extrémité de recevoir des rapports d'erreur pour certains types de corruption. Il est préférable de laisser la validation de bout en bout des messages d'erreur ICMP aux hôtes d'extrémité. De nombreuses piles TCP/IP d'hôte d''extrémité révisées mettent en œuvre les améliorations de la [RFC5461] et n'acceptent pas de messages d'erreur ICMP avec une somme de contrôle IP ou TCP discordante dans le paquet incorporé, si le datagramme incorporé contient un paquet IP complet et si la somme de contrôle TCP peut être calculée.

Dans le cas où la charge utile d'erreur ICMP inclut des extensions ICMP [RFC4884], l'appareil de NAT DOIT exclure le bourrage de zéros facultatif et les extensions ICMP quand il évalue la somme de contrôle de transport pour le paquet incorporé. Les lecteurs sont invités à se référer à la [RFC4884] pour des informations sur l'identification de la présence d'extensions ICMP dans un message ICMP.

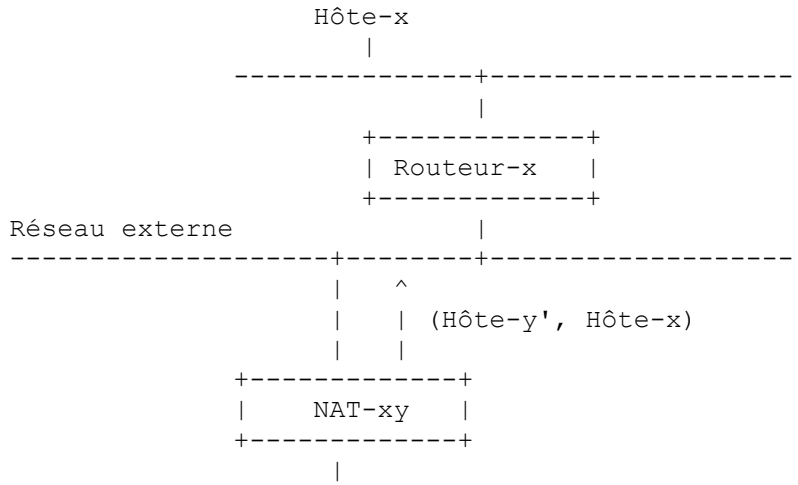
REQ-3 : Quand un paquet Erreur ICMP est reçu, si la somme de contrôle ICMP échoue à la validation, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Si la somme de contrôle ICMP est valide, on fait ce qui suit :

a) si la somme de contrôle IP du paquet incorporé échoue à la validation, le NAT DEVRAIT éliminer en silence le paquet d'erreur ;
b) si le paquet incorporé inclut des options IP, l'appareil de NAT DOIT traverser après les options IP pour localiser le début de l'en-tête de transport pour le paquet incorporé ;
c) l'appareil de NAT NE DEVRAIT PAS valider la somme de contrôle de transport du paquet incorporé au sein d'un message d'erreur ICMP, même quand il est possible de le faire ;
d) si la charge utile d'Erreur ICMP contient des extensions ICMP [RFC4884], l'appareil de NAT DOIT exclure le bourrage de zéros facultatif et les extensions ICMP quand il évalue la somme de contrôle de transport pour le paquet incorporé.

4.2 Traduction de paquet d'erreur ICMP

Le paragraphe 4.3 de la [RFC3022] décrit les champs d'un message d'erreur ICMP qu'un appareil de NAT traduit. Dans ce paragraphe, on décrit les exigences auxquelles un appareil de NAT doit se conformer en effectuant les traductions. Les exigences identifiées dans ce paragraphe sont nécessaires pour que les applications actuelles fonctionnent correctement.

Considérons le scénario de la Figure 1. Disons que le NAT-xy est un appareil de NAT connectant des hôtes dans des réseaux privés et externes. Le Routeur-x et l'Hôte-x sont dans le réseau externe. Le Routeur-y et l'Hôte-y sont dans le réseau privé. Les sous réseaux du réseau externe sont acheminables à partir des domaines privés aussi bien que externes. À l'opposé, les sous réseaux dans le réseau privé sont seulement acheminables au sein du domaine privé. Quand l'Hôte-y a initié une session avec l'Hôte-x, disons que l'appareil de NAT a transposé le point d'extrémité sur l'Hôte-y en l'Hôte-y' dans le réseau externe. Les paragraphes qui suivent décrivent le traitement des messages d'erreur ICMP sur l'appareil de NAT (NAT-xy) quand l'appareil de NAT reçoit un message d'erreur ICMP en réponse à un paquet relevant de cette session.



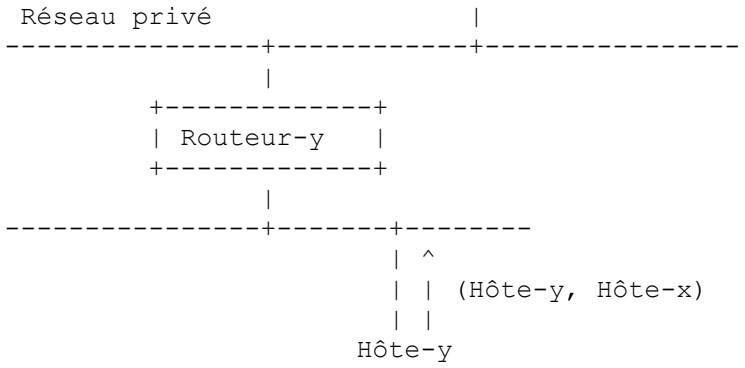


Figure 1 : Session provenant d'un hôte privé traversant un appareil de NAT

4.2.1 Paquet d'erreur ICMP reçu du domaine externe

Disons qu'un paquet de Hôte-y à l'Hôte-x a déclenché un message d'erreur ICMP provenant d'un Routeur-x ou Hôte-x (qui sont tous deux dans le domaine externe). Un tel paquet Erreur ICMP va avoir Routeur-x ou Hôte-x comme adresse IP de source et Hôte-y' comme adresse de destination IP, comme décrit dans la Figure 2 ci-dessous.

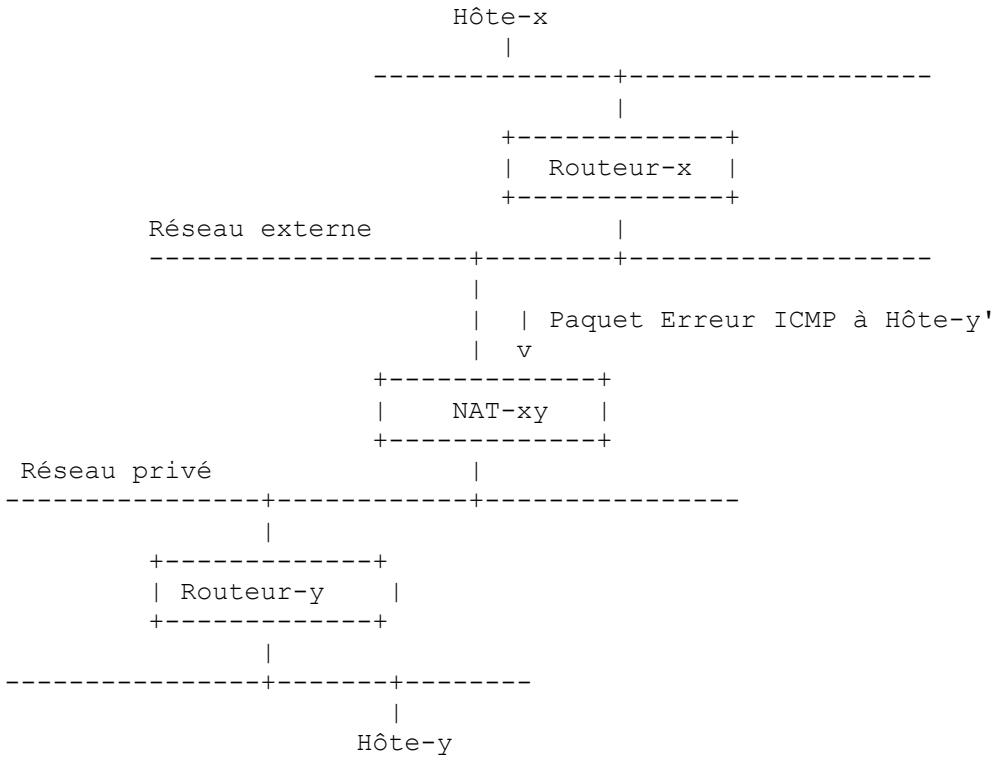


Figure 2 : Paquet Erreur ICMP reçu du réseau externe

Quand l'appareil de NAT reçoit le paquet Erreur ICMP, l'appareil de NAT utilise le paquet incorporé dans le message d'erreur ICMP (c'est-à-dire, le paquet IP de Hôte-y' à Hôte-x) pour chercher la session de NAT à laquelle appartient le paquet incorporé. Si l'appareil de NAT n'a pas une transposition active pour le paquet incorporé, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Autrement, l'appareil de NAT DOIT utiliser la session de NAT correspondante pour traduire le paquet incorporé ; c'est-à-dire, traduire l'adresse IP de source du paquet incorporé (par exemple, de Hôte-y' en Hôte-y) et les en-têtes de transport.

La charge utile Erreur ICMP peut contenir des objets d'extension ICMP [RFC4884]. Les NAT sont invités à prendre en charge les objets d'extension ICMP. Au moment de la rédaction, les auteurs n'ont pas connaissance d'objets d'extension ICMP standard contenant des informations spécifiques du domaine.

L'appareil de NAT DOIT aussi utiliser la session de NAT correspondante pour traduire l'adresse de destination IP en l'en-tête IP externe. Dans l'en-tête externe, l'adresse IP de source va rester inchangée parce que le générateur du message d'erreur ICMP (Hôte-x ou Routeur-x) est dans un domaine externe et est acheminable à partir du domaine privé.

REQ-4 : Si un appareil de NAT reçoit un paquet Erreur ICMP d'un domaine externe, et si l'appareil de NAT n'a pas une transposition active pour la charge utile incorporée, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Si le NAT a une transposition active pour la charge utile incorporée, alors le NAT DOIT faire ce qui suit avant de transmettre le paquet, sauf si c'est explicitement exclu par la politique locale :

a) ramener les en-têtes IP et de transport du paquet IP incorporé à leur forme d'origine, en utilisant la transposition correspondante ;
b) laisser le type et code d'erreur ICMP inchangés ;
c) modifier l'adresse de destination IP de l'en-tête IP externe pour qu'elle soit la même que l'adresse IP de source du paquet incorporé après traduction.

4.2.2 Paquet d'erreur ICMP reçu du domaine privé

Maintenant, disons qu'un paquet de l'Hôte-x à l'Hôte-y a déclenché un message d'erreur ICMP provenant du Routeur-y ou de l'Hôte-y (tous deux dans le domaine privé). Un tel paquet Erreur ICMP va avoir le Routeur-y ou l'Hôte-y comme adresse IP de source et l'Hôte-x comme adresse de destination IP, comme spécifié dans la Figure 3 ci-dessous.

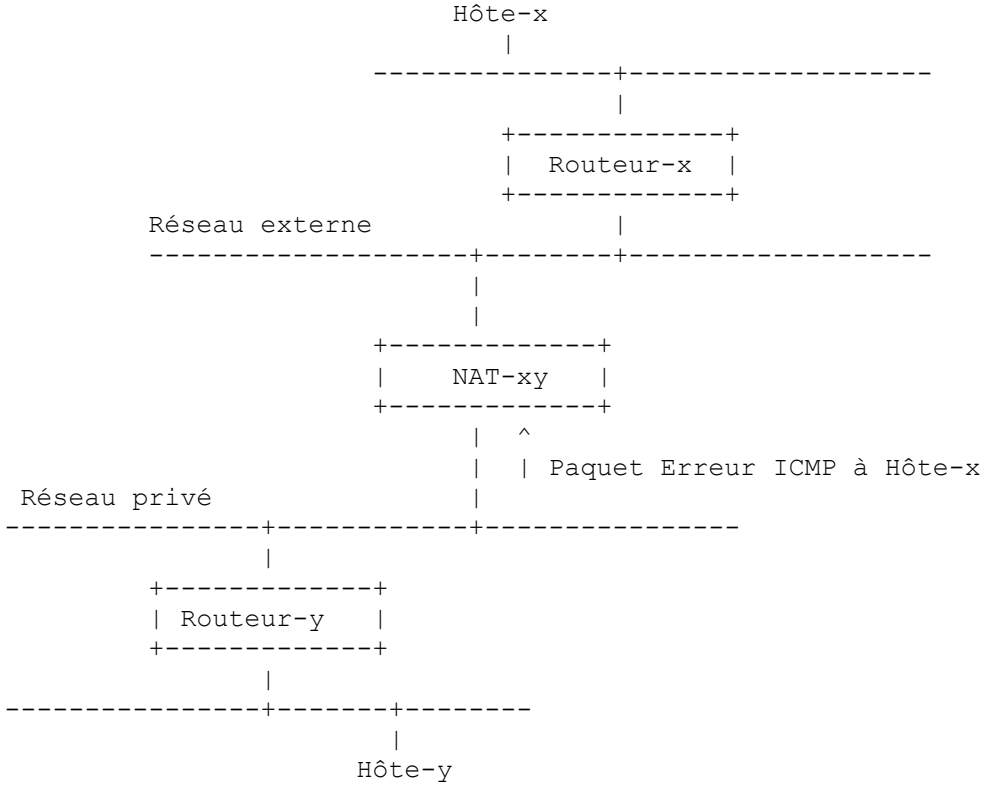


Figure 3 : Paquet Erreur ICMP reçu du réseau privé

Quand l'appareil de NAT reçoit le paquet Erreur ICMP, l'appareil de NAT DOIT utiliser le paquet incorporé dans le message d'erreur ICMP (c'est-à-dire, le paquet IP de l'Hôte-x à l'Hôte-y) pour chercher la session de NAT à laquelle appartient le paquet incorporé. Si l'appareil de NAT n'a pas une transposition active pour le paquet incorporé, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Autrement, l'appareil de NAT DOIT utiliser la session de NAT correspondante pour traduire le paquet incorporé.

La charge utile Erreur ICMP peut contenir des objets d'extension ICMP [RFC4884]. Les NAT sont invités à prendre en charge les objets d'extension ICMP. Au moment de la rédaction, les auteurs n'ont pas connaissance d'objets d'extension ICMP standard contenant des informations spécifiques du domaine.

Dans l'en-tête externe, l'adresse de destination IP va rester inchangée, car l'adresse IP pour Hôte-x est déjà dans le domaine externe. Si le message d'erreur ICMP est généré par l'Hôte-y, l'appareil de NAT doit simplement utiliser la session de NAT pour traduire l'adresse IP de source de Hôte-y en Hôte-y'. Si le message d'erreur ICMP est généré par le nœud intermédiaire Routeur-y, la traduction de l'adresse IP de source varie selon que la fonction de NAT de base ou la fonction de NAPT [RFC3022] est appliquée par l'appareil de NAT. Un appareil de NAT qui applique la fonction de NAT de base a un réservoir d'adresses IP publiques et applique la transposition d'adresse (qui est différente de la transposition de point d'extrémité appliquée par NAPT) quand un nœud privé initie une session sortante via l'appareil de NAT. Donc, si l'appareil de NAT a une transposition active pour l'adresse IP du nœud intermédiaire Routeur-y, l'appareil de NAT DOIT traduire l'adresse IP de source du paquet Erreur ICMP en l'adresse IP publique dans la transposition. Dans tous les autres cas, l'appareil de NAT DOIT simplement utiliser sa propre adresse IP dans le domaine externe pour traduire l'adresse IP de source.

REQ-5 : Si un appareil de NAT reçoit un paquet Erreur ICMP provenant du domaine privé, et si le NAT n'a pas une transposition active pour la charge utile incorporée, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Si le NAT a une transposition active pour la charge utile incorporée, alors le NAT DOIT faire ce qui suit avant de transmettre le paquet, sauf si c'est explicitement exclu par la politique locale :

a) ramener les en-têtes IP et de transport du paquet IP incorporé à leur forme d'origine, en utilisant la transposition correspondante ;
b) laisser inchangés le type et le code d'Erreur ICMP ;
c) si le NAT applique la fonction de NAT de base [RFC3022], et si le NAT a une transposition active pour l'adresse IP qui a envoyé l'erreur ICMP, traduire l'adresse IP de source du paquet Erreur ICMP en l'adressc IP publique dans la transposition. Dans tous les autres cas, traduire l'adresse IP de source du paquet Erreur ICMP en sa propre adresse publique IP.

4.3 Sessions de NAT relevant de la charge utile d'erreur ICMP

Lorsque il traite un paquet Erreur ICMP relevant d'un message Interrogation ICMP ou réponse d'interrogation ICMP, un appareil de NAT NE DOIT PAS rafraîchir ou supprimer la session de NAT qui relève de la charge utile incorporée au sein du paquet Erreur ICMP. Ceci en dépit du fait que l'appareil de NAT utilise la session de NAT pour traduire la charge utile incorporée. Cela assure que la session de NAT ne va pas être modifiée si quelqu'un est capable de falsifier les messages d'erreur ICMP pour la session. [ICMP-ATK] énumère un certain nombre d'attaques ICMP potentielles qui peuvent être tentées par des utilisateurs malveillants sur le réseau. Cette exigence est nécessaire pour que les applications actuelles fonctionnent correctement.

REQ-6 : Lorsque il traite un paquet Erreur ICMP relevant d'un message Interrogation ICMP ou réponse d'interrogation ICMP, un appareil de NAT NE DOIT PAS rafraîchir ou supprimer la session de NAT qui relève de la charge utile incorporée au sein du paquet Erreur ICMP.

5. Marquage de la prise en charge des paquets ICMP

Les [RFC4787] et [RFC5382] rendent obligatoire la prise en charge du marquage des sessions, respectivement, UDP et TCP sur les appareils de NAT. Un appareil de NAT a besoin de prendre aussi en charge le marquage des sessions d'interrogation ICMP. Spécifiquement, les appareils de NAT qui appliquent la fonction de NAT de base [RFC3022] DOIVENT prendre en charge la traversée des sessions d'interrogation ICMP marquées. Disons, par exemple, que des hôtes privés individuels enregistrent leur adresse IP externe allouée par le NAT avec un serveur de rendez-vous. D'autres hôtes qui souhaitent initier des sessions d'interrogation ICMP avec les hôtes enregistrés pourraient le faire en utilisant l'adresse publique enregistrée auprès du serveur de rendez-vous. Pour cette raison, il est exigé des appareils de NAT de base qu'ils prennent en charge la traversée des session d'interrogation ICMP marquées. Cette exigence est nécessaire pour que les applications actuelles fonctionnent correctement.

Les paquets qui appartiennent à une des sessions marquées pourraient, à leur tour, déclencher des messages d'erreur ICMP dirigés sur la source des paquets IP marqués. De tels messages d'erreur ICMP marqués vont traverser les appareils de NAT en route. Tous les appareils de NAT (c'est-à-dire, NAT de base aussi bien qu'appareils NAPT) DOIVENT prendre en charge la traversée des messages d'erreur ICMP marqués. Spécifiquement, l'appareil de NAT doit traduire non seulement le paquet marqué incorporé, mais aussi l'en-tête IP externe qui est marqué. Cette exigence est nécessaire pour que les applications actuelles fonctionnent correctement.

Un message d'erreur ICMP marqué est reçu d'un nœud dans un réseau privé. À ce titre l'exigence de traitement de l'Erreur

ICMP spécifiée dans la REQ-5 est applicable en totalité au traitement du message d'erreur ICMP. De plus, l'appareil de NAT DOIT traduire l'adresse de destination IP de l'en-tête IP externe comme la même que l'adresse IP de source du paquet IP incorporé après la traduction.

REQ-7 : Les appareils de NAT qui appliquent la fonction de NAT de base [RFC3022] DOIVENT prendre en charge la traversée des sessions d'interrogation ICMP marquées. Tous les appareils de NAT (c'est-à-dire, NAT de base aussi bien qu'appareils NAPT) DOIVENT prendre en charge la traversée des messages d'erreur ICMP marqués :

a) Quand il transmet un message d'erreur ICMP marqué, l'appareil de NAT DOIT traduire l'adresse de destination IP de l'en-tête IP externe comme la même que l'adresse IP de source du paquet IP incorporé après la traduction.

6. Rejet des flux sortants interdits par le NAT

Un appareil de NAT permet normalement toutes les sessions sortantes. Cependant, un appareil de NAT peut interdire certaines sessions sortantes du fait de contraintes de ressources ou de considérations administratives. Par exrmple, un appareil de NAT peut ne pas permettre le premier paquet d'une nouvelle session sortante si l'appareil de NAT est à bout de ressources (plus d'adresses ou accès TCP/UDP, ou plus de ressources de session de NAT) pour établir un état pour la session, ou, si la session spécifique est interdite administrativement par l'appareil de NAT.

Quand un appareil de NAT est incapable d'établir une session de NAT pour un nouveau flux de couche de transport (TCP, UDP, ICMP, etc.) du fait de contraintes de ressources ou de restrictions administratives, l'appareil de NAT DEVRAIT envoyer un message Destination ICMP injoignable, avec un code de 13 (Communication administrativement interdite) à l'envoyeur, et éliminer le paquet d'origine. Cette exigence est destinée principalement à une utilisation future. Les applications actuelles n'exigent pas cela pour fonctionner correctement. La justification de l'utilisation du code 13 ICMP dans le message d'erreur ICMP est la suivante : le paragraphe 5.2.7.1 de la [RFC1812] recommande que les routeurs utilisent le code 13 ICMP (Communication administrativement intrdite) quand ils filtrent administrativement les paquets. Le code 13 ICMP est une erreur douce et est à égalité avec les autres codes d'erreur douce générés en réponse à des événements transitoires comme un "réseau injoignable" (type ICMP 3, code 0).

Certains concepteurs de NAT optent pour ne jamais rejeter un flux sortant. Quand un NAT se trouve à court de ressources, ils préfèrent prendre des ressources provenant d'une session de NAT existante plutôt que de rejeter le flux sortant. Un tel choix de conception peut apparaître conforme à la REQ-8 ci-dessous. Cependant, ce choix de conception est en violation de l'esprit des deux REQ-8 et REQ-2. Un tel choix de conception est fortement déconseillé.

REQ-8 : Quand un appareil de NAT est incapable d'établir une session de NAT pour un nouveau flux de couche transport (TCP, UDP, ICMP, etc.) du fait de contraintes de ressources ou de restrictions administratives, l'appareil de NAT DEVRAIT envoyer un message ICMP destination injoignable, avec un code de 13 (Communication administrativement interdite) à l'envoyeur, et éliminer le paquet d'origine.

7. Conformité à la RFC 1812

Le présent document spécifie que les NAT aient un comportement cohérent avec la façon dont les routeurs traitent les messages ICMP, comme spécifié au paragraphe 4.3 de la [RFC1812]. Cependant, depuis la publication de la [RFC1812], certaines de ses exigences ne sont plus les bonnes pratiques actuelles. Donc, les exigences suivantes sont dérivées de la [RFC1812] et s'appliquent aux NAT conformes à la présente spécification :

REQ-9 : Un appareil de NAT PEUT mettre en œuvre un contrôle de politique qui empêche les messages ICMP d'être générés vers certaines interfaces. La mise en œuvre d'un tel contrôle de politique outrepasse les DOIT et DEVRAIT de la REQ-10.

REQ-10 : Sauf si il est outrepassé par la politique de la REQ-9, un appareil de NAT doit prendre en charge les messages ICMP comme ci-dessous, certains se conformant au paragraphe 4.3 de la [RFC1812] et certains se substituant aux exigences du paragraphe 4.3 de la [RFC1812] :

a. DOIT prendre en charge :
   1. Message Destination injoignable, comme décrit au paragraphe 7.1 de ce document.
   2. Message Délai dépassé, comme décrit au paragraphe 7.2 de ce document.
   3. Messages Écho de demande/réponse , comme décrit dans la REQ-1.

b. PEUT prendre en charge :
   1. Message Redirection, comme décrit au paragraphe 4.3.3.2 de la [RFC1812].
   2. Messages Horodatage et Réponse d'horodatage, comme décrit au paragraphe 4.3.3.8 de la [RFC1812].
   3. Options Route de source, comme décrit au paragraphe 7.3 de ce document.
   4. Message Demande/réponse de gabarit d'adresse, comme décrit au paragraphe 7.4 de ce document.
   5. Message Problème de paramètre, comme décrit au paragraphe 7.5 de ce document.
   6. Annonce et sollicitations de routeur, comme décrit au paragraphe 7.6 de ce document.

c. NE DEVRAIT PAS prendre en charge :
   1. Message extinction de source, comme décrit au paragraphe 4.3.3.3 de la [RFC1812].
   2. Demande/réponse d'information, comme décrit au paragraphe 4.3.3.7 de la [RFC1812].

De plus, il est RECOMMANDÉ qu'un appareil de NAT se conforme aux considérations de mise en œuvre suivantes :

d. Usage du champ DS, comme décrit au paragraphe 7.7 de ce document.
e. Quand ne pas envoyer d'erreurs ICMP, comme décrit au paragraphe 4.3.2.7 de la [RFC1812].
f. Limitation de débit, comme décrit au paragraphe 4.3.2.8 de la [RFC1812].

7.1 Fragmentation de paquet IP

De nombreuses applications de réseautage (qui incluent des applications fondées sur TCP aussi bien que sur UDP) dépendent des messages d'erreur ICMP provenant du réseau pour effectuer la découverte de la MTU de chemin de bout en bout [RFC1191]. Une fois que la MTU de chemin est découverte, une application qui choisit d'éviter la fragmentation peut le faire en générant des paquets IP qui tiennent dans la MTU de chemin en route et en établissant le bit DF *(Don't Fragment)* dans l'en-tête IP, afin que les nœuds intermédiaires en route ne fragmentent pas les paquets IP. Les paragraphes qui suivent discutent le besoin que les appareils de NAT respectent le bit DF dans l'en-tête IP et soient capables de générer le message d'erreur ICMP "Paquet trop gros" quand ils ne peuvent pas transmettre le paquet IP sans fragmentation. Le besoin de transmettre de façon transparente les messages d'erreur ICMP générés par d'autres appareils intermédiaires est aussi discuté.

7.1.1 Génération du message d'erreur ICMP "Paquet trop gros"

Quand un routeur est incapable de transmettre un datagramme parce qu'il excède la MTU du réseau de prochain bond et que son bit DF est établi, la [RFC1812] exige du routeur qu'il retourne un message ICMP Destination injoignable à la source du datagramme, avec le code indiquant "fragmentation nécessaire et DF établi". De plus, la [RFC1191] déclare que le routeur DOIT inclure la MTU de ce réseau de prochain bond dans les 16 bits de moindre poids du champ d'en-tête ICMP qui est marqué "non utilisé" dans la spécification ICMP [RFC0792].

Un appareil de NAT DOIT respecter le bit DF dans l'en-tête IP des paquets en transit. L'appareil de NAT peut n'être pas capable de transmettre un paquet IP sans fragmentation si la MTU sur l'interface de transmission de l'appareil de NAT n'est pas adéquate pour le paquet IP. Si le bit DF est établi sur un paquet IP en transit et si l'appareil de NAT ne peut pas transmettre le paquet sans fragmentation, l'appareil de NAT DOIT renvoyer un message ICMP "Paquet trop gros" (type ICMP 3, code 4) avec la MTU du prochain bond à l'envoyeur et éliminer le paquet IP original. L'envoyeur va généralement le renvoyer après avoir pris l'action corrective appropriée.

Si le bit DF n'est pas établi et si la MTU sur l'interface de transmission de l'appareil de NAT rend obligatoire la fragmentation, l'appareil de NAT DOIT fragmenter le paquet et transmettre les fragments [RFC1812].

7.1.2 Transmission du message d'erreur ICMP "Paquet trop gros"

C'est le revers de l'argument du paragraphe précédent. En vertu de la traduction d'adresse qu'effectue le NAT, il peut finir par être le receveur de messages "Paquet trop gros".

Quand l'appareil de NAT est le receveur d'un message ICMP "Paquet trop gros" provenant du réseau, l'appareil de NAT DOIT retransmettre le message ICMP au receveur prévu, conformément aux exigences exprimées précédemment (REQ-3, REQ-4, et REQ-5).

7.2 Message Temps dépassé

Un appareil de NAT DOIT générer un message d'erreur ICMP "Temps dépassé" quand il élimine un paquet à cause d'un champ TTL expiré. Un appareil de NAT PEUT avoir une option par interface pour désactiver la génération de ces messages sur cette interface, mais cette option DOIT par défaut permettre de générer les messages.

Quand un appareil de NAT se conforme à cette exigence, il assure que les applications traditionnelles comme Traceroute [RFC1470], [MS-TRCRT], qui dépendent du message d'erreur ICMP "Temps dépassé", vont continuer de fonctionner même quand des appareils de NAT sont sur le chemin.

7.3 Options de route de source

Un appareil de NAT PEUT prendre en charge la modification des adresses IP dans l'option Route de source afin que les adresses IP dans l'option Route de source soient conformes au domaine. Si un appareil de NAT ne prend pas en charge la transmission des paquets avec l'option Route de source, l'appareil de NAT NE DEVRAIT PAS transmettre les messages ICMP sortants qui contiennent l'option Route de source dans l'en-tête IP externe ou interne. C'est parce que ces messages pourraient révéler des adresses IP privées au domaine externe.

7.4 Messages de demande/réponse de gabarit d'adresse

Le paragraphe 4.3.3.9 de la [RFC1812] dit qu'un routeur IP DOIT mettre en œuvre la prise en charge de la réception des messages de demande de gabarit d'adresse ICMP et de répondre avec des messages de réponse de gabarit d'adresse ICMP. Cependant, plusieurs années (plus de 13 ans au moment de ce document) se sont écoulées depuis la rédaction du texte de la RFC 1812. Pendant ce temps, DHCP [RFC2131] a remplacé l'utilisation de la demande/réponse de gabarit d'adresse. À l'heure actuelle, on trouvera peu d'hôtes qui ne satisfassent pas les exigences pour les hôtes [RFC1122] et aient besoin d'un appareil de NAT pour prendre en charge les demandes/réponses de gabarit d'adresses.

Pour cette raison, un appareil de NAT n'est pas obligé de prendre en charge ce message ICMP.

Un appareil de NAT PEUT prendre en charge les demandes/réponses de gabarit d'adresses.

7.5 Message Problème de paramètre

Le paragraphe 4.3.3.5 de la [RFC1812] dit qu'un routeur IP DOIT générer un message Problème de paramètre pour toute erreur non spécifiquement couverte par un autre message ICMP. Cependant, ce message est rarement utilisé en pratique dans les réseaux où des NAT IPv4 sont déployés.

Pour cette raison, un appareil de NAT n'est pas obligé de prendre en charge ce message ICMP.

Un appareil de NAT PEUT prendre en charge les messages Problème de paramètre.

7.6 Annonce et sollicitations de routeur

Le paragraphe 4.3.3.10 de la [RFC1812] dit qu'un routeur IP DOIT prendre en charge la partie routeur du protocole de découverte de routeur ICMP sur tous les réseaux connectés sur lesquels le routeur prend en charge l'adressage de diffusion groupée IP ou de diffusion IP. Cependant, ce message est rarement utilisé en pratique dans les réseaux où des NAT IPv4 sont déployés.

Pour cette raison, un appareil de NAT n'est pas obligé de prendre en charge ce message ICMP.

Un appareil de NAT PEUT prendre en charge les annonces et sollicitations de routeur.

7.7 Usage du champ DS

La [RFC1812] se réfère à l'octet Type de service (TOS) dans l'en-tête IP, qui contient les champs TOS et préséance IP. Cependant, les champs TOS et préséance IP ne sont plus utilisés aujourd'hui. La [RFC2474] a rebaptisé l'octet TOS en champ DS et défini des classes diffserv dans le champ DS.

Quand il génère un message ICMP, un appareil de NAT DEVRAIT copier la classe diffserv du message qui cause l'envoi

du message d'erreur ICMP. Un appareil de NAT PEUT permettre la configuration de la classe diffserv à utiliser pour les différents types de messages ICMP.

8. Messages ICMP non d'interrogation-erreur

Dans les sections précédentes, les exigences ICMP étaient identifiées pour les appareils de NAT, en se concentrant principalement sur les messages ICMP d'interrogation et d'erreur ICMP, comme défini dans la section de terminologie (Section 2). Le présent document ne donne pas de directive sur le traitement des messages ICMP non d'interrogation-erreur par les appareils de NAT. Un NAT PEUT éliminer ou traiter de façon appropriée les messages ICMP non d'interrogation-erreur.

REQ-11 : un NAT PEUT éliminer ou traiter de façon appropriée les messages ICMP non d'interrogation-erreur. La sémantique des messages ICMP d'erreur non d'interrogation est définie à la Section 2.

9. Résumé des exigences

Voici un résumé de toutes les exigences.

REQ-1 : sauf explicitement outrepassé par la politique locale, un appareil de NAT DOIT permettre les interrogations ICMP et leurs réponses associées, quand l'interrogation est initiée d'un hôte privé aux hôtes externes.
a) la transposition par le NAT des identifiants d'interrogation ICMP DEVRAIT être indépendante de l'hôte externe.

REQ-2 : un temporisateur de session d'interrogation ICMP NE DOIT PAS expirer en moins de 60 secondes.
a) Il est RECOMMANDÉ que le temporisateur de session d'interrogation ICMP soit configurable.

REQ-3 : Quand un paquet Erreur ICMP est reçu, si la somme de contrôle ICMP échoue à la validation, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Si la somme de contrôle ICMP est valide, on fait ce qui suit :

a) si la somme de contrôle IP du paquet incorporé échoue à la validation, le NAT DEVRAIT éliminer en silence le paquet d'erreur ;
b) si le paquet incorporé inclut des options IP, l'appareil de NAT DOIT traverser après les options IP pour localiser le début de l'en-tête de transport pour le paquet incorporé ;
c) l'appareil de NAT NE DEVRAIT PAS valider la somme de contrôle de transport du paquet incorporé au sein d'un message d'erreur ICMP, même quand il est possible de le faire ;
d) si la charge utile d'Erreur ICMP contient des extensions ICMP [RFC4884], l'appareil de NAT DOIT exclure le bourrage de zéros facultatif et les extensions ICMP quand il évalue la somme de contrôle de transport pour le paquet incorporé.

REQ-4 : Si un appareil de NAT reçoit un paquet Erreur ICMP d'un domaine externe, et si l'appareil de NAT n'a pas une transposition active pour la charge utile incorporée, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Si le NAT a une transposition active pour la charge utile incorporée, alors le NAT DOIT faire ce qui suit avant de transmettre le paquet, sauf si c'est explicitement exclu par la politique locale :

a) ramener les en-têtes IP et de transport du paquet IP incorporé à leur forme d'origine, en utilisant la transposition correspondante ;
b) laisser le type et code d'erreur ICMP inchangés ;
c) modifier l'adresse de destination IP de l'en-tête IP externe pour qu'elle soit la même que l'adresse IP de source du paquet incorporé après traduction.

REQ-5 : Si un appareil de NAT reçoit un paquet Erreur ICMP provenant du domaine privé, et si le NAT n'a pas une transposition active pour la charge utile incorporée, le NAT DEVRAIT éliminer en silence le paquet Erreur ICMP. Si le NAT a une transposition active pour la charge utile incorporée, alors le NAT DOIT faire ce qui suit avant de transmettre le paquet, sauf si c'est explicitement exclu par la politique locale :

a) ramener les en-têtes IP et de transport du paquet IP incorporé à leur forme d'origine, en utilisant la transposition correspondante ;
b) laisser inchangés le type et le code d'Erreur ICMP ;
c) si le NAT applique la fonction de NAT de base [RFC3022], et si le NAT a une transposition active pour

l'adresse IP qui a envoyé l'erreur ICMP, traduire l'adresse IP de source du paquet Erreur ICMP en l'adresse IP publique dans la transposition. Dans tous les autres cas, traduire l'adresse IP de source du paquet Erreur ICMP en sa propre adresse publique IP.

REQ-6 : Lorsque il traite un paquet Erreur ICMP relevant d'un message Interrogation ICMP ou Réponse d'interrogation ICMP, un appareil de NAT NE DOIT PAS rafraîchir ou supprimer la session de NAT qui relève de la charge utile incorporée au sein du paquet Erreur ICMP.

REQ-7 : Les appareils de NAT qui appliquent la fonction de NAT de base [RFC3022] DOIVENT prendre en charge la traversée des sessions d'interrogation ICMP marquées. Tous les appareils de NAT (c'est-à-dire, NAT de base aussi bien qu'appareils NAPT) DOIVENT prendre en charge la traversée des messages d'erreur ICMP marqués :

a) Quand il transmet un message d'erreur ICMP marqué, l'appareil de NAT DOIT traduire l'adresse de destination IP de l'en-tête IP externe comme la même que l'adresse IP de source du paquet IP incorporé après la traduction.

REQ-8 : Quand un appareil de NAT est incapable d'établir une session de NAT pour un nouveau flux de couche transport (TCP, UDP, ICMP, etc.) du fait de contraintes de ressources ou de restrictions administratives, l'appareil de NAT DEVRAIT envoyer un message ICMP Destination injoignable, avec un code de 13 (Communication administrativement interdite) à l'envoyeur, et éliminer le paquet d'origine.

REQ-9 : Un appareil de NAT PEUT mettre en œuvre un contrôle de politique qui empêche les messages ICMP d'être générés vers certaines interfaces. La mise en œuvre d'un tel contrôle de politique outrepasse les DOIT et DEVRAIT de la REQ-10.

REQ-10 : Sauf si il est outrepassé par la politique de la REQ-9, un appareil de NAT doit prendre en charge les messages ICMP comme ci-dessous, certains se conformant au paragraphe 4.3 de la [RFC1812] et certains se substituant aux exigences du paragraphe 4.3 de la [RFC1812] :

a. DOIT prendre en charge :
   1. Message Destination injoignable, comme décrit au paragraphe 7.1 de ce document.
   2. Message Délai dépassé, comme décrit au paragraphe 7.2 de ce document.
   3. Messages Écho de demande/réponse , comme décrit dans la REQ-1.

b. PEUT prendre en charge :
   1. Message Redirection, comme décrit au paragraphe 4.3.3.2 de la [RFC1812].
   2. Messages Horodatage et Réponse d'horodatage, comme décrit au paragraphe 4.3.3.8 de la [RFC1812].
   3. Options Route de source, comme décrit au paragraphe 7.3 de ce document.
   4. Message Demande/réponse de gabarit d'adresse, comme décrit au paragraphe 7.4 de ce document.
   5. Message Problème de paramètre, comme décrit au paragraphe 7.5 de ce document.
   6. Annonce et sollicitations de routeur, comme décrit au paragraphe 7.6 de ce document.

c. NE DEVRAIT PAS prendre en charge :
   1. Message extinction de source, comme décrit au paragraphe 4.3.3.3 de la [RFC1812].
   2. Demande/réponse d'information, comme décrit au paragraphe 4.3.3.7 de la [RFC1812].

De plus, il est RECOMMANDÉ qu'un appareil de NAT se conforme aux considérations de mise en œuvre suivantes :

d. Usage du champ DS, comme décrit au paragraphe 7.7 de ce document.
e. Quand ne pas envoyer d'erreurs ICMP, comme décrit au paragraphe 4.3.2.7 de la [RFC1812].
f. Limitation de débit, comme décrit au paragraphe 4.3.2.8 de la [RFC1812].

REQ-11 : Un NAT PEUT éliminer ou traiter de façon appropriée les messages ICMP non d'interrogation-erreur. La sémantique des messages ICMP non d'interrogation-erreur est définie à la Section 2.

10. Considérations sur la sécurité

Le présent document n'introduit aucun nouveau problème de sécurité relatif au traitement du message ICMP dans les appareils de NAT. Cependant, les exigences dans le document atténuent certains problèmes de sécurité connus pour exister avec les messages ICMP.

[ICMP-ATK] énumère un certain nombre d'attaques ICMP qui peuvent être dirigées contre les piles TCP d'hôte d'extrémité. Par exemple, une entité malfaisante pourrait bombarder l'appareil de NAT avec un grand nombre d'erreurs ICMP. Si l'appareil de NAT n'a pas validé la légitimité des paquets d'erreur ICMP, les erreurs ICMP vont être transmises

directement aux nœuds d'extrémité. Les hôtes d'extrémité qui ne sont pas capables de se défendre contre de telles attaques d'erreur ICMP boguées pourraient être impactés par de telles attaques. La REQ-3 recommande de valider la somme de contrôle ICMP et la somme de contrôle IP de la charge utile incorporée avant la transmission. Ces validations de somme de contrôle ne protègent pas par elles-mêmes les hôtes d'extrémité contre les attaques. Cependant, la validation de somme de contrôle atténue l'impact sur les hôtes d'extrémité des attaques d'erreurs ICMP malformées. Les REQ-4 et REQ-5 rendent de plus obligatoire que quand un appareil de NAT ne trouve pas un choix de transposition pour la charge utile incorporée, le NAT devrait éliminer les paquets d'erreur ICMP, sans les transmettre.

Une source malveillante pourrait aussi essayer d'envoyer des messages d'erreur ICMP bogués pour les sessions de NAT actives, dans l'intention de détruire les sessions. La REQ-6 prévient de telles attaques en assurant qu'un message d'erreur ICMP n'affecte pas l'état d'une session sur l'appareil de NAT.

La REQ-8 recommande qu'un appareil de NAT envoie un message d'erreur ICMP quand l'appareil de NAT est incapable de créer une session de NAT du fait d'un manque de ressources. Des administrateurs peuvent choisir que l'appareil de NAT n'envoie pas de message d'erreur ICMP, car le faire confirmerait à l'attaquant malveillant que l'attaque a réussi. Pour cette raison, l'envoi du message d'erreur ICMP spécifique déclaré dans la REQ-8 est laissé à la discrétion de l'administrateur de l'appareil de NAT.

Malheureusement, les messages ICMP sont parfois bloqués aux frontières de réseau du fait de la politique locale de sécurité. Donc, certaines des exigences de ce document permettent à la politique locale d'outrepasser les recommandations de ce document. Bloquer de tels messages ICMP est connu pour casser certaines caractéristiques de protocoles (en particulier la découverte de la MTU) et certaines applications (par exemple, ping, traceroute) et un tel blocage N'est PAS RECOMMANDÉ.

11. Remerciements

Les auteurs souhaitent remercier Fernando Gont, Dan Wing, Carlos Pignataro, Philip Matthews, et les membres du groupe de travail BEHAVE pour leur relecture serrée des premières versions du document et pour la fourniture d'apports précieurx et du don généreux de leur temps pour la formulation des exigences pour ICMP. Leurs précieux retours ont rendu meilleure la lecture de ce document. Dan Wing et Fernando Gont ont été une source solide d'encouragements. Fernando Gont a passé de nombreuses heures à préparer des transparents et à présenter le document dans une réunion de l'IETF au nom des auteurs. Les auteurs remercient aussi Carlos Pignataro et Dan Tappan, auteurs de la [RFC4884], pour leurs retours sur les extensions ICMP. Les auteurs remercient Philip Matthews d'avoir accepter d'être le réviseur technique du document. Enfin, les auteurs ont hautement apprécié les retours rigoureux des membres de l'IESG.

12. Références

12.1 Références normatives

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. *(MàJ par la* RFC6633)

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, DOI 10.17487/RFC0793, septembre 1981. (*Remplacée par* RFC9293)

[RFC1812] F. Baker, "Exigences pour les routeurs IP version 4", juin 1995. *(MàJ par les* RFC2644, RFC6633)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

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

[RFC4787] F. Audet, éd., C. Jennings, "Exigences sur le comportement des traducteurs d'adresse réseau (NAT) pour UDP en envoi individuel", janvier 2007. (BCP0127) *(MàJ par* RFC7857)

[RFC4884] R. Bonica et autres, "ICMP étendu pour la prise en charge de messages multiparties", avril 2007. (*MàJ*

RFC0792, RFC4443) *(P.S. ; MàJ par* RFC8335)

12.2 Références pour information

[BEH-APP] Ford, B., Srisuresh, P., and D. Kegel, "Application Design Guidelines for Traversal through Network Address Translators", Travail en cours, mars 2007.

[ICMP-ATK] Gont, F., "ICMP Attacks against TCP", Travail en cours, octobre 2008.

[MS-TRCRT] Microsoft Support, "How to use the Tracert command-line utility to troubleshoot TCP/IP problems in Windows", http://support.microsoft.com/kb/162326, octobre 2006.

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, DOI 10.17487/RFC1122, octobre 1989. *(MàJ par* RFC6633, 8029, 9293)

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", DOI 10.17487/RFC1191, novembre 1990.

[RFC1256] S. Deering, éditeur, "Messages ICMP de découverte de routeur", septembre 1991.

[RFC1470] R. Enger et J. Reynolds, "Outils pour la surveillance et le débogage d'internets et appareils connectés TCP/IP", FYI0002, août 1993. *(Information)*

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(DS) (Mà J par* RFC3396, RFC4361, RFC5494, et RFC6849)

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6", DOI 10.17487/RFC2474, décembre 1998. *(P.S. ; MàJ par* RFC3168, RFC3260, RFC8436)

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

[RFC3424] L. Daigle, éd., IAB, "Considérations de l'IAB sur l'auto correction d'adressage unilatérale (UNSAF) à travers la traduction d'adresse réseau", novembre 2002, DOI 10.17487/RFC3424. *(Information)*

[RFC4008] R. Rohit et autres, "Définitions des objets gérés pour les traducteurs d'adresse réseau (NAT)", mars 2005. *(P.S. ; Remplacée par* RFC7658)

[RFC4065] J. Kempf, "Instructions pour les allocations par l'IANA à Seamoby et au protocole expérimental de mobilité", juillet 2005. *(Expérimentale)*

[RFC5245] J. Rosenberg,"Établissement de connexité interactive (ICE) : Protocole pour la traversée de traducteur d'adresse réseau (NAT) pour les protocoles d'offre/réponse", avril 2010. (*P.S. ;remplace* RFC4091, 4092 *; remplacée par* 8445)

[RFC5382] S. Guha et autres, "Exigences sur le comportement des NAT pour TCP", octobre 2008. (BCP0142) *(MàJ par* RFC7857)

[RFC5461] F. Gont, "Réaction de TCP aux erreurs logicielles", DOI 10.17487/RFC5461, février 2009. *(Information)*

Adresse des auteurs

Pyda Srisuresh
Kazeon Systems, Inc.
1161 San Antonio Rd.
Mountain View, CA 94043
U.S.A.
téléphone : +1 408 836 4773

Bryan Ford
Max Planck Institute for Software Systems
Campus Building E1 4
D-66123 Saarbruecken
Germany
téléphone : +49-681-9325657

Senthil Sivakumar
Cisco Systems, Inc.
7100-8 Kit Creek Road
Research Triangle Park,
NC 27709-4987
U.S.A.

mél : srisuresh@yahoo.com mél : baford@mpi-sws.org mél : ssenthil@cisco.com

Saikat Guha
Cornell University
331 Upson Hall
Ithaca, NY 14853
U.S.A.
téléphone : +1 607 255 1008
mél : saikat@cs.cornell.edu