Groupe de travail Réseau
Request for Comment : 2003
Catégorie : Sur la voie de la normalisation

C. Perkins, IBM
octobre 1996
Traduction Claude Brière de L'Isle

Encapsulation IP dans d'IP

Résumé
Le présent document spécifie une méthode par laquelle un datagramme IP peut être encapsulé (porté comme charge utile) au sein d'un datagramme IP. L'encapsulation est suggérée comme un moyen d'altérer l'acheminement IP normal des datagrammes, en les livrant à une destination intermédiaire qui autrement ne serait pas choisie par le champ Adresse de destination IP (la partie réseau de l'adresse) dans l'en-tête IP d'origine. L'encapsulation peut servir à divers objets, tels que la livraison d'un datagramme sur un nœud mobile utilisant IP Mobile.

Table des matières

1. Introduction

Le présent document spécifie une méthode par laquelle un datagramme IP peut être encapsulé (porté comme charge utile) au sein d'un datagramme IP. L'encapsulation est suggérée comme un moyen d'altérer l'acheminement IP normal des datagrammes, en les livrant à une destination intermédiaire qui autrement ne serait pas choisie sur la base du champ Adresse IP de destination (la partie réseau de l'adresse) dans l'en-tête IP d'origine. Une fois que le datagramme encapsulé arrive à son nœud de destination intermédiaire, il est désencapsulé, donnant le datagramme IP d'origine, qui est alors délivré à la destination indiquée par le champ Adresse de destination original. Cette utilisation de l'encapsulation et de la désencapsulation d'un datagramme est fréquemment désignée comme le "tunnelage" de datagramme, et l'encapsuleur et le désencapsuleur sont alors considérés comme étant les "points d'extrémité" du tunnel.

Dans le cas le plus général de tunnelage, nous avons :

source ---> encapsuleur --------> désencapsuleur ---> destination

où source, encapsuleur, désencapsuleur, et destination sont des nœuds séparés. Le nœud encapsuleur est considéré comme le "point d'entrée" du tunnel, et le nœud désencapsuleur est considéré comme le "point de sortie" du tunnel. Il peut en général y avoir plusieurs paires source-destination qui utilisent le même tunnel entre l'encapsuleur et le désencapsuleur.

2. Motivation

Le groupe de travail IP Mobile a spécifié l'utilisation de l'encapsulation comme moyen de livrer des datagrammes à partir du "réseau de rattachement" d'un nœud mobile à un agent qui peut délivrer localement des datagrammes par des moyens conventionnels au nœud mobile à sa localisation actuelle loin de son réseau de rattachement [RFC2002]. L'utilisation de l'encapsulation peut aussi être désirable chaque fois que la source (ou un routeur intermédiaire) d'un datagramme IP doit influencer le chemin par lequel un datagramme doit être livré à sa destination ultime. D'autres applications possibles de l'encapsulation sont la diffusion groupée, la facturation préférentielle, le choix de chemins avec des attributs de sécurité choisis, et l'acheminement de politique générale.

Il est généralement vrai que l'encapsulation et l'option d'acheminement de source IP lâche [RFC0791] peuvent être utilisées de façon similaire pour affecter l'acheminement d'un datagramme, mais il y a plusieurs raisons techniques pour préférer l'encapsulation :

- Des problèmes de sécurité non résolus sont associés à l'utilisation des options de route de source IP.

- Les routeurs actuels de l'Internet montrent des problèmes de performances lors de la transmission de datagrammes qui contiennent des options IP, y compris les options d'acheminement de source IP.

- De nombreux nœuds actuels de l'Internet traitent incorrectement les options d'acheminement de source IP.

- Les pare-feu peuvent exclure les datagrammes à acheminement de source IP.

- L'insertion d'une option route de source IP peut compliquer le traitement des informations d'authentification par la source et/ou la destination d'un datagramme, selon la façon dont est spécifiée la réalisation de l'authentification.

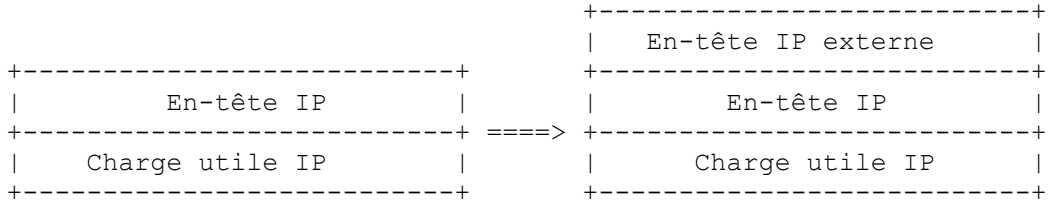
- Il est considéré comme impoli que les routeurs intermédiaires fassent des modifications aux datagrammes qu'ils n'ont pas généré.

Ces avantages techniques doivent être pondérés par les inconvénients que présente l'utilisation de l'encapsulation :
- Les datagrammes encapsulés sont normalement plus gros que les datagrammes à acheminement de source.
- L'encapsulation ne peut pas être utilisée si on ne sait pas à l'avance que le nœud au point de sortie du tunnel peut désencapsuler le datagramme.

Comme aujourd'hui la majorité des nœuds de l'Internet ne fonctionnent pas bien lorsque on utilise les options de route de source IP lâche, le second désavantage technique de l'encapsulation n'est pas si sérieux qu'il pourrait paraître de prime abord.

3. Encapsulation IP dans IP

Pour encapsuler un datagramme IP en utilisant l'encapsulation IP dans IP, un en-tête IP extérieur [RFC0791] est inséré avant l'en-tête IP existant du datagramme, comme suit :



L'adresse de source et l'adresse de destination de l'en-tête IP externe identifient les "points d'extrémité" du tunnel. L'adresse de source et l'adresse de destination de l'en-tête IP interne identifient respectivement l'envoyeur d'origine et le receveur du

datagramme. L'en-tête interne IP n'est pas changé par l'encapsuleur, excepté pour décrémenter le TTL comme noté ci-dessous, et reste inchangé durant sa livraison au point de sortie du tunnel. Aucun changement des options IP ne survient dans l'en-tête interne durant la livraison du datagramme encapsulé à travers le tunnel. Si besoin est, d'autres en-têtes de protocole tels que l'en-tête d'authentification IP [RFC1826] peuvent être insérés entre l'en-tête IP externe et l'en-tête IP interne. Noter que les options de sécurité de l'en-tête interne IP PEUVENT affecter le choix des options de sécurité pour l'en-tête IP encapsulant (externe).

3.1 Champs d'en-tête IP et traitement

Les champs dans l'en-tête IP externe sont réglés comme suit par l'encapsuleur :

Version : 4

IHL : Longueur d'en-tête Internet (IHL) est la longueur de l'en-tête IP externe mesuré en mots de 32 bits [RFC0791].

TOS : Le Type de service (TOS) est copié de l'en-tête IP interne.

Longueur totale
La longueur totale mesure la longueur du datagramme IP encapsulé entier, y compris l'en-tête IP externe, l'en-tête IP interne, et sa charge utile.

Identification, fanions, décalage de fragment
Ces trois champs sont réglés comme spécifié dans [RFC0791]. Cependant, si le bit "Ne pas fragmenter" est mis dans l'en-tête IP interne, il DOIT être mis dans l'en-tête IP externe ; si le bit "Ne pas fragmenter" n'est pas mis dans l'en-tête IP interne, il PEUT être mis dans l'en-tête IP externe, comme décrit au paragraphe 5.1.

Durée de vie
Le champ Durée de vie (TTL) dans l'en-tête IP externe est mis à une valeur appropriée pour la livraison du datagramme encapsulé au point de sortie du tunnel.

Protocole : 4

Somme de contrôle d'en-tête : C'est la somme de contrôle d'en-tête Internet [RFC0791] de l'en-tête IP externe.

Adresse de source : C'est l'adresse IP de l'encapsuleur, c'est-à-dire, du point d'entrée du tunnel.

Adresse de destination : C'est l'adresse IP du désencapsuleur, c'est-à-dire du point de sortie du tunnel.

Options
Aucune option présente dans l'en-tête IP interne n'est en général copiée dans l'en-tête IP externe. Cependant, de nouvelles options spécifiques du chemin de tunnel PEUVENT être ajoutées. En particulier, tous les types d'options de sécurité pris en charge dans l'en-tête IP interne PEUVENT affecter le choix des options de sécurité pour l'en-tête externe. Il n'est pas prévu qu'il y ait une correspondance biunivoque des options ou des en-têtes de sécurité choisis pour le tunnel.

Lors de l'encapsulation d'un datagramme, le TTL dans l'en-tête IP interne est décrémenté de un si le tunnelage est effectué au titre de la transmission du datagramme ; autrement, le TTL de l'en-tête interne n'est pas changé durant l'encapsulation. Si le TTL résultant dans l'en-tête IP interne est 0, le datagramme est éliminé et un message ICMP Durée épuisée DEVRAIT être retourné à l'envoyeur. Un encapsuleur NE DOI PAS encapsuler un datagramme dont le TTL = 0.

Le TTL dans l'en-tête IP interne n'est pas changé lors de la désencapsulation. Si, après désencapsulation, le datagramme interne a un TTL = 0, le désencapsuleur DOIT éliminer le datagramme. Si, après désencapsulation, le désencapsuleur transmet le datagramme à une de ses interfaces réseau, il va décrémenter le TTL comme résultat d'une transmission IP normale. Voir aussi au paragraphe 4.4.

L'encapsuleur peut utiliser tout mécanisme IP existant approprié à la livraison de la charge utile encapsulée au point de sortie du tunnel. En particulier, l'utilisation d'options IP est permise, et l'utilisation de la fragmentation est permise sauf si le bit "Ne pas fragmenter" est mis dans l'en-tête IP interne. Cette restriction à la fragmentation est exigée afin que les nœuds qui emploient la découverte de MTU du chemin [RFC1191] puissent obtenir les informations qu'ils cherchent.

3.2 Défaillances d'acheminement

Les boucles d'acheminement au sein d'un tunnel sont particulièrement dangereuses lorsqu'elles causent le retour des datagrammes à l'encapsuleur. Supposons qu'un datagramme arrive pour transmission à un routeur, et que le routeur détermine que le datagramme doit être encapsulé avant d'être livré plus avant. Alors :

- Si l'adresse IP de source du datagramme correspond à la propre adresse IP du routeur sur une de ses interfaces réseau, le routeur NE DOIT PAS tunneler le datagramme ; le datagramme DEVRAIT plutôt être éliminé.
- Si l'adresse de source IP du datagramme correspond à l'adresse IP de la destination du tunnel (le point de sortie du tunnel est normalement choisi par le routeur sur la base de l'adresse de destination de l'en-tête IP du datagramme) le routeur NE DOIT PAS tunneler le datagramme ; le datagramme DEVRAIT plutôt être éliminé.

Voir aussi au paragraphe 4.4.

4. Messages ICMP de l'intérieur du tunnel

Après l'envoi d'un datagramme encapsulé, l'encapsuleur peut recevoir un message ICMP [RFC0792] de tout routeur intermédiaire au sein du tunnel, autre que le point de sortie du tunnel. L'action prise par l'encapsuleur dépend du type de message ICMP reçu. Lorsque le message reçu contient assez d'informations, l'encapsuleur PEUT utiliser le message entrant pour créer un message ICMP similaire, pour qu'il soit envoyé à l'origine du datagramme IP original non encapsulé (l'envoyeur original). Ce processus est appelé le "relais" du message ICMP provenant du tunnel.

Les messages ICMP indiquant une erreur de traitement d'un datagramme comportent une copie (une portion du) datagramme qui cause l'erreur. Le relais d'un message ICMP exige que l'encapsuleur retire l'en-tête IP externe de la copie retournée du datagramme d'origine. Pour les cas dans lesquels le message ICMP reçu ne contient pas assez de données pour relayer le message, voir à la Section 5.

4.1 Destination injoignable (Type 3)

Les messages ICMP Destination injoignable sont traités par l'encapsuleur selon leur champ Code. Le modèle suggéré ici permet au tunnel "d'étendre" un réseau pour inclure des nœuds non locaux (par exemple, mobiles). Et donc, si la destination d'origine dans le datagramme non encapsulé est sur le même réseau que l'encapsuleur, certaines valeurs de code Destination injoignable peuvent être modifiées pour se conformer au modèle suggéré.

Réseau injoignable (Code 0)
Un message ICMP Destination injoignable DEVRAIT être retourné à l'envoyeur d'origine. Si la destination d'origine dans le datagramme non encapsulé est sur le même réseau que l'encapsuleur, le message Destination injoignable nouvellement généré par l'encapsuleur PEUT avoir le code 1 (Hôte injoignable) car vraisemblablement le datagramme est arrivé au réseau correct et l'encapsuleur essaye de créer l'apparence que la destination d'origine est locale pour le réseau même si elle ne l'est pas. Autrement, si l'encapsuleur retourne un message Destination injoignable, le champ Code DOIT être réglé à 0 (Réseau injoignable).

Hôte injoignable (Code 1)
L'encapsuleur DEVRAIT relayer les messages Hôte injoignable à l'envoyeur du datagramme non encapsulé d'origine, si possible.

Protocole injoignable (Code 2)
Lorsque l'encapsuleur reçoit un message ICMP Protocole injoignable, il DEVRAIT envoyer un message Destination injoignable avec le code 0 ou 1 (voir la discussion sur le code 0) à l'envoyeur du datagramme non encapsulé d'origine. Comme l'envoyeur d'origine n'a pas utilisé le protocole 4 lors de l'envoi du datagramme, il n'y aurait aucun sens à retourner le code 2 à cet envoyeur.

Accès injoignable (Code 3)
Ce code ne devrait jamais être reçu par l'encapsuleur, car l'en-tête IP externe ne se réfère à aucun numéro d'accès. Il NE DOIT PAS être relayé à l'envoyeur du datagramme non encapsulé d'origine.

Datagramme trop gros (Code 4)
L'encapsuleur DOIT relayer les messages ICMP Datagramme trop gros à l'envoyeur du datagramme non encapsulé d'origine.

Échec de route de source (Code 5)
Ce code DEVRAIT être traité par l'encapsuleur lui-même. Il NE DOIT PAS être relayé à l'envoyeur du datagramme non encapsulé d'origine.

4.2 Extinction de source (Type 4)

L'encapsuleur NE DEVRAIT PAS relayer les messages ICMP Extinction de source *(Source Quench)* à l'envoyeur du datagramme non encapsulé d'origine, mais DEVRAIT plutôt activer tout mécanisme de contrôle d'encombrement qu'il met en œuvre pour aider à alléger l'encombrement détecté au sein du tunnel.

4.3 Redirection (Type 5)

L'encapsuleur PEUT traiter lui-même le message ICMP Redirection. Il NE DOIT PAS relayer le Redirection à l'envoyeur du datagramme non encapsulé d'origine.

4.4 Durée de vie écoulée (Type 11)

Les messages ICMP Durée de vie écoulée *(Time Exceeded)* font rapport de boucles (présumées) d'acheminement au sein du tunnel lui-même. La réception de messages Durée de vie écoulée par l'encapsuleur DOIT être rapportée à l'envoyeur du datagramme non encapsulé d'origine comme Hôte injoignable (Type 3, code 1). Hôte injoignable est préférable à Réseau injoignable; car le datagramme a été traité par l'encapsuleur, et l'encapsuleur est souvent considéré comme étant sur le même réseau que l'adresse de destination dans le datagramme non encapsulé d'origine, et le datagramme est considéré comme ayant atteint le réseau correct, mais pas le nœud de destination correct au sein de ce réseau.

4.5 Problème de paramètre (Type 12)

Si le message Problème de paramètre pointe sur un champ copié du datagramme non encapsulé d'origine, l'encapsuleur PEUT relayer le message ICMP à l'envoyeur du datagramme non encapsulé d'origine ; autrement, si le problème survient avec une option IP insérée par l'encapsuleur, celui-ci NE DOIT PAS relayer le message ICMP à l'envoyeur d'origine. Noter qu'un encapsuleur qui suit les pratiques courantes dominantes ne va jamais insérer d'options IP dans le datagramme encapsulé, sauf éventuellement pour des raisons de sécurité.

4.6 Autres messages ICMP

Les autres messages ICMP ne sont pas en rapport avec les opérations d'encapsulation décrites dans la présente spécification de protocole, et devraient être traités par l'encapsuleur comme spécifié dans [RFC0792].

5. Gestion de tunnel

Malheureusement ICMP exige seulement des routeurs IP qu'ils retournent 8 octets (64 bits) du datagramme au delà de l'en-tête IP. Cela n'est pas assez pour inclure une copie de l'en-tête IP encapsulé (interne) IP, de sorte qu'il n'est pas toujours possible à l'encapsuleur de relayer le message ICMP provenant de l'intérieur d'un tunnel en retour à l'envoyeur d'origine. Cependant, en entretenant soigneusement un "état conditionnel" sur les tunnels dans lesquels il envoie, l'encapsuleur peut retourner des messages ICMP précis dans la plupart des cas à l'envoyeur d'origine. L'encapsuleur DEVRAIT entretenir au moins les informations d'état conditionnel suivantes sur chaque tunnel :

- la MTU du tunnel (paragraphe 5.1)
- le TTL (longueur du chemin) du tunnel,
- accessibilité à la fin du tunnel.

L'encapsuleur utilise les messages ICMP qu'il reçoit de l'intérieur d'un tunnel pour mettre à jour les informations d'état conditionnel pour ce tunnel. Les erreurs ICMP qui pourraient être reçues d'un des routeurs le long de l'intérieur du tunnel comportent :

- Datagramme trop gros,
- Durée de vie écoulée,
- Destination injoignable,
- Source éteinte

Lorsque arrivent les datagrammes suivants pour transiter par le tunnel, l'encapsuleur vérifie l'état conditionnel du tunnel. Si le datagramme violerait l'état du tunnel (par exemple, le TTL du nouveau datagramme est inférieur au TTL "d'état conditionnel" du tunnel) l'encapsuleur renvoie un message d'erreur ICMP à l'envoyeur du datagramme originel, mais encapsule aussi le datagramme et le transmet dans le tunnel.

En utilisant cette technique, les messages d'erreur ICMP envoyés par l'encapsuleur ne vont pas toujours correspondre un à un aux erreurs rencontrées au sein du tunnel, mais ils vont refléter précisément l'état du réseau.

L'état conditionnel de tunnel a été développé à l'origine pour la spécification d'encapsulation d'adresse IP (IPAE, *IP Address Encapsulation*) [RFC2893].

5.1 Découverte de la MTU de tunnel

Lorsque le bit Ne pas fragmenter est mis par le générateur et copié dans l'en-tête IP externe, la MTU appropriée du tunnel sera apprise des messages ICMP Datagramme trop gros (Type 3, code 4) rapportés à l'encapsuleur. Pour prendre en charge les nœuds d'envoi qui utilisent la découverte de la MTU du chemin, toutes les mises en œuvre d'encapsuleur DOIVENT prendre en charge l'état conditionnel de découverte de la MTU de chemin [RFC1435], [RFC1191] au sein de leur tunnel. Dans cette application particulière, il y a plusieurs avantages :

- Au bénéfice de la découverte de la MTU de chemin au sein du tunnel, toute fragmentation qui survient à cause de la taille de l'en-tête d'encapsulation n'est effectuée qu'une seule fois après l'encapsulation. Cela empêche des fragmentations multiples d'un seul datagramme, ce qui améliore l'efficacité du traitement du désencapsuleur et des routeurs au sein du tunnel.

- Si la source du datagramme non encapsulé effectue la découverte de la MTU du chemin, il est alors désirable que l'encapsuleur sache la MTU du tunnel. Tous les messages ICMP Datagramme trop gros provenant de l'intérieur du tunnel sont retournés à l'encapsuleur, et comme noté à la Section 5, il n'est pas toujours possible à l'encapsuleur de relayer les messages ICMP à la source du datagramme original non encapsulé. En maintenant un "état conditionnel" sur la MTU du tunnel, l'encapsuleur peut retourner des messages ICMP Datagramme trop gros corrects à l'envoyeur original du datagramme non encapsulé pour la prise en charge de sa propre découverte de la MTU du chemin. Dans ce cas, la MTU qui est convoyée à l'envoyeur original par l'encapsuleur DEVRAIT être la MTU du tunnel moins la taille de l'en-tête IP encapsulant. Cela va éviter la fragmentation du datagramme IP original par l'encapsuleur.

- Si la source du datagramme non encapsulé original ne fait pas la découverte de la MTU du chemin, il est encore souhaitable pour l'encapsuleur de connaître la MTU du tunnel. En particulier, il est bien préférable de fragmenter le datagramme original lors de l'encapsulation, que de permettre la fragmentation du datagramme encapsulé. La fragmentation du datagramme original peut être faîte par l'encapsuleur sans exigences particulières de mémoire tampon et sans qu'il soit besoin de conserver l'état de réassemblage dans le désencapsuleur. À l'opposé, si le datagramme encapsulé est fragmenté, le désencapsuleur doit alors réassembler le datagramme fragmenté (encapsulé) avant de le désencapsuler, ce qui exige l'état de réassemblage et de l'espace de mémoire tampon au sein du désencapsuleur.

Et donc, l'encapsuleur DEVRAIT normalement faire la découverte de la MTU du chemin, ce qui exige de lui qu'il envoie tous les datagrammes dans le tunnel avec le bit "Ne pas fragmenter" mis dans l'en-tête IP externe. Il y a cependant des problèmes avec cette approche. Lorsque l'envoyeur d'origine établit le bit "Ne pas fragmenter", l'envoyeur peut réagir rapidement à tout message d'erreur ICMP Datagramme trop gros en retransmettant le datagramme original. D'un autre côté, supposons que l'encapsuleur reçoive un message ICMP Datagramme trop gros de l'intérieur du tunnel. Dans ce cas, si l'envoyeur d'origine du datagramme non encapsulé n'avait pas mis le bit "Ne pas fragmenter", il n'y a rien que puisse faire l'encapsuleur pour faire savoir l'erreur à l'envoyeur d'origine. L'encapsuleur PEUT garder une copie du datagramme envoyé chaque fois qu'il essaye d'augmenter la MTU du tunnel, afin de lui permettre de fragmenter et renvoyer le datagramme si il reçoit une réponse Datagramme trop gros. Autrement, l'encapsuleur PEUT être configuré pour que certains types de datagrammes ne comportent pas le bit "Ne pas fragmenter" établi lorsque l'envoyeur original du datagramme non encapsulé n'a pas mis le bit "Ne pas fragmenter".

5.2 Encombrement

Un encapsuleur peut recevoir des indications d'encombrement de la part du tunnel, par exemple, en recevant des messages ICMP Source éteinte de la part de nœuds au sein du tunnel. De plus, certaines couches de liaison de divers protocoles sans rapport avec la suite des protocoles de l'Internet pourraient fournir de telles indications sous la forme d'un fanion

Encombrement rencontré [RFC1254]. L'encapsuleur DEVRAIT refléter les conditions d'encombrement dans son "état conditionnel" pour le tunnel, et lors de la transmission ultérieure de datagrammes dans le tunnel, l'encapsuleur DEVRAIT utiliser des moyens appropriés pour contrôler l'encombrement [RFC1812] ; cependant, l'encapsuleur NE DEVRAIT PAS envoyer de messages ICMP Source éteinte à l'envoyeur original du datagramme non encapsulé.

6. Considérations pour la sécurité

L'encapsulation IP peut réduire la sécurité de l'Internet, et il faut y faire attention lors de la mise en œuvre et du déploiement de l'encapsulation IP. Par exemple, l'encapsulation IP rend difficile aux routeurs frontières de filtrer les datagrammes sur la base des champs d'en-tête. En particulier, les valeurs d'origine des champs Adresse de source, Adresse de destination, et Protocole dans l'en-tête IP, et le numéro d'accès utilisé dans tout en-tête de transport au sein du datagramme, ne sont pas situés dans leur position normale au sein du datagramme après encapsulation. Comme tout datagramme IP peut être encapsulé et passé à travers un tunnel, un tel filtrage des routeurs frontières doit examiner soigneusement tous les datagrammes.

6.1 Considérations sur les routeurs

Les routeurs doivent être au courant des protocoles d'encapsulation IP afin de filtrer correctement les datagrammes entrants. Il est souhaitable qu'un tel filtrage soit intégré dans l'authentification IP [RFC1826]. Lorsque l'authentification IP est utilisée, les paquets encapsulés peuvent être admis à entrer dans une organisation si les paquets encapsulants (externes) ou les paquets encapsulés (internes) sont envoyé par une source de confiance authentifiée. Les paquets encapsulés qui ne contiennent pas une telle authentification représentent un risque potentiellement élevé pour la sécurité.

Les datagrammes IP qui sont encapsulés et chiffrés [RFC1827] peuvent aussi poser un problème aux routeurs filtrants. Dans ce cas, le routeur ne peut filtrer le datagramme que si il partage l'association de sécurité utilisée pour le chiffrement. Pour permettre cette sorte de chiffrement dans les environnements dans lesquels tous les paquets doivent être filtrés (ou au moins pris en compte) un mécanisme doit être en place pour que le nœud receveur communique en toute sécurité l'association de sécurité au routeur frontière. Cela peut, plus rarement, s'appliquer aussi à l'association de sécurité utilisée pour les datagrammes sortants.

6.2 Considérations sur les hôtes

Les mises en œuvre d'hôtes qui sont capables de recevoir des datagrammes IP encapsulés DEVRAIENT n'admettre que les datagrammes qui rentrent dans une ou plusieurs des catégories suivantes :

- Le protocole est sans danger : l'authentification fondée sur l'adresse de source n'est pas nécessaire.

- Le datagramme encapsulant (externe) provient d'une source de confiance dont l'identification est authentifiée. L'authenticité de la source pourrait être établie en s'appuyant sur la sécurité physique en plus de la configuration du routeur frontière, mais va plus vraisemblablement venir de l'utilisation de l'en-tête d'authentification IP [RFC1826].

- Le datagramme encapsulé (interne) comporte un en-tête d'authentification IP.

- Le datagramme encapsulé (interne) est adressé à une interface réseau qui appartient au désencapsuleur, ou à un nœud avec lequel le désencapsuleur est entré dans une relation particulière pour la livraison de ces datagrammes encapsulés.

Certaines de ces vérifications, ou toutes peuvent être effectuées dans les routeurs frontières plutôt que dans le nœud de réception, mais il est préférable que les vérifications du routeur frontière soient utilisées comme sauvegarde plutôt que d'être la seule vérification.

7. Remerciements

Des parties des Sections 3 et 5 du présent document ont été tirées de parties de versions précédentes (rédigées par Bill Simpson) du projet Internet IP mobile [RFC2002]. Le texte original de la section 6 (Considérations pour la sécurité) a été rédigé par Bob Smart. De bonnes idées ont aussi été tirées de la [RFC1853], rédigée également par Bill Simpson.

Merci aussi à Anders Klemets pour avoir relevé les erreurs et suggéré des améliorations au projet. Finalement, merci à David Johnson pour sa révision soigneuse du projet, les fautes relevées, et l'amélioration de la cohérence, et ses nombreuses améliorations au projet.

Références

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

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

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

[RFC1254] A. Mankin et K. Ramakrishnan, "Enquête de contrôle sur l'encombrement des routeurs", août 1991. *(Info)*

[RFC1435] S. Knowles, "Avis de l'IESG d'une expérience avec découverte de la MTU de chemin", mars 1993. *(Info)*

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

[RFC1826] R. Atkinson, "En-tête d'authentification IP", août 1995. *(Obsolète, voir la* RFC2402)

[RFC1827] R. Atkinson, "Encapsulation dans IP de charge utile de sécurité (ESP)", août 1995. *(Obsolète, voir* RFC2406)

[RFC1853] W. Simpson, "Tunnel IP dans IP", octobre 1995. *(Information)*

[RFC2002] C. Perkins, éd., "Prise en charge de la mobilité sur IP", octobre 1996. (*Obsolète, voir* RFC3220) *(P.S.)*

[RFC2893] R. Gilligan, E. Nordmark, "Mécanismes de transition pour les hôtes et routeurs IPv6", août 2000. (*Obs., voir* RFC4213)

Adresse de l'auteur

Les questions sur le présent mémoire peuvent être adressées à

Charles Perkins
Room H3-D34
T. J. Watson Research Center
IBM Corporation
30 Saw Mill River Rd.
Hawthorne, NY 10532
USA

téléphone : +1-914-784-7350
Fax : +1-914-784-6205
mél : perk@watson.ibm.com

Le groupe de travail peut être contacté via le président actuel :

Jim Solomon
Motorola, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196
USA
téléphone : +1-847-576-2753
mél : solomon@comm.mot.com