Groupe de travail Réseau
Request for Comments : 2004
Catégorie : En cours de normalisation

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

Encapsulation minimale au sein d'IP

Résumé

Le présent document spécifie une méthode pour encapsuler (porter comme charge utile) un datagramme IP au sein d'un datagramme IP, avec moins de redondance que dans l'encapsulation IP "conventionnelle"qui ajoute un second en-tête IP à chaque datagramme encapsulé. L'encapsulation est suggérée comme un moyen d'altérer l'acheminement IP normal pour les datagrammes, en les livrant à une destination intermédiaire qui ne serait autrement pas choisie par le champ (la partie réseau du champ) Adresse de destination IP dans l'en-tête IP d'origine. L'encapsulation peut servir à divers objets, comme la livraison de datagrammes à un nœud mobile utilisant IP Mobile.

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, avec moins de redondance qu'une encapsulation IP "conventionnelle" [4] qui ajoute un second en-tête IP à chaque datagramme encapsulé. L'encapsulation est suggérée comme moyen pour altérer l'acheminement IP normal pour les datagrammes, en les livrant à une destination intermédiaire qui ne serait autrement pas choisie par la (la partie réseau du) champ Adresse de destination IP de l'en-tête IP d'origine. Le traitement de l'encapsulation et de la désencapsulation d'un datagramme est fréquemment appelée le "tunnelage" du datagramme, et l'encapsuleur et le désencapsuleur sont alors considérés comme étant les "points d'extrémité" du tunnel ; le nœud encapsuleur est appelé le "point d'entrée" du tunnel, et le nœud désencapsuleur est appelé le "point de sortie" du tunnel.

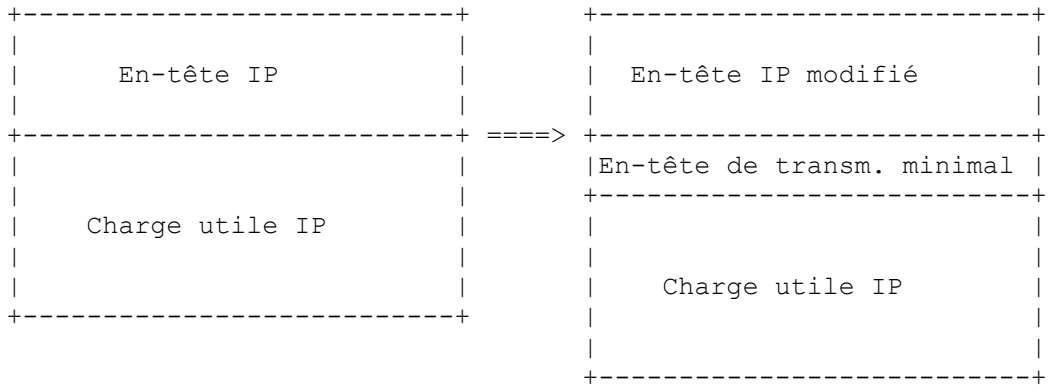
2. Motivation

Le groupe de travail IP Mobile a spécifié l'utilisation de l'encapsulation comme moyen de livrer les paquets provenant du "réseau de rattachement" d'un nœud mobile à un agent qui peut livrer localement les datagrammes par des moyens conventionnels au nœud mobile à sa localisation actuelle éloignée de son rattachement [5]. L'utilisation de l'encapsulation peut aussi être indiquée 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 incluent la diffusion groupée, la facturation préférentielle, le choix de chemins avec des attributs de sécurité choisis, et la régulation d'acheminement générale.

Voir dans [4] un exposé concernant les avantages de l'encapsulation par rapport à l'option IP d'acheminement de source lâche. L'utilisation des en-têtes IP pour encapsuler les datagrammes IP exige la duplication inutile de plusieurs champs au sein de l'en-tête IP interne ; il est possible d'économiser un peu d'espace supplémentaire en spécifiant un nouveau mécanisme d'encapsulation qui élimine la duplication. Le schéma avancé ici provient du groupe de travail IP Mobile (dans des projets Internet antérieurs) et il est similaire à celui qui a été défini dans [2].

3. Encapsulation minimale

Un en-tête de transmission minimal est défini pour les datagrammes qui ne sont pas fragmentés avant l'encapsulation. L'utilisation de cette méthode d'encapsulation est facultative. L'encapsulation minimale NE DOIT PAS être utilisée lorsque le datagramme original est déjà fragmenté, car il n'y a pas de place dans l'en-tête minimal de transmission pour mémoriser les informations de fragmentation. Pour encapsuler un datagramme IP en utilisant l'encapsulation minimale, l'en-tête de transmission minimal est inséré comme suit dans le datagramme :



L'en-tête IP du datagramme original est modifié, et l'en-tête minimal de transmission est inséré dans le datagramme après l'en-tête IP, suivi par la charge utile IP non modifiée du datagramme original (par exemple, l'en-tête de transport et les données de transport). Aucun en-tête IP supplémentaire n'est ajouté au datagramme.

En encapsulant le datagramme, l'en-tête IP original [6] est modifié comme suit :

- Le champ Protocole dans l'en-tête IP est remplacé par le numéro de protocole 55 pour le protocole d'encapsulation minimale.
- Le champ Adresse de destination dans l'en-tête IP est remplacé par l'adresse IP du point de sortie du tunnel.

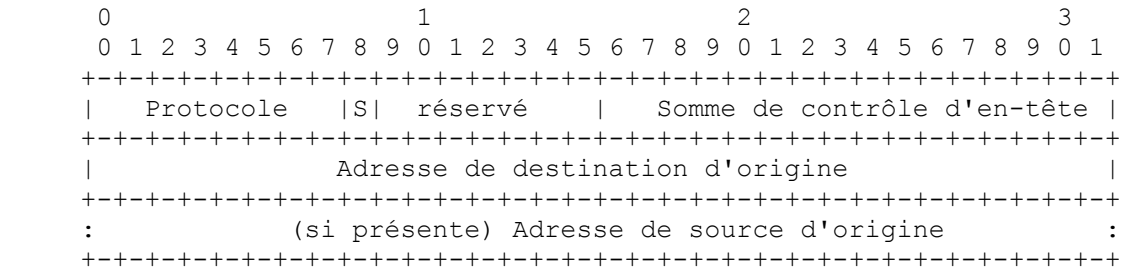
- Si l'encapsuleur n'est pas la source originale du datagramme, le champ Adresse de source dans l'en-tête IP est remplacée par l'adresse IP de l'encapsuleur.

- Le champ Longueur totale dans l'en-tête IP est incrémenté de la taille de l'en-tête minimal de transmission ajouté au datagramme. Cette taille d'incrément est de 12 ou de 8 octets, selon que le bit Adresse de source d'origine présente (S) est mis ou non dans l'en-tête de transmission.

- Le champ Somme de contrôle d'en-tête dans l'en-tête IP est recalculé [6] ou mis à jour pour tenir compte des changements décrits ici dans l'en-tête IP pour l'encapsulation.

Noter qu'à la différence de l'encapsulation IP dans IP [4], le champ Durée de vie (TTL, *Time to Live*) dans l'en-tête IP n'est pas modifié durant l'encapsulation ; si l'encapsuleur transmet le datagramme, il va décrémenter le TTL par suite de la transmission IP normale. Aussi, comme le TTL original reste dans l'en-tête IP après l'encapsulation, les bonds pris par le datagramme au sein du tunnel sont visibles, par exemple, pour "traceroute".

Le format de l'en-tête minimal de transmission est le suivant :



Protocole : Copié du champ Protocole de l'en-tête IP original.

Adresse de source originale présente (S)

0 Le champ Adresse de source d'origine n'est pas présent. La longueur de l'en-tête minimal de tunnelage est de 8 octets dans ce cas.

1 Le champ Adresse de source d'origine est présent. La longueur de l'en-tête minimal de tunnelage est de 12 octets dans ce cas.

réservé Envoyé à zéro; ignoré à réception.

Somme de contrôle d'en-tête

Le complément à un de 16 bits de la somme des compléments à un de tous les mots de 16 bits dans l'en-tête minimal de transmission. Pour les besoins du calcul de la somme de contrôle, la valeur du champ de somme de contrôle est 0. L'en-tête IP et la charge utile IP (après l'en-tête minimal de transmission) ne sont pas inclus dans ce calcul de somme de contrôle.

Adresse de destination d'origine
Copiée dans le champ Adresse de destination dans l'en-tête IP original.

Adresse de source d'origine
Copiée du champ Adresse de source dans l'en-tête IP d'origine. Ce champ n'est présent que si le bit Adresse de source originale présente (S) est mis.

Lors de la désencapsulation d'un datagramme, les champs dans l'en-tête minimal de transmission sont restaurés dans l'en-tête IP, et l'en-tête de transmission est retiré du datagramme. De plus, le champ Longueur totale dans l'en-tête IP est décrémenté de la taille de l'en-tête minimal de transmission retiré du datagramme, et le champ Somme de contrôle d'en-tête dans l'en-tête IP est recalculé [6] ou mis à jour pour tenir compte des changements à l'en-tête IP décrits ici pour la désencapsulation.

L'encapsulateur peut utiliser les mécanismes IP existants qui sont appropriés pour la livraison de la charge utile encapsulée au point de sortie du tunnel. En particulier, l'utilisation des 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. Cette restriction à la fragmentation est requise de telle sorte que les nœuds qui emploient la découverte de la MTU de chemin [3] puissent obtenir les informations qu'ils cherchent.

4. Défaillances d'acheminement

L'utilisation de toute méthode d'encapsulation pour les besoins de l'acheminement amène avec elle une susceptibilité accrue aux boucles d'acheminement. Pour éviter ce danger, un routeur devrait suivre les mêmes procédures que décrites dans [4].

5. Messages ICMP de l'intérieur du tunnel

Les messages ICMP sont à traiter comme spécifié dans [4], y compris la maintenance de "l'état conditionnel" de tunnel.

6. Considérations pour la sécurité

Les questions de sécurité ne sont pas abordées dans le présent document, mais sont généralement similaires à celles avancées dans [4].

7. Remerciements

Le texte original de la plus grande partie de la Section 3 a été tiré du projet IP Mobile [1]. Merci à David Johnson qui a amélioré la cohérence de ce projet auquel il a apporté de nombreuses autres améliorations.

Références

[1] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", RFC3220, janvier 2002. (*Obsolète, voir* RFC3344) *(P.S.)*

[2] David B. Johnson. Scalable and Robust Internetwork Routing for Mobile Hosts. Dans Proceedings of the 14th International Conference on Distributed Computing Systems, pages 2--11, juin 1994.

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

[4] C. Perkins, "Encapsulation de IP dans IP", RFC2003, octobre 1996.

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

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

Adresse de l'auteur

Les questions au sujet du 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
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
téléphone : +1-847-576-2753
mél : solomon@comm.mot.com