Groupe de travail Réseau	B. Carpenter, IBM
Request for Comments : 2529	C. Jung, 3Com
Catégorie : En cours de normalisation	marsh 1999
Traduction Claude Brière de L'Isle	

Transmission de IPv6 sur domaines IPv4 sans tunnels explicites

Résumé
Le présent mémoire spécifie le format de trame pour la transmission des paquets IPv6 [RFC2460] et la méthode de formation des adresses IPv6 de liaison locale sur les domaines IPv4. Il spécifie aussi le contenu de l'option Adresse de couche liaison de source/cible utilisée dans les messages Sollicitation de routeur, Annonce de routeur, Sollicitation de voisin, Annonce de voisin et Redirection, lorsque ces messages sont transmis sur un réseau IPv4 de diffusion groupée.

La motivation de cette méthode est de permettre à des hôtes IPv6 isolés, situés sur une liaison physique qui n'a pas de routeur IPv6 directement connecté, de devenir des hôtes IPv6 pleinement fonctionnels en utilisant un domaine IPv4 qui prenne en charge la diffusion groupée IPv4 comme liaison locale virtuelle. Elle utilise la diffusion groupée IPv4 comme un "Ethernet virtuel".

Table des matières

1. Introduction....1
2. Unité maximum de transmission....2
3. Format de trame....2
4. Autoconfiguration sans état et adresses de liaison locale....2
5. Transposition d'adresse – Envoi individuel....3
6. Transposition d'adresse – Diffusion groupée....3
7. Questions d'adaptabilité et de transition....4
8. Considérations relatives à l'IANA....4
9. Considérations pour la sécurité....4
Remerciements....4
Références....5
Appendice A : Adresses IPv4 de diffusion groupée pour la découverte de voisin....5
Déclaration complète de droits de reproduction....6

1. Introduction

Le présent mémoire spécifie le format de trame pour la transmission des paquets IPv6 [RFC2460] et la méthode de formation d'adresses IPv6 de liaison locale sur les "domaines" de diffusion groupée IPv4. Pour les besoins du présent document, un domaine IPv4 est un ensemble pleinement interconnecté de sous réseaux IPv4, au sein de la même portée de diffusion groupée locale, sur laquelle il y a au moins deux nœuds IPv6 qui se conforment à la présente spécification. Ce domaine IPv4 pourrait faire partie de l'espace d'adresse IPv4 unique au monde, ou faire partie d'un réseau privé IPv4 [RFC1918].

Le présent mémoire spécifie aussi le contenu de l'option Adresse de source/cible de couche liaison utilisée dans les messages Sollicitation de routeur, Annonce de routeur, Sollicitation de voisin, Annonce de voisin et Redirection décrits dans la [RFC2361], lorsque ces messages sont transmis sur un domaine IPv4 de diffusion groupée.

La motivation de cette méthode est de permettre à des hôtes IPv6 isolés, situés sur une liaison physique qui n'a pas de

routeur IPv6 directement connecté, de devenir des hôtes IPv6 pleinement fonctionnels par l'utilisation d'un domaine IPv4 de diffusion groupée comme leur liaison locale virtuelle. Donc, au moins un routeur IPv6 utilisant la même méthode doit être connecté au même domaine IPv4 si l'acheminement IPv6 vers d'autres liaisons est requis.

Les hôtes IPv6 connectés en utilisant cette méthode n'ont pas besoin d'adresses compatibles IPv4 ou de tunnels configurés. De cette façon, IPv6 gagne une indépendance considérable à l'égard des liaisons sous-jacentes et peut sauter de nombreux bonds de sous-réseaux IPv4. Ce mécanisme est connu formellement comme "IPv6 sur IPv4" ou "6sur4" et familièrement comme "Ethernet virtuel".

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

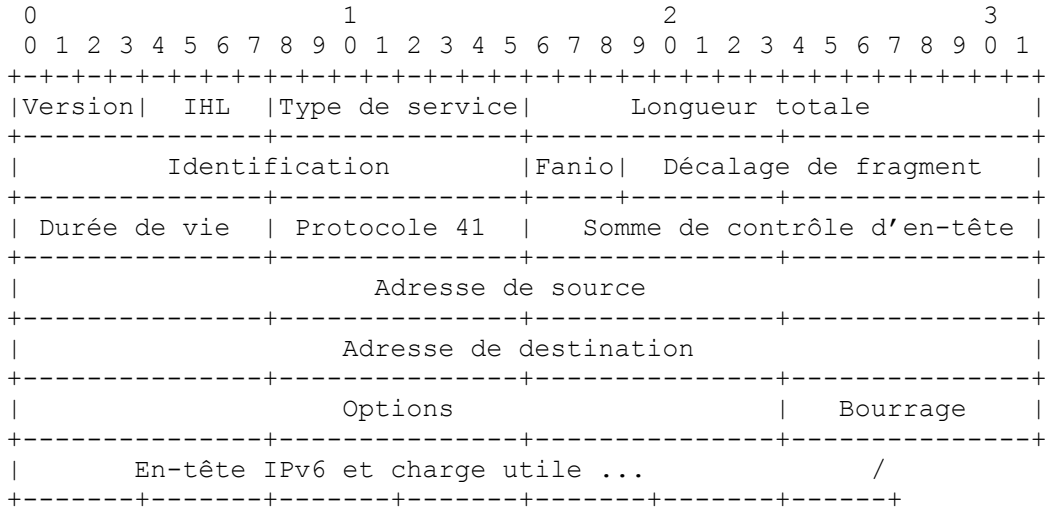
2. Unité maximum de transmission

La taille de MTU par défaut pour les paquets IPv6 sur un domaine IPv4 est de 1480 octets. Cette taille peut être changée par une Annonce de routeur [RFC2361] qui contient une option MTU qui spécifie une MTU différente, ou par configuration manuelle de chaque nœud.

Noter que si par hasard la taille de la MTU IPv6 se révèle être trop grande pour un réseau IPv4 intermédiaire, il va s'ensuivre la fragmentation IPv4. Bien qu'indésirable, ceci n'est pas un désastre. Cependant, le bit IPv4 "Ne pas fragmenter" NE DOIT PAS être établi dans l'en-tête IPv4 encapsulant.

3. Format de trame

Les paquets IPv6 sont transmis dans des paquets IPv4 [RFC0791] avec un type de protocole IPv4 de 41, le même que celui qui a été alloué dans la [RFC1933] aux paquets IPv6 qui sont tunnelés dans des trames IPv4. L'en-tête IPv4 contient les adresses IPv4 de destination et de source. Le corps du paquet IPv4 contient l'en-tête IPv6 suivi immédiatement par la charge utile.



Si il y a des options IPv4, le bourrage DEVRAIT alors être ajouté à l'en-tête IPv4 de telle sorte que l'en-tête IPv6 commence sur une limite d'un décalage de 32 bits à partir de la fin de l'en-tête de liaison des données.

Le champ Durée de vie DEVRAIT être réglé à une faible valeur, pour prévenir la fuite accidentelle de tels paquets en dehors du domaine IPv4. Ceci DOIT être un paramètre configurable, avec une valeur par défaut recommandée de 8.

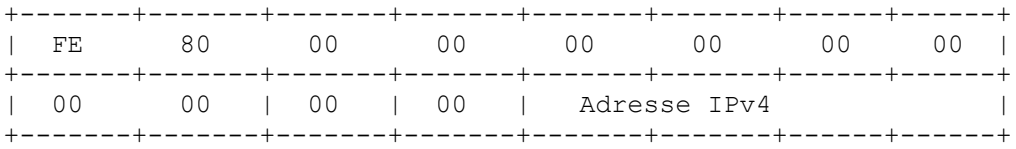
4. Autoconfiguration sans état et adresses de liaison locale

L'identifiant d'interface [RFC2373] d'une interface IPv4 est l'adresse IPv4 de 32 bits de cette interface, avec les octets dans le même ordre que celui dans lequel ils apparaîtraient dans l'en-tête d'un paquet IPv4, bourré à gauche avec des zéros

jusqu'à un total de 64 bits. Noter que le bit "Universel/Local" est à zéro, ce qui indique que l'identifiant d'interface n'est pas unique au monde. Lorsque l'hôte a plus d'une adresse IPv4 utilisée sur l'interface physique concernée, il est fait un choix administratif d'une de ces adresses IPv4.

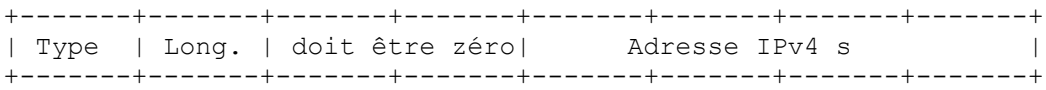
Un préfixe d'adresse IPv6 utilisé pour l'autoconfiguration sans état [RFC2362] d'une interface IPv4 DOIT avoir une longueur de 64 bits, sauf pour le cas particulier mentionné à la Section 7.

L'adresse IPv6 de liaison locale [RFC2373] pour une interface IPv4 virtuelle est formée en ajoutant l'identifiant d'interface, comme défini ci-dessus, au préfixe FE80::/64.



5. Transposition d'adresse – Envoi individuel

La procédure pour transposer les adresses IPv6 en adresses IPv4 virtuelles de couche liaison est décrite dans la [RFC2361]. L'option Adresse de source/cible de couche liaison a la forme suivante lorsque la couche de liaison est IPv4. Comme le champ Longueur est en unités de huit octets, la valeur ci-dessous est 1.



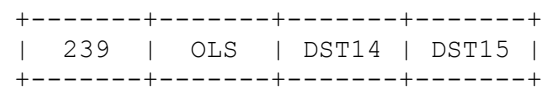
Type :
1 : Adresse de source de couche liaison.
2 : Adresse de cible de couche liaison.

Longueur : 1 (en unités de 8 octets).

Adresse IPv4 :
Adresse IPv4 de 32 bits, dans l'ordre des octets du réseau. C'est l'adresse à laquelle l'interface répond actuellement, et qui peut être différente de l'identifiant d'interface pour l'autoconfiguration sans état.

6. Transposition d'adresse – Diffusion groupée

La diffusion groupée IPv4 DOIT être disponible. Un paquet IPv6 avec une adresse de destination de diffusion groupée DST DOIT être transmis à l'adresse de diffusion groupée IPv4 de portée d'organisation locale en utilisant la transposition ci-dessous. Ces adresses de diffusion groupée IPv4 DEVRAIENT être tirées du bloc 239.192.0.0/16, qui est un sous-bloc du bloc d'adresses de portée d'organisation locale, ou, si aucune de celles-ci n'est disponible, des blocs d'expansion définis dans la [RFC2365]. Noter que quand elles sont formées en utilisant les blocs d'expansion, elles n'utilisent qu'un bloc de taille /16.



DST14, DST15 les deux derniers octets de l'adresse IPv6 de diffusion groupée.

OLS tiré du bloc d'adresses de portée d'organisation locale configuré. DEVRAIT être 192, voir les détails dans la [RFC2365].

Aucune nouvelle procédure d'enregistrement de l'IANA n'est requise pour les éléments ci-dessus. Voir à l'Appendice A. la liste des groupes de diffusion groupée qui doivent être joints pour la prise en charge de la découverte de voisin.

7. Questions d'adaptabilité et de transition

Le mécanisme de diffusion groupée décrit à la Section 6 ci-dessus apparaît avoir essentiellement les mêmes propriétés d'adaptabilité que l'IPv6 natif sur la plupart des supports, excepté la légère réduction de la taille de la MTU qui va un peu réduire le débit brut. Sur un réseau ATM, où la diffusion groupée IPv4 s'appuie sur des mécanismes relativement complexes, on peut s'attendre à ce que IPv6 sur IPv4 sur ATM s'accomplisse moins bien que l'IPv6 natif sur ATM.

Le mécanisme de "IPv6 sur IPv4" est destiné à prendre sa place dans la gamme des options disponibles pour la transition de IPv4 à IPv6. En particulier, il permet à un site de fonctionner en coexistence sur IPv4 et IPv6, sans avoir à configurer les hôtes IPv6 avec des adresses compatibles IPv4 ou avec des tunnels. Les interfaces du routeur IPv6 et des hôtes auront, bien sûr, besoin d'être activées en mode "6sur4".

Un site peut choisir de commencer sa transition à IPv6 en configurant un routeur IPv6 pour prendre en charge "6sur4" sur une interface connectée au domaine IPv4 du site, et un autre format IPv6 sur une interface connectée à l'Internet IPv6. Tout hôte activé en "6sur4" dans le domaine IPv4 va alors être capable de communiquer à la fois avec le routeur et avec l'Internet IPv6, sans configuration manuelle d'un tunnel et sans avoir besoin d'une adresse IPv6 compatible IPv4, la configuration d'adresse sans état ou à états pleins fournissant l'adresse IPv6 de l'hôte IPv6.

Durant la transition, les routeurs peuvent avoir besoin d'annoncer au moins deux préfixes IPv6, un pour le LAN natif (par exemple, Ethernet) et un pour "6sur4". Comme avec tout préfixe IPv6 alloué à un sous-réseau IPv6, le premier DOIT être unique au sein de sa portée, qu'on utilise un adressage de site local ou mondial.

Noter aussi que lorsque un routeur traite aussi bien un LAN natif qu'un "6sur4" sur la même interface physique, durant l'autoconfiguration sans état, il y a une période pendant laquelle les adresses IPv6 de liaison locale sont utilisées dans les deux cas avec le préfixe FE80::/64. Noter que la longueur du préfixe pour ces adresses de liaison locale DOIT alors être de 128 afin qu'on puisse distinguer les deux cas.

Lorsque le site installe des routeurs IPv6 supplémentaires, les hôtes "6sur4" qui deviennent physiquement adjacents aux routeurs IPv6 peuvent être changés pour fonctionner comme des hôtes IPv6 natifs, le seul impact sur les applications IPv6 étant une légère augmentation de la taille de la MTU. À certaines étapes de la transition, il peut être pratique de donner un double rattachement à des hôtes dans les deux modes LAN natif et "6sur4", mais ce n'est pas obligé.

8. Considérations relatives à l'IANA

Aucune allocation n'est requise de l'IANA au delà de celles qui figurent dans la [RFC2365].

9. Considérations pour la sécurité

Ceux qui mettent en œuvre le présent document devraient être conscients que, en plus de possibles attaques contre IPv6, des atteintes à la sécurité menées contre IPv4 doivent aussi être prises en considération. L'utilisation de la sécurité IP aux deux niveaux de IPv4 et IPv6 devrait néanmoins être évitée, pour des raisons d'efficacité. Par exemple, si IPv6 fonctionne avec chiffrement, le chiffrage de IPv4 serait redondant sauf si on pense que l'analyse de trafic est une menace. Si IPv6 fonctionne avec authentification, alors l'authentification de IPv4 n'apportera pas grand chose. À l'inverse, la sécurité IPv4 ne va pas protéger le trafic IPv6 une fois qu'il a quitté le domaine IPv6 sur IPv4. Donc, la mise en œuvre de la sécurité IPv6 est exigée même si la sécurité IPv4 est disponible.

Il y a une attaque d'usurpation d'identité possible dans laquelle des paquets 6sur4 parasites sont injectés dans un domaine 6sur4 de l'extérieur. Donc, les routeurs frontières DOIVENT éliminer les paquets IPv4 en diffusion groupée qui ont des adresses de diffusion groupée de source ou de destination de portée d'organisation locale comme défini à la section 6 ci-dessus, si ils arrivent sur des interfaces physiques en-dehors de cette portée. Pour se défendre contre les paquets 6sur4 en envoi individuel parasites, les routeurs frontières DOIVENT éliminer les paquets IPv4 entrants avec un type de protocole de 41 qui proviennent de sources inconnues, c'est-à-dire que les tunnels IPv6 dans IPv4 ne doivent être acceptés que de sources de confiance. Sauf si l'authentification IPsec est disponible, la technique RECOMMANDÉE pour cela est de configurer le routeur frontière à n'accepter de paquets de type de protocole 41 que d'adresses de source qui sont dans une ou des gammes de confiance.

Remerciements

L'idée de base présentée ici n'est pas originale, et nous avons reçu des commentaires d'une valeur inestimable de Matt Crawford, Steve Deering, Dan Harrington, Rich Draves, Erik Nordmark, Quang Nguyen, Thomas Narten, et autres membres des groupes de travail IPNG et NGTRANS.

Le présent document est largement dérivé de la RFC 1972 écrite par Matt Crawford. Brian Carpenter était au CERN lorsque ce travail a été commencé.

Références

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC4291) *(PS)*

[RFC2365] D. Meyer, "Diffusion groupée sur IP limitée administrativement", juillet 1998. (BCP0023)

[RFC2462] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", décembre 1998. (*Obsolète, voir* RFC4862) *(D.S.)*

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par RFC5095, D.S)*

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

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC1933] R. Gilligan, E. Nordmark, "Mécanismes de transition pour hôtes et routeurs IPv6", avril 1996. (*Obsolète., voir* RFC2893) *(P.S.)*

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

[RFC1972] M. Crawford, "Méthode de transmission de paquets IPv6 sur réseaux Ethernet", août 1996. (*Obsolète, voir* RFC2464) *(P.S.)*

Appendice A : Adresses IPv4 de diffusion groupée pour la découverte de voisin

Les groupes de diffusion groupée IPv4 suivants sont utilisés pour prendre en charge la découverte de voisins avec la présente spécification. Les adresses IPv4 énumérées dans la présente section ont été obtenues en regardant les adresses de diffusion groupée IPv6 qu'utilise la découverte de voisins, et en déduisant les adresses IPv4 résultantes de "couche de liaison virtuelle" qui sont générées à partir d'elles en utilisant l'algorithme de la Section 6.

Adresse de diffusion groupée Tous les nœuds
C'est l'adresse de diffusion groupée IPv4 à portée limitée administrativement utilisée pour atteindre tous les nœuds dans le domaine IPv4 local qui prend en charge la présente spécification : 239.OLS.0.1

Adresse de diffusion groupée Tous les routeurs
C'est l'adresse de diffusion groupée IPv4 à portée limitée administrativement utilisée pour atteindre tous les routeurs dans le domaine IPv4 local qui prend en charge la présente spécification : 239.OLS.0.2

Adresse de diffusion groupée de nœud sollicité
C'est une adresse de diffusion groupée à portée limitée administrativement qui est calculée comme une fonction de l'adresse de la cible sollicitée en prenant les 24 bits de moindre poids de l'adresse IPv4 utilisée pour former l'adresse IPv6, et en ajoutant le préfixe FF02:0:0:0:0:1:FF00::/104 [RFC2373]. Cela est ensuite transposé en l'adresse de diffusion groupée IPv4 par la méthode décrite dans ce document. Par exemple, si l'adresse IPv4 utilisée pour former l'adresse IPv6 est W.X.Y.Z, alors l'adresse IPv6 de diffusion groupée du nœud sollicité est FF02::1:255.X.Y.Z et l'adresse IPv4 de diffusion groupée correspondante est 239.OLS.Y.Z

Adresse des auteurs

Brian E. CarpenterInternet Division
IBM United Kingdom Laboratories
MP 185, Hursley Park
Winchester, Hampshire S021 2JN, UK
mél : brian@hursley.ibm.com

Cyndi Jung
3Com Corporation
5400 Bayfront Plaza, Mailstop 3219
Santa Clara, California 95052-8145
mél : cmj@3Com.com

Déclaration complète de droits de reproduction

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