Groupe de travail Réseau
Request for Comments : 4604
RFC mises à jour : 3376, 3810
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

H. Holbrook, Arastra, Inc.
B. Cain, Acopia Networks
B. Haberman, JHU APL
août 2006

Utilisation du protocole de gestion de groupe Internet version 3 (IGMPv3) et du protocole de découverte de l'écouteur de diffusion groupée version 2 (MLDv2) pour la diffusion groupée spécifique de source

Résumé
Le protocole de gestion de groupe Internet version 3 (IGMPv3) et le protocole de découverte de l'écouteur de diffusion groupée version 2 (MLDv2) sont des protocoles qui permettent à un hôte d'informer les routeurs de son voisinage de son désir de recevoir des transmissions respectivement IPv4 et IPv6 en diffusion groupée. La diffusion groupée spécifique de source (SSM) est une forme de diffusion groupée dans laquelle un receveur est obligé de spécifier à la fois l'adresse de couche réseau de la source et l'adresse de destination de diffusion groupée afin de recevoir la transmission en diffusion groupée. Le présent document définit la notion de routeur et d'hôte "capable de SSM", et précise et (dans certains cas) modifie le comportement de IGMPv3 et MLDv2 sur les routeurs et hôtes capables de SSM pour s'accommoder de la diffusion groupée spécifique de source. Le présent document met à jour les spécifications IGMPv3 et MLDv2.

1. Introduction

Le protocole de gestion de groupe Internet (IGMP, *Internet Group Management Protocol*) [RFC1112], [RFC2236], [RFC3376] permet à un hôte IPv4 de communiquer des informations sur l'adhésion aux groupes de diffusion groupée IP à ses routeurs voisins. IGMP version 3 [RFC3376] procure à un hôte la capacité de demander de façon sélective ou de filtrer du trafic provenant de sources individuelles au sein d'un groupe de diffusion groupée.

Le protocole de découverte d'écouteur de diffusion groupée (MLD, *Multicast Listener Discovery Protocol*) [RFC2710], [RFC3810] offre une fonctionnalité similaire pour les hôtes IPv6. MLD version 2 (MLDv2) procure la fonctionnalité analogue de "filtrage de source" que IGMPv3 pour IPv6.

Du fait de la communauté de fonction, le terme de "protocole de gestion de groupe", ou "GMP", sera utilisé pour se référer à la fois à IGMP et à MLD. Le terme de "filtrage de source GMP", ou "SFGMP", sera utilisé pour se référer conjointement aux protocoles de gestion de groupe IGMPv3 et MLDv2.

L'utilisation de la diffusion groupée spécifique de source est facilitée par de petits changements aux protocoles SFGMP à la fois sur les hôtes et les routeurs. La [RFC4607] définit les "exigences générales" qui doivent être respectées par les systèmes qui mettent en œuvre le modèle de service SSM ; le présent document définit l'application concrètes de ces exigences pour les systèmes qui mettent en œuvre IGMPv3 et MLDv2. Ce faisant, le présent document définit des modifications aux portions hôte et routeur de IGMPv3 et MLDv2 à utiliser avec SSM, et présente un certain nombre de précisions sur leur comportement lorsque utilisées avec des adresses SSM. Le document met à jour les spécifications IGMPv3 et MLDv2.

1.1 Terminologie

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

Afin de souligner le parties du présent document qui modifient les spécifications actuelles des protocoles ([RFC2710, [RFC3810], [RFC3376]) par opposition à de simples précisions, toute modification de protocole est marquée "MODIFICATION".

2. Exigences d'hôte pour la diffusion groupée spécifique de source

La présente section définit la notion d'hôte "conscient de SSM" et décrit les exigences d'API et les exigences du protocole SFGMP sur un hôte conscient de SSM. Il est important de noter que SSM peut être utilisé par tout hôte qui prend en charge les API de filtrage de source et dont le système d'exploitation prend en charge le SFGMP approprié. Les modifications de SFGMP décrites dans cette section font mieux fonctionner SSM sur un hôte conscient de SSM, mais ne sont pas des exigences strictes de l'utilisation de SSM.

La gamme d'adresses 232/8 de IPv4 est actuellement allouée à SSM par l'IANA [IANA-ALLOCATION]. Dans IPv6, la gamme FF3x::/32 (où 'x' est une valeur valide de domaine de diffusion groupée IPv6) est réservée pour la sémantique de SSM [RFC3306], bien qu'aujourd'hui les allocations de SSM soient restreintes à FF3x::/96. (La [RFC4607] a une discussion très serrée sur ce sujet.) Un hôte qui connaît la gamme d'adresses SSM et est capable de lui appliquer la sémantique de SSM est décrit comme un hôte "conscient de SSM".

Un hôte ou un routeur peut être configuré pour appliquer la sémantique de SSM à des adresses autres que celles de la gamme allouée par l'IANA. Le module GMP sur un hôte ou un routeur DEVRAIT avoir une option de configuration pour établir la ou les gammes d'adresse SSM. Si cette option de configuration existe, elle DOIT par défaut revenir à la gamme SSM allouée par l'IANA. Le mécanisme d'établissement de cette option de configuration DOIT au moins permettre une configuration manuelle. Les mécanismes de protocole pour établir cette option pourront être définis à l'avenir.

2.1 Exigences d'API

Si le module IP d'hôte d'un hôte conscient de SSM reçoit une demande non spécifique de source pour recevoir du trafic en diffusion groupée envoyé à une adresse de destination SSM, il DEVRAIT retourner une erreur à l'application, comme spécifié dans la [RFC3678] (MODIFICATION). Sur un hôte non conscient de SSM, une application qui utilise la mauvaise API (par exemple, "join(G)", "IPMulticastListen(G,EXCLUDE(S1))" pour IGMPv3, ou "IPv6MulticastListen(G,EXCLUDE(S2))" pour MLDv2) pour demander la livraison des paquets envoyés à une adresse SSM ne recevra pas le service demandé, parce qu'un routeur capable de SSM (suivant les règles du présent document) refusera de traiter la demande, et l'application ne recevra pas d'indication autre qu'un échec à recevoir le trafic demandé.

2.2 Exigences de GMP

Ce paragraphe définit le comportement du module de protocole SFGMP d'un hôte conscient de SSM, y compris deux modifications au protocoles comme décrit dans les [RFC3376], [RFC3810]. Il inclut aussi un certain nombre de précisions sur les opérations de protocole. Ce faisant, il expose le comportement d'un hôte conscient de SSM en ce qui concerne l'envoi et la réception des types suivants de message GMP :

- Rapports IGMPv1/v2 et MLDv1 (2.2.1)
- Rapports IGMPv3 et MLDv2 (2.2.2)
- Interrogations IGMPv1, interrogations générales IGMPv2 et MLDv1 (2.2.3)
- Quitter IGMPv2 et MLDv1 Done (2.2.4)
- Interrogation spécifique de groupe IGMPv2 et MLDv1 (2.2.5)
- Interrogation spécifique de groupe IGMPv3 et MLDv2 (2.2.6)
- Interrogation spécifique de groupe et de source IGMPv3 et MLDv2 (2.2.7)

2.2.1 Rapports IGMPv1/v2 et MLDv1

Un hôte conscient de SSM fonctionnant conformément aux [RFC3376], [RFC3810] pourrait envoyer un rapport IGMPv1, IGMPv2, ou MLDv1 pour une adresse SSM lorsqu'il fonctionne dans un "mode de compatibilité d'une version plus ancienne." C'est une condition (d'erreur) exceptionnelle, qui indique que le ou les routeurs ne peuvent pas fournir la prise en charge de SFGMP nécessaire pour SSM, et une erreur est enregistrée lorsque l'hôte entre en mode de compatibilité pour une adresse SSM, comme décrit ci-dessous. Dans cette situation, il est vraisemblable que le trafic envoyé à un canal (S,G) ne sera pas livré à l'hôte de réception qui a demandé à recevoir le canal (S,G).

Les [RFC3376] et [RFC3810] spécifient qu'un hôte PEUT permettre qu'un rapport de version plus ancienne supprime son propre enregistrement d'adhésion IGMPv3 ou MLDv2. Cependant, un hôte conscient de SSM NE DOIT PAS permettre que son rapport soit supprimé dans cette situation (MODIFICATION). La suppression de rapports dans ce scénario serait la porte ouverte à des attaques de déni de service SSM aux autres hôtes sur la liaison.

2.2.2 Rapports IGMPv3 et MLDv2

Une mise en œuvre d'hôte peut rapporter plus d'un seul canal SSM dans un seul rapport soit en incluant plusieurs sources au sein d'un enregistrement de groupe, soit en incluant plusieurs enregistrements de groupe.

Un enregistrement de groupe pour une adresse de destination spécifique de la source peut (en fonctionnement normal) être d'un des types suivants :
- MODE_IS_INCLUDE au titre de l'enregistrement de l'état actuel
- ALLOW_NEW_SOURCES au titre de l'enregistrement de changement d'état
- BLOCK_OLD_SOURCES au titre de l'enregistrement de changement d'état

Un rapport peut inclure à la fois des adresses de destination SSM et non spécifiques de source, c'est-à-dire, des adresses de destination toute source en diffusion groupée (ASM, *Any-Source Multicast*), dans le même message.

De plus, un enregistrement CHANGE_TO_INCLUDE_MODE peut être envoyé par un hôte dans certains cas, par exemple, lorsque la gamme des adresses SSM est changée par la configuration. Un routeur devrait traiter un tel enregistrement conformément aux règles SFGMP normales.

Un hôte conscient de SSM NE DEVRAIT PAS envoyer les types d'enregistrements suivants pour une adresse SSM.
- MODE_IS_EXCLUDE au titre de l'enregistrement de l'état actuel
- CHANGE_TO_EXCLUDE_MODE au titre d'un enregistrement Changer-de-Mode-de-Filtre

C'est une MODIFICATION à [RFC3376], [RFC3810], qui impose une restriction de son utilisation pour les adresses de destination SSM. La raison en est que le mode EXCLUDE ne s'applique pas aux adresses SSM, et un routeur capable de SSM ignorera les demandes MODE_IS_EXCLUDE et CHANGE_TO_EXCLUDE_MODE dans la gamme SSM, comme décrit ci-dessous.

2.2.3 Interrogations IGMPv1, interrogations générales IGMPv2 et MLDv1

Si une Interrogation IGMPv1, ou une Interrogation générale IGMPv2 ou MLDv1 est reçue, les spécifications du protocole SFGMP exigent que l'hôte revienne à l'ancien mode de fonctionnement (IGMPv1, IGMPv2, ou MLDv1) sur cette interface. Si cela se produit, l'hôte arrêtera de rapporter des abonnements spécifiques de source sur cette interface et commencera d'utiliser IGMPv1, IGMPv2, ou MLDv1 pour rapporter son intérêt pour toutes les adresses de destination SSM, non qualifiées par une adresse de source. Il en résulte que la sémantique SSM ne sera plus appliquée aux adresses de groupe en diffusion groupée par le routeur.

Un routeur conforme au présent document ne génèrera jamais d'interrogation IGMPv1, IGMPv2, ou MLDv1 pour une adresse dans la gamme SSM ; et donc, cette situation ne survient que si le routeur n'est pas conscient de SSM, ou si l'hôte et le routeur sont en désaccord sur la gamme d'adresses SSM (par exemple, si ils ont des configurations manuelles non cohérentes).

Un hôte DEVRAIT enregistrer une erreur si il reçoit une interrogation IGMPv1, IGMPv2, ou MLDv1 pour une adresse SSM (MODIFICATION).

Afin d'atténuer ce problème, il doit être administrativement assuré que tous les routeurs sur un réseau à support partagé donné sont conformes au présent document et sont en accord sur la gamme des adresses SSM.

2.2.4 IGMPv2 Leave et MLDv1 Done

Les messages IGMP Leave et MLD Done ne sont pas traités par les hôtes. Les messages IGMPv2 Leave et MLDv1 Done ne devraient pas être envoyés pour une adresse SSM, à moins que l'hôte émetteur soit repassé à un mode de compatibilité de version plus ancienne, avec toutes les précautions décrites ci-dessus.

2.2.5 Interrogation spécifique de groupe IGMPv2 et MLDv1

Si un hôte reçoit une interrogation spécifique de groupe IGMPv2 ou MLDv1 pour une adresse dans toute gamme spécifique

de source configurée, il devrait traiter normalement l'interrogation conformément à [RFC3376], [RFC2236], même si le groupe demandé est une adresse de destination spécifique de la source. La transmission d'une telle interrogation indique vraisemblablement que le routeur émetteur n'est pas conforme au présent document ou qu'il n'est pas configuré avec la ou les mêmes gammes d'adresses SSM que l'hôte de réception. Un hôte DEVRAIT inscrire une erreur dans ce cas (MODIFICATION).

2.2.6 Interrogation spécifique de groupe IGMPv3 et MLDv2

Si un hôte conscient de SSM reçoit une interrogation spécifique de groupe SFGMP pour une adresse SSM, il doit répondre par un rapport si le groupe correspond à l'adresse de destination spécifique de la source de l'un de ses canaux spécifiques de source souscrits, comme spécifié dans [RFC3376], [RFC3810].

La raison en est que, bien que dans la spécification actuelle du protocole SFGMP, un routeur n'aurait aucune raison d'en envoyer une, la sémantique d'une telle interrogation est bien définie dans cette gamme et des mises en œuvre futures pourraient avoir des raisons d'envoyer une telle interrogation. Soyez libéraux dans ce que vous acceptez.

2.2.7 Interrogation spécifique de groupe et de source IGMPv3 et MLDv2

Un routeur SFGMP utilise normalement une interrogation spécifique de groupe et de source pour interroger un canal SSM qu'un hôte a demandé à quitter via un enregistrement BLOCK_OLD_SOURCES. Un hôte doit répondre à une interrogation spécifique de groupe et de source pour laquelle le groupe et la source dans l'interrogation correspondent à tout canal pour lequel l'hôte a un abonnement, comme exigé par [RFC3376], [RFC3810]. L'utilisation d'une adresse SSM ne change pas ce comportement.

Un hôte doit être capable de traiter une interrogation avec une liste de plusieurs sources par groupe, comme là aussi exigé par [RFC3376], [RFC3810]. L'utilisation d'une adresse SSM ne change pas le comportement de SFGMP à cet égard.

3. Exigences de routeur pour la diffusion groupée spécifique de source

Les routeurs doivent être conscients de la gamme des adresses SSM afin de fournir le modèle de service SSM. Un routeur qui connaît la gamme des adresses SSM et est capable de lui appliquer la sémantique SSM comme décrit dans la présente section est décrit comme un routeur "conscient de SSM". Un routeur capable de SSM PEUT avoir une option de configuration pour appliquer la sémantique de SSM à des adresses autres que de la gamme allouée par l'IANA, mais si une telle option existe, elle DOIT revenir par défaut à la gamme allouée par l'IANA.

La présente section expose le comportement des routeurs en ce qui concerne les types suivants de messages SFGMP pour les adresses de destination spécifiques de la source :
- Rapports IGMPv3 et MLDv2 (3.1)
- Interrogations générales IGMPv3 et MLDv2 (3.2)
- Interrogations spécifiques de groupe IGMPv3 et MLDv2 (3.3)
- Interrogations spécifiques de groupe et source IGMPv3 et MLDv2 (3.4)
- Rapports IGMPv1/v2 et MLDv1 (3.5)
- Interrogations IGMPv1/v2 et MLDv1 (3.6)
- Quitter IGMPv2 et MLDv1 Done (3.7)

3.1 Rapports IGMPv3 et MLDv2

Les rapports SFGMP sont utilisés pour faire rapport des abonnements spécifiques de source dans la gamme des adresses SSM. Un routeur DEVRAIT ignorer un enregistrement de groupe d'un des types suivants si il se réfère à une adresse de destination SSM :
- Enregistrement d'état actuel MODE_IS_EXCLUDE
- Enregistrement de changement de mode de filtre CHANGE_TO_EXCLUDE_MODE

Un routeur PEUT choisir d'enregistrer une erreur dans l'un et l'autre cas. Il DOIT traiter tout autre enregistrement de groupe au sein du même rapport. Ces comportements sont des MODIFICATIONS à [RFC3376], MLDv2] pour empêcher des sémantiques non spécifiques de la source de s'appliquer aux adresses SSM, et éviter de revenir à un mode de compatibilité de version plus ancienne.

Un enregistrement de changement de mode de filtre CHANGE_TO_INCLUDE_MODE est traité selon les règles normales

de SFGMP ; le paragraphe 2.2.2 décrit un scénario légitime d'une telle situation potentielle :

3.2 Interrogations générales IGMPv3 et MLDv2

Un routeur SSM envoie des interrogations générales SFGMP périodiques conformément aux spécifications IGMPv3 et MLDv2. Aucun changement de comportement n'est exigé pour SSM.

3.3 Interrogations spécifiques de groupe IGMPv3 et MLDv2

Les routeurs SFGMP qui prennent en charge la diffusion groupée spécifique de source peuvent envoyer des interrogations spécifiques de groupe pour les adresses dans la gamme spécifique de la source. La présente spécification n'interdit pas explicitement un tel message, bien que, au moment de la rédaction de ce mémoire, un routeur conforme à [RFC3376], [RFC3810] n'en enverrait pas.

3.4 Interrogations spécifiques de groupe et de source IGMPv3 et MLDv2

Les interrogations spécifiques de groupe et de source SFGMP sont utilisées lorsque un receveur a indiqué qu'il n'est plus intéressé à recevoir du trafic d'une paire (S,G) particulière pour déterminer si il y reste des hôtes rattachés directement qui s'intéressent à cette paire (S,G). Les interrogations spécifiques de groupe et de source sont utilisées au sein de la gamme d'adresses spécifiques de source lorsque un routeur reçoit un enregistrement BLOCK_OLD_SOURCES pour un ou plusieurs groupes spécifiques de source. Ces interrogations sont envoyées normalement, conformément à [RFC3376], [RFC2236].

3.5 Rapports IGMPv1/v2 et MLDv1

Un rapport IGMPv1/v2 ou MLDv1 pour une adresse dans la gamme spécifique de source pourrait être envoyé par un hôte non conscient de SSM. Un routeur DEVRAIT ignorer tous les rapports de cette sorte et précisément NE DEVRAIT PAS les utiliser pour établir un état de transmission IP. C'est une MODIFICATION à [RFC3376], [RFC3810]. Un routeur PEUT enregistrer une erreur si il reçoit un tel rapport (c'est aussi une MODIFICATION).

3.6 Interrogations IGMPv1/v2 et MLDv1

Un routeur SFGMP qui perd le choix d'un interrogateur pour un routeur de version inférieure doit enregistrer une erreur, comme spécifié dans [RFC3376], [RFC3810].

3.7 IGMPv2 Leave et MLDv1 Done

Un message Quitter IGMPv2 ou MLDv1 Done peut être envoyé par un hôte non conscient de SSM. Un routeur DEVRAIT ignorer tous les messages de cette sorte dans la gamme d'adresses spécifiques de source et PEUT enregistrer une erreur (MODIFICATION).

4. Considérations pour la sécurité

Les modifications spécifiques de protocole décrites dans le présent document ne sont pas susceptibles de créer de problèmes de sécurité qui ne soient déjà présents lors de l'utilisation de IGMPv3 ou MLDv2 avec la diffusion groupée de style ASM. Le lecteur se reportera à la [RFC4607] pour une analyse des questions de sécurité spécifiques de SSM.

Il est important qu'un routeur n'accepte pas de demandes de réception non spécifiques de la source pour une adresse de destination SSM. Les règles de la [RFC3376] et de la [RFC3810] exigent qu'un routeur, à réception d'un tel rapport d'adhésion, revienne à un mode de compatibilité de version antérieure pour le groupe en question. Si le routeur devait revenir à cette situation, cela empêcherait un hôte capable de IGMPv3 de recevoir le service SSM pour cette adresse de destination, créant ainsi une potentialité d'attaque de déni de service SSM pour les autres hôtes sur la même liaison.

5. Remerciements

Les auteurs tiennent à remercier Vince Laviano, Nidhi Bhaskar, Steve Deering, Toerless Eckert, et Pekka Savola pour leurs apports et leur relecture attentive.

6. Références normatives

[RFC1112] S. Deering, "Extensions d'hôte pour la diffusion groupée IP", STD 5, août 1989.

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

[RFC2236] W. Fenner, "Protocole de gestion de groupe Internet, version 2", novembre 1997.

[RFC2710] S. Deering, W. Fenner et B. Haberman, "Découverte de l'écouteur de diffusion groupée (MLD) pour IPv6", octobre 1999.

[RFC3376] B. Cain, S. Deering, I. Kouvelas, B. Fenner et A. Thyagarajan, "Protocole de gestion de groupe Internet, version 3", octobre 2002.

[RFC3678] D. Thaler, B. Fenner et B. Quinn, "Extensions d'interface de prise pour filtres de source en diffusion groupée", janvier 2004.

[RFC3810] R. Vida et L. Costa, "Découverte de l'écouteur de diffusion groupée, version 2 (MLDv2) pour IPv6", juin 2004.

[RFC4607] H. Holbrook et B. Cain, "Diffusion groupée spécifique de source pour IP", août 2006.

8. Références informatives

[IANA-ALLOC] Internet Assigned Numbers Authority, http://www.iana.org/assignments/multicast-addresses.

[RFC3306] B. Haberman et D. Thaler, "Adresses de diffusion groupée IPv6 fondées sur le préfixe d'envoi individuel", août 2002.

Adresse des auteurs

Hugh Holbrook
Arastra, Inc.
P.O. Box 10905
Palo Alto, CA 94303
téléphone : +1 650 331-1620
mél : holbrook@arastra.com

Brad Cain
Acopia Networks
mél : bcain99@gmail.com

Brian Haberman
Johns Hopkins University Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723-6099
mél : brian@innovationslab.net

Déclaration complète de droits de reproduction

Propriété intellectuelle

pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif (IASA) de l'IETF.