Groupe de travail Réseau
Request for Comments : 4607
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

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

Diffusion groupée spécifique de source pour IP

Résumé
Les adresses IP version 4 (IPv4) dans la gamme 232/8 (232.0.0.0 à 232.255.255.255) sont conçues comme des adresses de destination de diffusion groupée spécifique de source (SSM, *source-specific multicast*) et sont réservée pour des applications et protocoles spécifiques de source. Pour IP version 6 (IPv6), le préfixe d'adresse FF3x::/32 est réservé pour la diffusion groupée spécifique de source. Le présent document définit une extension au service réseau Internet qui s'applique aux datagrammes envoyés aux adresses SSM et définit les exigences d'hôte et de routeur pour la prise en charge de cette extension.

Table des Matières

1. Introduction

Le modèle de service de diffusion groupée du protocole Internet (IP) est défini dans la [RFC1112]. La RFC1112 spécifie qu'un datagramme envoyé à une adresse de diffusion groupée IP G (de 224.0.0.0 à 239.255.255.255) est livré à chaque "module de protocole de couche supérieure" qui a demandé la réception des datagrammes envoyés à l'adresse G. La RFC1112 appelle "groupe hôte" le service réseau identifié par une adresse de destination de diffusion groupée G. Ce modèle accepte à la fois la communication de un à plusieurs et de plusieurs à plusieurs. Le présent document utilise le terme de diffusion groupée toutes sources (ASM, *Any-Source Multicast*) pour se référer au modèle de diffusion groupée défini dans la RFC1112. La [RFC3513] spécifie la forme des adresses de diffusion groupée IPv6 avec la sémantique de l'ASM.

Les adresses IPv4 dans la gamme 232/8 (de 232.0.0.0 à 232.255.255.255) sont actuellement désignées comme adresses de destination de diffusion groupée spécifique de source (SSM, *source-specific multicast*) et sont réservées pour les applications et protocoles spécifiques de source [IANA-ALLOC].

Pour IPv6, le préfixe d'adresse FF3x::/32 est réservé à la diffusion groupée spécifique de source, où 'x' est tout identifiant de portée valide, par la [RFC3306]. En utilisant la terminologie de la [RFC3306], toutes les adresses SSM doivent avoir P=1, T=1, et plen=0. La [RFC3307] rend obligatoire que le champ Préfixe réseau d'une adresse SSM soit aussi réglé à zéro, donc, toutes les adresses SSM tombent dans la gamme FF3x::/96. De futurs documents pourront permettre un champ Préfixe réseau différent de zéro si, par exemple, une nouvelle transposition d'adresse IP à adresse MAC était définie. Donc, l'allocation d'adresse devrait se faire dans la gamme FF3x::/96, mais un système devrait traiter tous les FF3x::/32 comme des adresses SSM, pour permettre la compatibilité avec d'éventuelles utilisations futures du champ Préfixe réseau.

Les adresses dans la gamme FF3x::4000:0001 à FF3x::7FFF:FFFF sont réservées dans la [RFC3307] pour l'allocation par l'IANA. Les adresses dans la gamme FF3x::8000:0000 à FF3x::FFFF:FFFF sont permises pour les allocations dynamiques par un hôte, comme décrit dans la [RFC3307]. Les adresses dans la gamme FF3x::0000:0000 à FF3x::3FFF:FFFF sont invalides comme adresses SSM IPv6. (La [RFC3307] indique que FF3x::0000:0001 à FF3x::3FFF:FFFF doivent régler P=0 et T=0, mais pour SSM, la [RFC3306] rend obligatoire que P=1 et T=1, d'où leur désignation comme invalides.) Le traitement d'un paquet envoyé à une telle adresse invalide est indéfini -- un routeur ou hôte PEUT choisir d'éliminer un tel paquet.

La sémantique de la livraison de la diffusion groupée spécifique de source est fournie pour un datagramme envoyé à une adresse SSM. C'est-à-dire qu'un datagramme avec l'adresse IP de source S et l'adresse de destination SSM G est livré à chaque "prise" de couche supérieure qui a spécifiquement demandé la réception des datagrammes envoyés à l'adresse G par la source S, et seulement à ces prises. Le service réseau identifié par (S,G), pour l'adresse SSM G et l'adresse d'hôte de source S, est appelé un "canal". À la différence du modèle ASM de la RFC1112, SSM ne fournit la prise en charge de la couche réseau que pour la livraison de un à plusieurs.

Les avantages de la diffusion groupée spécifique de source incluent :

- l'élimination de la livraison croisée du trafic lorsque deux sources utilisent simultanément la même adresse de destination spécifique de source. L'utilisation simultanée d'une adresse de destination SSM par plusieurs sources et différentes applications est explicitement acceptée.
- d'éviter d'avoir besoin d'une coordination inter hôtes lors du choix d'adresses spécifiques de source, comme conséquence de ce qui précède.
- d'éviter qu'il soit besoin de nombreux protocoles et algorithmes de routeur pour fournir le modèle de service ASM. Par exemple, les "arborescences partagées" et les points de rendez-vous du protocole PIM – Mode épars (PIM-SM) [RFC4601] ne sont pas nécessaires pour la prise en charge du modèle spécifique de source. Les mécanismes de routeur nécessaires pour la prise en charge de SSM sont en fait largement un sous ensemble de ceux qui sont utilisés pour la prise en charge d'ASM. Par exemple, le mécanisme d'arborescence de plus court chemin du protocole PIM-SM peut être adapté pour fournir la sémantique de SSM.

Comme dans ASM, l'ensemble des receveurs est inconnu d'un envoyeur SSM. Une source SSM n'a connaissance ni du nombre ni de l'identité des receveurs.

SSM convient particulièrement bien pour les applications de style dissémination avec un ou plusieurs envoyeurs dont les identités sont connues avant le début de l'application. Par exemple, une application de dissémination de données qui désire fournir une source de données secondaire en cas de défaillance de la source principale peut mettre cela en œuvre en utilisant un canal pour chaque source et les annoncer toutes deux aux receveurs. SSM peut être utilisé pour construire des applications multi sources où toutes les identités des participants ne sont pas connues à l'avance, mais la fonctionnalité de "rendez-vous" multi sources ne se produit pas à la couche réseau dans ce cas. Tout comme dans une application qui utilise l'envoi individuel comme transport sous-jacent, cette fonctionnalité peut être mise en œuvre par l'application ou par une bibliothèque de couche application.

La découverte des ressource de diffusion groupée d'une forme dans laquelle un client envoie une interrogation en diffusion groupée directement à un "groupe de localisation de service" sur lequel écoutent les serveurs n'est pas directement prise en charge par SSM.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Le présent document définit la sémantique des adresses de diffusion groupée spécifique de source et spécifie les politiques qui gouvernent leur utilisation. En particulier, il définit une extension au service réseau Internet qui s'applique aux

datagrammes envoyés aux adresses SSM et il définit des extensions d'hôtes pour la prise en charge du service réseau. Les hôtes, routeurs, applications, et protocoles qui utilisent ces adresses DOIVENT se conformer aux politiques présentées dans le présent document. La non conformité d'un hôte peut empêcher cet hôte ou les autres hôtes sur le même LAN de recevoir le trafic envoyé à un canal SSM. Le défaut de conformité d'un routeur peut causer la livraison du trafic SSM à des parties du réseau où il n'est pas voulu, surchargeant inutilement le réseau.

2. Sémantique des adresses de diffusion groupée spécifique de source

Le service de diffusion groupée spécifique de source se définit comme suit :

Un datagramme envoyé avec l'adresse IP de source S et l'adresse IP de destination G dans la gamme SSM est livré à chaque prise d'hôte qui a spécifiquement demandé la livraison des datagrammes envoyés par S à G, et seulement à ces prises.

Où; en utilisant la terminologie de la [RFC3376], "prise" est un paramètre spécifique de la mise en œuvre utilisé pour distinguer les différentes entités demandeuses (par exemple, des programmes ou des processus ou des points d'extrémité de communication au sein d'un programme ou processus) au sein de l'hôte demandeur ; le paramètre prise des appels du système BSD Unix en est un exemple spécifique.

Tout hôte peut envoyer un datagramme à toute adresse SSM, et la livraison est effectuée conformément à la sémantique ci-dessus.

L'interface de module IP avec les protocoles de couche supérieure est étendue pour permettre à une prise de "s'abonner" ou "se désabonner" à un canal particulier identifié par une adresse de destination SSM et une adresse IP de source. L'interface étendue est définie au paragraphe 4.1. Il n'est pas significatif pour une application ou un hôte de demander la réception des datagrammes envoyés à une adresse de destination SSM G, comme c'est accepté dans le modèle de diffusion groupée toutes sources, sans aussi spécifier une adresse de source correspondante, et les routeurs DOIVENT ignorer de telles demandes.

Plusieurs applications source sur différents hôtes peuvent utiliser la même adresse de destination SSM G sans conflit parce que les datagrammes envoyés par chaque hôte de source Si ne sont livrés qu'aux prises qui ont demandé la livraison des datagrammes envoyés à G spécifiquement par Si.

La propriété distinctive clé du modèle est qu'un canal est identifié (adressé) par la combinaison d'une adresse d'envoi individuel de source et d'une adresse de destination de diffusion groupée dans la gamme SSM. Ainsi, par exemple, le canal S,G = (192.0.2.1, 232.7.8.9) diffère de S,G = (192.0.2.2, 232.7.8.9), bien qu'ils aient la même portion d'adresse de destination.

De même, pour IPv6, S,G = (2001:3618::1, FF33::1234) et S,G = (2001:3618::2, FF33::1234) sont des canaux différents.

3. Terminologie

Pour réduire la confusion quand on parle des modèles de diffusion groupée toutes sources et spécifique de source, on utilise une terminologie différente pour chacun d'eux.

On utilise le terme de "canal" pour se référer au service associé à une adresse SSM. Un canal est identifié par la combinaison d'une adresse de destination SSM et d'une source spécifique, par exemple, une paire (S,G).

On utilise le terme "groupe hôte" (utilisé dans la RFC1112) pour se référer au service associé aux adresses "régulières" de diffusion groupée ASM (excluant celles de la gamme SSM). Un groupe hôte est identifié par une seule adresse de diffusion groupée.

Tout hôte peut envoyer à un groupe hôte, et de façon similaire, tout hôte peut envoyer à une adresse de destination SSM. Un paquet envoyé par un hôte S à une adresse de destination ASM G est livré au groupe hôte identifié par G. Un paquet envoyé par l'hôte S à une adresse de destination SSM G est livré au canal identifié par (S,G). Les opérations de réception permises sur un groupe hôte sont appelées "join(G)" et "leave(G)" (selon la RFC1112). Les opérations de réception permises sur un canal sont appelées "Subscribe(S,G)" et "Unsubscribe(S,G)".

Le tableau suivant résume la terminologie :

Modèle de service	**toute source**	**spécifique de source**
Abstraction de réseau :	groupe	canal
Identifiant :	G	S,G
Opérations de réception :	Join, Leave	Subscribe, Unsubscribe

On note que, bien que le présent document spécifie un nouveau modèle de service disponible aux applications, les protocoles et techniques nécessaires pour prendre en charge le modèle de service sont largement un sous ensemble de ceux utilisés pour la prise en charge de l'ASM.

4. Exigences pour l'hôte

Cette section décrit les exigences portant sur les hôtes qui prennent en charge la diffusion groupée spécifique de source, qui incluent :
- les extensions à l'interface de module IP
- les extensions au module IP
- l'allocation des adresses SSM

4.1 Extensions à l'interface de module IP

L'interface de module IP avec les protocoles de couche supérieure est étendue pour permettre aux protocoles de demander la réception de tous les datagrammes envoyés à un certain canal.

Subscribe (prise, adresse de source, adresse de groupe, interface)
Unsubscribe (prise, adresse de source, adresse de groupe, interface)

où
"prise" est défini à la Section 2,

et, en paraphrasant la [RFC3376],
"interface" est un identifiant local de l'interface réseau sur laquelle la réception du canal identifié par la paire (adresse de source, adresse de groupe) est à activer ou désactiver. Une valeur particulière peut être utilisée pour indiquer une interface "par défaut". Si la réception du même canal est désirée sur plusieurs interfaces, Subscribe est invoqué une fois pour chaque.

Les interfaces ci-dessus sont des interfaces fonctionnelles abstraites strictes -- la fonctionnalité peut être fournie d'une façon spécifique de la mise en œuvre. Sur un hôte qui prend en charge l'interface de programmation d'application de filtrage de source de diffusion groupée de la [RFC3678], par exemple, les interfaces Subscribe et Unsubscribe peuvent être prises en charge via cette API. Lorsque un hôte a été configuré à connaître la gamme d'adresses SSM (que le mécanisme de configuration soit manuel ou par l'intermédiaire d'un protocole) le système d'exploitation de l'hôte DEVRAIT retourner une erreur à une application qui fait une demande non spécifique de source pour recevoir de la diffusion groupée envoyée à une adresse de destination SSM.

Un hôte qui ne prend pas en charge des interfaces de module IP (par exemple, des hôtes seulement en ASM) et leurs protocoles sous-jacents ne peut pas s'attendre à recevoir de façon fiable le trafic envoyé sur un canal SSM. Comme spécifié ci-dessous au paragraphe 5.2, les routeurs ne vont pas établir l'état de transmission SSM ou transmettre de datagrammes en réponse à une demande ASM Join.

Les mises en œuvre les plus courantes de l'interface de réception de paquet IP (par exemple, l'invocation de système recvfrom() dans le BSD Unix) ne permettent pas à un receveur de déterminer l'adresse de destination à laquelle a été envoyé un datagramme. Sur un hôte qui a une telle mise en œuvre, l'adresse de destination d'un datagramme ne peut pas être déduite lorsque la prise sur laquelle le datagramme est reçu est abonnée à plusieurs canaux. Les systèmes d'exploitation d'hôtes DEVRAIENT donner à un hôte les moyens de déterminer les deux adresses de source et de destination auxquelles un datagramme a été envoyé. (On a pour exemple le système d'exploitation Linux qui fournit la destination d'un paquet au titre de la réponse à l'invocation système recvmsg().) Jusqu'à ce que cette capacité soit présente, les applications peuvent être forcées d'utiliser des mécanismes de couche supérieure pour identifier le canal auquel un datagramme a été envoyé.

4.2 Exigence sur le module IP d'hôte

Un datagramme entrant destiné à une adresse SSM DOIT être livré par le module IP à toutes les prises qui ont indiqué (via Subscribe) leur désir de recevoir les données qui correspondent à l'adresse de source, à l'adresse de destination, et à l'interface d'arrivée du datagramme. Il NE DOIT PAS être livré aux autres prises.

Lorsque la première prise sur l'hôte H s'abonne à un canal (S,G) sur l'interface I, le module IP de l'hôte sur H envoie une demande sur l'interface I pour indiquer aux routeurs du voisinage que l'hôte souhaite recevoir le trafic envoyé par la source S à la destination de diffusion groupée spécifique de source G. De même, lorsque la dernière prise sur un hôte se désabonne d'un canal sur une interface I, le module IP d'hôte envoie une demande de désabonnement pour ce canal à l'interface I.

Ces demandes vont normalement être des messages du protocole de gestion de groupe Internet version 3 (IGMPv3, *Internet Group Management Protocol version 3*) pour IPv4, ou des messages de découverte d'écouteur de diffusion groupée version 2 (MLDv2, *Multicast Listener Discovery Version 2*) pour IPv6 [RFC3376], [RFC3810]. Un hôte qui accepte le modèle de service SSM DOIT mettre en œuvre la portion hôte de la [RFC3376] pour IPv4 et de la [RFC3810] pour IPv6. Il DOIT aussi se conformer au comportement IGMPv3/MLDv2 décrit dans la [RFC4604].

4.3 Allocation des adresses de diffusion groupé spécifiques de source

L'adresse de destination SSM 232.0.0.0 est réservée, et elle ne doit pas être utilisée comme adresse de destination. De même, FF3x::4000:0000 est aussi réservée. L'objectif de la réservation de ces deux adresses est de préserver une destination SSM invalide pour IPv4 et IPv6, qui peuvent être utiles dans une mise en œuvre sur une valeur nulle. La gamme d'adresses de 232.0.0.1 à 232.0.0.255 est actuellement réservée pour des allocations par l'IANA. Les adresses de destination SSM dans la gamme FF3x::4000:0001 à FF3x::7FFF:FFFF sont également réservées pou l'allocation par l'IANA [RFC3307]. La raison de la réservation de ces adresses est précisé à la Section 9, "Considérations relatives à l'IANA".

La politique d'allocation du reste des adresses SSM aux applications envoyeuses est déterminée de façon strictement locale par l'hôte envoyeur.

Lors d'une allocation dynamique des adresses SSM, un hôte ou le système d'exploitation d'un hôte NE DOIT PAS allouer à la suite en commençant par la première adresse permise. Il est RECOMMANDÉ d'allouer au hasard les adresses SSM aux applications, tout en s'assurant que les adresses allouées ne sont pas données simultanément à plusieurs applications (et en évitant les adresses réservées). Pour IPv6, l'aléation devrait s'appliquer aux 31 bits de moindre poids de l'adresse.

Comme décrit à la Section 6, la transposition d'un paquet IP avec une adresse de destination SSM en une adresse de diffusion groupée de couche liaison ne tient pas compte de l'adresse IP de source du datagramme (sur les couches de liaison couramment utilisées comme Ethernet). Si tous les hôtes commençaient par la première adresse permise, il serait alors très probable que de nombreux canaux spécifiques de source sur des réseaux de zone locale à support partagé utiliseraient la même adresse de diffusion groupée de couche liaison. Il en résulterait que le trafic destiné à un abonné à un canal serait livré au module IP d'un autre, qui devrait alors éliminer le datagramme.

Un système d'exploitation d'hôte DEVRAIT fournir une interface pour permettre à une application de demander une allocation unique d'une adresse de destination de canal à l'avance du commencement d'une session, et cette base de données d'allocation DEVRAIT persister à travers les réamorçages d'hôte. En fournissant des allocations persistantes, une application d'hôte peut annoncer la session à l'avance de son début sur une page de la Toile ou dans un autre répertoire. (On note que cette question n'est pas spécifique des applications SSM -- le même problème survient pour ASM.)

Le présent document ne définit pas les interfaces pour demander ou retourner les adresses ni ne spécifie les algorithmes des hôtes pour mémoriser ces allocations. Une API abstraite plausible est définie dans la [RFC2771]. Noter que la RFC2771 permet à une application de demander une adresse au sein d'une gamme spécifique d'adresses. Si cette interface est utilisée, l'adresse de début de la gamme DEVRAIT être choisie au hasard par l'application.

Pour IPv6, les adresses de canal à portée limitée administrativement sont créées en choisissant un identifiant de portée approprié pour l'adresse de destination SSM. Des frontières normales de portée de diffusion groupée IPv6 [RFC4007] sont appliquées au trafic envoyé à une adresse de destination SSM, incluant toutes frontières pertinentes appliquées aux adresses de source comme de destination.

Aucune gamme d'adresses à portée limitée administrativement [RFC2365] mondialement acceptée n'est actuellement définie pour la diffusion groupée IPv4 spécifique de source. Pour IPv4, la limitation administrative de portée des adresses SSM peut être mise en œuvre au sein d'un domaine administratif en filtrant le trafic SSM sortant envoyé à une adresse à portée limitée au routeurs frontière du domaine.

5. Exigences pour le routeur

5.1 Transmission de paquet

Un routeur qui reçoit un datagramme IP avec une adresse de destination spécifique de source DOIT l'éliminer en silence sauf si un hôte ou routeur voisin a communiqué son désir de recevoir les paquets envoyés de la source et à l'adresse de destination du paquet reçu.

5.2 Protocoles

Certains protocoles d'acheminement de diffusion groupée IP ont déjà la capacité de communiquer des adhésions spécifiques de source aux routeurs du voisinage (en particulier, PIM-SM [RFC4601]) et ces protocoles peuvent, avec de légères modifications, être utilisés pour fournir une sémantique spécifique de source. Un routeur qui prend en charge le modèle de service SSM DOIT mettre en œuvre le sous-ensemble PIM-SSM du protocole PIM-SM de la [RFC4601] et DOIT mettre en œuvre la portion routeur de la [RFC3376] pour IPv4 et de la [RFC3810] pour IPv6. Un routeur SSM DOIT aussi se conformer au comportement IGMPv3/MLDv2 décrit dans la [RFC4604].

Avec PIM-SSM, le bon établissement d'un chemin de transmission (S,G) depuis la source S jusqu'à tous les receveurs dépend de la transmission bond par bond de la demande d'adhésion explicite du receveur vers la source. Le ou les protocoles et algorithmes qui sont utilisés pour choisir le chemin de transmission de cette adhésion explicite doivent assurer un chemin sans boucle. Lors de l'utilisation de PIM-SSM, la mise en œuvre de PIM-SSM DOIT (au moins) prendre en charge la capacité d'utiliser à cette fin la base de données de topologie d'envoi individuel.

Un réseau peut prendre concurremment en charge SSM dans la gamme d'adresses SSM et la diffusion groupée toutes sources dans le reste de l'espace d'adresses de diffusion groupée, et il est prévu que ce soit très courant. Dans un tel réseau, un routeur peut recevoir une demande non spécifique de source, ou "(*,G)" dans la terminologie conventionnelle, pour livrer du trafic dans la gamme SSM à partir d'un voisin qui ne met pas en œuvre la diffusion groupée spécifique de source d'une manière conforme au présent document. Un routeur qui reçoit une telle demande non spécifique de source pour des données dans la gamme SSM NE DOIT PAS utiliser la demande pour établir un état de transmission et NE DOIT PAS propager la demande aux autres routeurs du voisinage. Un routeur PEUT enregistrer une erreur dans un tel cas. Cela s'applique à la fois à toute demande reçue d'un hôte (par exemple, un rapport d'hôte IGMPv1 ou IGMPv2 [RFC2236]) et à toute demande reçue d'un protocole d'acheminement (par exemple, une adhésion PIM-SM (*,G)). Le cas de l'inter-routeur est exposé plus en détails à la Section 8, "Considérations de transition".

Il est essentiel que tous les routeurs du réseau donnent une sémantique spécifique de source à la même gamme d'adresses afin de tirer le meilleur parti de SSM. Pour se conformer à la présente spécification, un routeur DOIT traiter TOUTES les adresses SSM allouées par l'IANA avec la sémantique spécifique de source.

6. Transmission des datagrammes à la couche liaison

Les paquets de diffusion groupée spécifique de source sont transmis sur les réseau de couche liaison comme spécifié dans la [RFC1112] pour IPv4 et comme dans la [RFC2464] pour IPv6. Sur la plupart des réseaux de couche liaison à support partagé qui prennent en charge la diffusion groupée (par exemple, Ethernet) l'adresse IP de source n'est pas utilisée dans le choix de l'adresse de destination de couche liaison. Par conséquent, sur un tel réseau, tous les paquets envoyés à l'adresse de destination G seront livrés à tout hôte qui s'est abonné à tout canal (S,G), sans considération de S. Donc, le module IP DOIT filtrer les paquets qu'il reçoit de la couche liaison avant de les livrer à la couche de prise.

7. Considérations sur la sécurité

La présente section développe les questions de sécurité qui relèvent de SSM. Les sujets suivants sont traités : IPsec, attaques de déni de service, falsification de source, et questions de sécurité en rapport avec la limitation administrative de portée.

7.1 IPsec et SSM

L'en-tête d'authentification IPsec (AH, *Authentication Header*) et l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) peuvent être utilisés pour sécuriser le trafic SSM, si une mise en œuvre d'IPsec à capacité de diffusion groupée (comme exigé dans la [RFC4301]) est utilisée par les receveurs.

7.2 SSM et IPsec (RFC2401)

Pour les mises en œuvre existantes d'IPsec de la [RFC2401] (maintenant subrogée par la [RFC4301]) il y a quelques avertissements en rapport avec SSM. Leur liste est donnée ici. Dans l'IPsec de la RFC2401, l'adresse de source n'est pas utilisée au titre de la clé dans la recherche de base de données d'association de sécurité (SAD, *Security Association Database*). Il en résulte que deux envoyeurs qui se trouvent utiliser la même adresse de destination SSM et le même indice de paramètre de sécurité (SPI, *Security Parameter Index*) vont "entrer en collision" dans la SAD chez tout hôte qui reçoit les deux canaux. Comme les adresses de canal et les SPI sont tous deux alloués de façon autonome par les envoyeurs, il n'y a pas de moyen raisonnable pour s'assurer que chaque envoyeur utilise une adresse de destination ou un SPI unique.

Un problème survient si un receveur s'abonne simultanément à deux canaux sans relations en utilisant IPsec et si les sources se trouvent utiliser la même adresse de destination IP (IPDA, *IP destination address*) et le même SPI IPsec. Comme les adresses de destination de canal sont allouées de façon autonome par les envoyeurs, deux hôtes quelconques peuvent simultanément utiliser la même adresse de destination, et il n'y a pas de moyen raisonnable pour s'assurer que cela ne se produit pas. Le couple <IPDA,SPI>, consiste cependant en 56 bits qui sont généralement choisis au hasard (24 bits de la destination IP et 32 bits du SPI) et un conflit est peu probable.

Si une telle collision se produit, un receveur ne sera pas capable de recevoir simultanément du trafic protégé par IPsec des deux sources en collision. Un receveur peut détecter cette condition en remarquant qu'il reçoit du trafic de deux sources différentes avec le même SPI et la même adresse de destination SSM.

7.3 Déni de service

Une demande d'abonnement crée l'état (S,G) dans un routeur pour enregistrer l'abonnement, invoque le traitement sur ce routeur, et cause éventuellement le traitement chez les routeurs du voisinage. Un hôte peut monter une attaque de déni de service en demandant un grand nombre d'abonnements. Il peut en résulter un déni de service si :

- une grande quantité de trafic arrive alors qu'il est par ailleurs non désiré, consommant les ressources du réseau pour le livrer et les ressources de l'hôte pour l'éliminer ;
- une grande quantité d'état de diffusion groupée spécifique de source est créée dans les routeurs du réseau, utilisant de la mémoire de routeur et des ressources de CPU pour mémoriser et traiter l'état ; ou
- une grande quantité de trafic de contrôle est générée pour gérer l'état spécifique de source, utilisant la CPU du routeur et la bande passante du réseau.

Pour réduire les dommages d'une telle attaque, un routeur PEUT avoir des options de configuration pour limiter, par exemple, les éléments suivants :

- le taux total auquel tout hôte est autorisé sur toute interface à initier des abonnements (pour limiter les dommages causés par les attaques d'adresse source falsifiée) ;
- le nombre total d'abonnements qui peuvent être initiés à partir de toute interface ou hôte.

Toute décision d'une mise en œuvre de limiter artificiellement le taux ou le nombre des abonnements devrait cependant être prise avec précaution, car les futures applications pourraient utiliser de grands nombres de canaux. Des limites strictes sur le taux ou le nombre d'abonnements de canaux entraveraient le développement de telles applications.

Un routeur DEVRAIT vérifier que la source d'une demande d'abonnement est une adresse valide pour l'interface sur laquelle elle a été reçue. Manquer à le faire exacerberait l'attaque d'adresse de source falsifiée.

On note que ces attaques ne sont pas le privilège de SSM – elles sont aussi présentes dans la diffusion groupée toutes sources.

7.4 Adresses de source falsifiées

En falsifiant l'adresse de source dans un datagramme, un attaquant peut éventuellement violer le modèle de service SSM en transmettant des datagrammes sur un canal qui appartient à un autre hôte. Donc, une application qui exige une authentification forte ne devrait pas supposer que tous les paquets qui arrivent sur un canal ont été envoyés par la source demandée sans des mécanismes d'authentification de couche supérieure. L'en-tête d'authentification IPSEC [RFC2401], [RFC4301] peut être utilisé pour authentifier la source d'une transmission SSM, par exemple.

Un certain niveau de protection contre les adresses de source falsifiées dans la diffusion groupé est déjà largement répandu,

parce que les protocoles d'acheminement de diffusion groupée IP actuellement déployés [RFC1075], [RFC3973], [RFC4601] incorporent une "vérification de transmission sur le chemin inverse" qui valide qu'un paquet en diffusion groupée est arrivé sur l'interface attendue pour son adresse de source. Les protocoles d'acheminement utilisés pour SSM DEVRAIT incorporer une telle vérification.

L'acheminement de source [RFC0791] (aussi bien Lâche que Strict) en combinaison avec la falsification d'adresse de source peut être utilisé pour permettre à un imposteur sur la vraie source du canal d'injecter des paquets sur un canal SSM. Un routeur SSM DEVRAIT par défaut désactiver l'acheminement de source sur une adresse de destination SSM. Un routeur PEUT avoir une option de configuration pour permettre l'acheminement de source. Des mécanismes contre la falsification de source, comme un filtrage d'adresse de source aux bordures du réseau, sont aussi fortement encouragés.

7.5 Portée administrativement limitée

La limitation administrative de portée ne devrait être considérée comme une mesure de sécurité [RFC2365] ; cependant, dans certains cas, elle peut être une partie d'une solution de sécurité. On devrait noter qu'il n'existe aucune limitation administrative de portée pour la diffusion groupée spécifique de source IPv4. Une approche de remplacement est de configurer manuellement le filtrage du trafic pour créer si nécessaire une telle limitation de portée.

De plus, pour IPv6, la limitation de portée d'adresse ni de source ni de destination ne devrait être utilisée comme mesure de sécurité. Dans certains routeurs IPv6 actuellement déployés (ceux qui ne se conforment pas à la [RFC4007]), les limites de portée ne sont pas toujours appliquées à toutes les adresses de source (par exemple, une mise en œuvre peut filtrer les adresses de liaison locale et rien d'autre). Un tel routeur peut incorrectement transmettre un canal SSM (S,G) à travers une limite de portée pour S.

8. Considérations sur la transition

Un hôte qui se conforme au présent document va envoyer SEULEMENT des rapports d'hôte spécifiques de source pour les adresses dans la gamme SSM. Comme on l'a dit plus haut, un routeur qui reçoit un rapport d'hôte non spécifique de source (par exemple, IGMPv1 ou IGMPv2 ou MLDv1 [RFC2710]) pour une adresse de destination de diffusion groupée spécifique de source DOIT ignorer ces rapports. Manquer à le faire violerait le modèle de service SSM promis à l'envoyeur : qu'un paquet envoyé à (S,G) ne sera livré qu'aux hôtes qui ont spécifiquement demandé la livraison des paquets envoyés à G par S.

Durant une période de transition, il serait possible de livrer des datagrammes SSM dans un domaine où les routeurs ne prennent pas en charge la sémantique SSM en transmettant simplement tout paquet destiné à G à tous les hôtes qui ont demandé l'abonnement de (S,G) pour tout S. Cependant, cette mise en œuvre risque de surcharger indûment l'infrastructure du réseau en livrant les datagrammes (S,G) aux hôtes qui ne les ont pas demandé. Une telle mise en œuvre pour les adresses dans la gamme SSM est spécifiquement non conforme au paragraphe 5.2 du présent document.

9. Considérations relatives à l'IANA

L'IANA alloue les adresses IPv4 dans la gamme 232.0.0.1 à 232.0.0.255 et les adresses IPv6 dans la gamme FF3x:4000:0001 à FF3x::7FFF:FFFF. Ces adresses sont allouées selon le consensus de l'IETF [RFC2434]. Ces gammes d'adresses sont réservée pour les services d'une large applicabilité qui l'exigent ou qui tirerait un fort avantage que tous les hôtes utilisent une adresse de destination SSM bien connue pour ce service. Toute proposition d'allocation doit considérer le fait que, sur un réseau Ethernet, tous les datagrammes envoyés à toute adresse de destination SSM seront transmis avec la même adresse de destination de couche liaison, sans considération de la source. De plus, le fait que les destinations SSM dans les tranches 232.0.0.0/24 et 232.128.0.0/24 utilisent les mêmes adresses de couche liaison que la gamme réservée du groupe de diffusion groupée IP 224.0.0.0/24 doit aussi être pris en considération. Une attention similaire devrait être portée aux adresses réservées de diffusion groupée IPv6. 232.0.0.0 et FF3x::4000:0000 ne devraient pas être allouées, comme on le suggère plus haut.

Sauf pour les adresses susmentionnées, l'IANA NE DEVRA PAS allouer d'adresse de destination SSM à une entité ou application particulière. Le faire compromettrait un des avantages importants du modèle spécifique de source : la capacité pour un hôte d'allouer simplement et de façon autonome une adresse de diffusion groupé spécifique de source à partir d'un grand espace d'adresses plat.

10. Remerciements

Le modèle de service SSM s'appuie sur divers travaux antérieurs sur d'autres approches de la diffusion groupée IP, incluant le modèle de diffusion groupée EXPRESS de Holbrook et Cheriton [EXPRESS], le [SMRP] de Green, et la proposition de diffusion groupée simple de Perlman, et al. [SIMPLE]. On tient aussi à remercier Jon Postel et David Cheriton de leur soutien pour la réallocation de la gamme d'adresses 232/8 au SSM. Brian Haberman a contribué à la portion IPv6 de ce document. Merci à Pekka Savola pour sa relecture attentive.

11. Références normatives

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

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989. *(Mise à jour par la* RFC 2236*)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2464] M. Crawford, "Transmission de paquets IPv6 sur réseaux Ethernet", décembre 1998. *(P.S.)*

[RFC3306] B. Haberman, D. Thaler, "Adresses de diffusion groupée IPv6 fondées sur des préfixes d'envoi individuel", août 2002. (*MàJ par* RFC3956, RFC4489 et RFC7371) *(P.S.)*

[RFC3307] B. Haberman, "Lignes directrices pour l'allocation des adresses de diffusion groupée IPv6", août 2002. *(P.S.)*

[RFC3376] B. Cain et autres, "Protocole Internet de gestion de groupe, IGMP version 3", octobre 2002. *(P.S.)*

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obs. voir* RFC4291)

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

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401*)*

[RFC4601] B. Fenner et autres, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : spécification du protocole (Révisée)", août 2006. (*Remplace* RFC2362) (*MàJ par* RFC5059) *(P.S.)*

[RFC4604] H. Holbrook et autres, "Utilisation de la version 3 du protocole de gestion de groupe Internet (IGMPv3) et de la version 2 du protocole de découverte d'écoutant de diffusion groupée (MLDv2) pour la diffusion groupée spécifique de source", août 2006. (*MàJ* RFC3376, RFC3810) *(P.S.)*

12. Références pour information

[EXPRESS] Holbrook, H., and Cheriton, D. "Explicitly Requested Source-Specific Multicast: EXPRESS support for Large-scale Single-source Applications". Proceedings of ACM SIGCOMM '99, Cambridge, MA, septembre 1999.

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

[RFC1075] D. Waitzman et autres, "Protocole d'acheminement en diffusion groupée par vecteur de distance", nov. 1988.

[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. *(Remplacée par RFC*3376*)*

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Obsolète, voir la RFC5226)*

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

[RFC2771] R. Finlayson, "API abstraite pour allocation d'adresse de diffusion groupée", février 2000. *(Information)*

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

[RFC3973] A. Adams et autres, "Diffusion groupée indépendante du protocole - Mode dense (PIM-DM) : Spécification du protocole (révisée)", janvier 2005. *(Expérimentale)*

[RFC4007] S. Deering et autres, "Architecture d'adresse IPv6 calibrée", mars 2005. *(P.S.)*

[SIMPLE] R. Perlman, C-Y. Lee, A. Ballardie, J. Crowcroft, Z. Wang, T. Maufer, C. Diot, and M. Green, "Simple Multicast: A Design for Simple, Low-Overhead Multicast", Work in Progress, October 1999.

[SMRP] Green, M. "Method and System of Multicast Routing for Groups with a Single Transmitter." United States Patent Number 5,517,494.

Adresse des auteurs

Brad Cain
Acopia Networks
mél : bcain99@gmail.com

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

Déclaration complète de droits de reproduction

Propriété intellectuelle

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.