Groupe de travail Réseau
Request for Comments : 3956
RFC mise à jour : 3306
Catégorie : En cours de normalisation

P. Savola, CSC/FUNET
B. Haberman, JHU APL
novembre 2004
Traduction Claude Brière de L'Isle

Incorporation de l'adresse de point de rendez-vous (RP) dans une adresse de diffusion groupée IPv6

Résumé
Le présent mémoire définit une politique d'allocation d'adresse dans laquelle l'adresse du point de rendez-vous (RP) est codée dans une adresse de groupe de diffusion groupée IPv6. Pour le mode épars de diffusion groupée indépendante du protocole (PIM-SM, *Protocol Independent Multicast - Sparse Mode*) ceci peut être vu comme une spécification d'un mécanisme de transposition de groupe en RP. Cela permet un déploiement aisé de diffusion groupée inter domaines adaptable et simplifie aussi la configuration de diffusion groupée intra domaine. Le présent mémoire met à jour le format d'adressage présenté dans la RFC 3306.

Table des Matières

1. Introduction

1.1 Fondements

Comme on l'a remarqué [V6MISSUES], il existe un problème de déploiement de la diffusion groupée IPv6 mondiale inter domaines : les points de rendez-vous PIM-SM [RFC4601] n'ont aucun moyen de communiquer les informations sur les sources (actives) de diffusion groupée aux autres domaines de diffusion groupée, car le protocole de découverte de source de diffusion groupée (MSDP, *Multicast Source Discovery Protocol*) [RFC3618] a été spécifié en excluant délibérément IPv6. Donc le modèle entier d'inter domaine de destination acceptant toute source en diffusion groupée (ASM, *Any Source Multicast*) est rendu inutilisable ; la diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) [RFC4607] évite ces problèmes mais n'est pas une solution complète pour plusieurs raisons, comme on l'exposera plus loin.

De plus, on a noté qu'il y a des problèmes avec la prise en charge et le déploiement des mécanismes qu'exigerait SSM [V6MISSUES] : il semble peu probable que SSM puisse être utilisable à court terme comme seul mécanisme d'acheminement de diffusion groupée inter domaines.

1.2 Solution

Le présent mémoire décrit une politique d'allocation d'adresse de diffusion groupée dans laquelle l'adresse du point de rendez-vous (RP) est codée dans l'adresse de groupe de diffusion groupée IPv6, et spécifie une transposition de groupe en RP PIM-SM pour utiliser le codage, la démultiplication, et l'extension de l'adressage fondé sur le préfixe d'envoi individuel [RFC3306].

Ce mécanisme ne fournit pas seulement une solution simple pour la diffusion groupée toutes sources inter domaines IPv6 mais peut aussi être utilisé comme solution simple pour l'ASM IPv6 intra domaine avec des adresses de diffusion groupée à portée limitée.

Il peut aussi être utilisé comme mécanisme automatique de découverte de RP dans les scénarios de déploiement qui auraient été précédemment utilisés par le protocole de routeur Bootstrap (BSR, *Bootstrap Router protocol*) [RFC5059].

La solution consiste en trois éléments :
- o la spécification d'une sous gamme d'adresses de groupe de diffusion groupée IPv6 [RFC3306] définie en réglant un bit précédemment non utilisé du champ Fanions à "1",
- o la spécification de la transposition par laquelle une telle adresse de groupe code l'adresse de RP qui doit être utilisée avec le groupe, et
- o une description des procédures de fonctionnement pour faire fonctionner ASM avec PIM-SM sur ces groupes de diffusion groupée IPv6.

Les adresses dans la sous gamme seront appelées des adresses de RP incorporés.

Ce schéma évite le besoin de MSDP, et les routeurs ne sont pas obligés d'inclure de configuration de diffusion groupée, sauf lorsque ils agissent comme RP.

Le présent mémoire met à jour le format d'adressage présenté dans la RFC 3306.

Certains compromis de conception sont exposés à l'Appendice A.

1.3 Hypothèses et domaine d'application

Une adresse de RP de 128 bits ne peut pas être incorporée dans une adresse de groupe de 128 bits avec de l'espace laissé pour porter l'identité du groupe lui-même. Une forme appropriée de codage est donc définie en exigeant que les identifiants d'interface des RP dans la gamme de RP incorporés puissent être alloués comme valeur spécifique.

Si ces hypothèses peuvent être satisfaites, les procédures et la configuration de fonctionnement doivent être légèrement changées, sinon le mécanisme ne peut être utilisé.

L'allocation d'adresses de diffusion groupée sort du domaine d'application du présent document ; il appartient au RP et aux applications de s'assurer que les adresses de groupe sont uniques en utilisant une méthode qui n'est pas spécifiée. Cependant, le mécanisme est probablement similaire à ceux utilisés avec la [RFC3306].

De façon similaire, les méthodes de gestion d'échec de RP, comme la diffusion de RP à la cantonade, sortent du domaine d'application du présent document. Elles ne fonctionnent pas sans une spécification ou déploiement supplémentaire. Ceci est traité brièvement au paragraphe 6.1.

1.4 Terminologie

Le RP incorporé se comporte comme si tous les membres du groupe étaient intra domaine pour la distribution des informations. Cependant, comme elle donne une solution pour la diffusion groupée IPv6 globale dans l'Internet, s'étendant sur plusieurs domaines administratifs, on dit que c'est une solution pour la diffusion groupée inter domaines.

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

1.5 Abréviations

ASM *(Any-Source Multicast)* : en diffusion groupée toute source
BSR *(Bootstrap Router)* : routeur d'amorçage
DR *(Designated Routeur)* : routeur désigné
IGP *(Interior Gateway Protocol)* : protocole de passerelle intérieure
MLD *(Multicast Listener Discovery)* : découverte d'écoutant de diffusion groupée
MSDP *(Multicast Source Discovery Protocol)* : protocole de découverte de source de diffusion groupée
PIM *(Protocol Independent Multicast)* : diffusion groupée indépendante du protocole
PIM-SM *(Protocol Independent Multicast – Sparse Mode)* : diffusion groupée indépendante du protocole en mode épars
RIID *(RP Interface ID)* : identifiant d'interface de point de rendez-vous
RP *(Rendezvous Point)* : point de rendez-vous
RPF *(Reverse Path Forwarding)* : transmission sur le chemin inverse
SPT *(shortest path tree)* : arborescence de plus court chemin
SSM *(Source-Specific Multicast)* : diffusion groupée spécifique de la source

2. Format d'adresse fondé sur le préfixe d'envoi individuel

Comme décrit dans la [RFC3306], le format d'adresse de diffusion groupée est le suivant :

```
|   8    |  4 |  4 |   8    | 8  |       64       |      32     |
+--------+----+----+--------+----+----------------+-------------+
|11111111|fans|port|réservé |plen| préfixe réseau | ID de groupe|
+--------+----+----+--------+----+----------------+-------------+
```

Où fans (fanions) est "0011". (Les deux premiers bits sont encore indéfinis, envoyés à zéro et ignorés à réception.)

3. Format d'adresse fondé sur le préfixe d'envoi individuel modifié

Le présent mémoire spécifie une modification au format d'adresse fondé sur le préfixe d'envoi individuel en spécifiant le second bit de poids fort ("bit R") comme suit :

```
|   8    |  4 |  4 |  4 |  4 | 8  |       64       |      32     |
+--------+----+----+----+----+----+----------------+-------------+
|11111111|fans|port|rsvé|RIID|plen| préfixe réseau | ID de groupe|
+--------+----+----+----+----+----+----------------+-------------+
                                          +-+-+-+-+
fans est un ensemble de quatre fanions :  |0|R|P|T|
                                          +-+-+-+-+
```

Lorsque le bit de poids fort est 0, R = 1 indique une adresse de diffusion groupée qui incorpore l'adresse sur le RP. P DOIT alors être réglé à 1, et par conséquent T DOIT être réglé à 1, comme spécifié dans la [RFC3306]. En effet, cela implique le préfixe FF70::/12. Dans ce cas, les quatre derniers bits du champ antérieurement réservé sont interprétés comme incorporant l'identifiant d'interface de RP, comme le spécifie le présent mémoire.

Le comportement est inspécifié si P ou T n'est pas réglé à 1, car alors le préfixe ne serait pas FF70::/12. De même, le codage et le mode de protocole utilisé lorsque deux bits de poids fort dans "fanions" sont réglés à 11 ("FFF0::/12") sont intentionnellement inspécifiés jusqu'au moment où le bit de poids fort sera défini. Sans autre spécification de l'IETF, les mises en œuvre NE DEVRAIENT PAS traiter la gamme FFF0::/12 comme un RP incorporé.

R = 0 indique une adresse de diffusion groupée qui n'incorpore pas l'adresse du RP et suit la sémantique définie dans les [RFC3513] et [RFC3306]. Dans ce contexte, la valeur de "RIID" DOIT être envoyée à zéro et DOIT être ignorée à réception.

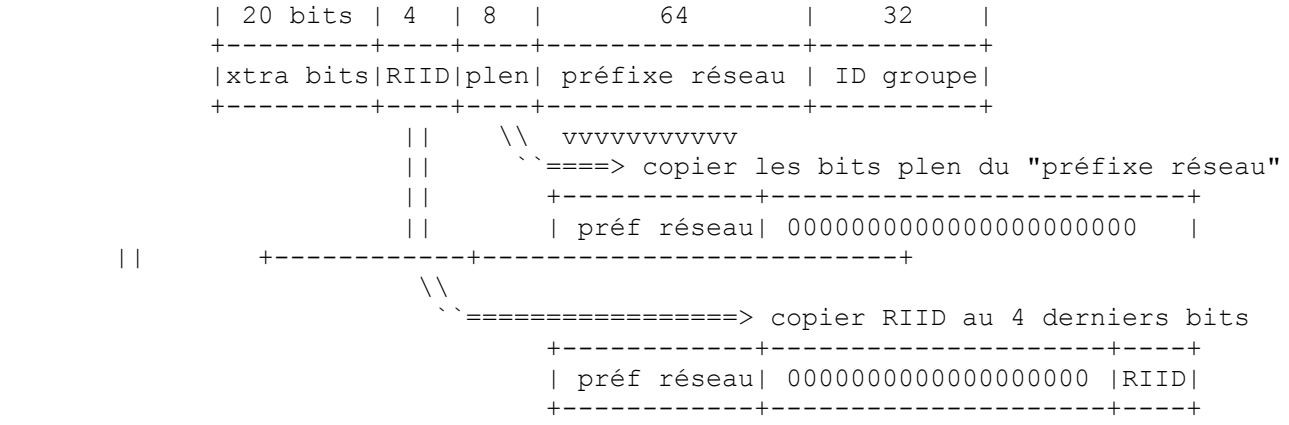
4. Incorporation de l'adresse du RP dans l'adresse de diffusion groupée

L'adresse du RP ne peut être incorporée que dans les adresses ASM fondées sur le préfixe d'envoi individuel.

C'est-à-dire que pour identifier si c'est une adresse de diffusion groupée comme spécifié dans le présent mémoire et pour qu'elle subisse la suite du traitement, une adresse doit satisfaire à toutes les conditions suivantes :
- o Elle DOIT être une adresse de diffusion groupée avec "fans" réglé à 0111, c'est-à-dire, être du préfixe FF70::/12,
- o "plen" NE DOIT PAS être 0 (c'est-à-dire, pas SSM), et
- o "plen" NE DOIT PAS être supérieur à 64.

L'adresse du RP peut être obtenue d'une adresse de diffusion groupée satisfaisant aux critères ci-dessus selon les deux étapes suivantes :
1. copier le premier bit "plen" du "préfixe réseau" dans une structure d'adresse de 128 bits zéroïsée, et
2. remplacer les 4 derniers bits par le contenu de "RIID".

Ces deux étapes pourraient être illustrées comme suit :



On notera qu'il y a plusieurs scénarios de fonctionnement (voir l'exemple 3 ci-dessous) lorsque on ignore la déclaration de la [RFC3306] "tous les bits non significatifs du champ préfixe de réseau DEVRAIENT être à zéro". Ceci pour permettre que les allocations d'adresse de groupe de diffusion groupée soient cohérentes avec les préfixes d'envoi individuel ; les adresses de diffusion groupée vont quand même utiliser le RP associé au préfixe réseau.

"plen" supérieur à 64 NE DOIT PAS être utilisé, car cela se chevaucherait avec les bits de poids fort de l'identifiant de groupe de diffusion groupée.

Lorsque ils traitent un codage pour obtenir l'adresse du RP, les routeurs de diffusion groupée DOIVENT effectuer au moins les mêmes vérifications de validité d'adresse sur l'adresse de RP calculée que sur une adresse reçue par d'autres moyens (comme BSR [RFC5059] ou MSDP pour IPv4). Au moins fe80::/10, ::/16, et ff00::/8 DOIVENT être exclues. Ceci est particulièrement important, car les informations sont obtenues d'une source qui n'est pas de confiance, c'est-à-dire, n'importe quelle entrée d'utilisateur de l'Internet.

On notera que les quatre bits réservés pour "RIID" établissent la limite supérieure des RP pour la combinaison de la portée, du préfixe réseau, et de l'identifiant de groupe – sans en changer aucun, on peut avoir 2^4-1 = 15 RP différents (car RIID=0 est réservé, voir au paragraphe 6.3). Cependant, chacun d'eux est une adresse de groupe IPv6 de plein droit (c'est-à-dire, il peut seulement y avoir un RP par adresse de diffusion groupée).

5. Exemples

Quatre exemples d'allocation d'adresse de diffusion groupée et des transpositions résultantes de groupe en RP sont décrits ici pour mieux illustrer les possibilités fournies par le codage.

5.1 Exemple 1

L'administrateur réseau de 2001:DB8::/32 veut établir un RP pour le réseau et tous les clients, en le plaçant sur un sous réseau existant, par exemple, 2001:DB8:BEEF:FEED::/64.

Dans ce cas, les adresses de groupe vont être quelque chose comme "FF7x:y40:2001:DB8:BEEF:FEED::/96", et leur adresse de RP serait "2001:DB8:BEEF:FEED::y". Il y a encore 32 bits d'identifiants de groupe de diffusion groupée à allouer aux clients et à soi-même ("y" pourrait être n'importe quoi de 1 à F, car 0 ne doit pas être utilisé).

5.2 Exemple 2

Comme dans l'exemple 1, l'administrateur réseau de 2001:DB8::/32 veut établir le RP mais, pour le rendre plus souple, il veut le placer sur un sous réseau à acheminement spécifique et veut garder un plus large espace d'adresses pour les allocations de groupe. C'est-à-dire que l'administrateur choisit la partie la moins spécifique du préfixe d'envoi individuel, avec plen=32, et les adresses de groupe seront tirées du préfixe de diffusion groupée :

FF7x:y20:2001:DB8::/64

où "x" est la portée de diffusion groupée, "y" est l'identifiant d'interface de l'adresse du RP, et il y a 64 bits pour les identifiants de groupe ou les allocations. Dans ce cas, l'adresse du RP serait :

2001:DB8::y

L'adresse 2001:DB8::y/128 est allouée à un routeur comme adresse de mise en boucle et est injectée dans le système d'acheminement ; si l'administrateur du réseau établit seulement un ou deux RP (et, par exemple, pas un RP par sous réseau) cette approche peut être préférable à celle décrite dans l'exemple 1.

5.3 Exemple 3

Comme dans l'exemple 2, l'administrateur du réseau peut aussi allouer des préfixes de diffusion groupée tels que "FF7x:y20:2001:DB8:DEAD::/80" à certains clients. Dans ce cas, l'adresse du RP serait toujours "2001:DB8::y". (Noter que c'est juste un sous cas plus spécifique de l'exemple 2, où l'administrateur alloue un préfixe de diffusion groupée, pas seulement des identifiants de groupe individuels.)

Noter que la seconde règle de déduction de l'adresse de RP, le champ "plen" dans l'adresse de diffusion groupée, 0x20 = 32, se réfère à la longueur du champ "préfixe réseau" considéré lors de l'obtention de l'adresse du RP. Dans ce cas, seuls les 32 premiers bits du champ Préfixe de réseau, "2001:DB8", sont préservés : la valeur de "plen" ne prend pas position sur les longueurs réelles de préfixe d'envoi individuel/diffusion groupée alloués ou utilisés dans les réseaux, ici, de 2001:DB8:DEAD::/48.

En bref, cette distinction permet une configuration plus souple de l'adresse de RP dans les scénarios où il est souhaitable que les adresses de groupe soient cohérentes avec les allocations de préfixe d'envoi individuel.

5.4 Exemple 4

Dans le réseau des exemples 1, 2, et 3, l'administrateur du réseau établit les adresses à utiliser par les clients, mais une organisation veut avoir son propre domaine PIM-SM. L'organisation peut prendre des adresses de diffusion groupée comme "FF7x:y30:2001:DB8:BEEF::/80", et alors l'adresse de RP serait "2001:DB8:BEEF::y".

6. Considérations de fonctionnement

Cette section décrit les considérations de fonctionnement majeures pour le déploiement de ce mécanisme.

6.1 Redondance de RP

Une technique appelée "RP à la cantonade" est utilisée au sein d'un domaine PIM-SM pour partager une adresse et des informations d'état de diffusion groupée entre un ensemble de RP principalement pour des raisons de redondance. Normalement, MSDP a été utilisé pour cela ainsi que la [RFC3446]. Il y a aussi d'autres approches, comme celle d'utiliser PIM pour partager ces informations [RFC4610].
Le candidat le plus crédible pour une reprise sur défaillance de RP est d'utiliser PIM pour RP à la cantonade ou "l'envoi à la cantonade" (c'est-à-dire, le modèle d'envoi individuel partagé [ANYCAST]) de l'adresse de RP dans le protocole de passerelle intérieure (IGP, *Interior Gateway Protocol*) sans partage d'état (bien que cela dépende des exigences de redondance, cela peut suffire ou non). Cependant, les mécanismes de redondance sortent du domaine d'application du présent mémoire.

6.2 Déploiement de RP

Comme il n'est pas besoin de partager l'état inter domaines avec MSDP, chaque routeur désigné qui connecte des sources de diffusion groupée pourrait agir comme RP sans souci d'adaptabilité concernant l'établissement et le maintien de sessions MSDP.

Cela pourrait être particulièrement intéressant lorsque on se préoccupe de la redondance de RP. Dans le cas où le DR proche d'une source majeure pour un groupe agit comme RP, une certaine quantité de propriétés de partage équitable peut être obtenue sans utiliser de mécanisme de reprise sur défaillance de RP : si le DR tombe en panne, la transmission en diffusion groupée ne peut plus fonctionner de toutes façons.

Allant dans le même sens, il peut aussi être souhaitable de répartir les responsabilités de RP entre plusieurs RP. Tant que des RP différents servent des groupes différents, ceci est trivial : chaque groupe peut se transposer en un RP différent (ou de nombreux RP suffisamment différents pour que la charge sur un RP ne pose pas de problème). Cependant, les défis de partage de charge auxquels un groupe doit faire face sont similaires à ceux du RP à la cantonade.

6.3 Lignes directrices pour allouer des adresses IPv6 aux RP

Avec ce mécanisme, le RP peut recevoir tout préfixe de réseau d'envoi individuel jusqu'à /64. L'identifiant d'interface devra être configuré manuellement pour correspondre au "RIID".

RIID = 0 ne doit pas être utilisé, car cela causerait une ambiguïté avec l'adresse de routeur de sous réseau d'envoi à la cantonade [RFC3513].

Si un administrateur souhaite utiliser une adresse de RP qui ne se conforme pas à la topologie d'adressage mais est quand même dans le préfixe d'envoi individuel du fournisseur de réseau (par exemple, une adresse de rebouclage supplémentaire allouée à un routeur, comme décrit dans l'exemple 2 du paragraphe 5.1) cette adresse peut être injectée dans le système d'acheminement via un chemin d'hôte.

6.4 Utilisation comme substitut de BSR

Avec le RP incorporé, l'utilisation de BSR ou autre mécanisme de configuration de RP à travers le domaine PIM n'est pas nécessaire, car chaque adresse de groupe spécifie le RP à utiliser.

6.5 Contrôle de l'utilisation des RP

Comparé au modèle ASM inter domaines de MSDP, le contrôle et la gestion de qui peut utiliser un RP, et comment, change légèrement et mérite une discussion explicite.

Le filtrage d'annonces MSDP comporte normalement au moins deux capacités : le filtrage de qui est capable de créer une session globale ("filtrage de source") et le filtrage des groupes qui devraient être globalement accessibles ("filtrage de groupe"). Il sont faits pour empêcher que des groupes locaux soient annoncés à l'extérieur ou que des envoyeurs non autorisés créent des groupes globaux.

Cependant, un tel contrôle n'empêche pas les extérieurs d'utiliser de tels groupes, car ils peuvent se joindre aux groupes même sans annonce "Source active" avec un Join (Source, Groupe) ou (S,G) en devinant/apprenant l'adresse de la source et/ou du groupe. Pour une protection appropriée, on devrait établir, par exemple, les limites de portée de diffusion groupée PIM aux routeurs de bordure. Donc, le RP incorporé a par défaut un niveau de "protection" équivalent à celui de MSDP avec filtrage de SA.

Un nouveau problème avec le contrôle est que les nœuds dans un "domaine étranger" peuvent s'enregistrer à un RP, ou envoyer un Join PIM à un RP. (Ceci était déjà possible aussi dans le passé, dans une certaine mesure, mais seulement par des tentatives volontaires ou une configuration de RP délibérée aux DR.) La principale menace dans ce cas est qu'un extérieur puisse illégalement utiliser le RP pour héberger son ou ses propres groupes. Ceci peut être atténué dans uns certaine mesure en filtrant les groupes ou gammes de groupes qui sont permis au RP ; les contrôles plus spécifiques sortent du domaine d'application du présent mémoire. Noter que ceci ne semble pas à première vue être une menace sérieuse car quiconque a un préfixe d'envoi individuel de /64 peut créer son propre RP sans avoir à l'obtenir illégitimement de quelqu'un d'autre.

7. Mécanisme de transposition de groupe en RP pour le RP incorporé

Cette Section spécifie le mécanisme de transposition de groupe en RP pour le RP incorporé.

7.1 Transposition dans PIM en mode épars de groupe en RP

La seule modification exigée pour PIM-SM est de mettre en œuvre ce mécanisme comme méthode de transposition de groupe en RP.

La mise en œuvre devra reconnaître le format d'adresse et déduire et utiliser l'adresse de RP en utilisant les règles de la Section 4. Ces informations sont utilisées au moins en effectuant les recherches de transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) lors du traitement des messages Join/Prune, ou en effectuant l'enregistrement d'encapsulation.

Pour éviter des boucles et des incohérences, pour les adresses dans la gamme FF70::/12, la transposition de RP incorporé DOIT être considérée comme la plus longue correspondance possible et la plus forte priorité que tout autre mécanisme.

On notera que comparée aux autres mécanismes de transposition de groupe à RP, qui peuvent être précalculés, la transposition de RP incorporé doit être refaite pour toute nouvelle adresse de groupe IPv6 qui se transposerait dans un RP différent. Pour être efficace, le résultat peut être mis en antémémoire d'une manière spécifique de la mise en œuvre, pour éviter des calculs à chaque paquet de RP incorporé.

Ce mécanisme de transposition de groupe en RP doit être pris en charge par le RP, le DR adjacent aux envoyeurs, et tout routeur sur le chemin entre tout receveur et le RP. Les chemins pour la formation d'arborescence de plus court chemin (SPT, *Shortest Path Tree*) et pour "Register-Stop" n'exigent pas cette prise en charge, car cela est réalisé avec un "Join (S,G)".

7.2 Vue d'ensemble du modèle

Ce paragraphe donne une vue d'ensemble générale non normative de la façon dont fonctionne le RP incorporé, comme spécifié au paragraphe précédent.

Un receveur qui souhaite se joindre à un groupe va parcourir les étapes suivantes :

1. Le receveur va choisir un moyen de trouver l'adresse du groupe (par exemple, SDR ou une page de la Toile).

2. Le receveur produit un rapport de découverte d'écoutant de diffusion groupée (MLD, *Multicast Listener Discovery*) pour se joindre au groupe.

3. Le DR du receveur va initier le processus Join PIM-SM à l'égard du RP codé dans l'adresse de diffusion groupée, sans considérer si il est dans le domaine PIM "local" ou "distant".

Les étapes lorsque un envoyeur souhaite envoyer à un groupe sont les suivantes :

1. Un envoyeur trouve une adresse de groupe en utilisant une méthode non spécifiée (par exemple, en contactant l'administrateur pour une allocation de groupe ou en utilisant un protocole d'allocation d'adresse de diffusion groupée).

2. L'envoyeur envoie au groupe.

3. Le DR de l'envoyeur va envoyer les paquets encapsulés en envoi individuel dans les messages Register de PIM-SM à l'adresse de RP codée dans l'adresse de diffusion groupée (dans le cas particulier où le DR est le RP, un tel envoi est seulement conceptuel).

En fait, tous les messages sont comme spécifié dans la [RFC4601] ; le RP incorporé agit juste comme un mécanisme de

transposition de groupe en RP. Au lieu d'obtenir l'adresse du RP de la configuration locale ou des protocoles de configuration (par exemple, BSR) l'algorithme le déduit de façon transparente de l'adresse de diffusion groupée codée.

8. Analyse de l'adaptabilité

Le modèle MSDP inter domaines pour connecter les domaines PIM-SM est essentiellement hiérarchique dans sa configuration et son déploiement, mais plat à l'égard de la distribution des informations. Le modèle inter domaines de RP incorporé se comporte comme si chaque groupe formait son propre domaine PIM sur tout l'Internet, avec la transposition du groupe en un seul RP, quelle que soit la localisation des receveurs ou des envoyeurs. Donc, la diffusion groupée inter domaines devient une topologie plate, centrée sur le RP. Les problèmes d'adaptabilité sont décrits ci-dessous.

Précédemment, les sources étrangères envoyaient les données encapsulées en envoi individuel à leur RP "local" ; maintenant elles sont envoyées au RP "étranger" responsable du groupe spécifique. Ceci est particulièrement important avec les grands groupes de diffusion groupée où il y a beaucoup de gros envoyeurs – en particulier si les mises en œuvre ne traitent pas bien la désencapsulation d'envoi individuel.

Avec la diffusion groupée ASM IPv4, il y a en gros deux sortes d'états au niveau de l'Internet : l'état d'acheminement MSDP (propagé partout) et l'état d'acheminement de diffusion groupée (sur les branches receveur ou envoyeur). Le premier est éliminé, mais les routeurs du cœur de réseau peuvent finir avec l'état (*, G) et (S, G, rpt) entre les receveurs (et les receveurs passés, pour les élagages de PIM) et le RP, en plus des états (S, G) entre les receveurs et les envoyeurs, si SPT est utilisé. Cependant, la quantité totale d'état est plus petite.

Dans les deux cas inter domaines et intra domaine, le modèle du RP incorporé est pratiquement identique au PIM-SM traditionnel dans l'intra domaine. D'un autre côté, PIM-SM a été déployé (dans IPv4) dans l'inter domaines en utilisant MSDP ; comparé à ce modèle inter domaines, la présente spécification simplifie la construction de l'arborescence (c'est-à-dire, l'acheminement de diffusion groupée) en retirant le RP pour les envoyeurs et les receveurs dans les domaines étrangers et en éliminant la distribution des informations de MSDP.

Comme l'adresse du RP est liée à l'adresse de diffusion groupée, la gestion de l'échec de RP devient plus difficile, car les mécanismes de reprise sur échec ou de redondance déployés (par exemple, BSR, RP en envoi à la cantonade avec MSDP) ne peuvent pas être utilisés tels quels. Cependant, le RP en envoi à la cantonade en utilisant PIM assure une redondance égale ; ceci est brièvement décrit au paragraphe 6.1.

La spécification PIM-SM déclare : "Toute adresse de RP configurée ou apprise DOIT être une adresse accessible dans tout le domaine". Ce que signifie précisément "accessible" n'est pas clair, même sans RP incorporé. Cette déclaration ne peut pas être prouvée, en particulier avec les RP étrangers, car on ne peut même pas garantir que le RP existe. Au lieu de configurer manuellement les RP et les DR (configurer un RP non existant était possible, mais rare) avec la présente spécification les hôtes et usagers utilisant la diffusion groupée spécifient indirectement eux-mêmes le RP, diminuant l'attente de l'accessibilité du RP. C'est un problème relativement significatif mais pas très différent de celui du déploiement actuel de la diffusion groupée : par exemple, les "join (S,G)" MLDv2, en ASM ou SSM, donnent le même résultat [RFC4609].

Être capable de joindre/envoyer aux RP distants soulève des problèmes de sécurité qui sont considérés séparément, mais cela a aussi un avantage : chaque groupe a un "RP responsable" qui est capable de contrôler (dans une certaine mesure) qui est capable d'envoyer au groupe.

Une description plus détaillée et une comparaison des modèles d'acheminement de diffusion groupée inter domaines (ASM traditionnel avec MSDP, RP incorporé, SSM) et leurs propriétés de sécurité a été donnée dans la [RFC4609].

9. Remerciements

Jerome Durand a fait des commentaires sur une version antérieure du présent mémoire. Marshall Eubanks a noté un problème concernant les valeurs courtes de "plen". Tom Pusateri a noté des problèmes avec une approche antérieure de "SPT-join". Rami Lehtonen a souligné des problèmes sur la portée de l'état de SA et a fourni des commentaires détaillés. Nidhi Bhaskar a fait une relecture complète du document. Toerless Eckert, Hugh Holbrook, et Dave Meyer ont fourni des retours abondants. En particulier, Pavlin Radoslavov, Dino Farinacci, Nidhi Bhaskar, et Jerome Durand ont fourni de bons commentaires durant et après le dernier appel du groupe de travail. Mark Allman, Bill Fenner, Thomas Narten, et Alex Zinin ont fourni des commentaires substantiels durant l'évaluation de l'IESG. Le groupe de travail MboneD a droit aussi à notre reconnaissance pour son soutien continu et ses commentaires.

10. Considérations sur la sécurité

Les adresses des RP sont codées dans les adresses de diffusion groupée, devenant donc plus visibles comme seuls points de défaillance. Même si cela n'affecte pas de façon significative la sécurité de l'acheminement de diffusion groupée, cela peut exposer le RP à d'autres sortes d'attaques. Les opérateurs sont invités à porter une attention particulière à la sécurité de ces routeurs. Voir au paragraphe 6.1 les considérations sur la reprise sur défaillance et au paragraphe 6.2 le placement des RP conduisant à un niveau de propriétés de partage des risques.

Comme tout RP aura à accepter les messages PIM-SM Join/Prune/Register provenant de tout DR, cela peut causer un scénario potentiel d'attaque de déni de service. Cependant, cela peut être atténué car le RP peut éliminer de tels messages pour toutes les adresses de diffusion groupée qui ne codent pas l'adresse du RP. Les attaques fondées aussi bien sur l'envoyeur que sur le receveur sont décrites plus en détails dans la [RFC4609].

De plus, les mises en œuvre DEVRAIENT aussi permettre la configuration manuelle des préfixes de diffusion groupée dont l'utilisation est autorisée. Ceci peut être utilisé pour limiter seulement d'usage du RP pur les groupes désignés. Dans certains cas, être capable de restreindre (au RP) quelles adresses d'envoi individuel ont la permission d'envoyer ou se joindre à un groupe est souhaitable. (Cependant, noter que les messages Join/Prune vont quand même laisser un état dans le réseau, et les messages Register peuvent être falsifiés [RFC4609].) Évidemment, ces contrôles ne sont possibles qu'au RP, et pas aux routeurs intermédiaires ou au DR.

Il est RECOMMANDÉ que les routeurs qui prennent en charge la présente spécification n'agissent pas comme des RP sauf si ils sont explicitement configurés à le faire, car devenir un RP n'exige aucune annonce (par exemple, par BSR ou manuellement). Autrement, tout routeur pourrait devenir un RP (et être détourné à ce titre). De plus, les groupes de diffusion groupée ou les gammes de groupes à desservir PEUVENT avoir besoin d'être explicitement configurés aux RP, pour les protéger contre une utilisation contre leur gré. Noter que les contrôles les plus spécifiques (par exemple, les modèles "l'interne doit créer" ou "l'externe invite") sur qui a la permission d'utiliser les groupes sortent du domaine d'application du présent mémoire.

Exclure les groupes seulement internes des annonces MSDP ne protège pas les groupes contre les extérieurs mais offre seulement la sécurité par l'obscurité ; le RP incorporé offre un niveau de protection similaire. Lorsque on désire une protection réelle, par exemple PIM à portée limitée, devrait être établi aux frontières. Ceci est décrit plus en détails au paragraphe 6.5.

On devrait observer que modèle de menace du RP incorporé est en fait assez similaire au SSM ; les deux mécanismes réduisent significativement les menaces du côté de l'envoyeur. Du côté du receveur, les menaces sont assez comparables, car un attaquant pourrait faire un "join (S,G)" MLDv2 à l'égard d'une source non existante, que le RP local ne pourrait pas bloquer sur la base des informations MSDP.

La mise en œuvre DOIT effectuer au moins les mêmes vérifications de validité d'adresse sur l'adresse de RP incorporé que celles qui seraient faites sur une reçue par d'autres moyens ; au moins fe80::/10, ::/16, et ff00::/8 devraient être exclus. Ceci est particulièrement important, car les informations sont déduites de la source qui n'est pas de confiance (c'est-à-dire, n'importe quel utilisateur de l'Internet et non pas de la configuration locale.

Une description et une comparaison plus détaillée des modèles de diffusion groupée inter domaine (l'ASM traditionnel avec MSDP, le RP incorporé, SSM) et leurs propriétés de sécurité a été faite séparément dans la [RFC4609].

11. Références

11.1 Références normatives

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

[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.)*

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

11.2 Références pour information

[ANYCAST] Hagino, J. and K. Ettikan, "An analysis of IPv6 anycast", Travail en cours, juin 2003.

[RFC3446] D. Kim et autres, "Mécanisme de point de rendez-vous (RP) en envoi à la cantonade utilisant la diffusion groupée indépendante du protocole (PIM) et le protocole de découverte de source de diffusion groupée (MSDP)", janvier 2003. *(Information)*

[RFC3618] B. Fenner et D. Meyer, éd., "Protocole de découverte de source de diffusion groupée (MSDP)", octobre 2003. *(Expérimentale)*

[RFC4601] B. Fenner et autres, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : spécification du protocole (Révisée)", août 2006. (*Remplacée par* RFC7761*, STD 83)*

[RFC4607] H. Holbrook, B. Cain, "Diffusion groupée spécifique de source pour IP", août 2006. *(P.S.)*

[RFC4609] P. Savola et autres, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : questions de sécurité de l'acheminement de la diffusion groupée et améliorations", octobre 2006. *(Information)*

[RFC4610] D. Farinacci, Y. Cai, "Point de rendez-vous d'envoi à la cantonade utilisant la diffusion groupée indépendante du protocole (PIM)", août 2006. *(P.S.)*

[RFC5059] N. Bhaskar et autres, "Mécanisme de routeur d'amorçage (BSR) pour la diffusion groupée indépendante du protocole (PIM)", janvier 2008. (*Remplace* RFC2362) (*MàJ* RFC4601) *(P.S.)*

[V6MISSUES] Savola, P., "IPv6 Multicast Deployment Issues", Travail en cours, septembre 2004.

A. Discussion sur les compromis de conception

Le document ne spécifie pour l'instant que FF70::/12 ; si/quand le bit de poids fort est utilisé, on doit spécifier comment FFF0::/12 s'applique au RP incorporé. Par exemple, un mode différent de PIM ou un autre protocole pourrait utiliser cette gamme, par opposition à FF70::/12, comme actuellement spécifié, comme étant seulement pour PIM-SM.
Au lieu d'utiliser les bits fanions ("FF70::/12") on aurait pu utiliser les bits réservés de gauche ("FF3x:8000::/17").
On a objecté que au lieu de permettre à l'opérateur de spécifier RIID, la valeur aurait pu être prédéterminée (par exemple, "1"). Cependant, cela n'a pas été adopté, car cela élimine la souplesse d'allocation d'adresse chez l'opérateur.

Les valeurs 64 < "plen" < 96 se chevaucheraient avec les bits de poids forts de l'identifiant de groupe de diffusion groupée ; à cause de cette restriction, "plen" ne doit pas excéder 64 bits. Ceci est conforme à la RFC 3306.

L'adressage de RP incorporé pourrait être utilisé pour porter aussi d'autres informations (autres que l'adresse de RP) par exemple, ce que devrait être le seuil RPT pour PIM-SM. Cela pourrait, faisable ou non, être codé dans l'adresse de RP, ou dans l'adresse de groupe de diffusion groupée. Dans tous les cas, ces modifications sortent du domaine d'application du présent mémoire.

Pour les cas où les RP n'existent pas ou sont inaccessibles, ou si trop d'état serait généré pour l'atteindre dans une attaque de déni de service par épuisement de ressources, certaines formes de limitation de taux ou autres mécanismes pourraient être déployés pour atténuer ces menaces tout en essayant de ne pas perturber l'usage légitime. Cependant, comme les menaces sont génériques, elles sont considérées comme sortant du domaine d'application de ce document et sont discutées séparément dans la [RFC4609].

Adresse des auteurs

Pekka Savola
CSC/FUNET
Espoo,
Finland
mél : psavola@funet.fi

Brian Haberman
Johns Hopkins University Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723-6099
USA
téléphone : +1 443 778 1319
mél : brian@innovationslab.net

Déclaration complète de droits de reproduction

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