Groupe de travail Réseau
Request for Comments : 5110
Catégorie : Information

P. Savola, CSC/FUNET
janvier 2008
Traduction Claude Brière de L'Isle

Vue générale de l'architecture d'acheminement de diffusion groupée de l'Internet

Statut de ce mémoire

Le présent mémoire donne des informations pour la communauté de l'Internet. Il ne spécifié aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document décrit les architectures d'acheminement de la diffusion groupée qui sont actuellement en usage sur l'Internet. Le présent document décrit brièvement ces protocoles et fait référence à leurs spécifications.

Le présent mémoire classe aussi dans la catégorie "Historique" plusieurs RFC anciennes. Ces RFC décrivent des protocoles d'acheminement en diffusion groupée qui n'ont jamais été largement déployés ou sont tombés en désuétude.

Table des matières

1. Introduction

Le présent document donne un bref aperçu des architectures d'acheminement de diffusion groupée qui sont actuellement déployées sur l'Internet et de la façon dont ces protocoles s'accordent ensemble. Il décrit aussi les protocoles d'acheminement de diffusion groupée qui n'ont jamais été largement déployés ou sont tombés en désuétude. Un document voisin [ADDRARCH] décrit les architectures d'adressage de diffusion groupée.

Précisément, le présent mémoire traite de :
- o l'établissement de l'état de transmission en diffusion groupée (paragraphe 2.1),
- o la distribution des informations de topologie de diffusion groupée (paragraphe 2.2),
- o l'acquisition des sources actives (paragraphe 2.3),
- o la configuration et la distribution des informations de point de rendez-vous (RP) (paragraphe 2.4),
- o mécanismes de redondance améliorée (paragraphe 2.5),
- o l'interaction avec les hôtes (paragraphe 2.6),
- o restriction du flux de diffusion groupées à la couche de liaison (paragraphe 2.7).

La section 2 commence par décrire un exemple simpliste de la façon dont ces classes de mécanismes s'accordent ensemble. Certaines questions du transport des données de diffusion groupée sont aussi abordées à l'Appendice A.

Le présent mémoire reclasse en "Historique" [RFC2026] les RFC suivantes :
- o Protocole de diffusion groupée des routeurs frontière (BGMP, *Border Gateway Multicast Protocol*) [RFC3913],
- o Arborescences fondées sur le noyau (CBT, *Core Based Trees*) [RFC2189] [RFC2201],
- o Diffusion groupée en OSPF (MOSPF, *Multicast OSPF*) [RFC1584].

Pour la plus grande part, ces protocoles sont tombés en désuétude. Il peut exister des mises en œuvre de certains de ces protocoles, elles ne sont pas affectés par cette reclassification. Il en est dit plus sur chacun de ces protocoles au paragraphe 2.1.

On trouvera d'autres éléments d'historique par exemple, dans les [RFC1458], [IMRP-ISSUES], et [IM-GAPS].

1.1 Abréviations en rapport avec la diffusion groupée

ASM *(Any Source Multicast)* : diffusion groupée toutes sources
BGMP *(Border Gateway Multicast Protocol)* : protocole de diffusion groupée de routeur frontière
BSR *(Bootstrap Router)* : routeur d'amorçage
CBT *(Core Based Trees)* : arborescences fondées sur le noyau
CGMP *(Cisco Group Management Protocol)* : protocole Cisco de gestion de groupe
DR *(Designated Router)* : routeur désigné
DVMRP *(Distance Vector Multicast Routing Protocol)* : protocole d'acheminement de diffusion groupée par vecteur de distance
GARP (IEEE 802.1D-2004) *(Generic Attribute Registration Protocol)* : protocole générique d'enregistrement d'attribut
GMRP *(GARP Multicast Registration Protocol)* : protocole d'enregistrement de diffusion groupée de GARP
IGMP *(Internet Group Management Protocol)* : protocole de gestion de groupe Internet
MBGP *(Multiprotocol BGP)* (*pas* "Multicast BGP") : BGP multiprotocoles
MLD *(Multicast Listener Discovery)* : découverte des appareils en veille sur la diffusion groupée
MRP (IEEE 802.1ak) *(Multiple Registration Protocol)* : protocole d'enregistrement multiple
MMRP (IEEE 802.1ak) *(Multicast Multiple Registration Protocol)* : protocole d'enregistrement multiple en diffusion groupée
MOSPF *(Multicast OSPF)* : diffusion groupée en OSPF

MSDP *(Multicast Source Discovery Protocol)* : Protocole de découverte de source de diffusion groupée
PGM *(Pragmatic General Multicast)* : diffusion groupée générale pragmatique
PIM *(Protocol Independent Multicast)* : diffusion groupée indépendante du protocole
PIM-DM *(PIM - Dense Mode)* : diffusion groupée indépendante du protocole en mode dense
PIM-SM *(PIM - Sparse Mode)* : diffusion groupée indépendante du protocole en mode dispersé
PIM-SSM *(PIM - Source-Specific Multicast)* : diffusion groupée indépendante du protocole spécifique de la source
RGMP*(Router Group Management Protocol)* : protocole (de Cisco) de gestion de groupe de routeurs
RP *(Rendezvous Point)* : point de rendez-vous
RPF *(Reverse Path Forwarding)* : transmission sur le chemin inverse
SAFI *(Subsequent Address Family Identifier)* : identifiant de la famille d'adresses suivante
SDP *(Session Description Protocol)* : protocole de description de session
SSM *(Source-Specific Multicast)* : diffusion groupée spécifique d'une source

2. Acheminement de la diffusion groupée

Dans le but d'établir un sommaire simplifié de la façon dont chacune de ces classes de mécanismes s'accordent ensemble, considérons le scénario suivant de réception de diffusion groupée.

Certains protocoles et configurations doivent être en place avant que l'acheminement de la diffusion groupée puisse fonctionner. Précisément, lorsque l'ASM est employé, un routeur aura besoin de savoir son ou ses adresses de RP (paragraphes 2.4, 2.5). Avec IPv4, les RP doivent être connectés aux autres RP en utilisant MSDP de sorte que les informations sur les sources connectées aux autres RP puissent être distribuées (paragraphe 2.3). De plus, les routeurs ont besoin de savoir si, et comment, la topologie de diffusion groupée diffère de la topologie d'envoi individuel, et les extensions de protocole d'acheminement peuvent fournir cette information (paragraphe 2.2).

Lorsqu'un hôte veut recevoir une transmission, il a d'abord besoin de trouver l'adresse de groupe de diffusion groupée (et avec SSM, l'adresse de source) en utilisant des moyens variés (par exemple, le fichier de description SDP [RFC4566] ou à la main). Ensuite il va signaler son intérêt à son routeur de premier bond en utilisant IGMP (IPv4) ou MLD (IPv6) (paragraphe 2.6). Le routeur initie l'état de transmission de diffusion groupée bond par bond (paragraphe 2.1) vers la source (e SSM) ou le premier à travers le RP (en ASM). Les routeurs utilisent un RP pour découvrir toutes les sources pour un groupe (paragraphe 2.3). Lorsqu'une transmission en diffusion groupée arrive au LAN du receveur, elle est arrosée sur chaque accès de commutation Ethernet sauf si une réduction de l'arrosage telle que la surveillance de trafic IGMP est employée (paragraphe 2.7).

2.1 Établissement de l'état de transmission de diffusion groupée

La partie la plus importante de l'acheminement de diffusion groupée est d'établir l'état de transmission de diffusion groupée. La maintenance d'état exige un échange de messages périodique parce que l'état de transmission a une temporisation. Ce paragraphe décrit les protocoles couramment utilisés à cette fin.

2.1.1 PIM-SM

Le protocole d'acheminement de diffusion groupée le plus couramment utilisé est PIM-SM [RFC4601]. Le protocole PIM-SM inclut les deux fonctionnalités d'envoi à la cantonade (ASM, *Any Source Multicast*) et de diffusion groupée spécifique d'une source (SSM, *Source-Specific Multicast*). PIM-SSM est un sous-ensemble de PIM-SM qui n'utilise pas les RP mais exige à la place que les receveurs connaissent la paire (source, groupe) et le signalent explicitement. La plupart des plates-formes d'acheminement actuelles prennent en charge PIM-SM.

Les routeurs PIM choisissent un routeur désigné (DR) sur chaque LAN et le DR est responsable de l'échange de messages et l'enregistrement de source PIM au nom des hôtes. Le DR encapsule plusieurs paquets de diffusion groupée originaires du LAN dans un tunnel en envoi individuel au RP. PIM-SM construit un arbre de distribution unidirectionnel, spécifique du groupe comportant les receveurs intéressés d'un groupe. Au départ, l'arbre de distribution de diffusion groupée a sa racine au RP mais ensuite, les DR ont la faculté d'optimiser la livraison en construisant des arbres spécifiques de la paire (source, groupe).

On trouvera une introduction plus développée à PIM-SM à la Section 3 de la [RFC4601].

2.1.2 PIM-DM

Alors que PIM-SM a été conçu pour éviter un arrosage inutile des sonnées de diffusion groupée, PIM-DM [RFC3973] suppose que presque chaque sous–réseau d'un site a au moins un receveur pour un groupe. PIM-DM arrose les transmissions de diffusion groupée sur tout le réseau ("arroser et élaguer") sauf si les parties terminales du réseau indiquent périodiquement qu'elles ne sont pas intéressées à ce groupe particulier.

PIM-DM peut être un compromis acceptable dans de petits et/ou simples réseaux, où l'établissement d'un RP serait inutile, et éventuellement dans des cas où un fort pourcentage d'usagers sont supposés vouloir recevoir la transmission de sorte que la quantité d'états que le réseau doit conserver est minimale.

PIM-DM était utilisé comme première étape dans la transition à partir de DVMRP. Il est aussi devenu évident que la plupart des réseaux n'auraient pas de receveurs pour la plupart des groupes, et pour éviter le gaspillage de bande passante et d'états, le paradigme de l'arrosage a été progressivement abandonné. La transition de PIM-DM à PIM-SM était facile car PIM-SM a été conçu pour utiliser des formats de paquet compatibles et le fonctionnement en mode dense pouvait aussi être satisfait par un protocole épars. PIM-DM n'est plus très largement utilisé.

De nombreuses mises en œuvre prennent aussi en charge une configuration dite "éparse-dense", où le mode épars est utilisé par défaut, mais le mode dense est seulement utilisé pour les gammes de groupe de diffusion groupée configurés (tels que Auto-RP au paragraphe 2.4.3). Plus tard, de nombreux réseaux ont quitté le mode épars-dense pour le seul mode épars.

2.1.3 PIM bidirectionnel

Le PIM bidirectionnel [RFC5015] est un protocole de transmission de diffusion groupée qui établit un chemin partagé commun pour toutes les sources avec une seule racine. Il peut être utilisé comme solution de remplacement à PIM-SM à l'intérieur d'un seul domaine. Il n'a pas d'événement actionnés par les données ou d'encapsulation des données. Comme il ne conserve pas d'état spécifique de la source, il peut être une approche attractive en particulier dans les sites avec un grand nombre de sources.

Au moment de cette publication, il n'y a pas de solution inter domaine pour configurer une gamme de groupe à utiliser le PIM bidirectionnel.

2.1.4 DVMRP

Le protocole d'acheminement de diffusion groupée par vecteur de distance (DVMRP, *Distance Vector Multicast Routing Protocol*) [RFC1075] [DVMRPv3] [DVMRPv3-AS] était le premier protocole conçu pour la diffusion groupée. Pour surmonter les obstacles du développement initial, il incluait aussi des capacités de tunnelage, qui faisaient partie de ses fonctions de topologie de diffusion groupée.

Actuellement, DVMRP n'est utilisé que très rarement dans les réseaux d'opérateur, et il a été remplacé par PIM-SM. L'utilisation la plus typique de lDVMRP est dans un réseau d'extrémité, pour aller d'un pare-feu traditionnel ne prenant en charge que DVMRP au réseau interne. Cependant, le tunnelage d'encapsulage générique d'acheminement (GRE, *Generic Routing Encapsulation*) [RFC2784] semble avoir pris le dessus sur DVMRP dans cette fonctionnalité, et il reste relativement peu d'avenir pour DVMRP en dehors des utilisations résiduelles.

2.1.5 MOSPF

MOSPF [RFC1584] a été mis en œuvre par plusieurs fabricants et a connu un certain développement dans les réseaux intra domaine. Cependant, comme il se fonde sur le chemin le plus court ouvert en premier (OSPF, *Open Shortest Path First*) intra domaine, il n'est pas à l'échelle pour le cas inter domaine, et les opérateurs ont trouvé plus facile de développer un seul protocole à utiliser à la fois dans l'intra domaine et l'inter domaine aussi n'est-il plus activement déployé.

2.1.6 BGMP

BGMP [RFC3913] n'a pas reçu suffisamment de soutien au sein de la communauté des fournisseurs de service pour être adopté et poussé en avant dans le processus de normalisation de l'IETF. Aucune mise en œuvre ou développement sur le terrain n'a été rapporté.

2.1.7 CBT

CBT [RFC2201][RFC2189] était un projet académique qui fournissait les bases pour des arborescences partagées de PIM en mode épars. Une fois la fonctionnalité d'arborescence partagée incorporée dans les mises en œuvre de PIM, il n'y avait plus

besoin de mettre en œuvre CBT sur le terrain. Donc, CBT n'a jamais connu de développement pratique.

2.1.8 Interactions et résumés

On peut noter qu'il est possible de faire fonctionner différents protocoles avec des gammes différentes de groupes de diffusion. Par exemple, traiter certains groupes comme denses or bidirectionnels dans un réseau PIM-SM ; cela exige normalement une configuration manuelle des groupes ou un mécanisme comme BSR (paragraphe 2.4.3). Il est aussi possible d'interagir entre différent protocoles ; par exemple, utiliser DVMRP dans le réseau d'extrémité, mais PIM-SM en amont. Les bases des interactions entre les différents protocoles ont été décrites dans la [RFC2715].

Le tableau suivant donne un résumé concis de l'état de développement des différents protocoles au moment de cette publication.

	Inter-domaine	**Intra-domaine**	**État**
PIM-SM	Oui	Oui	Actif
PIM-DM	Plus utilisé	Plus utilisé	Peu d'usage
BIDIR-PIM	Non	oui	Quelques utilisations
DVMRP	Plus utilisé	Seulement en réseau de bout	Sortant
MOSPF	Non	Plus utilisé	Inactif
CBT	Non	Non	Jamais déployé
BGMP	Non	Non	Jamais déployé

D'après de tableau, il est clair que PIM en mode épars est le seul protocole d'acheminement de diffusion groupée qui soit déployé en inter domaine et donc, est le plus fréquemment utilisé aussi au sein des domaines de diffusion groupée.

2.2 Distribution des informations de topologie

PIM est devenu de fait le protocole de transmission de la diffusion groupée, mais comme son nom l'implique, il est indépendant du protocole d'acheminement d'envoi individuel sous-jacent. Lorsque les topologies d'envoi individuel et de diffusion groupée ont la même "congruence", c'est à dire, utilisent les mêmes tableaux d'acheminement (base d'informations d'acheminement, RIB), il a été considéré qu'il était suffisant de simplement distribuer un ensemble d'informations d'accessibilité pour les utiliser en conjonction avec un protocole qui établisse l'état de transmission de diffusion groupée(par exemple, PIM-SM).

Cependant, lorsque PIM qui par défaut construit une topologie de diffusion groupée fondée sur la topologie d'envoi individuel a gagné en popularité, il est devenu évident qu'il serait nécessaire d'être capable de distribuer aussi des informations d'accessibilité de diffusion groupé non congruentes dans les protocoles normaux d'envoi individuel. Cela ne posait pas de problème auparavant , parce que DVMRP construisait ses propres informations d'accessibilité.

Les informations topologiques sont nécessaires pour effectuer une distribution efficace des transmissions en diffusion groupée et empêcher les transmissions en boucle en appliquant la vérification de transmission sur le chemin inverse (RPF).

Ce paragraphe introduit ces protocoles.

2.2.1 BGP multiprotocole

Les extensions multiprotocole à BGP-4 [RFC4760] (souvent désignées par le terme "MBGP" ; il faut cependant noter que "MBGP" ne veut pas dire "BGP en diffusion groupée") spécifient un mécanisme par lequel BGP peut être utilisé pour distribuer différentes informations d'accessibilité pour l'envoi individuel (SAFI=1) et du trafic en diffusion groupée (SAFI=2). BGP multiprotocole a été largement déployé pendant des années, et est aussi nécessaire pour l'acheminement IPv6. Noter que SAFI=3 était à l'origine spécifié aussi bien pour l'envoi individuel que pour la diffusion groupée mais est maintenant devenu déconseillé.

Ces extensions sont d'usage courant chaque fois que BGP est utilisé pour distribuer des informations de topologie en envoi individuel. Les réseaux à capacité de diffusion groupé qui utilisent BGP devraient utiliser BGP multiprotocole pour distribuer explicitement des informations d'accessibilité de diffusion groupé même si les topologies sont congruentes pour faire une déclaration explicite sur l'accessibilité de la diffusion groupé. Un certain nombre de fournisseurs de transit de diffusion groupée significative l'exigent même, en ne fondant les recherches de RPF que sur la famille d'adresses de diffusion groupée annoncée explicitement.

2.2.2 Extensions multi topologies OSPF/IS-IS

De même que BGP, certains protocoles de routeur intérieur (IGP) peuvent aussi fournir la capacité de signalisation de différences de topologie, par exemple les extensions multi-topologie IS-IS [RFC5120]. Celles-ci peuvent être utilisée pour une topologie de diffusion groupée qui diffère de l'envoi individuel. Un travail similaire mais moins répandu existe pour OSPF [RFC4915].

Il vaut de noter que les incongruences inter domaine et intra domaine sont orthogonale, aussi l'une ne doit pas exiger l'autre. Précisément, l'incongruence inter domaine est assez courante, alors que l'incongruence intra domaine ne l'est pas, de sorte qu'on voit plus de développements de MBGP que de MT-ISIS/OSPF. Les réseaux couramment déployés se sont bien gérés sans avoir de protocoles pour traiter l'incongruence intra domaine. Cependant, la disponibilité de mécanismes multi-topologie peut remplacer en partie les astuces normalement utilisées en remplacement comme les tunnels.

2.2.3 Problème : topologies d'envoi individuel/diffusion groupée en chevauchement

Un cas intéressant survient lorsque certains routeurs ne distribuent pas explicitement les informations de topologie de diffusion groupée alors que d'autres le font. En particulier, cela arrive lorsque certains sites de diffusion groupé dans l'Internet utilisent BGP complet alors que d'autres utilisent MBGP.

Des mises en œuvre différentes ont chacune leur traitement. Parfois, des mécanismes RPF de diffusion groupée commencent par chercher le tableau d'acheminement de diffusion groupée, ou M-RIB ("base de données de topologie") avec l'algorithme de correspondance du plus long préfixe, et si ils trouvent une entrée (y compris une route par défaut), c'est elle qui est utilisée ; si aucune correspondance n'est trouvée, on utilise à la place le tableau d'acheminement.

Une autre approche est d'utiliser la correspondance du plus long préfixe sur l'union des tableaux d'acheminement de l'envoi individuel et de la diffusion groupée ; une technique de mise en œuvre est ici de copier tout le tableau d'acheminement d'envoi individuel dans le tableau d'acheminement de la diffusion groupée. Le point important dont il faut se souvenir est de ne pas outrepasser les chemins seulement en diffusion groupée ; si la correspondance du plus long préfixe trouve à la fois un chemin en envoi individuel (copié) et un chemin de diffusion groupée seule, ce dernier devrait être traité comme le préféré.

Une autre approche de mise en œuvre est de simplement rechercher les informations dans le tableau d'acheminement d'envoi individuel, et de donner à l'utilisateur la capacité d'en changer en tant que de besoin, en utilisant par exemple les fonction de copie exposées plus haut.

2.2.4 Résumé

Une topologie congruente peut être déployée en utilisant les protocoles d'acheminement en envoi individuel qui ne fournissent pas de prise en charge d'une topologie de diffusion groupée séparée. Dans l'intra domaine, cette approche est souvent adéquate. Cependant, il est recommandé que si l'acheminement inter domaine utilise BGP, les sites à capacité de diffusion groupée devraient utiliser SAFI=2 de MP-BGP pour la diffusion groupée et SAFI=1 pour l'envoi individuel même si la topologie est congruente pour signaler explicitement "oui, nous utilisons la diffusion groupée".

Le tableau suivant résume les approches qui peuvent être utilisées pour distribuer les informations de topologie de diffusion groupée.

	Interdomaine	**Intradomaine**
MP-BGP SAFI=2	Oui	Oui
MP-BGP SAFI=3	Ne fonctionne pas	Ne fonctionne pas
IS-IS multi-topologie	Pas applicable	Oui
OSPF multi-topologie	Pas applicable	Peu de mises en œuvre

"Pas applicable" se réfère au fait que les protocoles IGP ne peuvent pas être utilisés dans l'acheminement inter domaine. "Ne fonctionne pas" signifie qu'alors que le SAFI=3 MP-BGP a été défini et pourrait s'appliquer, cette partie de la spécification n'a pas été mise en œuvre et ne peut pas être utilisée en pratique. "Oui" fait la liste des mécanismes qui sont généralement applicables et savent comment fonctionner. "Peu de mises en œuvre" signifie que l'approche pourrait fonctionner mais n'est pas couramment disponible.

2.3 Apprendre les sources (actives)

Pour construire un arbre de distribution de diffusion groupée, le protocole d'acheminement a besoin de découvrir où sont les sources pour le groupe. Dans le cas de SSM, l'usager spécifie l'adresse IP de source qui autrement est apprise hors bande.

En ASM, les RP savent tout des sources actives dans un domaine PIM local. Il en résulte que quand on utilise PIM-SM ou BIDIR-PIM en intra domaine, les sources sont apprises au titre du protocole lui-même.

Avoir un seul domaine PIM-SM pour la totalité de l'Internet est un modèle insuffisant pour de nombreuses raisons, parmi lesquelles les problèmes d'échelle, de frontières administratives, et différents compromis techniques. Donc, il est nécessaire d'être capable de partager les infrastructures d'acheminement de diffusion groupée en de plus petits domaines, et il doit y avoir un moyen de partager les informations sur les sources actives en utilisant certains mécanismes si le modèle ASM doit être pris en charge.

La présente section expose les options d'apprentissage des sources actives qui s'appliquent dans un environnement inter domaine.

2.3.1 SSM

La diffusion groupée spécifique de source [RFC4607] (parfois aussi appelée "diffusion groupé à source unique") ne compte pas sur l'apprentissage des sources actives dans le réseau. Les receveurs ont besoin en utilisant un mécanisme hors bande de savoir les adresses IP de source qui sont utilisées pour s'abonner au canal (de source, de groupe). L'acheminement de la diffusion groupée utilise les adresses de source pour établir l'état et aucune autre découverte de source n'est nécessaire.

Au moment de la rédaction de ce document, il y a des tentatives d'analyse et/ou définition de fonctions de découverte de source hors bande qui pourraient aider SSM, en particulier [DYNSSM-REQ].

2.3.2 MSDP

Le protocole de découverte de source de diffusion groupée [RFC3618] a été inventé comme mécanisme bouche trou, lorsqu'il est devenu évident que plusieurs domaines PIM-SM (et RP) étaient nécessaires dans le réseau, et qu'il était nécessaire de diffuser des informations sur les sources actives entre les domaines PIM-SM utilisant un autre protocole.

MSDP est aussi utilisé pour partager l'état des sources entre plusieurs RP dans un seul domaine pour, par exemple, des besoins de redondance [RFC3446]. On peut obtenir le même résultat en utilisant les extensions de PIM [RFC4610]. Voir un complément d'information au paragraphe 2.5.

Il n'est pas prévu de définir MSDP pour IPv6, mais plutôt d'utiliser seulement SSM et des RP incorporés [MCAST-ISSUES].

2.3.3 Point de rendez-vous incorporé

Le RP incorporé [RFC3956] est une technique de IPv6 seul pour transposer l'adresse du RP en adresse de groupe de diffusion groupée. En utilisant cette méthode, il est possible d'éviter l'utilisation de MSDP tout en permettant quand même plusieurs domaines de diffusion groupée (au sens traditionnel).

Le modèle fonctionne avec la définition d'une seule adresse de RP pour un groupe particulier pour tout l'Internet, de sorte qu'il n'est pas besoin de partager l'état avec d'autres RP. Si nécessaire, la redondance de RP peut encore être réalisée avec un RP d'envoi à la cantonade en utilisant PIM [RFC4610].

2.3.4 Résumé

Le tableau suivant résume les approches de découverte de source et leur état :

	IPv4	**IPv6**	**État**
Un seul domaine bidirectionnel	Oui	Oui	OK mais seulement pour l'intra-domaine
Un seul domaine PIM-SM	Oui	Oui	OK
PIM-SM avec MSDP	Oui	Non	De fait ASM inter-domaine v4
PIM-SM avec RP incorporé	Non	Oui	Option meilleur ASM inter domaine
SSM	Oui	Oui	Pas encore de décollage significatif

2.4 Configurer et distribuer les informations de PIM RP

Il existe les mécanismes de configuration PIM-SM et BIDIR-PIM, qui sont utilisés pour configurer les adresses de RP et les groupes qui vont utiliser ces points de rendez vous dans les routeurs. Cette section développe les approches.

2.4.1 Configuration manuelle de RP

Le plus facile est souvent de configurer manuellement les informations de RP dans les routeurs lorsque PIM-SM est utilisé.

À l'origine, la transposition de RP statique était considérée comme sous optimale car elle exigeait des changements de configuration explicites chaque fois que changeait l'adresse du RP. Cependant, avec l'avènement de l'adressage de RP à la cantonade, l'adresse du RP ne va vraisemblablement plus jamais changer. Donc, le fardeau administratif est généralement limité à la configuration initiale. Comme il y a généralement de toutes façons une grande quantité de configuration en diffusion groupée qui est exigée sur tous les routeurs (par exemple, PIM sur toutes les interfaces), l'ajout statique de l'adresse de RP ne pose pas de réel problème. De plus, la transposition statique de RP à la cantonade a pour avantage de partager la charge des points de rendez-vous et de donner de la redondance (voir au paragraphe 2.5) sans la complexité qu'on trouve dans les mécanismes dynamiques comme ceux de l'auto-RP et du routeur d'amorçage (BSR).

Avec une telle conception, un point de rendez-vous à la cantonade utilise une adresse qui est configurée sur une interface de bouclage des routeurs qui agissent actuellement comme points de rendez-vous, et l'état est distribué à l'aide de PIM [RFC4610] ou de MSDP [RFC3446].

En utilisant cette technique, chaque routeur peut seulement avoir besoin d'être configuré avec une seule adresse de RP portable.

2.4.2 Points de rendez-vous incorporés

Le RP incorporé fournit les information sur l'adresse du RP dans les adresses de groupe qui sont déléguées à ceux qui utilisent le RP, aussi, si aucun autre ASM que le RP incorporé n'est utilisé, l'administrateur de réseau a seulement besoin de configurer les routeurs points de rendez-vous.

Alors que dans la plupart des cas le point de rendez-vous incorporé est suffisant pour IPv6, d'autres méthodes de configuration de RP sont nécessaires si on a besoin de fournir un service d'ASM pour d'autres que les adresses de groupe du point de rendez-vous incorporé. En particulier, le type d'application découverte de services peut avoir besoin d'adresses gravées dans le matériel qui ne dépendent pas des adresses de point de rendez-vous local.

Comme l'adresse du point de rendez-vous est exposée aux usagers et aux applications, il est très important de s'assurer qu'elle ne change pas souvent, par exemple, en utilisant la configuration manuelle d'une adresse d'envoi à la cantonade.

2.4.3 BSR et Auto-RP

BSR [RFC5059] est un mécanisme pour configurer l'adresse de point de rendez-vous pour les groupes. Il pourrait n'être plus d'aussi large utilisation que par le passé avec IPv4, et pour IPv6, le point de rendez-vous incorporé sera suffisant dans bien des cas.

Auto-RP de Cisco est une méthode brevetée plus ancienne pour distribuer des transpositions de groupe sur des points de rendez-vous, , similaire à BSR. Auto-RP est peu utilisé aujourd'hui.

Auto-RP et BSR exigent tous deux une certaine forme de contrôle aux routeurs pour s'assurer que seuls des routeurs valides sont capables de s'annoncer comme points de rendez-vous. De plus, l'arrosage de messages de BSR et d'Auto-RP doit être empêché aux frontières de PIM. Il faut ajouter que les administrateurs doivent surveiller que les routeurs utilisent bien en réalité le ou les points de rendez-vous qu'ils pensent qu'ils devraient utiliser, par exemple, si un routeur (qui peut être sous le contrôle d'un utilisateur) s'annonce lui-même de façon inappropriée. Tout bien compris, alors que BSR et Auto-RP fournissent une configuration facile, ils présentent aussi une complexité de configuration et de gestion très significative.

Il vaut de noter que Auto-RP et BSR ont tous deux été déployés avant que l'utilisation d'adresses de points de rendez-vous d'envoi à la cantonade configurées manuellement ne devienne aussi courante, et il y a en réalité assez peu de besoin d'eux aujourd'hui, sauf lorsqu'il est nécessaire de configurer différentes propriétés (par exemple, épars, dense, bidirectionnel) de façon dynamique.

2.4.4 Résumé

Le tableau suivant résume les mécanismes de découverte de point de rendez-vous et de leur état. À l'exception de RP incorporé, chaque mécanisme fonctionne au sein d'un domaine PIM.

	IPv4	IPv6	Déploiement
RP statique	oui	oui	particulièrement chez les ISP
Auto-RP	oui	non	déploiement résiduel
BSR	oui	oui	un peu, en envoi individuel
RP incorporé	non	oui	croissant

2.5 Mécanismes pour améliorer la redondance

Avoir un seul point de rendez-vous dans un domaine PIM-SM serait un seul point de défaillance pour la totalité du domaine de diffusion groupée. Par conséquent, un certain nombre de mécanismes ont été développés soit pour éliminer la fonctionnalité de point de rendez-vous, soit pour améliorer la redondance des points de rendez-vous, la résilience aux défaillances, et la récupération rapide de ces défaillances. La présente section résume explicitement ces techniques.

2.5.1 RP d'envoi à la cantonade

Comme mentionné au paragraphe 2.3.2, MSDP est aussi utilisa pour partager l'état sur les sources entre plusieurs points de rendez-vous dans un seul domaine, par exemple pour les besoins de la redondance [RFC3446]. L'objet de MSDP dans ce contexte est de partager les mêmes informations d'état entre plusieurs points de rendez-vous pour les mêmes groupes afin d'améliorer la robustesse du service.

De récentes extensions de PIM [RFC4610] fournissent aussi cette fonctionnalité. Par opposition à MSDP, cette approche fonctionne aussi bien pour IPv4 que pour IPv6.

2.5.2 Reprise sur défaillance de point de rendez-vous sans état

Alors que le point de rendez-vous d'envoi à la cantonade partage l'état entre les RP de façon que la défaillance du RP ne cause que peu de dérangement, les approches sans état sont aussi possibles avec une résilience plus limitée. Un mécanisme traditionnel a été d'utiliser l'Auto-RP ou BSR (voir au paragraphe 2.4.3) pour choisir un autre RP lorsque celui qui est actif est défaillant. Cependant, la même fonctionnalité pourrait être réalisée en utilisant l'adresse de point de rendez-vous partagée en envoi individuel ("RP en envoi à la cantonade sans partage d'état") sans la complexité d'un mécanisme dynamique. De plus, RP en envoi à la cantonade permet une stratégie d'atténuation des défaillance significativement plus large, de sorte qu'aujourd'hui, il y a en réalité un besoin très faible d'utilisation des mécanismes de récupération sur incident sans état, en particulier de ceux qui sont dynamiques, pour les besoins de la redondance.

2.5.3 PIM bidirectionnel

Comme la PIM bidirectionnelle (voir au paragraphe 2.1.3) ne commute pas sur l'arbre de plus court chemin (SPT), l'arbre de diffusion groupée final peut être établi plus rapidement. D'un autre côté, PIM-SM ou SSM peuvent converger plus vite, en particulier dans des scénarios (par exemple, de changement d'acheminement d'envoi individuel) où le bidirectionnel a besoin de refaire le choix de transmetteur désigné.

2.5.4 Résumé

Le tableau suivant résume les techniques de redondance améliorée.

	IPv4	IPv6	Déploiement
Point de rendez-vous d'envoi à la cantonade avec MSDP	Oui	Non	approche de facto
Point de rendez-vous d'envoi à la cantonade avec PIM	Oui	Ouis	approche plus nouvelle
Défaillance de point de rendez-vous sans état	Oui	Oui	cause des dérangements
BIDIR-PIM	Oui	Oui	Déployée sur certains sites

2.6 Interactions avec les hôtes

Les sections précédentes traitaient des composants requis des routeurs pour qu'ils soient capables de faire l'acheminement en diffusion groupée. Évidemment, les véritables utilisateurs de la diffusion groupée sont les hôtes : qu'ils envoient ou qu'ils reçoivent ladiffusion groupée. Cette section décrit les interactions exigées des hôtes.

2.6.1 Hôtes qui envoient de la diffusion groupée

Après avoir choisi un groupe de diffusion groupée par divers moyens, les hôtes envoient simplement les paquets à l'adresse de diffusion groupée de couche liaison, et le routeur désigné va recevoir tous les paquets de diffusion groupée et commencer à les transmettre comme approprié. Un hôte n'a pas besoin d'être membre du groupe pour lui faire des envois [RFC1112].

Dans l'intra domaine ou dans les scénarios de point de rendez-vous incorporé, les envoyeurs d'ASM peuvent passer à une nouvelle adresse IP sans impact significatif sur la livraison de leur transmission. Les envoyeurs de SSM ne peuvent pas changer l'adresse IP à moins que les receveurs ne rejoignent le nouveau canal ou que l'envoyeur n'utilise une technique de mobilité sur IP qui soit transparente pour les receveurs.

2.6.2 Hôtes qui reçoivent de la diffusion groupée

Les hôtes signalent leur intérêt à recevoir un groupe ou canal de diffusion groupé en utilisant IGMP [RFC3376] et MLD [RFC3810]. IGMPv2 et MLDv1 sont toujours d'utilisation courante, mais ils sont aussi souvent utilisés dans de nouveaux développements. Certains fabricants prennent aussi en charge les techniques de transposition de SSM pour les receveurs qui utilisent une plus ancienne version d'IGMP/MLD où le routeur transpose la demande jointe en un canal SSM sur la base de moyens de configuration divers, ordinairement assez complexes.

2.6.3 Résumé

Le tableau suivant résume les techniques d'interaction d'hôte.

	IPv4	**IPv6**	**Notes**
Hôte qui envoie	Oui	Oui	Pas de prise en charge nécessaire
Hôte qui reçoit l'ASM	IGMP	MLD	Toute version IGMP/MLD
Hôte qui reçoit la SSM	IGMPv3	MLDv2	Toute version w/ SSM-mapping

2.7 Restriction de l'arrosage de diffusion groupée dans la couche de liaison

La transmission de diffusion groupée dans la couche liaison, par exemple Ethernet, comporte normalement certaines formes d'arrosage des paquets à travers un LAN. Cela cause une utilisation inutile de bande passante et l'élimination des trames non désirées sur les nœuds qui ne veulent pas recevoir la transmission de diffusion groupée.

Donc un certain nombre de techniques ont été développées, à utiliser dans les commutateurs Ethernet entre les routeurs, ou entre routeurs et hôtes, pour limiter l'arrosage.

Certains mécanismes fonctionnent avec des adresses IP, d'autres avec des adresses MAC. Si le filtrage est fait sur la base des adresses MAC, les hôtes peuvent recevoir du trafic de diffusion groupée inutile (filtré à la couche IP des hôtes) si plus d'une adresse de groupe de diffusion groupée IP se transposent en la même adresse MAC, ou si les filtres de source IGMPv3/MLDv2 sont utilisés. Le filtrage fondé sur les adresses de destination IP, ou sur les adresses de destination et de sources, va aider à éviter cela, mais cela exige l'analyse de la charge utile de trame Ethernet.

Ces options sont exposées dans les paragraphes suivants.

2.7.1 Réduction de l'arrosage de routeur à routeur

Cisco a développé une solution brevetée, RGMP [RFC3488], pour réduire la quantité d'arrosage entre les routeurs dans les réseaux commutés. Ceci n'est normalement considéré comme posant un problème que dans certains points d'échange Internet ou VPN fondés sur Ethernet.

Il y a eu des propositions pour observer ("snoop") et éventuellement réagir aux messages de PIM [PIM-SNOOP].

2.7.2 Réduction de l'arrosage d'hôte/routeur

Il existe un certain nombre de techniques pour aider à réduire l'arrosage à la fois de routeur à hôtes, et d'hôtes à routeurs (et autres hôtes).

Le protocole CGMP [CGMP] breveté par Cisco fournit une solution dans laquelle les routeurs notifient les commutateurs, mais permet aussi aux commutateurs de surveiller les paquets IGMP pour permettre une notification plus rapide des hôtes

qui ne souhaitent plus recevoir un groupe. les mises en œuvre de CGMP ne prennent pas en charge le comportement d'abandon rapide avec IGMPv3. Du fait de la suppression du rapport IGMP dans IGMPv1 et IGMPv2, la diffusion groupée est toujours arrosée sur les accès qui ont été membres d'un groupe tant qu'il y a au moins un receveur sur la liaison. Les restrictions d'arrosage ne sont faites que sur la base des adresses MAC de diffusion groupée. Les mises en œuvre de CGMP ne prennent pas en charge IPv6.

La spécification IEEE 802.1D-2004 décrit le protocole générique d'enregistrement d'attribut (GARP), le protocole d'enregistrement de diffusion groupée selon GARP [GMRP] est une application de groupe de diffusion groupée de couche liaison de GARP qui notifie aux commutateurs les membres des groupe de diffusion groupée MAC. Si GMRP est utilisé en conjonction avec la diffusion groupée IP, la fonction d'enregistrement de GMRP va se trouver associée avec un "joint" IGMP. Cependant, cette association GMRP-IGMP sort du domaine d'application de GMRP. GMRP exige la prise en charge au niveau de la pile de protocoles de l'hôte et n'a pas été largement mis en œuvre. De plus, IEEE 802.1 considère GARP et GMRP comme obsolètes, ayant été remplacés par le protocole d'enregistrement multiple (MRP) et le protocole d'enregistrement multiple en diffusion groupée (MMRP) qui ont été spécifiés dans la norme IEEE 802.1ak [802.1ak]. MMRP est prévu pour être principalement utilisé entre des ponts. Des informations complémentaires sur GARP/GMRP sont aussi disponibles à l'Appendice B de la [RFC3488].

La surveillance IGMP [RFC4541] apparaît comme la technique la plus largement mise en œuvre. La surveillance IGMP exige que les commutateurs mettent en œuvre une quantité significative d'inspection de paquet de niveau IP ; cela paraît être quelque chose qui est difficile à faire correctement, et souvent les mises à niveau sont aussi un vrai défi. La prise en charge de la surveillance est courante pour IGMPv1 et IGMPv2, mais moins de commutateurs prennent en charge la surveillance IGMPv3 ou MLD (toutes versions). Dans le pire des as, activer la surveillance IGMP sur un commutateur qui ne prend pas en charge la surveillance IGMPv3 casse les capacités de diffusion groupée des nœuds qui utilisent IGMPv3.

La commutateurs qui font la surveillance ont aussi besoin d'identifier les accès où résident les routeurs et donc où il faut arroser les paquets. Cela peut être accompli en utilisant le protocole de découverte des routeurs de diffusion groupée [RFC4286], en cherchant certaines interrogations IGMP [RFC4541], en cherchant les Hello de PIM et éventuellement d'autres messages, ou par une configuration manuelle. Un problème de la surveillance de PIM sur les LAN est que les messages de PIM ne peuvent pas arrêtés ou chiffrés, ce qui conduit à des problèmes de sécurité [RFC5294].

L'utilisation de mandataires IGMP [RFC4605] sert parfois en remplacement d'un protocole d'acheminement de diffusion groupée sur un petit routeur, ou pour agréger des rapports IGMP/MLD lors de la surveillance IGMP.

2.7.3 Résumé

Le tableau suivant résume les techniques de réduction d'arrosage de diffusion groupée à l'intérieur d'une seule liaison de routeur à routeur et des LAN de dernier bond.

	R-to-R	**LAN**	**Notes**
RGMP de Cisco	Oui	Non	Remplacé par la surveillance de PIM
Surveillance de PIM	Oui	Non	Problèmes de sécurité dans les LAN
Surveillance IGMP/MLD	Non	Oui	Courante, IGMPv3 ou MLD rare
Découverte de routeur de diff. groupée	Non	Oui	Encore peu de mises en œuvre, s'il en est
GMRP et MMRP de l'IEEE	Non	Non	Pas de déploiement d'hôte/routeur
CGMP de Cisco	Non	Oui	Remplacé par une autre surveillance

3. Remerciements

Alors qu'il pilotait la rédaction de plusieurs articles relatifs à la diffusion groupé, le regretté Kaarle Ritvanen [RITVANEN] a convaincu l'auteur de la nécessité de mettre à jour ce document sur l'acheminement de la diffusion groupée et l'allocation des adresses.

Leonard Giuliano, James Lingard, Jean-Jacques Pansiot, Dave Meyer, Stig Venaas, Tom Pusateri, Marshall Eubanks, Dino Farinacci, Bharat Joshi, Albert Manfredi, Jean-Jacques Pansiot, Spencer Dawkins, Sharon Chisholm, John Zwiebel, Dan Romascanu, Thomas Morin, Ron Bonica, Prashant Jhingran, et Tim Polk ont fourni de bons commentaires qui ont aidé à améliorer le présent document.

4. Considérations relatives à l'IANA

IANA a mis à jour les registres suivants en y ajoutant une référence au présent document :
- o Registre des options OSPFv2 : MC-bit
- o Type d'état de liaison OSPFv2 : Group-membership-LSA
- o Registre des propriétés de routeur OSPFv2 : W-bit
- o Registre des options OSPFv3 : MC-bit
- o Registre des codes de fonction de LSA OSPFv3 : Group-membership-LSA
- o Registre des options de préfixe OSPFv3 : MC-bit

5. Considérations pour la sécurité

Le présent mémoire ne fait que décrire différentes approches de l'acheminement de la diffusion groupée, et cela sans aucune considération pour la sécurité ; l'analyse de sécurité des protocoles mentionnés est en dehors du domaine d'application du présent mémoire.

Cependant, il y a eu une analyse de la sécurité des infrastructures d'acheminement de la diffusion groupée dans la [RFC4609], IGMP/MLD [MLD-SEC], et des problèmes du dernier bond PIM [RFC5294].

6. Références

6.1 Références normatives

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", BCP 9, RFC 2026, octobre 1996.

[RFC3376] B. Cain, S. Deering, I. Kouvelas, B. Fenner et A. Thyagarajan, "Protocole Internet de gestion de groupe, IGMP version 3", RFC 3376, octobre 2002.

[RFC3618] B. Fenner et D. Meyer, "Protocole de découverte de source de diffusion groupée (MSDP)", RFC 3618, octobre 2003.

[RFC3810] R. Vida et L. Costa, "Découverte d'écouteur de diffusion groupée version 2 (MLDv2) pour IPv6", RFC 3810, juin 2004.

[RFC3956] P. Savola et B. Haberman, "Incorporation de l'adresse de point de rendez-vous (RP) dans une adresse de diffusion groupée IPv6", RFC 3956, novembre 2004.

[RFC4601] B. Fenner, M. Handley, H. Holbrook et I. Kouvelas, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : spécification du protocole (Révisée)", RFC 4601, août 2006.

[RFC4607] H. Holbrook et B. Cain, "Diffusion groupée spécifique de source pour IP", RFC 4607, août 2006.

[RFC4760] T. Bates, R. Chandra, D. Katz et Y. Rekhter, "Extensions multi protocoles pour BGP-4", RFC 4760, janvier 2007.

[RFC4915] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen et P. Pillay-Esnault, "Acheminement multi topologies (MT) dans OSPF", RFC 4915, juin 2007.

[RFC5015] M. Handley, I. Kouvelas, T. Speakman et L. Vicisano, "Diffusion groupée bidirectionnelle indépendante du protocole (BIDIR-PIM)", RFC 5015, octobre 2007.

6.2 Références informatives

[802.1ak] "IEEE 802.1ak - Multiple Registration Protocol", <http://www.ieee802.org/1/pages/802.1ak.html>.

[ADDRARCH] Savola, P., "Overview of the Internet Multicast Addressing Architecture", Travail en cours, octobre 2006.

[CGMP] "Cisco Group Management Protocol", <http://www.javvin.com/protocolCGMP.html>.

[DVMRPv3] Pusateri, T., "Distance Vector Multicast Routing Protocol", Travail en cours, décembre 2003.

[DVMRPv3-AS] Pusateri, T., "Distance Vector Multicast Routing Protocol Applicability Statement", Travail en cours,

mai 2004.

[DYNSSM-REQ] Lehtonen, R., Venaas, S., and M. Hoerdt, "Requirements for discovery of dynamic SSM sources", Travail en cours, février 2005.

[GMRP] "GARP Multicast Registration Protocol", <http://www.javvin.com/protocolGMRP.html>.

[IM-GAPS] Meyer, D. and B. Nickless, "Internet Multicast Gap Analysis from the MBONED Working Group for the IESG [Expired]", Travail en cours, juillet 2002.

[IMRP-ISSUES] D. Meyer, "Some Issues for an Inter-domain Multicast Routing Protocol", Travail en cours, novembre 1997.

[MCAST-ISSUES] P. Savola, "IPv6 Multicast Deployment Issues", Travail en cours, février 2005.

[MLD-SEC] Daley, G. and G. Kurup, "Trust Models and Security in Multicast Listener Discovery", Travail en cours, juillet 2004.

[PIM-SNOOP] V. Hemige, "PIM Snooping over VPLS", Travail en cours, mars 2007.

[RFC1075] D. Waitzman, C. Partridge et S. Deering, "Protocole d'acheminement en diffusion groupée par vecteur de distance", RFC 1075, novembre 1988.

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, RFC 1112, août 1989.

[RFC1458] B. Braudes et S. Zabele, "Exigences pour les protocoles de diffusion groupée", RFC 1458, mai 1993.

[RFC1584] J. Moy, "Extensions de diffusion groupée à OSPF", RFC 1584, mars 1994.

[RFC2189] T. Ballardie, "Acheminement de diffusion groupée en arborescences fondées sur le cœur de réseau (CBT version 2)", RFC 2189, septembre 1997.

[RFC2201] T. Ballardie, "Architecture d'acheminement de diffusion groupée d'arborescences fondées sur le cœur (CBT)", RFC 2201, septembre 1997.

[RFC2715] D. Thaler, "Règles d'interopérabilité pour les protocoles d'acheminement de diffusion groupée", RFC 2715, octobre 1999.

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", RFC 2784, mars 2000.

[RFC3208] T. Speakman, J. Crowcroft, J. Gemmell, D. Farinacci, S. Lin, D. Leshchiner, M. Luby, T. Montgomery, L. Rizzo, A. Tweedly, N. Bhaskar, R. Edmonstone, R. Sumanasekera et L. Vicisano, "Spécification du protocole PGM de transport fiable", RFC 3208, décembre 2001.

[RFC3446] D. Kim, D. Meyer, H. Kilmer et D. Farinacci, "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)", RFC 3446, janvier 2003.

[RFC3488] I. Wu et T. Eckert, "Protocole de gestion de groupe d'accès de routeur de Cisco Systems (RGMP)", RFC 3488, février 2003.

[RFC3740] T. Hardjono et B. Weis, "Architecture de sécurité de groupe de diffusion groupée", RFC 3740, mars 2004.

[RFC3913] D. Thaler, "Protocole de routeur frontière de diffusion groupée (BGMP) : spécification du protocole, RFC 3913, septembre 2004.

[RFC3973] A. Adams, J. Nicholas et W. Siadak, "Diffusion groupée indépendante du protocole - Mode dense (PIM-DM) : Spécification du protocole (révisée)", RFC 3973, janvier 2005.

[RFC4286] B. Haberman et J. Martin, "Découverte de routeur de diffusion groupée", RFC 4286, décembre 2005.[RFC4541] M. Christensen, K. Kimball et F. Solensky, "Considérations sur les commutateurs d'observation du protocole de gestion de groupe Internet (IGMP) et de découverte d'écoutant de diffusion groupée (MLD)", RFC 4541, mai 2006.

[RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", RFC 4566, juillet 2006.

[RFC4605] B. Fenner, H. He, B. Haberman et H. Sandick, "Transmission de diffusion groupée fondée sur la découverte d'écoutant de diffusion groupée (MLD) du protocole de gestion de groupe Internet (IGMP) ("mandataire IGMP/MLD")", RFC 4605, août 2006.

[RFC4609] P. Savola, R. Lehtonen et D. Meyer, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : questions de sécurité de l'acheminement de la diffusion groupée et améliorations", RFC 4609, octobre 2006.

[RFC4610] D. Farinacci et Y. Cai, "Point de rendez-vous d'envoi à la cantonade utilisant la diffusion groupée indépendante

du protocole (PIM)", RFC 4610, août 2006.

[RFC5059] N. Bhaskar, A. Gall, J. Lingard et S. Venaas, "Mécanisme de routeur d'amorçage (BSR) pour la diffusion groupée indépendante du protocole (PIM)", RFC 5059, janvier 2008.

[RFC5120] T. Przygienda, N. Shen, N. Sheth, "M-ISIS : acheminement multi topologies (MT) de système intermédiaire à système intermédiaire (IS-IS)", février 2008. *(P.S.)*

[RFC5294] P. Savola, J. Lingard, "Menaces sur la diffusion groupée indépendante du protocole (PIM) au niveau de l'hôte", août 2008. *(Information)*

[RITVANEN] Ritvanen, K., "Multicast Routing and Addressing", HUT Report, Seminar on Internetworking, mai 2004, <http://www.tml.hut.fi/Studies/T-110.551/2004/ papers/>.

Appendice A. Extensions de transport de charge utile en diffusion groupée

Deux mécanismes ont été spécifiés pour améliorer les caractéristiques des données qui peuvent être transportées sur la diffusion groupée.

On décrit les mécanismes qui ont un impact sur l'infrastructure d'acheminement de la diffusion groupée, par exemple, qui exigent ou spécifient l'assistance du routeur ou son implication d'une façon ou d'une autre. Les protocoles qui sont purement de bout en bout ou fondés sur l'hôte ne sont pas visés.

A.1 Diffusion groupée fiable

Il y a eu des travaux sur la livraison fiable de diffusion groupée de sorte que les applications qui ont des exigences de fiabilité pourraient utiliser la diffusion groupée au lieu du simple UDP non fiable.

La plupart des mécanismes sont fondés sur l'hôte et comme tels sortent du domaine d'application du présent document, mais il en est un qui est pertinent du point de vue de l'acheminement en diffusion groupée et s'appelle Diffusion groupée générique pragmatique (PGM, Pragmatic Generic Multicast) [RFC3208]. Il n'exige pas de prise en charge de la part des routeurs, mais les routeurs à capacité PGM peuvent jouer un rôle d'assistance aux routeurs dans la livraison initiale et la retransmission éventuelle des données manquantes.

A.2 Groupe Sécurité en diffusion groupée

Le groupe de travail Sécurité en diffusion groupée a travaillé sur les méthodes par lesquelles l'intégrité, la confidentialité, et l'authentification des données envoyées aux groupes de diffusion peuvent être assurées en utilisant des techniques cryptographiques [RFC3740].

Adresse de l'auteur

Pekka Savola
CSC - Scientific Computing Ltd.
Espoo
Finland
mél : psavola@funet.fi

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait 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.