Groupe de travail Réseau
Request for Comments : 4611
BCP 121
Catégorie : Bonnes pratiques actuelles
Traduction Claude Brière de L'Isle

M. McBride
J. Meylor
D. Meyer
août 2006

Scénarios de déploiement du protocole de découverte de source de diffusion groupée (MSDP)

Statut du présent mémoire
Ce document spécifie les bonnes pratiques actuelles sur l'Internet pour la communauté de l'Internet, et demande des discussions et suggestions pour son amélioration. La diffusion du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright
Copyright (C) The Internet Society (2006).

Résumé
Le présent document décrit les bonnes pratiques actuelles pour le déploiement intra domaine et inter domaines du protocole de découverte de source de diffusion groupée (MSDP, *Multicast Source Discovery Protocol*) en conjonction avec le mode épars de diffusion groupée indépendante du protocole (PIM-SM, *Protocol Independent Multicast Sparse Mode*).

Table des matières

1. Introduction

MSDP [RFC3618] est utilisé principalement dans deux scénarios de déploiement :

o Entre des domaines PIM : MSDP peut être utilisé entre des domaines en mode épars de diffusion groupée indépendante du protocole (PIM-SM, *Protocol Independent Multicast Sparse Mode*) [RFC4601] pour porter des informations sur les sources actives disponibles dans d'autres domaines. L'échange de trafic MSDP utilisé dans de tels cas est généralement un échange de trafic de un à un, et utilise les règles déterministes de transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) de l'homologue décrites dans la spécification MSDP (c'est-à-dire, il n'utilise pas de groupes maillés).

Les échanges de trafic peuvent être agrégés sur un seul homologue MSDP. Un tel homologue peut normalement avoir de un à des centaines d'échanges de trafic, ce qui est similaire en échelle aux échanges de trafic de BGP.

- Au sein d'un domaine PIM : MSDP est souvent utilisé entre des points de rendez-vous (RP, *Rendezvous Point*) en envoi à la cantonnade (Anycast-RP) [RFC3446] au sein d'un domaine PIM pour synchroniser les informations sur les sources actives desservies par chaque homologue Anycast-RP (en vertu de l'accessibilité IGP). L'échange de trafic MSDP utilisé dans ce scénario est normalement fondé sur des groupes de maillage MSDP, où de deux à des dizaines d'homologues peuvent composer un groupe de maillage, bien que plus de dix ne soit pas courant. Un ou plusieurs de ces homologues de groupe de maillage peuvent aussi avoir des échanges de trafic supplémentaires de un à un avec des homologues MSDP en dehors de ce domaine PIM pour découvrir des sources externes. MSDP pour point de rendez-vous en envoi à la cantonnade sans échange de trafic MSDP externe est une option de déploiement valide et courante.

Les bonnes pratiques courantes pour les déploiement de MSDP utilisent PIM-SM et le protocole de routeur frontière avec des extensions multi protocoles (MBGP) [RFC4271], [RFC2858]. Le présent document souligne comment ces protocoles fonctionnent ensemble pour fournir un service de diffusion groupée toutes sources (ASM, *Any Source Multicast*) intra-domaine et inter-domaines.

La spécification PIM-SM suppose que le mode épars fonctionne seulement dans un domaine PIM. MSDP est utilisé pour permettre l'utilisation de plusieurs domaines PIM en distribuant les informations requises sur les sources actives de diffusion groupée aux autres domaines PIM. En partageant l'infrastructure de diffusion groupée de l'Internet en plusieurs domaines PIM, MSDP donne aussi la possibilité de mettre en place une politique sur la visibilité des groupes et sources.

Les fournisseurs IP de transit déploient normalement MSDP au titre de l'infrastructure globale de diffusion groupée en connectant les réseaux amont et homologue de diffusion groupée à leurs réseaux amont et homologue de diffusion groupée en utilisant MSDP.

Les réseaux de diffusion groupée de bordure ont normalement un choix : utiliser le RP de leur fournisseur Internet, ou avoir leur propre RP et le connecter à leur FAI en utilisant MSDP. En déployant leur propre RP et MSDP, ils peuvent utiliser des groupes de diffusion groupée internes qui ne sont pas visibles au RP du fournisseur. Cela aide la diffusion groupée interne à être capable de continuer à travailler en cas de problème de connexité au fournisseur ou si le RP/MSDP du fournisseur rencontre des difficultés.Dans les cas les plus simples, où aucun groupe de diffusion groupée interne n'est nécessaire, il n'est souvent pas nécessaire de déployer MSDP.

1.1 BCP, protocoles expérimentaux, et références normatives

Le présent document décrit les bonnes pratiques actuelles pour un protocole expérimental largement déployé, MSDP. Il n'est pas prévu d'avancer le statut de MSDP (par exemple, en proposition de norme). Les raisons sont :

- MSDP a été envisagé à l'origine comme un protocole temporaire destiné à être supplanté par ce que le groupe de travail IDMR produirait comme protocole inter domaines. Cependant, le groupe de travail IDMR (ou ensuite le groupe de travail BGMP) n'a jamais produit un protocole qui pourrait être déployé pour remplacer MSDP.

- Une des principales raisons données pour que MSDP soit classé comme expérimental était que le groupe de travail MSDP avait des modifications au protocole que le groupe estimait qu'il valait mieux que les mises en œuvre ne déploient pas. Sans ces modifications (par exemple, encapsulation UDP ou GRE) MSDP peut avoir des conséquences négatives sur les paquets initiaux dans les flux de datagrammes.

- Adaptabilité : bien qu'on ignore quelles sont les limites réelles, réannoncer tout ce qu'on sait toutes les 60 secondes limite clairement la quantité d'état qu'on peut annoncer.

- MSDP a atteint un déploiement presque universel comme norme de fait de protocole de diffusion groupée inter domaines dans l'Internet IPv4.

- Aucun consensus n'a pu être obtenu au sein de l'IETF pour retravailler MSDP afin de traiter les nombreux problèmes de divers constituants. Par suite, il a été décidé de documenter ce qui est (universellement) déployé et de passer ce document comme expérimental. Bien que l'avancement de MSDP au statut de proposition de norme ait été considéré, pour les raisons mentionnées ci-dessus, cela a été immédiatement éliminé.

- L'arrivée de protocoles comme la diffusion groupée spécifique de source et PIM bidirectionnel, ainsi que les techniques

de RP incorporé pour IPv6, ont encore réduit le consensus qu'un protocole de remplacement de MSDP pour l'Internet IPv4 était nécessaire.

La politique de l'éditeur des RFC concernant les références est qu'elles soient séparées en deux catégories connues comme "normatives" et "pour information". Les références normatives spécifient les documents qui doivent être lus pour qu'on comprenne ou mette en œuvre la technologie d'une RFC (ou dont la technologie doit être présente pour que celle de la nouvelle RFC fonctionne) [RFCED]. Afin de comprendre le présent document, on doit aussi comprendre les documents de PIM et de MSDP. Par suite, les références à ces documents sont normatives.

L'IETF a adopté comme politique que les BCP ne doivent pas avoir de références normatives à des protocoles expérimentaux. Cependant, le présent document est un cas particulier en ce que le document expérimental sous-jacent (MSDP) n'est pas prévu comme devant être avancé au statut de norme proposée.

Le groupe de travail MBONED a demandé l'approbation sous la procédure de variante documentée dans la [RFC2026]. L'IESG a suivi la procédure de variante, après un dernier appel à l'IETF de quatre semaines, a évalué les commentaires et le statut, et a approuvé le présent document.

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 le BCP 14, [RFC2119].

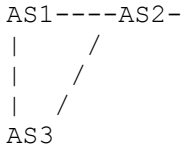
2. Scénarios d'échange de trafic MSDP inter domaines

Les paragraphes qui suivent décrivent les possibilités les plus courantes d'échange de trafic inter domaines de MSDP et leurs options de déploiement.

2.1 Échange de trafic entre routeurs PIM de bordures

Dans ce cas, les homologues MSDP au sein du domaine ont leur propre RP situé au sein d'un domaine PIM limité. De plus, le domaine va normalement avoir son propre numéro de système autonome (AS, *Autonomous System*) et un ou plusieurs locuteurs MBGP. Le domaine peut aussi avoir plusieurs locuteurs MSDP. Chaque routeur de bordure a un échange de trafic MSDP et MBGP avec ses routeurs homologues. Ces déploiements d'échange de trafic MSDP externes configurent normalement l'échange de trafic MBGP et l'échange de trafic MSDP en utilisant la même adresse IP d'homologue de prochain bond directement connecté ou une autre adresse IP du même routeur. Les déploiements normaux de ce type sont des fournisseurs qui ont un échange de trafic direct avec d'autres fournisseurs, des fournisseurs qui échangent du trafic à un commutateur, ou des fournisseurs qui utilisent leur routeur de bordure pour échanger du trafic MSDP/MBGP avec les clients.

Pour qu'un environnement d'échange de trafic inter domaines direct réussisse, le premier AS dans le meilleur chemin MBGP au RP d'origine devrait être le même que l'AS de l'homologue MSDP. Par exemple, considérons la topologie suivante :



Dans ce cas, AS4 reçoit un message Source Active (SA) généré par AS1, de AS2. AS2 a aussi un échange de trafic MBGP avec AS4. L'AS de premier bond MBGP provenant de AS4, dans le meilleur chemin pour le RP d'origine, est AS2. L'AS de l'homologue MSDP envoyeur est aussi AS2. Dans ce cas, la vérification de transmission sur le chemin inverse de l'homologue (RPF, *Reverse Path Forwarding)* réussit, et le message SA est transmis.

Une défaillance de RPF d'homologue va se produire dans cette topologie quand l'AS de premier bond MBGP, dans le meilleur chemin pour le RP d'origine, est AS2 et que l'AS d'origine de l'homologue MSDP envoyeur est AS3. S'appuyer sur les informations d'AS PATH BGP empêche des boucles sans fin des paquets de SA.

Le code du routeur, qui a adopté les dernières règles du document MSDP, va relâcher un peu les règles entre les AS. Dans la topologie suivante, on a un échange de trafic MSDP entre AS1<->AS3 et AS3<->AS4:

```
                              RP
AS1----AS2----AS3----AS4
```

Si le premier AS dans le meilleur chemin pour le RP n'est pas égal à l'homologue MSDP, l'homologue MSDP-RPF échoue. Donc AS1 ne peut pas échanger de trafic MSDP avec AS3, car AS2 est le premier AS dans le meilleur chemin MBGP pour le RP AS4. Avec le code conforme au dernier document MSDP, AS1 va choisir l'homologue dans le plus proche AS le long du meilleur chemin pour le RP. AS1 va alors accepter les SA venant de AS3. Si il y a plusieurs homologues MSDP pour les routeurs au sein du même AS, l'homologue avec la plus forte adresse IP est choisi comme homologue RPF.

2.2 Échange de trafic entre routeurs PIM non de bordure

Pour l'échange de trafic MSDP entre routeurs de bordure, l'adaptabilité MSDP intra domaine est restreinte parce que il est nécessaire de maintenir aussi les échanges de trafic MBGP et MSDP en interne vers leurs routeurs de bordure. Au sein de l'intra-domaine, le routeur de bordure devient l'annonceur du prochain bond vers le RP générateur. Cela exige que tous les échanges de trafic MSDP intra-domaine reflètent le chemin MBGP de retour vers le routeur de bordure. Les échanges de trafic MSDP externes (eMSDP) s'appuient sur le chemin d'AS pour la vérification de RPF d'homologue, tandis que les échanges de trafic MSDP internes (iMSDP) s'appuient sur l'annonceur du prochain bond.

Alors que l'homologue eMBGP est normalement directement connecté entre routeurs de bordure, il est courant que l'homologue eMSDP soit situé plus profondément dans l'AS du fournisseur de transit. Les fournisseurs, qui souhaitent plus de souplesse dans le placement de l'échange de trafic MSDP, choisissent couramment quelques routeurs dédiés au sein de leur cœur de réseau pour les échanges de trafic MSDP inter-domaines pour leur clients. Ces routeurs MSDP de cœur vont aussi être normalement dans le groupe de maillage MSDP intra domaine du fournisseur et être configurés comme RP d'envoi à la cantonnade. Tous les routeurs de diffusion groupée de l'AS du fournisseur devraient pointer statiquement sur l'adresse d'envoi à la cantonade du RP. L'allocation statique de RP est la méthode la plus couramment utilisée pour la transposition de groupe à RP du fait de sa nature déterministe. Les mécanismes de transposition dynamique de RP Auto-RP [RFC4601] et/ou de routeur Bootstrap [BSR] pourraient aussi être utilisés pour disséminer les informations de RP au sein du réseau du fournisseur.

Pour qu'un message SA soit accepté dans cet environnement (échange de trafic multi bonds) on s'appuie sur le prochain AS (ou le plus proche, avec la dernière spécification de MSDP) dans le meilleur chemin vers le RP générateur pour la vérification de RPF. L'adresse de l'homologue MSDP devrait être dans le même AS que l'AS de l'homologue MBGP du routeur de bordure. L'adresse de l'homologue MSDP devrait être annoncée via MBGP.

Par exemple, dans le diagramme ci-dessous, si le routeur R1 de client échange du trafic MBGP avec le routeur R2 et si R1 échange du trafic MBGP avec le routeur R3, alors R2 et R3 doivent être dans le même AS (ou doivent apparaître, à AS1, comme étant du même AS dans le cas où des numéros d'AS privés seraient déployés). L'homologue MSDP avec la plus forte adresse IP va être choisi comme homologue RPF MSDP. R1 doit aussi avoir l'adresse de l'homologue MSDP de R3 dans son tableau MBGP.

```
+--+    +--+    +--+
|R1|----|R2|----|R3|
+--+    +--+    +--+
AS1     AS2     AS2
```

Du point de vue de R3, AS1 (R1) est le prochain AS MBGP dans le meilleur chemin vers le RP générateur. Tant que AS1 est le prochain AS (ou le plus proche) dans le meilleur chemin vers le RP générateur, RPF va réussir sur les SA arrivant de R1.

À l'opposé, avec le scénario d'un seul bond, avec R2 (au lieu de R3) qui échange du trafic MSDP de bordure avec la bordure R1, l'adresse MBGP de R2 devient l'annonceur du prochain bond pour R3, vers le RP générateur, et R3 doit échanger du trafic avec cette adresse de R2. De plus, tous les homologues AS2 intra-domaine MSDP ont besoin de suivre les échanges de trafic iMBGP (ou d'un autre IGP) vers R2 car iMSDP est dépendant de l'échange de trafic avec l'adresse de l'annonceur MBGP (ou autre IGP) du prochain bond.

2.3 Échange de trafic MSDP sans BGP

Dans ce cas, une entreprise maintient son propre RP et a un échange de trafic MSDP avec son fournisseur de service mais n'échange pas de trafic BGP avec eux. MSDP s'appuie sur les informations de chemin BGP pour apprendre la topologie MSDP pour la vérification RPF de SA d'homologue. MSDP peut cependant être déployé sans BGP, et par suite, il y a des cas particuliers où l'exigence d'effectuer une vérification de RPF d'homologue sur les informations de chemin BGP est suspendue. Ces cas sont :

- o Il y a une seule connexion d'homologue MSDP.
- o Un homologue par défaut (chemin MSDP par défaut) est configuré.
- o Le RP générateur est directement connecté.
- o Un groupe maillé est utilisé.
- o Une mise en œuvre qui permet la vérification RPF d'homologue MSDP utilisant un IGP est utilisée.

Une entreprise va normalement configurer un chemin d'envoi individuel par défaut de son routeur bordure au routeur bordure du fournisseur et ensuite échanger du trafic MSDP avec le routeur MSDP du fournisseur. Si les échanges de trafic interne MSDP sont aussi utilisés au sein de l'entreprise, alors un homologue MSDP par défaut va devoir être configuré sur le routeur bordure qui pointe sur le fournisseur. De cette façon, toutes les sources externes de diffusion groupée vont être apprises, et les sources internes peuvent être annoncées. Si seulement un échange de trafic MSDP est utilisé (pas d'échange de trafic interne MSDP) vers le fournisseur, alors ce site d'extrémité va échanger du trafic MSDP par défaut vers le fournisseur et sauter la vérification de RPF d'homologue.

2.4 Échange de trafic MSDP à un commutateur de diffusion groupée

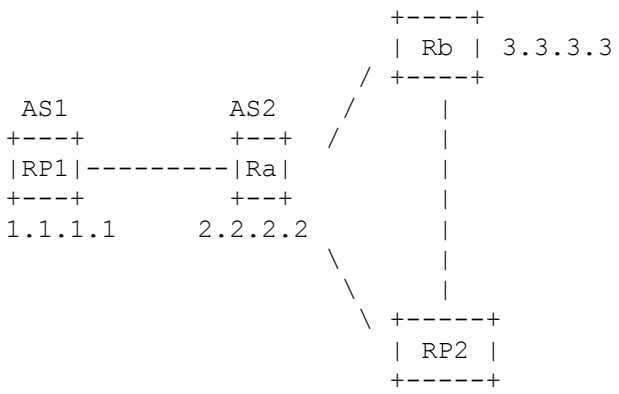
Les échanges de diffusion groupée permettent aux fournisseurs de diffusion groupée d'échanger du trafic sur un sous réseau IP commun (ou en utilisant des LAN virtuels en point à point) et de partager des mises à jour de SA MSDP. Chaque fournisseur va échanger du trafic MSDP et MBGP avec chaque autre adresse IP directement connectée. Chaque routeur d'échange va envoyer/recevoir des SA de/pour ses homologues MSDP. Ils seront alors capables de transmettre les SA à travers leur domaine à leurs clients et à tout fournisseur direct d'échange de trafic.

3. Scénarios d'échange de trafic MSDP intra domaine

Les paragraphes qui suivent décrivent les différentes possibilités d'échange de trafic MSDP intra-domaine et leurs options de déploiement.

3.1. Échange de trafic entre routeurs configurés MSDP et routeurs configurés MBGP

L'adresse IP de prochain bond de l'homologue iBGP est normalement utilisée pour la vérification d'homologue MSDP-RPF (IGP peut aussi être utilisé). Ceci est différent du cas inter-domaines BGP/MSDP, où les informations de chemin d'AS sont utilisées pour la vérification d'homologue RPF. Pour cette raison, il est nécessaire que l'adresse IP de la connexion de l'homologue MSDP soit la même que celle de la connexion interne d'homologue MBGP, que les homologues MSDP/MBGP soient ou non directement connectés. Un déploiement réussi serait similaire à ce schéma :



où RP2 MSDP et MBGP échangent du trafic avec Ra (en utilisant 2.2.2.2) et avec Rb (en utilisant 3.3.3.3). Quand la mise à

jour de SA MSDP arrive sur RP2 de Ra, la vérification de RPF MSDP pour 1.1.1.1 passe parce que RP2 reçoit la mise à jour de SA de l'homologue MSDP 2.2.2.2, qui est aussi le prochain bond MBGP correct pour 1.1.1.1.

Quand RP2 reçoit la même mise à jour de SA de l'homologue MSDP 3.3.3.3, la recherche MBGP pour 1.1.1.1 montre un prochain bond de 2.2.2.2, de sorte que RPF échoue correctement, empêchant une boucle.

Ce déploiement pourrait aussi échouer sur une mise à jour de Ra à RP2 si RP2 était un échange de trafic MBGP sur une adresse autre que 2.2.2.2 sur Ra. Les déploiements intra-domaine doivent avoir des adresses d'échange de trafic MSDP et MBGP (ou autre IGP) qui corresponent, sauf si une méthode pour sauter la vérification d'homologue RPF est utilisée.

3.2 L'homologue MSDP n'est pas un homologue BGP (ou homologue non BGP)

Ceci est un déploiement commun intra-domaine MSDP dans des environnements où peu de routeurs utilisent MBGP ou lorsque le domaine n'utilise pas MBGP. Le problème est ici que l'adresse de l'homologue MSDP doit être la même que l'adresse de l'homologue MBGP. Pour contourner cette exigence, les règles de RPF d'intra-domaine MSDP ont été relâchées dans les topologies suivantes :

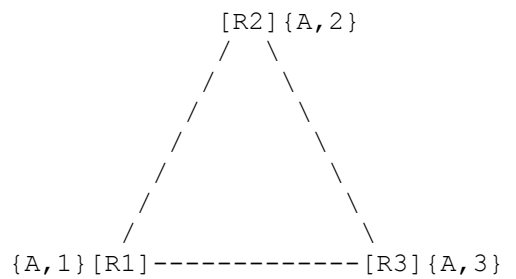
- o en configurant l'homologue MSDP comme un homologue de groupe maillé ;
- o en faisant que l'homologue MSDP soit le seul homologue MSDP ;
- o en configurant un homologue MSDP par défaut ;
- o en échangeant du trafic avec le RP générateur ;
- o en s'appuyant sur un IGP pour le RPF d'homologue.

Le choix courant autour de l'exigence d'échange de trafic intra-domaine BGP, quand plus d'un homologue MSDP est configuré, est de déployer des groupes de maillage MSDP. Quand un groupe de maillage MSDP est déployé, il n'y a pas de vérification de RPF à l'arrivée de messages SA quand ils sont reçus d'un homologue de groupe de maillage. Ensuite, les messages SA sont toujours acceptés des homologues de groupe de maillage. Les groupes de maillage MSDP ont été développés pour réduire la quantité de trafic de SA dans le réseau car les SA, qui arrivent d'un homologue de groupe de maillage, ne sont pas arrosés aux homologues au sein d'un même groupe de maillage. Les groupes de maillage doivent être pleinement maillés.

Si le code de routeur récent (mais pas encore largement déployé actuellement) qui fonctionne est pleinement conforme au dernier document MSDP, une autre option, pour contourner le fait de ne pas avoir d'homologue RPF de BGP à MSDP, esr que la RPF utilise un IGP comme OSPF, IS-IS, RIP, etc. Cette nouvelle capacité va permettre aux clients d'entreprises, qui ne fonctionnent pas avec BGP et qui ne veulent pas faire fonctionner de groupes maillés, d'utiliser leur IGP existant pour satisfaire aux règles de RPF de l'homologue MSDP.

3.3. Groupes de maillage hiérarchique

Les groupes maillés hiérarchiques sont occasionnellement déployés dans des environnements intra-domaine où il y a un grand nombre d'homologues MSDP. Permettre à plusieurs groupes maillés de transmettre à un autre groupe peut réduire le nombre d'échanges de trafic MSDP par routeur (dû à l'exigence de maillage complet) et donc réduire la charge du routeur. Une bonne mise en œuvre de groupe maillé hiérarchique (une qui empêche les boucles) contient un groupe de maillage de cœur dans le cœur de réseau, et ces routeurs de cœur servent de routeurs d'agrégation de groupe maillé :



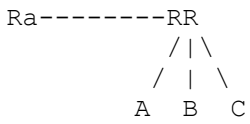
Dans cet exemple, R1, R2, et R3 sont dans le groupe maillé MSDP A (le groupe maillé de cœur) et chacun sert de routeur d'agrégation MSDP pour ses groupes maillés de "feuille" (ou second rang) 1, 2, et 3. Comme les messages SA reçus d'un homologue de groupe maillé ne sont pas transmis aux homologues au sein du même groupe maillé, les messages SA ne vont pas être en boucle. Il ne faut pas créer de topologies qui connectent des groupes maillés dans une boucle. Dans l'exemple ci-dessus, par exemple, les groupes maillés 1, 2, et 3 du second rang ne doivent pas échanger directement de

messages SA les uns avec les autres ou une boucle sans fin de SA va se produire.

La redondance entre groupes maillés va aussi causer une boucle et n'est donc pas disponible avec des groupes maillés hiérarchiques. Par exemple, supposons que R3 ait deux routeurs qui connectent son groupe feuille maillé 3 avec le groupe maillé de cœur A. Une boucle va être créée entre le groupe maillé 3 et le groupe maillé A parce que chaque groupe maillé doit être pleinement maillé entre les homologues.

3.4 MSDP et réflecteurs de chemin

BGP exige que tous les locuteurs iBGP qui ne sont pas des clients de réflecteur de chemin (RR, *router reflector*) ou des membres de confédération soient pleinement maillés pour empêcher les boucles. Dans l'environnement de RR, MSDP exige que les clients de RR échangent du trafic avec le RR car le RR est l'annonceur BGP du prochain bond vers le RP générateur. Le RR n'est pas le prochain bond BGP, mais est l'annonceur du prochain bond BGP. L'annonceur du prochain bond est l'adresse normalement utilisée pour les vérifications d'homologue MSDP-RPF. Par exemple, considérons le cas suivant :



Ra transmet des SA MSDP au réflecteur de chemin RR. Les routeurs A, B, et C échangent aussi du trafic MSDP avec RR. Quand RR transmet le SA à A, B, et C, ces RR clients vont accepter le SA parce que RR est l'annonceur de prochain bond à l'adresse de RP générateur.

Un SA va échouer sur l'homologue RPF si Ra MSDP échange directement du trafic avec les routeurs A, B, ou C parce que l'annonceur de prochain bond est RR mais que la mise à jour de SA vient de Ra. Le déploiement approprié est d'avoir les clients RR qui échangent du trafic MSDP avec le RR. Les groupes de maillage MSDP peuvent être utilisés pour contourner cette exigences. Les échanges de trafic MSDP externes vont aussi empêcher de satisfaire cette exigence car le prochain AS est comparé entre les échanges de trafic MBGP et MSDP, plutôt que l'adresse IP de l'annonceur du prochain bond.

Certaines mises en œuvre récentes de MSDP se conforment au dernier document MSDP, qui relâche l'exigence de l'échange de trafic avec l'annonceur du prochain bond (le réflecteur de chemin). Cette nouvelle règle permet l'échange de trafic avec le prochain bond, en plus de avec l'annonceur du prochain bond. Dans l'exemple ci-dessus, par exemple, si Ra est le prochain bond (peut-être à cause de l'utilisation de l'attribut d'auto prochain bond de BGP) et si les routeurs A, B, et C échangent du trafic avec Ra, le SA reçu de Ra va maintenant réussir.

3.5 MSDP et RP en envoi à la cantonnade

Un réseau avec plusieurs RP peut réaliser un partage de charge de RP et une redondance en utilisant le mécanisme de RP en envoi à la cantonnade en conjonction avec des groupes de maillage MSDP [RFC3446]. Ce mécanisme est une technique de déploiement courante utilisée au sein d'un domaine par les fournisseurs de services et les entreprises qui déploient plusieurs RP dans leur domaine. Ces RP vont avoir chacun la même adresse IP configurée sur une interface de rebouclage (en faisant une adresse d'envoi à la cantonnade). Ces RP vont échanger du trafic MSDP les uns avec les autres en utilisant une interface de rebouclage séparée et font partie du même groupe pleinement maillé MSDP. Cette interface de rebouclage, utilisée pour l'échange de trafic MSDP, va normalement être aussi utilisée pour l'échange de trafic MBGP. Tous les routeurs au sein du domaine du fournisseur vont apprendre l'adresse d'envoi à la cantonnade du RP par Auto-RP, BSR, ou une allocation statique de RP. Chaque routeur désigné dans le domaine va envoyer des "source register" et "group join" à l'adresse d'envoi à la cantonnade de RP. L'acheminement en envoi individuel va diriger ces "register" et "join" sur le plus proche RP en envoi à la cantonnade. Si un routeur de RP d'envoi à la cantonnade particulier échoue, l'acheminement en envoi individuel va diriger les "register" et "join" suivants sur le plus proche RP en envoi à la cantonnade. Ce RP va alors transmettre une mise à jour MSDP à tous les homologues au sein du groupe maillé MSDP d'envoi à la cantonnade. Chaque RP va alors transmettre (ou recevoir) les SA aux (des) consommateurs et fournisseurs externes.

4. Considérations sur la sécurité

Un service MSDP devrait être sécurisé en contrôlant explicitement l'état qui est créé par, et passé dans, le service MSDP.

Comme avec l'état d'acheminement en envoi individuel, l'état MSDP devrait être contrôlé localement, aux points de bordure de l'origine. Un filtrage sélectif aux bords du service de diffusion groupée aide à s'assurer que seules les sources voulues résultent en la création de message SA, et ce contrôle aide à réduire la probabilité de problèmes liés à l'agrégation d'état dans le cœur. Il y a divers points où la politique locale devrait être appliquée au service MSDP.

4.1 Filtrage des messages SA

Le processus de génération des messages SA devrait être filtré pour s'assurer que seules les sources locales voulues résultent en la génération de message SA. De plus, les locuteurs MSDP devraient filtrer quels messages SA sont reçus et transmis.

Normalement, il y a une grande quantité de l'état (S,G) dans un domaine PIM-SM qui est local pour le domaine. Cependant, sans un filtrage approprié, les messages SA contenant ces annonces locales (S,G) peuvent être annoncés à l'infrastructure MSDP globale. Des exemples de cela incluent des applications de domaine local qui utilisent des adresses de diffusion groupée IP globales et des sources qui utilisent des adresses de la [RFC1918]. Pour améliorer l'adaptabilité de MSDP et pour éviter une visibilité globale des informations (S,G) de domaine local, une liste de filtre externe de SA est recommandée pour prévenir la création, transmission, et mise en antémémoire inutiles de sources bien connues de domaine local.

4.2 Limites de l'état de message SA

Un filtrage approprié sur la génération, réception, et transmission des messages SA va significativement réduire la probabilité de pointes indésirables et inattendues dans l'état MSDP. Cependant, une limite d'état d'antémémoire de SA DEVRAIT être configurée comme garde-fou final contre les pointes d'état. Quand un échange de trafic MSDP a atteint un état stable (c'est-à-dire, quand l'échange de trafic a été établi et que l'état initial de SA a été transféré) il peut aussi être souhaitable de configurer un limiteur de débit pour la création de nouvelles entrées d'état de SA.

5. Remerciements

Les auteurs tiennent à remercier Pekka Savola, John Zwiebel, Swapna Yelamanchi, Greg Shepherd, et Jay Ford de leurs commentaires sur les versions antérieures de ce document.

6. Références

6.1 Références normatives

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

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2858] T. Bates et autres, "Extensions multiprotocoles pour BGP-4", juin 2000. (*Obsolète, voir* RFC4760) *(P.S.)*

[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. *(Info.)*

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

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212)

[RFC4601] B. Fenner et autres, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : spécification du

protocole (Révisée)", août 2006. (*Remplacée par* RFC7761, STD83)

6.2 Références pour information

[BSR] Fenner, W., and al., "Bootstrap Router (BSR) Mechanism for PIM Sparse Mode", Travail en cours, février 2003.

[RFCED] http://www.rfc-editor.org/policy.html

Adresse des auteurs

Mike McBride
Cisco Systems
mél : mcbride@cisco.com

John Meylor
Cisco Systems
mél : jmeylor@cisco.com

David Meyer
mél : dmm@1-4-5.net

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2006).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

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.

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