Network Working Group
Request for Comments : 3488
Categorie : Informationel

I. Wu
T. Eckert
Cisco Systems

Février 2003

Cisco Systems Router-port Group Management Protocol (RGMP)

Statut de ce Mémo

Ce mémo fournit des informations pour la communauté d'Internet. Il ne spécifie un standard Internet en aucune manière. La distribution de ce mémo n'est pas limitée.

Copyright Notice

Résumé

Ce document décrit le Protocole de Gestion de Groupe de Port de Routeur (RGMP). Ce protocole a été développé par Cisco Systems et est utilisé entre les routeurs multicast et les switches pour restreindre le forwarding de paquets en multicast dans les switches vers les routeurs qui peuvent avoir besoin de ces paquets.

RGMP est concu pour les backbone de réseaux switchés où de multiples routeurs à haute vitesse sont interconnectés.

1. Conventions utilisées dans ce document

Les mots clés ["MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL"] "DOIT", "NE DOIT PAS", "REQUIS", "DEVRAIT", "NE DEVRAIT PAS", [NDT : obligation morale, je crois, non ?], "DEVRAIT", "NE DEVRAIT PAS", [NDT : conseil] "RECOMMANDE", "PEUT" et "OPTIONNEL" dans ce document doivent etre interprétés comme décrit dans le document dans BCP 14, RFC 2119 [2].

2. Introduction

Le Snooping IGMP est un mécanisme populaire mais pas bien documenté pour restreindre le trafic multicast, dans les réseaux switchés, vers les ports qui veulent recevoir le trafic multicast. Il établit dynamiquement et termine le forwarding multicast de groupe spécifique dans les switches qui supportent cette fonctionnalité.

La principale limitation du Snooping IGMP est qu'il peut seulement

restreindre le trafic multicast dans les ports de switch où les hôtes de reception sont connectés directement ou indirectement via d'autres switches. Le Snooping IGMP ne peut pas restreindre le trafic multicast vers les ports dans lesquels au moins un routeur multicast est connecté. Ce devrait être du flood de trafic multicast vers ces ports. Le Snooping sur les messages IGMP seuls est une limitation intrinseque. A travers ceci, un switch peut seulement apprendre quels flux multicast sont requested par des hôtes. Un switch ne peut pas apprendre a travers IGMP quels flux de trafic ont besoin d'être recu par part les ports du switch pour être routés parce que les routeurs ne reportent pas ces flux via IGMP.

Dans les situations où de multiples routeurs multicast sont connectés a un backbone switché, le Snooping IGMP ne réduira pas la charge de trafic multicast. Ni aidera pour augmenter la bande passante interne à travers l'usage de switches dans le réseau.

Dans les réseaux à backbone switchés ou les points d'échange, où les routeurs prédominants sont connectés entre eux, une large somme de trafic multicast peut mener à une congestion non-attendue. Cela mène également à plus de consommation de ressources dans les routeurs parce qu'ils doivent mettre de côté le trafic multicast non-désiré.

Le protocole RGMP décrit dans ce document restreint le trafic multicast aux ports de routeur. Pour restreindre effectivement le trafic, il doit être supporté par les switches et les routeurs dans le réseau.

Le format de message RGMP ressemble au format de message IGMPv2 donc les switches exsistants, capables de Snooping IGMP, peuvent facilement être rehaussés de cette fonctionnalité. Ses messages sont encapsulés dans des datagrames IPv4, avec un numéro de protocole de 2, le même que IGMP. Tous les messages IGMP sont envoyés avec un TTL 1, vers l'adresse de destination 224.0.0.25. Cette adresse a été assignée par l'IANA pour porter les messages depuis les routeurs jusqu'aux switches [3].

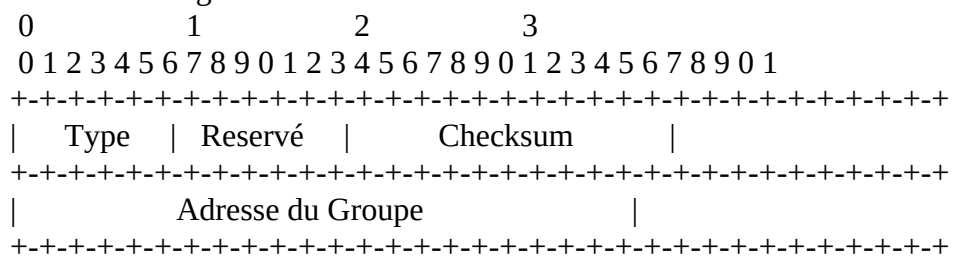
RGMP est conçu pour fonctionner en conjonction avec les protocoles de routage multicast où un joindre/tailler est effectué implicitement sur l'arbre de distribution. PIM-SM [4] est un exemple d'un tel protocole.

Le protocole RGMP spécifie les opérations seulement pour le routage multicat IPv4. IP version 6 n'est pas considéré.

Pour garder RGMP simple, efficace et facile à implémenter, il est convenu pour les switches de ne s'attendre à des messages RGMP de seulement une source par port. Pour cette raison, RGMP ne supporte qu'un seul routeur RGMP en marche d'être connecté directement à un port d'un switch RGMP en marche. Une telle topologie devrait être

habituelle quand on connecte des routeurs aux switches du backbone et ne pose donc aucune limite au développement de RGMP.

Tous les messages RGMP ont le format suivant :



Les champs réservés dans le message DOIVENT être transmis comme des zéros et ignorés a la reception.

2.1 Type

Il y a quatre types de messages RGMP concernant l'interaction routeur-switch. Les codes de types sont définis pour être les plus hautes valeurs dans un octet pour éviter la réutilisation de codes de types RGMP déjà assignés.

0xFF = Bonjour
0xFE = Au revoir
0xFD = Joindre un groupe
0xFC = Quitter un groupe

Les messages non-reconnus devraient être ignorés silencieusement.

Note :

RGMP et son assignement IANA de l'adresse 224.0.0.25 précède la RFC 3228 [9]. RGMP définit les valeurs Type qui sont assignées dans la RFC 3228 à un protocole de test et d'expérimentation. Ce n'est pas un problème opérationel pour RGMP lui-même parce que seuls les paquets RGMP utilisent l'adresse destination IPv4 224.0.0.25. Les valeurs Type définies ci-dessus ne sont par conséquent SEULEMENT valide qu'en conjonction avec l'adresse de destination RGMP.

2.2 Checksum

La checksum couvre le message RGMP (le payload IPv4 entier). L'algorithme et l'interception de la checksum sont les mêmes que ceux pour les messages IGMP comme décrits dans la RFC 3376 [5].

2.3 Adresse de Groupe

Dans un message RGMP Bonjour ou Au revoir, le champ adresse de groupe est mis à zéro.

Dans un message RGMP Joindre ou Quitter, le champ adresse de groupe garde l'adresse IPV4 multicast de groupe du groupe qui est joint ou quitté.

2.4 En-tête IPv4

Les messages RGMP sont envoyés par les routeurs aux switches. L'adresse IPv4 source d'un paquet RGMP est l'interface d'envoi adresse IPv4 du routeur originel. L'adresse IPv4 de destination d'un paquet RGMP est 224.0.0.25. Les switches supportant RGMP ont besoin d'écouter les paquets de ce groupe.

3. Description du Protocole RGMP

3.1 Description du Protocole RGMP côté routeur

Les switches du backbone utilisent RGMP pour apprendre quels groupes sont désirés à chacun de ses ports. Les routeurs multicast utilisent RGMP pour passer ces informations aux switches. Seuls les routeurs envoient des messages RGMP. Ils ignorent les messages RGMP reçus.

Un routeur activé pour RGMP sur une interface envoie périodiquement [NDT : Intervalle de Bonjour : Hello Interval] un message RGMP Bonjour au réseau attaché pour indiquer que RGMP est activé. Lorsque RGMP est desactivé sur l'interface d'un routeur, il émettra un message RGMP Au Revoir sur cette interface, indiquant qu'il veut à nouveau recevoir immoralement du trafic multicast IPv4 en provenance de cettte interface.

Lorsqu'une interface a le RGMP activé, un routeur émet un message RGMP Joindre à travers cette interface à chaque groupe dont il veut recevoir le trafic depuis l'interface. Le routeur a besoin de ré-envoyer periodiquement [Join Interval] un RGMP Joindre pour un groupe pour indiquer sont désir de continuer à recevoir le trafic multicast.

Les routeurs supportant RGMP NE DOIVENT PAS envoyer de RGMP Joindre ou Quitter pour les groupes 224.0.0.x (x=0...255), 224.0.1.39 et 224.0.1.40. Les deux derniers sont connus comme cisco-rp-announce and cisco-rp-discovery [3].

Lorsqu'un routeur n'a plus besoin de recevoir du trafic pour un groupe particulier, il envoie un message RGMP Quitter pour ce groupe. Pour la robustesse, le routeur POURRAIT [NDT : MAY] envoyer plus d'un de ces messages.

Si les paquets multicast IPv4 pour un groupe non-désiré sont recus par un routeur en provenance d'un switch, le routeur POURRAIT [NDT

:MAY] envoyer un message RGMP Quitter pour ce groupe au switch. Ces messages sont appelés messages RGMP Quitter déclenchés par des données et le routeur DEVRAIT [NDT : SHOULD] les limiter par ratio. Le routeur POURRAIT [NDT : MAY] interdire d'envoyer un message RGMP Quitter déclenché par des données si il a un groupe désiré qui a la même adresse MAC de destination que le groupe non-désiré (Voir la RFC 1112 [6] pour l'ambiguïté d'adresse MAC). Une telle interdiction de messages RGMP Quitter déclenchés par des données DEVRAIT [NDT : SHOULD] être configurable si elle est supportéee.

3.2 Description du Protocole RGMP côté switch.

Un switch activé pour le RGMP consomme des messages RGMP en provenance des ports du réseau et les traîte comme décrit ci-dessous. S'il est activé pour RGMP, le switch NE DOIT PAS forwarder/flooder les messages RGMP reçus vers les autres ports du réseau.

RGMP sur un switch opère sur une base par port, établissant un état de forwarding par groupe sur les ports où RGMP est activé. Un port revient dans un port avec RGMP activé au port du dessus par réception d'un message RGMP Bonjour sur le port, et un timer [5 * Hello Interval] débute. Ce timer est remis a zéro a chaque message RGMP Bonjour arrivant au port. Si ce timer expire ou s'il est supprimé par l'arrivée d'un message RGMP Au revoir, alors le port revient à son état premier de forwarding de trafic multicast.

Un deploiement correct de RGMP est un routeur avec RGMP activé directement connecté à un port sur un switch qui supporte RGMP. Le port sur le switch POURRAIT [MAY] vouloir garder la trace de l'adresse IPv4 de l'origine des messages RGMP Bonjour et Au revoir qu'il reçoit sur ce port. Dans l'eventualité où il reçoit plusieurs adresses IPv4 d'origine dans des messages RGMP sur un port, le switch POURRAIT [MAY] générer une alerte pour avertir l'administrateur/administratrice. Le swithch pourrait [MAY] également sauvegarder une option de configuration qui autorisera l'opérateur à désactiver RGMP est qui fera tomber le switch en arrière vers du flooding de trafic IPv4 sur ce port, bien que ceci soit une option potentiellement dangereuse.

Par défaut, connecter deux routeurs avec RGMP activé ou plus à un port de switch causera d'intermittants trous noirs de trafic multicast IPv4 du côté de ces routeurs. Les trous noirs se produisent lorsque qu'un RGMP Quitter est reçu en provenance d'un routeur alors que l'autre routeur est toujours joint.

Cette malfonction est non seulement facilement reconnue par les utilisateurs actuels connectés au travers des routeurs, mais elle adhère également au principe qu'une situation de d'erreur cause

plutot moins de trafic que plus. Renvoyer au flooding maintient plus facilement l'illusion que tout fonctionne parfaitement. L'exception est que les bénéfices de contrainte de RGMP ne sont pas réalisés. Ceci suggère que des congestions arrivent longtemps apres la mauvaise configuration et ne peuvent donc plus être facilement mises en corrélation avec la cause.

Parce que les routeurs supportant RGMP ne sont pas requis pour envoyer des messages RGMP Joindre ou Quitter pour les groupes 224.0.0.x (x=0...255), 224.0.1.39 et 224.0.1.40, les ports avec RGMP activé ont toujours besoin de recevoir du trafic pour ces groupes. Le trafic pour d'autres groupes est initialement non forwardé vers un port avec RGMP activé.

Les messages RGMP Joindre et Quitter sont acceptés s'ils arrivent sur un port avec RGMP activé, sinon ils seront mis de côté. Sur acceptation d'un message RGMP Joindre, le switch DOIT [MUST] débuter le forwarding pour le groupe vers le port. Sur acceptation d'un message RGMP Quitter, le switch DEVRAIT [SHOULD] stopper le forwarding du trafic pour le groupe vers ce port. La capacité du switch à stopper le forwarding de trafic pour un groupe peut être limitée, par exemple à cause du forwarding basé sur l'adresse MAC de destination dans le switch. Par conséquent, il est nécessaire pour un switch de toujours forwarder le trafic pour tous les groupes multicast IPv4 avec adresse MAC ambigües (voir [6] pour les ambiguïtés d'adresse MAC).

Pour stopper le forwarding de trafic pour un groupe dans l'eventualité de message(s) RGMP Quitter perdus, un switch POURRAIT [MAY] limiter en temps l'état de forwarding RGMP sur un port pour un groupe [5 * Join Interval] après que le dernier RGMP Joindre pour ce groupe ait été reçu sur le port.

Sans aucune méthode de filtrage de multicast de la couche 2 de IPv4 en fonctionnement, un switch a besoin de flooder le trafic multicast vers tous les ports. Si un switch fait tourner actuellement un ou plusieurs mecanisme auprès de RGMP pour filtrer le trafic multicast IPv4, comme le snooping IGMP [10], alors par défaut il ne floodera plus le trafic multicast IPv4 vers tous les ports. A la place, le switch tentera de déterminer quels ports ont par défaut toujours besoin de recevoir tout le trafic IPv4, et quels ports n'en n'ont pas besoin.

La compatibilité avec cette spécification requiert qu'un switch DOIT [MUST] être capable d'élire un port pour le flooding à travers la présence de messages PIM Bonjour [4] arrivant depuis le port et également à travers une option de configuration manuelle. En plus, le switch DEVRAIT [SHOULD] reconnaître un port connecté à un routeur par d'autres paquets de protocoles appropriés ou un routeur dédié aux mécanismes de découverte de multicast IPv4 comme MRDISC [11]. La

configuration manuelle est requise pour supporter les routeurs qui ne supportent pas PIM ou d'autres méthodes reconnues par le switch.

Des mécanismes plus avancés pour la restriction de trafic multicast IPv4 peuvent également être utilisés sur des ports avec RGMP activé. Dans ce cas, le forwarding pour un groupe sur le port doit être établit si l'un ou l'autre des mécanisme le requiert, et il ne doit être supprimé que si plus aucun mécanisme ne le requiert.

4. Notes opérationnelles

4.1. Support pour les réseaux à switches multiples.

Pour être simple à implémenter sur des switches et souple vis-à-vis de modifications potentielles de la topologie d'un réseau de couche 2, RGMP ne spécifie pas comment restreindre le trafic sur les liens reliants des witches les uns aux autres. Avec juste RGMP en utilisation, le trafic multicast sera donc floodé sur les liens inter-switch dans un réseau si au moins un routeur est connecté à chacun des switches.

Ceci arrive implicitement car le switch ne va pas flooder/forwarder les messages RGMP reçus vers le lien inter-switch et donc le switch de l'autre côté ne reconnaîtra le port que comme un port de routeur via les messages PIM Bonjour floodés par le switch. Une configuration manuelle pour les liens inter-switch peut être requise si des routeurs non-PIM sont utilisés, cela dépend des autres capacités du switch.

S'il est approprié, un switch peut émettre des messages RGMP sur des ports pour le faire ressembler à un routeur avec RGMP activé pour un switch potentiel de l'autre côté du lien. Ceci contraindrait le trafic multicast IPv4 entre les switches, mais ce type de "RGMP Spoofing" par le switch est en dehors de l'objectif de cette spécification.

4.2. Interopérabilité avec des routeurs non- RGMP

Comme les messages RGMP reçus à un switch n'affectent que le stade de leurs ports [ingress], la restriction de trafic ne s'applique que là. Les routeurs non-RGMP recevront le trafic multicast pour tous les groupes multicast.

4.3. RGMP et les protocoles de routage multicast

Un résultat de la simplicité de RGMP sont ses restrictions dans le support de protocoles spécifiques de routage. Les paragraphes suivants listent quelques restrictions connues.

Un routeur sur qui tourne RGMP sur un réseau switché ne recevra pas le trafic pour un groupe multicast tant qu'il ne le demandera pas explicitement par des messages RGMP Joindre (auprès des rangs de groupes spécifiés pour être floodés en 3.1). Pour cette raison, il n'est pas possible de faire tourner un protocole comme PIM Dense-Mode ou DVMRP dans un réseau contenant des routeurs avec RGMP activé.

Dans Bidir-PIM, un routeur élu pour être le DF ne doit pas être active pour RGMP sur le réseau, parce qu'il a besoin sans condition de forwarder le trafic reçu en provenance du réseau vers le RP. Si un routeur n'est pas le DF pour quelque groupe que ce soit sur le réseau, il peut être activé pour RGMP sur ce réseau.

Dans PIM-SM, des sources connectées directement au réseau ne peuvent pas être supportées si le DR élu fait tourner RGMP, parce que ce DR a besoin de recevoir sans condition le trafic en provenance de sources directement connectées pour déclencher le processus d'enregistrement PIM-SM sur le DR. Dans PIM-SM, les sources directement connectées ne peuvent être supportées par des routeurs avec RGMP activé.

Dans PIM-SM et PIM-SSM, les routeurs qui forwardent en amont le trafic à l'intérieur du réseau switché ont besoin d'envoyer des RGMP Joindre pour le groupe en support du processus d'affirmation de PIM.

5. Liste des timers et des valeurs par défaut.

5.1. Hello Interval

Le Hello Interval est l'intervalle entre les messages RGMP Bonjour envoyés par un routeur avec RGMP activé vers un switch avec RGMP activé. Par défaut : 60 secondes.

5.2 Join Interval

Le Join Interval est l'intervalle entre les messages périodiques RGMP Bonjour envoyés par un routeur avec RGMP activé vers un switch avec RGMP activé pour une adresse de groupe donnée. Par défaut : 60 secondes.

6. Considérations de sécurité

Le protocole RGMP suppose que la sécurité du port physique peut être garantie pour les ports de switch en provenance desquels les messages RGMP sont acceptés. La sécurité du port physique pour RGMP signifie que des mesures physiques assurerons que de tels ports dont spécialement connectés à un système qui agit comme un routeur

supportant RGMP. Ceci est également la configuration recommandée pour influer au mieux sur le bénéfice du protocole RGMP (i.e., éviter les tierces-parties non-voulues de trafic multicast IPv4 arrivant sur lesdits ports.)

Les attaques DoS RGMP spécifiques apparaissent en provenance des messages RGMP fogés. Si plus d'un système est connecté à un port du switch RGMP, alors un système pourrait forger des messages RGMP et affecter les opérations du/des autre(s) système(s) sur le même port. Ceci est un risque potentiel de sécurité.

Lorsque la sécurité physique assure que seul un système est connecté à un port de routeur RGMP sur un switch, alors des messages forgés en provenance de ce système lui-même peuvent être affectés. De tels messages forgés peuvent toujours être évités par des mesures systèmes locales.

Nous considérons les ramifications d'un messages forgé de chaque type :

Message Bonjour :

> Un message RGMP Bonjour forgé peut resteindre les données multicast vers un routeur sans RGMP activé sur le même port. Ceci introduit effectivement une attaque blackholing DoS [NDT : Déni de Service "trou noir"].

Message Quitter :

> Un message RGMP Quitter forgé peut restreindre le trafic IPv4 multicast pour des groupes individuels vers le port. La conséquence en est une possible attaque blackholing DoS similaire à un message RGMP Bonjour sauf que cela n'affecte pas tout le trafic IPv4 mais seulement celui des groupes indiqués dans les messages forgés. Cela n'affectera également un port que si il n'y a officiellement qu'un seul routeur avec RGMP activé qui lui est connecté (i.e., si le port a RGMP activé).

Message Au revoir :

> Un message RGMP Au revoir forgé peut diriger désactiver RGMP du port. Ceci pourrait, indirectement, causer une attaque basée sur un DoS sur le port étant surchargé avec du trafic multicast IPv4 si la bande passate du réseau était provisionnée avec l'espérance que RGMP supprimera les messages multicast IPv4 non-désirés.
>
> Ce type d'attaque DoS ré-établit simplement un comportement de port comme si RGMP n'était pas configuré et invalide le bénéfice de RGMP. Ceci, toutefois, n'introduit pas un problème qui

n'aurait pas été là sans RGMP en premier lieu.

Message Joindre

Un message RGMP Joindre forgé pourrait attirer des paquets multicast IPv4 vers le port d'où il est reçu. La conséquence est similaire à un message RGMP Au revoir sauf que cela n'affecte pas tout le trafic multicast IPv4 mais seulement les groupes indiqués dans les messages forgés. Le message affectera un port seulement si il n'y a officiellement qu'un seul routeur avec RGMP activé qui lui est connecté (i.e., si le port a RGMP activé).

7. Références de Normes

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P. and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC 2362, June 1998.

[5] Cain, B., Deering, S., Kouvelas, I., Fenner, W. and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[6] Deering, S., "Host Extensions for IP Multicasting", STD 5, RFC 1112, August 1989.

[7] ANSI/IEEE Std 802.1D 1998 Edition, "Media Access Control (MAC) Bridges", 1998.

8. Références Informatives

[3] Internet Multicast Addresses, http://www.iana.org/assignments/multicast-addresses

[8] Farinacci D., Tweedly D., Speakman T., "Cisco Group Management Protocol (CGMP)", 1996/1997 ftp://ftpeng.cisco.com/ipmulticast/specs/cgmp.txt

[9] Fenner, B., "IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)", RFC 3228, February 2002.

[10] Christensen, M. and F. Solensky, "IGMP and MLD snooping switches", Work In Progress.

[11] Biswas, S., Cain, B. and B. Haberman, "IGMP Multicast Router Discovery", Work In Progress.

9. Reconnaissances

Les auteurs aimeraient remercier Gorry Fairhurst, Bill Fenner, Giovanni Meo, Mike Norton, Pavlin Radoslavov et Alex Zinin pour leur relecture du document et leurs suggestions.

Annexe A. Droits de Propriété Intellectuelle

L'IETF a été avertie des droits de propriété intellectuelle revendiqués en regard de tout ou partie des spécifications contenues dans ce document. Pour plus d'informations consultez la liste en ligne des droits revendiqués.

Annexe B. Comparaison avec GARP/GMRP

Cette annexe ne fait pas partie de la spécification de RGMP mais est fournie pour information uniquement.

GARP/GMRP (défini dans IEEE.1D [7]) est la suite de protocoles ANSI/ISO/IEC/IEEE pour contraindre le trafic ethernet multicast dans les réseaux ethernet bridgés. Comme tel il est donc une alternative possible à RGMP dans la tâche de contraindre le trafic multicast vers les ports de routeur. Cette annexe expliquera la motivation de ne pas se fier à GARP/GMRP, et en quoi GARP/GMRP et GRMP diffèrent.

Le facteur-clé en mettant en place GARP/GMRP aurait été de remplacer complètement le Snooping IGMP. Ceci était le but de la conception de GARP/GRMP. Pour des opérations efficaces, le Snooping IGMP requiert le support du filtrage matériel dans le switch (pour différentier les rapports d'appartenance des hôtes et le trafic multicast IPv4 actuel). Spécialement dans certains routeurs anciens, ce support n'existe pas. Les contructeurs ont essayé de trouver un moyen de dépasser ce problème pour fournir le bénéfice de contraindre le trafic multicast IPv4 dans un LAN switché sans avoir à construire des switches plus onéreux. GARP/RGMP est un protocole résulant de ceci. CGMP de chez Cisco en est un autre. Alors que CGMP résoud le problème sans requérir de changement sur la pile software de l'hôte, GARP/GMRP requiert son support par la pile de l'hôte.

A ce jour GARP/GMRP n'a pas fait d'avancées significatives dans les solutions déployées. Le Snooping IGMP (et CGMP) sont la norme pour cet environnement. Par conséquent, GARP/GMRP n'est pas nécessairement supporté par les switches de Niveau 2. De plus, GARP/GMRP n'adresse pas clairement les problèmes aue RGMP tente de résoudre. D'un côté, GARP/GMRP fournit beaucoup plus de fonctionnalités et autant de complexité que requis dans l'immédiat. D'un autre côté, GARP/GMRP est limité en étant un standart prédominant du point de vue Ethernet.

Au-delà des raisons de processus et d'applicabilité, les pricipales différances entre GARP/GMRP et RGMP sont les suivantes :

- Les switches/systèmes GARP/GMRP ont besoin d'envoyer et d'écouter/réagir aux messages GARP/GMRP. Dans RGMP, les routeurs ont seulement besoin d'envoyer des messages RGMP et les swichtes ont seulement besoin de les écouter. L'approche de ce protocole mène à une simplification de l'implémentation, des opérations et du dépannage.

- Les mêmes switchs avec RGMP dans un réseau backbone verront probablement plus d'états en marchant sur le fil du rasoir en faisant du Snooping IGMP, le rendant préférable pour garder le compte de traitement par groupe et des besoins en mémoire dans RGMP en plsu de bonds qu'il n'est possible avec le Snooping IGMP et GARP/GMRP : dans GARP/GMRP, un timer (multiple) basé sur l'état-machine a besoin d'être maintenu sur une adresse ethernet par groupe, en RGMP la maintenace du timer est complètement optionnelle et il n'y a que deux états par groupe (Joint ou non-Joint).

- GARP/GMRP est un protocole niveau ethernet de la IEEE. Il supporte de contraindre le trafic pour les adresses (groupes) ethernet. RGMP contraint le trafic pour les groupes multicast IPv4. Aujourd(hui ceci est au-delà même des capacités des plates-formes switch typiques utilisées comme switches de Niveau 2. Des extensions pour supporter des entités plus avancées sont probablement plus faciles à venir au travers d'extensions pour RGMP que pour GARP/GMRP.

- RGMP partage le format de paquet basique avec IGMP (version 2) et est comme tel facile à ajouter aux plates-formes de routeurs et de switches qui supportent dejà IGMP et le Snooping IGMP, respectivement. Ceci est spécialement vraie pour les switches qui peuvent en hardware différentier les paquets du type du protocole IGMP et le reste du trafic multicast IPv4 envoyé au même groupe (ou à une adresse MAC ambigüe). De plus, à cause de la simplicité d'état de RGMP il est simple d'intégrer le Snooping IGMP et les opérations RGMP dans le le contrôle

multicast IPv4 et dans le plan de forwarding d'un switch.

- GARP/GMRP supporte plus d'un système (hôte/routeur) sur un port de switch, ce qui est une raison de sa complexité. Dans RGMP, cette configuration esq explicitement non-supportée : plus d'un routeur par port switché est non seulement un scénario commun dans les réseaux à switches de Niveau 2 d'aujourd'hui, mais c'est également une configuration indésirable lorsque le trafic multicast IPv4 est à tenir éloigné des routeurs.

- GARP/GMRP définit comment contraindre le trafic multicast entre les switches, autre raison de sa complexité. RGMP ne le supporte pas explicitement comme faisant partie du protocole pour les raisons suivantes :

  - Il n'est pas nécessaire s'inclure cette fonction comme part de la description du protocole RGMP car les implémentations de switch peuvent décider de supporter cette fonction (voir 4.1 à propos de ceci "RGMP Spofing").

  - D'importants déploiements au travers desquels de grandes sommes de trafic multicast IPv4 sont déplacées de nos jours sont typiquement les switches uniques MIX - Multicast Internet eXchange points.

  - Eviter les congestion sur les liens inter-switch est, en général, plus complexe que simplement contraidre le trafic multicast IPv4 vers les chemins où il en est besoin. Avec ou sans multicast IPv4, la bande passante globale dont on a besoin entre les switches peut facilement être la bande passante globale requise pour les routeurs d'un autre côté. Pour cette raison, la bande passante inter-switch est le plus souvent sur-provisoinnée de façon appropriée. De plus, la probabilité pour les routeurs à la réception de n'être que du côté des sources d'un lien inter-switch est en général plutôt faible. Les cas où la contrainte du trafic sur les liens inter-switch est requis et utile est donc limité et peut être évité ou dévié. Changer le réseau vers un réseau routé de Niveau 3 est souvent la meilleure soluttion, supporter le Spoofing RGMP (voir section 4.1) en est une autre.

Annexe C. Possibles extensions futures / comparaison au Snooping PIM

Cette annexe ne fait pas partie de la spécification de RGMP mais est fournie pour information uniquement.

Cette annexe présente une discussion des extensions possibles à RGMP. Sont inclus les points sur pourquoi les extensions ne sont

pas inclues et, de plus, une motivation pour RGMP en comparaison avec le snooping (PIM).

- Support de multiples switches

  Comme discuté dans "Spoofing RGMP", chapitre 4.1 et la comparaison avec GARP/GMRP dans l'Annexe B.

- Support de SSM

  Alors que RGMP fonctionne avec PIM-SSM, il n'a pas de messages explicites pour que le routeur se joigne selectivement aux canaux (S, G) individuellement. A la place le routeur doit RGMP-Joindre à tout les canaux (Si, G) en se joignant à G. Etendre RGMP pour inclure les Joindre/Quitter (S, G) est faisable. De toute façon, aujourd'hui la majorité des switches ne supporte pas la contrainte de trafic par canal. De plus, la probabilité pour la collision de canal actuel (deux canaux SSM utilisant le même groupe) ne deviendra un problème que lorsque SSM sera pleinement déployé.

- Support de IPv6

  RGMP pourrait être facilement étendu pour supporter IPv6 en mappant le format de paquet dans le format de paquet MLD/IPv6. Ceci n'a pas été fait pour cette spécification parce que la plupart des switches d'aujourd'hui ne supportent toujours pas le snooping MLD.

- Support de plusieurs routeurs par port.

  Comme il décrit dans l'annexe B. Ceci est probablement une extension qui devrait être évitée. Plusieurs routeurs par port sont inappropriés pour une contrainte efficace du trafic multicast.

- Support de protocoles / élements de protocoles non basés sur des messages Joindre.

  Pour les protocoles comme PIM dense-mode, DVMRP ou les routeurs DF Bidir-PIM, des messages RGMP additionnels pourraient être ajoutés pour permettre aux routeurs d'indiquer que le trafic de certains groupes (rangs) a besoin d'être floodé de leur provenance (dense-mode) ou à leur destination (Bidir-PIM).

- Support du switching à plusieurs politiques.

  Dans les environnement de Points d'Echange Multicast (MIXes) il existe des situations où différants routeurs en aval ont besoin pour des raisons de politique de recevoir le même flux de

différants routeurs en amont.

Ce problème pourrait être résolu en fournissant actuellement un champ voisinage amont dans les messages Joindre/Quitter. Le switch RGMP forwarderait ensuite le trafic en provenance d'un routeur amont seulement à ces routeurs en aval qui veulent avoir le trafic de ce routeur amont précis. Cette extension irait pour le mieux de concert avec des changements au protocole de routage de Niveau 3 fonctionnant entre les routeurs.

Comme mentioné précedemment, RGMP fut conçu pour être simple à implémenter et pour supporter les simples switches de Niveau 2. Les implémentations pourraient également être appliquées aux switches au-delà du Niveau 2. Si toutes les possibles extensions futures ci-dessus devaient être supportées par une évolution de RGMP, on pourrait se demander si un tel protocole pourrait être de toute façon moins complexe que l'actuel snooping dans le protocole de routage IPV4 de Niveau 3 fonctionnant entre les routeurs dans un LAN switché.

Du point de vue architecture du protocole il est certainement plus approprié d'avoir un protocole séparé comme RGMP ou GARP/GMRP pour cette tâche. Là encore, plus complexes sont les besoins, plus la duplication de l'effort est compliquée et le snooping sems devenir une option plus attractive.

Même s'il existe un protocole de routage dominant, PIM, dans le multicast IPv4, router avec PIM lui-même est extrêmement complexe pour un switch pour snooper dedans. PIM possède deux versions principales, des modes différants - sparse, dense, Bidir, SSM, des messages join / prune /graft (dépendant du mode du groupe), des options PIM Hello variées, différantes versions d'affirmation, deux protocoles d'annonce de mode dynamiques (BSR, AutoRP), et enfin il supporte IPv4 et IPV6.

Un switch snoopant dans PIM est très probable pour n'implémenter qu'une sous-partie de l'ensemble de ses fonctionnalités, rendant très difficile à l'utilisateur de déterminer le niveau de contrainte de trafic appliqué tant qu'il n'existe pas une spécification claire pour l'implémentation (ou mieux la méthode par se.). De plus, il y a toujours le danger qu'une telle implémentation de snooping puisse casser de nouvelles fonctionnalités du protocole de routage qu'il n'était pas conçu pour intercepter (probablement parce qu'elles n'avaient pas pu être prévues). Par exemple, ceci peut arriver avec les switches utilisant des implémentations de snooping IGMP (v2) qui sont soumises aux messages IGMP version 3 - elles cassent IGMPv3.

En somme, avec PIM toujours en évolution, l'approche prise par RGMP est la plus sûre pour les problèmes immédiats à portée de main, et les extensions comme celles listées devraient être considérées à

temps pour la demande actuelle. Le snooping (PIM) est une alternative valide une fois que la somme totale des fonctionnalité qui ont besoin d'être supportées en font une solution également attractive (en respectant la complexité) à un protocole dedié et si ses fonctions sont bien définies pour permettre de prévoir ses effets - mais toujours au prix de possibles incompatibilités avec les extensions à venir du protocole PIM tant que le support pour les switches de Niveau 2 est explicitement considéré en poussant vers l'avant les protocoles PIM.

Adresses des Auteurs

Ishan Wu
cisco Systems
170 West Tasman Drive
San Jose, CA 95134

Phone: (408) 526-5673
EMail: iwu@cisco.com

Toerless Eckert
cisco Systems
170 West Tasman Drive
San Jose, CA 95134

Phone: (408) 853-5856
Email: eckert@cisco.com

Traduction :
[DegenereScience]DecereBrain, le Lundi 4 Juillet 2003, 04:53.
Ce document est une traduction non-officielle de la RFC 2088.
L'auteur de cette traduction décline toute responsabilité sur l'utilisation de ce document et/ou sur d'éventuelles erreurs de traduction.

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.