Groupe de travail Réseau
Request for Comments : 4286
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

B. Haberman, JHU APL
J. Martin, Netzwert AG

décembre 2005

Découverte de routeur de diffusion groupée

Statut de ce mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le concept d'inspection du protocole de gestion de groupe Internet (IGMP, *Internet Group Management Protocol*) et du protocole de découverte d'écoutant de diffusion groupée (MLD, *Multicast Listener Discovery*) exige la capacité d'identifier la localisation des routeurs de diffusion groupée. Comme l'inspection n'est pas normalisée, il y a de nombreux mécanismes qui sont utilisés pour identifier les routeurs de diffusion groupée. Cependant, cela peut conduire à des problèmes d'interopérabilité entre les routeurs de diffusion groupée et les commutateurs d'inspection provenant de fabricants différents.

Le présent document introduit un mécanisme général qui permet la découverte des routeurs de diffusion groupée. Ce nouveau mécanisme, découverte de routeur de diffusion groupée (MRD, *Multicast Router Discovery*), introduit un moyen normalisé d'identifier les routeurs de diffusion groupée sans dépendance à un protocole d'acheminement de diffusion groupée particulier.

Table des matières

1. Introduction

Les messages de découverte de routeur de diffusion groupée (MRD, *Multicast Router Discovery*) sont utiles pour déterminer quels nœuds rattachés à un commutateur ont activé l'acheminement de diffusion groupée. Cette capacité est utile dans un domaine de pontage de couche 2 avec des commutateurs d'inspection. En utilisant les messages MRD, les commutateurs de couche 2 peuvent déterminer où envoyer les données de source de diffusion groupée et les messages d'adhésion à un groupe [RFC1112], [RFC3376]. Les données de source de diffusion groupée et les rapports d'adhésion de groupe doivent être reçus par tous les routeurs de diffusion groupée sur un segment. Utiliser les messages Interrogation du protocole d'adhésion de groupe pour découvrir les routeurs de diffusion groupée est insuffisant du fait de la suppression de l'interrogation.

Bien que les messages MRD pourraient être envoyés comme messages ICMP, les protocoles de gestion de groupe ont été choisis car cette fonctionnalité est spécifique de la diffusion groupée. L'ajout de cette fonctionnalité au protocole d'adhésion de groupe permet aussi aux opérateurs d'avoir une congruence entre les problèmes de MRD et les questions de transmission des données.

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. Vue d'ensemble du protocole

La découverte de routeur de diffusion groupée consiste en trois messages pour découvrir les routeurs de diffusion groupée. L'annonce de routeur de diffusion groupée est envoyée par les routeurs pour annoncer que la transmission de diffusion groupée IP est activée. Les appareils peuvent envoyer des messages Sollicitation de routeur de diffusion groupée afin de solliciter des messages Annonce de la part des routeurs de diffusion groupée. Les messages Terminaison de routeur de diffusion groupée sont envoyés quand un routeur arrête les fonctions d'acheminement de diffusion groupée IP sur une interface.

Les routeurs de diffusion groupée envoient périodiquement des annonces non sollicitées sur toutes les interfaces sur lesquelles la transmission de diffusion groupée est activée. Les messages Annonce sont aussi envoyés en réponse aux Sollicitations. En plus d'annoncer la localisation des routeurs de diffusion groupée, les annonces portent aussi des informations utiles concernant les variables de protocole de gestion de groupe. Ces informations peuvent être utilisées pour des vérifications de cohérence sur le sous réseau.

Un appareil envoie des messages Sollicitation chaque fois qu'il souhaite découvrir des routeurs de diffusion groupée sur une liaison directement rattachée.

Un routeur envoie des messages Terminaison quand il termine la fonction d'acheminement de diffusion groupée sur une interface.

Tous les messages MRD sont envoyés avec une durée de vie (TTL, *Time to Live*) IPv4 ou une limite de bonds IPv6 de 1 et contiennent l'option d'alerte de routeur [RFC2113], [RFC2711]. Tous les messages MRD DEVRAIENT être limités en débit conformément à la variable MaxMessageRate *(taux maximum de message)*.

Les messages Annonce et Terminaison sont envoyés à l'adresse de diffusion groupée "All-Snoopers" *(tous les inspecteurs)*.

Les messages Sollicitation sont envoyés à l'adresse de diffusion groupée "All-Routers" *(tous les routeurs)*.

Toutes les données au delà du format de message fixé DOIVENT être ignorées.

3. Annonce de routeur de diffusion groupée

Les annonces de routeur de diffusion groupée sont envoyées périodiquement sans sollicitation sur toutes les interfaces de routeur sur lesquelles la transmission de diffusion groupée est activée. Elles sont aussi envoyées en réponse aux messages de sollicitation de routeur de diffusion groupée.

Les annonces sont envoyées :
1. à l'expiration d'un temporisateur périodique (modulo une valeur aléatoire)
2. au titre de la procédure de démarrage d'un routeur,
3. durant le redémarrage d'une interface de transmission de diffusion groupée,
4. à réception d'un message Sollicitation.

Toutes les annonces sont envoyées comme des messages du protocole de gestion de groupe Internet (pour IPv4) ou de découverte d'écoutant de diffusion groupée (pour IPv6) à l'adresse de diffusion groupée "All-Snoopers". Ces messages DEVRAIENT être limités en débit conformément à la variable MaxMessageRate.

3.1 Variables de configuration d'annonce

Une mise en œuvre de MRD DOIT prendre en charge la configuration des variables suivantes par la gestion du système. Les valeurs par défaut sont spécifiées pour rendre inutile la configuration de toutes ces variables dans de nombreux cas.

3.1.1 **AdvertisementInterval** (intervalle d'annonce)

Cette variable est l'intervalle de base (en secondes entières) entre la transmissions des annonces non sollicitées sur une interface. Cette valeur DOIT être de pas moins de 4 secondes et pas plus de 180 secondes. Par défaut : 20 secondes.

3.1.2 **AdvertisementJitter** (gigue d'annonce)

C'est la durée maximale (en secondes) pendant laquelle l'intervalle d'annonce est perturbé pour chaque annonce non sollicitée. Noter que l'objet de cette gigue est d'éviter la synchronisation de plusieurs routeurs sur un réseau, donc le choix d'une valeur de zéro est déconseillée. Cette valeur DOIT être un entier de pas moins de 0 seconde et pas plus de AdvertisementInterval. AdvertisementJitter DOIT être de 0,025*AdvertisementInterval.

3.1.3 **MaxInitialAdvertisementInterval** ***(intervalle maximum d'annonce)***

La première annonce non sollicitée transmise sur une interface est envoyée après l'attente d'un intervalle aléatoire (en secondes) de moins que cette variable. Cela empêche une inondation d'annonces lorsque plusieurs routeurs démarrent au même moment. Par défaut : 2 secondes.

3.1.4 **MaxInitialAdvertisements**

Cette variable est le nombre maximum d'annonces non sollicitées qui vont être transmises par l'interface d'annonces quand MRD démarre. Par défaut : 3.

3.1.5 **NeighborDeadInterval**

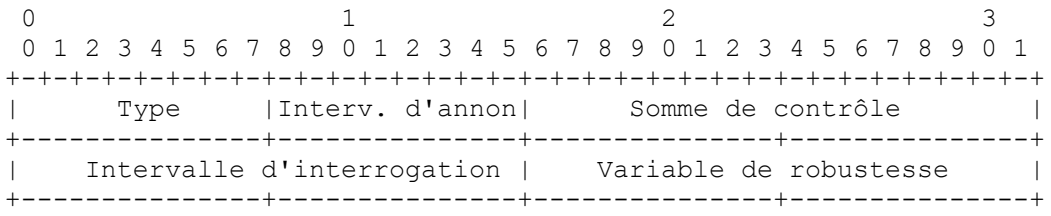
La variable NeighborDeadInterval *(intervalle de voisin mort)* est la durée maximale (en secondes) permise (après la réception de la dernière annonce valide) avant qu'un routeur voisin soit déclaré inaccessible. Cette variable est tenue par voisin. Un receveur MRD devrait régler NeighborDeadInterval à 3 fois la somme du champ Intervalle d'annonce reçu plus le AdvertisementJitter calculé à partir du champ Intervalle d'annonce reçu. Cela assure un comportement cohérent entre les divers appareils d'un réseau. Par défaut : 3 * (champ Intervalle d'annonce + AdvertisementJitter calculé).

3.1.6 **MaxMessageRate**

La variable MaxMessageRate *(taux maximum de message)* est le nombre maximum agrégé de messages qu'une mise en œuvre de MRD DEVRAIT envoyer (par seconde) par interface ou par destination de gestion ou d'enregistrement. Par défaut : 10.

3.2 Format du paquet d'annonce

Le message d'annonce a le format suivant :



3.2.1 Champ Type

Le champ Type identifie le message comme annonce. Il est réglé à 0x30 pour IPv4 et à 151 pour IPv6.

3.2.2 Champ Intervalle d'annonce

Ce champ spécifie l'intervalle périodique auquel les messages d'annonce non sollicités sont transmis, en unités de secondes. Cette valeur est réglée à l'intervalle d'annonce configuré.

3.2.3 Champ Somme de contrôle

Le champ Somme de contrôle est réglé comme suit :

1. Pour IPv4 c'est le complément à un sur 16 bits de la somme des compléments à un du message IGMP, commençant par le champ Type. Pour calculer la somme de contrôle, le champ Somme de contrôle est réglé à 0.
2. Pour IPv6, c'est la somme de contrôle ICMPv6 comme spécifié dans la [RFC2463].

3.2.4 Champ Intervalle d'interrogation

Le champ Intervalle d'interrogation est réglé à la valeur d'intervalle d'interrogation (en secondes) utilisé par IGMP ou MLD sur l'interface. Si IGMP ou MLD n'est pas activé sur l'interface annonceuse, ce champ DOIT être à 0. Noter qu'il s'agit de l'intervalle d'interrogation de l'interrogateur (QQI, *Querier's Query Interval*) et non du code d'intervalle d'interrogation de l'interrogateur (QQIC, *Querier's Query Interval Code*) comme spécifié dans IGMP/MLD.

3.2.5 Champ Variable de robustesse

Ce champ est réglé à la variable de robustesse utilisée par IGMPv2 [RFC2236], IGMPv3 [RFC3376], ou MLD [RFC2710], [RFC3810] sur l'interface annonceuse. Si IGMPv1 est utilisé ou si aucune protocole de gestion de groupe n'est activé sur l'interface, ce champ DOIT être réglé à 0.

3.3 Champs d'en-tête IP

3.3.1 Adresse de source

L'adresse IP de source est réglée à une adresse IP configurée sur l'interface annonceuse. Pour IPv6, une adresse de liaison locale DOIT être utilisée.

3.3.2 Adresse de destination

L'adresse IP de destination est réglée à l'adresse de diffusion groupée "All-Snoopers".

3.3.3 Durée de vie / Limite de bonds

La TTL IPv4 et la limite de bonds IPv6 sont réglés à 1.

3.3.4 Protocole IPv4

Le champ Protocole IPv4 est réglé à IGMP (2).

3.3.5 Prochain en-tête IPv6

L'en-tête ICMPv6 est identifié par une valeur de Prochain en-tête de 58 dans l'en-tête immédiatement précédant [RFC2463].

3.4 Envoi des annonces de routeur de diffusion groupée

Les messages d'annonce sont envoyés quand les événements suivants se produisent :

1. Expiration du temporisateur d'intervalle périodique d'annonce. Noter que ce temporisateur n'est pas strictement périodique car l'intervalle d'annonce de base varie à chaque intervalle d'une valeur aléatoire de plus ou moins AdvertisementJitter secondes.

2. Après un délai aléatoire de moins de MaxInitialAdvertisementInterval quand une interface est activée pour la première fois, est (ré-)initialisée, ou quand MRD est activé. Un routeur peut envoyer jusqu'à un maximum de MaxInitialAdvertisements annonces, attendant pendant un délai aléatoire de moins de MaxInitialAdvertisementInterval entre chaque message. Plusieurs annonces sont envoyées pour la robustesse à la perte de paquet sur le réseau.

C'est pour empêcher une explosion d'annonces. Un exemple de cela serait quand de nombreux routeurs sont mis sous tension en même temps. Quand une sollicitation est reçue, une annonce est envoyée en réponse avec un délai aléatoire de moins de MAX_RESPONSE_DELAY. Si une sollicitation est reçue pendant qu'une annonce est en cours, cette sollicitation DOIT être ignorée.

Des changements de l'intervalle d'interrogation ou de la variable de robustesse NE DOIVENT PAS déclencher une nouvelle annonce ; cependant, les nouvelles valeurs DOIVENT être utilisées dans tous les futurs messages d'annonce.

Quand une annonce est envoyée, le temporisateur d'intervalle d'annonce périodique DOIT être remis à zéro.

3.5 Réception des annonces de routeur de diffusion groupée

À réception d'un message d'annonce, les appareils valident le message selon les critères suivants :
1. La somme de contrôle est correcte,
2. L'adresse IP de destination est égale à l'adresse de diffusion groupée "All-Snoopers",
3. Pour IPv6, l'adresse IP de source est une adresse de liaison locale.

Une annonce qui ne satisfait pas à ces exigences de validité DOIT être éliminée en silence et peut être enregistrée selon des modalités limitées en débit conformément à la variable MaxMessageRate.

Si une annonce n'est pas reçue pour un certain voisin dans l'intervalle de temps NeighborDeadInterval, le voisin est alors considéré comme injoignable.

4. Sollicitation de routeur de diffusion groupée

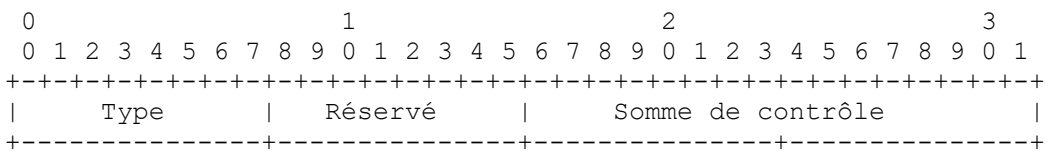
Les messages de sollicitation de routeur de diffusion groupée sont utilisés pour solliciter des annonces de la part des routeurs de diffusion groupée sur un segment. Ces messages sont utilisés quand un appareil souhaite découvrir des routeurs de diffusion groupée. À réception d'une sollicitation sur une interface à capacité de transmission de diffusion groupée IP et à MRD activée, un routeur va répondre par une annonce.

Les sollicitations peuvent être envoyées en présence des événements suivants :
1. Une interface est (ré)initialisée,
2. MRD est activé.

Les sollicitations sont envoyées à l'adresse de diffusion groupée "All-Routers" et DEVRAIENT être limitées en débit, selon la variable MaxMessageRate.

4.1 Format du paquet Sollicitation

Le message Sollicitation a le format suivant :



4.1.1 Champ Type

Le champ Type identifie le message comme une sollicitation. Il est réglé à 0x31 pour IPv4 et à 152 pour IPv6.

4.1.2 Champ Réservé

Le champ Réservé est réglé à 0 à l'émission et ignoré à réception.

4.1.3 Champ Somme de contrôle

Le champ Somme de contrôle est réglé comme suit :

- Pour IPv4 c'est le complément à un de 16 bits de la somme des complément à un du message IGMP, commençant par le champ Type. Pour calculer la somme de contrôle, le champ Somme de contrôle est réglé à 0.
- Pour IPv6, c'est la somme de contrôle ICMPv6 comme spécifiée dans la [RFC2463].

4.2 Champs d'en-tête IP

4.2.1 Adresse de source

L'adresse IP de source est réglée à l'adresse IP configurée sur l'interface qui sollicite. Pour IPv6, une adresse de liaison locale DOIT être utilisée.

4.2.2 Adresse de destination

L'adresse de destination IP est réglé à l'adresse de diffusion groupée "All-Routers".

4.2.3 Durée de vie / Limite de bonds

La TTL IPv4 et la limite de bond IPv6 sont réglées à 1.

4.2.4 Protocole IPv4

Le champ Protocole IPv4 est réglé à IGMP (2).

4.2.5 Prochain en-tête IPv6

L'en-tête ICMPv6 est identifié par une valeur de prochain en-tête de 58 dans l'en-tête précédant immédiatement [RFC2463].

4.3 Envoi des sollicitations de routeur de diffusion groupée

Les messages Sollicitation sont envoyés lorsque surviennent les événements suivants :

- Après l'attente d'un délai aléatoire de moins de MAX_SOLICITATION_DELAY quand une interface devient opérationnelle pour la première fois, est (ré)initialisée, ou que MRD est activé. Un appareil peut envoyer jusqu'à un maximum de MAX_SOLICITATIONS, attendant pendant un délai aléatoire de moins de MAX_SOLICITATION_DELAY entre chaque sollicitation.
- Facultativement, pour un événement spécifique de la mise en œuvre.

Les sollicitations DOIVENT être limitées en débit selon la variable MaxMessageRate ; la mise en œuvre DOIT n'envoyer pas plus de MAX_SOLICITATIONS en MAX_SOLICITATION_DELAY secondes.

4.4. Réception des sollicitations de routeur de diffusion groupée

Un message Sollicitation DOIT être validé avant l'envoi d'une réponse. Un routeur DOIT vérifier :
- o que la somme de contrôle est correcte,
- o que l'adresse de destination IP est l'adresse de diffusion groupée "All-Routers",
- o Pour IPv6, que l'adresse IP de source DOIT être une adresse de liaison locale.

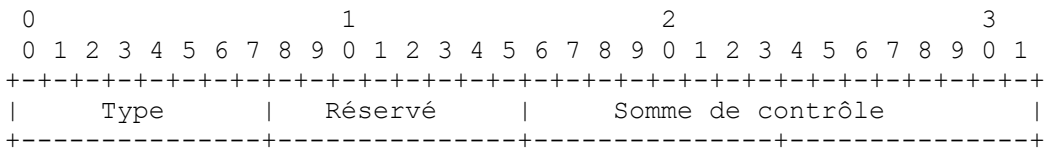
Les sollicitations qui ne satisfont pas aux exigences de validité DEVRAIENT être éliminées en silence et peuvent être enregistrées dans un journal de manière limitée en débit selon la variable MaxMessageRate.

5. Terminaison de routeur de diffusion groupée

Le message Terminaison de routeur de diffusion groupée est utilisé pour dépêcher la notification d'un changement de l'état des fonctions de transmission de diffusion groupée d'un routeur. Les routeurs de diffusion groupée envoient le message Terminaison quand la transmission de diffusion groupée est désactivée sur l'interface annonceuse.

5.1 Format du paquet Terminaison

Le message Terminaison a le format suivant :



5.1.1 Champ Type

Le champ Type identifie le message comme Terminaison. Il est réglé à 0x32 pour IPv4 et à 153 pour IPv6.

5.1.2 Champ Réservé

Le champ Réservé est réglé à 0 à l'émission et ignoré à réception.

5.1.3 Champ Somme de contrôle

Le champ Somme de contrôle est réglé comme suit :
- o Pour IPv4, c'est le complément à un de 16 bits de la somme des compléments à un du message IGMP, en commençant par le champ Type. Pour calculer la somme de contrôle, le champ Somme de contrôle est mis à 0.
- o Pour IPv6, c'est la somme de contrôle ICMPv6 comme spécifiée dans la [RFC2463].

5.2 Champs d'en-tête IP

5.2.1 Adresse de source

L'adresse IP de source est réglé à une adresse IP configurée sur l'interface annonceuse. Pour IPv6, une adresse de liaison locale DOIT être utilisée.

5.2.2 Adresse de destination

L'adresse IP de destination est réglée à l'adresse de diffusion groupée "All-Snoopers".

5.2.3 Durée de vie / Limite de bonds

La TTL IPv4 et la limite de bonds IPv6 sont réglées à 1.

5.2.4 Protocole IPv4

Le champ Protocole IP est réglé à IGMP (2).

5.2.5 Prochain en-tête IPv6

L'en-tête ICMPv6 est identifié par une valeur de Prochain en-tête de 58 dans l'en-tête précédent immédiat [RFC2463].

5.3 Envoi de Terminaison de routeur de diffusion groupée

Les messages Terminaison sont envoyés par les routeurs de diffusion groupée quand :
- o la transmission de la diffusion groupées est désactivée sur une interface,
- o une interface est désactivée administrativement,
- o le routeur est fermé en douceur,
- o MRD est désactivé.

L'envoi des messages Terminaison DEVRAIT être limité en débit conformément à la variable MaxMessageRate.

5.4 Réception de Terminaison de routeur de diffusion groupée

À réception d'un message Terminaison, les appareils valident le message. Les critères de validation sont les suivants :
- o la somme de contrôle DOIT être correcte,
- o l'adresse de destination IP DOIT être égale à l'adresse de diffusion groupée "All-Snoopers",
- o pour IPv6, l'adresse IP de source DOIT être une adresse de liaison locale.

Les messages de terminaison qui ne satisfont pas aux exigences de validité DOIVENT être éliminés en silence et peuvent être enregistrés dans un journal de façon limitée en débit conformément à la variable MaxMessageRate.

Si le message réussit à ces étapes de validation, une sollicitation est envoyée. Si une annonce n'est pas reçue dans l'intervalle de voisin mort *(NeighborDeadInterval)* le routeur envoyeur est retiré de la liste des routeurs de diffusion groupée actifs.

6. Constantes du protocole

La liste suivante identifie les constantes utilisées dans le protocole MRD. Ces constantes sont utilisées au calcul des paramètres.
- o MAX_RESPONSE_DELAY : 2 secondes
- o MAX_SOLICITATION_DELAY : 1 seconde
- o MAX_SOLICITATIONS : 3 transmissions

7. Considérations sur la sécurité

Comme la MRD est un protocole de liaison locale, il n'y a pas de circonstances dans lesquelles il serait correct qu'un receveur MRD reçoive du trafic MRD d'une source extérieure à son réseau. Pour IPv6, les messages MRD DOIVENT avoir une adresse valide de liaison locale. Tout message reçu sans une adresse de source valide de liaison locale DOIT être éliminé. De même, pour IPv4, le receveur MRD DOIT déterminer si l'adresse de source est locale pour l'interface receveuse, et DOIT éliminer tout message qui a une source non locale. Déterminer quel réseau est local peut se faire par des informations de configuration ou par des capacités opérationnelles.

Des nœuds félons peuvent tenter d'attaquer un réseau fonctionnant avec MRD en envoyant des messages Annonce, Sollicitation, ou Terminaison falsifiés. Chaque type de message falsifié peut être traité en utilisant la technologie existante.

Un nœud félon peut tenter d'interrompre le service de diffusion groupée en envoyant des messages Terminaison falsifiés. Comme décrit au paragraphe 5.4, tous les messages Terminaison sont validés par l'envoi d'un message Sollicitation. Par l'envoi d'une Sollicitation, le nœud force la transmission d'une Annonce par un routeur actif.

Les messages Sollicitation falsifiés ne causent aucun dommage opérationnel. Ils peuvent être utilisés comme mécanisme d'attaque d'inondation contre un routeur de diffusion groupée. Cette attaque peut être atténuée par la recommandation de limitation de débit de tous les messages MRD.

Le message Annonce de routeur de diffusion groupée peut permettre à des machines félonnes de se faire passer pour des routeurs de diffusion groupée. Cela pourrait permettre à ces machines d'espionner les transmissions de données de diffusion groupée. De plus, cela pourrait constituer une attaque de déni de service contre les autres hôtes du même domaine d'inspection ou qui partagent le même accès d'appareil en présence de flux de diffusion groupée à haut débit.

La technologie disponible dans SEND [RFC3971] peut être utilisée pour régler le problème de la falsification des messages d'annonce dans les réseaux IPv6. Les routeurs de diffusion groupée dans un réseau à capacité MRD peuvent utiliser des adresses de liaison locale fondées sur SEND comme adresses de source IPv6 pour les messages MRD. Quand un commutateur reçoit une Annonce initiale, il peut utiliser les informations de l'adresse fondée sur SEND pour mettre au défi le routeur de s'authentifier. On notera que cette approche ne s'applique qu'aux réseaux IPv6.

Une autre solution qui prend en charge les deux IPv4 et IPv6 est d'utiliser IPsec en mode d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC2406] pour protéger contre les attaques en s'assurant que les messages viennent bien d'un système qui a la bonne clé. Quand on utilise IPsec, les messages envoyés à l'adresse "All-Snoopers" devraient être authentifiés en utilisant ESP. Si le chiffrement n'est pas désiré, ESP avec un algorithme de chiffrement nul et un algorithme d'authentification symétrique, comme HMAC-SHA-1, est viable. Pour le chiffrement, un algorithme de signature symétrique avec une seule clé configurée manuellement est utilisé pour les routeurs qui envoient les annonces. Cela permet la validation que le message MRD a été envoyé par un système qui a la clé. On notera que cela n'empêche pas qu'un système qui a la clé falsifie un message et cela exige la désactivation de la protection contre la répétition de IPsec. Il est de la responsabilité de l'administrateur du réseau de s'assurer que la même clé est présente sur tous les participants MRD possibles.

8. Considérations relatives à l'IANA

Le présent document introduit trois nouveaux messages IGMP. Chacun de ces messages exige une nouvelle valeur de type IGMP. L'IANA a alloué trois nouvelles valeurs de type IGMP au protocole de découverte de routeur de diffusion groupée.

Type IGMP	Paragraphe	Nom du message
0x30	3.2.1	Annonce de routeur de diffusion groupée
0x31	4.1.1	Sollicitation de routeur de diffusion groupée
0x32	5.1.1	Terminaison de routeur de diffusion groupée

Le présent document introduit aussi trois nouveaux messages MLD. Chacun de ces messages exige une nouvelle valeur de Type ICMPv6. L'IANA a alloué trois nouvelles valeurs de Type ICMPv6 dans la gamme pour information :

Type IGMPv6	Paragraphe	Nom du message
151	3.2.1	Annonce de routeur de diffusion groupée
152	4.1.1	Sollicitation de routeur de diffusion groupée
153	5.1.1	Terminaison de routeur de diffusion groupée

Le présent document exige aussi l'allocation d'une adresse de diffusion groupée "All-Snoopers" pour IPv4. Cette adresse de diffusion groupée est dans la gamme 224.0.0/24 car elle est utilisée pour les messages de contrôle de liaison locale. L'adresse IPv4 de diffusion groupée pour "All-Snoopers" est 224.0.0.106.

Une adresse IPv6 correspondante a aussi été allouée. Suivant les lignes directrices de la [RFC3307], l'adresse de diffusion groupée IPv6 est de portée liaison locale et a une valeur d'identifiant de groupe égale aux 8 bits de moindre poids de l'adresse de diffusion groupée IPv4 demandée. L'adresse IPv6 de diffusion groupée est FF02:0:0:0:0:0:0:6A.

9. Remerciements

Brad Cain et Shantam Biswis sont les auteurs de la proposition originale de découverte de routeur de diffusion groupée.

La découverte de routeur ICMP [RFC1256] a été utilisée comme modèle général pour la découverte de routeur de diffusion groupée.

Morten Christensen, Pekka Savola, Hugh Holbrook, et Isidor Kouvelas ont fourni d'utiles retours sur diverses versions de ce document.

10. Références

10.1 Références normatives

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989. *(Mise à jour par la* RFC2236*)*

[RFC2113] D. Katz, "Option d'alerte de routeur IP", février 1997. (*MàJ par* RFC5350, RFC6398) *(P.S.)*

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

[RFC2236] W. Fenner, "Protocole de gestion de groupe Internet, version 2", novembre 1997. *(P.S. ; MàJ* RFC1112 *; MàJ par* RFC3376)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

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

[RFC2711] C. Partridge, A. Jackson, "Option d'alerte de routeur IPv6", octobre 1999. *(P.S.)*

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

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

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

[RFC3971] J. Arkko et autres, "Découverte de voisin sûr (SEND)", mars 2005. (*MàJ par* RFC6494) *(P.S.)*

10.2 Références pour information

[RFC1256] S. Deering, éditeur, "Messages ICMP de découverte de routeur", septembre 1991.

Adresse des auteurs

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

Jim Martin
Netzwert AG
An den Treptowers 1
D-12435 Berlin
Germany
téléphone : +49.30/5 900 80-1180
mél : jim@netzwert.ag

Déclaration complète de droits de reproduction

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