Groupe de travail Réseau
**Request for Comments : 3376**
RFC rendue obsolète : 2236
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

B. Cain, Cereva Networks
S. Deering, Cisco Systems
I. Kouvelas, Cisco Systems
B. Fenner, AT&T Labs - Research
A. Thyagarajan, Ericsson
octobre2002

# Protocole de gestion de groupe Internet, (IGMP) version 3

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



**Résumé**
Le présent document spécifie la version 3 du protocole de gestion de groupe Internet (IGMP, *Internet Group Management Protocol*) IGMPv3. IGMP est le protocole utilisé par les systèmes IPv4 pour faire rapport des adhésions à leur groupe de diffusion groupée IP aux routeurs de diffusion groupée de leur voisinage. La version 3 d'IGMP ajoute la prise en charge du "filtrage de source", c'est-à-dire, la capacité pour un système de ne montrer son intérêt pour la réception de paquets *que* de la part d'adresses de source spécifiques, ou de la part de *toutes les adresses de source spécifiques sauf*, envoyées à une adresse de diffusion groupée particulière. Ces informations peuvent être utilisées par les protocoles d'acheminement de diffusion groupée pour éviter de livrer des paquets en diffusion groupée provenant de sources spécifiques à des réseaux où il n'y a pas de receveurs intéressés.

Le présent document rend obsolète la RFC 2236.

## Table des matières

## 1. Introduction

Le protocole de gestion de groupe Internet (IGMP, *Internet Group Management Protocol*) est utilisé par les systèmes IPv4 (hôtes et routeurs) pour faire rapport des adhérents aux groupes de diffusion groupée IP à tout routeur de diffusion groupée du voisinage. Noter qu'un routeur IP de diffusion groupée peut lui-même être un membre d'un ou plusieurs groupes de diffusion groupée, auquel cas il effectue à la fois la "partie routeur de diffusion groupée" du protocole (pour collecter les informations sur les membres nécessaires pour son protocole d'acheminement de diffusion groupée) et la "partie membre du groupe" du protocole (pour informer lui-même et les autres routeurs de diffusion groupée du voisinage, de son adhésion).

IGMP est aussi utilisé pour d'autres fonctions de gestion de diffusion groupée IP, en utilisant des types de message autres que ceux nécessaires pour le rapport d'adhésion de groupe. Le présent document ne spécifie que les fonctions et messages de rapport d'adhésion de groupe.

Le présent document spécifie la version 3 de IGMP. La version 1, spécifiée dans la [RFC1112], était la première version largement développée et la première à devenir une norme de l'Internet. La version 2, spécifiée dans la [RFC2236], ajoutait la prise en charge de la "faible latence de départ", c'est-à-dire, une réduction du temps nécessaire pour qu'un routeur de diffusion groupée apprenne qu'il n'y a plus aucun membre d'un groupe particulier présent sur un réseau rattaché. La version 3 ajoutait la prise en charge du "filtrage de source", c'est-à-dire, la capacité d'un système à manifester son intérêt pour la réception de paquets *seulement* d'adresses d'une source spécifique, comme nécessaire pour la prise en charge de la diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) [RFC3569], ou de *tout sauf* les adresses spécifiques de source envoyées à une adresse de diffusion groupée particulière. La version 3 est conçue pour être interopérable avec les versions 1 et 2.

La découverte des appareils en veille sur la diffusion groupée (MLD, *Multicast Listener Discovery*) est utilisée de façon similaire par les systèmes IPv6. La version 1 de la [RFC2710] met en œuvre la fonctionnalité de IGMP version 2 ; MLD version 2 [RFC3810] met en œuvre la fonctionnalité de IGMP version 3.

Les termes en majuscules "DOIT", "DEVRAIT", "PEUT", "NE DEVRAIT PAS", "NE DOIT PAS", et "RECOMMANDE" sont utilisés selon la définition de la RFC 2119. Du fait de l'absence d'italiques en texte brut, l'emphase est indiquée en encadrant un mot ou une phrase avec le caractère "*".

## 2. Interface de service pour demander la réception en diffusion groupée IP

Au sein d'un système IP, il y a (au moins conceptuellement) une interface de service utilisée par les protocoles de couche supérieure ou les programmes d'application pour demander à la couche IP d'activer et désactiver la réception de paquets envoyés à des adresses spécifiques de diffusion groupée IP. Afin de tirer pleinement parti des capacités de IGMPv3, une interface de service TP d'un système doit prendre en charge l'opération suivante :

IPMulticastListen ( prise, interface, adresse-de-diffusion-groupée, mode-filtre, liste-de-source )

où :

- "prise" est un paramètre spécifique de la mise en œuvre utilisé pour distinguer entre différentes entités demandeuses (par exemple, des programmes ou des processus) au sein du système ; le paramètre 'socket' des appels système BSD Unix en est un exemple spécifique.

- "interface" est un identifiant local de l'interface réseau sur laquelle la réception de l'adresse de diffusion groupée spécifiée est à activer ou à désactiver. Les interfaces peuvent être physiques (par exemple, une interface Ethernet) ou virtuelles (par exemple, le point d'extrémité d'un circuit virtuel de relais de trame ou le point d'extrémité d'un "tunnel" IP dans IP). Une mise en œuvre peut permettre qu'une valeur spéciale "non spécifiée" soit passée comme paramètre d'interface, auquel cas la demande va s'appliquer à l'interface "primaire" ou "par défaut" du système (peut-être établie par configuration du système). Si la réception de la même adresse de diffusion groupée est souhaitée sur plus d'une interface, IPMulticastListen est invoqué séparément pour chaque interface désirée.

- "adresse-de-diffusion-groupée" est l'adresse de diffusion groupée IP, ou groupe, à laquelle appartient la demande. Si la réception de plus d'une adresse de diffusion groupée est désirée sur une interface donnée, IPMulticastListen est invoqué séparément pour chaque adresse de diffusion groupée désirée.

- "mode-filtre" peut être INCLURE ou EXCLURE. En mode INCLURE, la réception des paquets envoyés à l'adresse de diffusion groupée spécifiée est demandée *seulement* aux adresses IP de source dont la liste figure dans le paramètre liste-de-sources. En mode EXCLURE, la réception des paquets envoyés à l'adresse de diffusion groupée donnée est demandée à toutes les adresses IP de source *excepté* celles figurant sur la liste du paramètre liste-de-sources.

- "liste-de-source" est une liste non ordonnée de zéro, une ou plusieurs adresses IP d'envoi individuel d'où la réception en diffusion groupée est désirée ou non désirée, selon le mode de filtre. Une mise en œuvre PEUT imposer une limite à la taille des listes de source, mais cette limite NE DOIT PAS être inférieure à 64 adresses par liste. Lorsque une opération cause le dépassement de la limite de la taille de liste de sources, l'interface de service DOIT retourner une erreur.

Pour une combinaison donnée de prise, interface, et adresse de diffusion groupée, un seul mode de filtre et une seule liste de sources peuvent être actifs à un instant donné. Cependant, soit le mode de filtre, soit la liste de source, soit les deux peuvent être changés par les demandes IPMulticastListen suivantes qui spécifient la même prise, interface, et adresse de diffusion groupée. Chaque demande ultérieure remplace complètement toute demande antérieure pour la prise, interface et adresse de diffusion groupée données.

Les précédentes versions de IGMP ne prenaient pas en charge les filtres de source et avaient une interface de service plus simple consistant en opérations Join et Leave pour activer et désactiver la réception d'une adresse de diffusion groupée donnée (de *toutes* sources) sur une interface donnée. Ci-après figurent les opérations équivalentes dans la nouvelle interface de service.

L'opération Join est équivalente à

IPMulticastListen ( prise, interface, adresse-de-diffusion-groupée, EXCLURE, {} )

et l'opération Leave est équivalente à :

IPMulticastListen ( prise, interface, adresse-de-diffusion-groupée, INCLURE, {} )

où {} est une liste-de-source vide.

Un exemple d'API fournissant les capacités soulignées dans cette interface de service figure dans la [RFC3678]

## 3. État de réception de diffusion groupée entretenu par les systèmes

### 3.1 État Prise

Pour chaque prise sur laquelle IPMulticastListen a été invoqué, le système enregistre l'état de réception en diffusion groupée désiré pour cette prise. Cet état consiste conceptuellement en un ensemble d'enregistrements de la forme :

(interface, adresse-de-diffusion-groupée, mode-de-filtre, liste-de-sources)

L'état de la prise évolue en réponse à chaque invocation de IPMulticastListen sur la prise, comme suit :

- Si le mode de filtre demandé est INCLURE *et* si la liste de sources demandée est vide, l'entrée correspondant à l'interface et l'adresse de diffusion groupée demandée est alors supprimée si elle est présente. Si une telle entrée n'est pas présente, la demande est ignorée.
- Si le mode de filtre demandé est EXCLURE *ou* si la liste de sources demandée n'est pas vide, l'entrée correspondant à l'interface et l'adresse de diffusion groupée demandée, si elle est présente, est alors changée pour contenir le mode de filtre et la liste de sources demandés. Si une telle entrée n'est pas présente, une nouvelle entrée est créée, en utilisant les paramètres spécifiés dans la demande.

### 3.2 État Interface

En plus de l'état de réception en diffusion groupée par prise, un système doit aussi entretenir ou calculer l'état de réception en diffusion groupée pour chacune de ses interfaces. Cet état consiste conceptuellement en un ensemble d'enregistrements de la forme :

(adresse-de-diffusion-groupée, mode-filtre, liste-de-sources)

Au plus un enregistrement par adresse-de-diffusion-groupée existe pour une certaine interface. Cet état par interface est déduit de l'état par prise, mais peut différer de l'état par prise lorsque différentes prises ont des modes de filtre et/ou des listes des sources différents pour la même adresse et interface de diffusion groupée. Par exemple, supposons qu'une application ou processus invoque l'opération suivante sur la prise s1 :

IPMulticastListen ( s1, i, m, INCLURE, {a, b, c} )

qui demande la réception sur l'interface i des paquets envoyés à l'adresse de diffusion groupée m, *seulement* si ils viennent des sources a, b, ou c. Supposons qu'une autre application ou processus invoque l'opération suivante sur la prise s2 :

IPMulticastListen ( s2, i, m, INCLURE, {b, c, d} )

qui demande la réception sur la même interface i des paquets envoyés à la même adresse de diffusion groupée m, seulement si ils viennent des sources b, c, ou d. Afin de satisfaire les exigences de réception des deux prises, il est nécessaire que l'interface i reçoive les paquets envoyés à m de toute source a, b, c, ou d. Donc, dans cet exemple, l'état de réception de l'interface i pour l'adresse de diffusion groupée m a le mode de filtre INCLURE et la liste des sources {a, b, c, d}.

Après qu'un paquet en diffusion groupée a été accepté d'une interface par la couche IP, sa livraison ultérieure à l'application ou processus qui écoute sur une prise particulière dépend de l'état de réception en diffusion groupée de cette prise (et éventuellement aussi d'autres conditions, telles que l'accès de couche transport auquel est liée cette prise). Ainsi, dans l'exemple ci-dessus, si un paquet arrive sur l'interface i, destiné à l'adresse de diffusion groupée m, avec l'adresse de source a, il sera livré sur la prise s1 mais pas sur la prise s2. Noter que les interrogations et rapports IGMP ne sont pas soumis au filtrage de source et doivent toujours être traités par les hôtes et routeurs.

Le filtrage des paquets sur la base de l'état de réception en diffusion groupée d'une prise est une nouvelle caractéristique de cette interface de service. La précédente interface de service [RFC1112] ne décrivait pas de filtrage fondé sur l'état de jonction à la diffusion groupée, mais plutôt une jonction à une prise causait simplement la jonction de l'hôte à un groupe sur l'interface considérée, et les paquets destinés à ce groupe pouvaient être livrés à toutes les prises qu'elles se soient jointes ou non.

Les règles générales pour déduire l'état par interface de l'état par prise sont les suivantes : pour chaque paire distincte (interface, adresse-de-diffusion-groupée) qui apparaît dans tout état de prise, un enregistrement par interface est créé pour cette adresse de diffusion groupée sur cette interface. Si on considère tous les enregistrements de prise qui contiennent la même paire (interface, adresse-de-diffusion-groupée) :

- si *un quelconque* de ces enregistrements a un mode de filtre de EXCLURE, alors le mode de filtre de l'enregistrement d'interface est EXCLURE, et la liste des sources de l'enregistrement d'interface est l'intersection de la liste des sources de tous les enregistrements de prise en mode EXCLURE, moins les adresses de source qui apparaissent dans tout enregistrement de prise en mode INCLURE. Par exemple, si les enregistrements de prise pour l'adresse de diffusion groupée m sur l'interface i sont :
  de la prise s1 : ( i, m, EXCLURE, {a, b, c, d} )
  de la prise s2 : ( i, m, EXCLURE, {b, c, d, e} )
  de la prise s3 : ( i, m, INCLURE, {d, e, f} )
  alors l'enregistrement d'interface correspondant sur l'interface i est :
  ( m, EXCLURE, {b, c} )
  Si une quatrième prise est ajoutée, telle que :
  de la prise s4 : ( i, m, EXCLURE, {} )
  alors, l'enregistrement d'interface devient : ( m, EXCLURE, {} )
- Si *tous* ces enregistrements ont un mode de filtre de INCLURE, alors, le mode de filtre de l'enregistrement d'interface est INCLURE, et la liste des sources de l'enregistrement d'interface est l'union des listes des sources de tous les enregistrements de prise. Par exemple, si les enregistrements de prise pour l'adresse de diffusion groupée m sur l'interface i sont :
  de la prise s1 : ( i, m, INCLURE, {a, b, c} )
  de la prise s2 : ( i, m, INCLURE, {b, c, d} )
  de la prise s3 : ( i, m, INCLURE, {e, f} )
  alors, l'enregistrement d'interface correspondant sur l'interface i est : ( m, INCLURE, {a, b, c, d, e, f} )

Une mise en œuvre NE DOIT PAS utiliser un enregistrement d'interface EXCLURE pour représenter un groupe lorsque toutes les prises pour ce groupe sont dans l'état INCLURE. Si les limites de ressource du système sont atteintes lorsque est calculée la liste des sources d'un état d'interface, une erreur DOIT être retournée à l'application qui a demandé cette opération.

Les règles de déduction d'état d'interface ci-dessus sont (ré)évaluées chaque fois qu'une invocation IPMulticastListen modifie l'état de la prise en ajoutant, supprimant, ou modifiant un enregistrement d'état par prise. Noter qu'un changement d'état de prise ne résulte pas nécessairement en un changement de l'état de l'interface.

## 4. Formats de message

Les messages IGMP sont encapsulés dans des datagrammes IPv4, avec un numéro de protocole IP de 2. Chaque message IGMP décrit dans le présent document est envoyé avec une durée de vie (TTL, *Time-to-Live*) IP de 1, une préséance IP de Internetwork Control (par exemple, Type de service 0xc0) et porte une option d'alerte de routeur IP [RFC2113] dans son en-tête IP. Les types de message IGMP sont enregistrés par l'IANA [IANA-REG] comme décrit dans la [RFC3228].

Il y a deux types de message IGMP intéressants pour le protocole IGMPv3 qui sont décrits dans le présent document :

| **Numéro de type (hex)** | **Nom de message** |
|---|---|
| 0x11 | Interrogation sur les adhésions |
| 0x22 | Rapport d'adhésion version 3 |

Une mise en œuvre de IGMPv3 DOIT aussi prendre en charge les trois types de message suivants, pour l'interopération avec les précédentes versions de IGMP (voir la section 7) :

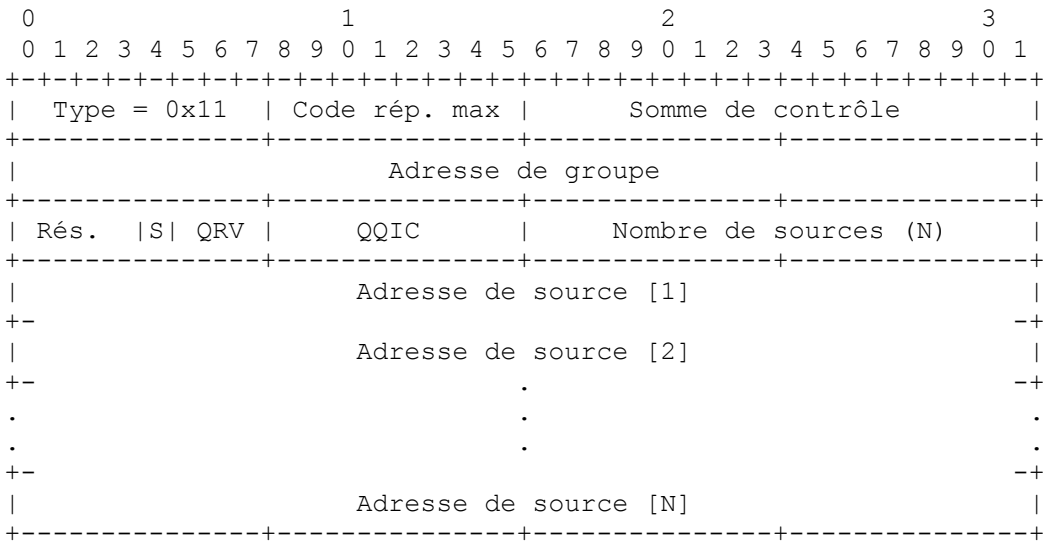
| | | |
|---|---|---|
| 0x12 | Rapport d'adhésion version 1 | [RFC1112] |
| 0x16 | Rapport d'adhésion version 2 | [RFC2236] |
| 0x17 | Version 2 Leave Group | [RFC2236] |

Les types de message non reconnus DOIVENT être ignorés en silence. Les autres types de message peuvent être utilisés par de nouvelles versions ou extensions de IGMP, par des protocoles d'acheminement de diffusion groupée, ou pour d'autres usages.

Dans le présent document, sauf qualification contraire, les mots commençant pas une majuscule "Interrogation" et "Rapport" se réfèrent respectivement à l'interrogation d'adhésion IGMP et au rapport d'adhésion IGMP version 3.

### 4.1 Message d'interrogation sur les adhésions

Les interrogations d'adhésion sont envoyées par les routeurs de diffusion groupée IP pour interroger l'état de réception en diffusion groupée des interfaces du voisinage. Les interrogations ont le format suivant :



#### 4.1.1 Code rép. max

Le champ Code rép. max spécifie le nombre maximum de fois permis avant d'envoyer un rapport en réponse. Le temps réel accordé, appelé Délai rép. max, est représenté en unités de 1/10 de seconde et est déduit du Code rép. max de la façon suivante :

Si Code rép. max < 128, Délai rép. max = Code rép. max

Si Code rép. max ≥ 128, Code rép. max représente une valeur en virgule flottante comme suit :

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|1| exp |mantis.|
+-+-+-+-+-+-+-+-+
```

Délai rép. max = (mantisse | 0x10) << (exp + 3)

Les petites valeurs de Délai rép. max permettent aux routeurs IGMPv3 de temporiser la "latence de départ" (le temps qui s'écoule entre le moment où le dernier hôte quitte un groupe et le moment où le protocole d'acheminement est notifié qu'il n'y a plus de membre). Les plus grandes valeurs, en particulier dans la gamme exponentielle, permette le réglage de la sporadicité du trafic IGMP sur un réseau.

#### 4.1.2 Somme de contrôle

La somme de contrôle est les 16 bits du complément à un de la somme des compléments à un du message IGMP entier (la charge utile IP entière). Pour le calcul de la somme de contrôle, le champ Somme de contrôle est réglé à zéro. Lorsque on reçoit des paquets, la somme de contrôle DOIT être vérifiée avant le traitement d'un paquet. [RFC1071]

#### 4.1.3 Adresse de groupe

Le champ Adresse de groupe est réglé à zéro lors de l'envoi d'une interrogation générale, et réglé à l'adresse IP de diffusion groupée sur laquelle porte l'interrogation lors de l'envoi d'une interrogation spécifique de groupe ou d'une interrogation spécifique de groupe et de source (voir au paragraphe 4.1.9).

#### 4.1.4 Rés. (réservé)

Le champ Rés. est réglé à zéro à l'émission, et ignoré à réception.

#### 4.1.5 Fanion S (Supprimer le traitement côté routeur)

Lorsque établi à un, le fanion S indique à tout routeur receveur de diffusion groupée qu'il doit supprimer les mises à jour normales de temporisateur qu'il effectue lorsqu'il entend une Interrogation. Cela ne supprime cependant pas le choix de l'interrogateur ni le traitement normal "côté hôte" d'une Interrogation qu'un routeur peut être obligé d'effectuer par suite du fait qu'il est lui-même membre d'un groupe.

#### 4.1.6 Variable de robustesse de l'interrogateur

Si il n'est pas à zéro, le champ QRV *(Querier's Robustness Variable)* contient la variable [Variable de robustesse] utilisée par l'interrogateur, c'est-à-dire, l'envoyeur de l'Interrogation. Si la [Variable de robustesse] de l'interrogateur excède 7, valeur maximum du champ QRV, la QRV est réglée à zéro. Les routeurs adoptent la valeur de QRV provenant de l'Interrogation la plus récente reçue comme propre [Variable de robustesse], sauf si cette QRV la plus récemment reçue est de zéro, auquel cas le receveur utilise la valeur de [Variable de robustesse] par défaut spécifiée au paragraphe 8.1 ou une valeur de configuration statique.

#### 4.1.7 Code d'intervalle d'interrogation de l'interrogateur

Le champ QQIC *(Querier's Query Interval Code)* spécifie l'intervalle d'interrogation utilisé par l'interrogateur. L'intervalle réel, appelé intervalle d'interrogation de l'interrogateur (QQI, *Querier's Query Interval*) est représenté en unités de secondes et est déduit du code d'intervalle d'interrogation de l'interrogateur de la façon suivante :

Si QQIC < 128, QQI = QQIC

SI QQIC ≥ 128, QQIC représente une valeur à virgule flottante comme suit :

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|1| exp |mantis.|
+-+-+-+-+-+-+-+-+
```

QQI = (mantisse | 0x10) << (exp + 3)

Les routeurs de diffusion groupée qui ne sont pas l'interrogateur actuel adoptent la valeur du QQI de l'interrogation la plus récemment reçue comme leur propre valeur d'intervalle d'interrogation, sauf si cette QQI la plus récemment reçue était zéro, auquel cas le routeur receveur utilisera la valeur par défaut d'intervalle d'interrogation spécifiée au paragraphe 8.2.

#### 4.1.8 Nombre de sources (N)

Le champ Nombre de sources (N) spécifie combien d'adresses de sources sont présentes dans l'interrogation. Ce nombre est de zéro dans une interrogation générale ou une interrogation spécifique de groupe, et différent de zéro dans une interrogation spécifique de groupe et de source. Ce nombre est limité par la MTU du réseau sur lequel l'interrogation est transmise. Par exemple, sur un Ethernet avec une MTU de 1500 octets, l'en-tête IP incluant l'option d'alerte de routeur consomme 24 octets, et le champs IGMP jusque et y compris le champ Nombre de sources (N) consomme 12 octets, laissant 1464 octets pour les adresses de sources, ce qui limite le nombre d'adresses de sources à 366 (1464/4).

#### 4.1.9 Adresse de source [i]

Le champ Adresse de source [i] est un vecteur de n adresses IP d'envoi individuel, où n est la valeur dans le champ Nombre de sources (N).

#### 4.1.10 Données supplémentaires

Si le champ Longueur de paquet dans l'en-tête IP d'une Interrogation reçue indique que sont présents des octets de données supplémentaires, au delà des champs décrits ici, les mises en œuvre de IGMPv3 DOIVENT inclure ces octets dans le calcul pour vérifier la somme de contrôle IGMP reçue, mais DOIVENT autrement ignorer ces octets supplémentaires. Lors de l'envoi d'une Interrogation, une mise en œuvre d'IGMPv3 NE DOIT PAS inclure d'octets supplémentaires au delà des champs qui sont décrits ici.

#### 4.1.11 Variantes d'interrogation

Il y a trois variantes du message Interrogation :

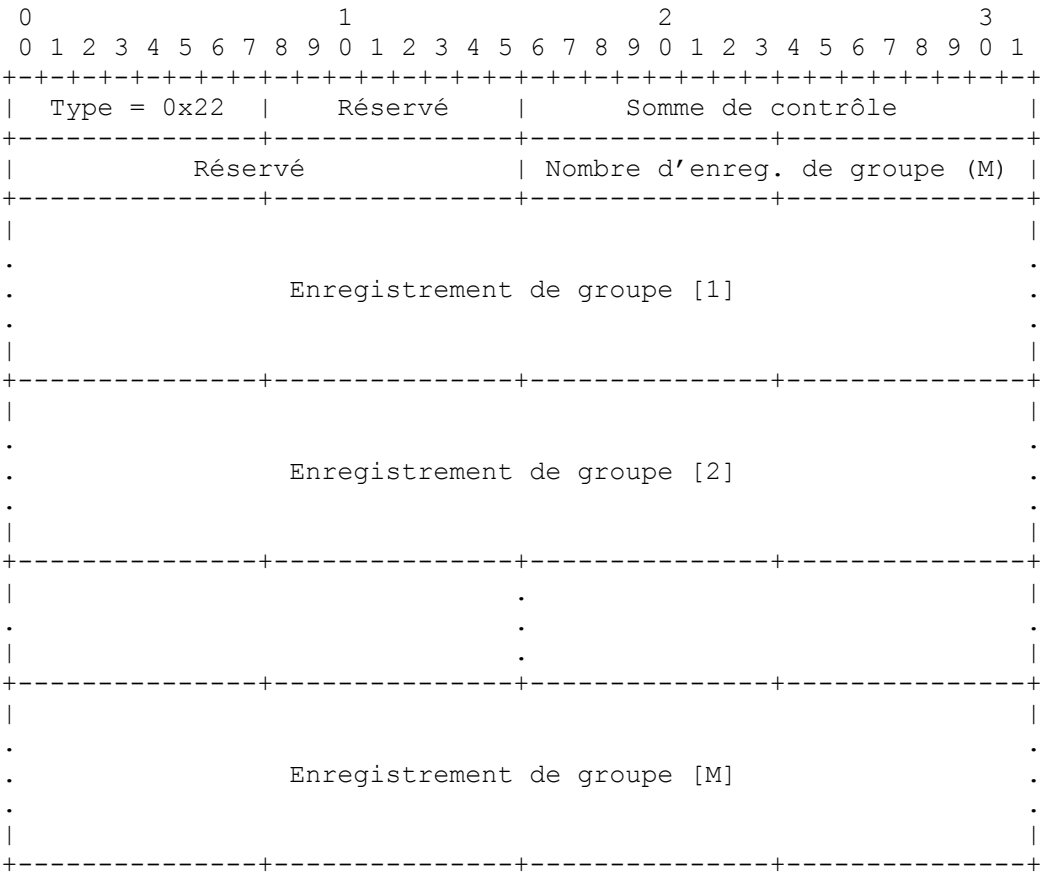
1. Une "interrogation générale" est envoyée par un routeur de diffusion groupée pour apprendre l'achèvement de l'état de réception en diffusion groupée des interfaces du voisinage (c'est-à-dire, les interfaces rattachées au réseau sur lequel l'Interrogation est transmise). Dans une interrogation générale, les champs Adresse de groupe et Nombre de sources (N) sont tous deux à zéro.
2. Une "interrogation spécifique de groupe" est envoyée par un routeur de diffusion groupée pour apprendre l'état de réception, par rapport à une *seule* adresse de diffusion groupée, des interfaces du voisinage. Dans une Interrogation spécifique de groupe, le champ Adresse de groupe contient l'adresse de diffusion groupée concernée, et le champ Nombre de Sources (N) contient zéro.
3. Une "Interrogation spécifique de groupe et de source" est envoyée par un routeur de diffusion groupée pour apprendre si une interface du voisinage désire la réception de paquets envoyés à une adresse de diffusion groupée spécifiée, à partir d'une des sources spécifiées par la liste des sources. Dans une Interrogation spécifique de groupe et de source, le champ Adresse de source contient l'adresse de diffusion groupée concernée, et les champs Adresse de source [i] contiennent la ou les adresses de source concernées.

#### 4.1.12 Adresses de destination IP pour les interrogations

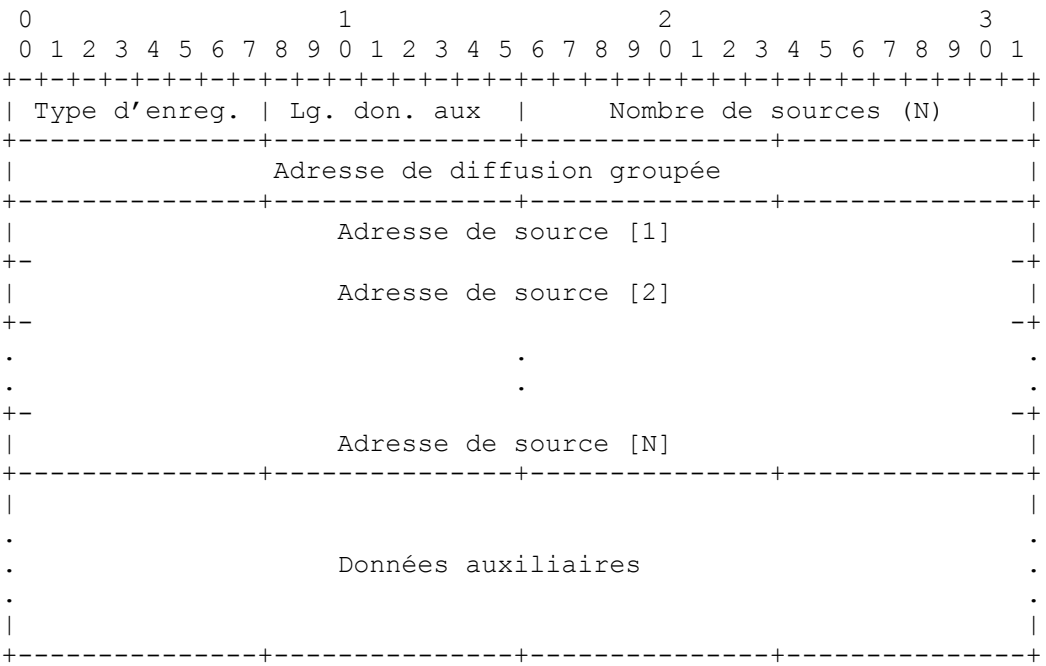
Dans IGMPv3, les interrogations générales sont envoyées avec une adresse IP de destination de 224.0.0.1, l'adresse de diffusion groupée Tous-systèmes. Les interrogations spécifiques de groupe et spécifique de groupe et de source sont envoyées avec l'adresse IP de destination égale à l'adresse de diffusion groupée concernée. *Cependant*, un système DOIT accepter et traiter toute Interrogation dont le champ Adresse IP de destination contient *une* des adresses (envoi individuel ou envoi en diffusion groupée) allouée à l'interface sur laquelle arrive l'Interrogation.

### 4.2 Message de rapport d'adhésion version 3

Les rapports d'adhésion version 3 sont envoyés par les systèmes IP pour rapporter (aux routeurs du voisinage) l'état actuel de réception en diffusion groupée, ou les changements dans l'état de réception en diffusion groupée, de leurs interfaces. Les rapports ont le format suivant :




où chaque Enregistrement de groupe a le format interne suivant :




#### 4.2.1 Réservé

Les champs Réservé sont réglés à zéro à l'émission, et ignorés à réception.

#### 4.2.2 Somme de contrôle

La somme de contrôle de 16 bits est le complément à un de la somme des compléments à un de tout le message IGMP (toute la charge utile IP). Pour calculer la somme de contrôle, le champ Somme de contrôle est réglé à zéro. Lors de la réception des paquets, la somme de contrôle DOIT être vérifiée avant de traiter un message.

#### 4.2.3 Nombre d'enregistrements de groupe (M)

Le champ Nombre d'enregistrements de groupe (M) spécifie combien d'enregistrements de groupe sont présents dans ce rapport.

#### 4.2.4 Enregistrement de groupe

Chaque enregistrement de groupe est un bloc de champs contenant des informations relatives aux membres de l'envoyeur dans un seul groupe de diffusion groupée sur l'interface d'où le rapport est envoyé.

#### 4.2.5 Type d'enregistrement

Voir au paragraphe 4.2.12.

#### 4.2.6 Longueur des données auxiliaires

Le champ Longueur des données auxiliaires contient la longueur du champ Données auxiliaires dans cet enregistrement de groupe, en unités de mots de 32 bits. Il peut contenir zéro, pour indique l'absence de toutes données auxiliaires.

#### 4.2.7 Nombre de sources (N)

Le champ Nombre de sources (N) spécifie combien d'adresses de sources sont présentes dans cet enregistrement de groupe.

#### 4.2.8 Adresse de diffusion groupée

Le champ Adresse de diffusion groupée contient l'adresse de diffusion groupée IP à laquelle appartient l'enregistrement de groupe.

#### 4.2.9 Adresse de source [i]

Les champs Adresse de source [i] sont un vecteur de n adresses IP d'envoi individuel, où n est la valeur du champ Nombre de sources (N) dans cet enregistrement.

#### 4.2.10 Données auxiliaires

Le champ Données auxiliaires, s'il est présent, contient des informations supplémentaires relevant de cet enregistrement de groupe. Le protocole spécifié dans le présent document, IGMPv3, ne définit aucune donnée auxiliaire. Donc, les mises en œuvre de IGMPv3 NE DOIVENT PAS inclure de données auxiliaires (c'est-à-dire, DOIVENT régler le champ Longueur de données auxiliaires à zéro) dans tout enregistrement de groupe transmis et DOIVENT ignorer toutes données auxiliaires présentes dans tout enregistrement de groupe reçu. La sémantique et le codage interne du champ Données auxiliaires seront à définir pour toute version ou extension future d'IGMP qui utilisera ce champ.

#### 4.2.11 Données supplémentaires

Si le champ Longueur du paquet dans l'en-tête IP d'un rapport reçu indique qu'il y a des octets de données supplémentaires présents, au delà du dernier enregistrement de groupe, les mises en œuvre IGMPv3 DOIVENT inclure ces octets dans le calcul pour vérifier la somme de contrôle IGMP reçue, mais DOIVENT autrement ignorer ces octets supplémentaires. Lors de l'envoi d'un rapport, une mise en œuvre IGMPv3 NE DOIT PAS inclure d'octets supplémentaires au delà du dernier enregistrement de groupe.

#### 4.2.12 Types d'enregistrements de groupe

Il y a un certain nombre de différents types d'enregistrements de groupe qui peuvent être inclus dans un message Rapport :

o Un "enregistrement d'état en cours" est envoyé par un système en réponse à une Interrogation reçue sur une interface. Il rapporte l'état de réception actuel de cette interface, par rapport à une seule adresse de diffusion groupée. Le type d'enregistrement d'un enregistrement d'état en cours peut être une des deux valeurs suivantes :

**Valeur Nom et signification**

1 MODE_EST_INCLUS – indique que l'interface a un mode de filtre de INCLUS pour l'adresse de diffusion groupée spécifiée. Les champs Adresse de source [i] dans cet enregistrement de groupe contiennent la liste des sources de l'interface pour l'adresse de diffusion groupée spécifiée, si elle n'est pas vide.

2 MODE_EST_EXCLU – indique que l'interface a un mode de filtre de EXCLU pour l'adresse de diffusion groupée spécifiée. Les champs Adresse de source [i] dans cet enregistrement de groupe contiennent la liste des sources de l'interface pour l'adresse de diffusion groupée spécifiée, si elle n'est pas vide.

- Un "enregistrement de changement de mode de filtre" est envoyé par un système chaque fois qu'une invocation locale de IPMulticastListen cause un changement du mode de filtre (c'est-à-dire, un changement de INCLURE à EXCLURE, ou de EXCLURE à INCLURE) de l'entrée d'état de niveau d'interface pour une adresse de diffusion groupée particulière. L'enregistrement est inclus dans un rapport envoyé de l'interface sur laquelle le changement est survenu. Le type d'enregistrement d'un type d'enregistrement de changement de mode de filtre peut être de l'une des deux valeurs suivantes :

3 CHANGER_POUR_MODE_INCLURE – indique que l'interface a changé en INCLURE le mode de filtre pour l'adresse de diffusion groupée spécifiée. Les champs Adresse de source [i] dans cet enregistrement de groupe contiennent la nouvelle liste des sources de l'interface pour l'adresse de diffusion groupée spécifiée, si elle n'est pas vide.

4 CHANGER_POUR_MODE_EXCLURE – indique que l'interface a changé pour le mode de filtre EXCLURE pour l'adresse de diffusion groupée spécifiée. Les champs Adresse de source [i] dans cet enregistrement de groupe contiennent la nouvelle liste des sources de l'interface pour l'adresse de diffusion groupée spécifiée, si elle n'est pas vide.

o Un "enregistrement de changement de liste des sources" est envoyé par un système chaque fois qu'une invocation locale de IPMulticastListen cause un changement de la liste des sources qui est *non* coïncident avec un changement de mode de filtre, de l'entrée d'état de niveau d'interface pour une adresse de diffusion groupée particulière. L'enregistrement est inclus dans un rapport envoyé de l'interface sur laquelle le changement s'est produit. Le type d'enregistrement d'un type d'enregistrement de changement de liste des sources peut être une des deux valeurs suivantes :

5 PERMET_NOUVELLES_SOURCES – indique que les champs Adresse de source [i] dans cet enregistrement de groupe contiennent une liste des sources supplémentaires que le système souhaite apprendre, pour les paquets envoyés à l'adresse de diffusion groupée spécifiée. Si le changement était de INCLURE la liste des sources, celles-ci sont les adresses qui ont été ajoutées à la liste ; si le changement était un EXCLURE la liste des sources, celles-ci sont les adresses qui ont été supprimées de la liste.

6 BLOQUER_LES_VIEILLES_SOURCES – indique que les champs Adresse de source [i] dans cet enregistrement de groupe contiennent une liste des sources dont le système ne souhaite plus entendre parler, pour les paquets envoyés à l'adresse de diffusion groupée spécifiée. Si le changement est d'INCLURE la liste des sources, celles-ci sont les adresses qui ont été supprimées de la liste ; si le changement est d'EXCLURE la liste des sources, celles-ci sont les adresses ajoutées à la liste.

Si un changement de liste des sources résulte à la fois à permettre de nouvelles sources et à bloquer les vieilles sources, alors deux enregistrements de groupe sont envoyés pour la même adresse de diffusion groupée, une du type PERMET_DE_NOUVELLES_SOURCES et une du type BLOQUER_LES_VIEILLES_SOURCES.

On utilise le terme "enregistrement de changement d'état" pour désigner aussi bien un enregistrement de changement de mode de filtre qu'un enregistrement de changement de liste des sources.

Les valeurs de type d'enregistrement non reconnu DOIVENT être ignorées en silence.

#### 4.2.13 Adresses IP de source pour les rapports

Un rapport IGMP est envoyé avec une adresse IP de source valide pour le sous-réseau de destination. L'adresse de source 0.0.0.0 peut être utilisée par un système qui n'a pas encore acquis une adresse IP. Noter que l'adresse de source 0.0.0.0 peut simultanément être utilisée par plusieurs systèmes sur un LAN. Les routeurs DOIVENT accepter un rapport avec une adresse de source de 0.0.0.0.

#### 4.2.14 Adresses IP de destination pour les rapports

Les rapports de version 3 sont envoyés avec une adresse IP de destination de 224.0.0.22, à laquelle écoutent tous les routeurs de diffusion groupée à capacité IGMPv3. Un système qui fonctionne en modes de compatibilité de version 1 ou de version 2 envoie des rapports de version 1 ou de version 2 au groupe de diffusion groupée spécifié dans le champ Adresse de groupe du rapport. De plus, un système DOIT accepter et traiter tout rapport de version 1 ou de version 2 dont le champ Adresse IP de destination contient *toutes* les adresses (d'envoi individuel ou de diffusion groupée) allouées à l'interface sur laquelle arrive le rapport.

#### 4.2.15 Notation des enregistrements de groupe

Dans le reste du présent document, on utilise la notation suivante pour décrire le contenu d'un enregistrement de groupe appartenant à une adresse de diffusion groupée particulière :

IS_IN ( x ) - Type MODE_EST_INCLURE, adresses de source x
IS_EX ( x ) - Type MODE_EST_EXCLURE, adresses de source x
TO_IN ( x ) - Type CHANGER_POUR_MODE_INCLURE, adresses de source x
TO_EX ( x ) - Type CHANGER_POUR_MODE_EXCLURE, adresses de source x
PERMET ( x ) - Type PERMET_NOUVELLES_SOURCES, adresses de source x
BLOQUE ( x ) - Type BLOQUER_NOUVELLES_SOURCES, adresses de source x

où x est :

- une lettre majuscule (par exemple, "A") pour représenter l'ensemble des adresses de source, ou
- une expression d'ensemble (par exemple, "A+B") où "A+B" signifie l'union des ensembles A et B, "A*B" signifie l'intersection des ensembles A et B, et "A-B" signifie le retrait de tous les éléments de l'ensemble B de l'ensemble A.

#### 4.2.16 Taille de rapport d'adhésion

Si l'ensemble d'enregistrements de groupe exigé dans un rapport ne tient pas dans les limites de taille d'un seul message Rapport (comme déterminé par la MTU du réseau sur lequel il va être envoyé) les enregistrements de groupe sont envoyés en autant de messages Rapport que nécessaire pour faire rapport de la totalité de l'ensemble.

Si un seul enregistrement de groupe contient tant d'adresses de source qu'il ne tient pas dans les limites de taille d'un seul message Rapport, si son type n'est pas MODE_EST_EXCLURE ou CHANGER_POUR_MODE_EXCLURE, il est divisé en plusieurs enregistrements de groupe, contenant chacun un sous-ensemble différent des adresses de source et envoyé chacun dans un message Rapport distinct. Si son type est MODE_EST_EXCLURE ou CHANGER_POUR_MODE_EXCLURE, un seul enregistrement de groupe est envoyé, contenant autant d'adresses de source qu'il peut en tenir, et les adresses de source restantes ne sont pas rapportées; bien que le choix des sources à rapporter soit arbitraire, il est préférable de faire rapport du même ensemble de sources dans chaque rapport suivant, plutôt que de faire rapport de sources différentes à chaque fois.

## 5. Description du protocole pour les membres du groupe

IGMP est un protocole asymétrique, qui spécifie des comportements distincts pour chaque membre du groupe – c'est-à-dire, les hôtes ou routeurs qui souhaitent recevoir les paquets en diffusion groupée – et les routeurs de diffusion groupée. Cette section décrit la partie de IGMPv3 qui s'applique à tous les membres du groupe. (Noter qu'un routeur de diffusion groupée qui est aussi un membre du groupe effectue les deux parties de IGMPv3, recevant et répondant à ses propres transmissions de messages IGMP aussi bien qu'à celles de ses voisins. La partie routeur de diffusion groupée d'IGMPv3 est décrite à la section 6.)

Un système effectue le protocole décrit dans la présente section sur toutes les interfaces sur lesquelles la réception en diffusion groupée est prise en charge, même si plus d'une de ces interfaces est connectée au même réseau.

Pour l'interopérabilité avec les routeurs de diffusion groupée qui fonctionnent avec de plus anciennes versions d'IGMP, les systèmes entretiennent une variable MulticastRouterVersion pour chaque interface sur laquelle est prise en charge la réception en diffusion groupée. La présente section décrit le comportement des systèmes de membres de groupe sur des interfaces pour lesquelles MulticastRouterVersion = 3. L'algorithme pour déterminer MulticastRouterVersion, et le comportement pour les versions autres que 3, sont décrits à la section 7.

L'adresse de diffusion groupée Tous_systèmes, 224.0.0.1, est traitée comme un cas particulier. Sur tous les systèmes – c'est-à-dire tous les hôtes et routeurs, y compris les routeurs de diffusion groupée – la réception de paquets destinés à l'adresse de diffusion groupée Tous_systèmes, à partir de toutes les sources, est activée de façon permanente sur toutes les interfaces sur lesquelles la réception en diffusion groupée est prise en charge. Aucun message IGMP n'est jamais envoyé à l'adresse de diffusion groupée Tous_systèmes.

Il y a deux types d'événements qui déclanchent les actions du protocole IGMPv3 sur une interface :
- o un changement de l'état de réception de l'interface, causé par une invocation locale de IPMulticastListen ;
- o la réception d'une interrogation.

(Les messages IGMP reçus de types autres que Interrogation sont ignorés en silence, sauf quand exigés pour l'interopération avec de plus anciennes versions d'IGMP.)

Les paragraphes qui suivent décrivent les actions à entreprendre pour chacun de ces deux cas. Dans ces descriptions, les noms de temporisateur et de compteur apparaissent entre crochets. Les valeurs par défaut de ces temporisateurs et compteurs sont spécifiées à la section 8.

## 5.1 Action sur changement d'état d'interface

Une invocation de IPMulticastListen peut causer un changement de l'état de réception en diffusion groupée d'une interface, conformément aux règles du paragraphe 3.2. Chacun de ces changements affecte l'entrée par interface pour une seule adresse de diffusion groupée.

Un changement de l'état de l'interface cause la transmission immédiate par le système d'un rapport Changement d'état pour cette interface. Le type et le contenu du ou des enregistrements de groupe dans ce rapport sont déterminés par comparaison du mode de filtre et de la liste des sources pour l'adresse de diffusion groupée affectée avant et après le changement, conformément au tableau ci-dessous. Si aucun état d'interface n'existait pour cette adresse de diffusion groupée avant le changement (c'est-à-dire, si le changement consistait en la création d'un nouvel enregistrement par interface) ou si aucun état n'existe après le changement (c'est-à-dire, si le changement consistait en la suppression d'un enregistrement par interface) alors l'état "non existant" est considéré avoir un mode de filtre de INCLURE et une liste des sources vide.

| **Vieil état** | **Nouvel état** | **Enregistrement de changement d'état envoyé** |
|---|---|---|
| INCLURE (A) | INCLURE (B) | PERMET (B-A), BLOQUE (A-B) |
| EXCLURE (A) | EXCLURE (B) | PERMET (A-B), BLOQUE (B-A) |
| INCLURE (A) | EXCLURE (B) | TO_EX (B) |
| EXCLURE (A) | INCLURE (B) | TO_IN (B) |

Si la liste des sources calculée pour un enregistrement de changement d'état PERMET ou BLOQUE est vide, cet enregistrement est omis du message Rapport.

Pour couvrir la possibilité que le rapport de changement d'état ait été manqué par un ou plusieurs routeurs de diffusion groupée, il est retransmis [Variable de robustesse] - 1 fois, à des intervalles choisis au hasard dans la gamme (0, [Intervalle de rapport non sollicité]).

Si plus de changements à la même entrée d'état d'interface surviennent avant que toutes les retransmissions du rapport de changement d'état depuis le premier changement aient été achevées, chacun de ces changements supplémentaires déclanche la transmission immédiate d'un nouveau rapport de changement d'état.

Le contenu du nouveau rapport transmis est calculé comme suit : comme il a été fait avec le premier rapport, l'état de l'interface pour le groupe affecté est comparé avant et après le dernier changement. Les enregistrements de rapport qui expriment la différence sont construits selon le tableau ci-dessus. Cependant ces enregistrements ne sont pas transmis dans un message mais plutôt fusionnés avec le contenu du rapport en instance, pour créer le nouveau rapport de changement d'état. Les règles pour la fusion du rapport de différence résultant du changement d'état et du rapport en instance sont décrites ci-dessous.

La transmission du rapport fusionné de changement d'état termine les retransmissions des rapports du changement d'état précédent pour la même adresse de diffusion groupée, et devient la première des [Variable de robustesse] transmissions de rapports de changement d'état.

Chaque fois qu'une source est incluse dans le rapport de différence calculé ci-dessus, l'état de retransmission doit être

maintenu pour cet état jusqu'à ce que [Variable de robustesse] rapports de changement d'état aient été envoyés par l'hôte. On fait cela pour assurer qu'une série de changements d'état successifs n'affaiblit pas la robustesse du protocole.

Si le changement d'état de l'interface qui déclanche le nouveau rapport est un changement de mode de filtre, les [Variable de robustesse] prochains rapports de changement d'état vont alors inclure un enregistrement Changement de mode de filtre. Cela s'applique même si un nombre quelconque de changements de liste-de-sources survient dans cette période. L'hôte doit maintenir l'état de retransmission pour le groupe jusqu'à ce qu'aient été envoyés les [Variable de robustesse] rapports de changement d'état. Lorsque [Variable de robustesse] rapports de changement d'état avec les enregistrements de Changement-de-mode-de-filtre ont été transmis après le dernier changement de mode de filtre, et si les changements de liste-de-sources à l'interface de réception ont programmé des rapports supplémentaires, le prochain rapport de changement d'état va inclure des enregistrements de Changement-de-liste-de-source.

Chaque fois qu'un rapport de changement d'état est transmis, le contenu est déterminé comme suit. Si les rapports devraient contenir un enregistrement Changement-de-mode-de-filtre, alors si le mode de filtre actuel de l'interface est INCLURE, un enregistrement TO_IN est inclus dans le rapport, autrement, un enregistrement TO_EX est inclus. Si au lieu de cela le rapport devrait contenir des enregistrements de Changement-de-liste-de-source, un enregistrement PERMET et un BLOQUE sont inclus. Le contenu de ces enregistrements est construit conformément au tableau ci-dessous :

| **Enregistrements** | **Sources incluses** |
|---|---|
| TO_IN | Tout ce qui doit être transmis dans l'état d'interface actuel |
| TO_EX | Tout ce qui doit être bloqué dans l'état d'interface actuel |
| PERMET | Tout ce qui doit être transmis dans l'état de retransmission |
| BLOQUE | Tout ce qui doit être bloqué dans l'état de retransmission |

Si la liste des sources calculée pour un enregistrement PERMET ou BLOQUE est vide, cet enregistrement est omis dans le rapport de changement d'état.

Note : Lorsque le premier rapport de changement d'état est envoyé, le rapport en instance non existant avec lequel fusionner peut être traité comme un rapport de changement de source avec des enregistrements PERMET et BLOQUE vides (aucune source n'a d'état de retransmission).

## 5.2 Action à réception d'une interrogation

Lorsque un système reçoit une interrogation, il ne répond pas immédiatement. Il retarde plutôt sa réponse d'une durée aléatoire, limitée par la valeur de Temps-de-réponse-max déduite du code de réponse maximum dans le message Interrogation reçu. Un système peut recevoir diverses interrogations sur des interfaces différentes et de différentes sortes (par exemple, Interrogations générales, Interrogations spécifiques de groupe, et Interrogations spécifiques de groupe et de source) chacune d'elles pouvant exiger sa propre réponse retardée.

Avant de programmer une réponse à une interrogation, le système doit d'abord considérer les réponses en cours précédemment programmées et dans de nombreux cas, programmer une réponse combinée. Donc, le système doit être capable de conserver l'état suivant :

- Un temporisateur par interface pour programmer les réponses aux interrogations générales.
- Un temporisateur par groupe et interface pour programmer les réponses aux interrogations spécifiques de groupe et spécifiques de groupe et de source.
- Une liste de sources par groupe et interface à rapporter dans la réponse à une interrogation spécifique de groupe et de source.

Lorsque arrive sur une interface une nouvelle interrogation avec l'option Alerte de routeur, pourvu que le système ait un état à rapporter, un retard de réponse est choisi de façon aléatoire dans la gamme (0, [Temps de réponse max]) où Temps de réponse max est déduit de Code de réponse max dans le message Interrogation reçu. Les règles suivantes sont alors utilisées pour déterminer si un rapport doit être programmé et le type de rapport à programmer. Les règles sont prises en compte dans l'ordre et seule la première règle qui correspond est appliquée.

1. Si il y a une réponse en instance à une interrogation générale antérieure programmée plus tôt que le retard choisi, aucune réponse supplémentaire n'a besoin d'être programmée.

2. Si l'interrogation reçue est une Interrogation générale, le temporisateur d'interface est utilisé pour programmer une réponse à l'interrogation générale après le retard choisi. Toute réponse en instance antérieure à une interrogation générale est annulée.

3. Si l'interrogation reçue est une interrogation spécifique de groupe ou une interrogation spécifique de groupe et de

source et si il n'y a pas de réponse en instance à une interrogation antérieure pour ce groupe, le temporisateur de groupe est alors utilisé pour programmer un rapport. Si l'interrogation reçue est une interrogation spécifique de groupe et de source, la liste des sources interrogées est enregistrée pour être utilisée lors de la génération d'une réponse.

4. Si il y a déjà en instance une réponse à une interrogation précédente programmée pour ce groupe, et si la nouvelle interrogation est une interrogation spécifique de groupe ou si la liste-de-sources enregistrée associée au groupe est vide, alors la liste-de-sources du groupe est éliminée et une seule réponse est programmée en utilisant le temporisateur de groupe. La nouvelle réponse est programmée pour être envoyée au plus tôt du temps restant pour le rapport en instance et du retard choisi.

5. Si l'interrogation reçue est une interrogation spécifique de groupe et de source, et si il y a une réponse en cours pour ce groupe avec une liste-de-sources non vide, alors la liste des sources du groupe est augmentée de façon à contenir la liste des sources de la nouvelle interrogation et une seule réponse est programmée en utilisant le temporisateur de groupe. La nouvelle réponse est programmée pour être envoyée au plus tôt du temps restant pour le rapport en instance et du retard choisi.

Lorsque le temporisateur arrive à expiration dans une réponse en instance, le système transmet, sur l'interface associée, un ou plusieurs messages Rapport qui portent un ou plusieurs enregistrements État-en-cours (voir au paragraphe 4.2.12) comme suit :

1. Si le temporisateur expiré est le temporisateur d'interface (c'est-à-dire, si c'est une réponse en instance à une interrogation générale) un enregistrement État-en-cours est alors envoyé pour chaque adresse de diffusion groupée pour laquelle l'interface spécifiée a l'état de réception, comme décrit au paragraphe 3.2. L'enregistrement État-en-cours porte l'adresse de diffusion groupée et son mode de filtre associé (MODE_EST_INCLURE ou MODE_EST_EXCLURE) et la liste des sources. Plusieurs enregistrements État-en-cours sont empaquetés dans les messages Rapport individuels, dans la mesure du possible.

   Cet algorithme enfantin peut résulter en salves de paquets lorsque un système est un membre d'un grand nombre de groupes. Au lieu d'utiliser un seul temporisateur d'interface, il est recommandé aux mises en œuvre d'étaler la transmission de tels messages Rapport sur l'intervalle (0, [Temps de réponse max]). Noter qu'une telle mise en œuvre DOIT éviter le problème de "l'explosion d'accusés de réception", c'est-à-dire, NE DOIT PAS envoyer un Rapport immédiatement à réception d'une interrogation générale.

2. Si le temporisateur qui arrive à expiration est un temporisateur de groupe et si la liste des sources enregistrées pour ce groupe est vide (c'est-à-dire, si c'est une réponse en instance à une interrogation spécifique de groupe) alors si et seulement si l'interface a l'état de réception pour cette adresse de groupe, un seul enregistrement État-en-cours est envoyé pour cette adresse. L'enregistrement État-en-cours porte l'adresse de diffusion groupée et son mode de filtre associé (MODE_EST_INCLURE ou MODE_EST_EXCLURE) et la liste des sources.

3. Si le temporisateur qui arrive à expiration est un temporisateur de groupe et si la liste des sources enregistrées pour ce groupe est non vide (c'est-à-dire, si c'est une réponse en instance à une interrogation spécifique de groupe et de source) alors si et seulement si l'interface a l'état de réception pour cette adresse de groupe, le contenu de l'enregistrement État-en-cours répondant est déterminé à partir de l'état de l'interface et de l'enregistrement de la réponse en instance, comme spécifié dans le tableau suivant :

| Ensemble de sources dans | | |
|---|---|---|
| l'état d'interface | l'enregistrement de réponse en instance | l'enregistrement État-en-cours |
| INCLURE (A) | B | IS_IN (A*B) |
| EXCLURE (A) | B | IS_IN (B-A) |

Si l'enregistrement État-en-cours résultant a un ensemble d'adresses de source vide, aucune réponse n'est alors envoyée.

Finalement, après que tous les messages Rapport exigés ont été générés, les listes des sources associées à tous les groupes rapportés sont éliminées.

## 6. Description du protocole pour les routeurs de diffusion groupée

L'objet d'IGMP est de permettre au routeur de diffusion groupée d'apprendre, pour chacun de ses réseaux directement rattachés, quelles adresses de diffusion groupée sont intéressantes pour les systèmes rattachés à ces réseaux. IGMP version 3 ajoute la capacité pour un routeur de diffusion groupée d'apprendre aussi quelles *sources* sont intéressantes

pour les systèmes du voisinage, pour les paquets envoyés à toute adresse de diffusion groupée particulière. Les informations collectées par IGMP sont fournies quel que soit le protocole d'acheminement de diffusion groupée qui est utilisé par le routeur, afin d'assurer que les paquets de diffusion groupée sont livrés à tous les réseaux où il y a des receveurs intéressés.

La présente section décrit la partie d'IGMPv3 qui est effectuée par les routeurs de diffusion groupée. Les routeurs de diffusion groupée peuvent aussi devenir eux-mêmes membres de groupes de diffusion groupée, et donc effectuer aussi la partie de membre de groupe de IGMPv3, décrite à la section 5.

Un routeur de diffusion groupée effectue le protocole décrit dans cette section sur chacun des réseaux qui lui sont directement rattachés. Si un routeur de diffusion groupée a plus d'une interface sur le même réseau, il a seulement besoin de faire fonctionner ce protocole sur une de ces interfaces. Sur chaque interface sur laquelle ce protocole fonctionne, le routeur DOIT permettre la réception de l'adresse de diffusion groupée 224.0.0.22, à partir de toutes les sources (et DOIT effectuer la partie de membre de groupe de IGMPv3 pour cette adresse sur cette interface).

Les routeurs de diffusion groupée ont besoin de savoir seulement que *au moins un* système sur un réseau rattaché est intéressé par les paquets pour une adresse de diffusion groupée particulière à partir d'une source particulière ; un routeur de diffusion groupée n'est pas obligé de garder trace de l'intérêt de chaque système individuel du voisinage. (Cependant, voir à l'Appendice A.2 la discussion du point 1.)

IGMPv3 est rétro compatible avec les versions précédentes du protocole IGMP. Afin de rester rétro compatible avec les anciens systèmes IGMP, les routeurs de diffusion groupée IGMPv3 DOIVENT aussi mettre en œuvre les versions 1 et 2 du protocole (voir la section 7).

## 6.1 Conditions pour les interrogations IGMP

Les routeurs de diffusion groupée envoient périodiquement des interrogations générales pour demander aux réseaux rattachés les informations d'adhésion aux groupes. Ces interrogations sont utilisées pour construire et rafraîchir l'état des adhésion aux groupes des systèmes sur les réseaux rattachés. Les systèmes répondent à ces interrogations en rapportant leur état d'adhésions aux groupes (et leur ensemble désiré de sources) avec les enregistrements d'état actuel de groupe dans les rapports d'adhésion IGMPv3.

En tant que membre d'un groupe de diffusion groupée, un système peut exprimer son intérêt à recevoir ou non du trafic provenant de sources particulières. Lorsque l'état de réception désiré d'un système change, il rapporte ces changements en utilisant des enregistrements Changement-de-mode-de-filtre ou Changement-de-liste-de-sources. Ces enregistrements indiquent un changement d'état explicite dans un groupe à un système dans la liste des sources de l'enregistrement du groupe ou dans son mode-filtre. Lorsque l'adhésion à un groupe est terminée sur un système ou lorsque le trafic provenant d'une source particulière n'est plus désiré, un routeur de diffusion groupée doit interroger sur les autres membres du groupe ou les écoutants de la source avant de supprimer le groupe (ou la source) et d'éliminer son trafic.

Pour permettre à tous les systèmes d'un réseau de répondre aux changements d'adhésions à un groupe, les routeurs de diffusion groupée envoient des interrogations spécifiques. Une interrogation spécifique de groupe est envoyée pour vérifier qu'il n'y a pas de système qui désire la réception du groupe spécifié ou pour "reconstruire" l'état de réception désirée pour un groupe particulier. Les interrogations spécifiques de groupe sont envoyées lorsque un routeur reçoit un enregistrement Changement d'état qui indique qu'un système quitte un groupe.

Une interrogation spécifique de groupe et de source est utilisée pour vérifier qu'il n'y a pas de système sur un réseau qui désire recevoir du trafic provenant d'un ensemble de sources. Les interrogations spécifiques de groupe et de source font pour un groupe particulier la liste des sources dont il a été demandé qu'elles ne soient plus transmises. Cette interrogation est envoyée par un routeur de diffusion groupée pour apprendre si des systèmes désirent la réception de paquets pour l'adresse de groupe spécifiée de la part des adresses de source spécifiées. Les interrogations spécifiques de groupe et de source ne sont envoyées qu'en réponse aux enregistrements Changement-d'état et jamais en réponse aux enregistrements État-en-cours. Le paragraphe 4.1.11 décrit chaque interrogation plus en détail.

## 6.2 État IGMP entretenu par les routeurs de diffusion groupée

Les routeurs de diffusion groupée qui mettent en œuvre IGMPv3 conservent l'état par groupe par réseau rattaché. Cet état de groupe consiste en un mode-filtre, une liste-de-sources, et divers temporisateurs. Pour chaque réseau rattaché qui fonctionne avec IGMP, un routeur de diffusion groupée enregistre l'état de réception désiré pour ce réseau. Conceptuellement, cet état consiste en un ensemble d'enregistrements de la forme :

(adresse de diffusion groupée, temporisateur de groupe, mode-filtre, (enregistrements de source))

Chaque enregistrement de source est de la forme :

(adresse de source, temporisateur de source)

Si toutes les sources sont désirées au sein d'un certain groupe, une liste d'enregistrements de source vide est conservée avec le mode-filtre réglé à EXCLURE. Cela signifie que les hôtes de ce réseau veulent que soient transmises toutes les sources pour ce groupe. C'est l'équivalent IGMPv3 d'une adhésion de groupe IGMPv1 ou IGMPv2.

### 6.2.1 Définition du routeur en mode filtre

Pour réduire l'état interne, les routeurs IGMPv3 conservent un mode-filtre par groupe par réseau rattaché. Ce mode-filtre est utilisé pour condenser l'état total de réception désiré d'un groupe en un ensemble minimum tel que les adhésions à tous les systèmes soient satisfaites. Ce mode-filtre peut changer en réponse à la réception d'un type particulier d'enregistrements de groupe ou lorsque certaines conditions de temporisation surviennent. Dans les paragraphes qui suivent, on utilise le terme "mode filtre de routeur" pour se référer au mode-filtre d'un groupe particulier au sein d'un routeur. Le paragraphe 6.4 décrit les changements d'un mode filtre de routeur par enregistrement de groupe reçu.

Conceptuellement, lorsque un enregistrement de groupe est reçu, le mode filtre de routeur pour ce groupe est mis à jour pour couvrir toutes les sources demandées en utilisant la plus faible quantité d'état. La règle est qu'une fois qu'est reçu un enregistrement de groupe avec un mode-filtre de EXCLURE, le mode filtre de routeur pour ce groupe sera EXCLURE.

Lorsque un mode filtre de routeur pour un groupe est EXCLURE, la liste d'enregistrements de source contient deux types de sources. Le premier type est l'ensemble qui représente les conflits dans l'état de réception désiré ; cet ensemble doit être transmis par un routeur sur le réseau. Le second type est l'ensemble des sources dont les hôtes ont demandé qu'elles ne soient pas transmises. L'Appendice A décrit les raisons de conserver ce second ensemble dans le mode EXCLURE.

Lorsque le mode filtre de routeur pour un groupe est INCLURE, la liste d'enregistrements de source est la liste des sources désirées pour le groupe. C'est l'ensemble total des sources désirées pour ce groupe. Chaque source dans la liste des enregistrements de sources doit être transmise par un routeur sur le réseau.

Comme un enregistrement de groupe rapporté avec un mode-filtre de EXCLURE va causer la transformation du mode filtre du routeur pour ce groupe en EXCLURE, un mécanisme pour ramener le mode filtre d'un routeur à INCLURE doit exister. Si tous les systèmes avec un enregistrement de groupe en mode-filtre EXCLURE cessent de faire rapport, il est souhaitable que le mode filtre de routeur pour ce groupe revienne au mode INCLURE. Cette transition survient lorsque le temporisateur de groupe expire et elle est expliquée en détails au paragraphe 6.5.

### 6.2.2 Définition des temporisateurs de groupe

Le temporisateur de groupe n'est utilisé que lorsque un groupe est en mode EXCLURE et il représente la quantité de temps au bout de laquelle le *mode-filtre* du groupe arrive à expiration et passe en mode INCLURE. On définit un temporisateur de groupe comme un temporisateur qui décrémente, avec une limite inférieure de zéro et qui est tenu par groupe et par réseau rattaché. Les temporisateurs de groupe sont mis à jour selon les types d'enregistrements de groupe reçus.

Un temporisateur de groupe qui arrive à expiration lorsque un mode filtre de routeur pour le groupe est EXCLURE signifie que sur le réseau rattaché il n'y a pas d'écoutant qui soit en mode EXCLURE. À ce moment, un routeur va passer au mode-filtre INCLURE. Le paragraphe 6.5 décrit les actions à effectuer lorsque un temporisateur de groupe expire et qu'il est en mode EXCLURE.

Le tableau suivant résume le rôle du temporisateur de groupe. Le paragraphe 6.4 décrit les détails du réglage du temporisateur de groupe par type d'enregistrement de groupe reçu.

| Mode de filtre de groupe | Valeur de temporisateur de groupe | Actions/Commentaires |
|---|---|---|
| INCLURE | Temporisateur ≥ 0 | Tous les membres en mode INCLURE. |
| EXCLURE | Temporisateur > 0 | Au moins un membre en mode EXCLURE. |
| EXCLURE | Temporisateur == 0 | Plus d'écoutant du groupe. Si tous les temporisateurs de source ont expiré, supprimer alors l'enregistrement de groupe. Si il y a encore des temporisateurs d'enregistrement de source qui fonctionnent, passer au mode-filtre INCLURE en utilisant les enregistrements de source avec des temporisateurs qui tournent comme l'état d'enregistrement de source INCLURE . |

### 6.2.3 Définition des temporisateurs de source

Un temporisateur de source est tenu pour chaque enregistrement de source et c'est un temporisateur décrémenté avec une limite inférieure de zéro. Les temporisateurs de source sont mis à jour en fonction du type et du mode-filtre de l'enregistrement de groupe reçu. Les temporisateurs de source sont toujours mis à jour (pour un groupe particulier) chaque fois que la source est présente dans un enregistrement reçu pour ce groupe. Le paragraphe 6.4 décrit le réglage des temporisateurs de source par type d'enregistrements de groupe reçu.

Un enregistrement de source avec un temporisateur qui fonctionne avec un mode filtre de routeur pour le groupe de INCLURE signifie qu'il y a actuellement un ou plusieurs systèmes (en mode-filtre INCLURE) qui désirent recevoir cette source. Si un temporisateur de source expire avec un mode filtre de routeur pour le groupe de INCLURE, le routeur en conclut que le trafic provenant de cette source n'est plus désiré sur le réseau rattaché, et supprime l'enregistrement de source associé.

Les temporisateurs de source sont traités différemment lorsque le mode filtre de routeur pour un group est EXCLURE. Si un enregistrement de source a un temporisateur en cours avec un mode filtre de routeur pour le groupe de EXCLURE, cela signifie qu'au moins un système désire la source. Il devrait donc être transmis par un routeur sur le réseau. L'Appendice A décrit les raisons de conservation de l'état pour les sources dont la transmission a été demandée alors que l'état est EXCLURE.

Si un temporisateur de source expire avec un mode filtre de routeur pour le groupe de EXCLURE, le routeur informe le protocole d'acheminement qu'il n'y a plus sur le réseau de receveur intéressé par le trafic provenant de cette source.

Lorsque le mode filtre de routeur pour un groupe est EXCLURE, les enregistrements de source ne sont supprimés que lorsque le temporisateur de groupe expire. Le paragraphe 6.3 décrit les actions qui devraient être entreprises selon la valeur du temporisateur de source.

## 6.3 Règles de transmission spécifiques de source pour IGMPv3

Lorsque un routeur de diffusion groupée reçoit un datagramme provenant d'une source destinée à un groupe particulier, il faut qu'il prenne une décision pour savoir si il faut transmettre ou non le datagramme sur un réseau rattaché. Le protocole d'acheminement de diffusion groupée utilisé est chargé de cette décision, et devrait utiliser les informations d'IGMPv3 pour s'assurer que toutes les sources/groupes désirés sur un sous-réseau sont transmis à ce sous-réseau. Les informations de IGMPv3 n'outrepassent pas les informations d'acheminement de diffusion groupée ; par exemple, si le mode-filtre de groupe IGMPv3 pour G est EXCLURE, un routeur peut quand même transmettre des paquets pour des sources exclues à un sous-réseau de transit.

Pour résumer, le tableau qui suit décrit les suggestions de transmission faites par IGMP au protocole d'acheminement pour le trafic généré par une source et destiné à un groupe. Il résume aussi les actions effectuées à l'expiration d'un temporisateur de source sur la base du mode de filtre du routeur du groupe.

| Mode de filtre du groupe | Valeur du temporisateur de source | Action |
|---|---|---|
| INCLURE | Temporisateur > 0 | Suggère de transmettre le trafic de la source. |
| INCLURE | Temporisateur == 0 | Suggère d'arrêter de transmettre le trafic de la source et de retirer l'enregistrement de source. Si il n'y a plus d'enregistrement de source pour le groupe, supprimer l'enregistrement de groupe. |
| INCLURE | Pas d'élément source | Suggère de ne pas transmettre la source |
| EXCLURE | Temporisateur > 0 | Suggère de transmettre le trafic de la source. |
| EXCLURE | Temporisateur == 0 | Suggère de ne pas transmettre le trafic de la source (NE PAS retirer l'enregistrement) |
| EXCLURE | Pas d'élément source | Suggère de transmettre le trafic de la source. |

## 6.4 Action à réception des rapports

### 6.4.1 Réception des rapports sur l'état en cours

À réception d'enregistrements État-en-cours, un routeur met à jour son groupe et son temporisateur de sources. Dans certaines circonstances, la réception d'un type d'enregistrement de groupe va être cause que le mode filtre de routeur pour ce groupe change. Le tableau ci-dessous décrit les actions, par rapport à l'état et aux temporisateurs, que subit l'état d'un routeur à réception d'enregistrements État-en-cours.

La notation suivante est utilisée pour décrire la mise à jour des temporisateurs de source. La notation ( A, B ) sera utilisée pour représenter le nombre total de sources pour un groupe particulier, où

A = ensemble des enregistrements de source dont le temporisateur de source > 0 (Les sources dont au moins un hôte a demandé la transmission).

B = ensemble des enregistrements de source dont le temporisateur de source = 0 (Sources que IGMP va suggérer au protocole d'acheminement de ne pas transmettre).

Noter qu'il y aura seulement deux ensembles lorsque le mode-filtre d'un routeur pour un groupe est EXCLURE. Lorsque le mode-filtre d'un routeur pour un groupe est INCLURE, un seul ensemble est utilisé pour décrire l'ensemble des sources dont la transmission est demandée (par exemple, simplement (A)).

Dans les tableaux suivants, des abréviations sont utilisées pour plusieurs variables (qui sont toutes décrites en détail à la section 8). La variable GMI est une abréviation pour l'intervalle d'adhésion de groupe *(Group Membership Interval)* qui est le temps qui va s'écouler jusqu'à l'arrivée à expiration de l'adhésion de groupe. La variable LMQT est l'abréviation du temps écoulé depuis la dernière interrogation d'un membre *(Last Member Query Time)* qui est le temps total écoulé depuis la dernière retransmission du compte de la dernière interrogation de membre. LMQT représente la "latence de départ", ou la différence entre la transmission d'un changement d'adhésion et le changement des informations données au protocole d'acheminement.

Dans la colonne "Actions" des tableaux d'état du routeur, on utilise la notation 'A = J', qui signifie que l'ensemble A des enregistrements de source devrait avoir ses temporisateurs de source réglés à la valeur J. 'Supprimer A' signifie que l'ensemble A d'enregistrements de source devrait être supprimé. 'Temporisateur de groupe = J' signifie que le temporisateur de groupe pour le groupe devrait être réglé à la valeur J.

| **État du routeur** | **Rapport reçu** | **Nouvel état du routeur** | **Actions** |
|---|---|---|---|
| INCLURE (A) | IS_IN (B) | INCLURE (A+B) | (B) = GMI |
| INCLURE (A) | IS_EX (B) | EXCLURE (A*B,B-A) | (B-A) = 0 |
| | | Supprimer (A-B) | |
| | | Temporisateur de groupe = GMI | |
| EXCLURE (X,Y) | IS_IN (A) | EXCLURE (X+A,Y-A) | (A) = GMI |
| EXCLURE (X,Y) | IS_EX (A) | EXCLURE (A-Y,Y*A) | (A-X-Y) = GMI |
| | | Supprimer (X-A) | |
| | | Supprimer (Y-A) | |
| | | Temporisateur de groupe r=GMI | |

### 6.4.2 Réception des rapports de changement de mode de filtre et de changement de liste de source

Lorsque un changement de l'état global d'un groupe survient dans un système, le système envoie un enregistrement Changement-de-liste-de-sources ou Changement-de-mode-de-filtre pour ce groupe. Comme avec un enregistrement État-en-cours, les routeurs doivent agir sur ces enregistrements et éventuellement changer leur propre état pour refléter le nouvel état d'adhésion désiré du réseau.

Les routeurs doivent interroger les sources dont il est demandé qu'elles ne soient plus transmises à un groupe. Lorsque un routeur interroge ou reçoit une interrogation pour un ensemble spécifique de sources, il diminue son temporisateur de sources pour ces sources jusqu'à un petit intervalle de [Temps-d'interrogation-du-dernier-membre] secondes. Si des enregistrements de groupe sont reçus en réponse aux interrogations qui expriment un intérêt à recevoir du trafic des sources interrogées, les temporisateurs correspondants sont mis à jour.

De même, lorsque un routeur interroge un groupe spécifique, il diminue son temporisateur de groupe pour ce groupe jusqu'à un petit intervalle de [Temps-d'interrogation-du-dernier-membre] secondes. Si des enregistrements de groupe exprimant un intérêt de mode EXCLURE pour le groupe sont reçus dans l'intervalle, le temporisateur de groupe pour le groupe est mis à jour et la suggestion au protocole d'acheminement de transmettre au groupe tient sans aucune interruption.

Durant une période d'interrogation (c'est-à-dire, pendant [Temps-d'interrogation-du-dernier-membre] secondes) le composant IGMP dans le routeur continue de suggérer au protocole d'acheminement qu'il transmette le trafic provenant des groupes ou sources qu'il interroge. Ce n'est qu'après [Temps-d'interrogation-du-dernier-membre] secondes sans recevoir d'enregistrement exprimant de l'intérêt pour le groupe ou les sources interrogés que le routeur peut éliminer le groupe ou les sources du réseau.

Le tableau suivant décrit les changements de l'état de groupe et la ou les actions entreprises lors de la réception d'enregistrements Changement-de-mode-de-filtre ou Changement-de-liste-de-sources. Ce tableau décrit aussi les interrogations qui sont envoyées par l'interrogateur lorsque un rapport particulier est reçu.

On utilise la notation suivante pour décrire les interrogations qui sont envoyées. On note 'Q(G)' pour décrire une interrogation spécifique de groupe à G. On note 'Q(G,A)' pour décrire une interrogation spécifique de groupe et de source à G avec liste-de-sources A. Si liste-de-sources A est nul par suite de l'action (par exemple, A*B) aucune interrogation n'est alors envoyée par suite de l'opération.

Afin de conserver la robustesse du protocole, les interrogations envoyées par les actions dans le tableau ci-dessous doivent être transmises [Compte-d'interrogation-du-dernier-membre] fois, une fois tous les [Intervalle-d'interrogation-du-dernier-membre].

Si lors de la programmation de nouvelles interrogations il y a déjà des interrogations en instance à retransmettre pour le même groupe, les nouvelles interrogations et celles en instance doivent être fusionnées. De plus, les rapports d'hôte reçus pour un groupe alors que des interrogations sont en instance peuvent affecter le contenu de ces interrogations. Le paragraphe 6.6.3 décrit le processus de construction et de maintenance de l'état des interrogations en instance.

| **État de routeur** | **Rapport reçu** | **Nouvel état de routeur** | **Actions** |
|---|---|---|---|
| INCLURE (A) | PERMET (B) | INCLURE (A+B) | (B) = GMI |
| INCLURE (A) | BLOQUE (B) | INCLURE (A) | Envoie Q(G,A*B) |
| INCLURE (A) | TO_EX (B) | EXCLURE (A*B,B-A)<br>Supprime (A-B)<br>Envoie Q(G,A*B)<br>Temporisateur de groupe =GMI | (B-A) = 0 |
| INCLURE (A) | TO_IN (B) | INCLURE (A+B)<br>Envoie Q(G,A-B) | (B) = GMI |
| EXCLURE (X,Y) | PERMET (A) | EXCLURE (X+A,Y-A) | (A) = GMI |
| EXCLURE (X,Y) | BLOQUE (A) | EXCLURE (X+(A-Y),Y)<br>Envoie Q(G,A-Y) | (A-X-Y) = Temporisateur de groupe |
| EXCLURE (X,Y) | TO_EX (A) | EXCLURE (A-Y,Y*A)<br>Supprime (X-A)<br>Supprime (Y-A)<br>Envoie Q(G,A-Y)<br>Temporisateur de groupe =GMI | (A-X-Y) = Temporisateur de groupe |
| EXCLURE (X,Y) | TO_IN (A) | EXCLURE (X+A,Y-A)<br>Envoie Q(G,X-A)<br>Envoie Q(G) | (A) = GMI |

## 6.5 Changement des modes de filtre de routeur

Le temporisateur de groupe est utilisé comme mécanisme de transition du mode-filtre du routeur de EXCLURE en INCLURE.

Lorsque un temporisateur de groupe expire avec un mode filtre de routeur de EXCLURE, un routeur suppose qu'il n'y a pas de système avec un *mode-filtre* de EXCLURE présent sur le réseau rattaché. Lorsque le mode-filtre d'un routeur pour un groupe est EXCLURE et que le temporisateur de groupe arrive à expiration, le mode-filtre de routeur pour le groupe passe à INCLURE.

Un routeur utilise les enregistrements de source avec un temporisateur de sources lorsque son état passe à un mode-filtre de INCLURE. Si il y a des enregistrements de source avec un temporisateur de sources supérieur à zéro (c'est-à-dire, dont la transmission est demandée) un routeur passe au mode-filtre de INCLURE en utilisant ces enregistrements de source. Les enregistrements de source dont le temporisateur est à zéro (depuis le précédent mode EXCLURE) sont supprimés.

Par exemple, si l'état d'un routeur pour un groupe est EXCLURE(X,Y) et si le temporisateur de groupe arrive à expiration pour ce groupe, le routeur passe au mode-filtre de INCLURE avec l'état INCLURE(X).

## 6.6 Action à réception des interrogations

### 6.6.1 Mise à jour de temporisateur

Lorsque un routeur envoie ou reçoit une interrogation avec un clair fanion Supprimer-le-traitement-côté-routeur, il doit mettre à jour ses temporisateurs pour refléter les valeurs de temporisation correctes pour le groupe ou sources interrogé. Le tableau qui suit décrit les actions de temporisation lors de l'envoi ou la réception d'une interrogation spécifique de groupe ou interrogation spécifique de groupe et de source avec le fanion Supprimer-le-traitement-côté-routeur non établi *(mis à zéro)*.

| Interrogation | Action |
|---|---|
| Q(G,A) | Les temporisateurs de source pour les sources dans A sont abaissés au LMQT |
| Q(G) | Le temporisateur de groupe est abaissé au LMQT |

Lorsque un routeur envoie ou reçoit une interrogation avec le fanion Supprimer-le-traitement-côté-routeur établi *(à un)*, il ne met pas ses temporisateurs à jour.

### 6.6.2 Choix de l'interrogateur

IGMPv3 désigne un seul interrogateur par sous réseau en utilisant le même mécanisme de choix d'interrogateur que IGMPv2, à savoir par l'adresse IP. Lorsque un routeur reçoit une interrogation avec une adresse IP inférieure, il règle le temporisateur Autre-interrogateur-présent à l'intervalle Autre-interrogateur-présent et cesse d'envoyer des interrogations sur le réseau si c'est l'interrogateur qui avait été choisi précédemment. Après l'expiration du temporisateur Autre-interrogateur-présent, il devrait commencer à envoyer des interrogations générales.

Si un routeur reçoit une interrogation d'une plus ancienne version, il DOIT utiliser cette plus ancienne version d'IGMP sur le réseau. Pour une description détaillée des questions de compatibilité entre les versions d'IGMP, voir à la section 7.

### 6.6.3 Construction et envoi d'interrogations spécifiques

#### 6.6.3.1 Construction et envoi d'interrogations spécifiques de groupe

Lorsque se rencontre une action "Envoie Q(G)" du tableau, le temporisateur de groupe doit alors être diminué à LMQT. Le routeur doit alors immédiatement envoyer une interrogation spécifique de groupe et programmer [Compte-d'interrogation-du-dernier-membre - 1] retransmissions d'interrogation à envoyer tous les [Intervalle-d'interrogation-du-dernier-membre] pendant [Temps-d'interrogation-du-dernier-membre].

Lors de la transmission d'une interrogation spécifique de groupe, si le temporisateur de groupe est plus grand que LMQT, le bit "Supprimer le traitement côté routeur" est établi dans le message d'interrogation.

#### 6.6.3.2 Construction et envoi d'interrogations spécifiques de groupe et de source

Lorsque un interrogateur rencontre une action "Envoie Q(G,X)" du tableau du paragraphe 6.4.2, les actions suivantes doivent être effectuées pour chacune des sources en X du groupe G, avec un temporisateur de source supérieur au LMQT :

- o régler le nombre de retransmissions pour chaque source à [Compte-d'interrogation-du-dernier-membre].
- o diminuer le temporisateur de source au LMQT.

Le routeur doit alors immédiatement envoyer une interrogation spécifique de groupe et de source ainsi que programmer [Compte-d'interrogation-du-dernier-membre - 1] retransmissions d'interrogation à envoyer tous les [Intervalle-d'interrogation-du-dernier-membre] pendant [Temps-d'interrogation-du-dernier-membre]. Le contenu de ces interrogations est calculé de la façon suivante. Quand on construit une interrogation spécifique de groupe et de source pour un groupe G, deux messages d'interrogation distincts sont envoyés pour le groupe. Le premier a le bit "Supprimer le traitement côté routeur" établi et contient toutes les sources qui ont leur état de retransmission et leur temporisateur supérieur au LMQT. Le second a le bit "Supprimer le traitement côte routeur" à zéro et contient toutes les sources qui ont l'état de retransmission et le temporisateur inférieur ou égal au LMQT. Si l'un ou l'autre des deux messages calculés ne contient aucune source, sa transmission est alors supprimée.

Note : Si une interrogation spécifique de groupe est programmée pour être transmise en même temps qu'une interrogation spécifique de groupe et de source pour le même groupe, la transmission du message spécifique de groupe et de source avec le bit "Supprimer le traitement côte routeur" établi peut être supprimée.

# 7. Interopération avec d'anciennes versions d'IGMP

Les hôtes et routeurs IGMP version 3 interopèrent avec les hôtes et routeurs qui n'ont pas encore été mis à niveau avec IGMPv3. Cette compatibilité est maintenue par les hôtes et routeurs en prenant les actions appropriées selon les versions de IGMP qui fonctionnent sur les hôtes et routeurs au sein d'un réseau.

## 7.1 Distinctions de version d'interrogation

La version IGMP d'un message d'interrogation sur les membres est déterminée comme suit :
Interrogation IGMPv1 : longueur = 8 octets ET champ Code de réponse max de zéro
Interrogation IGMPv2 : longueur = 8 octets ET champ Code de réponse max différent de zéro
Interrogation IGMPv3 : longueur ≥ 12 octets

Les messages Interrogation qui ne correspondent à aucune des conditions ci-dessus (par exemple, une interrogation d'une longueur de 10 octets) DOIVENT être ignorés en silence.

## 7.2 Comportement de membre de groupe

### 7.2.1 En présence d'interrogateurs de version plus ancienne

Afin d'être compatibles avec les routeurs de version plus ancienne, les hôtes IGMPv3 DOIVENT fonctionner en mode de compatibilité de version 1 et version 2. Les hôtes IGMPv3 DOIVENT garder l'état par interface locale en ce qui concerne le mode de compatibilité de chaque réseau rattaché. Le mode de compatibilité d'un hôte est déterminé à partir de la variable Mode de compatibilité d'hôte qui peut être un des trois états suivants : IGMPv1, IGMPv2 ou IGMPv3. Cette variable est conservée par interface et dépend de la version des interrogations générales entendues sur cette interface ainsi que des temporisateurs de présence d'interrogateur de version plus ancienne pour cette interface.

Afin de passer en douceur d'une version de IGMP à l'autre, les hôtes conservent à la fois le temporisateur Interrogateur de IGMPv1 présent et un temporisateur Interrogateur de IGMPv2 présent par interface. Interrogateur IGMPv1 présent est réglé à [Temporisation de présence d'interrogateur d'ancienne version] secondes chaque fois qu'une interrogation d'adhésion IGMPv1 est reçue. Interrogateur IGMPv2 présent est réglé à [Temporisation de présence d'interrogateur de plus ancienne version] secondes chaque fois qu'une interrogation générale IGMPv2 est reçue.

Le mode de compatibilité d'hôte d'une interface change chaque fois qu'une interrogation de plus ancienne version (que le mode de compatibilité actuel) est entendue ou quant certaines conditions de temporisateur surviennent. Lorsque le temporisateur Interrogateur IGMPv1 présent arrive à expiration, un hôte passe au mode de compatibilité d'hôte de IGMPv2 si il a un temporisateur Interrogateur IGMPv2 présent en cours. Si il n'en a pas, il passe alors à la compatibilité d'hôte de IGMPv3. Lorsque le temporisateur Interrogateur IGMPv2 présent arrive à expiration, un hôte passe au mode de compatibilité de IGMPv3.

La variable Mode de compatibilité d'hôte se fonde sur la question de savoir si une interrogation générale d'ancienne version a été entendue dans les dernières Temporisation-de-présence-d'interrogateur-d'ancienne-version secondes. Le mode de compatibilité d'hôte est réglé selon ce qui suit :

| Mode de compatibilité d'hôte | État du temporisateur |
|---|---|
| IGMPv3 (par défaut) | Interrogateur IGMPv2 présent ne court pas et interrogateur IGMPv1 présent ne court pas |
| IGMPv2 | Interrogateur IGMPv2 présent court et interrogateur IGMPv1 présent ne court pas |
| IGMPv1 | Interrogateur IGMPv1 présent court |

Si un hôte reçoit une interrogation qui cause la mise à jour de ses temporisateurs Interrogateur présent et de son mode de compatibilité correspondant, il devrait changer immédiatement ses modes de compatibilité.

Lorsque le mode de compatibilité d'hôte est IGMPv3, un hôte agit en utilisant le protocole IGMPv3 sur cette interface. Lorsque le mode de compatibilité d'hôte est IGMPv2, un hôte agit en mode de compatibilité IGMPv2, en utilisant seulement le protocole IGMPv2 sur cette interface. Lorsque le mode de compatibilité d'hôte est IGMPv1, un hôte agit en mode de compatibilité IGMPv1, en utilisant seulement le protocole IGMPv1 sur cette interface.

Un routeur IGMPv1 va envoyer des interrogations générales avec le code de réponse max réglé à 0. Cela DOIT être interprété comme une valeur de 100 (10 secondes).

Un routeur IGMPv2 va envoyer des interrogations générales avec le code de réponse max réglé au Temps de réponse max désiré, c'est-à-dire, toute la gamme de ce champ est linéaire et l'algorithme exponentiel décrit au paragraphe 4.1.1 n'est pas utilisé.

Chaque fois qu'un hôte change son mode de compatibilité, il annule tous ses temporisateurs de réponse et retransmission en cours.

### 7.2.2 En présence de membres de groupe de version plus ancienne

Un hôte IGMPv3 peut être placé sur un réseau où il y a des hôtes qui n'ont pas encore été mis à niveau avec IGMPv3. Un hôte PEUT permettre que soit supprimé son enregistrement d'adhésion IGMPv3 par un rapport d'adhésion de version 1, ou par un rapport d'adhésion de version 2.

## 7.3 Comportement de routeur de diffusion groupée

### 7.3.1 En présence d'interrogateurs de version plus ancienne

Les routeurs IGMPv3 peuvent être placés sur un réseau où au moins un routeur sur le réseau n'a pas encore été mis à niveau avec IGMPv3. Les exigences suivantes s'appliquent :

- Si une des plus anciennes versions de IGMP est présente sur les routeurs, l'interrogateur DOIT utiliser la plus basse version de IGMP présente sur le réseau. Cela doit être assuré administrativement ; les routeurs qui désirent être compatibles avec IGMPv1 et IGMPv2 DOIVENT avoir une option de configuration pour agir en mode de compatibilité IGMPv1 ou IGMPv2. En mode IGMPv1, les routeurs DOIVENT envoyer des interrogations périodiques avec un Code de réponse max de 0 et tronquées au champ Adresse de groupe (c'est-à-dire, longues de 8 octets) et DOIVENT ignorer les messages Groupe quitté. Ils DEVRAIENT aussi mettre en garde contre la réception d'une interrogation IGMPv2 ou IGMPv3, mais une telle mise en garde DOIT être limitée en débit. En mode IGMPv2, les routeurs DOIVENT envoyer des interrogations périodiques tronquées au champ Adresse de groupe (c'est-à-dire, longues de 8 octets) et DEVRAIENT aussi mettre en garde contre la réception d'une interrogation IGMPv3 (de telles mises en garde DOIVENT être limitées en débit). Ils DOIVENT aussi remplir le Temps de réponse max dans le champ Code de réponse max, c'est-à-dire que l'algorithme exponentiel décrit au paragraphe 4.1.1 n'est pas utilisé.

- Si un routeur n'est pas explicitement configuré pour utiliser IGMPv1 ou IGMPv2 et entend une interrogation IGMPv1 ou une interrogation générale IGMPv2, il DEVRAIT enregistrer un avertissement dans son journal. Ces avertissements DOIVENT être limités en débit.

### 7.3.2 En présence de membres de groupe de version plus ancienne

Les routeurs IGMPv3 peuvent être placés sur un réseau où il y a des hôtes qui n'ont pas encore été mis à niveau avec IGMPv3. Afin d'être compatibles avec les plus anciennes versions d'hôtes, les routeurs IGMPv3 DOIVENT fonctionner en modes de compatibilité version 1 et version 2. Les routeurs IGMPv3 tiennent un mode de compatibilité par enregistrement de groupe. Le mode de compatibilité d'un groupe est déterminé à partir de la variable Mode de compatibilité de groupe qui peut être dans un des trois états IGMPv1, IGMPv2 ou IGMPv3. Cette variable est tenue par enregistrement de groupe et dépend de la version des rapports d'adhésion entendus pour ce groupe ainsi que du temporisateur Ancienne-version-d'hôte-présente pour le groupe.

Afin de passer en douceur d'une version d'IGMP à l'autre, les routeurs tiennent un temporisateur Hôte-IGMPv1-présent et un temporisateur Hôte-IGMPv2-présent par enregistrement de groupe. Le temporisateur Hôte-IGMPv1-présent est réglé à Temporisation-d'ancienne-version-d'hôte-présent secondes chaque fois qu'un rapport d'adhésion IGMPv1 est reçu. Le temporisateur Hôte-IGMPv2-présent est réglé à Temporisation-d'ancienne-version-d'hôte-présent secondes chaque fois qu'un rapport d'adhésion IGMPv2 est reçu.

Le mode de compatibilité de groupe d'un enregistrement de groupe change chaque fois qu'un rapport de version plus ancienne (que celle du mode de compatibilité en cours) est entendu ou quand surviennent certaines conditions de temporisateur. Lorsque le temporisateur Hôte-IGMPv1-présent arrive à expiration, un routeur passe au mode de compatibilité de groupe IGMPv2 si il a un temporisateur Hôte-IGMPv2-présent en cours. Si il n'en a pas, il passe alors à la compatibilité de groupe IGMPv3. Lorsque le temporisateur Hôte-IGMPv2-présent arrive à expiration et que le temporisateur Hôte-IGMPv1-présent ne court pas, un routeur passe en mode de compatibilité de groupe IGMPv3. Noter que lorsque un groupe repasse en mode IGMPv3, il lui faut un certain temps pour retrouver ses informations d'état spécifique de source. Les informations spécifiques de source seront apprises durant la prochaine interrogation générale, mais les sources qui devraient être bloquées ne le seront pas pendant [Intervalle-d'adhésion-de-groupe] après cela.

La variable Mode de compatibilité de groupe se fonde sur le fait qu'un rapport de plus ancienne version a été entendu dans les dernières Temporisation-de-présence-d'hôte-d'ancienne-version secondes. Le réglage du mode de compatibilité de groupe dépend du tableau suivant :

| Mode de compatibilité de groupe | État du temporisateur |
|---|---|
| IGMPv3 (par défaut) | Hôte-IGMPv2-présent ne court pas et Hôte-IGMPv1-présent ne court pas |
| IGMPv2 | Hôte-IGMPv2-présent court et Hôte-IGMPv1-présent ne court pas |
| IGMPv1 | Hôte-IGMPv1-présent court |

Si un routeur reçoit un rapport qui cause la mise à jour de ses temporisateurs Présence-d'hôte-d'ancienne-version et de son mode de compatibilité correspondant, il DEVRAIT changer immédiatement les modes de compatibilité.

Lorsque le mode de compatibilité de groupe est IGMPv3, un routeur agit en utilisant le protocole IGMPv3 pour ce groupe.

Lorsque le mode de compatibilité de groupe est IGMPv2, un routeur traduit en interne les messages IGMPv2 suivants pour ce groupe en leurs équivalents IGMPv3 :

| Message IGMPv2 | Équivalent IGMPv3 |
|---|---|
| Rapport | IS_EX( {} ) |
| Quitte | TO_IN( {} ) |

Les messages IGMPv3 BLOQUE sont ignorés, car ils sont des liste-de-sources dans les messages TO_EX() (c'est-à-dire que tout message TO_EX() est traité comme TO_EX( {} )).

Lorsque le mode de compatibilité de groupe est IGMPv1, un routeur traduit en interne les messages IGMPv1 et IGMPv2 suivants pour ce groupe en leurs équivalents IGMPv3 :

| Message IGMP | Équivalent IGMPv3 |
|---|---|
| Rapport v1 | IS_EX( {} ) |
| Rapport v2 | IS_EX( {} ) |

En plus d'ignorer les messages IGMPv3 BLOQUE et liste-de-sources dans les messages TO_EX() comme dans le mode de compatibilité de groupe IGMPv2, les messages IGMPv2 Quitte et les messages IGMPv3 TO_IN() sont aussi ignorés.

## 8. Liste des temporisateurs et compteurs, et valeurs par défaut

La plupart de ces temporisateurs sont configurables. Si des réglages autres que par défaut sont utilisés, ils DOIVENT être cohérents pour tous les systèmes sur une liaison. Noter que des parenthèses sont utilisées pour grouper les expressions afin de rendre l'algèbre claire.

### 8.1 Variable de robustesse

La variable de robustesse permet un réglage de la perte de paquet attendue sur un réseau. Si on s'attend à ce qu'un réseau soit enclin aux pertes, la variable de robustesse peut être augmentée. IGMP est robuste à (Variable-de-robustesse - 1) perte de paquets. La variable de robustesse NE DOIT PAS être zéro, et NE DEVRAIT PAS être un. Par défaut : 2

### 8.2 Intervalle-d'interrogation

L'intervalle d'interrogation est l'intervalle entre les interrogations générales envoyées par l'interrogateur. Par défaut : 125 s.

En faisant varier [Intervalle d'interrogation], un administrateur peut limiter le nombre de messages IGMP sur le réseau ; les valeurs plus élevées font que les Interrogations IGMP sont envoyées moins souvent.

### 8.3 Intervalle-de-réponse-d'interrogation

C'est le Temps-de-réponse-max utilisé pour calculer le Code-de-réponse-max inséré dans les interrogations générales périodiques. Par défaut : 100 (10 secondes)

En faisant varier [Intervalle de réponse aux interrogations], un administrateur peut régler la sporadicité des messages IGMP sur le réseau ; les plus grandes valeurs rendent le trafic moins sporadique, car les réponses des hôtes sont étalées sur un plus grand intervalle. Le nombre de secondes représenté par [Intervalle de réponse aux interrogations] doit être inférieur à celui de [Intervalle d'interrogation].

### 8.4 Intervalle-d'adhésion-de-groupe

L'intervalle d'adhésion de groupe est la quantité de temps qui doit s'écouler avant qu'un routeur de diffusion groupée décide qu'il n'y a plus de membre d'un groupe ou d'une certaine source sur un réseau.

Cette valeur DOIT être ((Variable-de-robustesse) fois (Intervalle-d'interrogation)) plus (Intervalle-de-réponse-d'interrogation).

### 8.5. Intervalle-de-autre-interrogateur-présent

Intervalle-de-autre-interrogateur-présent est la durée qui doit s'écouler avant qu'un routeur de diffusion groupée décide qu'il n'y a plus d'autre routeur de diffusion groupée qui devrait être l'interrogateur. Cette valeur DOIT être ((Variable-de-robustesse) fois (Intervalle-d'interrogation)) plus (moitié de Intervalle-de-réponse-d'interrogation).

### 8.6 Intervalle-d'interrogation-de-démarrage

L'Intervalle-d'interrogation-de-démarrage est l'intervalle entre les interrogations générales envoyées par un interrogateur au démarrage. Par défaut : 1/4 de l'intervalle d'interrogation.

### 8.7 Compte-d'interrogation-de-démarrage

Le Compte-d'interrogation-de-démarrage est le nombre d'interrogations envoyées au démarrage, séparées par l'intervalle d'interrogation de démarrage. Par défaut : la variable de robustesse.

### 8.8 Intervalle-d'interrogation-de-dernier-membre

L'Intervalle-d'interrogation-de-dernier-membre est le Temps-de-réponse-max utilisé pour calculer le Code-de-réponse-max inséré dans les interrogations spécifiques de groupe envoyées en réponse aux messages Quitter-groupe. C'est aussi le Temps-de-réponse-max utilisé pour le calcul du Code-de-réponse-max pour les messages Interrogation-spécifique-de-groupe-et-de-source. Par défaut : 10 (1 seconde).

Noter que pour les valeurs de LMQI supérieures à 12,8 seconde, un ensemble limité de valeurs peut être représenté, correspondant à la séquence des valeurs de Code-de-réponse-max. Lorsque on convertit une durée configurée en valeur de Code-de-réponse-max, il est recommandé d'utiliser la valeur exacte si possible, ou la valeur inférieure la plus proche si la valeur demandée n'est pas exactement représentable.

Cette valeur peut être réglé pour modifier la "latence de départ" du réseau. Une valeur réduite résulte en une durée réduite pour détecter la perte du dernier membre d'un groupe ou de la dernière source.

### 8.9 Compte d'interrogation de dernier membre

Le compte d'interrogation de dernier membre est le nombre d'interrogations spécifiques de groupe envoyées avant que le routeur suppose qu'il n'y a plus de membre local. Le compte d'interrogation de dernier membre est aussi le nombre d'interrogations spécifiques de groupe et de source envoyées avant que le routeur suppose qu'il n'y a plus d'écoutant pour une source particulière. Par défaut : la variable de robustesse.

### 8.10 Temps d'interrogation du dernier membre

Le temps d'interrogation du dernier membre est la valeur du temps représenté par l'intervalle d'interrogation du dernier membre, multipliée par le compte d'interrogation de dernier membre. Ce n'est pas une valeur réglable mais elle peut être réglée en changeant ses composants.

### 8.11 Intervalle de rapport non sollicité

L'intervalle de rapport non sollicité est la durée entre les répétitions du rapport initial d'adhésions à un groupe d'un hôte. Par défaut : 1 seconde.

### 8.12 Temporisation de présence d'un interrogateur de version ancienne

L'intervalle d'interrogateur d'ancienne version est la temporisation pour la transition d'un hôte pour retourner au mode IGMPv3 une fois qu'il a entendu une interrogation d'ancienne version. Lorsque une interrogation d'une ancienne version est reçue ; les hôtes règlent leur temporisateur de présence d'un interrogateur de version ancienne à Intervalle d'interrogateur d'ancienne version.

Cette valeur DOIT être ((Variable de robustesse) fois (Intervalle d'interrogation dans la dernière interrogation reçue)) plus (un Intervalle de réponse d'interrogation).

### 8.13 Intervalle de présence d'un ancien hôte

L'intervalle de présence d'un ancien hôte est la temporisation pour la transition d'un groupe pour retourner au mode IGMPv3 une fois qu'un rapport de version ancienne est envoyé pour ce groupe. Lorsque un rapport de version ancienne est reçu, les routeurs règlent leur temporisateur de présence d'un ancien hôte à Intervalle-de-présence-d'un-ancien-hôte.

Cette valeur DOIT être ((Variable de robustesse) fois (Intervalle d'interrogation)) plus (un intervalle de réponse d'interrogation).

## 8.14 Configuration des temporisateurs

Ce paragraphe est destiné à donner des conseils aux administrateurs de réseau sur la façon de régler ces paramètres sur leur réseau. Les mises en œuvre de routeur ambitieuses peuvent régler de façon dynamique ces paramètres sur la base des changements de caractéristiques du réseau.

### 8.14.1 Variable de robustesse

La variable de robustesse règle IGMP au niveau de pertes attendu sur une liaison. IGMPv3 est robuste à (Variable de robustesse - 1) pertes de paquet , par exemple, si la variable de robustesse est réglée à la valeur par défaut de 2, IGMPv3 est robuste à la perte d'un seul paquet mais peut fonctionner de façon imparfaite si plus d'une perte survient. Sur des sous-réseaux enclins aux pertes, la variable de robustesse devrait être augmentée pour permettre le niveau de perte de paquet attendu. Cependant, augmenter la variable de robustesse augmente la latence de départ du sous-réseau. (La latence de départ est la durée entre le moment où le dernier membre cesse d'écouter une source ou groupe et celui où le trafic cesse de s'écouler.)

### 8.14.2 Intervalle d'interrogation

Le niveau global du trafic périodique IGMP est inversement proportionnel à l'intervalle d'interrogation. Un plus long intervalle d'interrogation résulte en un niveau global inférieur du trafic IGMP. L'intervalle d'interrogation DOIT être égal à, ou plus long que, le temps de réponse max inséré dans les messages Interrogation générale.

### 8.14.3 Temps de réponse maximal

La sporadicité du trafic IGMP est inversement proportionnelle au temps de réponse max. Un plus long temps de réponse max va étaler les messages Rapport sur un plus long intervalle. Cependant, un plus long temps de réponse max dans les interrogations spécifiques de groupe et spécifiques de source et de groupe étend la latence de départ. (La latence de départ est la durée entre le moment où le dernier membre cesse d'écouter une source ou groupe et celui où le trafic cesse de s'écouler.) Le taux attendu de messages Rapport peut être calculé en divisant le nombre attendu de rapporteurs par le temps de réponse max. Le temps de réponse max peut être calculé de façon dynamique par interrogation en utilisant le nombre attendu de rapporteurs pour cette interrogation comme suit :

| **Type d'interrogation** | **Nombre de rapporteurs attendu** |
|---|---|
| Interrogation générale | Tous les systèmes sur le sous-réseau |
| Interrogation spécifique de groupe | Tous les systèmes qui ont exprimé de l'intérêt pour le groupe sur le sous-réseau |
| Interrogation spécifique de source et groupe | Tous les systèmes du sous-réseau qui ont exprimé de l'intérêt pour la source et le groupe |

Un routeur n'est pas obligé de calculer ces populations ou de régler de façon dynamique le temps de réponse max ; ces éléments sont simplement indicatifs.

## 9. Considérations pour la sécurité

On examine les ramifications d'un message falsifié de chaque type, et on décrit l'usage de l'en-tête d'authentification (AH) IPSEC pour authentifier les messages si on le souhaite.

### 9.1 Message d'interrogation

Un message Interrogation falsifié provenant d'une machine avec une adresse IP inférieure à l'interrogateur actuel va provoquer l'attribution des tâches de l'interrogateur au faussaire. Si le faussaire n'envoie alors plus de message Interrogation, le temporisateur Autres-interrogateurs-présents des autres routeurs va arriver à expiration et l'un d'eux va reprendre le rôle d'interrogateur. Pendant ce temps, si le faussaire ignore les messages Quitter, le trafic pourrait s'écouler vers des groupes sans membre pendant jusqu'à [Intervalle d'adhésion de groupe].

Une attaque de déni de service contre un hôte pourrait être mise en scène au moyen d'interrogations spécifiques de groupe et source falsifiées. L'attaquant peut trouver qui sont les membres d'un hôte spécifique avec une interrogation générale. Après cela, il pourrait envoyer un grand nombre d'interrogations spécifiques de groupe et source, chacune avec une grande liste des sources et le temps de réponse maximum réglé à une grande valeur. L'hôte va devoir mémoriser et entretenir les sources spécifiées dans toutes ces interrogations pendant tout le temps qu'il faudra pour envoyer la réponse retardée. Cela va consommer à la fois de la mémoire et des cycles de CPU afin d'augmenter les sources enregistrées des listes de sources incluses dans les interrogations successives.

Pour se protéger contre une telle attaque de DoS, une mise en œuvre de pile d'hôte pourrait restreindre le nombre d'interrogations spécifiques de groupe et source par membre de groupe au sein de cet intervalle, et/ou n'enregistrer qu'un nombre limité de sources.

Les messages Interrogations falsifiés provenant du réseau local peuvent être aisément traqués. Trois mesures sont nécessaires pour se défendre contre les interrogations falsifiées externes :

- o Les routeurs NE DEVRAIENT PAS transmettre les interrogations. Cela est plus facile à accomplir pour un routeur si l'interrogation porte l'option Alerte de routeur.
- o Les hôtes DEVRAIENT ignorer les interrogations v2 ou v3 qui n'ont pas l'option Alerte de routeur.
- o Les hôtes DEVRAIENT ignorer les interrogations générales v1, v2 ou v3 envoyées à une adresse de diffusion groupée autre que 224.0.0.1, l'adresse Tous-les-systèmes.

### 9.2 Messages de rapport d'état en cours

Un message Rapport falsifié peut amener un routeur de diffusion groupée à penser qu'il y a des membres d'un groupe sur un réseau alors qu'il n'y en a pas. Les messages Rapport provenant du réseau local n'ont aucun sens, car joindre un groupe sur un hôte est généralement une opération qui ne nécessite pas de privilège, de sorte qu'un utilisateur local peut obtenir très facilement le même résultat sans falsifier aucun message. Des messages Rapport falsifiés provenant de sources externes sont plus gênantes ; il y a deux défenses contre les rapports externes falsifiés :

- o Ignorer le Rapport si on ne peut pas identifier l'adresse de source du paquet comme appartenant à un réseau alloué à l'interface sur laquelle le paquet a été reçu. Cette solution signifie que les rapports envoyés par des hôtes mobiles sans adresse sur le réseau local seront ignorés. Les messages Rapport avec une adresse de source de 0.0.0.0 DEVRAIENT être acceptés sur toute interface.
- o Ignorer les messages Rapport sans option Alerte de routeur [RFC2113], et exiger que les routeurs ne transmettent pas les messages Rapport. (Cette exigence n'est pas celle d'un filtrage généralisé du chemin de transmission, car les paquets ont déjà sur eux l'option Alerte de routeur.) Cette solution rompt la rétro compatibilité avec les mises en œuvre IGMPv1 ou les premières versions de IGMPv2 qui n'exigent pas l'alerte de routeur.

Un message Rapport version 1 falsifié peut mettre un routeur dans l'état "Membres version 1 présents" pour un certain groupe, ce qui signifie que le routeur va ignorer les messages Quitter. Cela peut causer l'écoulement du trafic vers des groupes sans membre pendant jusqu'à [Intervalle d'adhésion de groupe]. Cela peut se résoudre en fournissant aux routeurs un commutateur de configuration pour ignorer complètement les messages de version 1. Cela casse la compatibilité automatique avec les hôtes de version 1, et ne devrait donc être utilisé que dans les situations où le "départ rapide" est critique.

Un message Rapport version 2 falsifié peut mettre un routeur dans l'état "Membres de version 2 présents" pour un certain groupe, ce qui signifie que le routeur va ignorer les messages d'état spécifique de source IGMPv3. Cela peut causer l'écoulement du trafic à partir de sources non désirées pendant jusqu'à [Intervalle d'adhésion de groupe]. Cela peut se résoudre en fournissant aux routeurs un commutateur de configuration pour ignorer complètement les messages de version 2. Cela casse la compatibilité automatique avec les hôtes de version 2, et ne devrait donc être utilisé que dans les situations où l'inclusion et l'exclusion de source sont critiques.

### 9.3 Messages de rapport de changement d'état

Un message Rapport de changement d'état falsifié va amener l'interrogateur à envoyer des interrogations spécifiques de groupe ou spécifiques de source et groupe pour le groupe en question. Cela cause un traitement supplémentaire à chaque routeur et chez chaque membre du groupe, mais ne peut pas causer de perte du trafic désiré. Il y a deux défenses contre les messages Rapport de changement d'état falsifiés provenant de l'extérieur :

- Ignorer le message Rapport de changement d'état si on ne peut pas identifier l'adresse de source du paquet comme appartenant à un sous-réseau alloué à l'interface sur laquelle le paquet a été reçu. Cette solution signifie que les messages Rapport de changement d'état envoyés par un hôte mobile sans adresse sur le sous-réseau local seront ignorés. Les messages Rapport de changement d'état avec une adresse de source de 0.0.0.0 DEVRAIENT être acceptés sur toutes les interfaces.
- Ignorer les messages Rapport de changement d'état sans l'option Alerte de routeur [RFC2113], et exiger que les routeurs ne transmettent pas les messages Rapport de changement d'état. (Cette exigence n'est pas celle de filtrage généralisé sur le chemin de transmission, car les paquets ont déjà en eux l'option Alerte de routeur.)

### 9.4 Utilisation d'IPsec

En plus de ces mesures, IPSEC en mode En-tête d'authentification (AH, *Authentication Heaader*) [RFC2402] peut être utilisé pour protéger contre les attaques à distance en s'assurant que les messages IGMPv3 proviennent d'un système sur le LAN (ou, plus précisément, d'un système qui a la clé appropriée). Quand on utilise IPsec, les messages envoyés au 224.0.0.1 et au 224.0.0.22 devraient être authentifiés en utilisant AH. Lors du chiffrement, il y a deux possibilités :

1. Utiliser un algorithme de signature symétrique avec une seule clé pour le LAN (ou une clé pour chaque groupe). Cela permet de valider qu'un paquet a été envoyé par un système qui a la clé. La limitation est que tout système qui a la clé peut falsifier un message ; il n'est pas possible d'authentifier avec précision l'envoyeur individuel. Cela exige aussi de désactiver la protection contre la répétition d'IPsec.
2. Lorsque des normes de gestion de clés appropriées auront été développées, l'utilisation d'un algorithme de signature asymétrique. Tous les systèmes ont besoin de connaître la clé publique de tous les routeurs, et tous les routeurs ont besoin de connaître la clé publique de tous les systèmes. Cela exige une grande quantité de gestion de clé mais présente l'avantage que les envoyeurs peuvent être authentifiés individuellement, de sorte que, par exemple, un hôte ne peut pas falsifier un message que seuls des routeurs devraient être autorisés à envoyer.

Cette solution ne s'applique directement qu'aux messages Interrogation et Quitter dans IGMPv1 et IGMPv2, car les Rapports sont envoyés au groupe sur lequel porte le rapport et il n'est pas possible de se mettre d'accord sur une clé pour les communications d'hôte à routeur pour des groupes de diffusion groupée arbitraires.

## 10. Considérations relatives à l'IANA

Tous les types IGMP décrits dans le présent document sont déjà alloués dans [IANA-REG].

## 11. Remerciements

Nous tenons à remercier Ran Atkinson, Luis Costa, Toerless Eckert, Dino Farinacci, Serge Fdida, Wilbert de Graaf, Sumit Gupta, Mark Handley, Bob Quinn, Michael Speer, Dave Thaler et Rolland Vida pour leurs commentaires et suggestions sur ce document.

Des portions du texte de ce document sont copiées des [RFC1112] et [RFC2236].

## 12. Références normatives

[IANA-REG] http://www.iana.org/assignments/igmp-type-numbers

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989. *(Màj par la RFC 2236)*

[RFC2113] D. Katz, "Option d'alerte de routeur IP", février 1997.

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

[RFC2236] W. Fenner, "Protocole de gestion de groupe Internet, version 2", novembre 1997.

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC3228] B. Fenner, "Considérations relatives à l'IANA pour le protocole de gestion de groupe Internet IPv4 (IGMP)", BCP 57, février 2002.

## 13. Références pour information

[RFC1071] R. Braden, D. Borman et C. Partridge, "Calcul de la somme de contrôle Internet", septembre 1988.

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

[RFC3569] S. Bhattacharyya et autres, "Généralités sur la diffusion groupée de source spécifique (SSM)", juillet 2003

[RFC3678] D. Thaler, B. Fenner et B. Quinn, "Extensions d'interface de prise pour filtres de source en diffusion groupée", janvier 2004.

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

## Appendice A. Raisons des choix de conception

### A.1 Besoin des messages Changement-d'état

IGMPv3 spécifie deux types de rapports d'adhésion : État-en-cours et Changement d'état. La présente section décrit les raisons du besoin de ces deux types de rapport.

Les routeurs ont besoin de distinguer les rapports d'adhésion qui ont été envoyés en réponse aux interrogations de ceux qui ont été envoyés par suite d'un changement de l'état de l'interface. Les rapports d'adhésion qui ont été envoyés en réponse aux interrogations d'adhésion sont principalement utilisés pour rafraîchir l'état existant au routeur ; ils ne causent normalement pas de transition d'état au routeur. Les rapports d'adhésion qui sont envoyés en réponse à des changements de l'état de l'interface exigent que le routeur effectue des action en réponse au rapport reçu (voir le paragraphe 6.4).

L"incapacité à distinguer ces deux types de rapports forcerait un routeur à traiter tous les rapports d'adhésion comme des changements d'état potentiels et pourrait résulter en une augmentation des traitements au routeur ainsi que du trafic IGMP dans le réseau.

### A.2 Suppression d'hôte

Dans IGMPv1 et IGMPv2, un hôte annulerait l'envoi des rapports d'adhésion en cours si un rapport similaire était observé de la part d'un autre membre sir le réseau. Dans IGMPv3, cette suppression des rapports d'adhésion d'un hôte a été retirée. Les points qui suivent expliquent les raisons de cette décision.

1. Les routeurs peuvent vouloir retracer le statut de membre par hôte sur une interface. Cela permet aux routeurs de mettre en œuvre des départs rapides (par exemple, pour des schémas de contrôle d'encombrement par couche de diffusion groupée) ainsi que de retracer le statut de membre pour des besoins de comptabilité.

2. La suppression du rapport d'adhésion ne fonctionne pas bien sur les LAN pontés. De nombreux ponts et commutateurs de couche 2/couche3 qui mettent en œuvre la surveillance d'IGMP ne transmettent pas les messages IGMP à travers les segments de LAN afin d'empêcher la suppression des rapports d'adhésion. Retirer la suppression des rapports d'adhésion facilite le travail de ces appareils de surveillance d'IGMP.

3. En éliminant la suppression des rapports d'adhésion, les hôtes ont moins de messages à traiter ; cela conduit à une mise en œuvre plus simple des automates à états.

4. Dans IGMPv3, un seul rapport d'adhésion regroupe maintenant plusieurs enregistrements de groupe de diffusion

groupée pour diminuer le nombre de paquets envoyés. Par comparaison, les précédentes versions de IGMP exigeaient que chaque groupe de diffusion groupée soit rapporté dans un message distinct.

### A.3 Modes de filtre de routeur de commutation de EXCLURE à INCLURE

Si pour un seul groupe de diffusion groupée dans un réseau il existe des hôtes dans les deux modes EXCLURE et INCLURE, le routeur doit lui aussi être en mode EXCLURE (voir au paragraphe 6.2.1). En mode EXCLURE, un routeur transmet le trafic provenant de toutes les sources, sauf si cette source existe dans la liste des sources exclues. Si tous les hôtes en mode EXCLURE cessent d'exister, il serait souhaitable que le routeur revienne au mode INCLURE sans interruption du flux de trafic aux receveurs existants.

Une des façons d'accomplir cela est que les routeurs gardent trace de toutes les sources désirées par les hôtes qui sont en mode INCLURE même si le routeur est lui-même en mode EXCLURE. Si le temporisateur de groupe arrive maintenant à expiration en mode EXCLURE, cela implique qu'il n'y a plus d'hôte en mode EXCLURE sur le réseau (autrement, un rapport d'adhésion provenant de cet hôte aurait rafraîchi le temporisateur de groupe). Le routeur peut alors passer au mode INCLURE sans heurt, la liste des sources en cours étant transmise dans sa liste des sources.

## Appendice B. Résumé des changements depuis IGMPv2

Bien que la principale caractéristique ajoutée à IGMPv3 soit le filtrage de source, on présente un sommaire des autres changements par rapport à la RFC2236 :

- o L'état est conservé comme Groupe + Liste-de-Sources, et non simplement Groupe comme dans IGMPv2.
- o L'interopérabilité avec les systèmes IGMPv1 et IGMPv2 est définie comme des opérations sur l'état IGMPv3.
- o L'interface de service IP a changé pour permettre la spécification de liste-de-sources.
- o L'interrogateur inclut sa variable Robustesse et son Intervalle d'interrogation dans les paquets Interrogation pour permettre la synchronisation de ces variables sur les non interrogateurs.
- o Le temps maximum de réponse dans les messages Interrogation a une gamme exponentielle, qui change le maximum de 25,5 secondes à environ 53 minutes, à utiliser sur des liaisons qui ont de très grands nombres de systèmes.
- o Les hôtes retransmettent les messages de changement d'état pour une robustesse accrue.
- o Des sections de données supplémentaires sont définies pour permettre des extensions ultérieures.
- o Les paquets de rapport sont envoyés au 224.0.0.22, pour aider les commutateurs de couche 2 à faire la "surveillance".
- o Les paquets de rapport peuvent contenir plusieurs enregistrements de groupe, pour permettre le rapport d'états en cours pleins en utilisant moins de paquets.
- o Les hôtes n'effectuent plus de suppression, pour simplifier la mise en œuvre et permettre un suivi explicite des adhésions.
- o Un nouveau fanion Supprimer-le-traitement-côté-routeur (S) dans les messages Interrogation règle les problèmes de robustesse qui étaient aussi présents dans IGMPv2.

**Adresse des auteurs**

Brad Cain
Cereva Networks

Ajit Thyagarajan
Ericsson IP Infrastructure

Steve Deering
Cisco Systems, Inc.
170 Tasman Drive
San Jose, CA 95134-1706
téléphone : +1-408-527-8213
mèl : deering@cisco.com

Bill Fenner
AT&T Labs – Research
75 Willow Rd.
Menlo Park, CA 94025
téléphone : +1-650-330-7893
mèl : fenner@research.att.com

Isidor Kouvelas
Cisco Systems, Inc.
170 Tasman Drive
San Jose, CA 95134-1706
téléphone : +1-408-525-0727
mèl : kouvelas@cisco.com

**Déclaration complète de droits de reproduction**

les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations qui y sont 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 ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

## Remerciement

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