

Groupe de travail Réseau
Request for Comments : 4860
 Catégorie : Sur la voie de la normalisation

F. Le Faucheur, Cisco Systems, Inc.
 B. Davie, Cisco Systems, Inc.
 P. Bose, Lockheed Martin
 C. Christou, Booz Allen Hamilton
 M. Davenport, Booz Allen Hamilton
 mai 2007

Traduction Claude Brière de L'Isle

Réservations agrégées génériques du protocole de réservation de ressource (RSVP)

Statut du présent mémoire

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

Notice de copyright

Copyright (C) The Internet Society (2007). Tous droits réservés.

Résumé

La RFC 3175 définit des réservations agrégées du protocole de réservation de ressources (RSVP, *Resource ReSerVation Protocol*) permettant que des ressources soient réservées dans un réseau Diffserv pour un certain comportement par bond (PHB, *Per Hop Behavior*) ou un ensemble de PHB donnés, à partir d'une certaine source pour une certaine destination. La RFC 3175 définit aussi comment des réservations RSVP de bout en bout peuvent être agrégées sur de telles réservations agrégées quand elles transitent à travers un nuage Diffserv. Il y a des situations où plusieurs de ces réservations agrégées sont nécessaires pour la même adresse IP de source, adresse IP de destination, et PHB (ou ensembles de PHB). Cependant, ceci n'est pas pris en charge par les réservations agrégées définies dans la RFC 3175. Afin de prendre en charge cela, le présent document définit un type plus souple de réservations RSVP agrégées, appelé une réservation agrégée générique. Plusieurs de ces réservations agrégées génériques peuvent être établies pour un certain PHB (ou ensemble de PHB) à partir d'une adresse IP de source donnée pour une adresse IP de destination donnée. Les réservations agrégées génériques peuvent être utilisées pour agréger des réservations RSVP de bout en bout. Le présent document définit aussi les procédures pour une telle agrégation. Les réservations agrégées génériques peuvent aussi être utilisée de bout en bout directement par les systèmes d'extrémité rattachés à un réseau Diffserv.

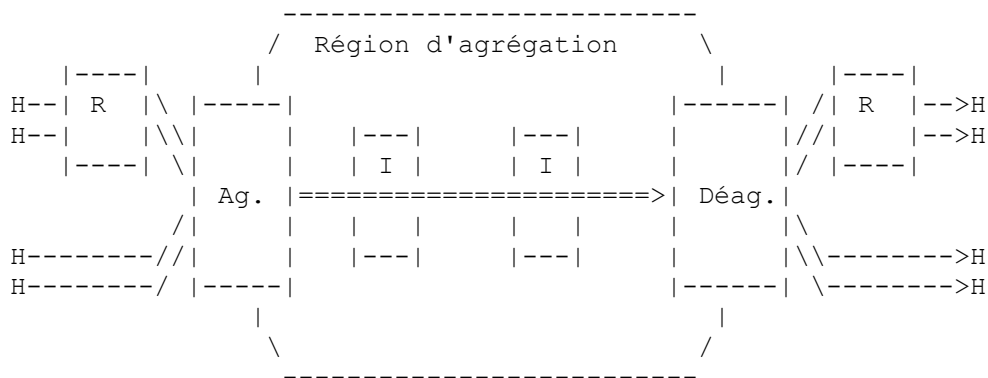
Table des matières

1. Introduction.....	1
1.1 Documents de l'IETF en relation.....	3
1.2 Organisation du document.....	4
1.3. Langage des exigences.....	4
2. Définition d'objet.....	4
2.1 Classe SESSION.....	5
2.2 Classe SESSION-OF-INTEREST (SOI).....	6
3. Règles de traitement des réservations agrégées génériques RSVP.....	7
3.1 Extensions au traitement de Path et Resv.....	7
4. Procédures d'agrégation sur réservations agrégées génériques RSVP.....	8
5. Exemple d'usage de plusieurs réservations agrégées génériques par PHB d'un certain agrégateur à un certain désagrégateur.....	10
6. Considérations sur la sécurité.....	12
7. Considérations relatives à l'IANA.....	13
8. Remerciements.....	14
9. Références normatives.....	14
10. Références pour information.....	14
Appendice A. Exemple de flux de signalisation.....	15
Adresse des auteurs.....	16
Déclaration complète de droits de reproduction.....	16

1. Introduction

La [RFC3175] définit des réservations agrégées RSVP qui permettent de réserver des ressources dans un réseau Diffserv pour un flux caractérisé par son triplet <adresse IP de source, adresse IP de destination, codet Diffserv>.

La [RFC3175] défint aussi les procédures pour l'agrégation de réservations RSVP de bout en bout (E2E, *end-to-end*) sur de telles réservations agrégées lors du transit à travers un nuage Diffserv. Une telle agrégation est illustrée à la Figure 1. Le présent document réutilise la terminologie définie dans la [RFC3175].



H = Hôte demandant des réservations RSVP de bout en bout

R = Routeur RSVP

Ag. = Agrégateur

Déag. = Désagrégateur

I = Routeur intérieur

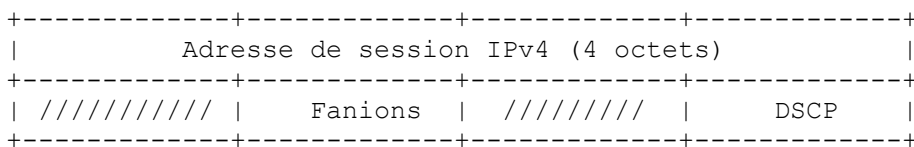
--> = réservation E2E RSVP

==> = réservation RSVP agrégée

Figure 1 : Agrégation de réservations de bout en bout sur des réservations RSVP agrégées

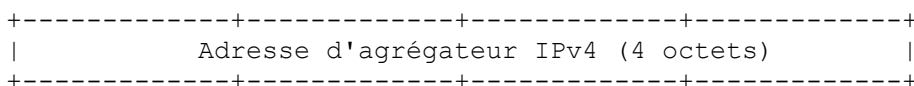
Ces réservations agrégées utilisent un type SESSION spécifié dans la [RFC3175] qui contient l'adresse IP du receveur (ou désagrégateur) et le codet Diffserv (DSCP, *Diffserv Code Point*) du comportement par bond (PHB, *Per Hop Behavior*) à partir duquel les ressources Diffserv sont à réserver. Par exemple, dans le cas de IPv4, l'objet SESSION est spécifié par :

- o Classe = SESSION, C-Type = RSVP-AGGREGATE-IP4



Ces réservations agrégées utilisent les types SENDER_TEMPLATE et FILTER_SPEC, spécifiés dans la [RFC3175], qui contiennent seulement l'adresse IP de l'expéditeur (ou agrégateur). Par exemple, dans le cas de IPv4, l'objet SENDER_TEMPLATE est spécifié comme :

- o Classe = SENDER_TEMPLATE, C-Type = RSVP-AGGREGATE-IP4



Donc, il est possible d'établir, à partir d'une adresse IP de source donnée pour une adresse IP de destination donnée, de telles réservations agrégées séparées pour les différents PHB (ou différents ensembles de PHB). Cependant, d'une certaine adresse IP de source à une certaine adresse IP de destination, seulement une réservation agrégée [RFC3175] peut être établie pour un certain PHB (ou ensemble donné de PHB).

Des situations ont depuis été identifiées où plusieurs de ces réservations agrégées sont nécessaires pour la même adresse IP de source, adresse IP de destination, et PHB (ou ensemble de PHB). Un exemple est lorsque des réservations de bout en bout utilisant différentes priorités de préemption (selon la [RFC3181]) ont besoin d'être agrégées à travers un nuage Diffserv en utilisant le même PHB. Utiliser plusieurs réservations agrégées pour le même PHB permet l'application de différentes priorités de préemption au sein de la région d'agrégation. À son tour, cela permet une gestion plus efficace des ressources de Diffserv, et dans des périodes de pénurie de ressources, cela permet de prendre en charge un plus grand nombre de réservations de bout en bout avec de plus fortes priorités de préemption.

Par exemple, la [RFC4923] discute en détails comment les réservations RSVP de bout en bout peuvent être établies dans un environnement de VPN incorporé grâce à l'agrégation RSVP. En particulier, la [RFC4923] décrit comment plusieurs réservations agrégées génériques parallèles (pour le même PHB) chacune avec des priorités de préemption différentes, peuvent être utilisées pour prendre en charge efficacement les priorités de préemption des réservations de bout en bout.

Le présent document vise cette exigence pour plusieurs réservations agrégées pour le même PHB (ou même ensemble de PHB) en définissant un type de réservations RSVP agrégées plus souples, appelées des réservations agrégées génériques. Cela est réalisé principalement en ajoutant les notions d'un accès de destination virtuel et d'un accès de destination virtuel étendu dans l'objet SESSSION RSVP.

La notion d'accès de destination virtuel a été introduite dans la [RFC2207] pour viser une exigence similaire (bien que dans un contexte différent) pour l'identification et le démultiplexage de sessions au delà de l'adresse IP de destination. Le présent document réutilise cette notion de la [RFC2207] pour l'identification et le démultiplexage de sessions agrégées génériques au delà de l'adresse de destination IP et du PHB. Cela permet d'établir plusieurs réservations agrégées génériques pour un certain PHB (ou ensemble de PHB) à partir d'une adresse IP de source donnée pour une adresse IP de destination donnée.

La [RFC3209] a introduit le concept d'un identifiant de tunnel étendu (en plus de l'adresse de sortie de tunnel et de l'identifiant de tunnel) dans l'objet SESSSION utilisé pour établir les tunnels d'ingénierie du trafic MPLS avec RSVP. L'identifiant de tunnel étendu fournit un mécanisme très pratique pour que le nœud d'entrée du tunnel rétrécisse la portée de la session à la paire entrée sortie. Le nœud d'entrée peut réaliser cela en utilisant une de ses propres adresses IP comme un identifiant unique au monde et l'inclure dans l'identifiant de tunnel étendu et donc au sein de l'objet SESSSION. Le présent document réutilise cette notion d'identifiant de tunnel étendu de la [RFC3209], en le renommant simplement accès de destination virtuel étendu. Cela donne un mécanisme pratique pour rétrécir la portée d'une session agrégée générique à une paire d'agrégateur-désagrégateur.

L'objet SESSSION RSVP pour les réservations agrégées génériques utilise le code d'identification de PHB (PHB-ID) défini dans la [RFC3140] pour identifier le PHB, ou ensemble de PHB, à partir duquel les ressources Diffserv vont être réservées. Cela remplace l'utilisation du codet Diffserv (DSCP) de la [RFC3175]. Utiliser le PHB-ID au lieu du DSCP permet une indication explicite de si les ressources Diffserv appartiennent à un seul PHB ou à un ensemble de PHB. Cela facilite aussi le traitement de situations où une réservation agrégée générique s'étend sur deux (ou plus) domaines Diffserv qui utilisent des valeurs de DSCP différentes pour le même PHB (ou ensemble de PHB) Diffserv à partir duquel les ressources sont réservées. C'est parce que l'identifiant de PHB permet de convoier le PHB (ou ensemble de PHB) indépendamment de la ou les valeurs de DSCP utilisées localement pour ce PHB (ou ensemble de PHB).

Les réservations agrégées génériques peuvent être utilisées pour agréger les réservations RSVP de bout en bout. Le présent document définit aussi les procédures pour une telle agrégation. Ces procédures se fondent sur celles de la [RFC3175], et le présent document spécifie seulement leurs différences.

Les réservations agrégées génériques peuvent aussi être utilisées de bout en bout directement par les systèmes d'extrémité rattachés à un réseau Diffserv.

1.1 Documents de l'IETF en relation

Le présent document s'appuie largement sur la [RFC3175]. Il réutilise la [RFC3175] chaque fois que c'est applicable et spécifie seulement les extensions à la [RFC3175] nécessaires.

Les mécanismes définis dans la [RFC4495] permettent qu'une réservation existante soit réduite dans la bande passante allouée par les routeurs RSVP au lieu de supprimer cette réservation. Ces mécanismes sont applicables à la réservation agrégée générique définie dans le présent document.

La [RFC2746] décrit une approche générale pour faire fonctionner RSVP sur divers types de tunnels. Un de ces types de tunnel, appelé "tunnel de type 2", a des similitudes avec la réservation agrégée générique décrite dans le présent document.

La similarité découle du fait qu'une seule réservation agrégée est faite pour le tunnel alors que de nombreux flux individuels sont portés sur ce tunnel. Cependant, la [RFC2746] ne traite pas de l'utilisation de classes fondées sur Diffserv et de programmation dans le cœur d'un réseau (entre les points d'extrémité de tunnel) mais s'appuie plutôt sur un en-tête de tunnel UDP/IP pour la classification. C'est pourquoi la [RFC3175] exigeait des objets et procédures supplémentaires au delà de celles de la [RFC2746]. Comme la [RFC3175], le présent document suppose aussi l'utilisation d'une classification et programmation fondées sur Diffserv dans la région d'agrégation, et donc exige des objets et procédures supplémentaires au delà de ceux de la [RFC2746].

Comme expliqué plus tôt, le présent document réutilise la notion d'un accès de destination virtuel de la [RFC2207] et la notion d'identifiant de tunnel étendu de la [RFC3209].

1.2 Organisation du document

La Section 2 définit les nouveaux objets RSVP relatifs aux réservations agrégées génériques et à l'agrégation de réservations de bout en bout sur celles-ci. La Section 3 décrit les règles de traitement des réservations agrégées génériques. La Section 4 spécifie les procédures pour l'agrégation des réservations RSVP de bout en bout sur les réservations RSVP génériques agrégées. La Section 5 donne un exemple d'usage des réservations agrégées génériques.

Les considérations sur la sécurité et les considérations relatives à l'IANA sont discutés respectivement dans les Sections 6 et 7.

Finalement, l'Appendice A donne un exemple de flux de signalisation qui illustre l'agrégation de réservations RSVP de bout en bout sur des réservations RSVP génériques agrégées.

1.3 Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Définition d'objet

Le présent document réutilise les objets RSVP-AGGREGATE-IP4 FILTER_SPEC, RSVP-AGGREGATE-IP6 FILTER_SPEC, RSVP-AGGREGATE-IP4 SENDER_TEMPLATE, et RSVP-AGGREGATE-IP6 SENDER_TEMPLATE définis dans la [RFC3175].

Le présent document définit :

- deux nouveaux objets (GENERIC-AGGREGATE-IP4 SESSION et GENERIC-AGGREGATE-IP6 SESSION) dans la classe SESSION existante, et
- deux nouveaux objets (GENERIC-AGG-IP4-SOI et GENERIC-AGG-IP6-SOI) sous une nouvelle classe SESSION-OF-INTEREST.

La description détaillée de ces objets est fournie plus loin dans cette section.

Les objets GENERIC-AGGREGATE-IP4 SESSION et GENERIC-AGGREGATE-IP6 SESSION sont applicables à tous les types de messages RSVP.

La présente spécification définit l'utilisation des objets GENERIC-AGG-IP4-SOI et GENERIC-AGG-IP6-SOI dans deux circonstances :

- dans un message E2E PathErr qui contient un code d'erreur de NEW-AGGREGATE-NEEDED afin de porter la session d'une nouvelle réservation agrégée générique qui doit être établie ;
- dans un message de réservation de bout en bout afin de porter la session de la réservation agrégée générique sur laquelle cette réservation de bout en bout doit être transposée.

Les détails des procédures correspondantes se trouvent à la Section 4.

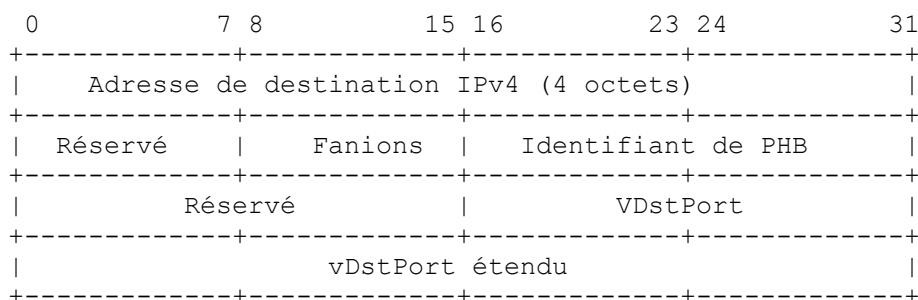
Cependant, il est envisagé que la capacité de signaler, dans les messages RSVP, la session d'une autre réservation (qui a une relation avec la réservation RSVP en cours) pourrait avoir d'autres applications à l'avenir. Donc, ces objets ont été spécifiés d'une façon plus générique sous une classe SESSION-OF-INTEREST plus souple.

Tous les nouveaux objets définis dans le présent document sont facultatifs à l'égard de RSVP, de sorte que les mises en œuvre générales de RSVP qui ne sont pas concernées par les réservations agrégées génériques n'ont pas à prendre en charge ces objets. Les routeurs RSVP qui prennent en charge les réservations génériques agrégées IPv4 ou IPv6 DOIVENT prendre en charge, respectivement, l'objet SESSION GENERIC-AGGREGATE-IP4 ou l'objet SESSSION GENERIC-AGGREGATE-IP6. Les routeurs RSVP qui prennent en charge l'agrégation RSVP sur des réservations génériques agrégées IPv4 ou IPv6 DOIVENT prendre en charge respectivement l'objet SOI GENERIC-AGG-IP4 ou GENERIC-AGG-IP6.

2.1 Classe SESSION

o objet SESSSION GENERIC-AGGREGATE-IP4 :

Classe = 1 (SESSION) ; C-Type = 17



Adresse de destination IPv4 : adresse IPv4 du receveur (ou désagrégateur).

Réserve : champ de 8 bits. Tous les bits DOIVENT être à 0 à l'émission. Ce champ DOIT être ignoré à réception.

Fanions : champ de 8 bits. Le contenu et le traitement de ce champ sont les mêmes que pour le champ Fanions de l'objet SESSSION IPv4/UDP (voir la [RFC2205]).

Identifiant de PHB : champ de 16 bits contenant le code d'identification de comportement par bond , ou de l'ensemble de PHB, à partir duquel les ressources Diffserv sont à réserver. Ce champ DOIT être codé comme spécifié à la Section 2 de la [RFC3140].

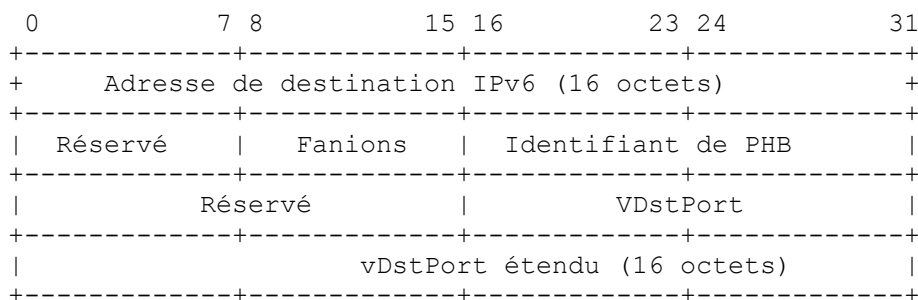
Réserve : champ de 16 bits. Tous les bits DOIVENT être à 0 à l'émission. Ce champ DOIT être ignoré à réception.

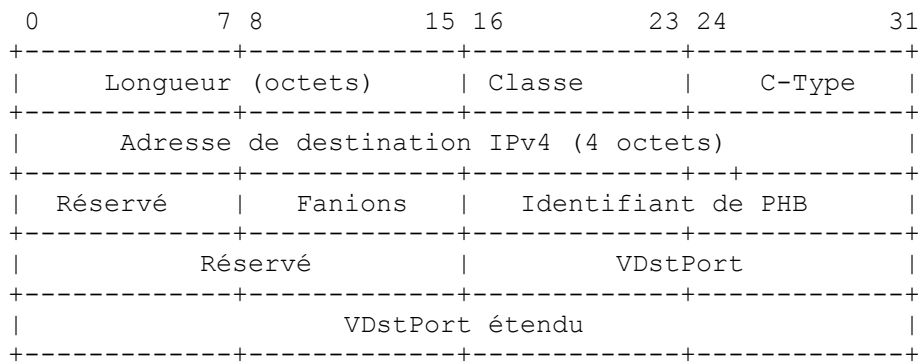
VDstPort (accès de destination virtuel) : identifiant de 16 bits utilisé dans la SESSION, qui reste constant pendant la vie de la réservation agrégée générique.

vDstPort étendu (accès de destination virtuel étendu) : identifiant de 32 bits utilisé dans la SESSION, qui reste constant sur la vie de la réservation agrégée générique. Un envoyeur (ou agrégateur) qui souhaite rétrécir la portée d'une SESSION à la paire envoyeur-receveur (ou agrégateur-désagrégateur) DEVRAIT placer ici son adresse IPv4 comme identifiant unique de réseau. Un envoyeur (ou agrégateur) qui souhaite utiliser une session commune avec d'autres envoyeurs (ou agrégateurs) afin d'utiliser une réservation partagée entre les envoyeurs (ou agrégateurs) DOIT régler ce champ tout à zéro.

o objet SESSSION GENERIC-AGGREGATE-IP6 :

Classe = 1 (SESSION) ; C-Type = 18





Noter qu'un objet SESSION-OF-INTEREST n'est pas un objet SESSSION par lui-même. Il ne remplace pas l'objet SESSSION dans les messages RSVP. Il ne modifie pas l'usage de l'objet SESSSION dans les messages RSVP. Il permet simplement de porter la session d'une autre réservation RSVP à l'intérieur des messages de signalisation RSVP, pour des objets particuliers. Dans le contexte du présent document, il est utilisé pour porter, à l'intérieur d'un message E2E RSVP relevant d'une réservation de bout en bout, la session d'une réservation agrégée générique associée à la réservation de bout en bout. Les détails des procédures correspondantes sont spécifiées à la Section 4.

3. Règles de traitement des réservations agrégées génériques RSVP

Cette Section présente les extensions au traitement des messages RSVP exigées par la [RFC2205] et présentées dans la [RFC2209]. Ces extensions sont exigées afin de traiter correctement l'objet SESSION GENERIC-AGGREGATE-IP4 ou GENERIC-AGGREGATE-IP6 et l'objet FILTER_SPEC RSVP-AGGREGATE-IP4 ou RSVP-AGGREGATE-IP6. Les valeurs pour les codes d'erreur référencés se trouvent dans la [RFC2205]. Comme avec les autres documents RSVP, les valeurs pour les erreurs rapportées en interne ne sont pas définies.

Quand on se réfère aux nouveaux objets SESSION GENERIC-AGGREGATE-IP4 et GENERIC-AGGREGATE-IP6, la version IP ne sera pas incluse, et on s'y réfère simplement comme session GENERIC-AGGREGATE, sauf si une distinction spécifique entre IPv4 et IPv6 est faite.

Quand on se réfère aux objets FILTER_SPEC, et SENDER_TEMPLATE RSVP-AGGREGATE-IP4 et RSVP-AGGREGATE-IP6 de la [RFC3175], la version IP ne sera pas incluse, et on s'y réfère simplement comme RSVP-AGGREGATE, sauf si une distinction spécifique entre IPv4 et IPv6 est faite.

3.1 Extensions au traitement de Path et Resv

Les changements suivants au traitement du message PATH sont définis :

- o Quand une session est définie en utilisant l'objet SESSSION GENERIC-AGGREGATE, seul le RSVP-AGGREGATE SENDER_TEMPLATE de la [RFC3175] peut être utilisé. Quand cette condition est violée dans un message PATH reçu par une station terminale RSVP, la station terminale RSVP DEVRAIT rapporter une erreur API "Conflit de C-Type" à l'application. Quand cette condition est violée dans un message PATH reçu par un routeur RSVP, le routeur RSVP DOIT considérer cela comme une erreur de format de message.
- o Pour les messages PATH qui contiennent l'objet SESSSION GENERIC-AGGREGATE, la valeur VDstPort, la valeur VDstPort étendue, et la valeur de PHB-ID devraient être enregistrées (en plus de l'adresse de destination/désagrégateur et de l'adresse de source/agrégateur). Ces valeurs font partie de l'état enregistré de la session. Le PHB-ID peut devoir être passé au contrôle de trafic ; cependant, le vDstPort et VDstPort étendus ne sont pas passés au contrôle de trafic car ils n'apparaissent pas dans les paquets de données de la réservation correspondante.

Les changements suivants au traitement du message RESV sont définis :

- o Quand un message RESV contient un FILTER_SPEC RSVP-AGGREGATE [RFC3175], la session DOIT être définie en utilisant l'objet SESSSION RSVP-AGGREGATE [RFC3175] ou l'objet SESSSION GENERIC-AGGREGATE (conformément au présent document). Si cette condition n'est pas satisfaite, un routeur RSVP ou une station d'extrémité

DOIT considérer que c'est une erreur de format de message.

- o Quand le FILTER_SPEC RSVP-AGGREGATE est utilisé et que le type de session est GENERIC-AGGREGATE, chaque nœud utilise des classeurs de données comme :
 - * Pour effectuer la classification Diffserv le nœud DOIT s'appuyer sur la classification de données Diffserv sur la base du seul DSCP. La ou les valeurs de DSCP pertinentes sont celles qui sont associées au PHB-ID de la réservation agrégée générique.
 - * Si le nœud a aussi besoin d'effectuer une classification fine (par exemple, pour effectuer une politique d'entrée fine à une frontière de confiance) alors le nœud DOIT créer un classement de données décrit par le triplet <Adresse de destination, Adresse de source, DSCP>. La ou les valeurs de DSCP pertinentes sont celles qui sont associées au PHB-ID de la réservation agrégée générique

Noter que si plusieurs réservations agrégées génériques sont établies avec des accès de destination virtuelle différents (et/ou des accès de destination virtuelle étendue différents) mais avec le même triplet <Adresse de destination, Adresse de source, Identifiant de PHB>, alors elles ne peuvent pas être distinguées par le classificateur. Si le routeur utilise le classificateur à des fins de régulation, le routeur va donc les réguler ensemble et DOIT programmer le taux de régulation à la somme des taux réservés à travers toutes les réservations correspondantes.

4. Procédures d'agrégation sur réservations agrégées génériques RSVP

Les procédures pour l'agrégation de réservations de bout en bout sur des réservations RSVP génériques agrégées sont les mêmes que les procédures spécifiées dans la [RFC3175] à l'exception des changements de procédure mentionnés dans cette section.

Comme spécifié dans la [RFC3175], le désagrégateur est responsable de la transposition d'une certaine réservation de bout en bout sur une certaine réservation agrégée. Le désagrégateur demande l'établissement d'une nouvelle réservation agrégée en envoyant à l'agrégateur un message E2E PathErr avec un code d'erreur de NEW-AGGREGATE-NEEDED. Dans la [RFC3175], le désagrégateur transporte le DSCP de la nouvelle réservation agrégée demandée en incluant un objet DCLASS dans le PathErr E2E et en codant le DSCP correspondant à l'intérieur. Le présent document modifie et étend cette procédure. Le désagrégateur DOIT inclure dans le message E2E PathErr un objet SESSION-OF-INTEREST qui contient la session GENERIC-AGGREGATE à utiliser pour l'établissement de la réservation agrégée générique demandée. Comme cette session GENERIC-AGGREGATE contient le PHB-ID, l'objet DCLASS n'a pas besoin d'être inclus dans le message PathErr.

Noter que le désagrégateur peut facilement s'assurer que des agrégateurs différents utilisent des sessions différentes pour leur chemin agrégé vers un certain désagrégateur. C'est parce que le désagrégateur peut facilement choisir des numéros de VDstPort et/ou VDstPort étendus qui sont différents pour chaque agrégateur (par exemple, en utilisant l'adresse de l'agrégateur comme VdstPort étendu) et peut les communiquer dans la session GENERIC-AGGREGATE incluse dans les objets SESSION-OF-INTEREST. Cela donne une solution facile pour établir des réservations séparées à partir de chaque agrégateur pour un certain désagrégateur. À l'inverse, si le partage de réservation était nécessaire à travers plusieurs agrégateurs, le désagrégateur pourrait le faciliter en allouant le même VDstPort et VdstPort étendu à plusieurs agrégateurs, et donc incluant la même session GENERIC-AGGREGATE à l'intérieur de l'objet SESSION-OF-INTEREST dans les messages PathErr E2E envoyés à ces agrégateurs. Les agrégateurs pourraient alors tous établir un chemin agrégé avec la même session GENERIC-AGGREGATE.

Donc, divers scénarios de partage peuvent facilement être pris en charge. Les politiques suivies par le désagrégateur pour déterminer quels agrégateurs ont besoin de réservations partagées ou séparées sortent du domaine d'application du présent document.

Le désagrégateur PEUT aussi inclure dans le message PathErr E2E (avec un code d'erreur de NEW-AGGREGATE-NEEDED) des objets RSVP supplémentaires qui sont à utiliser pour l'établissement des nouvelles réservations agrégées génériques nécessaires. Par exemple, le désagrégateur PEUT inclure dans le PathErr E2E un élément RSVP Politique de priorité de préemption signalée (comme spécifié dans la [RFC3181]).

Les procédures de la [RFC3175] pour le traitement d'un message PathErr E2E reçu avec un code d'erreur de NEW-AGGREGATE-NEEDED par l'agrégateur sont étendues de façon correspondante. À réception d'un tel message contenant un objet SESSION-OF-INTEREST, l'agrégateur DOIT déclencher l'établissement d'une réservation agrégée générique. En particulier, il DOIT commencer par envoyer des messages Chemin agrégé avec la session GENERIC-AGGREGATE trouvée dans les objets SESSION-OF-INTEREST reçus. Quand un élément RSVP Politique de priorité de préemption

signalée est contenu dans le message PathErr E2E reçu, l'agrégateur DOIT inclure cet objet dans le chemin agrégé pour la réservation agrégée générique correspondante. Quand d'autres objets supplémentaires sont contenus dans le message PathErr E2E reçu et qu'ils peuvent être sans ambiguïté interprétés comme relatifs à la nouvelle réservation agrégée générique nécessaire (par opposition à relatifs à la réservation de bout en bout) l'agrégateur DEVRAIT les inclure dans le chemin agrégé pour la réservation agrégée générique correspondante. L'agrégateur DOIT utiliser comme adresse de source (c'est-à-dire, comme adresse d'agrégateur dans le gabarit d'expéditeur) pour la réservation agrégée générique, l'adresse qu'il utilise pour s'identifier lui-même comme PHOP (bond RSVP précédent) quand il transmet les messages Path E2E correspondant au message PathErr E2E.

Le désagrégateur suit les mêmes procédures que décrites dans la [RFC3175] pour établir, maintenir et supprimer l'état agrégé Resv. Cependant, un désagrégateur se comportant conformément à la présente spécification DOIT utiliser les réservations agrégées génériques et donc utiliser la session GENERIC-AGGREGATE spécifiée précédemment dans le présent document.

Le présent document modifie aussi les procédures de la [RFC3175] relatives à l'échange de messages de réservation de bout en bout entre désagrégateur et agrégateur. Le désagrégateur DOIT inclure le nouvel objet SESSION-OF-INTEREST dans le message de réservation de bout en bout, afin d'indiquer à l'agrégateur la session agrégée générique à transposer en une certaine réservation de bout en bout. Là encore, comme la session GENERIC-AGGREGATE (incluse dans l'objet SESSION-OF-INTEREST) contient le PHB-ID, l'objet DCLASS n'a pas besoin d'être inclus dans le message de réservation de bout en bout. L'agrégateur DOIT interpréter l'objet SESSION-OF-INTEREST dans la réservation de bout en bout comme indiquant sur quelle session de réservation agrégée générique est transposée la réservation de bout en bout correspondante. L'agrégateur NE DOIT PAS inclure l'objet SESSION-OF-INTEREST quand il envoie une réservation de bout en bout en amont vers l'expéditeur.

Sur la base de la politique pertinente, le désagrégateur peut décider à un moment qu'une réservation agrégée n'est plus nécessaire et devrait être supprimée. Dans ce cas, le désagrégateur DOIT envoyer un ResvTear agrégé. À réception du ResvTear agrégé, l'agrégateur DEVRAIT envoyer un PathTear agrégé (sauf si la politique pertinente donne pour instruction à l'agrégateur de faire autrement ou d'attendre un certain temps avant de le faire, par exemple afin d'accélérer un potentiel rétablissement de la réservation agrégée à l'avenir).

La [RFC3175] décrit comment l'agrégateur et le désagrégateur peuvent se communiquer leur identités respectives. Par exemple, l'agrégateur inclut une de ses adresses IP dans l'objet RSVP HOP dans le chemin E2E qui est transmis vers l'aval et reçu par le désagrégateur une fois qu'il a traversé la région d'agrégation. De même, le désagrégateur s'identifie à l'agrégateur en incluant une de ses adresses IP dans divers champs, incluant la SPÉCIFICATION D'ERREUR du message E2E PathErr (contenant le code d'erreur NEW-AGGREGATE-NEEDED) et dans l'objet RSVP HOP du message de réservation de bout en bout. Cependant, la [RFC3175] ne précise pas quelles adresses IP doivent être choisies par l'agrégateur et le désagrégateur pour cela. Parce que ces adresses sont destinées à identifier l'agrégateur et le désagrégateur et non pour identifier une interface spécifique sur ces appareils, le présent document RECOMMANDE que l'agrégateur et le désagrégateur DEVRAIENT utiliser des adresses indépendantes de l'interface (par exemple, une adresse de rebouclage) chaque fois qu'ils se communiquent leurs identités respectives. Cela assure que l'identification respective de l'agrégateur et du désagrégateur n'est pas impactée par un changement d'état d'interface sur ces appareils. Il en résulte un fonctionnement plus stable et une signalisation RSVP considérablement réduite dans la région d'agrégation. Par exemple, si des adresses indépendantes de l'interface sont utilisées par l'agrégateur et le désagrégateur, une défaillance sur une interface de ces appareils peut alors simplement résulter en le réacheminement d'une certaine réservation agrégée générique, mais ne va pas résulter en la suppression de la réservation agrégée générique et l'établissement d'une autre. De plus, il ne va pas en résulter un changement de la transposition de réservations de bout en bout en réservations agrégées génériques (en supposant que l'agrégateur et le désagrégateur sont encore accessibles après la défaillance, et que l'agrégateur et le désagrégateur sont encore sur le plus court chemin vers la destination).

Cependant, quand ils s'identifient à des voisins RSVP réels (c'est-à-dire, des voisins qui ne sont pas de l'autre côté de la région d'agrégation) l'agrégateur et le désagrégateur DEVRAIENT continuer d'utiliser des adresses dépendantes de l'interface conformément aux procédures régulières de la [RFC2205]. Cela s'applique par exemple quand l'agrégateur s'identifie lui-même vers l'aval comme PHOP pour la réservation agrégée générique ou s'identifie lui-même vers l'amont comme NHOP (prochain bond RSVP) pour une réservation de bout en bout. Cela s'applique aussi quand le désagrégateur s'identifie lui-même vers l'aval comme PHOP pour la réservation de bout en bout ou s'identifie lui-même vers l'amont comme NHOP pour la réservation agrégée générique. Au titre du traitement des réservations agrégées génériques, les routeurs intérieurs (c'est-à-dire, routeurs au sein de la région d'agrégation) DEVRAIENT continuer d'utiliser des adresses dépendantes de l'interface conformément aux procédures régulières de la [RFC2205].

Plus généralement, au sein de la région d'agrégation (c'est-à-dire, entre l'agrégateur et le désagrégateur) le fonctionnement de RSVP devrait être modélisé avec la notion que les réservations de bout en bout sont transposées en réservations

agrégées et ne sont plus liées aux interfaces physiques (comme c'était le cas avec le RSVP régulier). Cependant, les réservations agrégées génériques (au sein de la région d'agrégation) ainsi que les réservations de bout en bout (en dehors de la région d'agrégation) conservent le modèle du RSVP régulier et restent liées aux interfaces physiques.

Comme mentionné précédemment, les réservations agrégées génériques peuvent être établies de bord à bord par suite de l'établissement de réservations de bout en bout (de l'extérieur de la région d'agrégation) qui sont à agréger sur la région d'agrégation. Cependant, les réservations agrégées génériques peuvent aussi être utilisées de bout en bout par les systèmes d'extrémité directement rattachés à un domaine Diffserv, comme une passerelle au réseau téléphonique public commuté (RTPC). Dans ce cas, les réservations agrégées génériques peuvent être établies par les systèmes d'extrémité en réponse à des déclenchements de niveau application comme la signalisation d'appel vocal. Autrement, les réservations agrégées génériques peuvent aussi être utilisées de bord à bord pour gérer la bande passante dans un nuage Diffserv même si RSVP n'est pas utilisé de bout en bout. Un simple exemple d'un tel usage serait la configuration statique d'une réservation agrégée générique pour une certaine bande passante pour du trafic d'un routeur d'entrée (agrégateur) à un routeur de sortie (désagrégateur).

Dans ce cas, l'établissement des réservations agrégées génériques est contrôlé par configuration chez l'agrégateur et chez le désagrégateur. La configuration chez l'agrégateur déclenche la génération du message Chemin agrégé et donne des informations suffisantes à l'agrégateur pour déduire le contenu de l'objet SESSION GENERIC-AGGREGATE. Cela devrait normalement inclure l'adresse IP du désagrégateur, l'identifiant de PHB, et éventuellement le VDstPort. La configuration chez le désagrégateur lui donnerait pour instruction de répondre au message de chemin agrégé générique reçu et donnerait des informations suffisantes au désagrégateur pour contrôler la réservation. Cela peut inclure la bande passante à réserver par le désagrégateur (pour un triplet <désagrégateur, PHB-ID, VDstPort> donné).

En l'absence de réservations de micro flux de bout en bout, l'agrégateur peut utiliser diverses politiques pour établir le DSCP des paquets qui passent dans la région d'agrégation et comment ils sont transposés en réservations agrégées génériques, donc déterminer si ils obtiennent l'accès aux ressources réservées par la réservation agrégée. Ces politiques sont une affaire de configuration locale, comme il est normal pour un appareil à la bordure d'un nuage Diffserv.

5. Exemple d'usage de plusieurs réservations agrégées génériques par PHB d'un certain agrégateur à un certain désagrégateur

Considérons l'environnement décrit à la Figure 2. L'agrégation RSVP est utilisée pour prendre en charge les réservations de bout en bout entre Nuage-1, Nuage-2, et Nuage-3.

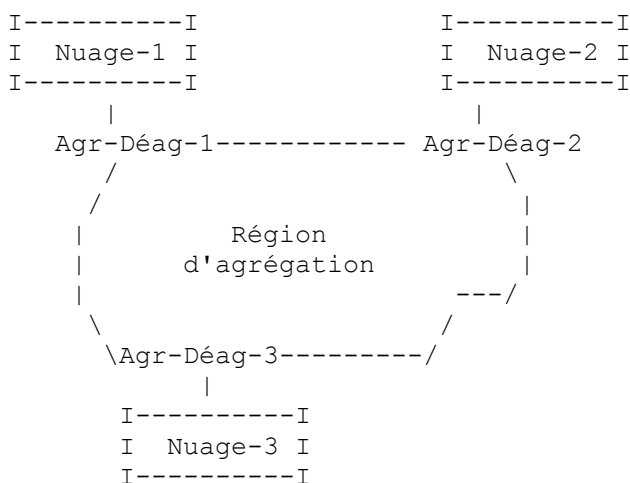


Figure 2 : Exemple d'usage de réservations génériques agrégées IP

Supposons que :

- o Les réservations de bout en bout de Nuage-1 à Nuage-3 ont une préemption de P1 ou P2.
- o Les réservations de bout en bout de Nuage-2 à Nuage-3 ont une préemption de P1 ou P2.
- o Les réservations de bout en bout sont seulement pour le vocal (qui doit être traité dans la région d'agrégation en utilisant le PHB EF (transmission expédiée)).
- o Le trafic des réservations de bout en bout est encapsulé dans les réservations agrégées IP de l'agrégateur au

désagrégateur en utilisant le tunnelage d'encapsulation d'acheminement générique [RFC2784].

Ensuite, les réservations RSVP génériques agrégées suivantes peuvent être établies de Agr-Déag-1 à Agr-Déag-3 pour l'agrégation des réservations RSVP de bout en bout:

(1) Une première réservation agrégée générique pour l'agrégation de réservations vocales de Nuage-1 à Nuage-3 exigeant l'utilisation de P1 :

- * SESSION GENERIC-AGGREGATE-IP4 :
 - IPv4 DestAddress = Agr-Déag-3
 - vDstPort = V1
 - PHB-ID = EF
 - VDstPort étendu = Agr-Déag-1
- * STYLE = FF ou SE
- * FILTER_SPEC IPv4/GPI :
 - IPv4 SrcAddress = Agr-Déag-1
- * POLICY_DATA (PREEMPTION_PRI) = P1

(2) Une seconde réservation agrégée générique pour l'agrégation de réservations vocales de Nuage-1 à Nuage-3 exigeant l'utilisation de P2 :

- * SESSION GENERIC-AGGREGATE-IP4 :
 - IPv4 DestAddress = Agr-Déag-3
 - vDstPort = V2
 - PHB-ID = EF
 - VdstPort étendu = Agr-Déag-1
- * STYLE = FF ou SE
- * FILTER_SPEC IPv4/GPI :
 - IPv4 SrcAddress = Agr-Déag-1
- * POLICY_DATA (PREEMPTION_PRI) = P2

où V1 et V2 sont des valeurs arbitraires de VDstPort prises par Agr-Déag-3.

Les réservations RSVP génériques agrégées suivantes peuvent être établies de Agr-Déag-2 à Agr-Déag-3 pour l'agrégation des réservations RSVP de bout en bout :

(3) Une troisième réservation agrégée générique pour l'agrégation de réservations vocales de Nuage-2 à Nuage-3 exigeant l'utilisation de P1 :

- * SESSION GENERIC-AGGREGATE-IP4 :
 - IPv4 DestAddress = Agr-Déag-3
 - vDstPort = V3
 - PHB-ID = EF
 - VdstPort étendu = Agr-Déag-2
- * STYLE = FF ou SE
- * FILTER_SPEC IPv4/GPI :
 - IPv4 SrcAddress = Agr-Déag-2
- * POLICY_DATA (PREEMPTION_PRI) = P1

(4) Une quatrième réservation agrégée générique pour l'agrégation des réservations vocales de Nuage-2 à Nuage-3 exigeant l'usage de P2 :

- * SESSION GENERIC-AGGREGATE-IP4 :
 - IPv4 DestAddress = Agr-Déag-3
 - vDstPort = V4
 - PHB-ID = EF
 - VDstPort étendu = Agr-Déag-2
- * STYLE = FF ou SE
- * FILTER_SPEC IPv4/GPI :
 - IPv4 SrcAddress = Agr-Déag-2
- * POLICY_DATA (PREEMPTION_PRI) = P2

où V3 et V4 sont des valeurs arbitraires de VDstPort prises par Agr-Déag-3.

Noter que V3 et V4 pourraient être égaux (respectivement) à V1 et V2 car dans cet exemple, le VDstPort étendu de la session GENERIC-AGGREGATE contient l'adresse de l'agrégateur et donc, assure que différentes sessions sont utilisées à

partir de chaque agrégateur.

6. Considérations sur la sécurité

Dans les environnements visés par ce document, les messages RSVP sont utilisés pour contrôler les réservations de ressources pour les réservations agrégées génériques et peuvent être utilisés pour contrôler les réservations de ressources pour les réservations de bout en bout qui sont agrégées sur les réservations agrégées génériques. Pour assurer l'intégrité de la réservation associée et des mécanismes de contrôle d'admission, les mécanismes d'authentification RSVP définis dans les [RFC2747] et [RFC3097] peuvent être utilisés. Ils protègent l'intégrité des messages RSVP bond par bond et assurent l'authentification du nœud ainsi que la protection contre la répétition, protégeant ainsi contre la corruption et l'usurpation d'identité des messages RSVP. Ces mécanismes d'intégrité bond par bond peuvent être naturellement utilisés pour protéger les messages RSVP utilisés pour les réservations agrégées génériques et pour protéger les messages RSVP utilisés pour les réservations de bout en bout en dehors de la région d'agrégation. Ces mécanismes d'intégrité RSVP bond par bond peuvent aussi être utilisés pour protéger les messages RSVP utilisés pour les réservations de bout en bout quand ils transitent à travers la région d'agrégation. C'est parce que l'agrégateur et le désagrégateur se comportent comme des voisins RSVP du point de vue des flux de bout en bout (même si ils ne sont pas nécessairement des voisins IP).

La [RFC2747] discute plusieurs approches pour la distribution des clés. D'abord, les clés partagées d'authentification RSVP peuvent être distribuées manuellement. C'est l'option de base et sa prise en charge est obligatoire pour toute mise en œuvre. Cependant, dans certains environnements, cette approche peut devenir une charge si les clés changent fréquemment. Autrement, un protocole standard de gestion de clé pour une distribution de clé sécurisée peut être utilisé. Cependant, les protocoles de distribution de clé existants peuvent n'être pas appropriés dans tous les environnements à cause de la complexité ou de la charge opérationnelle qu'ils impliquent.

L'utilisation de l'authentification RSVP dans des parties du réseau où il peut y avoir un ou plusieurs bonds IP entre deux voisins RSVP soulève un défi supplémentaire. C'est parce que, avec certains messages RSVP comme un message Path, un routeur RSVP ne connaît pas le prochain bond RSVP pour ce message au moment de le transmettre. En fait, une partie du rôle d'un message Path est précisément de découvrir le prochain bond RSVP (et de redécouvrir dynamiquement quand il change, par exemple à cause d'un changement d'acheminement). Donc, le routeur RSVP peut ne pas savoir quelle association de sécurité utiliser quand il transmet un tel message. Ceci s'applique en particulier au cas où les mécanismes d'authentification RSVP sont à utiliser pour la protection de messages RSVP de bout en bout (par exemple, E2E Path) quand ils transitent par une région d'agrégation et lorsque la procédure de détermination dynamique du désagrégateur définie dans la [RFC3175] est utilisée. Ceci est parce que l'agrégateur et le désagrégateur se comportent comme des voisins RSVP pour les réservations de bout en bout, alors qu'il peut y avoir un ou plusieurs bonds IP entre eux, et que l'agrégateur ne sait pas à l'avance quel routeur va agir comme désagrégateur.

Dans cette situation, une approche est de partager la même clé partagée d'authentification RSVP entre tous les routeurs RSVP d'une partie du réseau où il peut y avoir des voisins RSVP avec des bonds IP entre eux. Par exemple, tous les agrégateurs ou désagrégateurs d'une région d'agrégation pourraient partager la même clé d'authentification RSVP, tandis que des clés différentes par voisin pourraient être utilisées entre toute paire de routeurs RSVP s'écartant de la frontière entre deux domaines administratifs qui se sont accordés pour utiliser la signalisation RSVP.

Quand la même clé partagée d'authentification RSVP est à partager entre plusieurs voisins RSVP, une distribution de clés manuelle peut être utilisée. Pour des situations où RSVP est utilisé pour des flux en diffusion groupée, il pourrait aussi être possible, à l'avenir, d'adapter une méthode de gestion de clé de diffusion groupée (par exemple venant du groupe de travail Sécurité de la diffusion groupée de l'IETF) pour une distribution de clés avec un tel usage de diffusion groupée RSVP. Pour les situations où RSVP est utilisé pour des flux en envoi individuel à travers des frontières de domaines, il n'est actuellement pas clair de savoir comment on pourrait fournir une gestion de clés automatique.

La spécification d'une technique spécifique de gestion automatique de clés sort du domaine d'application du présent document. Les opérateurs devraient considérer ces problèmes de gestion de clés quand ils envisagent de déployer la présente spécification.

Les mécanismes d'authentification RSVP n'assurent pas la confidentialité. Si la confidentialité est requise, IPsec ESP [RFC4303] peut être utilisé, bien qu'il impose la charge de la distribution des clés. Il fait aussi face au problème supplémentaire discuté ci-dessus pour la gestion de clé dans le cas où il peut y avoir des bonds IP entre les bonds RSVP. À l'avenir, des solutions de confidentialité pourront être développées pour le cas où il peut y avoir des bonds IP entre les bonds RSVP, peut-être en adaptant les solutions de confidentialité développées dans le groupe de travail MSEC de l'IETF. De telles solutions de confidentialité pour RSVP sortent du domaine d'application de ce document.

La protection contre l'analyse de trafic n'est elle non plus assurée par l'authentification RSVP. Comme les réservations agrégées génériques sont destinées à réserver collectivement des ressources pour tout un ensemble d'utilisateurs ou hôtes, l'espionnage malveillant des messages RSVP correspondants pourrait fournir plus d'informations d'analyse de trafic que l'espionnage d'une réservation de bout en bout. Quand des voisins RSVP sont directement rattachés, des mécanismes tels qu'un chiffrement brut de liaison pourrait être utilisé quand la protection contre l'analyse de trafic est requise. Cette approche pourrait être utilisée à l'intérieur de la région d'agrégation pour la protection des réservations agrégées génériques. Elle peut aussi être utilisée en dehors de la région d'agrégation pour la protection de la réservation de bout en bout. Cependant, elle n'est pas applicable à la protection des réservations de bout en bout lorsque les messages RSVP de bout en bout correspondants transitent à travers la région d'agrégation.

Quand des réservations agrégées génériques sont utilisées pour l'agrégation de réservations de bout en bout, les considérations de sécurité discutées dans la [RFC3175] s'appliquent et elles sont revisitées ici.

D'abord, la perte d'une réservation agrégée au profit d'un agresseur cause la non réservation des flux de bout en bout, et la réservation d'un grand excès de bande passante peut résulter en un déni de service. Ces questions ne sont pas limitées aux extensions définies dans le présent document : RSVP lui-même les a. Cependant, elles peuvent être exacerbées ici par le fait que chaque réservation agrégée facilite normalement la communication pour de nombreuses sessions. Donc, compromettre une de ces réservations agrégées peut résulter en plus de dommages que de compromettre une réservation de bout en bout normale. L'utilisation des mécanismes de l'authentification RSVP pour se protéger contre de telles attaques a été discutée ci-dessus.

Une considération de sécurité supplémentaire, spécifique de l'agrégation RSVP implique la modification du numéro de protocole IP dans les messages Path RSVP qui traversent une région d'agrégation. La modification malveillante du numéro de protocole IP dans un message Path serait cause que le message soit ignoré par tous les appareils RSVP suivants sur son chemin, empêchant les réservations d'être faites. Il pourrait même être possible de corriger la valeur avant qu'elle atteigne le receveur, rendant difficile de détecter l'attaque. Noter que, en théorie, il serait aussi possible à un nœud de modifier le numéro de protocole IP pour des messages non RSVP, et donc d'interférer avec le fonctionnement d'autres protocoles. Il est RECOMMANDÉ que les mises en œuvre de la présente spécification prennent seulement en charge la modification du numéro de protocole IP pour les messages RSVP Path, PathTear, et ResvConf. C'est-à-dire qu'une facilité générale de modification du numéro de protocole IP NE DEVRAIT PAS être rendue disponible.

Les opérateurs de réseau qui déploient des routeurs avec une capacité d'agrégation RSVP devrait être conscients des risques de modification inappropriée du numéro de protocole IP et devraient prendre les mesures appropriées (sécurité physique, mot de passe de protection, etc.) pour réduire le risque qu'un routeur puisse être configuré par un attaquant à effectuer une modification malveillante du numéro de protocole.

7. Considérations relatives à l'IANA

L'IANA a modifié le registre des paramètres IP, sous registre 'Noms de classes, numéros de classes, et types de classes', et alloué deux nouveaux C-Types sous la classe SESSION existante (numéro de classe 1) comme décrit ci-dessous :

Numéro de classe	Nom de classe	Référence
1	SESSION	[RFC2205]
Types de classes ou C-Types :		
17	GENERIC-AGGREGATE-IP4	[RFC4860]
18	GENERIC-AGGREGATE-IP6	[RFC4860]

L'IANA a aussi modifié le registre des paramètres IP, sous registre 'Noms de classes, numéros de classes, et types de classes', et alloué un nouveau numéro de classe pour la classe SESSION-OF-INTEREST et deux nouveaux C-Types pour cette classe, selon le tableau ci-dessous :

Numéro de classe	Nom de classe	Référence
132	SESSION-OF-INTEREST	[RFC4860]
Types de classes ou C-Types :		
1	GENERIC-AGG-IP4-SOI	[RFC4860]
2	GENERIC-AGG-IP6-SOI	[RFC4860]

Ces allocations sont en accord avec la [RFC3936].

8. Remerciements

Le présent document emprunte beaucoup à la [RFC3175]. Il emprunte aussi les concepts d'accès de destination virtuel et d'accès de destination virtuel étendu à, respectivement, la [RFC2207] et la [RFC3209].

Nous remercions Fred Baker, Roger Levesque, Carol Iturralde, Daniel Voce, Anil Agarwal, Alexander Sayenko, et Anca Zamfir de leurs apports au contenu de ce document. Merci à Steve Kent de ses commentaires pertinents sur l'usage des réservations RSVP dans les environnements IPsec.

Ran Atkinson, Fred Baker, Luc Billot, Pascal Delprat, et Eric Vyncke ont fourni des conseils et suggestions pour la section des considérations sur la sécurité.

9. Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))
- [RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "[Protocole de réservation de ressource](#) (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (MàJ par [RFC2750](#), [RFC3936](#), [RFC4495](#), [RFC6780](#)) (P.S.)
- [RFC2207] L. Berger, T. O'Malley, "Extensions [RSVP pour flux de données IPsec](#)", septembre 1997. (P.S.)
- [RFC2747] F. Baker, B. Lindell, M. Talwar, "[Authentification cryptographique RSVP](#)", janvier 2000. (MàJ par [RFC3097](#)) (P.S.)
- [RFC3097] R. Braden, L. Zhang, "[Authentification cryptographique RSVP](#) – mise à jour de la valeur de type de message", avril 2001. (P.S.)
- [RFC3140] D. Black et autres, "[Codes d'identification de comportement par bond](#)", juin 2001. (P.S.)
- [RFC3175] F. Baker et autres, "[Agrégation de RSVP](#) pour réservations IPv4 et IPv6", septembre 2001. (MàJ par [RFC5350](#)) (P.S.)
- [RFC3936] K. Kompella, J. Lang, "[Procédures de modification du protocole de réservation de ressources](#) (RSVP)", octobre 2004. ([BCP0096](#))
- [RFC4303] S. Kent, "[Encapsulation de charge utile](#) de sécurité dans IP (ESP)", décembre 2005. (Remplace [RFC2406](#)) (P.S.)

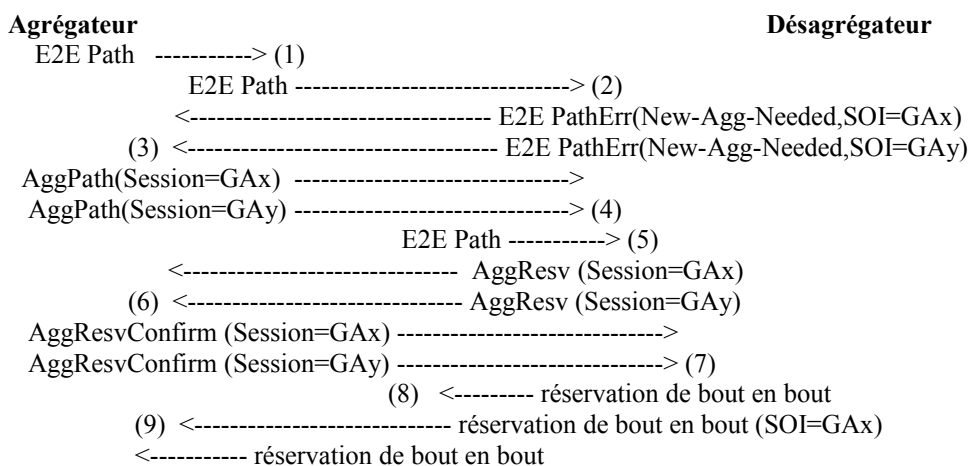
10. Références pour information

- [RFC2209] R. Braden, L. Zhang, "[Protocole de réservation de ressource](#) (RSVP) -- version 1 : règles de traitement de message", septembre 1997. (Information)
- [RFC2746] A. Terzis, J. Krawczyk, J. Wroclawski, L. Zhang, "Fonctionnement de [RSVP sur tunnels IP](#)", janvier 2000. (P.S.)
- [RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "[Encapsulation d'acheminement générique](#) (GRE)", mars 2000.
- [RFC3181] S. Herzog, "[Élément de politique de priorité](#) par préemption signalée", octobre 2001. (Remplace [RFC2751](#)) (P.S.)

- [RFC3209] D. Awduche, et autres, "[RSVP-TE : Extensions à RSVP pour les tunnels LSP](#)", décembre 2001. (Mise à jour par [RFC3936](#), [RFC4420](#), [RFC4874](#), [RFC5151](#), [RFC5420](#), [RFC6790](#))
- [RFC4495] J. Polk, S. Dhesikan, "[Extension au protocole de réservation](#) de ressource (RSVP) pour la réduction de bande passante d'un flux de réservation", mai 2006. (MàJ [RFC2205](#)) (P.S.)
- [RFC4923] F. Baker, P. Bose, "Signalisation de la qualité de service (QS) dans un réseau privé virtuel incorporé", août 2007. (Info.)

Appendice A. Exemple de flux de signalisation

Cet appendice ne fournit pas de spécification supplémentaire. Il illustre seulement la spécification détaillée à la Section 4 par un flux possible de messages de signalisation RSVP. Ce flux suppose un environnement où les réservations de bout en bout sont agrégées sur des réservations RSVP génériques agrégées. Il illustre un flux possible de messages RSVP qui pourrait avoir lieu dans l'établissement réussi d'une réservation en envoi individuel de bout en bout qui est la première entre une certaine paire d'agrégateur/désagrégateur.



- (1) L'agrégateur transmet le E2E Path dans la région d'agrégation après avoir modifié son numéro de protocole IP en RSVP-E2E-IGNORE
- (2) Supposons qu'il n'existe pas de chemin agrégé. Pour être capable de mettre précisément à jour l'ADSPEC du chemin de bout en bout, le désagrégateur a besoin de l'ADSPEC du chemin agrégé. Dans cet exemple, le désagrégateur choisit de donner pour instruction à l'agrégateur d'établir les états de chemin agrégé pour les deux identifiants de PHB pris en charge. Pour faire cela, le désagrégateur envoie deux messages E2E PathErr avec un code PathErr de New-Agg-Needed. Les deux messages PathErr contiennent aussi un objet SESSION-OF-INTEREST (SOI). Dans le premier E2E PathErr, le SOI contient une SESSION GENERIC-AGGREGATE (GAX) dont le PHB-ID est réglé à x. Dans le second E2E PathErr, le SOI contient une SESSION GENERIC-AGGREGATE (GAy) dont le PHB-ID est réglé à y. Dans les deux messages la SESSION GENERIC-AGGREGATE contient une adresse de désagrégateur indépendante de l'interface à l'intérieur de la DestAddress et les valeurs appropriées dans les champs vDstPort et Extended vDstPort.
- (3) L'agrégateur suit la demande du désagrégateur et signale un chemin agrégé pour les deux sessions GENERIC-AGGREGATE (GAX et GAy).
- (4) Le désagrégateur prend en compte les informations contenues dans l'ADSPEC provenant des deux chemins agrégés et met à jour en conséquence l'ADSPEC de chemin de bout en bout. Le désagrégateur modifie aussi le numéro de protocole IP du chemin de bout en bout à RSVP avant de le transmettre.
- (5) Dans cet exemple, le désagrégateur choisit de procéder immédiatement à l'établissement de réservations agrégées génériques pour les deux identifiants de PHB. En effet, le désagrégateur peut être vu comme anticipant la demande réelle de réservations de bout en bout afin que des ressources soient disponibles sur les réservations agrégées génériques quand les demandes de réservation de bout en bout arrivent, afin d'accélérer l'établissement des réservations de bout en bout. On suppose aussi que le désagrégateur inclut la demande facultative ResvConfirm Request dans ces réservations agrégées.

- (6) L'agrégateur se conforme simplement à la demande ResvConfirm reçue et retourne le ResvConfirm agrégé correspondant.
- (7) Le désagrégateur a une confirmation explicite que les deux réservations agrégées sont établies.
- (8) À réception de la réservation de bout en bout, le désagrégateur applique la politique de transposition définie par l'administrateur de réseau pour transposer la réservation de bout en bout en une réservation agrégée générique. Supposons que cette politique soit telle que la réservation de bout en bout soit transposée en la réservation agrégée générique avec le PHB-ID=x. Le désagrégateur sait qu'une réservation agrégée générique (GAX) est en place pour le PHB-ID correspondant depuis (7). Le désagrégateur effectue un contrôle d'admission de la réservation de bout en bout sur la réservation agrégée générique pour le PHB-ID=x (GAX). En supposant que la réservation agrégée générique pour le PHB-ID=x (GAX) a été établie avec une bande passante suffisante pour prendre en charge la réservation de bout en bout, le désagrégateur ajuste son compteur, traquant la bande passante inutilisée sur la réservation agrégée générique. Ensuite, il transmet la réservation de bout en bout à l'agrégateur en incluant un objet SESSION-OF-INTEREST portant la transposition choisie en GAX (et donc sur le PHB-ID=x).
- (9) L'agrégateur enregistre la transposition de la réservation de bout en bout sur GAX (et sur le PHB-ID=x). L'agrégateur retire l'objet SOI et transmet la réservation de bout en bout à l'envoyeur.

Adresse des auteurs

Francois Le Faucheur
Cisco Systems, Inc.
Village d'Entreprise Green Side - Batiment T3
400, Avenue de Roumanille
06410 Biot Sophia-Antipolis
France
mél : flefauch@cisco.com

Bruce Davie
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
mél : bds@cisco.com

Pratik Bose
Lockheed Martin
700 North Frederick Ave.
Gaithersburg, MD 20879
USA
mél : pratik.bose@lmco.com

Chris Christou
Booz Allen Hamilton
13200 Woodland Park Road
Herndon, VA 20171
USA
mél : christou_chris@bah.com

Michael Davenport
Booz Allen Hamilton
5220 Pacific Concourse Drive
Los Angeles, CA 90045
USA
mél : davenport_michael@bah.com

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2006)

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

Le présent document et les informations contenues sont fournies 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, le IETF TRUST et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat

de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

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