Groupe de travail Réseau
Request for Comments : 4804
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

F. Le Faucheur, éditeur
Cisco Systems, Inc.
février 2007

Agrégation des réservations du protocole de réservation de ressource (RSVP) sur tunnels TE/DS-TE MPLS

Résumé
La RFC 3175 spécifie l'agrégation des réservations de bout en bout du protocole de réservation de ressource (RSVP, *Resource ReSerVation Protocol*) sur des réservations RSVP agrégées. Le présent document spécifie l'agrégation de réservations RSVP de bout en bout sur des tunnels d'ingénierie du trafic MPLS (TE, *Traffic Engineering*) ou des tunnels d'ingénierie du trafic MPLS à capacité Diffserv (DS-TE, *Diffserv-aware MPLS Traffic Engineering*). Cette approche se fonde sur la RFC 3175 et modifie simplement les procédures correspondantes pour le fonctionnement sur les tunnels MPLS TE au lieu des réservations RSVP agrégées. Cette approche peut être utilisée pour réaliser le contrôle d'admission d'un très grand nombre de flux de manière adaptable car les appareils dans le cœur de réseau ne connaissent pas les réservations RSVP de bout en bout et connaissent seulement les tunnels MPLS TE.

Table des matières

1. Introduction

L'architecture des services intégrés (Intserv, *Integrated Services*) [RFC1633] donne un moyen pour la livraison de qualité de service de bout en bout aux applications sur des réseaux hétérogènes.

La [RFC2205] définit le protocole de réservation de ressources qui peut être utilisé par les applications pour demander des ressources au réseau. Le réseau répond en admettant ou rejetant explicitement ces demandes RSVP. Certaines applications qui ont des exigences de ressources quantifiables expriment ces exigences en utilisant les paramètres Intserv comme défini dans les spécifications de service Intserv appropriées ([RFC2212], [RFC2211]).

L'architecture des services différenciés (DiffServ, *Differentiated Services*) ([RFC2475]) a alors été développée pour prendre en charge le traitement différencié des paquets dans des environnements à très grande échelle. À la différence de l'orientation par flux de Intserv et RSVP, les réseaux Diffserv classent les paquets en un petit nombre de flux agrégés ou "classes", sur la base du codet Diffserv (DSCP, *Diffserv codepoint*) dans l'en-tête de paquet IP. À chaque routeur Diffserv, les paquets sont soumis à un "comportement par bond" (PHB, *per-hop behavior*) qui est invoqué par le DSCP. Le principal avantage de Diffserv est son adaptabilité. Diffserv élimine le besoin de l'état par flux et du traitement par flux, et donc s'adapte bien aux grands réseaux.

Cependant, DiffServ ne comporte aucun mécanisme pour la communication entre les applications et le réseau. Donc, comme précisé dans la [RFC2998], des avantages significatifs peuvent être obtenus en utilisant Intserv sur Diffserv incluant le contrôle d'admission fondé sur la ressource, le contrôle d'admission fondé sur la politique, l'assistance dans l'identification/classification du trafic, et le conditionnement du trafic. Comme exposé dans la [RFC2998], Intserv peut opérer sur Diffserv de nombreuses façons. Par exemple, la région Diffserv peut être provisionnée de façon statique ou avoir la capacité RSVP. Quand elle a la capacité RSVP, plusieurs mécanismes peuvent être utilisés pour prendre en charge le provisionnement dynamique et le contrôle d'admission fondé sur la topologie, incluant des réservations RSVP agrégées, RSVP par flux, ou un courtier de bande passante. L'avantage de l'utilisation de réservations RSVP agrégées est que cela offre un contrôle d'admission dynamique, connaissant la topologie sur la région Diffserv sans réservations par flux et le niveau associé de signalisation RSVP dans le cœur Diffserv. À son tour, cela permet un contrôle d'admission dynamique, conscient de la topologie, des flux qui exigent des réservations de qualité de service sur le cœur Diffserv même quand le nombre total de ces flux portés sur le cœur Diffserv est extrêmement grand.

Les [RFC3175] et [RFC4860] décrivent en détails comment effectuer une telle agrégation de réservations RSVP de bout en bout sur des réservations RSVP agrégées dans un nuage Diffserv. Elles établissent une architecture où plusieurs réservations RSVP de bout en bout partageant le même routeur d'entrée (agrégateur) et routeur de sortie (désagrégateur) aux bordures d'une "région d'agrégation" peuvent être transposées en une seule réservation agrégée au sein de la région d'agrégation. Cela réduit considérablement la quantité d'états de réservation qui doivent être conservés par les routeurs dans la région d'agrégation. De plus, le trafic appartenant aux réservations agrégées est classé dans le chemin des données en utilisant seulement le marquage Diffserv.

La [RFC2702] décrit comment les tunnels d'ingénierie du trafic (TE, *Traffic Engineering*) MPLS peuvent être utilisés pour porter des agrégats arbitraires de trafic pour les besoins de l'ingénierie du trafic. La [RFC3209] spécifie comment de tels tunnels MPLS TE peuvent être établis en utilisant la signalisation RSVP-TE. MPLS TE utilise l'acheminement fondé sur la contrainte pour calculer le chemin pour un tunnel TE. Ensuite, le contrôle d'admission est effectué durant l'établissement des tunnels TE pour assurer qu'ils reçoivent les ressources qu'ils demandent.

La [RFC3564] présente les exigences des fournisseurs de service pour la prise en charge de l'ingénierie de trafic MPLS à capacité Diffserv (DS-TE, *Diffserv-aware MPLS Traffic Engineering*). Avec DS-TE, des tunnels DS-TE séparés peuvent être utilisés pour porter différentes classes de trafic Diffserv, et différentes contraintes de ressources peuvent être appliquées pour ces différentes classes. La [RFC4124] spécifie les extensions de signalisation RSVP-TE ainsi que les extensions à OSPF et de système intermédiaire à système intermédiaire (IS-IS, *Intermediate System to Intermediate System*) pour la prise en charge de DS-TE.

Dans le reste de ce document, on se réfère aux tunnels TE aussi bien qu'aux tunnels DS-TE simplement comme "tunnels TE".

Les tunnels TE ont beaucoup en commun avec les réservations RSVP agrégées utilisées dans les [RFC3175] et [RFC4860] :

- Un tunnel TE est soumis au contrôle d'admission et est donc effectivement une réservation agrégée de bande passante.
- Dans le plan des données, la programmation des paquets s'appuie exclusivement sur la classe Diffserv et les PHB.
- Les tunnels TE et les réservations RSVP agrégées sont tous deux contrôlés par des appareils "intelligents" sur le bord

du "cœur d'agrégation" (extrémité de tête et extrémité de queue dans le cas des tunnels TE ; agrégateur et désagrégateur dans le cas des réservations RSVP agrégées.
- Les tunnels TE et les réservations RSVP agrégées sont signalés en utilisant le protocole RSVP (avec des extensions définie dans les [RFC3209] et [RFC4124] respectivement pour les tunnels TE et les tunnels DS-TE).

Le présent document fournit une spécification détaillée pour effectuer l'agrégation de réservations RSVP de bout en bout sur des tunnels MPLS TE (qui agissent comme des réservations agrégées dans le cœur). Le présent document s'appuie sur les procédures d'agrégation RSVP définies dans les [RFC3175] et [RFC4860], et change seulement ce qui est nécessaire pour opérer sur les tunnels TE. Avec les [RFC3175] et [RFC4860], un certain nombre de responsabilités (comme la transposition des réservations de bout en bout en réservations agrégées et le redimensionnement des réservations agrégées) sont attribuées au désagrégateur (qui est l'équivalent de l'extrémité de queue du tunnel) tandis qu'avec TE, les tunnels sont contrôles par l'extrémité de tête du tunnel. Donc, le principal changement par rapport aux procédures d'agrégation RSVP définies dans les [RFC3175] et [RFC4860] est de modifier ces procédures pour réallouer ces responsabilités du désagrégateur à l'agrégateur (c'est-à-dire, l'extrémité de tête du tunnel).

La [RFC4206] définit comment agréger les chemins de commutation d'étiquettes (LSP, *Label Switched Path*) de MPLS TE en créant une hiérarchie de ces LSP. Cela implique d'incorporer de bout en bout les LSP dans un LSP agrégé dans le cœur (en utilisant la construction de pile d'étiquettes). Comme les LSP TE de bout en bout sont eux-mêmes signalés avec RSVP-TE et réservent des ressources à chaque bond, cela peut être vu comme une forme d'agrégation de réservations RSVP(-TE) sur les tunnels MPLS TE. Le présent document s'appuie sur les similarités entre l'incorporation des LSP TE sur les tunnels TE et l'agrégation RSVP sur les tunnels TE, et réutilise les procédures de la [RFC4206] chaque fois que possible.

Le présent document s'appuie aussi sur les concepts de "RSVP sur tunnels" de la [RFC2746]. Il diffère de cette spécification de la façon suivante :
- Le présent document décrit le fonctionnement sur les tunnels MPLS, tandis que la RFC 2746 décrit le fonctionnement avec les tunnels IP. Une conséquence de cette différence est le besoin de traiter le saut de l'avant dernier bond (PHP, *penultimate hop popping*).
- Les tunnels MPLS-TE réservent par nature les ressources, tandis que les tunnels de la RFC 2746 n'ont pas de réservations de ressource par défaut. Cela conduit à des simplifications dans le présent document.
- Le présent document s'appuie sur le fait qu'il y a exactement une réservation agrégée par tunnel MPLS-TE, tandis que la RFC 2746 permet un modèle où une réservation est établie sur le chemin du tunnel pour chaque flux de bout en bout.
- On a supposé dans le présent document qu'un tunnel MPLS-TE va porter du trafic réservé et rien que du trafic réservé, ce qui va à l'encontre de l'exigence de la RFC 2746 de distinguer le trafic réservé et non réservé qui traverse le même tunnel en utilisant des encapsulations distinctes.
- Il peut y avoir plusieurs tunnels MPLS-TE qui partagent des routeurs commun d'extrémité de tête et d'extrémité de queue, avec la politique de l'extrémité de tête qui détermine quel tunnel est approprié pour un flux particulier. Ce scénario ne paraît pas être traité dans la RFC 2746.

En même temps, le présent document a bien de nombreuses similitudes avec la RFC 2746. Les tunnels MPLS-TE sont des tunnels de "type 2" dans la nomenclature de la RFC 2746 : "La liaison (logique) peut être capable de promettre qu'un certain niveau global de ressources est disponible pour porter le trafic, mais n'alloue pas les ressources spécifiquement à un flux de données individuel".

L'agrégation des réservations RSVP de bout en bout sur les tunnels TE combine les avantages de la [RFC3175] et de la [RFC4860] avec les avantages de MPLS, incluant que :

- Les applications peuvent bénéficier d'un contrôle d'admission dynamique, respectueux de la topologie, fondé sur les ressources sur tout segment du chemin de bout en bout, incluant le cœur.

- Conformément au comportement régulier de RSVP, RSVP n'impose pas de charge aux routeurs lorsque un tel contrôle d'admission n'est pas nécessaire (par exemple, si les liaisons amont et aval du cœur MPLS TE sont largement surdimensionnées comparées à la capacité du cœur, le contrôle d'admission n'est pas exigé sur ces liaisons surdimensionnées et RSVP n'a pas besoin d'être traité sur les bonds de routeur correspondants).

- L'adaptabilité du cœur n'est pas affectée (par rapport au modèle traditionnel de déploiement de MPLS TE) car le cœur reste ignorant des réservations RSVP de bout en bout et a seulement à conserver les tunnels TE agrégés par le classement du chemin des données et la programmation dans le cœur s'appuie simplement sur le mécanisme Diffserv (ou plus précisément sur les mécanismes MPLS Diffserv, comme spécifié dans la [RFC3270]).

- La réservation agrégée (et donc le trafic provenant des réservations de bout en bout correspondantes) peut être à ingénierie du réseau via l'utilisation de l'acheminement fondé sur la contrainte (par exemple, affinités, optimisation sur

différentes métriques) et quand nécessaire peut tirer parti des ressources sur d'autres chemins que le plus court.

- Les réservations agrégées (et donc le trafic provenant des réservations de bout en bout correspondantes) peuvent être protégées contre les défaillances par l'utilisation du réacheminement rapide de MPLS.

Le présent document, comme les [RFC3175] et [RFC4860], couvre l'agrégation de sessions en envoi individuel. L'agrégation de sessions en diffusion groupée fera l'objet d'études ultérieures.

2. Spécification 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].

3. Définitions

Pour faciliter la lisibilité, un certain nombre de définitions de la [RFC3175] ainsi que les définitions de termes couramment utilisés dans MPLS TE sont fournies ici :

Agrégateur : c'est le processus dans (ou associé au) le routeur au bord d'entrée de la région d'agrégation (par rapport à la réservation RSVP de bout en bout) et qui se comporte en accord avec la [RFC3175]. Dans ce document, c'est aussi l'extrémité de tête du tunnel TE.

Désagrégateur : c'est le processus dans le (ou associé au) routeur au bord de sortie de la région d'agrégation (par rapport à la réservation RSVP de bout en bout) et qui se comporte en accord avec la [RFC3175]. Dans ce document, c'est aussi l'extrémité de queue du tunnel TE.

E2E *(End to end)* : de bout en bout

Réservation E2E : c'est une réservation RSVP telle que :
(i) les messages Path correspondants sont initiés en amont de l'agrégateur et terminés en aval du désagrégateur, et
(ii) les messages Resv correspondants sont initiés en aval du désagrégateur et terminés en amont de l'agrégateur, et
(iii cette réservation RSVP est agrégée sur un tunnel MPLS-TE entre l'agrégateur et le désagrégateur.
Une réservation E2E RSVP peut être une réservation par flux. Autrement, la réservation E2E peut elle-même être une réservation agrégée de divers types (par exemple, réservation IP agrégée, réservation IPsec agrégée). Voir aux Sections 5 et 6 les détails des types de réservations RSVP de bout en bout. Selon le fonctionnement régulier de RSVP, les réservations RSVP de bout en bout sont unidirectionnelles.

Extrémité de tête : c'est le routeur de commutation d'étiquettes chargé d'établir, maintenir, et supprimer un tunnel TE.

Extrémité de queue : c'est le routeur de commutation d'étiquettes chargé de terminer un certain tunnel TE.

LSR de transit : c'est un routeur de commutation d'étiquettes qui est sur le chemin d'un certain tunnel TE et n'est ni l'extrémité de tête ni l'extrémité de queue.

4. Opérations d'agrégation RSVP sur TE avec des tunnels pré-établis

Les [RFC3175] et [RFC4860] prennent en charge les opérations à la fois dans le cas où les réservations RSVP agrégées sont pré-établies et dans celui où agrégateurs et désagrégateurs ont à se découvrir dynamiquement l'un l'autre et établir dynamiquement les réservations RSVP agrégées nécessaires.

De façon similaire, l'agrégation RSVP sur des tunnels TE pourrait opérer à la fois dans le cas où les tunnels TE sont pré-établis et dans celui où les tunnels doivent être établis dynamiquement.

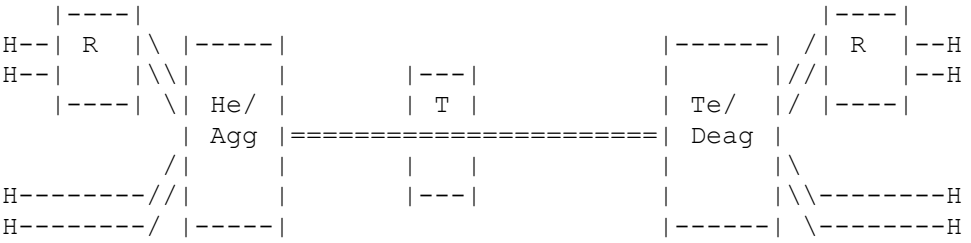
Dans le présent document, on fournit une description détaillée des procédures dans le cas où les tunnels TE sont déjà établis. Ces procédures se fondent sur celles définies dans la [RFC4206]. Les aspects d'acheminement discutés à la

Section 3 de la [RFC4206] ne sont pas pertinents ici parce que ils visent à permettre l'acheminement fondé sur la contrainte des LSP TE de bout en bout pour prendre en compte les tunnels TE (agrégats). Dans le présent document, les réservations RSVP de bout en bout à agréger sur les tunnels TE s'appuient sur l'acheminement de plus court chemin en premier (SPF, *Shortest Path First*) régulier. Cependant, comme déjà mentionné dans la [RFC4206], on note qu'un tunnel TE peut être annoncé dans IS-IS ou OSPF, pour être utilisé en SPF normal par les nœuds en amont de l'agrégateur. Ceci affecterait l'acheminement SPF et donc l'acheminement des réservations RSVP de bout en bout. Le contrôle des frontières d'agrégation discuté à la Section 6 de la [RFC4206] n'est pas non plus pertinent ici. Cela utilise des informations échangées dans les protocoles GMPLS pour découvrir dynamiquement la frontière d'agrégation. Dans le présent document, les tunnels TE sont pré-établis, de sorte que la frontière d'agrégation peut être facilement déduite. Les aspects de signalisation discutés au paragraphe 6.2 de la [RFC4206] s'appliquent à l'établissement/terminaison des tunnels TE agrégés quand c'est déclenché par les mécanismes de GMPLS (par exemple, par suite d'une demande d'établissement de LSP TE de bout en bout reçue à la frontière d'agrégation). Comme le présent document suppose des tunnels pré-établis, ces aspects ne sont pas pertinents ici. Les aspects de signalisation discutés au paragraphe 6.1 de la [RFC4206] se rapportent à l'établissement/maintenance des LSP TE de bout en bout sur le tunnel TE agrégé. Le présent document décrit comment utiliser les mêmes procédures que spécifiées au paragraphe 6.1 de la [RFC4206], mais pour l'établissement de réservations RSVP de bout en bout (au lieu de LSP TE de bout en bout) sur les tunnels TE. Ceci est traité à la Section 4 du présent document.

Le pré-établissement de tunnels TE peut être déclenché par tous mécanismes incluant, par exemple, la configuration manuelle ou l'établissement automatique d'un maillage de tunnels TE à travers la découverte dynamique de membres d'un maillage TE comme c'est permis par la [RFC4972].

Les procédures dans le cas de tunnels TE établis dynamiquement feront l'objet d'études ultérieures.

4.1 Modèle de référence



H = Hôte demandant des réservations RSVP de bout en bout
R = Routeur RSVP
He/Agg = tunnel TE extrémité de tête/agrégateur
Te/Deag = tunnel TE extrémité de queue/désagrégateur
T = LSR de transit
-- = réservation RSVP de bout en bout
== = tunnel TE

4.2 Réception du message Chemin de bout en bout par l'agrégateur

Le premier événement est l'arrivée du message Path E2E chez l'agrégateur. L'agrégateur DOIT suivre les procédures RSVP traditionnelles pour le traitement de ce message Path E2E augmenté des extensions documentées dans cette section.

L'agrégateur DOIT d'abord tenter de transposer la réservation E2E sur un tunnel TE. Cette décision est prise en accord avec les informations d'acheminement ainsi qu'avec toutes informations de politique locale qui peuvent être disponibles chez l'agrégateur. Des exemples de ces politiques apparaissent dans les paragraphes qui suivent. Juste à des fins d'illustration, parmi de nombreux autres critères, de telles politiques de transposition pourraient prendre en compte le type de service Intserv, l'identité d'application [RFC3182], et/ou la préemption signalée [RFC3181] de la réservation E2E (par exemple, l'agrégateur peut prendre en compte la priorité de préemption des réservations RSVP E2E et les priorités d'établissement de tunnel TE MPLS et/ou de garde quand il transpose la réservation E2E en un tunnel MPLS-TE).

Il y a des situations où l'agrégateur est capable de prendre une décision de transposition finale. Ce serait le cas, par exemple, si il y a un seul tunnel TE vers la destination et si la politique est de transposer toute réservation E2E RSVP sur les tunnels TE.

Il y a des situations où l'agrégateur n'est pas capable de faire une détermination finale. Ce serait le cas, par exemple, si

l'acheminement identifie deux tunnels DS-TE vers la destination, un appartenant au type de classe DS-TE 1 et un de type de classe 0, si la politique est de transposer les réservations de service Intserv garanti en tunnel de type de classe 1 et les réservations de charge contrôlée Intserv en un tunnel de type de classe 0, et si le message Path E2E RSVP annonce les deux service garanti et charge contrôlée.

Qu'elle soit finale ou tentative, l'agrégateur prend une décision de transposition et choisit un tunnel TE. Avant de transmettre le message Path E2E vers le receveur, l'agrégateur DEVRAIT mettre à jour la ADSPEC à l'intérieur du message Path E2E pour refléter l'impact du nuage MPLS TE sur la qualité de service réalisable par le flux E2E. Cette mise à jour est une affaire locale et peut être fondée sur des informations configurées, on sur les informations disponibles dans la base de données de topologie MPLS TE, sur le chemin actuel du tunnel TE, sur des informations collectées via la signalisation RSVP-TE, ou sur une combinaison de ces informations. Mettre à jour l'ADSPEC permet aux receveurs qui prennent en compte les informations collectées dans les ADSPEC au sein du réseau (comme les estimations de délai et de bande passante) de prendre des décisions de réservation mieux informées.

L'agrégateur DOIT ensuite transmettre le message Path E2E au désagrégateur (qui est l'extrémité de queue du tunnel TE choisi). En accord avec la [RFC4206], l'agrégateur DOIT envoyer le message Path E2E avec un objet IF_ID RSVP_HOP au lieu d'un objet RSVP_HOP. L'identification d'interface de données DOIT identifier le tunnel TE.

Pour envoyer le message Path E2E, l'agrégateur DOIT l'adresser directement au désagrégateur en réglant l'adresse de destination dans l'en-tête IP du message Path E2E à l'adresse du désagrégateur. L'alerte de routeur n'est pas établie dans le message Path E2E.

Facultativement, l'agrégateur PEUT aussi encapsuler le message Path E2E dans un tunnel IP ou dans le tunnel TE lui-même.

Sans considération de la méthode d'encapsulation, l'alerte de routeur n'est pas établie. Donc, le message Path E2E ne va pas être visible aux routeurs le long du chemin de l'agrégateur au désagrégateur. Donc, à la différence des procédures des [RFC3175] et [RFC4860], le numéro de protocole IP n'a pas besoin d'être modifié en "RSVP-E2E-IGNORE"; il DOIT être laissé tel qu'il est (indiquant "RSVP") réglé par l'agrégateur.

Dans certains environnements, l'agrégateur et le désagrégateur PEUVENT aussi agir comme passerelles de sécurité IPsec afin de fournir la protection IPsec au trafic E2E quand il transite entre l'agrégateur et le désagrégateur. Dans ce cas, pour transmettre le message Path E2E au désagrégateur, l'agrégateur DOIT envoyer le message Path E2E dans le tunnel IPsec pertinent se terminant sur le désagrégateur.

Les messages E2E PathTear et ResvConf DOIVENT être transmis par l'agrégateur au désagrégateur exactement comme les messages Path.

4.3 Traitement du message Chemin de bout en bout par les LSR de transit

Comme le message Path E2E est adressé directement au désagrégateur et n'a pas d'alerte de routeur établi, il est caché aux LSR de transit.

4.4 Réception du message Chemin de bout en bout par le désagrégateur

À réception du message Path E2E qui lui est adressé, le désagrégateur va remarquer que le numéro de protocole IP est réglé à "RSVP" et va donc effectuer le traitement RSVP du message Path E2E.

Comme dans la [RFC4206], la confrontation du TTL IP au TTL RSVP NE DOIT PAS être faite. Le désagrégateur est informé que cette confrontation ne doit pas être faite à cause de la présence de l'objet IF_ID RSVP HOP.

Le désagrégateur PEUT prendre en charge l'option d'effectuer les vérifications suivantes (définies dans la [RFC4206]) par le receveur Y de l'objet IF_ID RSVP_HOP :

1. S'assurer que l'interface de données identifiée dans l'objet IF_ID RSVP_HOP se termine bien sur Y.
2. Trouver "l'autre extrémité" de l'interface de données ci-dessus, c'est-à-dire, X. S'assurer que le bond précédent (PHOP, *Previous hop)* dans l'objet IF_ID RSVP_HOP est une adresse de canal de contrôle qui appartient au même nœud que X.

Les informations nécessaires pour effectuer ces vérifications ne peuvent pas toujours être disponibles au désagrégateur. Donc, le désagrégateur DOIT accepter de fonctionner dans les environnements où les vérifications ne peuvent pas être

faites.

Le désagrégateur DOIT transmettre le Path E2E en aval vers le receveur. Ce faisant, le désagrégateur règle l'adresse de destination dans l'en-tête IP du message Path E2E à l'adresse IP trouvée dans le champ Adresse de destination de l'objet Session. Le désagrégateur établit aussi l'alerte de routeur.

Un message PathErr E2E envoyé par le désagrégateur en réponse au message Path E2E (qui contient un objet IF_ID RSVP_HOP) DEVRAIT contenir un objet IF_ID RSVP_HOP.

4.5 Traitement du message Réservation de bout en bout par le désagrégateur

Conformément au fonctionnement normal de RSVP, après la réception du Path E2E, le receveur génère un message Resv E2E qui voyage vers l'amont bond par bond jusqu'à l'envoyeur.

À réception du Resv E2E, le désagrégateur DOIT suivre les procédures traditionnelles de RSVP pour la réception de message Resv E2E. Cela inclut d'effectuer le contrôle d'admission pour le segment en aval du désagrégateur et de transmettre le message Resv E2E au PHOP signalé plus tôt dans le message Path E2E et qui identifie l'agrégateur. Comme le message Resv E2E est adressé directement à l'agrégateur et ne porte pas l'option Alerte de routeur (conformément aux procédures traditionnelles de RSVP Resv) le message Resv E2E est caché aux routeurs entre le désagrégateur et l'agrégateur qui traitent donc le message Resv E2E comme un paquet IP normal.

Si l'agrégateur et le désagrégateur agissent aussi comme passerelles de sécurité IPsec, le désagrégateur DOIT envoyer le message Resv E2E dans le tunnel IPsec pertinent qui se termine sur l'agrégateur.

4.6 Traitement du message Réservation de bout en bout par l'agrégateur

L'agrégateur est chargé de s'assurer que la bande passante disponible et réservée est suffisante sur le tunnel TE approprié jusqu'au désagrégateur pour la réservation E2E.

À réception du message Resv E2E, l'agrégateur DOIT d'abord effectuer la transposition finale en le tunnel TE final (si la transposition précédente était seulement une tentative).

Si le tunnel n'a pas changé durant la transposition finale, l'agrégateur continue de traiter la réservation E2E comme décrit dans les quatre alinéas suivants.

L'agrégateur calcule la taille de la demande de ressources en utilisant les procédures RSVP traditionnelles. C'est-à-dire, il suit les procédures de la [RFC2205] pour déterminer les exigences de ressources à partir de la Tspec d'envoyeur et de la Flowspec contenues dans le message Resv. Ensuite il compare la demande de ressources avec les ressources disponibles du tunnel TE choisi.

Si une bande passante suffisante est disponible sur le tunnel TE final, l'agrégateur DOIT mettre à jour sa compréhension interne de la quantité du tunnel TE qui est utilisée et DOIT transmettre les messages Resv E2E au PHOP correspondant.

Comme noté dans la [RFC3175], une gamme de politiques PEUT être appliquée au redimensionnement de la réservation agrégée (dans ce cas, le tunnel TE). Par exemple, la politique peut être que la bande passante réservée du tunnel peut seulement être changée par configuration. Des politiques plus dynamiques sont aussi possibles, par lesquelles l'agrégateur peut tenter d'augmenter la bande passante réservée du tunnel en réponse à la quantité de bande passante allouée qui a été utilisée par les réservations de bout en bout. De plus, pour éviter les délais associés à l'augmentation de taille du tunnel, l'agrégateur peut tenter d'anticiper l'augmentation de la demande et ajuster la taille du tunnel TE avant le besoin réel des réservations de bout en bout. Afin de réduite les perturbations, l'agrégateur DEVRAIT utiliser les procédures de "faire avant de défaire" décrites dans la [RFC3209] pour altérer la bande passante du tunnel TE.
Si une bande passante suffisante n'est pas disponible sur le tunnel TE final, l'agrégateur DOIT suivre la procédure RSVP normale pour qu'une réservation soit faite avec une bande passante insuffisante pour la prendre en charge. C'est-à-dire, la réservation n'est pas installée et un message ResvError est renvoyé au receveur.
Si le tunnel n'a pas changé durant la transposition finale, l'agrégateur DOIT d'abord envoyer à nouveau au désagrégateur un message Path E2E avec l'identification d'interface de données IF_ID RSVP_HOP qui identifie le tunnel TE final. Si nécessaire, les informations d'ADSPEC dans ce message Path E2E DEVRAIENT être mises à jour. Ensuite, l'agrégateur DOIT

- soit éliminer le message Resv E2E

- soit poursuivre le traitement de la réservation de bout en bout de la même manière que dans le cas où le tunnel n'a pas changé (décrit plus haut).

Dans le premier cas, le contrôle d'admission sur le tunnel TE final (et la transmission du message Resv E2E en l'amont vers l'envoyeur) ne se produirait que quand l'agrégateur aura reçu le message Resv E2E suivant (qui va être envoyé par le désagrégateur en réponse au message Path E2E renvoyé). Dans le second cas, le contrôle d'admission sur le tunnel final est effectué immédiatement par l'agrégateur, et si il réussit, le message Resv E2E est généré en amont vers l'envoyeur.

À réception d'un message ResvConf E2E de l'agrégateur, le désagrégateur DOIT transmettre le ResvConf E2E en aval vers le receveur. Ce faisant, le désagrégateur règle l'adresse de destination dans l'en-tête IP du message ResvConf E2E à l'adresse IP trouvée dans l'objet RESV_CONFIRM de la réservation correspondante. Le désagrégateur établit aussi l'alerte de routeur.

4.7 Transmission du trafic de bout en bout par l'agrégateur

Quand l'agrégateur reçoit un paquet de données appartenant à des réservations de bout en bout actuellement transposées sur un certain tunnel TE, l'agrégateur DOIT encapsuler le paquet dans ce tunnel TE.
Si l'agrégateur et le désagrégateur agissent aussi comme passerelles de sécurité IPsec, l'agrégateur DOIT aussi encapsuler le paquet de données dans le tunnel IPsec pertinent qui se terminé au désagrégateur avant la transmission dans le tunnel TE MPLS.

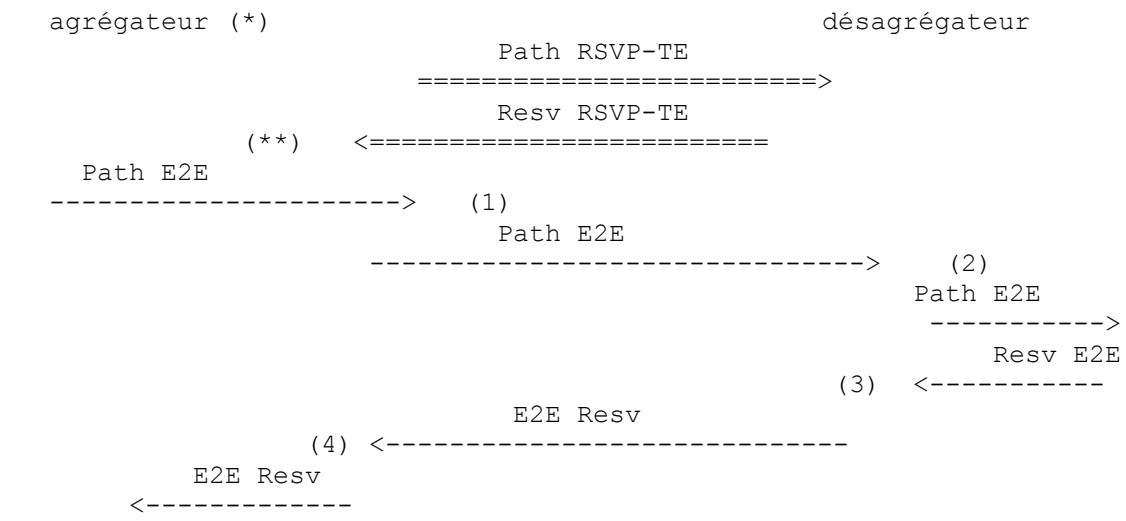
4.8 Suppression de réservations de bout en bout

Les réservations de bout en bout sont supprimées de la façon usuelle via PathTear, ResvTear, une fin de temporisation, ou par suite d'une condition d'erreur. Quand une réservation est retirée, l'agrégateur DOIT mettre à jour en conséquence sa vue locale des ressources disponibles sur le tunnel TE correspondant.

4.9 Suppression du tunnel TE

Si un tunnel TE devait disparaître (vraisemblablement à cause d'un changement de configuration, un changement de route, ou un événement de politique) l'agrégateur se comporte comme un routeur RSVP conventionnel en présence d'une défaillance de liaison. C'est-à-dire, il peut essayer de transmettre les messages Path sur un autre tunnel, si l'acheminement et la politique le permettent, ou il peut envoyer des messages Path_Error à l'envoyeur si un tunnel convenable n'existe pas. Dans le cas où les messages Path sont transmis sur un autre tunnel, qui se termine sur un désagrégateur différent, ou si la réservation est supprimée via des messages Path_Error, l'état de réservation établi sur le routeur qui agissait comme désagrégateur avant la disparition du tunnel TE, va arriver en fin de temporisation car il ne va plus être rafraîchi.

4.10 Exemple de flux de signalisation



(*) l'agrégateur est déclenché pour pré-établir le ou les tunnels TE
(**) le ou les tunnels TE sont pré-établis

(1) l'agrégateur tente de choisir le tunnel TE et transmet le message Path E2E au désagrégateur
(2) le désagrégateur transmet le message Path E2E au receveur
(3) le désagrégateur transmet le message Resv E2E à l'agrégateur
(4) l'agrégateur choisit le tunnel TE final, vérifie qu'il a une bande passante suffisante, et transmet le message Resv E2Eau PHOP. Si le tunnel final est différent du tunnel de la tentative de choix, l'agrégateur envoie à nouveau un message Path E2E avec un IF_ID RSVP_HOP mis à jour et éventuellement une ADSPEC mise à jour.

5. Applicabilité à IPv4 et IPv6

Les procédures définies dans ce document sont applicables à tous les cas suivants :
(1) Agrégation de réservations RSVP E2E IPv4 sur tunnels TE IPv4.
(2) Agrégation de réservations RSVP E2E IPv6 sur tunnels TE IPv6.
(3) Agrégation de réservations RSVP E2E IPv6 sur tunnels TE IPv4, pourvu qu'un mécanisme comme celui de la [RFC4798] soit utilisé par l'agrégateur et le désagrégateur pour l'acheminement du trafic IPv6 sur un cœur MPLS IPv4.
(4) Agrégation de réservations RSVP E2E IPv4 sur tunnels TE IPv6, pourvu qu'un mécanisme soit utilisé par l'agrégateur et le désagrégateur pour l'acheminement du trafic IPv4 sur MPLS IPv6.

6. Applicabilité des réservations de bout en bout

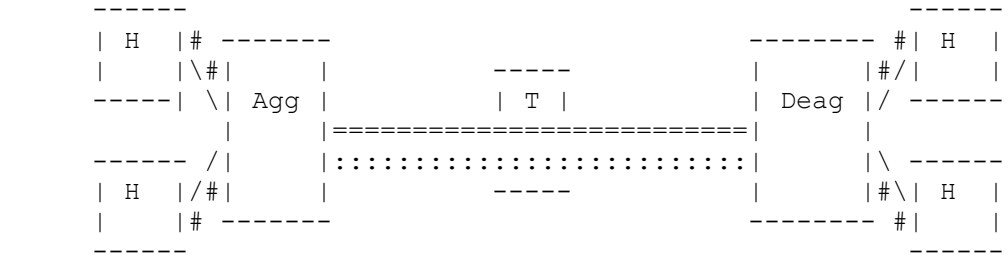
Les procédures définies dans ce document sont applicables à de nombreux types de réservations RSVP de bout en bout incluant les cas suivants :
(1) La réservation RSVP de bout en bout est une réservation par flux où le flux est caractérisé par le quintuplet usuel.
(2) La réservation de bout en bout est une réservation agrégée pour plusieurs flux, comme décrit dans la [RFC3175] ou la [RFC4860] où l'ensemble de flux est caractérisé par le triplet <adresse de source, adresse de destination, DSCP>.
(3) La réservation de bout en bout est une réservation pour flux protégé par IPsec. Par exemple, lorsque le flux est caractérisé par le triplet <adresse de source, adresse de destination, SPI> comme décrit dans la [RFC2207].

7. Exemples de scénarios de déploiement

7.1 Scénario de réservations de voix et de vidéo

Un exemple d'application des procédures spécifiées dans ce document est le contrôle d'admission de voix et de vidéo dans des environnements avec un très grand nombre d'hôtes. Dans l'exemple illustré ci-dessous, les hôtes génèrent des réservations de bout en bout par flux pour chacun de leurs flux vidéos associés à une visioconférence, chacun de leurs flux audios associés à une visioconférence, et chacun de leurs appels vocaux.

Ces réservations sont agrégées sur des tunnels DS-TE MPLS sur le cœur de paquet. La politique de transposition définie par l'utilisateur peut être que toutes les réservations pour les flux audio et vocaux soient transposées sur les tunnels DS-TE de type de classe 1, tandis que les réservations pour les flux vidéos soient transposées sur les tunnels DS-TE de type de classe 0.

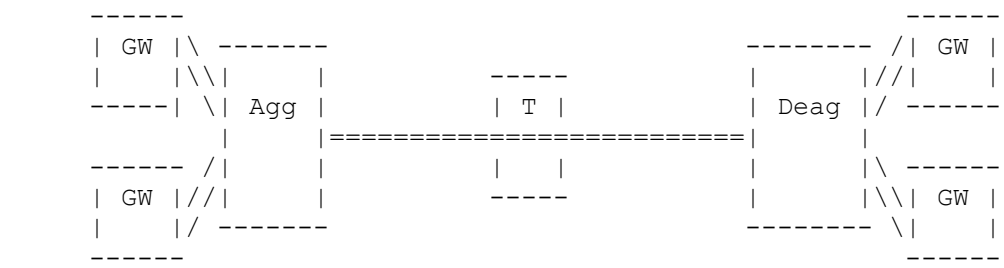


H = Hôte
Agg = agrégateur (extrémité de tête de tunnel TE)
Deagg = désagrégateur (extrémité de queue de tunnel TE)
T = LSR de transit

/ = réservation E2E RSVP pour un flux vocal
= réservation E2E RSVP pour un flux vidéo
== = tunnel DS-TE de type de classe 1
:: = tunnel DS-TE de type de classe 0

7.2 Scénario de circuit vocal RTPC/3G

Un exemple d'application des procédures spécifiées dans ce document est le contrôle d'admission d'appel vocal dans des environnements de circuits téléphoniques à grande échelle. Une passerelle de circuits VoIP peut générer une réservation RSVP agrégée pour tous les appels en place vers une autre passerelle de circuits VoIP distante donnée avec un redimensionnement de cette réservation agrégée dans une fonction d'étape dépendant du nombre actuel d'appels). Ensuite, ces réservations peuvent être agrégées sur des tunnels MPLS TE sur le cœur de paquet afin que l'extrémité de tête du tunnel agisse comme agrégateur et effectue le contrôle d'admission des réservations de passerelle de circuits en tunnels MPLS TE. Les tunnels MPLS TE peuvent être protégés par le réacheminement rapide MPLS. Ce scénario est illustré ci-dessous.



GW = passerelle VoIP
Agg = agrégateur (extrémité de tête de tunnel TE)
Deagg = désagrégateur (extrémité de queue de tunnel TE)
T = LSR de transit
/ = réservations agrégée RSVP de bout en bout de passerelle à passerelle
== = tunnel TE

8. Considérations sur la sécurité

Dans les environnements concernés par le présent document, les messages RSVP sont utilisés pour contrôler les réservations de ressources pour les flux de bout en bout en dehors de la région MPLS ainsi que pour contrôler les réservations de ressources pour les tunnels MPLS TE à l'intérieur de la région MPLS. Pour assurer l'intégrité de la réservation associée et des mécanismes de contrôle d'admission, les mécanismes définis dans les [RFC2747] et [RFC3097] peuvent être utilisés. Les mécanismes protègent l'intégrité des messages RSVP bond par bond et fournissent l'authentification des nœuds, protégeant par là contre la corruption et l'usurpation d'identité des messages RSVP. Ces mécanismes d'intégrité bond par bond peuvent naturellement être utilisés pour protéger les messages RSVP utilisés pour les réservations de bout en bout en dehors de la région MPLS, pour protéger les messages RSVP utilisés pour les tunnels MPLS TE à l'intérieur de la région MPLS, ou les deux. Ces mécanismes d'intégrité bond par bond RSVP peuvent aussi être utilisés pour protéger les messages RSVP utilisés pour les réservations de bout en bout quand ils transitent à travers la région MPLS. C'est parce que l'agrégateur et le désagrégateur se comportent comme des voisins RSVP du point de vue du flux de bout en bout (même si ils ne sont pas nécessairement des voisins IP ni des voisins RSVP-TE). Dans ce cas, l'agrégateur et le désagrégateur ont besoin d'utiliser un secret pré partagé.

Comme expliqué à la Section 6 de la [RFC3209], le filtrage du trafic associé à un tunnel MPLS TE peut seulement être effectué sur la base d'une étiquette MPLS, au lieu du quintuplé de la réservation conventionnelle RSVP selon la [RFC2205]. Donc, comme expliqué dans la [RFC3209], un administrateur peut souhaiter limiter le domaine sur lequel peuvent être établis les tunnels TE (qui sont utilisés pour l'agrégation des réservations RSVP de bout en bout conformément à la présente spécification). Voir à la Section 6 de la [RFC3209] une description de la façon dont le filtrage des messages RSVP associés aux tunnels MPLS TE peut être déployé à cette fin.

Le présent document se fonde en partie sur la [RFC3175], qui spécifie l'agrégation de réservations RSVP. La Section 5 de la [RFC3175] soulève le problème que parce que de nombreux flux de bout en bout peuvent partager une réservation agrégée, si la sécurité d'une réservation agrégée est compromise, cela a un effet multiplicateur dans ce sens que cela peut à

son tour compromettre la sécurité de nombreuses réservations de bout en bout dont la qualité de service dépend de la réservation agrégée. Ce souci s'applique aussi à l'agrégation RSVP sur les tunnels TE comme spécifié dans le présent document. Cependant, l'intégrité du fonctionnement des tunnels MPLS TE peut être protégée en utilisant les mécanismes discutés dans les paragraphes précédents. Aussi, alors que la [RFC3175] spécifie l'agrégation RSVP sur des réservations agrégées établies de façon dynamique, le présent document se restreint à l'agrégation RSVP sur des tunnels TE pré-établis. Cela réduit les risques pour la sécurité.

Dans le cas où les agrégateurs redimensionnent dynamiquement les tunnels TE sur la base du niveau actuel de réservation, il y a un risque que les tunnels TE utilisés pour l'agrégation RSVP accaparent les ressources dans le cœur, ce qui pourrait empêcher d'autres tunnels TE d'être établis. Il y a aussi des risques potentiels qu'un tel redimensionnement résulte en des calculs et de la signalisation significatifs ainsi que des désordres dans les chemins de tunnels. Ces risques peuvent être atténués par des options de configuration permettant le contrôle du redimensionnement dynamique de tunnel TE (taille maximum du tunnel TE, fréquence maximum de redimensionnement, etc.), et/ou éventuellement par utilisation, de la préemption TE.

La Section 5 de la [RFC3175] discute aussi de problèmes de sécurité spécifiques de l'agrégation RSVP relatifs à la nécessaire modification du numéro de protocole IP dans les messages Path RSVP de bout en bout qui traversent la région d'agrégation. Ce problème de sécurité ne s'applique pas au présent document car l'agrégation des réservations RSVP sur les tunnels TE n'utilise pas cette approche du changement du numéro de protocole dans les messages RSVP.

La Section 7 de la [RFC4206] discute les considérations de sécurité qui découlent du fait que l'hypothèse implicite d'un lien entre l'interface des données et l'interface sur laquelle un message de contrôle est envoyé n'est plus valide. Ces considérations de sécurité sont également applicables au présent document.

Si l'agrégateur et le désagrégateur agissent aussi comme passerelles de sécurité IPsec, les considérations de sécurité de la [RFC4301] s'appliquent.

9. Remerciements

Le présent document s'appuie sur les spécifications des [RFC3175], [RFC2746], et [RFC4206]. Nous tenons à remercier Tom Phelan, John Drake, Arthi Ayyangar, Fred Baker, Subha Dhesikan, Kwok-Ho Chan, Carol Iturralde, et James Gibson de leurs apports au présent document.

10. Références normatives

[RFC1633] R. Braden, D. Clark et S. Shenker, "Intégration de services dans l'architecture l'Internet : généralités", juin 1994. *(Info.)*

[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.)*

[RFC2211] J. Wroclawski, "Spécification du service d'élément de réseau à charge contrôlée", septembre 1997. *(P.S.)*

[RFC2212] S. Shenker, C. Partridge, R. Guerin, "Spécification de la qualité de service garantie", septembre 1997. *(P.S.)*

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss, "Architecture pour services différenciés", décembre 1998. *(MàJ par* RFC3260)

[RFC2702] D. Awduche et autres, "Exigences d'ingénierie du trafic sur MPLS", septembre 1999. *(Information)*

[RFC2747] F. Baker, B. Lindell, M. Talwar, "Authentification cryptographique RSVP", janvier 2000. (*MàJ par* RFC3097) *(P.S.)*

[RFC2998] Y. Bernet et autres, "Cadre de fonctionnement de services intégrés sur réseaux Diffserv", novembre 2000. *(Information)*

[RFC3097] R. Braden, L. Zhang, "Authentification cryptographique RSVP – mise à jour de la valeur de type de message", avril 2001. *(P.S.)*

[RFC3175] F. Baker et autres, "Agrégation de RSVP pour réservations IPv4 et IPv6", septembre 2001. (*MàJ par* RFC5350) *(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)

[RFC4124] F. Le Faucheur, éd., "Extensions de protocole pour la prise en charge de l'ingénierie de trafic MPLS avec capacité Diffserv", juin 2005. *(P.S.)*

[RFC4206] K. Kompella, Y. Rekhter, "Hiérarchie de chemins commutés par étiquettes (LSP) avec l'ingénierie de trafic (TE) de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

11. Références pour information

[RFC2207] L. Berger, T. O'Malley, "Extensions RSVP pour flux de données IPSEC", septembre 1997. *(P.S.)*

[RFC2746] A. Terzis, J. Krawczyk, J. Wroclawski, L. Zhang, "Fonctionnement de RSVP sur tunnels IP", janvier 2000. *(P.S.)*

[RFC3181] S. Herzog, "Élément de politique de priorité par préemption signalée", octobre 2001. (*Remplace* RFC2751) *(P.S.)*

[RFC3182] S. Yadav et autres, "Représentation d'identité pour RSVP", octobre 2001. *(P.S.)*

[RFC3270] F. Le Faucheur et autres, "Prise en charge des services différenciés par la commutation d'étiquettes multi-protocoles (MPLS)", mai 2002. *(P.S.)*

[RFC3312] G. Camarillo, éd., "Intégration de la gestion de ressource et du protocole d'initialisation de session (SIP)", octobre 2002. (*MàJ par* RFC4032, RFC5027) *(P.S.)*

[RFC3564] F. Le Faucheur, W. Lai, "Exigences pour la prise en charge de l'ingénierie de trafic MPLS capable de services différenciés", juillet 2003. *(Information)*

[RFC4798] J. De Clercq et autres, "Connexion d'îlots IPv6 sur MPLS IPv4 avec des routeurs de bordure IPv6 de fournisseur (6PE)", février 2007. *(P.S.)*

[RFC4860] F. Le Faucheur et autres, "Réservations du protocole de réservations de ressources (RSVP) génériques agrégées", mai 2007. *(P.S.)*

[RFC4972] JP. Vasseur et autres, "Extensions d'acheminement pour la découverte des membres maillés de l'ingénierie du trafic de routeur de commutation d'étiquettes multi protocoles (MPLS)", juillet 2007. *(P.S.)*

[RFC5945] F. Le Faucheur, J. Manner, D. Wing, A. Guillou, "Approches de mandataire dans le protocole de réservation de ressource (RSVP)", octobre 2010. *(Information)*

[RFC5946] F. Le Faucheur, J. Manner, A. Narayanan, A. Guillou, H. Malik, "Extensions au protocole de réservation de ressource (RSVP) pour le mandataire de receveur RSVP déclenché par le chemin", octobre 2010. (*MàJ RFC*2205) *(P.S.)*

[RSVP-PROXY1] Gai, et al., "mandataire RSVP", Travail en cours.

Appendice A. Utilisation facultative de mandataire RSVP su un agrégateur RSVP

Un certain nombre d'approches ([RSVP-PROXY1], [RFC5945], [RFC5946]) ont été discutées , ou sont en cours de discussion dans l'IETF afin de permettre à un nœud de réseau de se comporter comme mandataire RSVP qui :
- génère le message Resv (en réponse au message Path) au nom du nœud de destination ;
- génère le message Path (en réponse à un déclencheur) au nom du nœud source.

On observe que ces approches peuvent facultativement être utilisées en conjonction avec l'agrégation de réservations RSVP sur des tunnels MPLS TE comme spécifié dans le présent document. En particulier, on considère le cas où l'agrégateur/désagrégateur RSVP se comporte aussi comme mandataire RSVP.

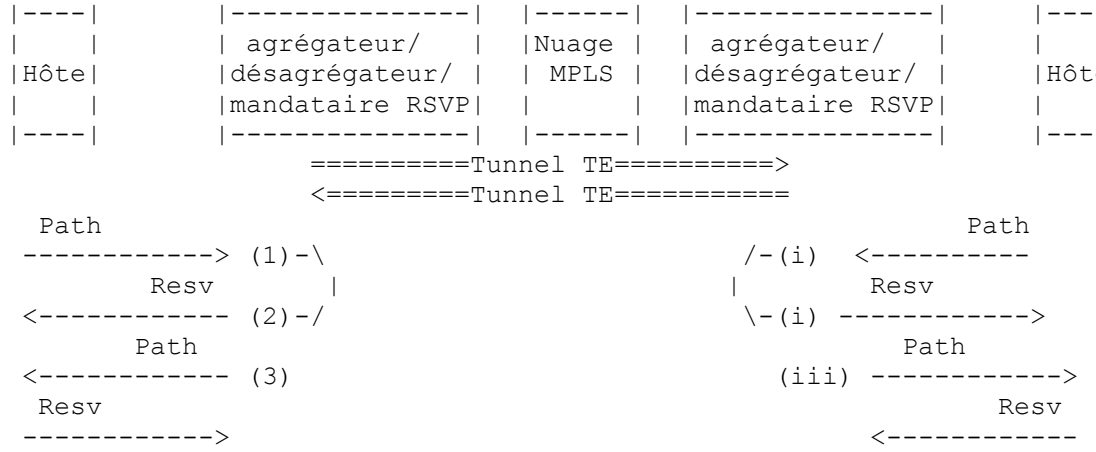
Les informations de cet Appendice sont purement informatives et illustratives.

Comme discuté dans [RSVP-PROXY1] :
"La fonction de mandataire n'implique pas simplement de générer un seul message Resv. Mandater les Resv implique d'installer l'état dans le nœud qui fait le mandataire, c'est-à-dire que le nœud mandataire devrait agir comme si il avait reçu un Resv du vrai point d'extrémité. Cela implique de réserver des ressources (si nécessaire) d'envoyer des rafraîchissements périodiques du message Resv et de supprimer la réservation si le chemin est supprimé."

Donc, quand il se comporte comme mandataire RSVP, l'agrégateur RSVP peut effectivement effectuer la réservation de ressource sur le tunnel TE MPLS (et donc sur tout le segment entre l'agrégateur RSVP et le désagrégateur RSVP) même si la signalisation RSVP n'a lieu qu'en amont du tunnel MPLS TE (c'est-à-dire, entre l'hôte et l'agrégateur RSVP).

Aussi, le mandataire RSVP peut générer le message Path au nom de l'hôte de source distant afin de réaliser la réservation dans la direction de retour (c'est-à-dire, de l'agrégateur/désagrégateur RSVP à l'hôte).

Le flux de signalisation résultant est illustré ci-dessous, couvrant les réservations pour les deux directions :



(1)(i) : l'agrégateur/désagrégateur/mandataire reçoit un message Path, choisit le tunnel TE, effectue le contrôle d'admission sur le tunnel TE. (1) et (i) se produisent indépendamment l'un de l'autre.

(2)(ii) :l'agrégateur/désagrégateur/mandataire génère le message Resv vers l'hôte. (2) est déclenché par (1) et (ii) est déclenché par (i). Avant de générer ce message Resv, l'agrégateur/mandataire effectue le contrôle d'admission de la réservation correspondante sur le tunnel TE qui va finalement porter le trafic correspondant.

(3)(iii) : l'agrégateur/désagrégateur/mandataire génère le message Path vers l'hôte pour la réservation dans la direction de retour. Le déclencheur réel de cela dépend de la solution réelle de mandataire RSVP. Par exemple, (3) et (iii) peuvent simplement être déclenchés respectivement par (1) et (i).

Noter que les détails du flux de signalisation peuvent varier légèrement selon l'approche utilisée pour le mandataire RSVP. Par exemple, si l'approche de la [RFC5946] était utilisée à la place de celle de [RSVP-PROXY1], un message PathRequest supplémentaire serait nécessaire de l'hôte à l'agrégateur/désagrégateur/mandataire afin de déclencher la génération du

message Path pour la direction de retour.

Mais sans considération des détails du flux d'appels et de l'approche réelle de mandataire RSVP, le mandataire RSVP peut facultativement être déployé en combinaison avec l'agrégation RSVP sur les tunnels MPLS TE, d'une façon telle qu'elle assure (quand utilisée sur les deux côtés hôte-agrégateur et désagrégateur-hôte, et quand les deux systèmes d'extrémité supportent RSVP) que :

(i) le contrôle d'admission et la réservation de ressource sont effectués sur chaque segment du chemin de bout en bout (c'est-à-dire, entre hôte de source et agrégateur, sur le tunnel TE entre l'agrégateur et le désagrégateur qui lui-même a fait l'objet du contrôle d'admission par MPLS TE, entre désagrégateur et hôte de destination) ;

(ii) c'est réalisé dans les deux directions ;

(iii) la signalisation RSVP est localisée entre les hôtes et l'agrégateur/désagrégateur, ce qui peut résulter en une réduction significative du délai d'établissement de réservation (et à son tour en délais post numérotation dans le cas où ces réservations sont des pré-conditions pour l'établissement d'appels vocaux) en particulier dans le cas où les tunnels MPLS TE s'étendent sur de longues distances avec de forts délais de propagation.

Appendice B - Exemple d'usage de l'agrégation RSVP sur tunnels DSTE pour contrôle d'admission d'appel VoIP

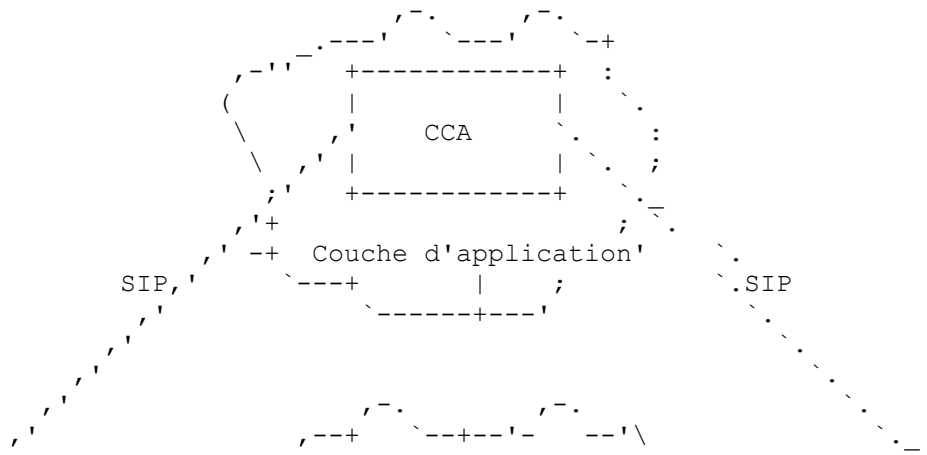
Cet Appendice présente un exemple de scénario où les mécanismes décrits dans ce document sont utilisés, en combinaison avec d'autres mécanismes spécifiés par l'IETF, pour réaliser le contrôle d'admission d'appel (CAC, *Call Admission Control*) du trafic de voix sur IP (VoIP, *Voice over IP*) sur le cœur de paquet.

Les informations de cet Appendice sont purement informatives et illustratives.

Considérons le scénario décrit à la Figure B1. Les passerelles VoIP GW1 et GW2 sont toutes deux des passerelles de signalisation et de supports. Elles sont connectées à un réseau MPLS via les routeurs de bordure respectivement PE1 et PE2. Dans chaque direction, un tunnel DSTE passe du routeur de bordure d'extrémité de tête, à travers les routeurs du cœur de réseau P, au routeur de bordure de l'extrémité de queue. GW1 et GW2 sont à capacité RSVP. Les réservations RSVP établies par GW1 et GW2 sont agrégées par PE1 et PE2 sur les tunnels DS-TE. Pour les réservations allant de GW1 à GW2, PE1 sert d'agrégateur/extrémité de tête et PE2 sert de désagrégateur/extrémité de queue. Pour les réservations allant de GW2 à GW2, PE2 sert d'agrégateur/extrémité de tête et PE1 sert de désagrégateur/extrémité de queue.

Pour déterminer si il y a suffisamment de bande passante dans le cœur MPLS pour achever une connexion, les passerelles d'origine et de destination envoient chacune pour chaque connexion une demande de bande passante RSVP au routeur de réseau PE auquel elles sont connectées. Au titre de son rôle d'agrégateur, le routeur PE effectue effectivement le contrôle d'admission de la demande de bande passante générée par la passerelle sur les ressources du tunnel DS-TE correspondant.

Dans cet exemple, en plus de se comporter comme agrégateur/désagrégateur, PE1 et PE2 se comportent comme mandataire RSVP. De sorte que quand PE reçoit un message Path d'une GW, il ne propage pas le message Path plus loin. Le PE effectue plutôt le contrôle d'admission de la bande passante signalée dans le message Path sur le tunnel DSTE vers la destination. En supposant qu'il y a assez de bande passante disponible sur ce tunnel, le PE ajuste ses annotations de bande passante disponible restante sur le tunnel et génère un message Resv en retour à la GW pour confirmer que les ressources ont été réservées sur le tunnel DSTE.



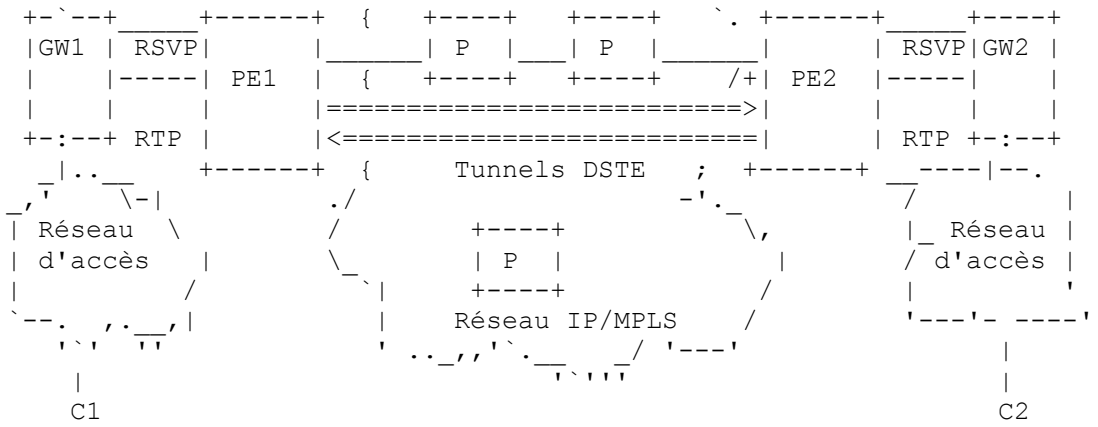


Figure B1. Intégration de gestion de ressource SIP et agrégation RSVP sur tunnels MPLS TE

La [RFC3312] discute la façon dont la qualité de service du réseau peut être une précondition pour l'établissement de sessions initiées par le protocole d'initialisation de session (SIP). Ces préconditions exigent que le participant réserve des ressources du réseau avant de continuer la session. La réservation de ressources du réseau est effectuée par un protocole de signalisation comme RSVP.

Par la collaboration entre la gestion de ressource SIP, la signalisation RSVP, l'agrégation RSVP et DS-TE comme décrit ci-dessus, on voit que :

a) PE et GW collaborent pour déterminer si il y a assez de bande passante sur le tunnel entre les GW appelante et appelée pour traiter la connexion,
b) la décision correspondante d'accepter/rejeter est communiquée aux GW connexion par connexion, et
c) le PE peut optimiser les ressources du réseau en ajustant dynamiquement la bande passante de chaque tunnel en accord avec la charge sur ce tunnel. Par exemple, si un tunnel fonctionne à presque sa limite de capacité, le réseau peut ajuster dynamiquement la taille du tunnel dans un ensemble de paramètres.

On note que le contrôle d'admission des appels vocaux sur la capacité de cœur de réseau est réalisée de manière hiérarchique par laquelle :
- les tunnels DSTE sont soumis au contrôle d'admission sur les ressources du cœur MPLS TE ;
- les appels vocaux sont soumis au CAC sur la bande passante du tunnel DSTE.

Cette hiérarchie est un élément clé de l'adaptabilité de cette solution de CAC pour les appels vocaux sur un cœur MPLS.

Il est aussi possible aux GW d'utiliser les réservations RSVP agrégées elles-mêmes au lieu des réservations RSVP par appel. Par exemple, au lieu d'établir une réservation pour chaque appel que GW1 a vers GW2, GW1 peut établir une (ou un petit nombre de) réservations agrégées comme défini dans la [RFC3175] ou la [RFC4860], qui est utilisée pour tous (ou un sous ensemble de tous) les appels vers GW2. Cela fournit effectivement un niveau supplémentaire de hiérarchie par lequel :
- les tunnels DSTE sont soumis au contrôle d'admission sur les ressources du cœur MPLS TE,
- les réservations RSVP agrégées (pour les appels d'une GW à une autre GW) sont soumises au contrôle d'admission sur les tunnels DSTE (conformément aux procédures "d'agrégation RSVP sur tunnels TE" définies dans ce document)
- les appels vocaux sont soumis au CAC par la GW sur la réservation agrégée vers la GW de destination appropriée.

Cela repousse encore plus les limites d'adaptabilité de cette architecture de CAC vocal.

Auteurs contributeurs

Le présent document a été l'œuvre collective de plusieurs auteurs. Le texte et le contenu sont des contributions de l'éditeur et des co-auteurs suivants.

Michael DiBiasio
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA
mél : dibiasio@cisco.com

Bruce Davie
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA
mél : bdavie@cisco.com

Christou Christou
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102
USA
mél : christou_chris@bah.com

Michael Davenport
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102
USA
mél : davenport_michael@bah.com

Jerry Ash
AT&T
200 Laurel Avenue
Middletown, NJ 07748
USA
mél : gash@att.com

Bur Goode
AT&T
32 Old Orchard Drive
Weston, CT 06883
USA
mél : bgoode@att.com

Adresse de l'éditeur

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

Déclaration complète de droits de reproduction

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