Groupe de travail Réseau
**Request for Comments : 5151**
RFC mises à jour : 3209, 3473
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

A. Farrel, éditeur, Old Dog Consulting
A. Ayyangar, Juniper Networks
JP. Vasseur, Cisco Systems, Inc.
février 2008

# MPLS inter-domaine et GMPLS à ingénierie du trafic – extensions du protocole de réservation de ressource à ingénierie du trafic (RSVP-TE)

**Statut du présent mémoire**

Le présent document spécifie un protocole 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

**Résumé**

Le présent document décrit les procédures et extensions de protocole à l'usage de la signalisation de protocole de réservation de ressource à ingénierie du trafic (RSVP-TE, *Resource Reservation Protocol-Traffic Engineering*) dans les réseaux de paquets de commutation d'étiquettes multi protocoles avec ingénierie du trafic (MPLS-TE, *Multiprotocol Label Switching-Traffic Engineering*) et les réseaux de paquets et non de paquets de MPLS généralisé (GMPLS, *Generalized MPLS*) pour prendre en charge l'établissement et la maintenance de chemins à commutation d'étiquettes (LSP, *Label Switched Path)* qui franchissent les frontières de domaine.

Pour les besoins du présent document, un domaine est considéré être toute collection d'éléments de réseau au sein d'un domaine commun d'espace d'adresses ou d'une responsabilité de calcul de chemin. Des exemples de tels domaines incluent des systèmes autonomes, des zones d'acheminement du protocole de passerelle intérieure (IGP, *Interior Gateway Protocol*) et des réseaux de recouvrement GMPLS.

## Table des Matières

1. Introduction....2
1.1 Spécification des exigences....2
1.2 Terminologie....2
2. Généralités sur la signalisation....3
2.1 Options de signalisation....3
3. Procédures sur le nœud de bordure du domaine....4
3.1 Règles de traitement de ERO....5
3.2 Échec d'établissement de LSP et de retour en arrière....5
3.3 Traitement de RRO à travers les domaines....6
3.4 Traitement du message Notify....6
4. Extensions de signalisation RSVP-TE....7
4.1 Contrôle du choix des méthodes de signalisation....7
5. Protection et récupération des LSP TE inter domaines....7
5.1 Prise en charge de la récupération rapide en utilisant le réacheminemen rapide MPLS-TE....8
5.2 Protection et récupération des LSP GMPLS....9
6. Réoptimisation des LSP TE inter domaines....9
7. Rétro compatibilité....10
8. Considérations sur la sécurité....10
9. Considérations relatives à l'IANA....11
9.1 Fanions d'attributs pour l'objet LSP_Attributes....11
9.2 Nouveaux codes d'erreur....12
10. Remerciements....12
11. Références....12
11.1 Références normatives....12
11.2 Références pour information....12
Adresse des auteurs....13
Déclaration complète de droits de reproduction....14

# 1. Introduction

Les exigences pour l'ingénierie du trafic (TE, *Traffic Engineering*) inter zones et inter systèmes autonomes (AS, *Autonomous System*) de commutation d'étiquettes multi protocoles (MPLS, *Multiprotocol Label Switching*) sont établies respectivement dans les [RFC4105] et [RFC4216]. Beaucoup de ces exigences s'appliquent aussi aux réseaux MPLS généralisé (GMPLS). Le cadre pour MPLS-TE inter domaines est fourni dans la [RFC4726].

Le présent document présente les procédures et extensions à la signalisation du protocole de réservation de ressources à ingénierie du trafic (RSVP-TE) pour l'établissement et la maintenance des chemins à commutation d'étiquette avec ingénierie du trafic (LSP TE) qui s'étendent sur plusieurs domaines dans les réseaux MPLS-TE ou GMPLS. Les procédures de signalisation décrites dans le présent document sont applicables aux LSP de paquets MPLS-TE établis en utilisant RSVP-TE ([RFC3209]) et tous les LSP (de paquet et non de paquest) qui utilisent les extensions GMPLS RSVP-TE comme décrit dans la [RFC3473].

Trois différentes méthodes de signalisation de RSVP-TE inter domaines sont identifiées dans la [RFC4726]. Les LSP contigus sont réalisés en utilisant les procédures des [RFC3209] et [RFC3473] pour créer un seul LSP de bout en bout qui s'étend sur tous les domaines. Les LSP incorporés sont établis en utilisant les techniques décrites dans la [RFC4206] pour porter le LSP de bout en bout dans un tunnel séparé à travers chaque domaine. Les LSP raccordés sont établis en utilisant les procédures de la [RFC5150] pour construire un LSP de bout en bout à partir de l'enchaînement de LSP séparés s'étendant chacun sur un domaine.

Le présent document définit les extensions au protocole RSVP-TE nécessaires pour contrôler et choisir lequel des trois mécanismes de signalisation est utilisé pour tout LSP TE de bout en bout inter domaines.

Pour les besoins du présent document, un domaine est considéré être toute collection d'éléments de réseau au sein d'un domaine commun d'espace d'adresses ou responsabilité de calcul de chemin. Des exemples de tels domaines incluent des systèmes autonomes, des zones IGP, et des réseaux de recouvrement GMPLS [RFC4208].

## 1.1 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].

## 1.2 Terminologie

AS *(Autonomous System)* : système autonome.

ASBR *(Autonomous System Border Router)* : routeur frontière de système autonome. Routeur utilisé pour connecter des AS de fournisseurs de service différents ou du même fournisseur de service via une ou plusieurs liaisons inter AS.

Tunnel de contournement : LSP utilisé pour protéger un ensemble de LSP passant sur une facilité commune.

ERO *(Explicit Route Object)* : objet Chemin explicite.

FA *(Forwarding Adjacency)* : adjacence de transmission.

LSR *(Label Switching Router)* : routeur de commutation d'étiquettes.

MP *(Merge Point)* : point de fusion. Nœud où les tunnels de contournement rencontrent le LSP protégé.

Tunnel de contournement de prochain bond (NHOP, *Next-Hop Bypass Tunnel*). Tunnel de sauvegarde, qui contourne une seule liaison du LSP protégé.

Tunnel de contournement de prochain prochain bond (NNHOP, *Next-Next-Hop Bypass Tunnel*). Tunnel de sauvegarde, qui contourne un seul nœud du LSP protégé.

PLR *(Point of Local Repair)* : point de réparation locale. Entrée d'un tunnel de contournement.

RRO *(Record Route Object)* : objet Record Route.

Liaison TE : liaison d'ingénierie du trafic.

## 2. Généralités sur la signalisation

La signalisation RSVP-TE d'un LSP TE au sein d'un seul domaine est décrite dans les [RFC3209] et [RFC3473]. Les LSP TE inter domaines peuvent être pris en charge par une des trois options décrites dans la [RFC4726] et réglées comme indiqué au paragraphe suivant :
- LSP contiguus
- LSP incorporés
- LSP raccordés.

En fait, comme souligné dans la [RFC4726], toute combinaison de ces trois options peut être utilisée dans le cours d'un LSP inter domaines de bout en bout. C'est-à-dire, les options devraient être considérées comme des options de transit par domaine afin qu'un LSP inter domaines de bout en bout qui commence dans le domaine A, transite par les domaines B, C, et D, et se termine dans le domaine E, puisse utiliser un LSP qui courre de façon contiguë de l'entrée du domaine A, à travers le domaine B jusqu'à la frontière avec le domaine C. Le transit à travers le domaine C pourrait être effectué en utilisant l'option de LSP incorporé pour atteindre la frontière avec le domaine D, et le transit à travers le domaine D pourrait être effectué en utilisant l'option de LSP raccordé pour atteindre la frontière avec le domaine E, d'où un LSP normal court jusqu'à la sortie.

Le présent document décrit les extensions de signalisation RSVP-TE nécessaires pour choisir et contrôler lequel des trois mécanisme de signalisation est utilisé.

Les extensions de protocole spécifiques requises pour signaler chaque type de LSP sont décrites dans d'autres documents et sortent du domaine d'application du présent document. De même le sont les extensions d'acheminement et les techniques de calcul de chemin nécessaires pour l'établissement de LSP inter domaines. Une mise en œuvre d'un LSR de transit ignore les options pour les LSP TE inter domaines car elle voit seulement des LSP TE. Une mise en œuvre d'un LSR de bordure de domaine doit décider quels mécanismes de prise en charge de LSP TE inter domaines inclure, mais doit dans tous les cas prendre en charge les LSP TE inter domaines contigus car c'est le mode de fonctionnement par défaut de RSVP-TE. Manquer à prendre en charge les LSP incorporés, ou les LSP raccordés, ou les deux, restreint les options des opérateurs, mais n'empêche pas l'établissement de LSP TE inter domaines.

### 2.1 Options de signalisation

Il y a trois façons de signaler un LSP TE RSVP à travers plusieurs domaines :

Contigu : un LSP TE contigu est un seul LSP TE qui est établi à travers plusieurs domaines en utilisant les procédures de signalisation RSVP-TE décrites dans les [RFC3209] et [RFC3473]. Aucun LSP TE supplémentaire n'est requis pour créer un LSP TE contigu, et les mêmes informations de RSVP-TE pour le LSP TE sont conservées le long du LSP entier. En particulier, le LSP TE a la même session RSVP-TE et le même identifiant de LSP à tout LSR le long de son chemin.

Incorporé : un ou plusieurs LSP TE peuvent être incorporés au sein d'un autre LSP TE comme décrit dans la [RFC4206]. Cette technique peut être utilisée pour incorporer un ou plusieurs LSP TE inter domaines dans un LSP hiérarchique (H-LSP) intra domaine. La construction de pile d'étiquettes est utilisée pour réaliser l'incorporation dans les réseaux de paquets. Dans le reste du présent document, le terme de H-LSP est utilisé pour se référer à un LSP qui permet à d'autres LSP d'être incorporés dans son sein. Un H-LSP peut être annoncé comme liaison TE au sein de la même instance de protocole d'acheminement qu'utilisée pour annoncer les liaisons TE à partir desquelles il a été créé, auquel cas il est une adjacence de transmission (FA, *Forwarding Adjacency*) [RFC4206].

Raccordé : le concept de raccordement de LSP ainsi que les procédures de signalisation requises sont décrites dans la [RFC5150]. Cette technique peut être utilisée pour raccorder ensemble de plus courts LSP (segments de LSP) pour créer un seul LSP plus long. Les segments de LSP d'un LSP inter domaines peuvent être des LSP intra domaine ou des LSP inter domaines.

Le processus de raccordement dans le plan des données résulte en un seul LSP contigu de bout en bout. Mais dans le plan de contrôle, chaque segment est signalé comme un LSP séparé (avec des sessions RSVP distinctes) et le LSP de bout en bout est signalé comme un autre LSP avec sa propre session RSVP. Donc, le fonctionnement du plan de contrôle pour le raccordement de LSP est très similaire à celui de l'incorporation.

Un LSP TE de bout en bout inter domaines peut être réalisé en utilisant une ou plusieurs des techniques de signalisation décrites. Le choix est une affaire de politique pour le nœud qui demande l'établissement du LSP (l'entrée) et pour chaque nœud de bordure de domaine successif. À réception d'une demande d'établissement de LSP (message Path RSVP-TE) pour un LSP TE inter domaines, la décision de signaler le LSP contigu ou de l'incorporer ou le raccorder à un autre LSP TE dépend des paramètres signalés à partir du nœud d'entrée et de la configuration du nœud local.

Le segment de LSP de raccordement ou le H-LSP utilisé pour traverser un domaine peut être pré-établi ou signalé de façon dynamique sur la base de la demande causée par l'arrivée de la demande d'établissement du LSP TE inter domaines.

## 3. Procédures sur le nœud de bordure du domaine

Qu'un LSP TE inter domaines soit contigu, incorporé, ou raccordé est limité par les méthodes de signalisation prises en charge ou configurées sur les nœuds intermédiaires. C'est généralement aux nœuds de bordure de domaine que cette restriction s'applique dans la mesure où les autres nœuds de transit sont ignorants du mécanisme utilisé. L'entrée du LSP peut de plus restreindre le choix en réglant des paramètres dans le message Path quand il est signalé.

Quand un nœud de bordure de domaine reçoit le message RSVP Path pour l'établissemen d'un LSP TE inter domaines, il DOIT effectuer les procédures suivantes avant de pouvoir transmettre le message Path au prochain nœud le long du chemin :

1. Appliquer les politiques pour le domaine et le nœud de bordure de domaine. Ces politiques peuvent restreindre l'établissement des LSP TE inter domaines. En cas d'une défaillance de la politique, le nœud DEVRAIT faire échouer l'établissement et envoyer un message PathErr avec le code d'erreur "Défaillance de contrôle de politique"/"Défaillance de politique inter domaines".

2. Déterminer la méthode de signalisation à utiliser pour traverser le domaine. Si le nœud d'entrée du LSP TE inter domaines a des restrictions spécifiées sur les méthodes à utiliser, elles DOIVENT être respectées. Dans la mesure de la libertée accordée par le nœud d'entrée, le nœud de bordure de domaine PEUT choisir toute méthode conforme à la configuration et les politiques locales. Si aucune méthode de signalisation résultante n'est disponible ou permise, le nœud de bordure de domaine DOIT envoyer un message PathErr avec un code d'erreur comme décrit au paragraphe 4.1.

   Donc, par exemple, une entrée peut demander un LSP contigu parce qu'elle souhaite exercer un contrôle maximal sur le chemin du LSP et contrôler quand la réoptimisation a lieu. Mais l'opérateur d'un domaine de transit peut décider (par exemple) que seulement le raccordement de LSP soit permis pour la raison exacte qui donne à l'opérateur une chance de réoptimiser son propre domaine sous son propre contrôle. Dans ce cas, la politique appliquée à l'entrée du domaine de transit va résulter en le retour d'un message PathErr et l'entrée a le choix entre :
   - trouver un autre chemin qui évite le domaine de transit,
   - relâcher ces exigences, ou
   - échouer à fournir le service.

3. Effectuer les procédures de ERO comme décrit à la Section 3 en plus des procédures des [RFC3209] et [RFC3473].

4. Effectuer tous les calculs de chemin nécessaires pour déterminer le chemin à travers le domaine et potentiellement choisir le point de sortie du domaine.

   La procédure de calcul de chemin sort du domaine d'application du présent document. Une option de calcul de chemin est spécifiée dans la [RFC5152], et une autre option est d'utiliser un élément de calcul de chemin (PCE, *Path Computation Element*) [RFC4655].

4a. Dans le cas d'une incorporation ou d'un raccordement, soit trouver un LSP TE intra domaine existant pour porter le LSP TE inter domaines, soit en signaler un nouveau, selon la politique locale.

Dans le cas d'une défaillance d'un calcul de chemin, un message PathErr DEVRAIT être envoyé avec un code d'erreur de "Problème d'acheminement" en utilisant une valeur d'erreur choisie conformément à la raison de l'échec du calcul. Un nœud de bordure de domaine PEUT opter pour éliminer en silence le message Path dans ce cas, comme décrit à la Section 8.

Dans le cas de la réception d'un message PathErr rapportant une défaillance de signalisation provenant de l'intérieur du domaine ou rapportée d'un domaine en aval, le nœud de bordure de domaine PEUT appliquer les procédures de retour en

arrière *(crankback)* comme décrit au paragraphe 3.2. Si le retour en arrière n'est pas appliqué, ou est épuisé, le nœud de bordure DOIT continuer le traitement de PathErr comme décrit dans les [RFC3209] et [RFC3473].

Dans le cas d'un traitement réussi d'un message Path ou Resv, le nœud de bordure de domaine DOIT effectuer les procédures de RRO comme décrit au paragraphe 3.3.

### 3.1 Règles de traitement de ERO

Le ERO qu'un nœud de bordure de domaine reçoit dans le message Path a été fourni par le nœud d'entrée du LSP TE et peut avoir été mis à jour par d'autres nœuds (par exemple, d'autres nœuds de bordure de domaine) lorsque le message Path a été propagé. Le contenu du ERO dépend de plusieurs facteurs incluant :
- les techniques de calcul de chemin utilisées,
- le degré de visibilité de TE disponible aux nœuds qui effectuent le calcul de chemin, et
- la politique aux nœuds qui créent/modifient le ERO.

En général, les H-LSP et les segments de LSP sont utilisés entre des nœuds de bordure de domaine, mais il n'y a pas de restriction sur l'utilisation de tels LSP s'étendant sur plusieurs bonds entièrement à l'intérieur d'un domaine. Donc, la discussion qui suit peut être également appliquée à tout nœud au sein d'un domaine bien que le terme de "nœud de bordure de domaine" continue d'être utilisé pour la clarté.

Quand un message Path atteint le nœud de bordure de domaine, les règles suivantes s'appliquent au traitement de ERO et pour la suite de la signalisation.

1. Si il y a des politiques relatives au traitement de ERO pour le LSP, elles DOIVENT être appliquées et les actions correspondantes DOIVENT être effectuées. Par exemple, il pourrait y avoir une politique de rejet des ERO qui identifient des nœuds au sein du domaine. Dans le cas de défaillances d'établissement de LSP inter domaines dues à des défaillances de politique relatives au traitement de l'ERO, le nœud DEVRAIT produire un PathErr avec le code d'erreur de "Défaillance de contrôle de politique"/"Rejet de chemin explicite inter domaines", mais PEUT être configuré à éliminer en silence le message Path ou à retourner un code d'erreur différent pour des raisons de sécurité.

2. Le paragraphe 8.2 de la [RFC4206] décrit comment un nœud à la bordure d'une région traite le ERO dans le message Path entrant et utilise cet ERO, soit pour trouver un H-LSP existant, soit pour signaler un nouveau H-LSP en utilisant les bonds de ERO. Ce processus inclut d'ajuster le ERO avant d'envoyer le message Path au prochain bond. Ces procédures DOIVENT être respectées pour l'incorporation ou le raccordement des LSP TE inter domaines.

3. Si un sous objet ERO identifie une liaison TE formée par l'annonce d'un H-LSP ou d'un segment de LSP (numéroté ou non) la signalisation contiguë NE DOIT PAS être utilisée. Le nœud DOIT utiliser l'incorporation ou le raccordement selon les capacités du LSP qui forme la liaison TE, les paramètres signalés dans le message Path, et la politique locale. Si il y a un conflit entre les capacités du LSP qui forme la liaison TE indiquée dans l'ERO et les paramètres du message Path, le nœud de bordure de domaine DEVRAIT envoyer un PathErr avec le code d'erreur "Problème d'acheminement"/"Conflit d'ERO avec la méthode de signalisation inter domaines", mais PEUT être configuré à éliminer en silence le message Path ou à retourner un code d'erreur différent pour des raisons de sécurité.

4. Un ERO dans un message Path reçu par un nœud de bordure de domaine peut avoir un bond lâche comme prochain bond. Ce peut être une adresse IP ou un numéro d'AS. Dans ce cas, le ERO DOIT être expansé pour déterminer le chemin pour le prochain bond en utilisant une forme de calcul de chemin qui peut, elle-même, générer des bonds lâches.

5. En l'absence de tout sous objet ERO au delà du nœud local de bordure de domaine, le LSP de sortie (la destination codée dans l'objet Session RSVP) DOIT être considéré comme le prochain bond lâche et la règle 4 être appliquée.

6. Dans le cas de toute autre défaillance de traitement de l'ERO, un message PathErr DEVRAIT être envoyé comme décrit dans la [RFC3209] ou la [RFC3473], mais un routeur de bordure de domaine PEUT être configuré à éliminer en silence le message Path ou à retourner un code d'erreur différent pour des raisons de sécurité.

### 3.2 Échec d'établissement de LSP et de retour en arrière

Quand une erreur survient durant l'établissement d'un LSP, un message PathErr est renvoyé au nœud d'entrée du LSP pour rapporter le problème. Si le LSP traverse plusieurs domaines, ce PathErr va être vu successivement par chaque nœud de bordure de domaine.

Les nœuds de bordure de domaine PEUVENT appliquer des politiques locales pour restreindre la propagation des informations sur le contenu du domaine. Par exemple, un nœud de bordure de domaine PEUT remplacer les informations du message PathErr qui indiquent une défaillance spécifique à un nœud particulier par des informations qui rapportent une erreur plus générale sur le domaine entier. Ces procédures sont similaires à celles décrites pour les bordures de réseau en reouvrement de la [RFC4208].

Cependant:
- Un nœud de bordure de domaine NE DOIT PAS supprimer la propagation d'un message PathErrsauf quand il tente de réacheminer comme décrit ci-dessous.
- Les nœuds autres que les nœuds de bordure de domaine NE DEVRAIENT PAS modifier le contenu d'un message PathErr.
- Les nœuds de bordure de domaine NE DEVRAIENT PAS modifier le contenu d'un message PathErr sauf si la confidentialité du domaine est une exigence spécifique.

Les nœuds de bordure de domaine fournissent une opportunité de réacheminement en arrière [RFC4920]. À réception d'un message PathErr généré à cause d'une défaillance d'établissement de LSP, un nœud de bordure de domaine PEUT conserver le PathErr et faire d'autres tentatives pour établir le LSP si c'est permis par la politique locale et par les paramètres signalés dans le message Path pour le LSP. De telles tentatives pourraient impliquer le calcul de chemins de remplacement à travers le domaine, ou le choix de domaines différents vers l'aval. Si une tentative suivante réussit, le routeur de bordure de domaine DOIT éliminer le message PathErr conservé, mais si toutes les tentatives suivantes échouent, le routeur de bordure de domaine DOIT envoyer le PathErr en amont au nœud d'entrée. Dans ce dernier cas, le routeur de bordure de domaine PEUT changer les informations du message PathErr pour fournir des détails supplémentaires sur le retour en arrière et des informations agrégées comme décrit dans la [RFC4920].

Le réacheminement en arrière PEUT aussi être utilisé pour traiter la défaillance des LSP après qu'ils ont été établis [RFC4920].

### 3.3 Traitement de RRO à travers les domaines

La [RFC3209] définit le RRO comme un objet facultatif utilisé pour la détection de boucles et pour fournir des informations sur les bonds traversés par les LSP.

Comme décrit pour les réseaux en recouvrement dans la [RFC4208], un nœud de bordure de domaine PEUT filtrer ou modifier les informations fournies dans un RRO pour des raisons de confidentialité conformément à la politique locale. Par exemple, une série d'identifiants de bonds au sein d'un domaine PEUT être remplacée par un identifaint de domaine (comme le numéro d'AS) ou être supprimé entièrement en laissant juste les nœuds de bordure de domaine.

Noter qu'un routeur de bordure de domaine NE DOIT PAS masquer sa propre présence, et DOIT s'inclure lui-même dans le RRO.

Un tel filtrage des informations de RRO n'impacte pas le fonctionnement du protocole de signalisation, mais la perte des informations suivantes peut rendre inopérantes les procédures de diagnostic de gestion ou au moins les rendre plus compliquées, exigeant la coordination des administrateurs de plusieurs domaines.

De même, les procédures de protocole qui dépendent de la présence des informations de RRO peuvent devenir inefficaces. Par exemple, les procédures de réacheminement rapide définies dans la [RFC4090] utilisent les informations du RRO pour déterminer les étiquettes à utiliser et le point de fusion aval.

### 3.4 Traitement du message Notify

Les messages Notify sont introduits dans la [RFC3473]. Ils peuvent être envoyés directement plutôt que bond par bond, et peuvent ainsi accélérer la propagation des informations d'erreur. Si un routeur de bordure de domaine est intéressé à voir de tels messages (par exemple, pour lui permettre de fournir une commutation de protection) il est RECOMMANDÉ que le routeur de bordure de domaine mette à jour les objets Demande de Notification dans les messages Path et Resv pour montrer sa propre adresse suivant les procédures de la [RFC3473].

Noter que le remplacement d'un receveur de Notify dans l'objet Demande de Notification signifie que des messages Notify (par exemple, ceux destinés à être livrés au LSR d'entrée) peuvent devoir être examinés, traités, et transmis aux bordures de domaine. C'est un problème évident de compromis car la capacité de traiter les événements notifiables en local (c'est-à-dire, au sein du domaine) peut ou non outrepasser le coût de traitement et de transmission des messages Notify au delà du domaine. On observea que le coût augmente de façon linéaire avec le nombre de domaines utilisés.

Noter aussi que, comme décrit à la Section 8, un administrateur de domaine peut souhaiter filtrer ou modifier les messages Notify qui sont générés au sein d'un domaine afin de préserver la sécurité ou la confidentialité des informations du réseau. Ceci est très facilement réalisé si les messages Notify sont envoyés via les bordures du domaine.

## 4. Extensions de signalisation RSVP-TE

Les extensions de signalisation RSVP-TE suivantes sont définies pour permettre l'établissement de LSP inter domaines.

### 4.1 Contrôle du choix des méthodes de signalisation

Dans de nombreux environnements de réseau, il peut y avoir une politique à l'échelle du réseau qui détermine laquelle des trois techniques de LSP inter domaines est utilisée. Dans ces cas, aucune extension de protocole n'est requise.

Cependant, dans les environnements qui prennent en charge plus d'une technique, un nœud d'entrée peut souhaiter contraindre le choix fait par les nœuds de bordure de domaine pour chaque LSP TE inter domaines qu'il génère.

La [RFC4420] définit l'objet LSP_Attributes qui peut être utilisé pour signaler les attributs exigés d'un LSP. Le TLV Fanions d'attribut inclut des fanions booléens qui définissent les attributs individuels.

Le présent document définit un nouveau bit dans le TLV qui peut être établi par le nœud d'entrée d'un LSP TE inter domaines pour restreindre les nœuds intermédiaires en utilisant la signalisation contiguë :

Bit LSP contigu (l'allocation du numéro de bit est au paragraphe 9.1)
Ce fanion est établi par le nœud d'entrée qui génère un message Path pour établir un LSP TE inter domaines si il exige que la technique du LSP contigu soit utilisée. Ce bit fanion est seulement à utiliser dans le TLV Fanions d'attributs.
Quand un LSR de bordure de domaine reçoit un message Path contenant ce bit établi (à un) le nœud NE DOIT PAS effectuer de raccordement ou d'incorporation pour le LSP TE inter domaines établi. Quand ce bit est à zéro, un LSR de bordure de domaine PEUT effectuer un raccordement ou une incorporation en accord avec la politique locale.

Ce bit NE DOIT PAS être modifié par un nœud de transit.

Un nœud intermédiaire qui prend en charge l'objet LSP_Attributes et le TLV Fanions d'attributs, et aussi reconnaît le bit "LSP contigu", mais ne peut pas prendre en charge des LSP TE contigus, DOIT envoyer un message Path Error avec un code d'erreur "Problème d'acheminement"/"Type de LSP contigu non pris en charge" si il reçoit un message Path avec ce bit établi.

Si un nœud intermédiaire qui reçoit un message Path avec le bit "LSP contigu" établi dans le champ Fanions de LSP_Attributes, reconnaît l'objet, le TLV, et le bit et prend aussi en charge le comportement désiré de LSP contigu, alors il DOIT signaler un LSP contigu. Si le nœud est un nœud de bordure de domaine, ou si le nœud étend un bond lâche dans le ERO, il DOIT inclure un sous objet Attributs RRO dans le RRO du message Resv correspondant (si un tel objet est présent) avec le bit "LSP contigu" établi pour rapporter ce comportement.

Les LSR de bordure de domaine DOIVENT prendre en charge et agir sur l'établissement du fanion "LSP contigu".

Cependant, si le nœud intermédiaire prend en charge l'objet LSP_Attributes mais ne reconnaît pas le TLV Fanions d'attributs, ou prend en charge le TLV mais ne reconnaît pas ce bit "LSP contigu", il DOIT alors transmettre l'objet non modifié.

Le choix de l'action par un nœud d'entrée qui reçoit un PathErr quand il demande l'utilisation d'un LSP contigu sort du domaine d'application du présent document, mais peut inclure le calcul d'un chemin de remplacement.

## 5. Protection et récupération des LSP TE inter domaines

Les procédures décrites aux Sections 3 et 4 DOIVENT être appliquées à tous les LSP TE inter domaines, incluant les tunnels de contournement, les LSP de détours [RFC4090], et les LSP de récupération de segment [RFC4873]. Cela signifie que ces LSP vont aussi être soumis au traitement, politiques, calcul de chemin, etc., de ERO.

Noter aussi que les chemins pour ces LSP de sauvegarde ont besoin d'être soit pré-configurés, calculés, et signalés avec le LSP protégé, soit d'être calculés à la demande au PLR. Tout comme avec tout LSP TE inter domaines, le ERO peut comporter des bonds stricts ou lâches et va dépendre de la visibilité TE du point de calcul dans le domaine suivant.

Si des bonds lâches sont présents dans le chemin du LSP de sauvegarde, l'expansion d'ERO va être requise à certains points le long du chemin ; probablement à un nœud de bordure de domaine. Afin que le chemin de sauvegarde reste disjoint du ou des LSP protégés, le nœud qui effectue l'expansion d'ERO doit être provisionné avec le chemin des LSP protégés entre le PLR et le MP. Ces informations peuvent être rassemblées à partir des RRO des LSP protégés et sont signalées dans l'objet DETOUR pour un réacheminement rapide [RFC4090] et utilisent l'exclusion de chemin [RFC4874] pour les autres schémas de protection.

### 5.1 Prise en charge de la récupération rapide en utilisant le réacheminemen rapide MPLS-TE

La [RFC4090] décrit deux méthodes pour la protection locale d'un paquet LSP TE en cas de défaillance de liaison, de groupe de liaisons à risques partagés (SRLG, *Shared Risk Link Group*) ou de nœud.

Ce paragraphe décrit comment fonctionnent ces mécanismes avec les solutions de signalisation proposées d'établissement de LSP TE inter domaines.

#### 5.1.1 Défaillance au sein d'un domaine (défaillance de liaison ou de nœud)

Le mode de fonctionnement du réacheminement rapide MPLS-TE pour protéger un LSP TE contigu, raccordé, ou incorporé au sein d'un domaine est identique aux procédures existantes décrites dans la [RFC4090]. Noter que, dans le cas de l'incorporation ou du raccordement, le LSP de bout en bout est automatiquement protégé par l'opération de protection effectuée sur le H-LSP ou le segment LSP de raccordement.

Aucune extension de protocole n'est requise.

#### 5.1.2 Défaillance d'une liaison à une bordure de domaine

Ce cas survient lorsque deux domaines sont connectés par une liaison TE. Dans ce cas, chaque domaine a son propre nœud de bordure de domaine, et ces deux nœuds sont connectés par la liaison TE. Un exemple de ce cas est lorsque les ASBR des deux AS sont connectés par une liaison TE.

Un LSP contigu peut être sauvegardé en utilisant tout PLR et MP, mais si le LSP utilise le raccordement ou l'incorporation dans l'un ou l'autre des domaines connectés, le PLR et MP DOIVENT être des nœuds de bordure de domaine pour ces domaines. Il serait normal de tenter d'utiliser les nœuds de bordure de domaine locaux (connectés par la liaison défaillante) comme PLR et MP.

Pour protéger une liaison inter domaines avec le réacheminement rapide MPLS-TE, un ensemble de tunnels de sauvegarde doivent être configurés ou calculés de façon dynamique entre le PLR et le MP de telle façon qu'ils aient des acheminements différents de la liaison inter domaines protégée et du LSP inter domaines protégé.

Chaque LSP inter domaines protégé en utilisant la liaison TE inter domaines protégée doit avoir un tunnel de contournement NHOP alloué qui soit différent du LSP protégé. Un tel tunnel de contournement NHOP peut être choisi en analysant les RRO dans les messages Resv des tunnels de contournement disponibles et le LSP TE protégé. Il peut être utile à ce processus que les extensions définies dans la [RFC4561] soient utilisées pour distinguer clairement les nœuds et les liaisons dans les RRO.

#### 5.1.3 Défaillance d'un nœud de bordure

Les cas de défaillance de deux nœuds de bordure existent. Si le domaine de bordure échoue sur une liaison comme décrit au paragraphe précédent, le nœud bordure à l'une ou l'autre extrémité de la liaison peut échouer. Autrement, si la bordure échoue sur un nœud de bordure (comme c'est le cas avec des zones IGP) ce seul nœud de bordure peut être défaillant.

On peut voir que si un raccordement ou une incorporation est utilisé, le nœud défaillant va être le début ou la fin (ou les deux) d'un segment de LSP de raccordement ou de H-LSP, et dans ce cas la protection doit être fournie à l'extrémité distante du segment de raccordement ou H-LSP. Donc, lorsque une de ces deux techniques est utilisée, le PLR va être le point d'entrée du domaine amont dans le cas de défaillance du point de sortie du domaine, et le MP va être le point de sortie

du domaine aval dans le cas de défaillance du point d'entrée du domaine. Lorsque la bordure de domaine a une défaillance à un seul nœud de bordure de domaine, les deux cas vont s'appliquer.

Si le mécanisme de LSP contigu est utilisé, le choix normal du PLR et MP peut être appliqué, et tout nœud au sein des domaines peut être utilisé pour remplir ces rôles.

Comme auparavant, le choix d'un tunnel de sauvegarde convenable (dans ce cas, une sauvegarde de NNHOP) doit considérer les chemins des LSP sauvegardés et les tunnels NNHOP disponibles en examinant leurs RRO.

Noter que lorsque le PLR n'est pas immédiatement en amont du nœud défaillant, le temps de propagation de l'erreur peut être retardé sauf si des mécanismes comme ceux de la [RFC5884] sont mis en œuvre, ou si un rapport direct, comme par le message Notify GMPLS [RFC3473], est employé.

### 5.2 Protection et récupération des LSP GMPLS

La [RFC4873] décrit la récupération de segment fondée sur GMPLS. Cela permet la protection contre une défaillance de portée, une défaillance de nœud, ou une défaillance sur toute portion particulière d'un réseau utilisé par un LSP.

Les cas de défaillance de bordure de domaine décrits au paragraphe 5.1 peuvent aussi se produire dans les réseaux GMPLS (incluant des réseaux de paquets) et peuvent être protégés en utilisant la protection de segment sans extension de protocole supplémentaire.

Noter que si des bonds lâches sont utilisés dans la construction des chemins de travail et de protection signalés pour la protection de segment, il faut faire attention à garder ces chemins disjoints. Si les chemins sont signalés de façon incrémentaire, alors l'exclusion de chemin de la [RFC4874] peut être utilisée pour s'assurer que les chemins sont disjoints. Autrement, une technique de calcul de chemin coordonné comme celle offerte par les éléments coopérants de calcul de chemin de la [RFC4655] peut fournir des chemins convenables.

## 6. Réoptimisation des LSP TE inter domaines

La réoptimisation d'un LSP TE est le processus de déplacement du LSP du chemin actuel à un chemin préféré. Cela implique la détermination du chemin préféré et les procédures de signalisation de "faire avant de casser" [RFC3209] pour minimiser la perturbation du trafic.

La réoptimisation d'un LSP TE inter domaines peut exiger un nouveau chemin dans plus d'un domaine.

La nature du mécanisme d'établissement de LSP inter domaines définit comment la réoptimisation peut être appliquée. Si le LSP est contigu, alors la signalisation du processus de "faire avant de casser" DOIT être initiée par le nœud d'entrée comme défini dans la [RFC3209]. Mais si la réoptimisation est limitée à un changement dans le chemin au sein d'un domaine (c'est-à-dire, si il n'y a pas de changement aux nœuds de bordure de domaine) et si l'incorporation ou le raccordement est utilisé, le H-LSP ou le segment de raccordement peut être réoptimisé indépendamment au sein du domaine sans impacter le LSP de bout en bout.

Dans tous les cas, cependant, le LSR d'entrée peut souhaiter exercer un contrôle et une coordination sur le processus de réoptimisation. Par exemple, un domaine de transit peut avoir connaissance du potentiel de réoptimisation, mais ne pas s'en soucier parce qu'il n'est pas intéressé par le niveau de service fourni à travers le domaine. Mais l'effet cumulatif sur le LSP de bout en bout peut causer des soucis à l'extrémité de tête et déclencher une demande de réoptimisation de bout en bout (bien sûr, le domaine de transit peut choisir d'ignorer la demande).

Un autre avantage de la réoptimisation de bout en bout sur la réoptimisation par domaine pour les LSP inter domaines non contigus est que la réoptimisation par domaine est restreinte pour préserver les points d'entrée et de sortie du domaine (car faire autrement casserait le LSP !). Mais la réoptimisation de bout en bout est plus souple et peut choisir de nouveaux LSR de bordure de domaine.

Il peut y avoir des considérations différentes d'analyse des coûts et des avantages entre la réoptimisation de bout en bout et la réoptimisation par domaine. Plus est grand le nombre de bonds impliqués dans la réoptimisation, plus est élevé le risque de perturbation du trafic. Plus le segment réoptimisé est court, moins on a de chances de faire des améliorations substantielles sur la qualité du LSP de bout en bout. Les politiques administratives devraient être appliquées avec prudence dans ce domaine.

La [RFC4736] décrit des mécanismes qui permettent :
- au nœud d'entrée de demander à chaque nœud avec un prochain bond lâche de reévaluer le chemin actuel afin de chercher un chemin plus optimal ;
- un nœud avec un prochain bond lâche d'informer le nœud d'entrée qu'un meilleur chemin existe.

Ces mécanismes DEVRAIENT être utilisés pour la réoptimisation d'un LSP TE inter domaines contigu.

Noter que la réoptimisation de bout en bout peut impliquer une modification non locale qui pourrait choisir de nouveaux points d'entrée/sortie. Dans ce cas, on peut observer que la réoptimisation locale est réalisée plus facilement et de façon plus souple en utilisant l'incorporation ou le raccordement. De plus, le "principe de localité" (c'est-à-dire, l'idée de ne garder des informations que quand elles sont nécessaires) est mieux réalisée en utilisant le raccordement ou l'incorporation. Ceci dit, un LSP contigu peut facilement être modifié pour tirer parti des réoptimisations locales (comme défini dans la [RFC4736]) même si cela exigerait la dissémination des informations et l'invocation de signalisation en dehors du domaine local.

## 7. Rétro compatibilité

Les procédures du présent document sont rétro compatibles avec les déploiements existants.

- Les LSR d'entrée ne sont pas obligés de prendre en charge les extensions du présent document pour provisionner les LSP intra domaine. Le comportement par défaut des LSR de transit qui reçoivent un message Path qui n'a pas le bit "LSP contigu" établi dans le TLV Fanions d'attributs dans l'objet LSP_Attributes ou n'a même pas l'objet présent est de permettre tous les modes de LSP TE inter domaines, de sorte que les LSR d'entrée de niveau inférieur sont capables d'initier des LSP inter domaines.

- Les LSR de transit non de bordure ne sont pas obligés d'effectuer de traitement particulier et vont passer l'objet LSP_Attributes non modifié en accord avec les règles de la [RFC2205]. Donc, les LSR de transit de niveau inférieur sont pleinement pris en charge.

- Les LSR de bordure de domaine vont devoir être mis à niveau avant que soient permis des LSP TE inter domaines. C'est à cause du besoin d'établir les contrôles de politique, administratifs, et de sécurité avant de permettre que le LSP inter domaines soit signalé à travers une frontière de domaine. Donc, les LSR de bordure de domaine traditionnels n'ont pas besoin d'être considérés.

Les ajouts de RRO dans le présent document sont pleinement rétro compatibles.

## 8. Considérations sur la sécurité

RSVP n'assure pas actuellement la gestion automatique de clés. La [RFC4107] formule l'exigence d'une gestion automatique de clés obligatoire sous certaines conditions. Un travail est en cours à l'IETF pour définir une amélioration de l'authentification incluant la gestion automatique de clés pour RSVP. Les mises en œuvre et déploiements de RSVP devraient surveiller les capacités et exigences qui seront produites par ces travaux.

Un document séparé est en préparation pour examiner les aspects de sécurité de la signalisation RSVP-TE avec une référence particulière aux scénarios multi domaines [RFC5920]. La [RFC4726] donne une vue d'ensemble des exigences pour la sécurité dans un environnement multi domaines MPLS-TE ou GMPLS.

Avant de choisir d'utiliser la signalisation inter domaines pour MPLS-TE, les administrateurs des domaines du voisinage DOIVENT se satisfaire de l'existence d'une relation de confiance convenable entre les domaines. En l'absence d'une telle relation, les administrateurs DEVRAIENT décider de ne pas déployer de signalisation inter domaines, et DEVRAIENT désactiver RSVP-TE sur toutes les interfaces inter domaines.

Quand il signale un LSP TE RSVP inter domaines, un opérateur PEUT utiliser les caractéristiques de sécurité déjà définies pour RSVP-TE [RFC3209]. Cela peut exiger une certaine coordination entre les domaines pour partager les clés (voir les [RFC2747] et [RFC3097]) et il faut veiller à s'assurer que les clés sont changées suffisamment fréquemment. Noter que cela peut impliquer une synchronisation supplémentaire, si les nœuds de bordure de domaine devaient être protégés avec le réacheminement rapide (FRR), car le MP et le PLR devraient aussi partager la clé.

Pour un LSP TE inter domaines, en particulier quand il traverse des domaines administratifs ou de confiance différents, les mécanismes suivants DEVRAIENT être fournis à un operateur (voir aussi la [RFC4216]) :

1) Un moyen d'appliquer les politiques et filtres aux bordures du domaine pour traiter les demandes entrantes d'établissement de LSP TE inter domaines (messages Path) sur la base d'un certain accord de confiance et niveau/contrat de service entre domaines. Divers attributs de LSP comme la bande passante, les priorités, etc. pourraient faire partie d'un tel contrat.

2) Une façon pour l'opérateur de limiter le débit des demandes d'établissement de LSP ou des notifications d'erreur provenant d'un domaine particulier.

3) Un mécanisme pour permettre le traitement de message RSVP sortant fondé sur la politique au nœud de bordure de domaine, qui peut impliquer le filtrage ou la modification de certaines adresses dans les objects et messages RSVP.

De plus, un opérateur peut souhaiter réduire les interactions de signalisation entre domaines pour améliorer la sécurité. Par exemple, l'opérateur pourrait ne pas faire confiance au domaine voisin pour fournir des informations de redémarrage correctes ou fiables [RFC5063] et pourrait s'assurer que la disponibilité de la fonction de redémarrage n'est pas configurée dans l'échange de messages Hello à travers la frontière de domaine. Donc, une configuration convenable DOIT être fournie dans une mise en œuvre de RSVP-TE pour permettre à l'opérateur de contrôler les caractéristiques facultatives de protocole qui peuvent être considérées comme présentant des risques pour la sécurité.
Voici des exemples des politiques décrites ci-dessus :

A) Un opérateur peut choisir de mettre en œuvre une sorte de politique de filtrage d'ERO sur le nœud de bordure de domaine pour interdire que les bonds au sein du domaine soient identifiés dans le ERO d'un message Path entrant ou pour les ignorer. C'est-à-dire, la politique est qu'un nœud en-dehors du domaine ne peut pas spécifier le chemin du LSP à l'intérieur du domaine. Le LSR de bordure de domaine peut mettre en œuvre cette politique d'une des deux façons suivantes :
   - il peut rejeter le message Path ;
   - il peut ignorer les bonds dans le ERO qui se tiennent dans le domaine.

B) Afin de préserver la confidentialité de la topologie du réseau, un opérateur peut choisir de ne pas permettre l'enregistrement des bonds au sein du domaine dans le RRO ou peut choisir de filtrer certaines adresses enregistrées de RRO au nœud de bordure de domaine.

C) Un opérateur peut exiger que le nœud de bordure modifie les adresses de certains messages comme PathErr ou Notify générés à partir de bonds au sein du domaine.

D) Dans le cas d'un échec de calcul de chemin, un opérateur peut demander au nœud de bordure d'éliminer en silence le message Path au lieu de retourner un PathErr. C'est parce que un message Path pourrait être interprété comme une sonde de réseau, et qu'un PathErr donne des informations sur les capacités et les politiques du réseau.

Noter que la spécification détaillée de ces politiques et de leur mise en œuvre sort du domaine d'application du présent document.

Les mécanismes d'opérations, administration, et maintenance (OAM) incluant les [RFC5884] et [RFC4379] sont couramment utilisés pour vérifier la connexité de bout en bout des LSP et pour retracer leurs chemins. Lorsque les LSP sont des LSP inter domaines, des telles techniques d'OAM PEUVENT exiger que les messages d'OAM soient interceptés ou modifiés aux bordures de domaines, ou soient passées de façon transparente à travers les domaines. Un exposé plus approfondi de ces sujets se trouve dans [INTERAS-PING] et la [RFC5920].

## 9. Considérations relatives à l'IANA

L'IANA a fait les allocations de codets décrites dans les paragraphes qui suivent.

### 9.1 Fanions d'attributs pour l'objet LSP_Attributes

Un nouveau bit a été alloué dans le sous registre "Fanions d'attributs" du registre "Paramètres RSVP TE".

| N ° de bit | Nom | Fanions d'attribut Path | Fanions de chemin Resv | RRO | Référence |
|---|---|---|---|---|---|
| 4 | LSP contigu | Oui | Non | Oui | [RFC5151] |

### 9.2 Nouveaux codes d'erreur

De nouveaux codes/valeurs d'erreur RSVP ont été alloués dans les sous registre "Codes d'erreur et sous codes de valeur d'erreur définies mondialement" du registre des "Paramètres RSVP".

Pour le code d'erreur existant "Défaillance de contrôle de politique" (valeur 2), deux nouvelles valeurs d'erreur ont été enregistrées comme suit :
103 = défaillance de politique inter-domaines
104 = rejet explicite de chemin inter domaines

Pour le code d'erreur existant "Problème d'acheminement" (valeur 24), deux nouvelles valeurs d'erreur ont été enregistrées comme suit :
28 = Type de LSP contigu non pris en charge
29 = Conflits d'ERO avec la méthode de signalisaion inter domaines

## 10. Remerciements

Les auteurs tiennent à remercier de ses apports et de ses utiles commentaires Kireeti Kompella sur divers aspects discutés dans ce document. Deborah Brungard et Dimitri Papadimitriou se sont livrés à une relecture très attentive. Merci à Sam Hartman de sa discussion détaillée des considérations. sur la sécurité

## 11. Références

### 11.1 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.)*

[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)

[RFC3473] L. Berger, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", janvier 2003. *(P.S., MàJ par 4003, 4201, 4420, 4783, 4784, 4873, 4974, 5063, 5151,* 8359)

[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.)*

[RFC4420] A. Farrel et autres, "Codage des attributs pour l'établissement de chemin à commutation d'étiquettes (LSP) de la commutation d'étiquettes multiprotocoles (MPLS) en utilisant le protocole de réservation de ressources avec extensions d'ingénierie de trafic (RSVP-TE)", février 2006. (*MàJ* RFC3209, RFC3473) *(P.S. : Obsolète, voir RFC 5420, )*

[RFC5150] A. Ayyangar et autres, "Raccordement de chemin à commutation d'étiquette avec la commutation généralisée d'étiquettes multiprotocoles à ingénierie de trafic (GMPLS-TE)", février 2008. *(P.S.)*

### 11.2 Références pour information

[INTERAS-PING] Nadeau, T.and G. Swallow, "Detecting MPLS Data Plane Failures in Inter-AS and inter-provider Scenarios", *Travail en cours*, octobre 2006.

[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.)*

[RFC4090] P. Pan et autres, "Extensions de réacheminement rapide à RSVP-TE pour les tunnels de LSP", mai 2005. *(P.S. ; MàJ par* RFC8271, RFC8537, RFC8796)

[RFC4105] J.-L. Le Roux, J.-P. Vasseur et J. Boyle, "Exigences pour l'ingénierie de trafic MPLS interzones", juin 2005.

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005. (BCP0107)

[RFC4208] G. Swallow et autres, "Interface usager-réseau (UNI) de commutation généralisée d'étiquettes multiprotocoles (GMPLS) : prise en charge du protocole de réservation de ressource - ingénierie du trafic (RSVP-TE) pour le modèle de recouvrement", octobre 2005. *(P.S.)*

[RFC4216] R. Zhang et J.-P. Vasseur, "Exigences pour l'ingénierie de trafic MPLS entre systèmes autonomes (AS)", novembre 2005. *(Information)*

[RFC4379] K. Kompella et G. Swallow, "Détection des défaillances de plan des données en commutation d'étiquettes multi protocole (MPLS)", février 2006. (*MàJ par la* RFC6424 *; Rendue obsolète par* RFC8029) *(P.S.)*

[RFC4561] J.-P. Vasseur et autres, "Définition d'un sous-objet Identifiant de nœud d'un objet Record Route (RRO)", juin 2006. *(P.S.)*

[RFC4655] A. Farrel, J.-P. Vasseur et J. Ash, "Architecture fondée sur l'élément de calcul de chemin (PCE)", août 2006.

[RFC4726] A. Farrel et autres, "Cadre pour l'ingénierie de trafic inter domaine de commutation d'étiquettes multi protocoles", novembre 2006. *(Information)*

[RFC4736] JP. Vasseur et autres, "Ré optimisation de chemin de commutation d'étiquettes (LSP) à acheminement lâche pour l'ingénierie du trafic de la commutation d'étiquettes multi protocoles (MPLS)", novembre 2006. *(Information)*

[RFC4873] L. Berger et autres, "Récupération de segment GMPLS", mai 2007. *(P.S. ; MàJ* RFC3473, RFC4872 ; *MàJ par* RFC9270*)*

[RFC4874] CY. Lee et autres, "Exclusion de chemins - Extension au protocole de réservation de Ressource avec ingénierie du trafic (RSVP-TE)", avril 2007. (*MàJ* RFC3209, RFC3473) *(P.S. ; MàJ par* RFC8390)

[RFC4920] A. Farrel et autres, "Extensions de signalisation de retour arrière pour RSVP-TE MPLS et GMPLS", juillet 2007. *(P.S.)*

[RFC5884] R. Aggarwal, K. Kompella, T. Nadeau, G. Swallow, "Détection de transmission bidirectionnelle (BFD) pour chemins à commutation d'étiquette (LSP) MPLS", juin 2010. (*MàJ* RFC1122). *(P. S.)*

[RFC5063] A. Satyanarayana et R. Rahman, éd. "Extensions au redémarrage en douceur GMPLS du protocole de réservation de ressources (RSVP)", octobre 2007. (*MàJ* RFC2961, RFC3473) *(P.S.)*

[RFC5152] JP. Vasseur et autres, "Méthode de calcul de chemin par domaine pour établir des chemins de commutation d'étiquettes (LSP) à ingénierie du trafic inter domaine", février 2008. *(P.S.)*

[RFC5920] L. Fang, "Cadre de sécurité pour réseaux MPLS et GMPLS", juillet 2010. *(Information)*

## Adresse des auteurs

Arthi Ayyangar
Juniper Networks
1194 N. Mathilda Avenue
Sunnyvale, CA 94089
mél : arthi@juniper.net

Adrian Farrel
Old Dog Consulting
mél : adrian@olddog.co.uk

Jean Philippe Vasseur
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
mél : jpv@cisco.com

## Déclaration complète de droits de reproduction