

Groupe de travail Réseau
Request for Comments : 4206
 Catégorie : Sur la voie de la normalisation

K. Kompella & Y. Rekhter, Juniper Networks
 octobre 2005
 Traduction Claude Brière de L'Isle

Hiérarchie de chemins à commutation d'étiquettes (LSP) avec l'ingénierie de trafic (TE) de commutation d'étiquettes multi protocoles généralisée (GMPLS)

Statut de ce mémoire

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

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

Pour améliorer l'adaptabilité de la commutation d'étiquettes multi protocoles généralisée (GMPLS, *Generalized Multi-Protocol Label Switching*) il peut être utile d'agréger les chemins commutés par étiquettes (LSP, *Label Switched Path*) en créant une hiérarchie de ces LSP. Une façon de créer une telle hiérarchie est (a) avec un routeur de commutation d'étiquettes (LSR, *Label Switching Router*) qui crée un chemin commuté par étiquette à ingénierie du trafic (TE LSP, *Traffic Engineering Label Switched Path*), (b) avec le LSR qui forme une adjacence de transmission (FA, *forwarding adjacency*) à partir de ce LSP (en annonçant ce LSP comme liaison d'ingénierie du trafic (TE, *Traffic Engineering*) dans la même instance de ISIS/OSPF que celle utilisée pour créer le LSP), (c) en permettant aux autres LSR d'utiliser des FA pour leur calcul de chemin, et (d) en incorporant les LSP générés par les autres LSR dans ce LSP (en utilisant la construction de piles d'étiquettes).

Le présent document décrit les mécanismes qui permettent de réaliser cela.

Table des Matières

1. Généralités.....	1
2. Spécification des exigences.....	2
3. Aspects d'acheminement.....	2
3.1 Paramètres d'ingénierie du trafic.....	3
4. Autres considérations.....	4
5. Contrôle des limites des FA-LSP.....	4
5.1 Régions de LSP.....	4
6. Aspects de signalisation.....	5
6.1 Procédures communes.....	5
6.2 Procédures spécifiques.....	6
6.3 Priorité de garde de FA-LSP.....	6
7. Considérations sur la sécurité.....	6
8. Remerciements.....	7
9. Références normatives.....	7
10. Références pour information.....	8
Adresse des auteurs.....	8
Déclaration complète de droits de reproduction.....	8

1. Généralités

Un LSR utilise les procédures d'ingénierie du trafic de MPLS généralisé (GMPLS, *Generalized MPLS*) pour créer et maintenir un LSP. Le LSR peut alors (sous le contrôle de la configuration locale) annoncer ce LSP comme liaison d'ingénierie de trafic dans la même instance du plan de contrôle GMPLS (ou plus précisément, son composant ISIS/OSPF) comme celui qui a été utilisé pour créer le LSP. On appelle une telle liaison une "adjacence de transmission" (FA, *forwarding adjacency*). On se réfère au LSP comme au "LSP d'adjacence de transmission", ou juste FA-LSP. Noter qu'un

FA-LSP est créé et utilisé comme liaison TE par exactement la même instance du plan de contrôle GMPLS. Donc, le concept de FA n'est applicable que quand un LSP est à la fois créé et utilisé comme liaison TE par exactement la même instance du plan de contrôle GMPLS. Noter aussi qu'une FA est une liaison TE entre deux nœuds GMPLS dont le chemin transite par zéro, un ou plusieurs nœuds (G)MPLS dans la même instance du plan de contrôle GMPLS.

Les nœuds connectés par une liaison TE "de base" peuvent avoir une adjacence d'acheminement ; cependant, les nœuds connectés par une FA ne vont généralement pas avoir d'adjacence d'acheminement. Une liaison TE de toute sorte (qu'elle soit "de base" ou FA) devrait avoir une adjacence de signalisation afin qu'elle soit utilisée pour établir un LSP à travers elle.

En général, la création/terminaison d'une FA et de son FA-LSP pourrait être piloté soit par des mécanismes extérieurs à GMPLS (par exemple, via le contrôle de configuration sur le LSR à l'extrémité de tête de l'adjacence) soit par des mécanismes au sein de GMPLS (par exemple, suite à la réception par le LSR à l'extrémité de tête de l'adjacence de demandes d'établissement de LSP générées par d'autres LSR).

ISIS/OSPF arrose les informations sur les FA tout comme sont arrosées les informations sur toutes autres liaisons. Par suite de cet arrosage, un LSR a dans sa base de données d'état de liaison TE les informations non seulement sur les liaisons TE de base, mais aussi sur les FA.

Un LSR, lorsque il effectue le calcul de chemin, n'utilise pas que les seules liaisons TE de base mais aussi les FA. Une fois qu'un chemin est calculé, le LSR utilise RSVP/CR-LDP [RFC3473], [RFC3472] pour établir les liens d'étiquettes le long du chemin.

Dans le présent document, on définit les mécanismes/procédures pour réaliser cela. Ces mécanismes/procédures couvrent les aspects d'acheminement (ISIS/OSPF) et de signalisation (RSVP/CR-LDP).

Noter qu'un LSP peut être annoncé comme liaison point à point dans ISIS ou OSPF, et être utilisée dans le SPF normal par des nœuds autres que l'extrémité de tête. Bien que ce soit similaire dans son esprit à une FA, cela sort du domaine d'application du présent document.

Les scénarios où un LSP est créé (et maintenu) par une instance du plan de contrôle GMPLS, et est utilisé comme liaison (TE) par une autre instance du plan de contrôle GMPLS, sortent du domaine d'application du présent document.

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. Aspects d'acheminement

Dans cette section, on décrit les procédures de construction des FA à partir des LSP, et le traitement des FA par ISIS/OSPF. Spécifiquement, cette section décrit comment construire les informations nécessaires pour annoncer les LSP comme liaisons dans ISIS/OSPF. Les procédures pour la création/terminaison de tels LSP sont définies à la Section 5, "Contrôle des limites de FA-LSP".

Les FA peuvent être représentées comme des liaisons non numérotées ou numérotées. Si les FA sont numérotées avec des adresses IPv4, les adresses IPv4 locales et distantes viennent d'un /31 qui est alloué par le LSR qui génère le FA-LSP ; l'adresse d'extrémité de tête du FA-LSP est celle spécifiée comme adresse d'expéditeur du tunnel IPv4 ; l'adresse distante (extrémité de queue) peut alors être déduite. Si le LSP est bidirectionnel, l'extrémité de queue peut donc savoir les adresses à allouer à la FA inverse.

Si il y a plusieurs LSP qui ont tous leur origine sur un LSR et se terminent tous sur un autre LSR, alors à une extrémité du spectre tous ces LSP pourraient être fusionnés (sous le contrôle du LSR d'extrémité de tête) en une seule FA en utilisant le concept de faisceau de liaisons (voir la [RFC4201]) ; tandis qu'à l'autre extrémité du spectre, chaque LSP pourrait être annoncé comme sa propre adjacence.

Lorsque une FA est créée sous contrôle administratif (provisionnement statique) les attributs du FA-LSP doivent être fournis via la configuration. Spécifiquement, les attributs suivants peuvent être configurés pour le FA-LSP : l'adresse de l'extrémité de tête (si elle reste non configurée, c'est par défaut l'identifiant de routeur du LSR d'extrémité de tête), l'adresse de l'extrémité de queue, la bande passante et les contraintes de couleur de ressource. Le chemin pris par le FA-LSP peut être

calculé par le LSR à l'extrémité de tête du FA-LSP, ou spécifié par configuration explicite ; ce choix est déterminé par configuration.

Quand une FA est créée de façon dynamique, les attributs de son FA-LSP sont hérités du LSP qui a provoqué sa création. Noter que la bande passante du FA-LSP doit être au moins celle du LSP qui l'a provoqué, mais elle peut être supérieure si seulement des bandes passantes discrètes sont disponibles pour le FA-LSP. En général, pour les FA provisionnées de façon dynamique, un mécanisme fondé sur la politique peut être nécessaire pour associer les attributs aux FA-LSP.

3.1 Paramètres d'ingénierie du trafic

Ce paragraphe décrit les paramètres d'ingénierie du trafic (voir la [RFC3630] et la [RFC3784]) pour les FA.

3.1.1 Type de liaison (seulement OSPF)

Le type de liaison d'une FA est réglé à "point à point".

3.1.2 Identifiant de liaison (seulement OSPF)

L'identifiant de liaison est réglé à l'identifiant de routeur de l'extrémité de queue du FA-LSP.

3.1.3 Adresse IP d'interface locale et distante

Si la FA doit être numérotée, l'adresse IP de l'interface locale (OSPF) ou l'adresse IPv4 de l'interface (ISIS) est réglée à l'adresse de l'extrémité de tête du FA-LSP. L'adresse IP d'interface distante (OSPF) ou l'adresse IPv4 du voisin (ISIS) est réglée à l'adresse de l'extrémité de queue du FA-LSP.

3.1.4 Identifiant de liaison locale et distante

Pour une FA non numérotée, l'allocation et le traitement des identifiants de liaison locaux et distants sont spécifiés dans les [RFC3477] et [RFC3480].

3.1.5 Métrique d'ingénierie du trafic

Par défaut, la métrique TE sur la FA est réglée à $\max(1, (\text{métrique TE du FA-LSP}) - 1)$ afin qu'elle attire le trafic plutôt que d'établir un nouveau LSP. Cela peut être outrepassé via configuration à l'extrémité de tête de la FA.

3.1.6 Bande passante maximum

Par défaut, la bande passante maximum réservable et la bande passante maximum initiale de LSP pour toutes les priorités de la FA sont réglées à la bande passante du FA-LSP. Cela peut être outrepassé via configuration à l'extrémité de tête de la FA (noter que la bande passante maximum de LSP à toute priorité ne devrait pas être supérieure à la bande passante du FA-LSP).

3.1.7 Bande passante non réservée

La bande passante initiale non réservée pour tous les niveaux de priorité de la FA est réglée à la bande passante du FA-LSP.

3.1.8 Classe/couleur de ressource

Par défaut, une FA n'a pas de couleur de ressource (groupes administratifs). Cela peut être outrepassé par configuration à l'extrémité de tête de la FA.

3.1.9 Capacités de commutation d'interface

La capacité de commutation d'interface (extrémité proche) associée à la FA est la capacité de commutation d'interface (extrémité proche) de la première liaison dans le FA-LSP.

Lorsque le champ Capacités de commutation d'interface (extrémité proche) est PSC-1, PSC-2, PSC-3, ou PSC-4, les informations spécifiques incluent la MTU d'interface et la bande passante minimum de LSP. La MTU d'interface est la

MTU minimum le long du chemin du FA-LSP ; la bande passante minimum de LSP est la bande passante du LSP.

3.1.10 Informations de SRLG

Une annonce de FA pourrait contenir des informations sur les groupes de liaisons à risques partagés (SRLG, *Shared Risk Link Group*) pour le chemin pris par le FA-LSP associé à cette FA. Ces informations peuvent être utilisées pour le calcul de chemin par les autres LSR. Les informations portées sont l'union des SRLG des liaisons TE sous-jacentes qui constituent le chemin FA-LSP ; elles sont portées dans le TLV SRLG dans IS-IS ou le sous TLV SRLG du TLV Liaison dans OSPF. Voir dans les [RFC4203] et [RFC4205] les détails du format de ces informations.

Il est possible que les informations sur le chemin sous-jacent changent avec le temps, via des mises à jour de configuration ou des modifications dynamiques du chemin, résultant en un changement du TLV SRLG.

Si les FA sont en faisceau (via la mise en faisceau de liaisons) et si la liaison en faisceau résultante porte un TLV SRLG, la liste des SRLG dans le chemin sous-jacent DOIT être la même que celle de chacun des FA-LSP qui forment les liaisons composantes (noter que les chemins exacts n'ont pas besoin d'être les mêmes).

4. Autres considérations

Il est prévu que les FA ne soient pas utilisées pour établir des relations ISIS/OSPF d'homologue à homologue entre les routeurs aux extrémités de l'adjacence.

Il peut être souhaité dans certains cas de n'utiliser les FA que dans les calculs de chemin d'ingénierie du trafic. Dans IS-IS, cela peut être réalisé en établissant la métrique par défaut du TLV Accessibilité IS étendue pour la FA à la métrique maximum de liaison ($2^{24} - 1$). Dans OSPF, cela peut être accompli en n'annonçant pas la liaison comme une LSA régulière, mais seulement comme LSA TE opaque.

5. Contrôle des limites des FA-LSP

Pour faciliter le contrôle des limites des FA-LSP, le présent document introduit deux nouveaux mécanismes : capacité de commutation d'interface (voir [RFC4203], [RFC4205]) et "région de LSP" (ou juste "région").

5.1 Régions de LSP

Les informations portées dans les capacités de commutation d'interface sont utilisées pour construire des régions de LSP et pour déterminer les limites des régions comme suit.

Définir comme suit l'ordre des capacités de commutation d'interface : $PSC-1 < PSC-2 < PSC-3 < PSC-4 < TDM < LSC < FSC$. Soient deux interfaces if-1 et if-2 avec les capacités de commutation d'interface respectives isc-1 et isc-2, on dit que if-1 < if-2 si $isc-1 < isc-2$ ou $isc-1 = isc-2 = TDM$, et si la bande passante maximum de LSP de if-1 est inférieure à la bande passante maximum de LSP de if-2.

Supposons que le chemin d'un LSP soit : nœud-0, liaison-1, nœud-1, liaison-2, nœud-2, ..., liaison-n, nœud-n. De plus, pour liaison-i notée par [liaison-i, nœud-(i-1)] l'interface qui connecte la liaison-i au nœud-(i-1), et par [liaison-i, nœud-i] l'interface qui connecte la liaison-i au nœud-i.

Si [liaison-(i+1), nœud-i] < [liaison-(i+1), nœud-(i+1)], on dit que le LSP a franchi une limite de région au nœud-i; par rapport à ce chemin de LSP, le LSR au nœud-i est un LSR bordure. L'autre "bordure" de la région par rapport au chemin de LSP est le nœud-k, où k est le plus petit nombre supérieur à i tel que [liaison-(i+1), nœud-(i+1)] = [liaison-k, nœud-(k-1)], et [liaison-k, nœud-(k-1)] > [liaison-k, nœud-k].

Le calcul de chemin peut prendre en compte les limites de région lors du calcul d'un chemin pour un LSP. Par exemple, le calcul de chemin peut restreindre le chemin pris par un LSP aux seules liaisons dont la capacité de commutation d'interface est PSC-1.

Noter qu'une interface peut avoir plusieurs capacités de commutation d'interface. Dans ce cas, la vérification est si if-i < if-j dépend des capacités de commutation d'interface choisies pour if-i et if-j, ce qui à son tour détermine si il y a ou non une limite de région au nœud-i.

6. Aspects de signalisation

Dans cette section, on décrit les procédures qu'utilise un LSR à l'extrémité de tête d'une FA pour traiter l'établissement de LSP générés par d'autres LSR.

Comme mentionné précédemment, l'établissement/terminaison des FA-LSP peut être déclenché par un mécanisme extérieur à GMPLS (par exemple, via une commande administrative) ou par un mécanisme interne à GMPLS (par exemple, par suite de la réception par le LSR à la bordure d'un LSP agrégé de demandes d'établissement de LSP générées par d'autres LSR au delà du LSP agrégé et de ses bordures). Les procédures décrites au paragraphe 6.1, "Procédures communes", s'appliquent aux deux cas. Les procédures décrites au paragraphe 6.2, "Procédures spécifique", ne s'appliquent qu'au dernier cas.

6.1 Procédures communes

Pour les besoins du traitement de l'objet EXPLICIT_ROUTE (ERO, *EXPLICIT_ROUTE object*) dans un message Path/Request d'un LSP qui doit être tunnelé sur une FA, un LSR à l'extrémité de tête du FA-LSP voit le LSR à la queue de ce FA-LSP comme adjacent (un bond IP plus loin).

Les paragraphes qui suivent décrivent comment cela est réalisé pour RSVP-TE et CR-LDP.

Dans l'un et l'autre cas (RSVP-TE ou CR-LDP) lorsque un LSP est tunnelé à travers un FA-LSP, le LSR à l'extrémité de tête du FA-LSP soustrait la bande passante du LSP de la bande passante non réservée de la FA.

En présence d'un faisceau de liaisons (lorsque la mise en faisceau de liaisons est appliquée aux FA) lorsque un LSP est tunnelé à travers un FA-LSP, le LSR à l'extrémité de tête du FA-LSP a aussi besoin d'ajuster la bande passante maximum de LSP de la FA.

6.1.1 RSVP-TE

Si on utilise RSVP-TE pour signaler un LSP à tunneler sur un FA-LSP, le message Path DOIT alors contenir un objet IF_ID RSVP_HOP [RFC3471], [RFC3473] au lieu d'un objet RSVP_HOP ; et l'identification de l'interface de données DOIT identifier le FA-LSP.

La méthode préférée d'envoi du message Path est de régler l'adresse IP de destination du message Path au prochain bond (NHOP) calculé pour ce message Path. Cette adresse de NHOP doit être une adresse acheminable ; dans le cas de plans de contrôle et de données séparés, ce doit être une adresse de plan de contrôle.

De plus, l'en-tête IP pour le message Path NE DOIT PAS avoir l'option Router Alert. Le message Path est destiné à être acheminé par IP à l'extrémité de queue du FA-LSP sans être intercepté ni traité comme un message RSVP par aucun des nœuds intermédiaires.

Finalement, la vérification TTL IP ou TTL RSVP NE DOIT PAS être faite. En général, si l'objet IF_ID RSVP_HOP est utilisé, cette vérification doit être désactivée, car le nombre de bonds sur le plan de contrôle peut être supérieur à un. À la place, les vérifications suivantes sont faites 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 effectivement sur Y.
2. Trouver l'autre extrémité de l'interface de données ci-dessus, disons X. S'assurer que le PHOP dans l'objet IF_ID RSVP_HOP est une adresse de canal de contrôle qui appartient au même nœud que X.

La façon de vérifier le n° 2 sort du domaine d'application du présent document ; il suffit de dire que cela peut exiger une base de données d'ingénierie du trafic, ou d'utiliser LMP [RFC4204], ou tout autre moyen.

Une autre méthode est d'encapsuler le message Path dans un tunnel IP (ou, dans le cas où la capacité de commutation d'interface du FA-LSP est PSC[1-4], dans le FA-LSP lui-même) et d'envoyer en individuel le message à l'extrémité de queue du FA-LSP, sans l'option Alerte de routeur. Cette option peut être nécessaire si des nœuds intermédiaires traitent les messages RSVP sans considérer si l'option Alerte de routeur est présente.

Un PathErr envoyé en réponse à un message Path avec un objet IF_ID RSVP_HOP DEVRAIT contenir un objet IF_ID HOP. (Noter qu'un PathErr ne porte normalement pas un objet RSVP_HOP, mais dans le cas de contrôle et données séparés, il est nécessaire d'identifier le canal de données dans le message PathErr.)

Le message Resv de retour à l'extrémité de tête du FA-LSP (PHOP) est acheminé par IP au PHOP dans le message Path. Si nécessaire, les messages Resv PEUVENT être encapsulés dans un autre en-tête IP dont l'adresse IP de destination est le PHOP du message Path reçu.

6.1.2 CR-LDP

Si on utilise CR-LDP pour signaler un LSP à tunneler sur un FA-LSP, le message Request DOIT alors contenir un objet TLV IF_ID [RFC3472], et l'identification d'interface de données DOIT identifier le FA-LSP.

De plus, le LSR d'extrémité de tête doit créer une session de LDP ciblée avec le LSR d'extrémité de queue. Le message Request (transposition) est en envoi individuel de l'extrémité de tête (extrémité de queue) à l'extrémité de queue (extrémité de tête).

6.2 Procédures spécifiques

Lorsque un LSR reçoit un message Demande/Chemin (*Path/Request*), le LSR détermine si il est à la bordure d'une région par rapport à l'ERO porté dans le message. Le LSR fait cela en examinant les capacités de commutation d'interface du bond précédent et du prochain bond dans sa base de données IGP, et en les comparant en utilisant la relation définie dans la présente section. Si le LSR n'est pas à la bordure d'une région, les procédures de cette section ne s'appliquent pas.

Si le LSR est à la bordure d'une région, il doit alors déterminer l'autre bordure de la région par rapport à l'ERO, en utilisant encore la base de données IGP. Le LSR extrait alors (de l'ERO) la succession de bonds de lui-même jusqu'à l'autre extrémité de la région.

Le LSR compare alors la succession des bonds avec tous les FA-LSP existants générés par le LSR. Si une correspondance est trouvée, si ce FA-LSP a assez de bande passante non réservée pour le LSP qui est signalé, le L3PID du FA-LSP est compatible avec le L3PID du LSP signalé, et le LSR utilise ce FA-LSP comme suit. Le message Path/Request pour le LSP original est envoyé à la sortie du FA-LSP, et non au prochain bond sur le chemin du FA-LSP. Le PHOP dans le message est l'adresse du LSR à l'extrémité de tête du FA-LSP. Avant d'envoyer le message Path/Request, le ERO dans ce message est ajusté en retirant la succession de ERO qui se trouve dans le FA-LSP, et en la remplaçant avec juste le point d'extrémité du FA-LSP.

Autrement (si on ne trouve aucun FA-LSP) le LSR établit un nouveau FA-LSP. C'est-à-dire qu'il initie un nouvel établissement de LSP juste pour le FA-LSP. Noter que le nouveau LSP peut traverser des liaisons TE "de base" ou des FA.

Après que le LSR a établi le nouveau FA-LSP, le LSR annonce ce LSP dans IS-IS/OSPF comme une FA.

La bande passante non réservée de la FA est calculée en soustrayant de la bande passante du FA-LSP la bande passante des sessions associées en cours d'établissement du FA-LSP.

Un FA-LSP pourrait être supprimé par le LSR à l'extrémité de tête du FA-LSP conformément à une politique locale du LSR. On s'attend à ce que le FA-LSP soit supprimé une fois qu'il n'y a plus de LSP portés par le FA-LSP. Lorsque le FA-LSP est supprimé, la FA associée au FA-LSP n'est plus annoncée dans IS-IS/OSPF.

6.3 Priorité de garde de FA-LSP

La valeur de la priorité de garde d'un FA-LSP doit être le minimum de la priorité de garde configurée du FA-LSP et des priorités de garde des LSP qui tunnelent à travers le FA-LSP (noter que les plus petites valeurs de priorité notent les plus fortes priorités). Donc, si un LSP de priorité supérieure au FA-LSP tunnelle à travers le FA-LSP, le FA-LSP est lui-même promu à la plus haute priorité. Cependant, si le LSP tunnelé est supprimé, le FA-LSP n'a pas besoin de revenir directement à son ancienne valeur de priorité ; il peut être conseillé d'appliquer l'hystérésis dans ce cas.

Si la priorité de garde d'un FA-LSP est configurée, le présent document la restreint à 0.

7. Considérations sur la sécurité

Du point de vue de la sécurité, le principal changement introduit dans ce document est que l'hypothèse implicite d'un lien entre les interfaces de données et l'interface sur laquelle un message de contrôle est envoyé n'est plus valide.

Cela signifie que "l'interface d'envoi" ou "l'interface receveuse" ne sont plus bien définies, car l'interface sur laquelle un message RSVP est envoyé peut changer lorsque l'acheminement change. Donc, les mécanismes qui dépendent de ces concepts (par exemple, la définition d'une association de sécurité) doivent être définis plus clairement.

La [RFC2747] donne une solution : au paragraphe 2.1, sous "Identifiant de clé", une adresse IP est un identifiant valide pour l'interface d'envoi (et par analogie, pour l'interface de réception). Comme les messages RSVP pour un certain LSP sont envoyés à une adresse IP qui identifie le prochain bond précédent pour le LSP, on peut remplacer toutes les occurrences d'interface d'envoi [réception] par l'adresse IP respectivement, de receveur [d'envoyeur]. Par exemple, à la Section 4, troisième alinéa, au lieu de : "Chaque envoyeur DEVRAIT avoir des associations de sécurité (et des clés) distinctes par interface (ou LIH) d'envoi sécurisée. ... Chez l'envoyeur, le choix de l'association de sécurité se fonde sur l'interface à travers laquelle le message est envoyé" on devrait lire : "Chaque envoyeur DEVRAIT avoir des associations de sécurité (et des clés) distinctes par adresse IP de receveur sécurisée. ... Chez l'envoyeur, le choix de l'association de sécurité se fonde sur l'adresse IP à laquelle le message est envoyé."

Noter que CR-LDP n'a pas ce problème, car les messages CR-LDP sont envoyés sur des sessions TCP, et aucune hypothèse n'est faite que ces sessions soient avec des voisins directs. Le mécanisme recommandé pour l'authentification et la protection de l'intégrité de l'échange de message LDP est d'utiliser l'option TCP MD5 [RFC3036].

Une autre conséquence (relevant de RSVP) des changements proposés dans le présent document est que l'adresse IP de destination des messages Path soit réglée à l'adresse du receveur, et non à la destination de la session. Donc, les objections soulevées au paragraphe 1.2 de la [RFC2747] devraient être revues pour voir si IPsec AH est maintenant un moyen viable de sécuriser les messages RSVP-TE.

8. Remerciements

Merci à Alan Hannan, dont les discussions avec Yakov Rekhter ont largement contribué à dégager la notion d'adjacence de transmission". Nous tenons aussi à remercier George Swallow, Quaizar Vohra et Ayan Banerjee.

9. Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))
- [RFC2747] F. Baker, B. Lindell, M. Talwar, "[Authentification cryptographique RSVP](#)", janvier 2000. (MàJ par [RFC3097](#)) (P.S.)
- [RFC3036] L. Andersson et autres, "Spécification de LDP", janvier 2001. (Rendue obsolète par la [RFC5036](#))
- [RFC3471] L. Berger, éd., "[Commutation d'étiquettes multi-protocoles généralisée](#) (GMPLS) : description fonctionnelle de la signalisation", janvier 2003. (MàJ par [RFC4201](#), [RFC4328](#), [RFC4872](#), [RFC8359](#)) (P.S.)
- [RFC3472] P. Ashwood-Smith et L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : [extensions au protocole de distribution d'étiquettes](#) acheminées sur la base des contraintes de signalisation (CR-LDP)", janvier 2003. (MàJ par [RFC3468](#), [RFC4201](#)) (P.S.)
- [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](#))
- [RFC3477] K. Kompella, Y. Rekhter, "[Signalisation des liaisons non numérotées](#) dans le protocole de réservation de ressource – ingénierie du trafic (RSVP-TE)", janvier 2003. (P.S.)
- [RFC3480] K. Kompella, Y. Rekhter, A. Kullberg, "[Signalisation des liaisons non numérotées](#) dans le protocole de distribution d'étiquettes acheminées sur la base des contraintes de signalisation (CR-LDP)", février 2003.

- [RFC3630] D. Katz, K. Kompella et D. Yeung, "[Extensions d'ingénierie de trafic](#) à OSPF version 2", septembre 2003.
- [RFC3784] H. Smit, T. Li, "Extensions de système intermédiaire à système intermédiaire (IS-IS) pour l'ingénierie du trafic (TE)", juin 2004. (P.S.) (Obsolète, voir [RFC5305](#)) (MàJ par [RFC4205](#))
- [RFC4203] K. Kompella et autres, "[Extensions OSPF](#) pour la prise en charge de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. (MàJ [RFC3630](#)) (P.S.)
- [RFC4205] K. Kompella et Y. Rekhter, éd., "Extensions de système intermédiaire à système intermédiaire (IS-IS) pour la prise en charge de la commutation généralisée d'étiquettes multiprotocoles (GMPLS)", octobre 2005. (P.S.) (Obsolète, voir [RFC5307](#)) (MàJ [RFC3784](#))

10. Références pour information

- [RFC4201] K. Kompella et autres, "[Faisceaux de liaisons](#) dans l'ingénierie du trafic MPLS", octobre 2005. (P.S.)
- [RFC4204] J. Lang, éd., "[Protocole de gestion de liaison](#) (LMP)", octobre 2005. (P.S.)

Adresse des auteurs

Kireeti Kompella
Juniper Networks, Inc.
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
mél : kireeti@juniper.net

Yakov Rekhter
Juniper Networks, Inc.
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
mél : yakov@juniper.net

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

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

Le présent document et les informations contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

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

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

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

Remerciement

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