Groupe de travail Réseau
Request for Comments : 4090
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Pan, éditeur, Hammerhead Systems
G. Swallow, éditeur, Cisco Systems
A. Atlas, éditeur, Avici Systems
mai 2005

Extensions de réacheminement rapide à RSVP-TE pour tunnels LSP

Statut de ce mémoire
Le présent document spécifie un protocole en cours de normalisation de l'Internet 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 définit des extensions à RSVP-TE pour établir des tunnels de chemins à commutation d'étiquettes (LSP, *label-switched path*) de secours pour la réparation en local de tunnels de LSP. Ces mécanismes permettent la re-direction du trafic sur des tunnels LSP de secours en 10èmes de millisecondes, en cas de défaillance.

Deux méthodes sont définies. La méthode de secours biunivoque crée des LSP de contournement pour chaque LSP protégé à chaque point de réparation local potentiel. La méthode de sauvegarde de facilité crée un tunnel de contournement pour protéger un point de défaillance potentiel ; en tirant parti de la mise en pile d'étiquettes MPLS, ce tunnel de sauvegarde peut protéger un ensemble de LSP qui ont des contraintes de sauvegarde similaires. Les deux méthodes peuvent être utilisées pour protéger des liaisons et des nœuds durant une défaillance de réseau. Le comportement et les extensions à RSVP décrits permet aux nœuds de mettre en œuvre l'une ou l'autre méthode ou les deux et d'interopérer dans un réseau mixte.

Table des Matières

1. Introduction....2
1.1 Fondements....2
2. Terminologie....3
3. Techniques de réparation locale....4
3.1 Sauvegarde d'un à un....4
3.2 Sauvegarde de facilité....4
4. Extensions RSVP....5
4.1 Objet FAST_REROUTE....5
4.2 Objet DETOUR....6
4.3 Fanions SESSION_ATTRIBUTE....8
4.4 Fanions de sous objet RRO IPv4/IPv6....8
5. Comportement de l'extrémité de tête....9
6. Comportement du point de réparation local....9
6.1 Signalisation d'un chemin de sauvegarde....10
6.2 Procédures de calcul du chemin de sauvegarde....11
6.3 Signalisation des sauvegardes pour la protection biunivoque....12
6.4 Signalisation de la protection de facilité....14
6.5 Procédures du PLR durant la réparation locale....15
7. Comportement du nœud de fusion....16
7.1 Traitement des messages Path de sauvegarde avant défaillance....16
7.2 Traitement des défaillances....18
8. Comportement de tous les LSR....18
8.1 Fusion de Detour avec la méthode spécifique du chemin....18
9. Considérations sur la sécurité....19
10. Considérations relatives à l'IANA....19
10.1 Objet DETOUR....19
10.2 Objet FAST_REROUTE....19
11. Contributeurs....19
12. Remerciements....20
13. Références normatives....20

Adresse des éditeurs.....20
Déclaration complète de droits de reproduction.....20

1. Introduction

Le présent document étend RSVP [RFC2205] pour établir des tunnels de sauvegarde de chemin de commutation d'étiquettes (LSP, *label-switched path*) pour la réparation locale des tunnels de LSP. Cette extension satisfait aux besoins des applications en temps réel comme la voix sur IP, pour laquelle le trafic d'utilisateur devrait être redirigé sur des tunnels LSP de sauvegarde en dixièmes de millisecondes. Cette exigence de temps peut être satisfaite en calculant et signalant les tunnels LSP de sauvegarde avant la défaillance et en redirigeant le trafic aussi près que possible du point de défaillance. De cette façon, le temps de redirection n'inclut pas de calcul de chemin et pas de délai de signalisation, mais inclut les délais pour propager la notification de défaillance entre les routeurs de commutation d'étiquettes (LSR, *label-switched router*). La vitesse de réparation est le principal avantage des méthodes et extensions décrites ici. Le terme de réparation locale est utilisé lorsque on se réfère aux techniques qui redirigent du trafic sur un tunnel LSP de sauvegarde en réponse à une défaillance locale.

Un LSP protégé est un LSP à acheminement explicite auquel est fourni une protection. Les méthodes de réparation décrites sont applicables aux seuls LSP à acheminement explicite. L'application de ces méthodes aux LSP qui changent leur acheminement de façon dynamique, comme les LSP utilisés dans l'acheminement IGP en envoi individuel, sortent du domaine d'application du présent document.

La Section 2 parle de la nouvelle terminologie utilisée dans le document. La Section 3 décrit les deux méthodes de base pour créer des LSP de sauvegarde. La Section 4 décrit les extensions au protocole RSVP qui prennent en charge la protection locale. La Section 5 présente le comportement d'un LSR qui cherche à demander une protection locale pour un LSP. Le comportement d'un potentiel point de réparation locale (PLR, *point of local repair*) est décrit à la Section 6, qui précise aussi comment déterminer la stratégie appropriée pour protéger un LSP et comment mettre en œuvre chaque stratégie. La Section 7 décrit le comportement d'un nœud de fusion, le LSR où un LSP protégé et son LSP de sauvegarde se rejoignent. Finalement, la Section 8 discute du comportement requis des autres nœuds dans le réseau.

Les méthodes discutées dans ce document dépendent de trois hypothèses :
- Un LSR qui est sur le chemin d'un LSP protégé devrait toujours supposer qu'il est un point de fusion. C'est nécessaire parce que la méthode de sauvegarde de facilité ne signale pas les sauvegardes à travers un tunnel de contournement avant la défaillance.
- Si la méthode de sauvegarde biunivoque est utilisée et si un objet DETOUR est inclus, les LSR dans le réseau à ingénierie du trafic devraient prendre en charge l'objet DETOUR. C'est nécessaire afin que les messages Path contenant l'objet DETOUR ne soient pas rejetés.
- La compréhension de l'objet DETOUR est nécessaire pour la prise en charge de la méthode spécifique du chemin, qui exige que les LSR dans le réseau à ingénierie du trafic soient capables de fusionner les détours.

1.1 Fondements

Plusieurs années avant que commence le travail sur le présent document, les réseaux opérationnels avaient déployé deux méthodes indépendantes pour faire le réacheminement rapide ; ces méthodes sont appelées ici sauvegarde biunivoque, et sauvegarde de facilité. Les fabricants qui essayent de prendre en charge les deux méthodes rencontrent des problèmes de compatibilité en essayant de produire une seule mise en œuvre capable d'interopérer avec les deux méthodes. Il y a des compromis techniques entre les deux méthodes. Ces compromis sont tellement dépendants de la topologie que la communauté n'a pas pu se mettre d'accord sur une seule approche.

Le présent document rationalise la signalisation RSVP pour les deux méthodes afin que toute mise en œuvre puisse reconnaître toutes les demandes de réacheminement rapide et répondre clairement. La réponse peut être positive si la méthode peut être effectuée, ou elle peut être une claire erreur pour informer le demandeur de chercher d'autres moyens de sauvegarde. Le présent document permet aussi qu'une seule mise en œuvre prenne en charge les deux méthodes, fournissant par là une gamme de capacités. Le comportement décrit et les extensions à RSVP permettent aux LER et LSR de mettre en œuvre l'une ou l'autre méthode ou les deux.

Bien que les deux méthodes puissent en principe être utilisées dans un seul réseau, on s'attend à ce que les opérateurs continuent de déployer l'une ou l'autre. Le but de ce document est de normaliser la signalisation RSVP afin qu'un réseau composé de LSR qui mettent en œuvre les deux méthodes ou un réseau composé de certains LSR qui prennent en charge une méthode et d'autres qui prennent en charge les deux puissent correctement faire la signalisation parmi ces LSR pour réaliser la restauration rapide.

2. Terminologie

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].

Le lecteur est supposé être familiarisé avec la terminologie des [RFC2205] et [RFC3209].

LSR (*Label-Switch Router*) : routeur à commutation d'étiquettes

LSP (*Label-Switched Path*) : chemin à commutation d'étiquettes MPLS. Ici, un LSP est toujours acheminé explicitement.

Réparation locale : techniques utilisées pour réparer rapidement les tunnels LSP lors d'une défaillance d'un nœud ou d'une liaison le long du LSP.

PLR (*Point of Local Repair*) . point de réparation local ; c'est le LSR d'extrémité de tête d'un tunnel de sauvegarde ou d'un LSP de détour.

Sauvegarde biunivoque *(One-to-One Backup)* : méthode de réparation locale dans laquelle un LSP de secours est créé séparément pour chaque LSP protégé à un PLR.

Sauvegarde de facilité : méthode de réparation locale dans laquelle un tunnel de contournement est utilisé pour protéger un ou plusieurs LSP protégés qui traversent le PLR, la ressource protégée, et le point de fusion, dans cet ordre.

LSP protégé : un LSP est dit être protégé à un certain bond si il a un ou plusieurs tunnels de sauvegarde associés qui ont leur origine à ce bond.

LSP de détour : LSP qui est utilisé pour réacheminer le trafic en contournant une défaillance dans une sauvegarde biunivoque.

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

Tunnel de sauvegarde : LSP utilisé pour sauvegarder un des nombreux LSP dans une sauvegarde de beaucoup à une.

Tunnel de contournement de prochain bond : tunnel de sauvegarde qui contourne une seule liaison du LSP protégé.

Tunnel de contournement du prochain prochain bond : tunnel de sauvegarde qui contourne un seul nœud du LSP protégé.

Chemin de sauvegarde : LSP qui est responsable de sauvegarder un LSP protégé. Un chemin de sauvegarde se réfère soit à un LSP de détour, soit à un tunnel de sauvegarde.

Point de fusion (MP, *Merge Point*) : LSR où un ou plusieurs tunnels de sauvegarde rejoignent le chemin du LSP protégé en aval de la défaillance potentielle. Le même LSR peut être à la fois un MP et un PLR.

Point de fusion de détour (DMP, *Detour Merge Point*) : Dans le cas d'une sauvegarde biunivoque, c'est un LSR où plusieurs détours convergent. Un seul détour est signalé au delà de ce LSR.

LSP réacheminable : Tout LSP pour lequel le LSR d'extrémité de tête demande une protection locale. Voir les détails à la Section 5.

Chemin le plus court en premier fondé sur la contrainte (CSPF, *Constraint-based Shortest Path First*).

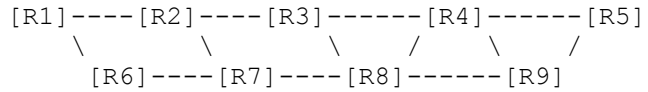
Groupe de liaisons à risques partagés (SRLG, *Shared Risk Link Group*) disjoint : un chemin est considéré être un SRLG disjoint à partir d'une certaine liaison ou nœud si le chemin n'utilise aucune liaison ou nœud qui appartient au même SRLG que cette liaison ou nœud.

3. Techniques de réparation locale

On décrit deux méthodes différentes pour la protection locale. Dans la méthode de sauvegarde biunivoque, un PLR calcule un LSP de sauvegarde séparé, appelé LSP de détour, pour chaque LSP que protège le PLR. Dans la méthode de sauvegarde de facilité, le PLR crée un seul tunnel de contournement qui peut être utilisé pour protéger plusieurs LSP.

3.1 Sauvegarde d'un à un

Dans la méthode biunivoque, un chemin à commutation d'étiquettes est établi qui coupe de LSP original quelque part en aval du point de défaillance de la liaison ou du nœud. Un LSP de sauvegarde séparé est établi pour chaque LSP qui est sauvegardé.



LSP protégé : [R1->R2->R3->R4->R5]
Sauvegarde de R1 : [R1->R6->R7->R8->R3]
Sauvegarde de R2 : [R2->R7->R8->R4]
Sauvegarde de R3 : [R3->R8->R9->R5]
Sauvegarde de R4 : [R4->R9->R5]

Exemple 1. Technique de sauvegarde biunivoque

Dans la topologie simple que montre l'exemple 1, le LSP protégé va de R1 à R5. R2 peut fournir la protection du trafic d'utilisateur en créant un LSP partiel de sauvegarde qui fusionne avec le LSP protégé en R4. On se réfère à un LSP partiel de sauvegarde biunivoque [R2->R7->R8->R4] comme un détour.

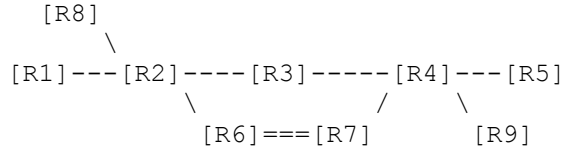
Pour protéger un LSP qui traverse pleinement N nœuds, il pourrait y avoir (N - 1) détours. L'exemple 1 montre les chemins pour les détours nécessaires pour protéger pleinement le LSP de l'exemple. Pour minimiser le nombre de LSP dans le réseau, il est souhaitable de fusionner un détour de façon à ce qu'il retourne à son LSP protégé, lorsque c'est faisable. Lorsque un détour LSP coupe son LSP protégé à un LSR avec la même interface sortante, il va être fusionné.

Lorsque une défaillance se produit sur le LSP protégé, le PLR redirige le trafic sur le détour local. Par exemple, si la liaison [R2->R3] a une défaillance dans l'exemple 1, R2 va passer le trafic reçu de R1 sur le LSP protégé le long de la liaison [R2->R7], en utilisant l'étiquette reçue lorsque R2 a créé le détour. Quand R4 reçoit du trafic avec l'étiquette fournie pour le détour de R2, R4 va passer ce trafic à la liaison [R4-R5], en utilisant l'étiquette reçue de R5 pour le LSP protégé. À aucun moment la profondeur de la pile d'étiquettes n'augmente par suite du détour. Alors que R2 utilise son détour, le trafic va prendre le chemin [R1->R2->R7->R8->R4->R5].

3.2 Sauvegarde de facilité

La méthode de sauvegarde de facilité tire parti de la pile d'étiquettes MPLS. Au lieu de créer un LSP séparé pour chaque LSP sauvegardé, un seul LSP est créé qui sert de sauvegarde pour un ensemble de LSP. On appelle un tel tunnel LSP un tunnel de contournement.

Le tunnel de contournement doit couper le chemin du ou des LSP d'origine quelque part en aval du PLR. Naturellement, cela restreint l'ensemble des LSP sauvegardés via ce tunnel de contournement à ceux qui passent à travers un nœud aval commun. Tous les LSP qui passent par le point de réparation local et à travers ce nœud commun qui n'utilisent pas aussi les facilités impliquées dans le tunnel de contournement sont candidats à cet ensemble de LSP.



LSP protégé 1 : [R1->R2->R3->R4->R5]
LSP protégé 2 : [R8->R2->R3->R4]
LSP protégé 3 : [R2->R3->R4->R9]
LSP tunnel de contournement : [R2->R6->R7->R4]

Exemple 2. Technique de sauvegarde de facilité.

Dans l'exemple 2, R2 a construit un tunnel de contournement qui protège contre les défaillance de liaison [R2->R3] et de nœud [R3]. Les lignes doubles représentent ce tunnel. Cette technique fournit une amélioration de l'adaptabilité, en ce que le même tunnel de contournement peut aussi être utilisé pour protéger les LSP de R1, R2, ou R8 à R4, R5, ou R9. L'exemple 2 décrit trois LSP protégés différents qui utilisent le même tunnel de contournement pour la protection.

Comme avec la méthode biunivoque, il peut y avoir jusqu'à (N-1) tunnels de contournement pour protéger pleinement un LSP qui traverse N nœuds. Cependant, chacun de ces tunnels de contournement pourrait protéger un ensemble de LSP.

Lorsque une défaillance se produit le long d'un LSP protégé,le PLR redirige le trafic sur le tunnel de contournement approprié. Par exemple, si la liaison [R2->R3] est défaillante dans l'exemple 2, R2 va commuter le trafic reçu de R1 sur le LSP protégé vers la liaison [R2->R6]. L'étiquette sera commutée en une qui sera comprise par R4 comme indiquant le LSP protégé, et l'étiquette du tunnel de contournement sera alors poussée sur la pile d'étiquettes des paquets redirigés. Si le saut d'avant dernier bond est utilisé, le point de fusion de l'exemple 2, R4, va recevoir le paquet redirigé avec une étiquette indiquant le LSP protégé que le paquet va suivre. Si le saut d'avant dernier bond n'est pas utilisé , R4 va sauter l'étiquette du tunnel de contournement et examiner l'étiquette en dessous pour déterminer le LSP protégé que le paquet doit suivre. Quand R2 utilise le tunnel de contournement pour le LSP protégé 1, le trafic prend le chemin [R1->R2->R6->R7->R4->R5] ; le tunnel de contournement est la connexion entre R2 et R4.

4. Extensions RSVP

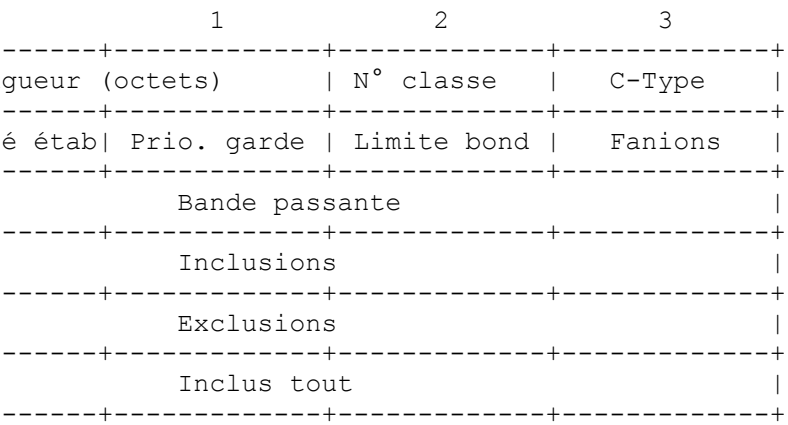
La présente spécification définit deux objets supplémentaires, FAST_REROUTE et DETOUR, pour étendre RSVP-TE pour la signalisation de redirection rapide. Ces nouveaux objets sont rétro compatibles avec les LSR qui ne les reconnaissent pas (voir le paragraphe 3.10 de la [RFC2205]). Les deux objets ne peuvent être portés que dans les messages RSVP Path.

Les objets SESSION_ATTRIBUTE et RECORD_ROUTE sont aussi étendus pour prendre en charge les dispositifs de protection de bande passante et de nœud.

4.1 Objet FAST_REROUTE

L'objet FAST_REROUTE est utilisé pour contrôler la sauvegarde utilisée pour le LSP protégé. Il spécifie les priorités d'établissement et de garde, les filtres d'attribut de session, et la bande passante à utiliser pour la protection. Il permet aussi une méthode spécifique de protection à demander. Cet objet DOIT être inséré seulement dans le message Path par l'extrémité de tête de LER et NE DOIT PAS être changé par les LSR en aval. L'objet FAST_REROUTE a le format suivant :

Numéro de classe = 205
C-Type = 1



Priorité d'établissement : priorité du chemin de sauvegarde par rapport à la prise de ressources, dans la gamme 0 à 7. La valeur 0 est la plus haute priorité. La priorité d'établissement est utilisée pour décider si cette session peut préempter une autre session. Voir la [RFC3209] sur l'utilisation des priorités.

Priorité de garde : priorité du chemin de sauvegarde par rapport aux ressources de garde, dans la gamme 0 à 7. La valeur 0

est la plus haute priorité. La priorité de garde est utilisée pour décider si cette session peut être préemptée par une autre session. Voir la [RFC3209] sur l'utilisation des priorités.

Limite de bond : nombre maximum de bonds supplémentaires que le chemin de sauvegarde peut prendre, du nœud actuel (un PLR) à un MP, le PLR et le MP étant exclus du compte. Par exemple, une limite de bonds de 0 signifie que seules les liaisons directes entre le PLR et le MP peuvent être prise en compte.

Fanions :
0x01 : sauvegarde biunivoque désirée. Demande la protection via la méthode de sauvegarde biunivoque.
0x02 : sauvegarde de facilité désirée. Demande la protection via la méthode de sauvegarde de facilité.

Bande passante : estimation de bande passante ; entier de 32 bits en virgule flottante IEEE, en octets par seconde.

Exclusions : valeur de 32 bits représentant un ensemble de filtres d'attributs associés à un chemin de sauvegarde, dont tous rendent une liaison inacceptable.

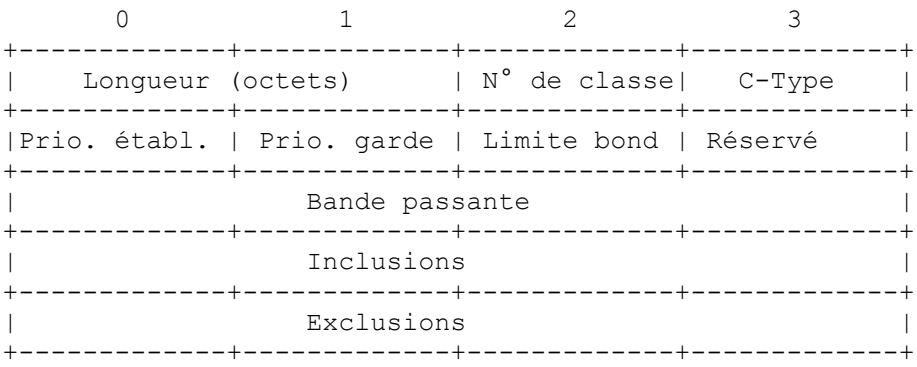
Inclusions : valeur de 32 bits représentant un ensemble de filtres d'attributs associés à un chemin de sauvegarde, dont tous rendent une liaison acceptable (par rapport à cet essai). Un ensemble nul (tous les bits à zéro) réussit automatiquement.

Inclus tout : valeur de 32 bits représentant un ensemble de filtres d'attributs associés à un chemin de sauvegarde, dont tous doivent être présents pour qu'une liaison soit acceptable (par rapport à cet essai). Un ensemble nul (tous les bits à zéro) réussit automatiquement.

Les deux bits de poids fort du numéro de classe (11) sont cause que les nœuds qui ne comprennent pas l'objet l'ignorent et le passent inchangé.

À des fins d'information, une valeur et un format différents de C-Type sont spécifiés ci-dessous pour l'objet FAST_REROUTE. Ils sont utilisés par les mises en œuvre traditionnelles. La signification des champs est la même que celle décrit pour le C-Type 1.

Numéro de classe = 205
C-Type = 7



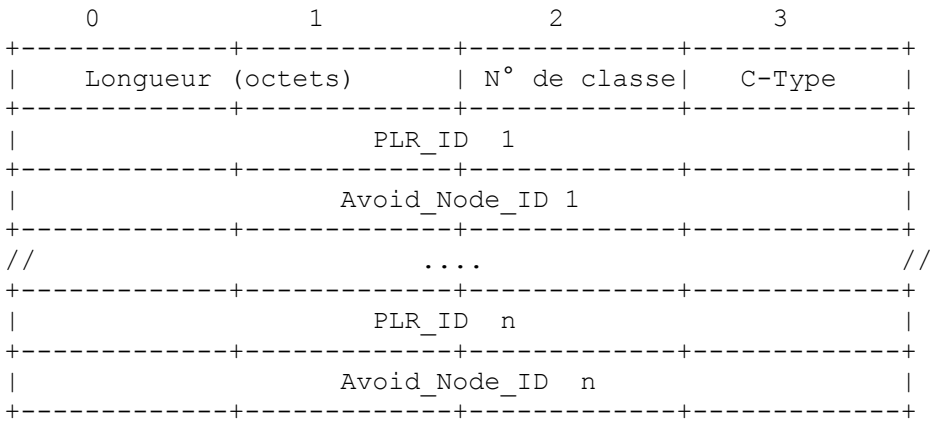
Les C-Types inconnus devraient être traités comme spécifié au paragraphe 3.10 de la [RFC2205].

4.2 Objet DETOUR

L'objet DETOUR est utilisé dans la méthode de sauvegarde biunivoque pour identifier les LSP de détour.

4.2.1 Objet DETOUR pour adresse IPv4

Numéro de classe = 63
C-Type = 7

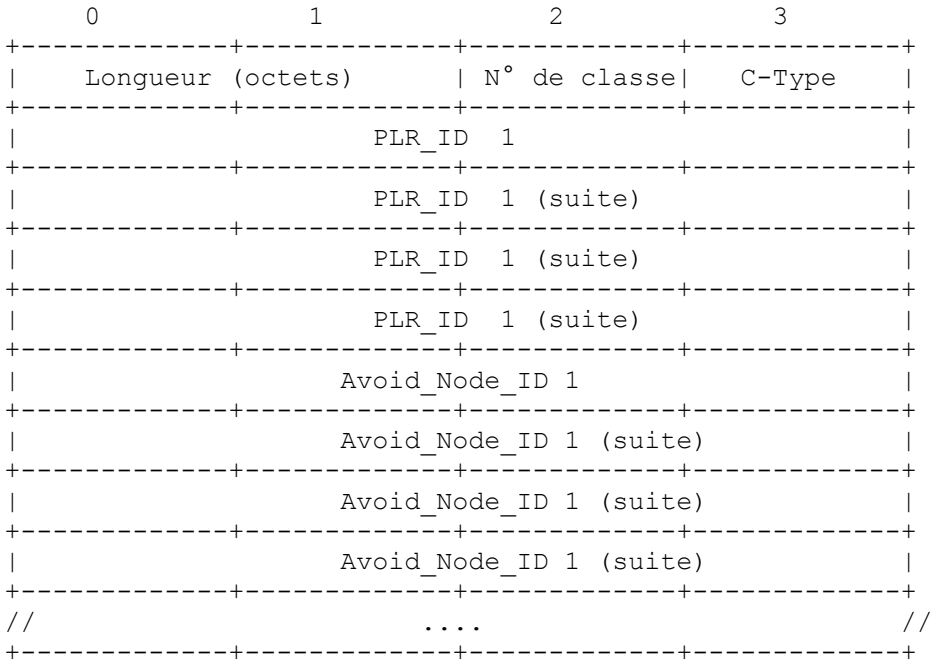


PLR_ID (1 - n) : adresse IPv4 qui identifie le PLR commençant le point de détour. Toute adresse locale sur le PLR peu être utilisée.

Avoid_Node_ID (1 - n) : adresse IPv4 qui identifie le nœud immédiatement en aval que le PLR essaye d'éviter. Toute adresse locale du nœud aval peut être utilisée. Ce champ est obligatoire et est utilisé par le MP pour les règles de fusion exposées plus loin.

4.2.2 Objet DETOUR pour adresse IPv6

Numéro de classe = 63
C-Type = 8



PLR_ID (1 - n) : adresse IPv6 de 128 bits d'hôte d'envoi individuel identifiant le PLR qui est le point de départ du détour. Toute adresse locale sur le PLR peut être utilisée.

Avoid_Node_ID (1 - n) : adresse IPv6 de 128 bits d'hôte d'envoi individuel identifiant le nœud immédiatement en aval que le PLR essaye d'éviter. Toute adresse locale du nœud aval peut être utilisée. Ce champ est obligatoire et est utilisé par le MP pour les règles de fusion exposées ci-dessous.

Il peut y avoir plus d'une paire d'entrées (PLR_ID, Avoid_Node_ID) dans un objet DETOUR. Sion désire la fusion de détours, après chaque opération de fusion, le point de fusion de détour devrait combiner touts les détours fusionnés dans les messages Path suivants.

Le bit de poids fort du numéro de classe est zéro ; les LSR qui ne prennent pas en charge les objets DETOUR DOIVENT rejeter tout message Path contenant un objet DETOUR et envoyer une PathErr pour le notifier au PLR. Cette PathErr

DEVRAIT être générée comme spécifié dans la [RFC2205] pour les objets inconnus avec un numéro de classe de forme "0bbbbbbb".

Les C-Types inconnus devraient être traités comme spécifié au paragraphe 3.10 de la [RFC2205].

4.3 Fanions SESSION_ATTRIBUTE

Pour demander explicitement la protection de la bande passante et du nœud, deux nouveaux fanions sont définis dans l'objet SESSION_ATTRIBUTE.

Pour les deux C-Type 1 et 7, l'objet SESSION_ATTRIBUTE a actuellement les fanions suivants définis dans la [RFC3209] :

Protection locales désirée : 0x01
Ce fanion permet aux routeurs de transit d'utiliser un mécanisme local de réparation qui peut résulter en une violation de l'objet Chemin explicite. Quand une faute est détectée sur la liaison ou nœud aval adjacent, un nœud de transit peut réacheminer le trafic pour une restauration rapide de service.

Enregistrement d'étiquette désiré : 0x02
Ce fanion indique que les informations d'étiquette devraient être incluses lors d'un enregistrement de chemin.

Style partagé explicite désiré : 0x04
(SE, *Shared Explicit*) Ce fanion indique que le nœud d'entrée du tunnel peut choisir de réacheminer ce tunnel sans le détruire. Un nœud de sortie de tunnel DEVRAIT utiliser le style SE en répondant avec un message Resv. Lors d'une demande de réacheminement rapide, le LSR d'extrémité de tête DEVRAIT établir ce fanion ; cela n'est pas nécessaire pour la méthode spécifique du chemin de la méthode de sauvegarde biunivoque.

Les nouveaux fanions suivants sont définis :

Protection de bande passante désirée : 0x08
Ce fanion indique aux PLR le long du LSP protégé qu'un chemin de sauvegarde avec une bande passante garantie est désiré. La bande passante à garantir est celle du LSP protégé, si aucun objet FAST_REROUTE n'est inclus dans le message Path ; si un objet FAST_REROUTE est dans le message Path, la bande passante qui y est spécifiée est à garantir.

Protection de nœud désirée : 0x10
Ce fanion indique aux PLR le long d'un LSP protégé qu'un chemin de sauvegarde qui contourne au moins le prochain nœud du LSP protégé est désiré.

4.4 Fanions de sous objet RRO IPv4/IPv6

Pour rapporter si la protection de bande passante et/ou de nœud est fournie comme demandé, on définit deux nouveaux fanions dans le sous objet RECORD_ROUTE *(RRO)* IPv4.

Les sous objets Adresse RRO IPv4 et IPv6 ont actuellement les fanions suivants définis dans la [RFC3209] :

Protection locale disponible : 0x01
Indique que la liaison en aval de ce nœud est protégée via un mécanisme de réparation local, qui peut être la sauvegarde biunivoque ou de facilité.

Protection locale en service : 0x02
Indique qu'un mécanisme de réparation local est en service pour maintenir ce tunnel (généralement face à une panne de la liaison sur laquelle il était précédemment acheminé, ou une panne du nœud voisin).

Deux nouveaux fanions sont définis :

Protection de bande passante : 0x04
Le PLR va établir ce bit quand ce LSP protégé a un chemin de sauvegarde garanti pour fournir la bande passante désirée qui est spécifiée dans l'objet FAST_REROUTE ou la bande passante du LSP protégé, si aucun objet FAST_REROUTE n'était inclus. Le PLR peut établir ce bit chaque fois que la bande passante désirée est garantie ; le PLR DOIT établir ce fanion quand la bande passante désirée est garantie et que le fanion "protection de bande passante désirée" est établi dans l'objet SESSION_ATTRIBUTE. Si la bande passante demandée n'est pas garantie, le PLR NE DOIT PAS établir ce fanion.

Protection du nœud : 0x08
Le PLR va établir ce bit quand le LSP protégé a un chemin de sauvegarde qui fournit la protection contre une défaillance du prochain LSR le long du LSP protégé. Le PLR peut établir ce bit chaque fois que la protection de nœud est fournie par le chemin de sauvegarde du LSP protégé ; le PLR DOIT établir ce fanion quand la protection de nœud est fournie et que le fanion "Protection de nœud désirée" est établi dans l'objet SESSION_ATTRIBUTE. Si la protection de nœud n'est pas fournie, le PLR NE DOIT PAS établir ce fanion. Donc, si un PLR n'a pas pu établir un chemin de sauvegarde de protection de liaison, le bit "Protection locale disponible" ne sera pas établi, mais le bit "Protection de nœud" sera à zéro.

5. Comportement de l'extrémité de tête

L'extrémité de tête d'un LSP détermine si la protection locale devrait être demandée pour ce LSP et quelle méthode de protection locale est désirée pour le LSP protégé. L'extrémité de tête détermine aussi quelles contraintes devraient être demandées pour les chemins de sauvegarde d'un LSP protégé.

Pour indiquer qu'un LSP devrait être protégé localement, le LSR d'extrémité de tête DOIT soit établir le fanion "Protection locale désirée" dans l'objet SESSION_ATTRIBUTE, soit inclure un objet FAST_REROUTE dans le message Path, ou les deux. Le fanion "Protection locale désirée" dans l'objet SESSION_ATTRIBUTE DEVRAIT toujours être établi. Si un LSR d'extrémité de tête signale un objet FAST_REROUTE, il DOIT être mémorisé pour les rafraîchissements de chemin.

Le LSR d'extrémité de tête d'un LSP protégé DOIT établir le fanion "Enregistrement d'étiquette désiré" dans l'objet SESSION_ATTRIBUTE. Cela facilite l'utilisation de la méthode de sauvegarde de facilité. Si la protection de nœud est désirée, le LSR d'extrémité de tête devrait établir le fanion "Protection de nœud désirée" dans l'objet SESSION_ATTRIBUTE ; autrement, ce fanion devrait être à zéro. De même, si une garantie de protection de bande passante est désirée, le fanion "Protection de bande passante désirée" dans l'objet SESSION_ATTRIBUTE devrait alors être établi ; autrement, ce fanion devrait être à zéro. Si le LSR d'extrémité de tête détermine que le contrôle des chemins de sauvegarde pour le LSP protégé est désiré, le LSR devrait alors inclure l'objet FAST_REROUTE. Les PLR vont utiliser les filtres d'attribut, la bande passante, la limite de bonds, et les priorités pour déterminer les chemins de sauvegarde.

Si le LSR d'extrémité de tête désire que la méthode de sauvegarde biunivoque soit utilisée pour le LSP protégé, le LSR d'extrémité de tête devrait alors inclure un objet FAST_REROUTE et établir le fanion "Sauvegarde biunivoque désirée". Si le LSR d'extrémité de tête désire que le LSP protégé soit protégé via la méthode de sauvegarde de facilité, le LSR d'extrémité de tête devrait alors inclure un objet FAST_REROUTE et établir le fanion "Sauvegarde de facilité désirée". L'absence d'un objet FAST_REROUTE, ou avoir ces deux fanions à zéro, devrait être traité par les PLR comme une absence de préférence. Si les deux fanions sont établis, un PLR peut utiliser l'une ou l'autre méthode ou les deux.

Le LSR d'extrémité de tête d'un LSP protégé DOIT prendre en charge les fanions supplémentaires définis au paragraphe 4.4 qu'ils soient établis ou non dans les sous objets RRO IPv4 et IPv6. Le LSR d'extrémité de tête d'un LSP protégé DOIT prendre en charge le sous objet Étiquette RRO.

Si le LSR d'extrémité de tête d'un LSP détermine que la protection locale est à nouveau désirée, cela DEVRAIT être signalé via le mécanisme "make-before-break" *(à faire avant la fin)*.

6. Comportement du point de réparation local

Chaque LSR le long d'un LSP protégé (sauf celui de sortie) DOIT suivre le comportement de PLR décrit dans le présent document.

Un PLR DEVRAIT prendre en charge l'objet FAST_REROUTE, les fanions "Protection locale désirée", "Enregistrement d'étiquette désirée", "Protection de nœud désirée", et "Protection de bande passante désirée" dans l'objet SESSION_ATTRIBUTE, et les fanions "Protection locale disponible", "Protection locale utilisée", "Protection de bande passante", et "Protection de nœud" dans les sous objets RRO IPv4 et IPv6. Un PLR PEUT prendre en charge l'objet DETOUR.

Un PLR DOIT considérer qu'un LSP a demandé la protection locale si le fanion "Protection locale désirée" est établi dans l'objet SESSION_ATTRIBUTE et/ou si l'objet FAST_REROUTE est inclus. Si l'objet FAST_REROUTE est inclus, un PLR DEVRAIT considérer de fournir la protection biunivoque si le fanion "Biunivoque désirée" est établi, et il DEVRAIT considérer de fournir la sauvegarde de facilité si le fanion "Sauvegarde de facilité désirée" est établi. Si le fanion "Protection de nœud désirée" est établi, le PLR DEVRAIT essayer de fournir la protection de nœud ; si ce n'est pas

faisable, le PLR DEVRAIT alors essayer de fournir la protection de liaison. Si le fanion "Protection de bande passante garantie" est établi, le PLR DEVRAIT essayer de fourni une garantie de bande passante ; si ce n'est pas faisable, le PLR DEVRAIT alors essayer de fournir une sauvegarde sans garantie de la bande passante complète.

Le traitement suivant doit être effectué pour les fanions de sous objet RRO IPv4 ou IPv6 si un RRO est inclus dans le message RESV du LSP protégé. Sur la base de ces informations supplémentaires, l'extrémité de tête peut prendre les mesures appropriées.

- Jusqu'à ce qu'un PLR ait un chemin de sauvegarde disponible, il DOIT mettre à zéro des quatre fanions pertinents dans le sous objet RRO IPv4 ou IPv6 correspondant.

- Chaque fois que le PLR a un chemin de sauvegarde disponible, il DOIT établir le fanion "Protection locale disponible". Si aucun LSP établi de sauvegarde biunivoque ou tunnel de contournement n'existe, ou si le LSP biunivoque et le tunnel de contournement est dans l'état "DOWN", le PLR DOIT mettre à zéro le fanion "Protection locale disponible" dans son sous objet Adresse IPv4 (ou IPv6) du RRO et DEVRAIT envoyer le RESV mis à jour.

- Le PLR DOIT mettre à zéro le fanion "Protection locale utilisée" sauf si il redirige activement le trafic sur le chemin de sauvegarde au lieu de sur le LSP protégé.

- Le PLR DEVRAIT aussi établir le fanion "Protection de nœud" si le chemin de sauvegarde protège contre la défaillance du nœud immédiatement en aval, et, si le chemin ne le fait pas, le PLR DEVRAIT mettre à zéro le fanion "Protection de nœud". Ceci DOIT être fait si le fanion "Protection de nœud désirée" était établi dans l'objet SESSION_ATTRIBUTE.

- Le PLR DEVRAIT établir le fanion "Protection de bande passante" si le chemin de sauvegarde offre une garantie de bande passante, et, si le chemin ne le fait pas, le PLR DEVRAIT mettre à zéro le fanion "Protection de bande passante". Ceci DOIT être fait si le fanion "Protection de bande passante désirée" était établi dans l'objet SESSION_ATTRIBUTE.

6.1 Signalisation d'un chemin de sauvegarde

Un certain nombre d'objectifs doivent être réalisés pour obtenir une solution de signalisation satisfaisante. Elles sont résumées comme suit :
1. Identifier sans ambiguïté et de façon univoque les chemins de sauvegarde.
2. Associer sans ambiguïté les LSP protégés à leurs chemins de sauvegarde.
3. Fonctionner avec les espaces d'étiquette globaux aussi bien que non globaux.
4. Permettre la fusion des chemins de sauvegarde.
5. Maintenir l'état RSVP durant et après la reprise sur défaillance.

Les tunnels LSP sont identifiés par une combinaison d'objets SESSION et SENDER_TEMPLATE [RFC3209]. Les champs pertinents sont les suivants.

Adresse IPv4 (ou IPv6) de point d'extrémité de tunnel

Adresse IPv4 (ou IPv6) du nœud de sortie du tunnel.

Identifiant de tunnel : identifiant de 16 bits utilisé dans l'objet SESSION, qui reste constant durant la vie du tunnel.

Identifiant de tunnel étendu : identifiant de 32 bits (IPv4) ou 128 bits (IPv6) utilisé dans le SESSION qui reste constant sur la vie du tunnel. Normalement il est réglé tout à zéro. Les nœuds d'entrée qui souhaitent réduire la portée d'une session à la paire entrée-sortie peuvent placer leur adresse IP ici comme identifiant unique au monde.

Adresse IPv4 (ou IPv6) de l'envoyeur du tunnel

Adresse IPv4 (ou IPv6) d'un nœud envoyeur.

Identifiant de LSP : identifiant de 16 bits utilisé dans le SENDER_TEMPLATE et le FILTER_SPEC, qui peut être changé pour permettre à un envoyeur de partager des ressources avec lui-même.

Les trois premiers sont dans l'objet SESSION et sont l'identification de base du tunnel. Régler le champ "Identifiant étendu de tunnel" à une adresse IP du LSR d'extrémité de tête permet que la portée de la SESSION soit réduite aux seuls LSP envoyés par ce LSR. Un LSP de sauvegarde est considéré faire partie de la même session que son LSP protégé ; donc ces trois champs ne peuvent pas être changés.

Les deux derniers sont dans le SENDER_TEMPLATE. Plusieurs LSP dans la même session peuvent être protégés et peuvent prendre de chemins différents ; ceci est courant lorsque un tunnel est réacheminé en utilisant le dispositif "make-before-break" *(faire avant la fin)*. Un chemin de sauvegarde doit être clairement identifié avec son LSP protégé pour permettre une fusion et un traitement d'état corrects. Donc, un chemin de sauvegarde doit hériter du LSP protégé associé son identifiant de LSP. Donc, le seul champ dans les objets SESSION et SENDER_TEMPLATE qui puisse être changé entre un chemin de sauvegarde et un LSP protégé est le champ "Adresse IPv4 (ou IPv6) de l'envoyeur du tunnel" dans le SENDER_TEMPLATE.

Il y a deux méthodes différentes pour identifier de façon univoque un chemin de sauvegarde, qui sont décrites ci dessous.

6.1.1 Identification du chemin de sauvegarde : spécifique de gabarit d'envoyeur

Dans cette approche, l'objet SESSION et le LSP_ID sont copiés du LSP protégé. Le champ "Adresse d'envoyeur de tunnel IPv4" est réglé à une adresse du PLR. Si l'extrémité de tête d'un tunnel agit aussi comme PLR, elle DOIT choisir une adresse IP différente de celle utilisée dans le SENDER_TEMPLATE du tunnel de LSP d'origine.

Lorsque l'approche spécifique de gabarit d'envoyeur est utilisée, le LSP protégés et les chemins de sauvegarde DEVRAIENT utiliser le style partagé explicite (SE, *Shared Explicit*). Cela permet le partage de bande passante entre plusieurs chemins de sauvegarde. Les chemins de sauvegarde et le LSP protégé PEUVENT être fusionnés par les points de fusion de détour, lorsque les objets EXPLICIT_ROUTE (ERO, *EXPLICITE-ROUTE Object*) du MP à la sortie sont les mêmes sur chaque LSP à fusionner, comme spécifié dans la [RFC3209].

6.1.2 Identification du chemin de sauvegarde : spécifique du chemin

Dans cette approche, plutôt que de changer les objets SESSION ou SENDER_TEMPLATE, une mise en œuvre utilise un nouvel objet, l'objet DETOUR, pour distinguer les messages Path pour un chemin de sauvegarde et le LSP protégé.

Donc, les chemins de sauvegarde utilisent les mêmes objets SESSION et SENDER_TEMPLATE que ceux utilisés dans le LSP protégé. La présence d'un objet DETOUR dans les messages Path signifie un chemin de sauvegarde ; la présence d'un objet FAST_REROUTE et/ou du fanion "Protection locale demandée" dans l'objet SESSION_ATTRIBUTE indique un LSP protégé.

Dans l'approche spécifique de message Path, un LSR fusionne les messages Path qui sont reçus avec les mêmes objets SESSION et SENDER_TEMPLATE et qui ont aussi le même objet Prochain bond. Sans ce comportement, il serait impossible d'associer les multiples messages RESV aux chemins de sauvegarde. Cependant, ce comportement de fusion réduit le nombre total d'états RSVP dans le réseau aux dépens de la fusion des LSP avec des ERO différents.

6.2 Procédures de calcul du chemin de sauvegarde

Avant qu'un PLR puisse créer un détour ou un tunnel de contournement, le chemin explicite désiré doit être déterminé. Ce peut être fait en utilisant un calcul de chemin le plus court en premier fondé sur la contrainte (CSPF, *Constraint-based Shortest Path First*). Avant le calcul de CSPF, les informations suivantes doivent être collectées au PLR :

- La liste des nœuds aval au travers desquels passe le LSP protégé. Cette information est directement disponible à partir des objets RECORD_ROUTE durant l'établissement du LSP. Cette information est aussi disponible à partir de l'ERO. Cependant, si le ERO contient des sous objets lâches, il peut ne pas fournir des informations adéquates.

- Les liaisons/nœuds vers l'aval dont on veut se protéger. Là encore, cette information est apprise des objets RECORD_ROUTE. Si la protection de nœud est désirée, elle est déterminée par le fanion "Protection de nœud" dans l'objet SESSION_ATTRIBUTE et par la politique locale.

- Les liaisons unidirectionnelles amont au travers desquelles le LSP protégé passe. Cette information est apprise des objets RECORD_ROUTE ; elle n'est nécessaire que pour établir une protection biunivoque. Dans la méthode spécifique du chemin, il est nécessaire d'éviter que le détour et le LSP protégé partagent un prochain bond commun en amont de la défaillance. Dans le mode spécifique de gabarit d'envoyeur, cette même restriction est nécessaire pour éviter le partage de bande passante entre le détour et son LSP protégé, lorsque cette bande passante n'a été réservée qu'une seule fois.

- Les filtres d'attribut de liaison à appliquer. Ceux-ci sont déduits de l'objet FAST_REROUTE, si il est inclus dans le message Path, ou autrement de l'objet SESSION_ATTRIBUTE.

- La bande passante à utiliser se trouve dans l'objet FAST_REROUTE, si il est inclus dans le message Path, ou autrement

dans l'objet SESSION_ATTRIBUTE. La politique locale peut modifier la bande passante à réserver.

- La limite de bonds, si un objet FAST_REROUTE était inclus dans le message Path.

Quand un algorithme de CSPF est utilisé pour calculer le chemin de sauvegarde, les contraintes suivantes doivent être respectées :

- Pour les LSP de détour, la destination DOIT être l'extrémité de queue du LSP protégé. Pour les tunnels de contournement (Section 7), la destination DOIT être l'adresse du MP.

- Lorsque la protection biunivoque est établie en utilisant la méthode spécifique de chemin, un détour NE DOIT PAS traverser les liaisons en amont du LSP protégé dans la même direction. Cela empêche la possibilité d'une fusion précoce du détour dans le LSP protégé. Lorsque la protection biunivoque est établie en utilisant la méthode spécifique du gabarit d'envoyeur, un détour ne devrait pas traverser les liaisons en amont du LSP protégé dans la même direction. Cela empêche de partager la bande passante entre un LSP protégé et sa sauvegarde en amont de la défaillance où la bande passante serait utilisée deux fois en cas de défaillance.

- Le LSP de sauvegarde ne peut pas traverser le nœud et/ou liaison vers l'aval dont on se protège de la défaillance. Noter que si le PLR est l'avant dernier bond, la protection de nœud n'est pas possible, et seule la liaison aval peut être évitée. Le chemin de sauvegarde peut être calculé comme étant le SRLG disjoint du nœud et/ou liaison vers l'aval qu'on évite.

- Le chemin de sauvegarde doit satisfaire aux exigences de ressource du LSP protégé. Cela inclut les filtres d'attribut de liaison, la bande passante, et les limites de bonds déterminées à partir des objets FAST_REROUTE et SESSION_ATTRIBUTE.

Si ce calcul réussit, le PLR devrait tenter d'établir un chemin de sauvegarde. Le PLR peut programmer un nouveau calcul ultérieurement pour découvrir de meilleurs chemins qui pourraient être apparus. Si pour une raison quelconque, le PLR est incapable d'établir un chemin de sauvegarde, il doit programmer un nouvel essai ultérieurement.

6.3 Signalisation des sauvegardes pour la protection biunivoque

Une fois qu'un PLR a décidé de protéger un LSP localement avec une sauvegarde biunivoque et a identifié le chemin désiré, il signale le détour.

Les transformations suivantes doivent être effectuées à réception du message Path du LSP protégé pour créer le message Path du LSP de détour.

- Si la méthode spécifique de gabarit d'envoyeur doit être utilisée, le PLR DOIT alors changer le champ "Adresse IPv4 (ou IPv6) d'envoyeur du tunnel" du SENDER_TEMPLATE en une adresse appartenant au PLR qui ne soit pas la même que celle utilisée pour le LSP protégé. De plus, l'objet DETOUR PEUT être ajouté au message Path.

- Si la méthode spécifique du chemin doit être utilisée, le PLR DOIT alors ajouter un objet DETOUR au message Path.

- Les fanions de SESSION_ATTRIBUTE "Protection locale désirée", "Protection de bande passante désirée", et "Protection de nœud désirée" DOIVENT être à zéro. Le fanion "Enregistrement d'étiquette désiré" PEUT être modifié. Si le message Path contenait un objet FAST_REROUTE et si le ERO n'est pas complètement strict, les champs "Inclusions", "Exclusions", et "Inclus tout" de l'objet FAST_REROUTE DEVRAIENT être copiés dans les champs correspondants de l'objet SESSION_ATTRIBUTE.

- Si le message Path du LSP protégé contenait un objet FAST_REROUTE, cet objet DOIT être retiré du message Path du LSP de détour.

- Le PLR DOIT générer un objet EXPLICIT_ROUTE vers la sortie. D'abord, le PLR doit supprimer tous les sous objets précédant la première adresse qui appartient au point de fusion (MP). Ensuite, le PLR DEVRAIT ajouter les sous objets correspondants au chemin de sauvegarde désiré entre le PLR et le MP.

- L'objet SENDER_TSPEC DEVRAIT contenir les informations de bande passante provenant de l'objet FAST_REROUTE reçu, si il est inclus dans le message Path du LSP protégé.

- L'objet RSVP_HOP contenant une adresse IP du PLR.

- Les LSP de détour DOIVENT utiliser le même style de réservation que le LSP protégé. Cela doit être correctement

reflété dans l'objet SESSION_ATTRIBUTE.

Les LSP de détour fonctionnent comme des LSP réguliers. Une fois qu'un chemin de détour a été bien calculé et que le LSP de détour est établi, le PLR n'a pas besoin de calculer de nouveau des chemins de détour, sauf (1) si le contenu de FAST_REROUTE a changé, ou (2) si l'interface et/ou le routeur de prochain bond vers l'aval pour un LSP protégé a changé. Le PLR peut recalculer les chemins de détour à tout moment.

6.3.1 "Make-before-break" avec des LSP de détour

Si la méthode spécifique de gabarit d'envoyeur est utilisée, il est possible de faire "make-before-break" avec les LSP de détour. Cela se fait en utilisant deux adresses IP différentes appartenant au PLR (qui n'ont pas été utilisées dans le SENDER_TEMPLATE du LSP protégé). Si le LSP de détour actuel utilise la première adresse IP dans son SENDER_TEMPLATE, le nouveau LSP de détour devrait alors être signalé en utilisant la seconde adresse IP de son SENDER_TEMPLATE. Une fois que le nouveau LSP de détour a été créé, le LSP de détour actuel peut être supprimé. En alternant l'utilisation de ces adresses IP, les LSP courant et nouveau vont avoir des SENDER_TEMPLATE différents, et donc, un état différent dans les LSR vers l'aval.

Ce mécanisme de "make-before-break", qui change l'adresse IP de PLR dans l'objet DETOUR, n'est pas faisable avec la méthode spécifique de chemin, car les messages Path pour les LSP de détour nouveau et actuel peuvent être fusionnés si ils sont partagés sur un prochain bond commun.

6.3.2 Traitement du message

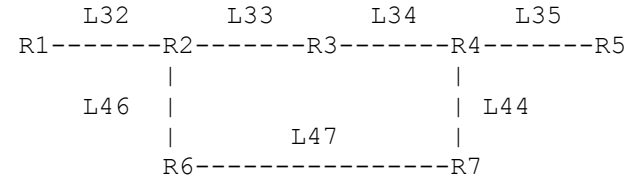
Les LSR doivent traiter les LSP de détour indépendamment des LSP protégés pour éviter de déclancher la procédure de détection de boucle de LSP décrite dans la [RFC3209].

Le PLR NE DOIT PAS mélanger les messages pour les LSP protégé et de détour. Lorsque un PLR reçoit des messages Resv, ResvTear, et PathErr de la destination de détour en aval, les messages NE DOIVENT PAS être transmis en amont. De même, quand un PLR reçoit des messages ResvErr et ResvConf d'un LSP protégé, il NE DOIT PAS les propager sur le LSP de détour associé.

Une demande de suppression de session est normalement générée par l'envoyeur via des messages PathTear. Lorsque un nœud PLR reçoit une message PathTear de l'amont, il DOIT supprimer à la fois le LSP protégé et le LSP de détour. Les messages PathTear DOIVENT se propager aux deux LSP protégé et de détour. Lors de conditions d'erreur, les LSR peuvent envoyer des messages ResvTear pour régler les problèmes sur le chemin défaillant. Quand un nœud PLR reçoit des messages ResvTear de l'aval pour un LSP protégé, tant qu'un détour est actif, les messages ResvTear NE DOIVENT PAS être envoyés plus loin en amont. Les messages PathErr devraient être traités de même.

6.3.3 Réacheminement local du trafic sur un LSP de détour

Quand le PLR détecte une défaillance sur le LSP protégé, il DOIT rapidement passer les paquets au LSP de sauvegarde du LSP protégé au lieu du segment de sortie normal du LSP protégé. Le but de cette méthode est d'effectuer la redirection dans un 10ème de milliseconde.



LSP protégé : [R1->R2->R3->R4->R5]
LSP de détour : [R2->R6->R7->R4]

Exemple 3 : Redirection sur le détour

Dans l'exemple 3, si la liaison [R2->R3] a une défaillance, R2 va faire ce qui suit. Tout le trafic reçu sur la liaison [R1->R2] avec l'étiquette L32 va être envoyé sur la liaison [R2->R6] avec l'étiquette L46 (sur le LSP de détour) au lieu de sur la liaison [R3->R4] avec l'étiquette L34 (sur le LSP protégé). Le point de fusion R4 va reconnaître que les paquets reçus sur la liaison [R7->R4] avec l'étiquette L44 devraient être envoyés sur la liaison [R4->R5] avec l'étiquette L35 et qu'ils devraient être fusionnés avec le LSP protégé.

6.4 Signalisation de la protection de facilité

Un PLR peut utiliser un ou plusieurs tunnels de contournement pour protéger de la défaillance d'une liaison et/ou d'un nœud. Ces tunnels de contournement peuvent être établis à l'avance ou peuvent être créés de façon dynamique lorsque de nouveaux LSP protégés sont signalés.

6.4.1 Découverte des étiquettes vers l'aval

Pour prendre en charge la sauvegarde de facilité, le PLR doit déterminer une étiquette qui va indiquer au MP que les paquets reçus avec cette étiquette devraient être passés sur le LSP protégé. Ce peut être fait sans signaler explicitement le chemin de sauvegarde si le MP utilise un espace d'étiquettes global pour ce LSR.

Comme décrit à la Section 6, le LSR d'extrémité de tête DOIT établir le fanion "Enregistrement d'étiquette demandé" dans l'objet SESSION_ATTRIBUTE pour les LSP qui exigent une protection locale. Cela va causer (comme spécifié dans la [RFC3209]) l'enregistrement par tous les LSR de leurs étiquettes INBOUND et ils vont noter via un fanion si l'étiquette est globale pour le LSR. Donc, quand un LSP protégé est signalé pour la première fois sur un PLR, le PLR peut examiner le RRO dans le message Resv et apprendre les étiquettes entrantes qui sont utilisées par les nœuds en aval pour ce LSP

Quand les MP utilisent les espaces d'étiquettes par interface, le PLR doit envoyer des messages Path (pour chaque LSP protégé en utilisant un tunnel de contournement) via ce tunnel de contournement avant la défaillance afin de découvrir l'étiquette de MP appropriée. Les procédures de signalisation pour cela sont au paragraphe 6.4.3.

6.4.2 Procédures pour le PLR avant réparation locale

Un PLR qui décide d'utiliser la sauvegarde de facilité pour protéger un certain LSP devrait choisir un tunnel de contournement à utiliser, en prenant en compte si la protection de nœud doit être fournie, quelle bande passante était demandée, si une garantie de bande passante est désirée, et quels filtres d'attribut de liaison étaient spécifiés dans l'objet FAST_REROUTE. Le choix d'un tunnel de contournement pour un LSP protégé est effectué par le PLR quand le LSP est établi.

6.4.3 Procédures pour le PLR durant la réparation locale

Lorsque le PLR détecte une condition de défaillance de liaison ou/et de nœud, il doit réacheminer le trafic de données sur le tunnel de contournement et commencer l'envoi du trafic de contrôle pour le LSP protégé sur le tunnel de contournement.

Le tunnel de sauvegarde est identifié en utilisant la méthode spécifique du gabarit d'envoyeur. Les procédures à suivre sont similaires à celles décrites au paragraphe 6.3.

- L'objet SESSION est inchangé.

- L'objet SESSION_ATTRIBUTE est inchangé sauf comme suit : les fanions "Protection locale désirée", "Protection de bande passante désirée", et "Protection de nœud désirée" DEVRAIENT être à zéro. Le fanion "Enregistrement d'étiquette désiré" PEUT être modifié.

- Le champ Adresse IPv4 (ou IPv6) d'envoyeur de tunnel de l'objet SENDER_TEMPLATE est réglé à une adresse appartenant au PLR.

- L'objet RSVP_HOP DOIT contenir une adresse IP de source appartenant au PLR. Par conséquent, le MP va renvoyer des messages au PLR avec cette adresse IP comme destination.

- Le PLR DOIT générer un objet EXPLICIT_ROUTE vers la sortie. Le détail du traitement de ERO est décrit plus loin.

- L'objet RECORD_ROUTE peut devoir être mis à jour comme décrit au paragraphe 6.5.

Le PLR envoie des messages Path, PathTear, et ResvConf via le tunnel de sauvegarde. Le MP envoie des messages Resv, ResvTear, et PathErr en les envoyant directement à l'adresse contenue dans l'objet RSVP_HOP, comme spécifié dans la [RFC2205].

Si il est nécessaire de signaler la sauvegarde avant la défaillance pour déterminer l'étiquette de MP à utiliser, le même message Path est alors envoyé. Dans ce cas, le PLR DEVRAIT continuer d'envoyer des messages Path pour le LSP protégé le long du chemin normal. Les messages PathTear devraient être dupliqués, l'un d'eux étant sur le chemin normal et l'autre envoyé à travers le tunnel de contournement. Le MP devrait dupliquer les messages Resv et ResvTear et les envoyer au

PLR et au LSR indiqués par l'objet RSVP_HOP du LSP protégé.

6.4.4 Traitement de l'ERO du tunnel de sauvegarde

Les procédures pour le traitement d'ERO sont décrites dans la [RFC3209]. Ce paragraphe décrit les procédures supplémentaires de mise à jour d'ERO pour les messages Path qui sont envoyés sur les tunnels de contournement. Si les règles normales de traitement d'ERO étaient suivies, le point de fusion examinerait le premier sous objet et le rejetterait probablement (Mauvais sous objet initial). C'est parce que le ERO non modifié pourrait contenir l'adresse IP d'un nœud qui a été sauté (dans le cas d'un tunnel de contournement NNHOP) ou d'une interface qui est actuellement fermée (dans le cas d'un tunnel de sauvegarde NHOP). Pour cette raison, le PLR invoque les procédures d'ERO suivantes avant d'envoyer un message Path via un tunnel de contournement.

Les sous objets qui appartiennent à des nœuds abstraits qui précèdent le point de fusion sont supprimés, ainsi que le premier sous objet appartenant au MP. Un sous objet identifiant la destination du tunnel de sauvegarde est alors ajouté.

Plus spécifiquement, le PLR DOIT :
- supprimer tous les sous objets en traitant la première adresse qui appartient au MP, et
- remplacer cette première adresse de MP par une adresse IP du MP. (Noter que ce peut être la même adresse qui vient d'être supprimée.)

6.5 Procédures du PLR durant la réparation locale

En plus de la signalisation spécifique de la méthode et du traitement de paquet, il y a une signalisation commune qui devrait être suivie.

Durant le réacheminement rapide, pour chaque LSP protégé contenant un RRO, le PLR obtient le RRO du RESV mémorisé du LSP protégé. Le PLR DOIT mettre à jour le sous objet IPv4 ou IPv6 qu'il a inséré dans le RRO en établissant les fanions "Protection locale utilisée" et "Protection locale disponible".

6.5.1 Notification de réparation locale

Dans de nombreuses situations, le chemin utilisé durant la réparation locale va être sous optimal. L'objet de la réparation locale est de continuer l'écoulement du trafic de haute priorité et sensible à la perte en attendant qu'un réacheminement plus optimal du tunnel puisse être effectué par l'extrémité de tête du tunnel. Donc, l'extrémité de tête doit être informée des défaillances afin qu'elle puisse re signaler un LSP optimal.

Pour faire cette notification, le PLR DEVRAIT envoyer un message "Path Error" avec le code d'erreur de "Notify" (code d'erreur = 25) et un champ de valeur d'erreur de ss00 cccc cccc cccc, où ss=00 et le sous code = 3 ("Tunnel réparé en local") (voir la [RFC3209]).

De plus, une extrémité de tête peut détecter qu'un LSP doit être déplacé à un chemin plus optimal en notifiant les défaillances rapportées via l'IGP. Noter que dans le cas d'un LSP TE inter zones (zones d'étendue de LSP TE) le LSR d'extrémité de tête va devoir s'appuyer exclusivement sur les messages Path Error pour être informé des défaillances dans une autre zone.

6.5.2 Comportement réversible

Lors d'une défaillance, un LSP TE protégé est réparé localement par le PLR. Il y a deux stratégies de base pour restaurer le LSP TE en chemin fonctionnel.

- Mode réversible global : le LSR d'extrémité de tête de chaque tunnel est responsable de la réoptimisation des LSP TE qui utilisaient la ressource défaillante. Il y a plusieurs déclencheurs potentiels de réoptimisation : les messages d'erreur RSVP, l'inspection des LSA OSPF ou des LSP ISIS, et les temporisateurs. Noter que ce processus de réoptimisation peut fonctionner aussitôt que la défaillance est détectée. Il n'est pas lié à la restauration de la ressource défaillante.

- Mode réversible local : à la détection de la restauration de la ressource, le PLR signale à nouveau chacun des LSP TE qui étaient acheminés sur la ressource restaurée. Chaque LSP TE resignalé avec succès le long de la ressource restaurée est reconnecté.

Il y a plusieurs circonstances dans lesquelles un mode réversible local peut n'être pas désirable. Dans le cas de flottement d'une ressource (type de défaillance courant) cela peut générer plusieurs perturbations du trafic. Donc, dans le mode

réversible local, le PLR devrait mettre en œuvre un moyen pour calmer le processus de resignalisation afin de limiter les perturbations potentielles dues au flottement.

Dans le mode réversible local, tout LSP TE va être recommuté, sans aucune distinction, tandis que dans le mode réversible global, la décision de réutiliser la ressource restaurée est prise par le LSR d'extrémité de tête sur la base des attributs du LSP TE. Quand l'extrémité de tête apprend la défaillance, elle peut réoptimiser le tunnel de LSP protégé sur un chemin différent et plus optimal, car elle a une vue plus complète des ressources et des contraintes du LSP TE. Cela signifie que le vieux LSP auquel on est revenu peut n'être plus optimal. Noter que dans le cas de LSP inter zones, où le calcul du chemin du LSP TE peut être fait sur un élément de calcul de chemin, le processus de réoptimisation peut encore être déclenché sur le LSP d'extrémité de tête. Le mode réversible local est facultatif.

Cependant, il y a des circonstances dans lesquelles l'extrémité de tête n'a pas la capacité de réacheminer le LSP TE (par exemple, si le LSP protégé est coincé, ou cela peut être désirable si les chemins sont déterminés en utilisant des outils d'optimisation hors ligne) ou si l'extrémité de tête n'a pas les informations de topologie TE complètes (selon le scénario de calcul de chemin). Dans ces cas, le mode réversible local peut être une option intéressante.

Le mode réversible global DEVRAIT toujours être utilisé. Noter qu'une "défaillance" de liaison ou de nœud peut être due à ce que la facilité est mise hors service de façon permanente. Le mode réversible local est facultatif. Lorsque il est utilisé en combinaison, le mode global peut ne s'appuyer que sur les temporisateurs pour faire la réoptimisation. Quand le mode réversible local n'est pas utilisé, les LSR d'extrémité de tête DEVRAIENT réagir aux messages d'erreur RSVP et/ou aux indications IGP afin de faire une réponse en temps voulu.

Interopérabilité : si un PLR est configuré avec le mode réversible local mais que le MP ne l'est pas, toute tentative du PLR de resignaler le LSP TE sur la ressource restaurée va échouer, car le MP ne va pas envoyer de message Resv. Le PLR va quand même rafraîchir le LSP TE LSP sur le tunnel de sauvegarde. Le LSP TE ne va pas revenir à la ressource restaurée ; à la place, il va continuer d'utiliser la sauvegarde jusqu'à ce qu'il soit réoptimisé.

7. Comportement du nœud de fusion

Un LSR est un point de fusion si il reçoit le message Path pour un LSP protégé et un ou plusieurs messages pour un LSP de sauvegarde qui est fusionné dans ce LSP protégé. Dans la méthode de sauvegarde biunivoque, le LSR sait qu'il est un nœud de fusion avant la défaillance. Dans la méthode de sauvegarde de facilité, le LSR peut ne pas savoir qu'il est un point de fusion jusqu'à ce qu'une défaillance se produise et qu'il reçoive un message Path du LSP de sauvegarde. Donc, un LSR qui est sur le chemin d'un LSP protégé DEVRAIT toujours supposer qu'il est un point de fusion.

Quand un MP reçoit un message Path d'un LSP de sauvegarde à travers un tunnel de contournement, le Send_TTL dans l'en-tête commun peut ne pas correspondre au TTL du paquet IP au sein duquel le message Path était transporté. Voici le comportement prévu.

7.1 Traitement des messages Path de sauvegarde avant défaillance

Il y a deux circonstances dans lesquelles un point de fusion va recevoir des messages Path pour un chemin de sauvegarde avant une défaillance. Dans le premier cas, si un PLR fournit une protection locale via la méthode de sauvegarde biunivoque, le détour sera signalé et doit être correctement traité par le MP.

Dans ce cas, le LSP de sauvegarde peut être signalé via la méthode spécifique de gabarit d'envoyeur ou via la méthode spécifique du chemin.

Dans le second cas, si le point de fusion ne fournit pas d'étiquettes globales au MP et les enregistre dans un sous objet "Label" du RRO, ou si le PLR n'utilise pas ces informations enregistrées, le PLR peut signaler le chemin de sauvegarde comme décrit au paragraphe 6.4.1. Cela va déterminer l'étiquette à utiliser si le PLR fournit la protection selon la méthode de la sauvegarde de facilité. Dans ce cas, le LSP de sauvegarde est signalé via la méthode spécifique du gabarit d'envoyeur.

La réception d'un message Path du LSP de sauvegarde n'indique pas qu'une défaillance s'est produite ou que le LSP protégé entrant ne sera plus utilisé.

7.1.1 Fusion des chemins de sauvegarde avec la méthode spécifique de gabarit d'envoyeur

Un LSR peut recevoir plusieurs messages Path pour un ou plusieurs LSP de sauvegarde et, éventuellement pour le LSP protégé. Chacun de ces messages Path va avoir un SENDER_TEMPLATE différent. Le LSP protégé peut être reconnu

parce qu'il va inclure l'objet FAST_REROUTE ou avoir le fanion "Protection locale désirée" établi dans l'objet SESSION_ATTRIBUTE, ou les deux.

Si l'interface sortante et le LSR de prochain bond sont les mêmes, les messages Path sont alors éligibles à la fusion. Comme dans la spécification de la [RFC3209] pour la fusion des messages RESV, seuls les messages Path dont le ERO de ce LSR à la sortie est le même peuvent être fusionnés. Si la fusion se produit et si un des messages Path fusionnés était pour le LSP protégé, le message Path final envoyé DOIT être celui du LSP protégé. Cela fusionne les LSP de sauvegarde dans le LSP protégé à ce LSR. Une fois le message Path final identifié, le MP DOIT commencer à le rafraîchir en aval périodiquement.

Si la fusion se produit et si tous les messages Path étaient pour les LSP de sauvegarde, l'objet DETOUR, si il en est, devrait alors être altéré comme spécifié au paragraphe 8.1

7.1.2 Fusion de Detour avec la méthode spécifique du chemin

Un LSR (un MP) peut recevoir plusieurs messages Path de différentes interfaces avec des objets SESSION et SENDER_TEMPLATE identiques. Dans ce cas, la fusion de l'état Path est EXIGÉE. La règle de fusion est la suivante :

Si tous les messages Path n'ont ni un objet FAST_REROUTE ni un objet DETOUR, ou si le MP est la sortie du LSP, aucune fusion n'est requise. Les messages sont traités conformément à la [RFC3209].

Autrement, le MP DOIT enregistrer l'état de chemin et l'interface entrante. Si les messages Path ne partagent pas d'interface sortante ni un LSR de prochain bond, le MP DOIT les considérer comme des LSP indépendants et NE DOIT PAS les fusionner.

Pour tous les messages Path qui partagent la même interface sortante et le même LSR de prochain bond, le MP utilise la procédure suivante pour créer un message Path à transmettre vers l'aval.

1. Si un ou plusieurs des messages Path sont pour le LSP protégé (un LSP protégé est généré à partir de ce nœud, ou avec l'objet FAST_REROUTE, ou sans l'objet DETOUR) l'un d'eux doit devenir le message Path choisi. Il pourrait y en avoir plus d'un ; dans ce cas, celui à choisir est une décision locale. Quitter.

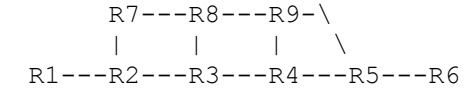
2. De l'ensemble restant de messages Path de détour, éliminer ceux qui traversent des nœuds que d'autres veulent éviter.

3. Si il en reste encore plusieurs, celui à transmettre est une décision locale. Si il n'en reste aucun, le MP PEUT alors essayer de trouver un nouveau chemin qui évite tous les nœuds que les chemins de détour qui fusionnent veulent éviter ; il va transmettre un message Path avec cet ERO.

Une fois que le message Path final a été identifié, le MP DOIT commencer à le rafraîchir périodiquement vers l'aval. D'autres LSP sont pris en considération pour la fusion à ce nœud. Pour les réservations de bande passante sur la liaison sortante, toute fusion devrait être considéré s'être produite avant que la bande passante soit réservée. Donc, même si le style de filtre fixe est spécifié, plusieurs détours et/ou leur LSP protégé (qui sont à fusionner du fait du partage d'une interface sortante et du LSR de prochain bond) vont réserver seulement la bande passante du message Path final sur cette interface sortante.

Si aucun message Path fusionné ne peut être construit, le MP DEVRAIT envoyer un message PathErr en réponse au message Path de détour le plus récemment reçu. Si un chemin protégé est choisi pour être transmis mais si il traverse des nœuds que certains détours veulent éviter, des messages PathErr DEVRAIENT être envoyés en réponse à ces messages Path de détour qui ne peuvent pas fusionner.

7.1.2.1 Exemple de fusion de messages Path



LSP protégé : [R1->R2->R3->R4->R5->R6]
Détour de R2 : [R2->R7->R8->R9->R4->R5->R6]
Détour de R3 : [R3->R8->R9->R5->R6]

Exemple 4 : Fusion de messages Path

Dans l'exemple 4, R8 va recevoir des messages Path qui ont les mêmes objets SESSION et SENDER_TEMPLATE des

détours pour R2 et R3. Durant la fusion à R8, parce que le détour R3 a un chemin d'ERO plus court (c'est-à-dire, l'ERO est [R9->R5->R6], et la longueur du chemin est 3) R8 va le choisir comme LSP final et va seulement propager ses messages Path en aval. À réception d'un message Resv (ou ResvTear) R8 doit relayer les messages vers R2 et R3.

R5 doit fusionner aussi, et il va choisir le LSP principal, car il a l'objet FAST_REROUTE. Donc, le LSP de détour se termine à R5.

7.1.3 Traitement de message pour la fusion de Detour

Lorsque un LSR reçoit un ResvTear pour un LSP, il doit déterminer si il a un LSP associé de remplacement. Par exemple, si le ResvTear a été reçu pour un LSP protégé mais si un LSP de sauvegarde associé n'a pas reçu de ResvTear, le LSR a un LSP associé de remplacement. Si le LSR n'a pas de LSP associé de remplacement, le MP DOIT alors propager le ResvTear à l'entrée du LSP, et pour chaque LSP de sauvegarde fusionné dans ce LSP à ce LSR, le ResvTear DEVRAIT aussi être propagé le long du LSP de sauvegarde.

Le MP peut recevoir des messages PathTear pour certains des LSP fusionnés. Les messages PathTear NE DEVRAIENT PAS être propagés en aval jusqu'à ce que le MP ait reçu les messages PathTear pour chacun des LSP fusionnés. Cependant, le fait que un ou plusieurs des LSP fusionnés aient été supprimés devrait être reflété dans le message vers l'aval, comme en changeant l'objet DETOUR, si il y en a un.

7.2 Traitement des défaillances

Lorsque un LSR en aval détecte une défaillance de liaison locale, pour tous les LSP protégés acheminés sur la liaison défaillante, les états Path et Resv NE DOIVENT PAS être supprimés, et les messages PathTear et ResvErr NE DOIVENT PAS être envoyés immédiatement. Si ce n'est pas le cas, la méthode de sauvegarde de facilité ne va alors pas fonctionner. De plus, un LSR aval DEVRAIT remettre à zéro les temporisateurs de rafraîchissement pour ces LSP comme si ils venaient juste d'être rafraîchis. C'est pour donner le temps au PLR de commencer à rafraîchir l'état via le tunnel de contournement. L'état DOIT être supprimé si il n'a pas été rafraîchi avant l'arrivée à expiration du temporisateur de rafraîchissement. Cela permet à la méthode de sauvegarde de facilité de fonctionner sans exiger qu'elle signale les chemins de sauvegarde à travers le tunnel de contournement avant une défaillance.

Après qu'une défaillance s'est produite, le MP doit quand même envoyer des messages Resv pour les LSP de sauvegarde associés aux LSP protégés qui sont défaillants. Si le LSP de sauvegarde a été envoyé à travers un tunnel de contournement, l'objet PHOP dans son message Path aura alors l'adresse IP du PLR associé. Cela va assurer que l'état Resv est rafraîchi.

Une fois que la liaison locale a récupéré, le MP peut ou non accepter les messages Path pour les LSP protégés existants qui étaient défaillants sur leur sauvegarde.

8. Comportement de tous les LSR

Les objets et méthodes définis dans le présent document exigent un comportement de la part de tous les LSR dans le réseau à ingénierie du trafic, même si un LSR n'est pas sur le chemin d'un LSP protégé.

D'abord, si un objet DETOUR est inclus dans le message Path d'un LSP de sauvegarde pour la méthode spécifique de gabarit d'envoyeur, les LSR dans le réseau à ingénierie du trafic devraient prendre en charge l'objet DETOUR.

Ensuite, si la méthode spécifique du chemin doit être prise en charge pour la méthode de sauvegarde biunivoque, il est nécessaire que les LSR dans le réseau à ingénierie du trafic soient capables de fusionner les détours comme spécifié au paragraphe 8.1.

Il est possible d'éviter des LSR spécifiques qui ne prennent pas en charge ce comportement en allouant un attribut de liaison à toutes les liaisons de ces LSP et de demander ensuite que les chemins de sauvegarde excluent cet attribut de liaison.

8.1 Fusion de Detour avec la méthode spécifique du chemin

Si plusieurs messages Path sont reçus pour des détours différents avec le même SESSION, SENDER_TEMPLATE, interface sortante, et LSR de prochain bond, le LSR doit alors fonctionner comme un point de fusion de détour et fusionner les messages Path de détour. Cette fusion devrait se produire comme spécifié au paragraphe 7.1.2 et montré à l'exemple 4.

De plus, il est nécessaire de mettre à jour l'objet DETOUR pour refléter la fusion qui vient d'avoir lieu. C'est fait en utilisant l'algorithme suivant pour formater l'objet DETOUR sortant pour le LSP final :
- Combiner toutes les paires (PLR_ID, Avoid_Node_ID) de tous les objets DETOUR de tous les LSP fusionnés dans un nouvel objet. L'ordre n'est pas significatif.

9. Considérations sur la sécurité

Le présent document n'introduit aucun nouveau problème de sécurité. Les considérations sur la sécurité relevant du protocole RSVP original [RFC2205] restent pertinentes.

Noter que la méthode de sauvegarde de facilité exige qu'un PLR et son point de fusion choisi fassent confiance aux messages RSVP reçus l'un de l'autre.

10. Considérations relatives à l'IANA

L'IANA [RFC2434] a alloué les numéros de classe RSVP suivants aux objets définis dans ce document.

10.1 Objet DETOUR

L'IANA a alloué :

63 DETOUR

Types de classe ou C-Types :
7 IPv4
8 IPv6

De futurs C-Types seront alloués en utilisant les lignes directrices suivantes : les C-Types de 0 à 127 sont alloués par action de normalisation. Les C-Types de 128 à 191 sont alloués par revue d'expert. Les C-Types de 192 à 255 sont réservés pour utilisation privée des fabricants. Pour les C-Types dans la gamme de 192 à 255, les quatre premiers octets de l'objet DETOUR après le C-Type doivent être le code d'entreprise privé de gestion de réseau SMI du fabricant (voir [ENT]) dans l'ordre des octets du réseau.

10.2 Objet FAST_REROUTE

L'IANA a alloué :

205 FAST_REROUTE

Types de classe ou C-Types :
1 FAST_REROUTE Type 1
7 RESERVED

Dans l'objet FAST_REROUTE, le C-Type 7 est réservé car il est encore utilisé par des mises en œuvre pré standard. De futurs C-Types seront alloués en utilisant les lignes directrices suivantes : les C-Types de 0 à 127 sont alloués par action de normalisation. Les C-Types de 128 à 191 sont alloués par revue d'expert. Les C-Types de 192 à 255 sont réservés pour utilisation privée des fabricants. Pour les C-Types dans la gamme de 192 à 255, les quatre premiers octets de l'objet FAST_REROUTE après le C-Type doivent être le code d'entreprise privé de gestion de réseau SMI du fabricant (voir [ENT]) dans l'ordre des octets du réseau.

11. Contributeurs

Ce document a été rédigé par George Swallow, Ping Pan, Alia Atlas, Jean Philippe Vasseur, Markus Jork, Der-Hwa Gan, et Dave Cooper.

Jean Philippe Vasseur
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA
tél. : +1 978 497 6238
mél : jpv@cisco.com

Markus Jork
Quarry Technologies
8 New England Executive Park
Burlington, MA 01803
USA
téléphone : +1 781 359 5071
mél : mjork@quarrytech.com

Der-Hwa Gan
Juniper Networks
1194 N.Mathilda Ave
Sunnyvale, CA 94089
USA
tél. : +1 408 745 2074
mél : dhg@juniper.net

Dave Cooper
Global Crossing
960 Hamlin Court
Sunnyvale, CA 94089
USA
tél. : +1 916 415 0437
mél: dcooper@gblx.net

12. Remerciements

Nous tenons à remercier de leurs apports et commentaires utiles Rob Goguen, Tony Li, Yakov Rekhter et Curtis Villamizar. En particulier, nons remercions ceux qui ont été impliqués dans la vérification de l'interopérabilité et le suivi des champs, et ont fourni de précieuses idées et suggestions. Ce sont Rob Goguen, Carol Iturralde, Brook Bailey, Safaa Hasan, Richard Southern, et Bijan Jabbari.

13. Références normatives

[ENT] IANA, Numéros d'entreprises privées, http://www.iana.org/assignments/enterprise-numbers

[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.)*

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[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)

Adresse des éditeurs

George Swallow
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA
téléphone : +1 978 244 8143
mél : swallow@cisco.com

Ping Pan
Hammerhead Systems
640 Clyde Court
Mountain View, CA 94043
USA
mél : ppan@hammerheadsystems.com

Alia Atlas
Avici Systems
101 Billerica Avenue
N. Billerica, MA 01862
USA
téléphone : +1 978 964 2070
mél : aatlas@avici.com

Déclaration complète de droits de reproduction

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