Groupe de travail Réseau
Request for Comments : 4872
RFC mise à jour : 3471
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J.P. Lang, éd., Sonos
Y. Rekhter, éd., Juniper
D. Papadimitriou, éd., Alcatel
mai 2007

Extensions à RSVP-TE pour la prise en charge de la récupération de commutation d'étiquettes multi protocoles généralisée (GMPLS) de bout en bout

Statut du présent 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 "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.
(La présente traduction incorpore les errata 928, 929, 930, 931, 932 et 933.)

Notice de Copyright

Résumé

Le présent document décrit des procédures et extensions spécifiques du protocole pour la signalisation du protocole de réservation de ressource avec ingénierie du trafic (RSVP-TE, *Resource ReSerVation Protocol - Traffic Engineering*) dans la commutation d'étiquettes multi protocoles généralisée (GMPLS, *Generalized Multi-Protocol Label Switching*) pour la prise en charge de la récupération de bout en bout de chemin de commutation d'étiquettes (LSP, *Label Switched Path*) qui note la protection et la restauration. Une description générique fonctionnelle de la récupération GMPLS peut être trouvée dans un document d'accompagnement, la RFC 4426.

Table des matières

1. Introduction

La commutation d'étiquettes multi protocoles généralisée (GMPLS) étend MPLS pour inclure la prise en charge des interfaces à capacité de commutateur de couche 2 (L2SC, *Layer-2 Switch Capable*) de multiplexage à division dans le temps (TDM, *Time-Division Multiplex*) à capacité de commutation lambda (LSC, *Lambda Switch Capable*) et à capacité de commutation sur fibre (FSC, *Fiber Switch Capable*). La récupération GMPLS utilise des mécanismes de plan de contrôle (c'est-à-dire, des mécanismes de signalisation, d'acheminement, et de gestion de liaison) pour prendre en charge la récupération de fautes du plan des données. Noter que les mécanismes analogues (de plan des données) de détection de faute sont obligés d'être présents en soutien des mécanismes du plan de contrôle. Dans le présent document, le terme de "récupération" est utilisé de façon générique pour noter à la fois la protection et la restauration ; les termes spécifiques de "protection" et de "restauration" sont seulement utilisés quand la différentiation est requise. La distinction subtile entre protection et restauration est faite sur la base de l'allocation de ressource faite durant la phase de récupération (voir la [RFC4427]).

Une description fonctionnelle de la récupération GMPLS est fournie dans la [RFC4426] et devrait être considérée comme un document d'accompagnement. Le présent document décrit les procédures spécifiques du protocole pour la signalisation de GMPLS RSVP-TE (voir la [RFC3473]) pour prendre en charge la récupération de bout en bout. La récupération de bout en bout se réfère à la récupération d'un LSP entier de son extrémité de tête (point d'extrémité du nœud d'entrée) à son extrémité de queue (point d'extrémité du nœud de sortie). Avec la récupération de bout en bout, les LSP actifs sont supposés être disjoints en ressources (où une ressource est une liaison, un nœud, ou un groupe de liaisons à partage de risque (SRLG, *Shared Risk Link Group*) dans le réseau afin qu'ils ne partagent aucune probabilité de défaillance, mais ceci n'est pas obligatoire. Par rapport à un certain ensemble de ressources du réseau, une paire de LSP actifs/protecteurs

DEVRAIT être à ressources disjointes en cas d'un type de récupération dédié (voir ci-dessous). Par ailleurs, en cas de récupération partagée (voir ci-dessous) un groupe de LSP actifs DEVRAIT être mutuellement à ressources disjointes afin de permettre un LSP de protection partagé (seul et en commun) lui-même en ressources disjointes provenant de chaque LSP actif. Noter que la disjonction de ressource est une condition nécessaire (mais pas suffisante) pour assurer la récupération de LSP.

Le présent document traite quatre types de récupération de bout en bout de LSP : 1) protection 1+1 (unidirectionnelle/bidirectionnelle) 2) protection 1:N ($N \geq 1$) de LSP avec trafic supplémentaire, 3) réacheminement pré progammé de LSP sans trafic supplémenatire (incluant le maillage partagé) et 4) le plein réacheminement de LSP.

1) La plus simple notion de protection de LSP de bout en bout est une protection 1+1 unidirectionnelle. En utilisant ce type de protection, un LSP de protection est signalé sur un chemin de remplacement à ressources disjointes dédié pour protéger un LSP actif associé. Le trafic normal est simultanément envoyé sur les deux LSP et un sélecteur est utilisé au nœud de sortie pour recevoir le trafic provenant d'un des LSP. Si une défaillance se produit le long d'un des LSP, le nœud de sortie choisit le trafic provenant du LSP valide. Aucune coordination n'est requise entre les nœuds d'extrémité quand se produit une défaillance/commutation. Dans la protection 1+1 bidirectionnelle, un LSP de protection est signalé sur un chemin de remplacement dédié à ressources disjointes pour protéger le LSP actif. Le trafic normal est envoyé simultanément sur les deux LSP (dans les deux directions) et un sélecteur est utilisé aux deux nœuds d'entrée et sortie pour recevoir le trafic provenant du même LSP. Cela exige une coordination entre les nœuds d'extrémité quand ils passent au LSP de protection.

2) Dans la protection 1:N ($N \geq 1$) avec trafic supplémentaire, le LSP de protection est un LSP pleinement provisionné et à ressources disjointes parmi les N LSP actifs, qui permet de porter le trafic supplémentaire. Les N LSP actifs PEUVENT être mutuellement à ressources disjointes. La coordination entre nœuds d'extrémité est requise quand on passe d'un des LSP actifs au LSP de protection. Comme le LSP de protection est pleinement provisionné, des opérations par défaut durant la commutation de protection sont spécifiées pour un LSP de protection qui porte du trafic supplémentaire, mais ceci n'est pas obligatoire. Noter que la protection M:N sort du domaine d'application du présent document (bien que les mécanismes qu'il définit puissent être étendus pour la couvrir).

3) Le réacheminement préprogrammé de LSP (ou restauration) s'appuie sur l'établissement entre la même paire de nœuds d'extrémité d'un LSP actif et d'un LSP de protection qui est disjoint de la liaison/nœud/SRLG du LSP actif. Ici, les ressources de récupération pour le LSP de protection sont pré réservées mais une action explicite est requise pour activer (c'est-à-dire, engager l'allocation de ressources au plan des données) un LSP de protection spécifique instancié durant la phase de (pré)provisionnement. Comme le LSP de protection n'est pas "actif" (c'est-à-dire, pleinement instancié) il ne peut pas porter de trafic supplémentaire. Cela ne signifie pas que les ressources correspondantes ne peuvent pas être utilisées par d'autres LSP. Donc, ce mécanisme protège contre les défaillances des LSP actifs mais exige l'activation du LSP de protection après la survenance d'une défaillance du LSP actif. Cela exige la signalisation de la restauration le long du chemin de protection. La restauration de "maillage partagé" peut être vue comme un cas particulier de réacheminement pré-programmé de LSP qui réduit les exigences de ressource de récupération en permettant que plusieurs LSP de protection partagent une liaison commune et des ressources de nœud. Les ressources de récupération sont pré-réservées mais une action explicite est requise pour activer (c'est-à-dire, engager l'allocation de ressource au plan des données) un LSP de protection spécifique instancié durant la phase de (pré)provisionnement. Cette procédure exige la signalisation de la restauration le long du chemin de protection.

Note : dans les deux cas, la bande passante pré-réservée pour un LSP de protection (mais non activé) peut être rendue disponible pour porter du trafic supplémentaire. Les LSP pour le trafic supplémentaire (avec une priorité de garde inférieure à celle du LSP de protection) peuvent alors être établis en utilisant la bande passante pré-réservée pour le LSP de protection. Aussi, tout LSP de priorité inférieure qui utilise les ressources pré-réservées pour le ou les LSP de protection doit être préempté durant l'activation du LSP de protection.

4) Le réacheminement complet de LSP (ou restauration) passe le trafic normal à un LSP de remplacement qui n'est même pas partiellement établi jusque après la survenance de la défaillance du LSP actif. Le nouveau chemin de remplacement est choisi au nœud d'extrémité de tête du LSP, il peut réutiliser les ressources du LSP défaillant aux nœuds intermédiaires et peut inclure des nœuds et/ou liaisons intermédiaires supplémentaires.

La signalisation de retour en arrière (voir la [RFC4920]) et la récupération de segment de LSP (voir la [RFC4873]) sont plus détaillés dans les documents d'accompagnement dédiés.

2. Conventions utilisées dans ce document

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].

De plus, le lecteur est supposé être familiarisé avec la terminologie utilisée dans les [RFC3945], [RFC3471], [RFC3473] et référencées aussi dans les [RFC4427] et [RFC4426].

3. Relations avec le réacheminement rapide (FRR)

Il n'y a pas d'impact sur le réacheminement rapide (FRR, *Fast ReRoute*) RSVP-TE [RFC4090] introduit par la récupération GMPLS de bout en bout, c'est-à-dire, il est possible d'utiliser l'une ou l'autre méthode définie dans le FRR avec la récupération GMPLS de bout en bout.

Les objets utilisés et/ou nouvellement introduits par la récupération de bout en bout vont être ignorés par les mises en œuvre conformes à la [RFC4090], et le FRR peut opérer sur une base par LSP comme défini dans la [RFC4090].

4. Définitions

4.1 Identification de LSP

Ce paragraphe revoit les termes précédemment définis dans les [RFC2205], [RFC3209], et [RFC3473]. Les LSP tunnels sont identifiés par une combinaison des objets SESSION et SENDER_TEMPLATE (voir aussi la [RFC3209]). Les champs pertinents sont les suivants :

Adresse de point d'extrémité de tunnel IPv4 (ou IPv6) : adresse IPv4 (ou IPv6) du nœud de sortie du tunnel.

Identifiant de tunnel : identifiant de 16 bits utilisé dans la SESSION qui reste constant sur la vie du tunnel.

Identifiant de tunnel étendu : identifiant de 32 bits (ou de 16 octets) utilisé dans la SESSION qui reste constant sur la vie du tunnel. Normalement réglé tout à zéro. Les nœuds d'entrée qui souhaitent restreindre la portée d'une SESSION à la paire entrée-sortie PEUVENT placer leur adresse IPv4 (ou IPv6) ici comme identifiant unique au monde.

Adresse d'envoyeur de tunnel IPv4 (ou IPv6) : adresse IPv4 (ou IPv6) pour un nœud envoyeur.

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

Les trois premiers champs sont portés dans l'objet SESSION (message Path et Resv) et constituent l'identification de base du LSP tunnel.

Les deux derniers champs sont portés dans les objets SENDER_TEMPLATE (message Path) et FILTER_SPEC (message Resv). L'identifiant de LSP est utilisé pour différencier les LSP qui appartiennent au même LSP tunnel (identifié par son identifiant de tunnel).

4.2 Attributs de récupération

Les attributs de récupération incluent tous les paramètres qui déterminent l'état d'un LSP au sein du schéma de récupération auquel il est associé. Ces attributs font partie de l'objet PROTECTION introduit à la Section 14.

4.2.1 État de LSP

Les bits suivants sont utilisés pour déterminer l'allocation de ressource et l'état du LSP au sein du groupe de LSP qui forme l'entité protégée :

- Bit S (secondaire) : permet la distinction entre LSP primaire et secondaire. Un LSP primaire est un LSP pleinement établi pour lequel l'allocation de ressource a été engagée au plan des données (c'est-à-dire, une interconnexion complète a été effectuée). Les deux LSP, actif et de protection peuvent être des LSP primaires. Un LSP secondaire est un LSP qui a été provisionné dans le plan de contrôle seulement, et pour lequel la sélection de ressources PEUT avoir été faite mais pour lequel l'allocation de ressources n'a pas été engagée au plan des données (par exemple, aucune interconnexion n'a été effectuée). Donc, un LSP secondaire n'est pas immédiatement disponible pour porter du trafic (exigeant donc que de la signalisation supplémentaire soit disponible). Un LSP secondaire peut seulement être un LSP de protection. Les ressources allouées (au plan des données) pour un LSP secondaire PEUVENT être utilisées par d'autres LSP jusqu'à ce que le LSP primaire se replie sur le LSP secondaire.

- Bit P (de protection) : permet la distinction entre les LSP actifs et de protection. Un LSP actif doit être un LSP primaire tandis qu'un LSP de protection peut être un LSP primaire ou secondaire. Quand des LSP de protection sont associés à un ou des LSP actifs, on appelle aussi ces derniers des LSP protégés.

Note : la combinaison "secondaire actif" n'est pas valide (seuls les LSP de protection peuvent être des LSP secondaires). Les LSP actifs sont toujours des LSP primaires (c'est-à-dire, pleinement établis) tandis que les LSP primaires peuvent être des LSP actifs ou de protection.

- Bit O (Opérationnel) : ce bit est établi quand un LSP de protection porte le trafic normal après le passage en protection (c'est-à-dire, il s'applique seulement en cas de LSP de protection dédié ou de LSP de protection avec trafic supplémentaire ; voir au paragraphe 4.2.2).

Dans le présent document, l'objet PROTECTION utilise comme base l'objet PROTECTION défini dans les [RFC3471] et [RFC3473] et y définit des champs additionnels. Les champs définis dans les [RFC3471] et [RFC3473] sont inchangés par le présent document.

4.2.2 Récupération de LSP

La classification suivante est utilisée pour distinguer le type LSP de protection auquel les LSP peuvent être associés aux nœuds d'extrémité (une valeur distincte est associée à chaque type de protection dans l'objet PROTECTION ; voir la Section 14) :

- Plein réacheminement de LSP : établi si un LSP primaire actif est récupérable dynamiquement en utilisant le réacheminement d'extémité de tête (non pré-programmé).

- Réacheminement pré-programmé de LSP sans trafic supplémentaire : établi si un LSP de protection est un LSP secondaire qui permet le partage des ressources pré-réservées de récupération entre une ou plusieurs paires <envoyeur-receveur>. Quand les ressources du LSP secondaire ne sont pas pré-réservées pour une seule paire <envoyeur-receveur>, ce type est appelé une récupération de "maillage partagé".

- LSP de protection avec trafic supplémentaire : établi si un LSP de protection est un LSP primaire dédié qui permet le transport de traffic supplémentaire et donc empêche tout partage des ressources de récupération entre plus d'une paire <envoyeur-receveur>. Ce type inclut la protection de 1:N LSP avec trafic supplémentaire.

- Protection de LSP dédié : établie si un LSP de protection ne permet pas le partage des ressources de récupération ni le transport de trafic supplémentaire (ce qui implique dans le présent contexte la duplication du signal sur les deux LSP, actif et de protection comme dans une protection 1+1 dédiée). Noter aussi que le présent document fait une distinction entre la protection de LSP 1+1 unidirectionnelle et bidirectionnelle dédiée.

Pour la protection du LSP, en particulier, quand le plan des données fournit des capacités automatisées de commutation de protection (voir par exemple la Recommandation UIT-T [G.841]) un bit Notification (N) est défini dans l'objet PROTECTION. Il permet la distinction entre la signalisation de commutation de protection via le plan de contrôle ou le plan des données.

Note : le présent document suppose que les valeurs de type de protection ont une signification de bout en bout et que la même valeur est envoyée sur le chemin protégé et le chemin protecteur. Dans ce contexte, le maillage partagé (par exemple) apparaît du point de vue des nœuds d'extrémité comme étant simplement un réacheminement de LSP sans service de trafic supplémentaire. Le résultat de cela est qu'un seul bit (le bit S seul) ne permet pas de déterminer si l'allocation de ressources devrait être effectuée par rapport à l'état du LSP au sein de l'entité protégée. L'introduction du bit P résout ce problème sans ambiguïté. Ces bits DOIVENT être traités bond par bond (indépendamment du

contexte du type de protection de LSP). Cela permet une mise en œuvre plus facile de l'inversion de signalisation (voir la Section 12) mais facilite aussi la livraison transparente des services protégés car un nœud intermédiaire n'est pas obligé de connaître la sémantique associée à la valeur du type de protection du LSP entrant.

4.3 Association de LSP

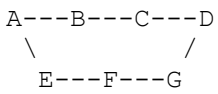
L'objet ASSOCIATION, introduit à la Section 16, est utilisé pour associer le LSP actif et le LSP protecteur.

Quand il est utilisé pour signaler le LSP actif, l'identifiant d'association de l'objet ASSOCIATION (Section 16) identifie le LSP de protection. Quand il est utilisé pour signaler le LSP de protection, ce champ identifie le LSP protégé par le LSP de protection.

5. Protection 1+1 unidirectionnelle

Une des plus simples notions de protection de LSP de bout en bout est la protection 1+1 unidirectionnelle.

Considérons la topologie de réseau suivante :



Les chemins [A,B,C,D] et [A,E,F,G,D] sont disjoints en nœud et en liaisonn, en ignorant les nœuds d'entrée/sortie A et D. Un chemin protégé 1+1 est établi de A à D sur [A,B,C,D] et [A,E,F,G,D], et le trafic est transmis simultanément sur les deux chemins composants (c'est-à-dire, des LSP).

Durant la phase de provisionnement, les deux LSP sont pleinement instanciés (et donc activés) de sorte qu'aucun partage de ressource ne peut être fait le long du LSP de protection (ni aucun trafic supplémentaire être transporté). Il est aussi RECOMMANDÉ d'établir le bit N car ainsi aucune signalisation de commutation de protection n'est supposée dans ce cas.

Quand une défaillance se produit (disons, au nœud B) et est détectée au nœud d'extrémité D, le receveur en D choisit le trafic normal provenant de l'autre LSP. De ce point de vue, la protection 1+1 unidirectionnelle peut être vue comme un mécanisme non coordonné de commutation de protection agissant indépendamment aux deux points d'extrémité. Aussi, pour le LSP en condition de défaillance, il est RECOMMANDÉ de ne pas établir le fanion État_de_chemin_retiré de l'objet ERROR_SPEC (voir la [RFC3473]) lors de la génération du message PathErr.

Note : il est nécessaire que les deux chemins soient de SRLG disjoints pour assurer la possibilité de récupération ; sinon, une seule défaillance peut impacter les deux LSP, actif et de protection.

5.1 Identifiants

Pour simplifier les opérations d'association, les deux LSP appartiennent à la même session. Donc, l'objet SESSION DOIT être le même pour les deux LSP. L'identifiant de LSP DOIT cependant être différent pour distinguer les deux LSP.

Un nouvel objet PROTECTION (voir la Section 14) est inclus dans le message Path. Cet objet porte le type de protection de LSP de bout en bout désiré – dans ce cas, "1+1 unidirectionnel". Cette valeur de type de protection de LSP est applicable aux deux LSP uni et bidirectionnels.

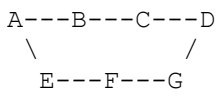
Pour permettre de distinguer le LSP actif (d'où le signal est pris) du LSP de protection, le LSP actif est signalé en réglant dans l'objet PROTECTION le bit S à 0, le bit P à 0, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP de protection. Le LSP de protection est signalé en réglant dans l'objet PROTECTION le bit S à 0, le bit P à 1, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant de LSP du LSP associé protégé.

Après l'achèvement de la commutation de protection, et après réception du message PathErr, pour garder trace du LSP d'où le signal est pris, le LSP de protection DEVRAIT être signalé avec le bit O établi. Le LSP anciennement actif PEUT être signalé avec le bit A établi dans l'objet ADMIN_STATUS (voir la [RFC3473]). Ce processus suppose que le nœud d'extrémité de queue a notifié au nœud d'extrémité de tête que le transfert de sélection du trafic a été effectué.

6. Protection 1+1 bidirectionnelle

La protection 1+1 bidirectionnelle est un schéma qui assure la protection de bout en bout pour les LSP bidirectionnels.

Considerons la topologie de réseau suivante :



Les LSP [A,B,C,D] et [A,E,F,G,D] sont disjoints en nœud et liaison, ignorant les nœuds d'entrée/sortie A et D. Un LSP bidirectionnel est établi de A à D sur chaque chemin, et le trafic est transmis simultanément sur les deux LSP. Dans ce schéma, les deux points d'extrémité doivent recevoir le trafic sur le même LSP. Noter aussi que les deux LSP sont pleinement instanciés (et donc activés) de sorte qu'aucun partage de ressources ne peut être fait le long du chemin de protection (ni aucun trafic supplémentaire être transporté).

Quand une défaillance est détectée par un des points d'extrémité du LSP ou les deux, les deux points d'extrémité doivent choisir le trafic provenant de l'autre LSP. Cette action doit être coordonnée entre le nœud A et le nœud D. De ce point de vue, la protection 1+1 bidirectionnelle peut être vue comme un mécanisme coordonné de commutation de protection entre les deux points d'extrémité.

Note : il est nécessaire que les deux chemins soient dans des SRLG disjoints pour assurer la possibilité de récupération ; sinon, une seule défaillance peut impacter les deux LSP, actif et de protection.

6.1 Identifiants

Pour simplifier les opérations d'association, les deux LSP appartiennent à la même session. Donc, l'objet SESSION DOIT être le même pour les deux LSP. L'identifiant de LSP DOIT cependant être différent pour distinguer les deux LSP.

Un nouvel objet PROTECTION (voir la Section 14) est inclus dans le message Path. Cet objet porte le type de protection de LSP désiré – dans ce cas, "1+1 bidirectionnel". Cette valeur de type de protection de LSP est seulement applicable aux LSP bidirectionnels.

Il est aussi désirable de permettre de distinguer le LSP actif (d'où le signal est pris) du LSP de protection. Ceci est réalisé pour le LSP actif en réglant dans l'objet PROTECTION le bit S à 0, le bit P à 0, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP de protection. Le LSP de protection est signalé en réglant dans l'objet PROTECTION le bit S à 0, le bit P à 1, et dans l'objet ASSOCIATION l'identifiant d'association à l'identifiant de LSP du LSP protégé associé.

6.2 Demande/réponse de commutation de bout en bout

Pour coordonner le transfert entre les points d'extrémité, un échange de demande/réponse de transfert de bout en bout est nécessaire car une défaillance affectant un des LSP résulte en ce que les deux points d'extrémité passent sur l'autre LSP (résultant en la réception du trafic provenant de l'autre LSP) dans leurs directions respectives.

La procédure est la suivante :

1. Si un nœud d'extrémité (A ou D) détecte la défaillance du LSP actif (ou une dégradation de la qualité du signal sur le LSP actif) ou reçoit un message Notify incluant son objet SESSION dans la <liste de sessions amont/aval> (voir la [RFC3473]) et si le nouveau code/sous code d'erreur "Notification d'erreur/LSP défaillant en local" dans l'objet (IF_ID)_ERROR_SPEC, il DOIT commencer à recevoir sur le LSP de protection. Noter que le <descripteur d'envoyeur> ou <descripteur de flux> est aussi présent dans le message Notify qui résout toute ambiguïté et condition de concurrence en identifiant (avec l'objet SESSION) le LSP en condition de défaillance.

Note : (IF_ID)_ERROR_SPEC indique que soit le ERROR_SPEC (C-Type 1/2) soit le ERROR_SPEC (C-Type 3/4, défini dans la [RFC3473]) peut être utilisé.

Ce nœud DOIT envoyer de façon fiable un message Notify, incluant l'objet MESSAGE_ID, à l'autre nœud d'extrémité (D ou A, respectivement) avec le nouveau code/sous code d'erreur "Notification d'erreur/défaillance de LSP" (Demande

de transfert) indiquant la défaillance du LSP actif. Ce message Notify DOIT être envoyé avec le fanion ACK_désiré établi dans l'objet MESSAGE_ID pour demander au receveur d'envoyer un accusé de réception du message (voir la [RFC2961]).

Ce message Notify (demande de transfert) PEUT indiquer l'identité de la liaison défaillante ou toute autre information pertinente en utilisant l'objet IF_ID ERROR_SPEC (voir la [RFC3473]). Dans ce cas, l'objet IF_ID ERROR_SPEC remplace l'objet ERROR_SPEC dans le message Notify ; autrement, les informations correspondantes (au plan des données) DEVRAIENT être reçues dans le message PathErr/ResvErr.

2. À réception du message Notify (demande de transfert) le nœud d'extrémité (D ou A, respectivement) DOIT commencer à recevoir du LSP de protection. Ce nœud DOIT envoyer de façon fiable un message Notify, incluant l'objet MESSAGE_ID, à l'autre nœud d'extrémité (A ou D, respectivement). Ce message Notify (demande de transfert) DOIT aussi inclure un objet MESSAGE_ID_ACK pour accuser réception du message Notify (demande de transfert). Ce message Notify (demande de transfert) PEUT indiquer l'identité de la liaison défaillante ou toute autre information pertinente en utilisant l'objet IF_ID ERROR_SPEC (voir la [RFC3473]).

Note : à réception du message Notify (demande de transfert), le nœud d'extrémité (A ou D, respectivement) DOIT envoyer un message Ack à l'autre nœud d'extrémité pour en accuser réception.

Comme les nœuds intermediaires (B, C, E, F, et G) sont supposés être capables de signalisation GMPLS RSVP-TE, chaque nœud adjacent de la défaillance PEUT générer un message Notify dirigé soit sur le LSP d'extrémité de tête (direction vers l'amont) soit sur le LSP d'extrémité de queue (direction vers l'aval) ou même sur les deux. Donc, il est attendu que ces nœuds de terminaison de LSP (qui PEUVENT aussi détecter la défaillance du LSP à partir du plan des données) fournissent soit le bon mécanisme de corrélation pour éviter la repetition de la procédure ci-dessus, soit éliminent simplement les messages Notify suivants qui correspondent à la même session. De plus, pour le LSP en condition de défaillance, il est RECOMMANDÉ de ne pas établir le fanion État_de_chemin_retiré de l'objet ERROR_SPEC (voir la [RFC3473]) lors de la génération du message PathErr.

Après l'achèvement de la commutation de protection (step 2), et après réception du message PathErr, pour garder trace du LSP d'où le signal est pris, le LSP de protection DEVRAIT être signalé avec le bit O établi. Le LSP anciennement actif PEUT être signalé avec le bit A établi dans l'objet ADMIN_STATUS (voir la [RFC3473]).

Note : quand le bit N est établi, l'échange de demande/réponse de transfert de bout en bout décrit ci-dessus donne seulement la coordination du plan de contrôle (aucune action n'est déclenchée au niveau du plan des données).

7. Protection 1:1 avec trafic supplémentaire

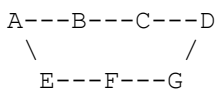
Le cas le plus courant de protection 1:N de bout en bout est d'établir, entre les mêmes points d'extrémité, un LSP actif de bout en bout (donc N = 1) et un LSP de protection dédié de bout en bout qui sont mutuellement disjoints en liaison/nœud/SRLG. Cela protège contre la ou les défaillances du LSP actif.

Le LSP de protection est utilisé pour le transfert quand le LSP actif a une défaillance. La signalisation GMPLS RSVP-TE permet le pré provisionnement des LSP de protection en indiquant dans le message Path (dans l'objet PROTECTION ; voir à la Section 14) que les LSP sont du type protecteur. Ici, les LSP, actif et de protection, sont signalés comme des LSP primaires ; tous deux sont pleinement instanciés durant la phase de provisionnement.

Bien que les ressources pour le LSP de protection soient pré-allouées, du trafic préemptable peut être porté de bout en bout en utilisant ce LSP. Donc, le LSP de protection est capable de porter du trafic supplémentaire avec l'avertisement que ce trafic sera préempté si le LSP actif est défaillant.

L'établissement du LSP actif DEVRAIT indiquer que le nœud d'extrémité de tête et d'extrémité de queue du LSP souhaite recevoir des messages Notify en utilisant l'objet NOTIFY REQUEST. Le nœud en amont de la défaillance (en amont en termes de la direction qu'un message Path traverse) DEVRAIT envoyer un message Notify au nœud d'extrémité de tête du LSP, et le nœud en aval de la défaillance DEVRAIT envoyer un message Notify au nœud d'extrémité de queue du LSP. À réception des messages Notify, les deux nœuds d'extrémité DOIVENT commuter le trafic (normal) provenant du LSP actif sur le LSP de protection pré-configuré (voir au paragraphe 7.2). De plus, une coordination est requise si du trafic supplémentaire est porté sur le LSP de protection de bout en bout. Noter que si le LSP actif et le LSP de protection sont établis entre les mêmes nœuds d'extrémité, aucune autre notification n'est requise pour indiquer que les LSP actifs ne sont plus protégés.

Considérons la topologie suivante :



Le LSP actif [A,B,C,D] pourrait être protégé par le LSP de protection [A,E,F,G,D]. Les deux LSP sont pleinement instanciés (les ressources sont allouées pour les deux LSP, actif et de protection) et aucun partage de ressources ne peut être fait le long du chemin de protection car le LSP de protection primaire peut porter du trafic supplémentaire.

Note : il est nécessaire que les deux chemins soient sur des SRLG disjoints pour assurer la possibilité de récupération ; sinon, une seule défaillance peut impacter les deux LSP, actif et de protection.

7.1 Identifiants

Pour simplifier les opérations d'association, les deux LSP appartiennent à la même session. Donc, l'objet SESSION DOIT être le même pour les deux LSP. L'identifiant de LSP DOIT cependant être différent pour distinguer le LSP protégé qui porte le trafic actif et le LSP de protection qui peut porter du trafic supplémentaire.

Un nouvel objet PROTECTION (voir la Section 14) est inclus dans le message Path utilisé pour établir les deux LSP. Cet objet porte le type de protection désirée de bout en bout pour le LSP – dans ce cas, "protection 1:N avec trafic supplémentaire". Cette valeur de type de protection de LSP est applicable aux LSP uni et bidirectionnels.

Le LSP actif est signalé en réglant dans le nouvel objet PROTECTION le bit S à 0, le bit P à 0, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP de protection.

Le LSP de protection est signalé en réglant dans le nouvel objet PROTECTION le bit S à 0, le bit P à 1, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP protégé associé.

7.2 Demande/réponse de commutation de bout en bout

Pour coordonner le transfert entre points d'extrémité, une demande/réponse de transfert de bout en bout est nécessaire afin que le LSP affecté soit déplacé au LSP de protection. La commutation de protection du LSP actif au LSP de protection (qui implique la préemption du trafic supplémentaire porté sur le LSP de protection) doit être initiée par un des nœuds d'extrémité (A ou D).

La procédure est la suivante :

1. Si un nœud d'extrémité (A ou D) détecte la défaillance du LSP actif (ou une dégradation de la qualité du signal sur le LSP actif) ou reçoit a message Notify incluant son objet SESSION dans la <liste de sessions amont/aval> (voir la [RFC3473]) et le nouveau code/sous code d'erreur "Notification d'erreur/défaillance locale du LSP" dans l'objet (IF_ID)_ERROR_SPEC, il déconnecte le trafic supplémentaire du LSP de protection. Noter que le <descripteur d'envoyeur> ou <descripteur de flux> est aussi présent dans le message Notify qui résout toute ambiguïté et condition de concurrence car il identifie (avec l'objet SESSION) le LSP en condition de défaillance. Ce nœud DOIT envoyer de façon fiable un message Notify, incluant l'objet MESSAGE_ID, à l'autre nœud d'extrémité (D ou A, respectivement) avec le nouveau code/sous code d'erreur "Notification d'erreur/défaillance du LSP" (demande de transfert) indiquant la défaillance du LSP actif. Ce message Notify DOIT être envoyé avec le fanion ACK_Désiré établi dans l'objet MESSAGE_ID pour demander que le receveur envoie un accusé de réception pour le message (voir la [RFC2961]). Ce message Notify (demande de transfert) PEUT indiquer l'identité de la liaison défaillante ou toute autre information pertinente en utilisant l'objet IF_ID ERROR_SPEC (voir la [RFC3473]). Dans ce cas, l'objet IF_ID ERROR_SPEC remplace l'objet ERROR_SPEC dans le message Notify ; autrement, les informations correspondantes (du plan des données) DEVRAIENT être reçues dans le message PathErr/ResvErr.

2. À réception du message Notify (demande de transfert) le nœud d'extrémité (D ou A, respectivement) DOIT déconnecter le trafic supplémentaire du LSP de protection et commencer à envoyer/recevoir le trafic normal de/vers le LSP de protection. Ce nœud DOIT envoyer de façon fiable un message Notify, incluant l'objet MESSAGE_ID, à l'autre nœud d'extrémité (A ou D, respectivement). Ce message Notify (demande de transfert) DOIT aussi inclure un objet MESSAGE_ID_ACK pour accuser réception du message Notify (demande de transfert). Ce message Notify (demande de transfert) PEUT indiquer l'identité de la liaison défaillante ou toute autre information pertinente en utilisant l'objet

IF_ID ERROR_SPEC (voir la [RFC3473]).

Note : comme le message Notify généré par l'autre nœud d'extrémité (A ou D, respectivement) est distinct de celui généré par un nœud intermédiaire, il n'y a pas de possibilité de connecter le trafic supplémentaire au LSP actif du fait de la réception d'un message Notify d'un nœud intermédiaire.

3. À réception du message Notify (demande de transfert) le nœud d'extrémité (A ou D, respectivement) DOIT commencer à recevoir le trafic normal provenant du LSP de protection ou à l'envoyer. Ce nœud DOIT aussi envoyer un message Ack à l'autre nœud d'extrémité (D ou A, respectivement) pour accuser réception du message Notify (demande de transfert).

Note 1 : une signalisation de commutation de protection en deux phases est utilisée dans le présent contexte ; une signalisation en trois phases (voir la [RFC4426]) qui impliquerait un message de notification, un message de demande de transfert, et un message de réponse de transfert n'est pas envisagé ici. Aussi, quand les LSP protecteurs ne portent pas de trafic supplémentaire, la signalisation de commutation de protection (comme définie au paragraphe 6.2) PEUT être utilisée à la place de la procédure décrite dans ce paragraphe.

Note 2 : quand le bit N est établi, l'échange de demande/réponse de transfert ci-dessus fournit seulement une coordination du plan de contrôle (aucune action n'est déclenchée au niveau du plan des données).

Après l'achèvement de la commutation de protection (étape 3), et après réception du message PathErr, pour garder trace du LSP d'où le trafic normal est pris, le LSP de protection DEVRAIT être signalé avec le bit O établi. De plus, le LSP anciennement actif PEUT être signalé avec le bit A établi dans l'objet ADMIN_STATUS (voir la [RFC3473]).

7.3 Protection 1:N (N > 1) avec trafic supplémentaire

La protection 1:N (N > 1) avec trafic supplémentaire suppose que le LSP de protection pleinement provisionné est à ressources disjointes des N LSP actifs. Ce LSP de protection permet ainsi de porter le trafic supplémentaire. Noter que les N LSP actifs et le LSP de protection sont tous entre la même paire de points d'extrémité. De plus, les N LSP actifs (considérés comme identiques en termes de paramètres de trafic) PEUVENT être mutuellement à ressources disjointes. La coordination entre nœuds d'extrémité est requise quand on commute d'un des LSP actifs au LSP de protection.

Chaque LSP actif est signalé avec les deux bits S et P réglés à 0. Le type de protection de LSP est réglé à 0x04 (protection 1:N avec trafic supplémentaire) durant l'établissement de LSP. Chaque identifiant d'association pointe sur l'identifiant du LSP de protection.

Le LSP de protection (portant du trafic supplémentaire) est signalé avec le bit S réglé à 0 et le bit P réglé à 1.Le type de protection de LSP est réglé à 0x04 (protection 1:N avec trafic supplémentaire) durant l'établissement de LSP. L'identifiant d'association DOIT être réglé par défaut à l'identifiant de LSP du LSP protégé correspondant à N = 1.

Toute procédure de signalisation applicable à la protection 1:1 avec trafic supplémentaire s'applique également à la protection 1:N avec trafic supplémentaire.

8. Réacheminement sans trafic supplémentaire

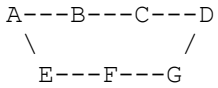
Le réacheminement de bout en bout (pré programmé) sans trafic supplémentaire s'appuie sur l'établissement entre la même paire de nœuds d'extrémité d'un LSP actif et d'un LSP de protection qui est disjoint en liaison/nœud/SRLG du LSP actif. Cependant, dans ce cas, le LSP de protection n'est pas pleinement instancié ; donc, il ne peut pas porter de trafic supplémentaire (noter que cela ne signifie pas que les ressources correspondantes ne peuvent pas être utilisées par d'autres LSP). Donc, ce mécanisme protège contre les défaillances du LSP actif mais exige l'activation du LSP de protection après qu'une défaillance se produit.

La signalisation est effectuée en indiquant dans le message Path (dans l'objet PROTECTION, voir la Section 14) que les LSP sont de type actif et de protection, respectivement. Les LSP de protection sont utilisés pour un transfert rapide quand les LSP actifs ont une défaillance. Dans ce cas, les LSP, actif et de protection, sont signalés comme LSP primaire et LSP secondaire, respectivement. Donc, seul le LSP actif est pleinement instancié durant la phase de provisionnement, et pour les LSP de protection, aucune ressource n'est engagée au niveau du plan des données (elles sont pré-réservées au niveau du plan de contrôle seulement). L'établissement du LSP actif DEVRAIT indiquer (en utilisant l'objet NOTIFY REQUEST

comme spécifié à la Section 4 de la [RFC3473]) que le nœud d'extrémité de tête du LSP (et éventuellement le nœud d'extrémité de queue) souhaite recevoir un message Notify si une défaillance de LSP se produit. À réception du message Notify, le nœud d'extrémité de tête DOIT commuter le trafic (normal) du LSP actif au LSP de protection après son activation. Noter que comme les LSP, actif et de protection, sont établis entre les mêmes nœuds d'extrémité, aucune autre notification n'est requise pour indiquer que les LSP actifs sont sans protection.

Pour rendre la bande passante pré-réservée pour un LSP de protection (mais non activé) disponible pour le trafic supplémentaire, cette bande passante pourrait être incluse dans la bande passante non réservée annoncée à une priorité inférieure (ce qui signifie d'un numéro plus élevé) que la priorité de garde du LSP de protection. De plus, le champ Bande passante maximale de LSP dans le sous TLV Descripteur de capacité de commutation d'interface devrait refléter le fait que la bande passante pré-réservée pour le LSP de protection est disponible pour le trafic supplémentaire. Les LSP pour le trafic supplémentaire peuvent alors être établis en utilisant la bande passante pré-réservée pour le LSP de protection en réglant (dans le message Path) le champ Priorité d'établissement de l'objet SESSION_ATTRIBUTE à X (où X est la priorité d'établissement du LSP de protection) et le champ Priorité de garde à au moins X+1. Aussi, si les ressources pré-réservées pour le LSP de protection sont utilisées par des LSP de priorité inférieure, ces LSP DOIVENT être préemptés quand le LSP de protection est activé (voir la Section 10).

Considérons la topologie suivante :



Le LSP actif [A,B,C,D] pourrait être protégé par le LSP de protection [A,E,F,G,D]. Seul le LSP protégé est pleinement instancié (les ressources sont seulement allouées pour le LSP actif). Donc, le LSP de protection ne peut pas porter de trafic supplémentaire. Quand une défaillance est détectée sur le LSP actif (disons, à B) l'erreur est propagée et/ou notifiée (en utilisant un message Notify avec le nouveau code/sous code d'erreur "Notification d'erreur/défaillance locale du LSP" dans l'objet (IF_ID)_ERROR_SPEC) au nœud d'entrée (A). À réception, ce dernier active le LSP secondaire de protection instancié durant la phase de (pré) provisionnement. Ceci exige :

(1) la capacité d'identifier un "LSP secondaire de protection" (ici appelé le "LSP secondaire") utilisé pour récupérer un autre LSP primaire actif (appelé ici le "LSP protégé")
(2) la capacité d'associer le LSP secondaire avec le LSP protégé
(3) la capacité d'activer un LSP secondaire après la survenance de la défaillance.

Dans les paragraphes qui suivent, ces caractéristiques sont décrites plus en détails.

8.1 Identifiants

Pour simplifier les opérations d'association, les deux LSP (c'est-à-dire,le LSP protégé et le LSP secondaire) appartiennent à la même session. Donc, l'objet SESSION DOIT être le même pour les deux LSP. L'identifiant de LSP DOIT cependant être différent pour distinguer le LSP protégé qui porte le trafic actif et le LSP secondaire qui ne peut pas porter de trafic supplémentaire.

Un nouvel objet PROTECTION (voir à la Section 14) est utilisé pour établir les deux LSP. Cet objet porte le type de protection de LSP de bout en bout désiré (dans ce cas, "Réacheminement sans trafic supplémentaire"). Cette valeur de type de protection de LSP est applicable aux LSP uni et bidirectionnels.

8.2 Signalisation des LSP primaires

Le nouvel objet PROTECTION est inclus dans le message Path durant la signalisation du LSP primaire actif, avec la valeur de type de protection de LSP de bout en bout réglée à "Réacheminement sans trafic supplémentaire".

Les LSP primaires actifs sont signalés en réglant dans le nouvel objet PROTECTION le bit S à 0, le bit P à 0, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP de protection secondaire associé.

8.3 Signalisation des LSP secondaires

Le nouvel objet PROTECTION est inclus dans le message Path durant la signalisation des LSP secondaires de protection, avec la valeur de type de protection de LSP de bout en bout réglée à "Réacheminement sans trafic supplémentaire".

Les LSP secondaires de protection sont signalés en réglant dans le nouvel objet PROTECTION le bit S et bit P à 1, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP actif primaire associé, qui DOIT être connu avant la signalisation du LSP secondaire.

Avec ce réglage, les ressources pour le LSP secondaire DEVRAIENT être pré-réservées, mais pas engagées au niveau du plan des données, ce qui signifie que l'intérieur de la commutation n'a pas besoin d'être établi jusqu'à ce qu'une action explicite soit effectuée pour activer ce LSP secondaire. L'activation d'un LSP secondaire est faite en utilisant un message Path modifié avec le bit S réglé à 0 dans l'objet PROTECTION. À ce point, les ressources de liaison et de nœud doivent être allouées pour ce LSP qui devient un LSP primaire (prêt à porter le trafic normal).

D'après la [RFC3945], le LSP secondaire est établi avec une pré-réservation de ressources mais avec ou sans pré-sélection d'étiquette (les deux permettant le partage des ressources de récupération). Dans le premier cas (défini comme par défaut, l'allocation d'étiquette durant la signalisation de LSP secondaire n'exige pas de procédure spécifique par rapport à la [RFC3473]. Cependant, dans le dernier cas, la réallocation d'étiquette (et donc de ressource) PEUT se produire durant l'activation du LSP secondaire. Cela signifie que durant la phase d'activation de LSP, les étiquettes PEUVENT être réallouées (avec une préséance supérieure aux allocations d'étiquette existantes ; voir aussi la [RFC3471]).

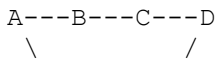
Note : dans certaines circonstances (par exemple, quand des ressources pré-réservées de protection sont utilisées par des LSP de priorité inférieure) il PEUT être désirable d'effectuer l'activation du LSP secondaire dans la direction amont (message de déclenchement de Resv) au lieu d'utiliser l'activation vers l'aval par défaut. Dans ce cas, tout dérangement et toute mauvaise interprétation entre un Resv de rafraîchissement (le long du LSP de priorité inférieure) et un message Resv de déclenchement (le long du LSP secondaire) DOIVENT être évités à tout nœud intermédiaire. Pour cela, à réception du message Path, le nœud de sortie PEUT inclure l'objet PROTECTION dans le message Resv. Il est alors traité bond par bond pour activer le LSP secondaire jusqu'à atteindre le nœud d'entrée. L'objet PROTECTION inclus dans le message Path DOIT être réglé comme spécifié dans cette section. Dans ce cas, l'objet PROTECTION avec le bit S DOIT être réglé à 0 et inclus dans le message Resv envoyé dans la direction amont. Le comportement d'activation amont DEVRAIT être configurable en local. Les détails concernant la préemption de LSP de priorité inféieure lors de l'activation de LSP secondaire sont donnés à la Section 10.

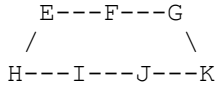
9. Restauration en maillage partagé

Une approche pour réduire les exigences de ressources de récupération est de faire que les LSP de protection partagent les ressources du réseau quand les LSP actifs qu'ils protègent sont physiquement disjoints (c'est-à-dire, liaison, nœud, SRLG, etc.). Ce mécanisme est appelé la restauration en maillage partagé et est décrite dans la [RFC4426]. La restauration en maillage partagé peut être vue comme un cas particulier de réacheminement pré-programmé de LSP (voir la Section 8) qui réduit les exigences de ressources de récupération en permettant que plusieurs LSP de protection partagent des ressources communes de liaison et de nœud. Ici aussi, les ressources de récupération pour les LSP de protection sont pré-réservées durant la phase de provisionnement, donc une action explicite de signalisation est nécessaire pour activer (c'est-à-dire, engager l'allocation de ressources au plan des données) un LSP de protection spécifique instancié durant la phase de (pré) provisionnement. Cela exige la signalisation de la restauration le long du LSP de protection.

Pour rendre la bande passante pré-réservée pour un LSP de protection (mais pas activé) disponible pour le trafic supplémentaire, cette bande passante pourrait être incluse dans la bande passante non réservée annoncée à une priorité inférieure (ce qui signifie numériquement plus élevée) à la priorité de garde du LSP de protection. De plus, le champ Bande passante maximum de LSP dans le sous TLV Descripteur de capacité de commutation d'interface devrait refléter le fait que la bande passante pré-réservée pour le LSP de protection est disponible pour du trafic supplémentaire. Les LSP pour le trafic supplémentaire peuvent alors être établis en utilisant la bande passante pré-réservée pour le LSP de protection en réglant (dans le message Path) le champ Priorité d'établissement de l'objet SESSION_ATTRIBUTE à X (où X est la priorité d'établissement du LSP de protection) et le champ Priorité de garde à au moins X+1. Aussi, si les ressources pré-réservées pour le LSP de protection sont utilisées par des LSP de priorité inférieure, ces LSP DOIT être préemptés quand le LSP de protection est activé (voir la Section 10). De plus, si les ressources de récupération sont partagées entre plusieurs LSP de protection, les nœuds d'extrémité de tête de LSP actifs correspondants doivent être informés qu'ils ne sont plus protégés quand le LSP de protection est activé pour récupérer le trafic normal pour le LSP actif défaillant.

Considérons la topologie suivante :





Les LSP actifs [A,B,C,D] et [H,I,J,K] pourraient être protégés par [A,E,F,G,D] et [H,E,F,G,K], respectivement. Selon la [RFC3209], afin de réaliser le partage de ressources durant la signalisation de ces LSP de protection, ils doivent avoir la même adresse de point d'extrémité de tunnel (au titre de leur objet SESSION). Cependant, ces adresses ne sont pas les mêmes dans cet exemple. Le partage de ressource le long de E, F, et G peut seulement être réalisé si les nœuds E, F, et G reconnaissent que le type de protection de LSP du LSP secondaire est réglé à "Réacheminement sans trafic supplémentaire" (voir l'objet PROTECTION, à la Section 14) et agissent en conséquence. Dans ce cas, les LSP de protection ne sont pas fusionnés (ce qui est utile car les chemins divergent en G) mais les ressources le long de E, F, G peuvent être partagées.

Quand une défaillance est détectée sur un des LSP actifs (disons, en B) l'erreur est propagée et/ou notifiée (en utilisant un message Notify avec le nouveau code/sous code d'erreur "Notification d'erreur/défaillance du LSP local" dans l'objet (IF_ID)_ERROR_SPEC) au nœud d'entrée (A). À réception, ce dernier active le LSP secondaire de protection (voir la Section 8). À ce point, il est important qu'une défaillance sur l'autre LSP (disons, en J) ne cause pas que l'autre entrée (H) envoie des données sur le LSP de protection alors que les ressources sont déjà utilisées. Cela peut être réalisé par le nœud E en utilisant la procédure suivante. Quand la capacité est d'abord réservée pour le LSP de protection, E devrait vérifier que les LSP protégés ([A,B,C,D] et [H,I,J,K], respectivement) ne partagent aucune ressource commune. Ensuite, quand une défaillance se produit (disons, en B) et que le LSP de protection [A,E,F,G,D] est activé, E devrait notifier à H que les ressources pour le LSP de protection [H,E,F,G,K] ne sont plus disponibles.

Les paragraphes qui suivent détaillent comment la restauration maillée partagée peut être mise en œuvre d'une façon interopérable en utilisant les extensions de GMPLS RSVP-TE (voir la [RFC3473]). Cela inclut :
(1) la capacité d'identifier un "LSP secondaire de protection" (appelé ici le "LSP secondaire") utilisé pour récupérer un autre LSP primaire actif (appelé ici le "LSP protégé"),
(2) la capacité d'associer le LSP secondaire avec le LSP protégé,
(3) la capacaté d'inclure des informations sur les ressources utilisées par le LSP protégé tout en instanciant le LSP secondaire,
(4 la capacité d'instancier durant la phase de provisionnement plusieurs LSP secondaires d'une manlère efficace,
(5) la capacité d'activer un LSP secondaire après la survenance d'une défaillance.

Dans les paragraphes qui suivent, ces caractéristiques sont décrites en détails.

9.1 Identifiants

Pour simplifier les opérations d'association, les deux LSP (c'est-à-dire, le LSP protégé et le LSP secondaire) appartienent à la même session. Donc, l'objet SESSION DOIT être le même pour les deux LSP. L'identifiant de LSP DOIT cependant être différent pour distinguer le LSP protégé portant le trafic actif et le LSP secondaire qui ne peut pas porter de trafic supplémentaire.

Un nouvel objet PROTECTION (voir la Section 14) est utilisé pour établir les deux LSP. Cet objet porte le type de protection de LSP désiré de bout en bout – dans ce cas, "Réacheminement sans trafic supplémentaire". Cette valeur de type de protection de LSP est applicable aux LSP uni et bidirectionnels.

9.2 Signalisation des LSP primaires

Le nouvel objet PROTECTION est inclus dans le message Path durant la signalisation des LSP primaires actifs, avec la valeur de type de protection de LSP de bout en bout réglée à "Réacheminement sans trafic supplémentaire".

Les LSP primaires actifs sont signalés en réglant dans le nouvel objet PROTECTION le bit S à 0, le bit P à 0, et dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP secondaire de protection associé.

9.3 Signalisation des LSP secondaires

Le nouvel objet PROTECTION est inclus dans le message Path durant la signalisation des LSP secondaires de protection, avec la valeur de type de protection de LSP de bout en bout réglée à "Réacheminement sans trafic supplémentaire".

Les LSP secondaires de protection sont signalés en réglant dans le nouvel objet PROTECTION le bit S et le bit P à 1, et

dans l'objet ASSOCIATION, l'identifiant d'association à l'identifiant du LSP primaire actif associé, qui DOIT être connu avant la signalisation du LSP secondaire. De plus, le message Path utilisé pour instancier le LSP secondaire DEVRAIT inclure au moins un objet PRIMARY_PATH_ROUTE (voir à la Section 15) qui permet de plus la récupération de ressource partagée à chaque nœud intermédiaire le long du chemin secondaire.

Avec ce réglage, les ressources pour le LSP secondaire DEVRAIENT être pré-réservées, mais pas engagées au niveau du plan des données, ce qui signifie que les constituants de la commutation n'ont pas besoin d'être établis tant qu'une action explicite n'est pas effectuée pour activer ce LSP. L'activation d'un LSP secondaire est faite en utilisant un message Path modifié avec le bit S réglé à 0 dans l'objet PROTECTION. À ce point, les ressources de liaison et de nœud doivent être allouées pour ce LSP qui devient un LSP primaire (prêt à porter le trafic normal).

D'après la [RFC3945], le LSP secondaire est établi avec des ressources pré-reservées mais avec ou sans choix préalable d'étiquette (les deux permettant le partage des ressources de récupération). Dans le prermier cas (défini par défaut) l'allocation d'étiquette durant la signalisation du LSP secondaire n'exige aucune procédure spécifique par rapport à la [RFC3473]. Cependant, dans le second cas, la réallocation d'étiquette (et donc de la ressource) PEUT se produire durant l'activation du LSP secondaire. Cela signifie que, durant la phasee d'activation du LSP, les étiquettes PEUVENT être réallouées (avec une préséance supérieure à celle de l'allocation d'étiquette existante ; voir aussi la [RFC3471]).

10. Préemption de LSP

Quand les ressources de protection sont seulement pré-réservées pour les LSP secondaires, elles PEUVENT être utilisées pour établir des LSP de priorité inférieure. Dans ce cas, ces ressources DOIVENT être préemptées quand le LSP de protection est activé. Une condition supplémentaire découle de l'évitement de mauvaise connexion entre le LSP secondaire de protection qui est activé et le ou les LSP de priorité inférieure qui sont préemptés. La procédure à appliquer quand le message Path du LSP secondaire de protection (c'est-à-dire, le LSP qui préempte) atteint un nœud en utilisant les ressources pour un ou des LSP de priorité inférieure (c'est-à-dire, des LSP préemptés) est la suivante :

1. Désallouer les ressources à utiliser par le LSP préempteur et libérer l'interconnexion. Noter que si le LSP préempteur est bidirectionnel, ces ressources peuvent venir d'un ou de deux LSP de priorité inférieure, et si elles viennent de deux LSP, elles peuvent être uni ou bidirectionnelles. Le nœud préempteur NE DEVRAIT PAS envoyer le message Path avant que soit achevée la désallocation des ressources car cela peut conduire à une mauvaise connexion du chemin vers l'aval si le nœud aval est capable de réallouer plus rapidement les ressources.

2. Envoyer les messages PathTear et PathErr avec le nouveau code/sous code d'erreur "Défaillance du contrôle de politique/préemption difficile" et le fanion Path_State_Removed établi pour le ou les LSP préemptés.

3. Réserver les ressources préemptées pour le LSP de protection. Le nœud préempteur NE DOIT PAS interconnecter les ressources amont d'un LSP bidirectionnel préempteur.

4. Envoyer le message Path.

5. À réception d'un message Resv déclencheur du nœud aval, interconnecter les ressources du chemin vers l'aval, et si le LSP préempteur est bidirectionnel, effectuer l'interconnexion pour les ressources de chemin vers l'amont.

Noter que l'étape 1 peut causer des alarmes pour le LSP préempté. Si on désire la suppression des alarmes, le nœud préempteur PEUT insérer les étapes suivantes avant l'étape 1 .

1a Avant de désallouer des ressources, envoyer un message Resv, incluant un objet ADMIN_STATUS, pour désactiver les alarmes pour le LSP préempté.

1b. Recevoir un message Path indiquant que les alarmes sont désactivées.

Au nœud aval (par rapport au LSP préempteur) il est RECOMMANDÉ que le traitement soit comme suit :

1. Recevoir un message PathTear (et/ou PathErr) pour le ou les LSP préemptés.

2a. Libérer les ressources associées au LSP sur l'interface avec le LSP préempteur, supprimer toutes les interconnexions, et libérer toutes les autres ressources associées au LSP préempté.

2b. Transmettre le message PathTear (et/ou PathErr) selon la [RFC3473].

3. Recevoir le message Path pour le LSP préempteur et le traiter normalement, en le transmettant au nœud aval.

4. Recevoir le message Resv pour le LSP préempteur et le traiter normalement, en le transmettant au nœud aval.

11. Réacheminement (complet) de LSP

Le réacheminement de LSP, par ailleurs, commute le trafic normal à un LSP de remplacement qui n'est pleinement établi qu'après que la défaillance est survenue. Le nouveau chemin (de remplacement) est choisi à l'extrémité de tête du LSP et peut réutiliser des nœuds intermédiaires inclus dans le chemin original ; il peut aussi inclure des nœuds intermédiaires supplémentaires. Pour un acheminement de bonds stricts, les exigences de TE peuvent être directement appliquées au calcul de chemin, et le nœud ou liaison défaillant peut être évité. Cependant, si la défaillance s'est produite au sein d'un bond à acheminement lâche, le nœud d'extrémité de tête peut n'avoir pas assez d'informations pour réacheminer le LSP en évitant la défaillance. La signalisation de retour en arrière (voir la [RFC4920]) et les techniques d'exclusion de chemin (voir la [RFC4874]) PEUVENT être utilisées dans ce cas.

Le chemin de remplacement PEUT être soit calculé à la demande (c'est-à-dire, quand la défaillance se produit ; c'est appelé un réacheminement complet de LSP) soit pré-calculé et mémorisé pour être utilisé quand la défaillance est rapportée. Cette dernière offre un temps de restauration plus rapide. Il y a cependant un risque que le chemin de remplacement soit périmé par d'autres changements dans le réseau ; ceci peut être atténué dans une certaine mesure par des calculs périodiques des chemins de remplacement inactifs.

Le réacheminement (complet) de LSP va être initié par le nœud d'extrémité de tête qui a détecté la défaillance de LSP ou reçu un message Notify et/ou un message PathErr avec le nouveau code/sous code d'erreur "Notification d'erreur/défaillance locale du LSP" pour ce LSP. Les ressources du nouveau LSP peuvent être établies en utilisant le mécanisme "faire avant de couper" *(make-before-break)* où le nouveau LSP est établi avant que le vieux LSP soit supprimé. Ceci est fait en utilisant les mécanismes de l'objet SESSION_ATTRIBUTE et le style de réservation de partage explicite (SE, *Shared-Explicit*) (voir la [RFC3209]). Les deux LSP, nouveau et ancien, peuvent partager des ressources aux nœuds communs.

Noter que le mécanisme "faire avant de couper" n'est pas utilisé pour éviter des perturbations du flux normal de trafic (ce dernier a déjà été cassé par la défaillance qui est en cours de réparation). Cependant, il est précieux pour conserver les ressources allouées sur le LSP d'origine qui vont être réutilisées par le nouveau LSP de remplacement.

11.1 Identifiants

L'adresse de point d'extrémité de tunnel, l'identifiant de tunnel, l'identifiant étendu de tunnel, et l'adresse d'envoyeur de tunnel identifient de façon univoque les deux LSP, ancien et nouveau. Seule la valeur d'identifiant de LSP différencie l'ancien du nouveau LSP de remplacement. Le nouveau LSP de remplacement est établi avant que l'ancien LSP soit supprimé en utilisant le style de réservation de partage explicite (SE). Cela assure que le nouveau LSP (de remplacement) est établi sans double compte des exigences de ressources le long des segments communs.

Le LSP de remplacement PEUT être établi avant qu'une défaillance se produise avec le style de réservation de ressource SE, car il partage les mêmes adresses de point d'extrémité de tunnel, identifiant de tunnel, identifiant de tunnel étendu, et adresse d'envoyeur de tunnel avec le LSP original (c'est-à-dire, seulement la valeur d'identifiant de LSP DOIT être différente).

Dans les deux cas, l'identifiant d'association de l'objet ASSOCIATION DOIT être établi à la valeur d'identifiant de LSPdu LSP signalé.

11.2 Signalisation des LSP réacheminables

Un nouvel objet PROTECTION est inclus dans le message Path durant la signalisaion de LSP réacheminables dynamiquement, avec la valeur de type de protection de LSP de bout en bout réglée à "réacheminement complet". Ces LSP qui peuvent être uni ou bidirectionnels sont signalés en réglant dans l'objet PROTECTION le bit S à 0, le bitP à 0, et la valeur d'identifiant d'association à la valeur de l'identifiant de LSP du LSP signalé. Toute action spécifique à entreprendre durant la phase de provisionnement est du ressort de la politique locale du nœud d'extrémité.

Note : quand le type de protection de LSP de bout en bout est réglé à "Non protégé", les deux bits S et P DOIVENT être réglés à 0, et le LSP NE DEVRAIT PAS être réacheminé au nœud d'extrémité de tête après la survenance d'une défaillance. La valeur Identifiant d'association DOIT être réglée à la valeur d'identifiant de LSP du LSP signalé. Cela ne signifie pas que le LSP non protégé ne peut pas être rétabli pour d'autres raisons comme une ré-optimisation de chemin et un ajustement de bande passante résultant de conditions de la politique.

12. Réversion

La réversion se réfère à une opération de commutation de récupération, où le trafic normal retourne au (ou reste) LSP actif quand il a récupéré de la défaillance. La réversion implique que les ressources restent allouées au LSP qui était à l'origine acheminé sur elles même après une défaillance. Il est important d'avoir des mécanismes qui permettent à la réversion d'être effectuée avec un minimum d'interruption et de reconfiguration de service.

Pour "la protection 1+1 bidirectionnelle", la réversion au LSP récupéré se produit en utilisant la séquence suivante :
1. Mettre à zéro le bit A de l'objet ADMIN_STATUS si il est établi pour le LSP récupéré.
2. Ensuite, appliquer la méthode décrite ci-dessous pour commuter le trafic normal du LSP de protection au LSP récupéré. Ceci est effectué en utilisant le nouveau code/sous code d'erreur "Notification d'erreur/LSP récupéré" (Demande de commutation en retour).

La procédure est la suivante :

1) Le nœud initiateur (source) envoie le trafic normal sur les deux LSP, actif et de protection. Une fois réalisé, le nœud source envoie de façon fiable un message Notify à la destination avec le nouveau code/sous code d'erreur "Notification d'erreur/LSP récupéré" (demande de commutation de retour). Ce message Notify inclut l'objet MESSAGE_ID. Le fanion ACK_Désiré DOIT être établi dans cet objet pour demander au receveur d'envoyer un accusé de réception pour le message (voir la [RFC2961]).

2) À réception de ce message, la destination choisit le trafic provenant du LSP actif. Au même moment, elle transmet le trafic sur les deux LSP, actif et de protection. La destination envoie alors de façon fiable un message Notify à la source confirmant l'achèvement de l'opération. Ce message inclut l'objet MESSAGE_ID_ACK pour accuser réception du message Notify reçu. Ce message Notify inclut aussi l'objet MESSAGE_ID. Le fanion ACK_Désiré DOIT être établi dans cet objet pour demander au receveur d'envoyer un accusé de réception du message (voir la [RFC2961]).

3) Quand le nœud source reçoit ce message Notify, il commute le trafic reçu du LSP actif. Le nœud source envoie alors un message Ack au nœud de destination confirmant que le LSP a été repris.

3. Finalement, on met à zéro le bit O de l'objet PROTECTION envoyé sur le LSP de protection.

Pour la "protection 1:N avec trafic supplémentaire", la réversion au LSP récupéré se produit en utilisant la séquence suivante :
1. Mettre à zéro le bit A de l'objet ADMIN_STATUS si il est établi pour le LSP récupéré.
2. Puis, appliquer la méthode décrite ci-dessous pour commuter le trafic normal du LSP de protection au LSP récupéré. Ceci est effectué en utilisant le nouveau code/sous code d'erreur "Notification d'erreur/LSP récupéré" (Demande de commutation de retour).

La procédure est la suivante :

1) Le nœud initiateur (source) envoie le trafic normal aux deux LSP, actif et de protection. Une fois l'envoi achevé, le nœud source envoie de façon fiable un message Notify à la destination avec le nouveau code/sous code d'erreur "Notification d'erreur/LSP récupéré" (Demande de commutation de retour). Ce message Notify inclut l'objet MESSAGE_ID. Le fanion ACK_Désiré DOIT être établi dans cet objet pour demander au receveur d'envoyer un accusé de réception du message (voir la [RFC2961]).

2) À réception de ce message, la destination choisit le trafic provenant du LSP actif. Au même moment, elle transmet le trafic aux deux LSP, actif et de protection. La destination envoie alors de façon fiable un message Notify à la source confirmant l'achèvement de l'opération. Ce message inclut l'objet MESSAGE_ID_ACK pour accuser réception du message Notify reçu. Ce message Notify inclut aussi l'objet MESSAGE_ID. Le fanion ACK_Désiré DOIT être établi dans cet objet pour demander au receveur d'envoyer un accusé de réception du message (voir la [RFC2961]).

3 Quand le nœud source reçoit ce message Notify, il commute pour recevoir le trafic provenant du LSP actif, et arrête de transmettre du trafic sur le LSP de protection. Le nœud source envoie alors un message Ack au nœud de destination confirmant que le LSP a été restauré.

4) À réception de ce message, le nœud de destination arrête de transmettre le trafic le long du LSP de protection.

3. Finalement, on met à zéro le bit O de l'objet PROTECTION envoyé sur le LSP de protection.

Pour le "Réacheminement sans trafic supplémentaire" (incluant le cas de récupération partagée) la réversion implique que le LSP anciennement actif n'a pas été supprimé par le nœud d'extrémité de tête à la réception du message PathErr, c'est-à-dire, le nœud d'extrémité de tête continue de rafraîchir le LSP actif en condition de défaillance. Cela assure que exactement les mêmes ressources sont restituées après la commutation de réversion (sauf si le LSP actif exige une nouvelle signalisation). La ré-activation est effectuée en utilisant la séquence suivante :

1. Mettre à zéro le bit A de l'objet ADMIN_STATUS si il est établi pour le LSP récupéré.
2. Puis, appliquer la méthode décrite ci-dessous pour commuter le trafic normal du LSP de protection au LSP récupéré. Ceci est effectué en utilisant le nouveau code/sous code d'erreur "Notification d'erreur/LSP récupéré" (Demande de commutation de retour).

La procédure est la suivante :

1) Le nœud initiateur (source) envoie le trafic normal aux deux LSP, actif et de protection. Une fois l'envoi achevé, le nœud source envoie de façon fiable un message Notify à la destination avec le nouveau code/sous code d'erreur "Notification d'erreur/LSP récupéré" (Demande de commutation de retour). Ce message Notify inclut l'objet MESSAGE_ID. Le fanion ACK_Désiré DOIT être établi dans cet objet pour demander au receveur d'envoyer un accusé de réception du message (voir la [RFC2961]).

2) À réception de ce message, la destination choisit le trafic provenant du LSP actif. Au même moment, elle transmet le trafic aux deux LSP, actif et de protection. La destination envoie alors de façon fiable un message Notify à la source confirmant l'achèvement de l'opération. Ce message inclut l'objet MESSAGE_ID_ACK pour accuser réception du message Notify reçu. Ce message Notify inclut aussi l'objet MESSAGE_ID. Le fanion ACK_Désiré DOIT être établi dans cet objet pour demander au receveur d'envoyer un accusé de réception du message (voir la [RFC2961]).

3) Quand le nœud source reçoit ce message Notify, il commute pour recevoir le trafic provenant du LSP actif, et arrête de transmettre du trafic sur le LSP de protection. Le nœud source envoie alors un message Ack au nœud de destination confirmant que le LSP a été restauré.

4) À réception de ce message, le nœud de destination arrête de transmettre le trafic le long du LSP de protection.

3. Finalement, désactiver le LSP de protection en réglant le bit S à 1 dans l'objet PROTECTION envoyé sur le LSP de protection.

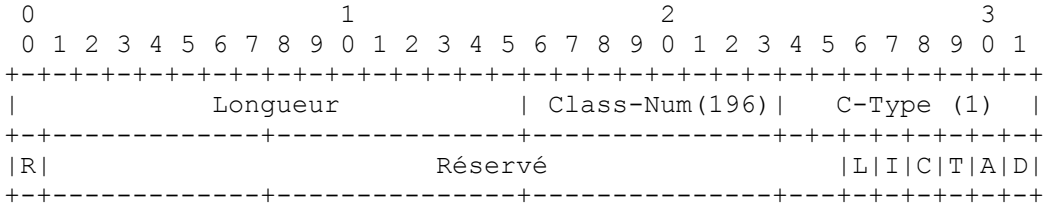
13. Commandes de récupération

Cette section spécifie le comportement au plan de contrôle en utilisant plusieurs commandes (voir la [RFC4427]) qui peuvent être utilisées pour influencer les opérations de récupération.

A. Verrouillage du LSP de récupération :

Le bit Verrouillage (L, Lockout) de l'objet ADMIN_STATUS est utilisé suivant les règles définies à la Section 8 de la [RFC3471] et à la Section 7 de la [RFC3473]. Le bit L doit être établi avec le bit Reflet (R) dans l'objet ADMIN_STATUS envoyé dans le message Path. À réception du message Resv avec le bit L établi, cela force le LSP de récupération à être temporairement indisponible pour transporter du trafic (normal ou supplémentaire). Le déverrouillage est effectué en mettant à zéro le bit L, suivant les règles définies à la Section 7 de la [RFC3473]. Cette procédure est seulement applicable quand le fanion Type de protection de LSP est établi à 0x04 (protection 1:N avec trafic supplémentaire) ou à 0x08 (protection 1+1 unidirectionnelle) ou à 0x10 (protection 1+1 bidirectionnelle).

Le format mis à jour de l'objet ADMIN_STATUS pour inclure le bit L bit est comme suit :



L (Lockout) : 1 bit. Réglé à 1, il force le LSP de récupération à être temporairement indisponible pour transporter du trafic (normal ou supplémentaire).

Les bits R (Reflet), T (essai), A (Administrativement mort), et D (suppression en cours) sont définis dans la [RFC3471]. Le bit C (Contrôle d'appel) est défini dans la [RFC4974], et le bit I (Inhibition de la communication d'alarme) dans la [RFC4783].

B. Verrouillage du trafic normal :
Le bit O de l'objet PROTECTION est réglé à 1 pour forcer le LSP de récupération à être temporairement indisponible au transport du trafic normal. Cette opération NE DOIT PAS se produire à moins que le LSP actif ne porte le trafic normal. Le déverrouillage est effectué en mettant à zéro le bit O sur le LSP de protection. Cette procédure n'est applicable que quand le fanion Type de protection de LSP est réglé à 0x04 (protection 1:N avec trafic supplémentaire) ou à 0x08 (protection 1+1 unidirectionnelle) ou à 0x10 (protection 1+1 bidirectionnelle).

C. Commutation forcée pour le trafic normal :
La signalisation de récupération est initiée pour commuter le trafic normal au LSP de récupération suivant les procédures définies aux Sections 6, 7, 8, et 9.

D. Commutation demandée pour le trafic normal :
La signalisation de récupération est initiée pour commuter le trafic normal au LSP de récupération suivant les procédures définies aux Sections 6, 7, 8, et 9. Cela se produit sauf si une condition de faute existe sur d'autres LSP ou portées (incluant le LSP de récupération) ou si une commande de commutation de priorité de force égale ou supérieure est en vigueur.

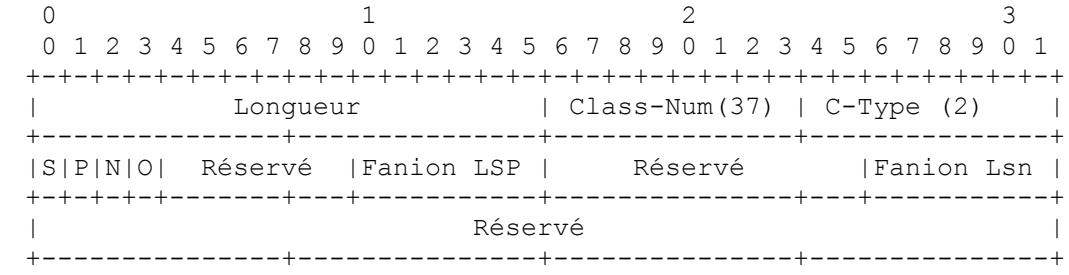
E. Commutation demandée pour le LSP de récupération:
La signalisation de récupération est initiée pour commuter le trafic normal au LSP actif suivant la procédure définie à la Section 12. Cette demande est exécutée sauf si une condition de faute existe sur le LSP actif ou si une commande de commutation de priorité égale ou supérieure est en vigueur.

14. Objet PROTECTION

Cette Section décrit les extensions à l'objet PROTECTION pour élargir son applicabilité à la récupération de LSP de bout en bout.

14.1 Format

Le format de l'objet PROTECTION (Class-Num = 37, C-Type = 2) est le suivant :



S (Secondaire) : 1 bit. Établi à 1, ce bit indique que le LSP demandé est un LSP secondaire. Réglé à 0 (par défaut) il indique que le LSP demandé est un LSP primaire.

P (Protection) : 1 bit. Établi à 1, ce bit indique que le LSP demandé est un LSP de protection. Réglé à 0 (par défaut) il indique que le LSP demandé est un LSP actif. La combinaison, S réglé à 1 avec P réglé à 0 n'est pas valide.

N (Notification) : 1 bit. Établi à 1, ce bit indique que l'échange de messages de plan de contrôle est seulement utilisé pour la notification durant la commutation de protection. Réglé à 0 (par défaut) il indique que les échanges de messages de plan de contrôle sont utilisés pour la commutation de protection. Le bit N n'est applicable que quand le fanion Type de protection de LSP est réglé à 0x04 (protection 1:N avec trafic supplémentaire) ou 0x08 (protection 1+1 unidirectionnelle) ou 0x10 (protection 1+1 bidirectionnelle). Le bit N DOIT être réglé à 0 dans tous les autres cas.

O (Opérationnel) : 1 bit. Établi à 1, ce bit indique que le LSP de protection porte le trafic normal après la commutation de protection. Le bit O n'est applicable que quand le bit P est réglé à 1, et que le fanion Type de protection de LSP est réglé à 0x04 (protection 1:N avec trafic supplémentaire) ou 0x08 (protection 1+1 unidirectionnelle) ou 0x10 (protection 1+1 bidirectionnelle). Le bit O DOIT être à 0 dans tous les autres cas.

Réservé : 6 bits. Ce champ est réservé. Il DOIT être à zéro en transmission et DOIT être ignoré à réception. Ces bits DEVRAIT être passés non modifiés par les nœuds de transit.

Fanion LSP (type de protection) : 6 bits. Indique le type désiré de récupération de LSP de bout en bout. Une valeur de 0 implique que le LSP est "non protégé". Seulement une valeur DEVRAIT être établie à la fois. Les valeurs suivantes sont définies. Toutes les autres valeurs sont réservées.
0x00 : non protégé
0x01 : réacheminement (complet)
0x02 : réacheminement sans trafic supplémentaire
0x04 : protection 1:N avec trafic supplémentaire
0x08 : protection 1+1 unidirectionnelle
0x10 : protection 1+1 bidirectionnelle

Réservé : 10 bits. Ce champ est réservé. Il DOIT être à zéro en transmission et DOIT être ignoré à réception. Ces bits DEVRAIT être passés non modifiés par les nœuds de transit.

Fanion Lsn : 6 bits. Indique le type désiré de protection de la liaison (voir la Section 7 de la [RFC3471]).

Réservé : 32 bits. Le codage de ce champ est détaillé dans la [RFC4873].

14.2 Traitement

Les nœuds intermédiaires et de sortie qui traitent un message Path contenant un objet PROTECTION DOIVENT vérifier que le type de protection de LSP demandé peut être satisfait par l'interface entrante. Si cela ne se peut pas, le nœud DOIT générer un message PathErr, avec le nouveau code/sous code d'erreur "Problème d'acheminement/protection de LSP non prise en charge".

Les nœuds intermédiaires qui traitent un message Path contenant un objet PROTECTION avec la valeur de type de protection de LSP réglée à 0x02 (réacheminement sans trafic supplémentaire) et un objet PRIMARY_PATH_ROUTE (voir la Section 15) DOIVENT vérifier que le type de protection de LSP demandé peut être pris en charge par l'interface sortante. Si cela ne se peut pas, le nœud DOIT générer un message PathErr avec le nouveau code/sous code d'erreur "Problème d'acheminement/protection de LSP non prise en charge".

15. Objet PRIMARY_PATH_ROUTE

L'objet PRIMARY_PATH_ROUTE (PPRO) est défini pour informer les nœuds le long du chemin d'un LSP secondaire de protection des ressources (liaisons/nœuds) qui sont utilisées par le LSP primaire protégé associé (comme spécifié par le champ Identifiant d'association). Si la valeur de type de protection de LSP est réglée à 0x02 (réacheminement sans trafic supplémentaire) cet objet DEVRAIT être présent dans le message Path pour le pré-provisionnement du LSP secondaire de protection pour permettre le partage des ressources de récupération entre un ou plusieurs LSP secondaires de protection (voir la Section 9). Le présent document ne suppose ni n'empêche aucun autre usage de cet objet.

Les objets PRIMARY_PATH_ROUTE portent des informations extraites de l'objet EXPLICIT ROUTE et/ou de l'objet RECORD ROUTE des LSP primaires actifs qu'ils protègent. Le choix du contenu du PPRO appartient à la politique locale du nœud d'extrémité de tête qui initie la demande. Donc, les informations incluses dans ces objets peuvent être utilisées comme contrôle d'admission fondé sur la politique pour assurer que les ressources de récupération sont seulement partagées entre les LSP secondaires de protection dont les LSP primaires associés ont des chemins de liaison/nœud/SRLG disjoints.

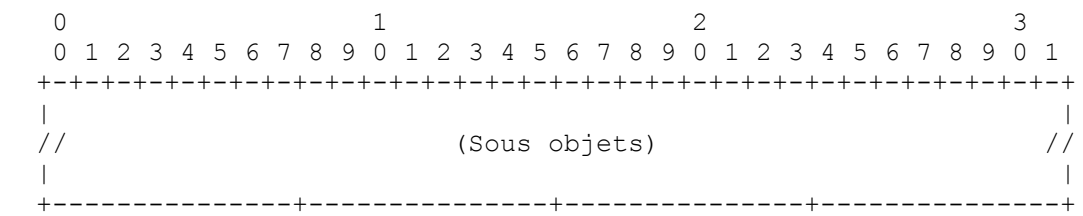
15.1 Format

Le chemin primaire est spécifié via l'objet PRIMARY_PATH_ROUTE (PPRO). Le numéro de classe (Class-Num) de

chemin primaire de forme 0bbbbbbb alloué par l'IANA est 38.

Actuellement un type de classe (C-Type) est défini, le type 1, chemin primaire. L'objet PRIMARY_PATH_ROUTE a le format suivant :

Class-Num = 38 (de forme 0bbbbbbb), C-Type = 1



Le contenu d'un objet PRIMARY_PATH_ROUTE est une série de longueur variable d'éléments de données appelés des sous objets (voir au paragraphe 15.2).

Pour signaler un LSP secondaire de protection, le message Path PEUT inclure un ou plusieurs objets PRIMARY_PATH_ROUTE, où chaque object est significatif. Ce dernier est utile quand un LSP secondaire de protection doit être de liaison/nœud/SRLG disjoint de plus d'un LSP primaire (c'est-à-dire, protège plus d'un LSP primaire).

15.2 Sous objets

L'objet PRIMARY_PATH_ROUTE est défini comme une liste d'éléments de données de longueur variable appelés des sous objets. Ces sous objets sont dérivés des sous objets de l'objet EXPLICIT ROUTE et/ou RECORD ROUTE du ou des LSP primaires actifs.

Chaque sous objet a son propre champ Longueur. La longueur contient la longueur totale du sous objet en octets, incluant les champs Type et Longueur. La longueur DOIT toujours être un multiple de 4, et au moins 4.

Les sous objets suivants sont actuellement définis pour l'objet PRIMARY_PATH_ROUTE :
- sous type 1 : adresse IPv4 (voir la [RFC3209])
- sous type 2 : adresse IPv6 (voir la [RFC3209])
- sous type 3 : étiquette (voir la [RFC3473])
- sous type 4 : interface non numérotée (voir la [RFC3477])

Un PPRO vide sans sous objet est considéré comme illégal. Un nœud qui reçoit un message Path contenant un PPRO vide DEVRAIT retourner un message PathErr avec le nouveau code/sous code d'erreur "Problème d'acheminement/mauvais objet PRIMARY_PATH_ROUTE".

Note : un nœud intermédiaire qui traite un PPRO peut déduire les identifiants de SRLG de la base de données IGP-TE locale en utilisant ses valeurs de sous objet de type 1, 2, ou 4 comme pointeurs sur les liaisons TE correspondantes (en supposant que chacune d'elles a un attribut SRLG TE associé).

15.3 Applicabilité

L'objet PRIMARY_PATH_ROUTE PEUT seulement être utilisé quand tous les nœuds GMPLS le long du chemin prennent en charge l'objet PRIMARY_PATH_ROUTE et qu'un LSP secondaire de protection est demandé. L'objet PRIMARY_PATH_ROUTE reçoit une valeur de classe de la forme 0bbbbbbb. Les nœuds GMPLS receveurs le long du chemin qui ne prennent pas en charge cet objet DOIVENT retourner un message PathErr avec le code d'erreur "Classe d'objet inconnue" (voir la [RFC2205]).

Les restrictions suivantes DOIVENT aussi être appliquées par rapport à l'usage du PPRO :

- Les PPRO PEUVENT seulement être inclus dans les messages Path dans la signalisation des LSP secondaires de protection (bit S = 1 et bit P = 1) et quand la valeur du type de protection de LSP est réglée à 0x02 (réacheminement sans trafic supplémentaire) dans l'objet PROTECTION (voir la Section 14).

- Les PRRO DEVRAIENT être présents dans le message Path pour le pré-provisionnement du LSP secondaire de protection afin de permettre le partage des ressources de récupération entre un ou plusieurs LSP secondaires de protection (voir le paragraphe 15.4).

- Les PPRO NE DOIVENT PAS être utilisés dans d'autres conditions. En particulier, si un PPRO est reçu quand le bit S est réglé à 0 dans l'objet PROTECTION, le nœud receveur DOIT retourner un message PathErr avec le nouveau code/sous code d'erreur "Problème d'acheminement/objet PRIMARY_PATH_ROUTE non applicable".

- Les échanges croisés de PPRO sur des LSP primaires sont interdits (c'est-à-dire, leur usage est restreint à un seul ensemble de LSP protégés).

- Le contenu du PPRO NE DOIT PAS inclure de sous objet venant d'autres PPRO. En particulier, les PPRO reçus NE DOIVENT PAS être réutilisés pour établir d'autres LSP actifs ou de protection.

15.4 Traitement

Le PPRO permet le partage des ressources de récupération entre un LSP secondaire de protection donné et un ou plusieurs LSP secondaires de protection si leurs LSP primaires actifs correspondants ont des chemins (liaison/nœud/SRLG) mutuellement disjoints. Considérons un nœud N à travers lequel des LSP secondaires de protection (disons, P[1],...,P[n]) ont déjà été établis qui protègent n LSP primaires actifs (disons, P'[1],...,P'[n]). Supposons aussi que ces n LSP secondaires actifs partagent une certaine ressource de liaison sortante (disons r).

Maintenant, supposons que le nœud N reçoive un message Path pour un LSP secondaire de protection supplémentaire (disons, Q, protégeant Q'). Le PPRO porté par ce message Path est traité comme suit :

- N vérifie si les LSP primaires actifs P'[1],...,P'[n] associés aux LSP P[1],...,P[n], respectivement, ont des liens, nœuds, et SLRG en commun avec le LSP primaire actif Q' (associé à Q) en comparant les sous objets PPRO mémorisés associés à P'[1],...,P'[n] avec les sous objets PPRO associés au Q' reçus dans le message Path.

- Si c'est le cas, N NE DEVRAIT PAS tenter de partager la ressource de liaison sortante r entre P[1],...,P[n] et Q. Cependant, selon une décision de politique locale, N PEUT allouer une autre liaison disponible (partagée) autre que r à utiliser par Q. Si ce n'est pas le cas (selon la décision de politique locale que l'allocation d'aucune autre liaison n'est permise pour Q) ou si aucune autre liaison n'est disponible pour Q, N DEVRAIT retourner un message PathErr avec le nouveau code/sous code d'erreur "Échec du contrôle d'admission/échec d'admission du LSP".

- Autrement (si P'[1],...,P'[n] et Q' sont pleinement disjoints) la liaison r choisie par N pour le LSP Q PEUT être exactement la même que celle choisie pour les LSP P[1],...,P[n]. Cela arrive après la vérification (d'après la politique locale du nœud) que la liaison choisie r peut être partagée entre ces LSP. Si ce n'est pas le cas (par exemple, le ratio de partage a atteint le maximum pour cette liaison) et si selon la décision de politique locale, l'allocation d'aucune autre liaison n'est permise pour Q, N DEVRAIT retourner un message PathErr avec le code/sous code d'erreur "Échec du contrôle d'admission/bande passante demandée indisponible" (voir la [RFC2205]). Autrement (si aucune autre liaison n'est disponible) N DEVRAIT retourner un message PathErr avec le nouveau code/sous code d'erreur "Échec du contrôle d'admission/échec d'admission du LSP".

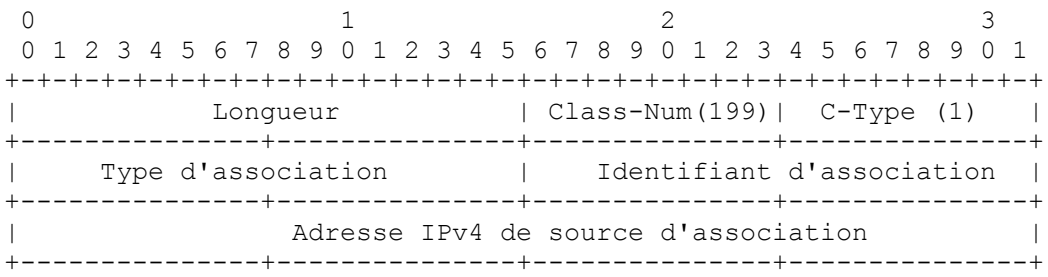
Noter que le processus par lequel m parmi les n ($m \leq n$) PPRO de LSP secondaires de protection peuvent être choisis sur une base locale pour effectuer la comparaison ci-dessus et le choix subséquent de liaison, sort du domaine d'application du présent document.

16. Objet ASSOCIATION

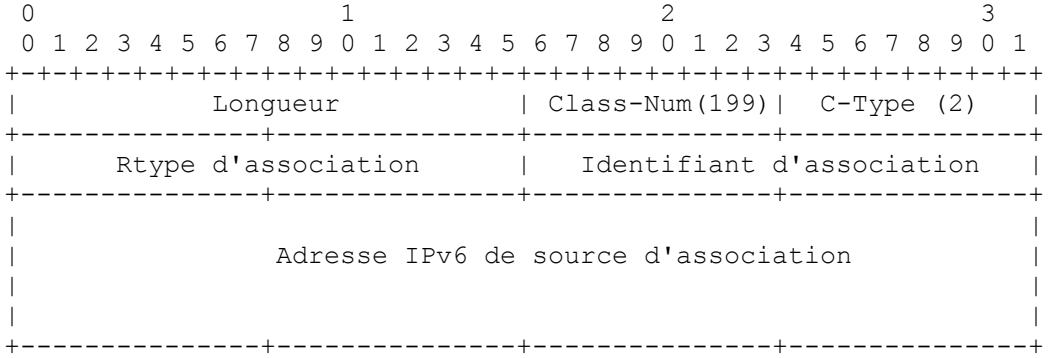
L'objet ASSOCIATION est utilisé pour associer les LSP les uns avec les autres. Dans le contexte de la récupération de LSP de bout en bout, l'association DOIT seulement identifier les LSP qui prennent en charge le même identifiant de tunnel ainsi que la même adresse d'envoyeur de tunnel et l'adresse de point d'extrémité de tunnel. Les champs Type d'association, Source d'association, et Identifiant d'association de l'objet identifient ensemble de façon univoque une association. L'objet utilise un numéro de classe d'objet de la forme11bbbbbb pour assurer la compatibilité avec les nœuds qui ne le prennent pas en charge.

16.1 Format

L'objet IPv4 ASSOCIATION (Class-Num de la forme 11bbbbbb avec la valeur = 199, C-Type = 1) a le format :



L'objet IPv6 ASSOCIATION (Class-Num de forme 11bbbbbb avec valeur = 199, C-Type = 2) a le format :



Type d'association : 16 bits. Indique le type d'association identifiée. Noter que cette valeur est considérée quand on détermine l'association. Les valeurs suivantes sont définies dans le présent document.

Valeur	Type
0	Réservé
1	Récupération (R)

Identifiant d'association : 16 bits. Valeur allouée par l'extrémité de tête du LSP. Quand elle est combinée avec le type d'association et la source de l'association, cette valeur identifie de façon univoque une association.

Adresse de source d'association : 4 ou 16 octets. Une adresse IPv4 ou IPv6, respectivement, associée au nœud qui a généré l'association.

16.2 Traitement

Dans le contexte de la récupération de LSP de bout en bout, l'objet ASSOCIATION est utilisé pour associer une récupération de LSP aux LSP qu'il protège ou un ou des LSP protégés avec son LSP de récupération. L'objet est porté dans les messages Path. Plus d'un objet PEUT être porté dans un seul message Path.

Les nœuds de transit DOIVENT transmettre, sans modification, tout objet ASSOCIATION reçu dans le message Path sortant correspondant.

Un objet ASSOCIATION avec un type d'association réglé à la valeur "Récupération" est utilisé pour identifier une association relative à la récupération de LSP. Tout nœud qui associe un LSP de récupération DOIT insérer un objet ASSOCIATION avec le réglage suivant :

- Le type d'association DOIT être réglé à la valeur "Récupération" dans le message Path du LSP de récupération.
- La source d'association (IPv4/IPv6) DOIT être réglée à l'adresse d'envoyeur du tunnel du LSP protégé.
- L'identifiant d'association DOIT être réglé à l'identifiant de LSP du LSP protégé par ce LSP ou du LSP protégeant ce LSP. Si il n'est pas connu, cette valeur est réglée à sa propre valeur d'identifiant de LSP signalé (par défaut). Aussi, la valeur de l'identifiant d'association PEUT changer durant la vie du LSP.

Les nœuds de terminaison utilisent l'objet ASSOCIATION reçu avec le type d'association réglé à la valeur "Récupération"

pour associer un LSP de récupération avec son LSP actif correspondant. Cette information est utilisée pour lier ensemble les LSP appropriés, actif et de récupération. Ces nœuds DOIVENT s'assurer que les messages Path reçus, incluant le ou les objets ASSOCIATION, sont traités avec les réglages appropriés d'objet PROTECTION, si ils sont présents (voir à la Section 14 le traitement de l'objet PROTECTION). Autrement, ce nœud DOIT retourner un message PathErr avec le nouveau code/sous code d'erreur "Échec d'admission de LSP/mauvais type d'association". De façon similaire, un message Path avec un objet PROTECTION exigeant une association entre le LSP actif et de récupération DOIT inclure un objet ASSOCIATION. Les nœuds de terminaison qui reçoivent de tels message Path sans un objet ASSOCIATION DOIVENT retourner un message PathErr avec le nouveau code/sous code d'erreur "Problème d'acheminement/objet PROTECTION non applicable".

17. Formats de message RSVP mis à jour

Cette Section présente les formats RSVP relatifs aux messages tels que modifiés par le présent document. Les formats de message RSVP non modifiés ne sont pas mentionnés.

Le format d'un message Path est comme suit :

```
<Message Path> ::= <En-tête commun> [ <INTEGRITY> ]
                   [ [<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ... ]
                   [ <MESSAGE_ID> ]
                   <SESSION> <RSVP_HOP>
                   <TIME_VALUES>
                   [ <EXPLICIT_ROUTE> ]
                   <LABEL_REQUEST>
                   [ <PROTECTION> ]
                   [ <LABEL_SET> ... ]
                   [ <SESSION_ATTRIBUTE> ]
                   [ <NOTIFY_REQUEST> ... ]
                   [ <ADMIN_STATUS> ]
                   [ <ASSOCIATION> ... ]
                   [ <PRIMARY_PATH_ROUTE> ... ]
                   [ <POLICY_DATA> ... ]
                   <descripteur d'envoyeur>
```

Le format du <descripteur d'envoyeur> pour les LSP unidirectionnels et bidirectionnels n'est pas modifié par le présent document.

Le format d'un message Resv est le suivant :

```
<Message Resv> ::= <En-tête commun> [ <INTEGRITY> ]
                   [ [<MESSAGE_ID_ACK> | <MESSAGE_ID_NACK>] ... ]
                   [ <MESSAGE_ID> ]
                   <SESSION> <RSVP_HOP>
                   <TIME_VALUES>
                   [ <RESV_CONFIRM> ]  [ <SCOPE> ]
                   [ <PROTECTION> ]
                   [ <NOTIFY_REQUEST> ]
                   [ <ADMIN_STATUS> ]
                   [ <POLICY_DATA> ... ]
                   <STYLE> <liste des descripteurs de flux>
```

<liste des descripteurs de flux> n'est pas modifié par le présent document.

18. Considérations sur la sécurité

Les menaces sur la sécurité identifiées dans la [RFC4426] peuvent être rencontrées à cause de l'échange de messages RSVP et des informations détaillés dans le présent document. Les mécanismes de sécurité suivants s'appliquent .

La signalisation RSVP DOIT être capable de fournir l'authentification et l'intégrité. L'authentification est exigée pour assurer que les messages de signalisation sont générés du bon endroit et n'ont pas été modifiés dans le transit.

À cette fin, la [RFC2747] fournit l'authentification et l'intégrité de message RSVP requise pour les échanges de messages RSVP bond par bond. Pour les échanges de messages RSVP qui ne sont pas bond par bond, l'intégrité et l'authentification standard fondées sur IPsec peuvent être utilisées comme expliqué dans la [RFC3473].

De plus, le présent document utilise l'échange de messages Notify. Cela empêche le modèle d'intégrité et d'authentication bond par bond de RSVP. Dans le cas où le même niveau de sécurité fourni par la [RFC2747] est désiré, l'intégrité et l'authentification standard fondées sur IPsec peuvent être utilisées comme expliqué dans la [RFC3473].

Pour prévenir les conséquences d'une mauvaise protection et le risque accru de mauvaise connexion, en particulier, quand du trafic supplémentaire est impliqué, qui délivrerait le mauvais trafic à la mauvaise destination, des mécanismes spécifiques ont été mis en place comme décrit aux paragraphes 7.2, 8.3, et à la Section 10.

19. Considérations relatives à l'IANA

L'IANA alloue les valeurs des paramètres du protocole RSVP. Dans le document actuel, un objet PROTECTION (nouveau C-Type) un objet PRIMARY_PATH_ROUTE, et un objet ASSOCIATION sont définis. De plus, de nouvelles valeurs de code/sous code d'erreur sont définies dans le présent document. Finalement, l'enregistrement des bits de l'objet ADMIN_STATUS est demandé.

Deux numéros de classe RSVP (Class-Num) et trois valeurs de type de classe (C-Types) doivent être définies par l'IANA dans le registre http://www.iana.org/assignments/rsvp-parameters

1) objet PROTECTION (défini au paragraphe 14.1) : Class-Num = 37 ; Type 2 : C-Type = 2

2) objet PRIMARY_PATH_ROUTE (défini au paragraphe 15.1) : Class-Num = 38 (de forme 0bbbbbbb),
Primary Path Route : C-Type = 1

3) objet ASSOCIATION (défini au paragraphe 16.1) : Class-Num = 199 (de forme 11bbbbbb)
- Association IPv4 : C-Type = 1
- Association IPv6 : C-Type = 2
Type d'association : les valeurs suivantes définies pour le champ Type d'association (16 bits) de l'objet ASSOCIATION.

Valeur	**Type**
0	Réservé
1	Récupération (R)

L'allocation de valeurs (de 2 à 65535) par l'IANA est soumise au processus de revue par expert de l'IETF, c'est-à-dire, dans une RFC de l'IETF sur la voie de la normalisation.

4) Valeurs de code/sous code d'erreur. Les valeurs suivantes de code/sous code d'erreur sont définies dans le présent document :

Code d'erreur = 01 : "Échec de contrôle d'admission" (voir la [RFC2205])
o "Échec de contrôle d'admission/échec d'admission de LSP" (4)
o "Échec de contrôle d'admission/mauvais type d'association" (5)

Code d'erreur = 02: "Échec de contrôle de politique" (voir la [RFC2205])
o "Défaillance de contrôle de politique/Difficile à préempter" (20)

Code d'erreur = 24: "Problème d'acheminement" (voir la [RFC3209])
o "Problème d'acheminement/Protection de LSP non prise en charge" (17)
o "Problème d'acheminement/objet PROTECTION non applicable" (18)
o "Problème d'acheminement/mauvais objet PRIMARY_PATH_ROUTE" (19)
o "Problème d'acheminement/objet PRIMARY_PATH_ROUTE non applicable" (20)

Code d'erreur = 25: "Notification d'erreur" (voir la [RFC3209])
o "Notification d'erreur/défaillance du LSP" (9)
o "Notification d'erreur/LSP Récupéré" (10)
o "Notification d'erreur/échec local du LSP" (11)

5) Enregistrement des bits de l'objet ADMIN_STATUS :
L'objet ADMIN_STATUS (Class-Num = 196, C-Type = 1) est défini dans la [RFC3473].

Il est aussi demandé à l'IANA de garder trace des bits de ADMIN_STATUS étendus par le présent document. À cette fin, des nouvelles entrées du registre ont été créées à http://www.iana.org/assignments/gmpls-sig-parameters

- Bits de ADMIN_STATUS :

Nom : bits de ADMIN_STATUS
Format : vecteur de 32 bits de bits Position :
[0] Bit Reflet (R) défini dans la [RFC3471].
[1..25] À allouer par l'IANA via action de normalisation de l'IETF par RFC sur la voie de la normalisation.
[26] Bit Verrouillage (L) défini à la Section 13.
[27] Bit Inhibition de communication d'alarme (I) dans la [RFC4783]
[28] Bit Contrôle d'appel (C) défini dans la [RFC4974]
[29] Bit Essai (T) défini dans la [RFC3471]
[30] Bit Administrativement mort (A) défini dans la [RFC3471]
[31] Bit Suppression en cours (D) défini dans la [RFC3471]

20. Remerciements

Les auteurs tiennent à remercier John Drake pour sa collaboration active, Adrian Farrel pour ses contributions au présent document (en particulier, aux Sections 10 et 11) et sa relcture attentive du document, Bart Rousseau (pour ses corrections rédactionnelles) Dominique Verchere, et Stefaan De Cnodder. Merci aussi à Ichiro Inoue pour ses précieux commentaires.

Les auteurs tiennent aussi à remercier Lou Berger du temps et des efforts qu'il a prodigué avec l'équipe de conception, en contribuant au présent document.

21. Références

21.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495, RFC6780)) *(P.S.)*

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

[RFC2961] L. Berger et autres, "Extensions de réduction de redondance de rafraîchissement pour RSVP", avril 2001. (*MàJ par* RFC5063) *(P.S.)*

[RFC3209] D. Awduche, et autres, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (*Mise à jour par* RFC3936, RFC4420, RFC4874, RFC5151, RFC5420, RFC6790)

[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.)*

[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.)*

[RFC3945] E. Mannie, éd., "Architecture de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", octobre 2004. *(P.S.)*

[RFC4426] J. Lang et autres, "Spécification fonctionnelle de récupération du protocole généralisé de commutation d'étiquettes multiprotocoles (GMPLS)", mars 2006. *(P.S.)*

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

21.2 Références pour information

[G.841] Recommandation UIT-T G.841, "Types et caractéristiques des architectures de protection de réseau SDH", octobre 1998. Disponible à http://www.itu.int/rec/T-REC-G.841-199810-1 .

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