Groupe de travail Réseau
Request for Comments : 4920
Catégorie : Sur la voie de la normalisation

A. Farrel, éd., Old Dog Consulting
A. Satyanarayana, Cisco Systems, Inc.
A. Iwata, NEC Corporation
N. Fujita, NEC Corporation
G. Ash, AT&T

Traduction Claude Brière de L'Isle
juillet 2007

Extensions de signalisation de retour arrière pour RSVP-TE sur MPLS et GMPLS

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "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 4480 et 1460)

Notice de copyright
Copyright (C) The IETF Trust (2007).

Résumé
Dans un environnement d'acheminement réparti fondé sur la contrainte, les informations utilisées pour calculer un chemin peuvent être périmées. Cela signifie que les demandes d'établissement de chemin de commutation d'étiquettes (LSP, *Label Switched Path*) d'ingénierie du trafic (TE, *Traffic Engineered*) de commutation d'étiquettes multi protocoles (MPLS, *Multiprotocol Label Switching*) et de MPLS généralisé (GMPLS, *Generalized MPLS*) peuvent être bloquées par des liaisons ou des nœuds qui n'ont pas des ressources suffisantes. Le retour arrière *(Crankback)* est un schéma dans lequel les informations d'échec d'établissement sont retournées du point de défaillance pour permettre de nouvelles tentatives d'établissement en évitant les ressources bloquées. le retour arrière peut aussi être appliqué à la récupération de LSP pour indiquer la localisation de la liaison ou nœud défaillant.

Le présent document spécifie les extensions de signalisation de retour arrière à utiliser dans la signalisation MPLS en utilisant RSVP-TE comme défini dans "RSVP-TE : Extensions à RSVP pour les LSP tunnels", RFC 3209, et la signalisation GMPLS comme définie dans "Description fonctionnelle de la signalisation de la commuatation d'étiquettes multi protocoles généralisée (GMPLS)", RFC 3471. Ces extensions signifient que la demande d'établissement de LSP peut être reessayée sur un chemin de remplacement qui contourne les liaisons ou nœuds bloqués. Cela offre des améliorations significatives aux ratios d'établissement et de récupération réussis pour les LSP, en particulier dans les situations où un grand nombre de demandes d'établissement sont déclenchées en même temps.

Table des matières

1. Introduction et cadre

1.1 Fondements

RSVP-TE (Extensions RSVP pour tunnels LSP) [RFC3209] peut être utilisé pour établir des LSP à acheminement explicite dans un réseau MPLS. En utilisant RSVP-TE, des ressources peuvent aussi être réservées le long d'un chemin pour garantir et/ou contrôler la qualité de service pour le trafic porté sur le LSP. Pour concevoir un chemin explicite qui satisfasse des garanties de qualité de service (QS) il est nécessaire de discerner les ressources disponibles pour chaque liaison ou nœud dans le réseau. Pour la collecte de telles informations de ressources, les protocoles d'acheminement, tels que OSPF et de système intermédiaire à système intermédiaire (IS-IS) peuvent être étendus pour distribuer des informations d'état supplémentaires [RFC2702].

Les chemins explicites peuvent être calculés sur la base des informations distribuées au LSR (entrée) qui initie un LSP et signalés comme des chemins explicites durant l'établissement du LSP. Les chemins explicites peuvent contenir des "bonds lâches" et des "nœuds" qui portent l'acheminement à travers une collection de nœuds. Ce mécanisme peut être utilisé pour confier une partie du calcul de chemin aux nœuds intermédiaire comme des LSR de bordure de zone.

Dans un environnement d'acheminement réparti, les informations de ressources utilisées pour calculer un chemin fondé sur la contrainte peuvent cependant être périmées. Cela signifie qu'une demande d'établissement peut être bloquée, par exemple, parce que une liaison ou un nœud le long du chemin choisi a des ressources insuffisantes.

Dans RSVP-TE, un établissement de LSP bloqué peut résulter en un message PathErr envoyé à l'entrée, ou un ResvErr envoyé à la sortie (terminaison). Ces messages peuvent résulter en l'abandon de l'établissement de LSP. Dans MPLS généralisé [RFC3473] le message Notify peut de plus être utilisé pour expédier des notifications de défaillances des LSP existants aux LSR d'entrée et de sortie, ou à un "point de réparation" spécifique -- un LSR chargé d'effectuer la protection ou la restauration.

Ces mécanismes existants fournissent une certaine quantité d'informations sur le chemin du LSP défaillant.

MPLS généralisé [RFC3471] et [RFC3473] étend MPLS dans les réseaux qui gèrent des ressources de couche 2, de multiplexage temporel et lambda ainsi que des ressources de paquets. Donc, l'acheminement de retour arrière est aussi utile dans les réseaux GMPLS.

Dans un réseau sans convertisseur de longueur d'onde, les demandes d'établissement vont probablement être bloquées plus souvent que dans un environnement MPLS conventionnel parce que la même longueur d'onde doit être allouée à chaque interconnexion optique sur un chemin explicite de bout en bout. Cela rend l'acheminement de retour arrière des plus importants dans certains réseaux GMPLS.

1.2 Séparation du plan de contrôle et du plan des données

Dans le présent document, les processus et techniques sont décrits comme si les éléments de plan de contrôle et de plan des données qui constituent le cœur d'un routeur de commutation d'étiquette (LSR, *Label Switching Router*) étaient en relation biunivoque. Ceci est seulement à des fins documentaires.

On devrait noter que les LSR GMPLS peuvent être décomposés de telle façon que les composants du plan de contrôle ne soient pas physiquement co-localisés. De plus, une présence dans le plan de contrôle peut contrôler plus d'un LSR dans le plan des données. Ces points ont plusieurs conséquences dans le présent document :

- o les nœuds, liaisons, et ressources qui sont rapportés comme en erreur, sont des entités du plan des données ;
- o les nœuds, zones, et systèmes autonomes (AS, *Autonomous System*) qui rapportent qu'ils ont tenté le réacheminement sont des entités du plan de contrôle ;
- o lorsque une seule entité de plan de contrôle est responsable de plus d'un LSR du plan des données, la signalisation de retour arrière peut être implicite tout comme peut l'être la signalisation de l'établissement d'un LSP.

Les points ci-dessus peuvent être considérés comme évidents, mais sont déclarés ici pour être absolument clair.

L'artifice stylistique consistant à se référer à l'élément du plan de contrôle chargé d'un seul LSR et du composant de plan de données de ce LSR simplement comme "le LSR" ne devrait pas être pris comme signifiant que le présent document n'est applicable qu'à une relation collocalisée biunivoque. De plus, dans la majorité des cas, les composants de plan de contrôle et de plan des données sont en rapport dans un ratio de 1:1 et sont généralement co-localisés.

1.3 Réparation et récupération

Si le LSR d'entrée ou le LSR intermédiaire de zone bordure connaît la localisation de la liaison ou nœud bloqué, il peut désigner un chemin de remplacement et réitérer alors la demande d'établissement. La détermination de l'identité de la liaison ou nœud bloqué peut être réalisée par le mécanisme connu comme acheminement de retour arrière [PNNI], [ASH1]. Dans RSVP-TE, la signalisation de retour arrière exige de notifier au LSR amont la localisation de la liaison ou nœud bloqué. Dans certains cas, cela exige plus d'informations qu'il n'est actuellement disponible dans les protocoles de signalisation.

Par ailleurs, divers schémas de récupération pour les défaillances de liaison ou nœud ont été proposés dans la [RFC3469] et incluent le réacheminement rapide. Ces schémas s'appuient sur l'existence d'un LSP de protection pour protéger le LSP actif, mais si les deux chemins, actif et de protection sont défaillants, il est nécessaire de rétablir le LSP de bout en bout, en évitant les défaillances connues. De même, le réacheminement rapide par l'établissement d'un chemin de récupération à la demande après une défaillance exige le calcul d'un nouveau LSP qui évite les défaillances connues. La récupération de bout en bout pour l'acheminement de remplacement exige la localisation de la liaison ou nœud défaillant. Les schémas d'acheminement de retour arrière pourraient être utilisés pour notifier les LSR en amont de la localisation de la défaillance.

De plus, dans les situations où de nombreuses défaillances de liaison ou nœud se produisent en même temps, la différence entre les informations d'acheminement distribuées et l'état du réseau en temps réel devient très supérieure à ce qu'elle est dans les établissements normaux de LSP. La récupération de LSP pourrait donc être effectuée avec des informations inappropriées, ce qui va probablement causer le blocage de l'établissement. L'acheminement de retour arrière pourrait améliorer la récupération de la défaillance dans ces situations.

L'exigence d'allocation de bout en bout des ressources lambda dans les réseaux GMPLS sans convertisseur de longueur d'onde signifie que la récupération de bout en bout peut être le seul moyen de récupérer des défaillances de LSP. C'est parce que la protection de segment peut être beaucoup plus difficile à réaliser dans les réseaux d'interconnexion photonique où un lambda particulier peut être déjà en usage sur d'autres liaisons : la protection de bout en bout offre le choix d'utiliser un autre lambda, mais ce choix n'est pas disponible dans la protection de segment.

Cette exigence rend le réacheminement de retour arrière particulièrement utile dans un réseau GMPLS, en particulier dans les cas de réacheminement dynamique de LSP (c'est-à-dire, quand il n'y a pas de pré établissement du LSP protecteur).

1.4. Interaction avec les mécanismes d'arrosage TE

GMPLS utilise les protocoles de passerelle intérieure (IGP, *Interior Gateway Protocol*) (OSPF et IS-IS) pour arroser les informations d'ingénierie du trafic (TE, *traffic engineering*) qui sont utilisées pour construire une base de données d'ingénierie du trafic (TED, *traffic engineering database*) qui agit comme source des données pour le calcul de chemin.

La signalisation de retour arrière n'est pas destinée à compléter ou remplacer le fonctionnement normal du mécanisme d'arrosage TE, car ces mécanismes sont indépendants l'un de l'autre. C'est-à-dire que les informations rassemblées par la signalisation de retour arrière peuvent être appliquées pour calculer un chemin de remplacement pour le LSP pour lequel les informations ont été signalées, mais les informations ne sont pas destinées à être utilisées pour influencer le calcul des chemins des autres LSP.

Toute exigence d'arroser rapidement les mises à jour sur les ressources disponibles afin qu'elles puissent être appliquées comme des deltas à la TED et utilisées dans les futurs calculs de chemin sort du domaine d'application du présent document.

1.5 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Discussion : Indications de réacheminement explicites ou implicites

Il y a eu des problèmes dans les réseaux de fournisseurs de services quand ils déduisent à partir d'informations indirectes que le réacheminement est permis. Le présent document propose l'utilisation d'une indication explicite de réacheminement qui autorise le réacheminement, et contraste avec l'indication déduite ou implicite de réacheminement qui était utilisée précédemment.

Diverses options et échanges de protocoles existants, incluant les valeurs d'erreur de message PathErr [RFC2205], [RFC3209] et de message Notify [RFC3473], permettent à une mise en œuvre de créer une situation où le réacheminement peut être effectué. Cela permet de récupérer d'erreurs du réseau ou de concurrence de ressources.

Cependant, une telle induction de signalisation de récupération n'est pas toujours souhaitable car elle peut être vouée à l'échec. Par exemple, l'expérience de l'utilisation de messages de libération dans les réseaux fondés sur le multiplexage par répartition dans le temps (TDM, *Time Division Multiplexing*) pour les besoins d'indications de réacheminement analogique implicite et explicite donne quelques lignes directrices. Ces informations sur les fondements sont données dans l'Appendice A.

Il est certain qu'avec la distribution des informations de topologie, telle qu'effectuée avec des protocoles d'acheminement comme OSPF, le LSR d'entrée pourrait en déduire la condition de réacheminement. Cependant, la convergence des informations de topologie en utilisant les protocoles d'acheminement est normalement plus lente que les temps d'établissement de LSP attendus. Une des raisons du retour arrière est d'éviter les frais généraux de l'arrosage de bande passante de liaison disponible, et d'utiliser plus efficacment les informations d'état local pour diriger l'acheminement de remplacement au point de calcul de chemin.

[ASH1] montre comment l'acheminement dépendant de l'événement peut juste utiliser le retour arrière, et pas l'arrosage de bande passante de liaison disponible, pour décider du chemin de réacheminement dans le réseau par des "modèles d'apprentissage". Réduire cet arrosage réduit lesfrais généraux et peut conduire à la capacité de prendre en charge des tailles d'AS beaucoup plus grandes.

Donc, l'utilisation de l'acheminement de remplacement devrait se fonder sur une indication explicite, et le mieux est de connaître séparément les informations suivantes :
- où le blocage/encombrement s'est produit ;
- si l'acheminement de remplacement "devrait" être tenté.

3. Fonctionnement requis

La Section 1 identifie certaines des circonstances où le retour arrière peut être utile. L'acheminement de retour arrière est effectué comme décrit dans les procédures qui suivent, quand une demande d'établissement de LSP est bloquée sur le chemin ou quand un LSP existant a une défaillance.

3.1 Échec ou indisponibilité de ressource

Quand une demande d'établissement de LSP est bloquée à cause de ressources indisponibles, un message de réponse d'erreur avec l'identifiant de localisation du blocage devrait être retourné au LSR initiateur de l'établissement du LSP (LSR d'entrée) au LSR de bordure de zone, au LSR de bordure d'AS, ou à quelque autre point de réparation.

Ce message d'erreur porte une spécification d'erreur en accord avec la [RFC3209] -- cela indique la cause de l'erreur et le nœud/liaison où l'erreur s'est produite. L'opération de retour arrière peut exiger plus d'informations comme indiqué au paragraphe 3.2.1 et à la Section 6.

Un point de réparation (par exemple, un LSR d'entrée) qui reçoit des informations de retour arrière résultant de la défaillance d'un LSP établi peut appliquer la politique locale pour décider comment il tente de réparer le LSP. Par exemple, il peut attribuer des priorités aux tentatives de réparation entre plusieurs LSP défaillants, et il peut considérer les LSP qui ont été réparés en local ([RFC4090]) comme étant des candidats moins urgents pour une réparation de bout en bout. De plus, il est probable que d'autres LSR sont aussi en train de tenter la réparation du LSP pour les LSP affectés par la même faute ce qui peut donner lieu à des conflits de ressources au sein du réseau, de sorte qu'un LSR peut échelonner ses tentatives de réparation afin de réduire les chances de compétition pour les ressources.

3.2 Calcul d'un chemin de remplacement

Dans un réseau plat sans partition de la topologie d'acheminement, quand le LSR d'entrée reçoit le message d'erreur, il calcule un chemin de remplacement contournant la liaison ou nœud bloqué pour satisfaire les garanties de qualité de service en utilisant les informations d'état de liaison sur le réseau. Si un chemin de remplacement est trouvé, une nouvelle demande d'établissement de LSP est envoyée sur ce chemin.

Par ailleurs, dans un réseau partitionné en zones comme avec OSPF, le LSR de bordure de zone peut intercepter et terminer la réponse d'erreur, et effectuer le (ré)acheminement de remplacement au sein de la zone en aval.

Dans un troisième scénario, tout nœud dans une zone peut agir comme un point de réparation. Dans ce cas, chaque LSR se comporte un peu comme un LSR de bordure de zone, comme décrit ci-dessus. Il peut intercepter et terminer la réponse d'erreur et effectuer l'acheminement de remplacement. Ceci peut être particulièrement utile lorsque des domaines de calcul sont appliqués au sein du réseau (partitionné) où de tels domains ne coincident pas avec les frontières de partition d'acheminement. Cependant si tous les nœuds dans le réseau effectuent le réacheminement, il est possible de dépenser des ressources excessives de réseau et de CPU à des tentatives de réacheminement qui seraient mieux utilisées en étant faites à des nœuds de réacheminement désignés. Ce scénario est un peu comme le "réacheminement rapide MPLS" de la [RFC4090], dans lequel tout nœud du domaine MPLS peut établir une "réparation locale" de LSP en cas de notification de défaillance.

3.2.1 Informations requises pour le réacheminement

Afin de calculer correctement un chemin qui évite le problème de blocage, un LSR de point de réparation doit collecter autant d'informations de retour arrière que possible. Idéalement, le nœud de réparation va obtenir le nœud, la liaison, et la raison de la défaillance.

La raison de la défaillance peut fournir un facteur de discrimination important pour aider à décider quelle action devrait être prise. Par exemple, une défaillance qui indique "Pas de chemin pour cette destination" va probablement donner lieu à un nouveau calcul de chemin excluant le LSR rapporteur, mais la raison "Encombrement temporaire du plan de contrôle" pourrait conduire à un nouvel essai après une attente convenable.

Cependant, même cette information peut n'être pas suffisante pour aider à un nouveau calcul. Considérons par exemple un chemin explicite qui contient un nœud abstrait ou bond lâche non explicite. Dans ce cas, le nœud et la liaison défaillants ne sont pas nécessairement suffisants pour dire au point de réparation quel bond dans le chemin explicite est défaillant. Les

informations de retour arrière doivent indiquer où, dans le chemin explicite, s'est produit le problème.

3.2.2 Signalisation d'un nouveau chemin

Si les informations de retour arrière peuvent être utilisées pour calculer un nouveau chemin évitant les ressources de réseau défaillantes/bloquantes, le chemin peut être signalé comme chemin explicite.

Cependant, il se peut que le point de réparation n'ait pas des informations de topologie suffisantes pour calculer un chemin explicite dont il soit garanti qu'il évite la liaison ou nœud défaillant. Dans ce cas, les exclusions de chemin de la [RFC4874] peuvent être particulièrement utiles. Pour réaliser cela, la [RFC4874] permet que les informations de retour arrière soient présentées comme des exclusions de chemin pour forcer l'évitement du nœud, liaison, ou ressource, défaillant.

3.3 Persistence des informations d'erreur

Le LSR de point de réparation qui calcule le chemin de remplacement devrait mémoriser les identifiants de localisation des blocages indiqués dans le message d'erreur jusqu'à ce que le LSP soit bien établi par les LSR en aval ou jusqu'à ce que le LSR de point de réparation abandonne les tentatives de réacheminement. Comme les informations de signalisation de retour arrière peuvent être retournées au même LSR de point de réparation plus d'une fois lors de l'établissement d'un LSP spécifique, le LSR de point de réparation DEVRAIT conserver un tableau de l'historique de tous les blocages rencontrés pour ce LSP (au moins jusqu'à ce que le protocole d'acheminement mette à jour l'état de ces informations) afin que le ou les claculs de chemin résultants puissent contourner tous les points de blocage.

Si une seconde réponse d'erreur est reçue par un point de réparation (pendant qu'il effectue un réacheminement de retour arrière) il devrait mettre à jour le tableau historique qui fait la liste de tous les blocages rencontrés, et utiliser toutes les informations rassemblées quand il fait une autre tentative de réacheminement.

Noter que l'objet du tableau historique est de corréler les informations quand des tentatives répétées d'essais sont faites par le même LSR. Par exemple, supposons qu'une tentative soit faite d'acheminer de A par B, et que B retourne un échec avec des informations de retour arrière, une tentative peut être faite pour acheminer à partir de A à travers C, et cela peut aussi échouer avec le retour d'informations de retour arrière. La tentative suivante NE DEVRAIT PAS être d'acheminer de A par B, et cela peut être réalisé en utilisant le tableau historique.

Le tableau historique peut être éliminé par le contrôleur de signalisation pour A si le LSP est bien établi à travers A. Le tableau historique PEUT être conservé après que le contrôleur de signalisation pour A a envoyé une erreur en amont, cependant la valeur que cela fournit est discutable car un futur essai par suite d'un réacheminement de retour arrière ne devrait pas tenter d'acheminer par A. Si les informations d'historique sont conservées pendant une plus longue période, elles DEVRAIENT être éliminées après l'expiration d'un temporisateur local. Ce temporisateur est exigé afin que le point de réparation n'applique pas le tableau historique à une tentative par l'entrée de rétablir un LSP défaillant, mais pour permettre que le tableau historique soit disponible pour l'utiliser dans des tentatives de réacheminement avant que l'entrée déclare que le LSP est défaillant.

Il est RECOMMANDÉ que le LSR de point de réparation élimine le tableau historique en utilisant un temporisateur pas plus long que le temporisateur de réessai de LSP configuré sur le LSR d'entrée. La corrélation des temporisateurs entre les LSR d'entrée et de point de réparation est normalement faite par la configuration manuelle des temporisateurs locaux de chaque LSR, et sort du domaine d'application du présent document.

Les informations dans le tableau historique ne sont pas destinées à compléter la TED pour le calcul des chemins des autres LSP.

3.4 Traitement d'un échec de réacheminement

Plusieurs blocages (pour le même LSP) peuvent survenir, et des tentatives successives d'essai d'établissement peuvent échouer. Conserver les informations d'erreur provenant des tentatives précédentes assure qu'il n'y a pas d'avalanche de tentaitves d'établissement, et la connaissance des blocages augmente à chaque tentative.

Il se peut qu'après plusieurs essais, un certain point de réparation soit incapable de calculer un chemin pour la destination (c'est-à-dire, la sortie du LSP) qui évite tous les blocages. Dans ce cas, il doit passer un message d'indication d'erreur en amont. Cela est très utile pour les nœuds en amont (et en particulier au LSR d'entrée) qui peuvent réparer des points pour l'établissement de LSP, si le message d'indication d'erreur identifie tous les blocages en aval et aussi le point de réparation

qui a été incapable de calculer un chemin de remplacement.

3.5 Limitation des tentatives de réacheminement

Il est important d'empêcher la répétition sans fin des tentatives d'établissement de LSP en utilisant les informations d'acheminement de retour arrière après que des conditions d'erreur sont signalées, ou durant des périodes de fort encombrement. Il peut aussi être utile de réduire le nombre d'essais, car les échecs d'essais vont augmenter la latence d'établissement et dégrader les performances en augmentant la quantité de traitement de signalisation et d'échange de messages au sein du réseau.

Le nombre maximum de tentatives de réacheminement de retour arrière permises peut être limité de diverses façons. Le présent document permet à un LSR de limiter les essais par LSP, et suppose qu'une telle limite va être appliquée soit comme configuration par nœud pour les LSR quit sont capables de réacheminement, soit comme une valeur de configuration à l'échelle du réseau.

Quand le nombre d'essais d'un certain LSR est dépassé, le LSR va rapporter la défaillance vers l'amont jusqu'à ce qu'il atteigne le prochain point de réparation où d'autres tentatives de réacheminement peuvent être tentées, ou qu'il atteigne l'entrée où il peut agir comme point de réparation, ou déclarer le LSP défaillant. Il est important que les informations de retour arrière que cela fournit indiquent que l'acheminement de retour par ce nœud ne va pas réussir ; cette situation est similaire à celle du paragraphe 3.4.

4. Prise en charge du protocole existant pour le réacheminement de retour arrière

Le réacheminement de retour arrière est approprié pour être utilisé avec RSVP-TE.

1) L'établissement de LSP peut échouer à cause d'une incapacité d'acheminement, peut-être parce que les liaisons sont désactivées. Dans ce cas, un message PathErr est retourné à l'entrée.

2) L'établissement de LSP peut échouer parce que les ressources sont indisponibles. Ceci est particulièrement pertinent dans GMPLS où le contrôle explicite d'étiquettes peut être utilisé. Là encore, un message PathErr est retourné à l'entrée.

3) La réservation de ressource peut échouer durant l'établissement de LSP, lorsque le message Resv est traité. Si les ressources ne sont pas disponibles sur la liaison demandée ou à un nœud spécifique, un message ResvErr est retourné au nœud de sortie indiquant "défaillance de contrôle d'admission" [RFC2205]. Il est permis à la sortie de changer la FLOWSPEC et d'essayer encore, mais dans le cas où ce n'est pas praticable ou pas accepté (en particulier dans le contexte non PSC) le LSR de sortie peut choisir d'effectuer une des actions suivantes ;
   - Ignorer la situation et permettre que la récupération se fasse par un message de rafraîchissement de chemin et un rafraîchissement de temporisation [RFC2205].
   - Envoyer un message PathErr à l'entrée en indiquant "Défaillance de contrôle d'admission".

   Noter que dans les réseaux multi zones/AS, le message ResvErr pourrait être intercepté et traité dans un routeur de bordure de zone/AS.

4) Il est aussi possible de faire des réservations de ressources sur le chemin de transmission lorsque le message Path est traité. Ce choix est compatible avec l'établissement de LSP dans les réseaux GMPLS [RFC3471], [RFC3473]. Dans ce cas, si les ressources ne sont pas disponibles, un message PathErr est retourné à l'entrée indiquant "Défaillance de contrôle d'admission".

Les informations de retour arrière vont être utiles à un nœud en amont (comme l'entrée) si elles sont fournies sur un message PathErr ou Notify qui est envoyé en amont.

4.1 RSVP-TE

Dans RSVP-TE, un échec de tentative d'établissement de LSP résulte en un message PathErr retourné en amont. Le message PathErr porte un objet ERROR_SPEC, qui indique le nœud ou interface qui rapporte l'erreur et la raison de la défaillance.

Le réacheminement de retour arrière peut être effectué explicitement, en évitant le nœud ou interface rapporté.

4.2 GMPLS-RSVP-TE

GMPLS étend le rapport d'erreur décrit ci-dessus en permettant aux LSR de rapporter l'interface en erreur en plus de l'identité du nœud qui rapporte l'erreur. Cela améliore encore la capacité de recalculer du nœud pour acheminer en contournant l'erreur.

GMPLS introduit un message Notify ciblé qui peut être utilisé pour rapporter les défaillances de LSP dirigées sur un nœud choisi. Ce message porte les mêmes facilités de rapport d'erreur que décrites ci-dessus. Le message Notify peut être utilisé pour expédier la propagation des notifications d'erreur, mais dans un réseau qui offre l'acheminement de retour arrière à plusieurs nœuds, il va y avoir besoin d'un accord entre les LSR sur si un PathErr ou un Notify fournit le stimulus pour l'opération de retour arrière. Cet accord est contraint par le choix du comportement de réacheminement (selon la liste du paragraphe 5.4). Autrement, plusieurs nœuds pourraient tenter de réparer le LSP en même temps, parce que :
1) ces messages peuvent s'écouler sur des chemins différents avant d'atteindre le LSR d'entrée, et
2) la destination du message Notify pourrait n'être pas le LSR d'entrée.

5. Contrôle des opérations de retour arrière

5.1. Demande de retour arrière et contrôle de réacheminement dans le réseau

Quand est faite une demande d'établissement d'un LSP tunnel, le LSR d'entrée devrait spécifier si il veut que des informations de retour arrière soient collectées en cas de défaillance, et si il demande des tentatives de réacheminement par un ou des nœuds intermédiaires spécifiques. À cette fin, un champ Fanions de réacheminement est ajouté aux messages de protocole de demande d'établissement. Les valeurs correspondantes sont mutuellement exclusives.

Pas de réacheminement : le nœud d'entrée PEUT tenter un réacheminement après défaillance. Les nœuds intermédiaires NE DEVRAIENT PAS tenter de réacheminement après défaillance. Les nœuds qui détectent des défaillances DOIVENT rapporter une erreur et PEUVENT fournir des informations de retour arrière. C'est l'option par défaut et elle est rétro compatible.

Réacheminement de bout en bout : le nœud d'entrée PEUT tenter le réacheminement après défaillance. Les nœuds intermédiaires NE DEVRAIENT PAS tenter de réacheminement après défaillance. Les nœuds qui détectent des défaillances DOIVENT rapporter une erreur et PEUVENT fournir des informations de retour arrière.

Réacheminement de frontière : les nœuds intermédiaires NE PEUVENT tenter le réacheminement après défaillance que si ils sont des routeurs de bordure de zone ou des routeurs de bordure d'AS (ABR/ASBR, *Area Border Router/AS Border Router*). L'ABR/ASBR peut décider de transmettre le message d'erreur en amont au LSR d'entrée ou essayer de choisir un autre LSR de frontière de sortie. Les autres nœuds intermédiaires NE DEVRAIENT PAS tenter de réacheminement. Les nœuds qui détectent des défaillances DOIVENT rapporter une erreur et DEVRAIENT fournir des informations de retour arrière.

Réacheminement fondé sur le segment : tout nœud PEUT tenter le réacheminement après avoir reçu un rapport d'erreur et avant de passer le rapport d'erreur plus en amont. Les nœuds qui détectent des défaillances DOIVENT rapporter une erreur et DEVRAIENT founir des informations de retour arrière complètes.

5.2 Action sur détection d'échec

Un nœud qui détecte la défaillance d'établissement d'un LSP ou la défaillance d'un LSP établi DEVRAIT agir en accord avec le fanion Réacheminement passé sur la demande d'établissement de LSP.

Si le réacheminement fondé sur le segment est permis, ou si le réacheminement de frontière est permis et que le nœud qui détecte est un ABR ou un ASBR, le nœud qui détecte PEUT tenter immédiatement de réacheminer.

Si le réacheminement de bout en bout est indiqué, ou si le réacheminement fondé sur le segment ou le réacheminement de frontière est permis et si le nœud qui détecte choisit de ne pas faire de tentative de réacheminement (ou a épuisé toutes les tentatives possibles de réacheminement) le nœud détecteur DOIT retourner une indication d'erreur de protocole et DEVRAIT inclure des informations de retour arrière complètes.

5.3 Limitation des tentatives de réacheminement

Chaque point de réparation DEVRAIT appliquer une limite configurable en local au nombre de tentatives de réacheminement d'un LSP. Cela aide à empêcher un usage excessif du réseau en cas de fautes significatives, et permet le repli sur d'autres point de réparation qui peuvent avoir de meilleures chances de contourner le problème.

5.3.1 Nouveaux codes d'état pour le réacheminement

Un code/valeur d'erreur de "Problème d'acheminement"/"Limite de réacheminement excédée" (24/22) est utilisé pour identifier qu'un nœud a abandonné le réacheminement de retour arrière parce que il a atteint un seuil des tentatives d'essais de réacheminement.

Un nœud qui reçoit une réponse d'erreur avec ce code d'état PEUT aussi tenter un réacheminement de retour arrière, mais il est RECOMMANDÉque ces tentatives soient limitées au LSR d'entrée.

5.4 Contrôle par le protocole du comportement de réacheminement

L'objet LSP_ATTRIBUTES défini dans la [RFC4420] est utilisé sur les messages Path pour porter le fanion Réacheminement décrit au paragraphe 4.1. Trois bits sont définis pour être inclus dans la TLV Attributs de LSP, comme suit. Les numéros de bit ci-dessous ont été alloués par l'IANA.

Numéro de bit	Nom et usage
1	Réacheminement de bout en bout désiré. Ce fanion indique le comportement de réacheminement de bout en bout pour un LSP en cours d'établissement. Cela PEUT aussi être utilisé pour spécifier le comportement de récupération de bout en bout de LSP pour des LSP établis.
2	Réacheminement de frontière désiré. Ce fanion indique le comportement de réacheminement de frontière pour un LSP en cours d'établissement. Cela PEUT aussi être utilisé pour spécifier la récupération de LSP fondée sur le segment par un retour arrière incorporé pour des LSP établis. Le ABR/ASBR peut décider de transmettre le message PathErr en amont à un ABR/ASBR en amont ou au LSR d'entrée. Autrement, il peut essayer de choisir un autre LSR frontière de sortie.
3	Réacheminement fondé sur le segment désiré. Ce fanion indique le comportement de réacheminement fondé sur le segment pour un LSP en cours d'établissement. Ceci PEUT aussi être utilisé pour spécifier la récupération de LSP fondée sur le segment pour des LSP établis.

6. Rapport des informations de retour arrière

6.1 Informations requises

Comme décrit ci-dessus, des informations de retour arrière complètes DEVRAIENT indiquer le nœud, la liaison, et les autres ressources, qui ont été tentés mais ont échoué à cause de problèmes d'allocation ou de défaillance du réseau.

Les informations de retour arrière par défaut DEVRAIENT inclure l'adresse de l'interface et du nœud.

Toute adresse rapportée dans de telles informations de retour arrière DEVRAIT être une adresse qui a été distribuée par les protocoles d'acheminement (OSPF et IS-IS) dans leurs annonces d'état de liaison TE. Cependant, des informations supplémentaires comme les identifiants de liaisons composantes s'y ajoutent.

6.2 Extensions au protocole

La [RFC3473] définit un objet ERROR_SPEC IF_ID qui peut être utilisé sur les messages PathErr, ResvErr et Notify pour convoyer les informations portées dans l'objet Error Spec défini dans la [RFC3209]. De plus, l'objet ERROR_SPEC IF_ID a la portée pour porter les TLV qui identifient la liaison associée à l'erreur.

Les TLV à utiliser avec cet objet sont définies dans la [RFC3471], et leur liste figure ci-dessous. Elles sont utilisées en deux endroits. Dans l'objet RSVP_HOP IF_ID elles sont utilisées pour identifier les liaisons. Dans l'objet ERROR_SPEC IF_ID, elles sont utilisées pour identifier la ressource défaillante qui est généralement la ressource en aval du nœud qui fait rapport.

Type	Longueur	Format	Description
1	8	adresse IPv4	IPv4 (Adresse d'interface)
2	20	adresse IPv6	IPv6 (Adresse d'interface)
3	12	composite	IF_INDEX (Indice d'interface)
4	12	composite	COMPONENT_IF_DOWNSTREAM (interface composante)
5	12	composite	COMPONENT_IF_UPSTREAM (interface composante)

Noter que les TLV 4 et 5 sont rendues obsolètes par la [RFC4201] et NE DEVRAIENT PAS être utilisées pour identifier des interfaces composantes dans les objets ERROR_SPEC IF_ID.

Afin de faciliter le rapport des informations de retour arrière, les TLV supplémentaires suivantes sont définies :

Type	Longueur	Format	Description
6	variable	voir ci-dessous	DOWNSTREAM_LABEL (étiquette GMPLS)
7	variable	voir ci-dessous	UPSTREAM_LABEL (étiquette GMPLS)
8	8	voir ci-dessous	NODE_ID (Identifiant de routeur TE)
9	x	voir ci-dessous	OSPF_AREA (identifiant de zone)
10	x	voir ci-dessous	ISIS_AREA (identifiant de zone)
11	8	voir ci-dessous	AUTONOMOUS_SYSTEM (système autonome)
12	variable	voir ci-dessous	ERO_CONTEXT (sous objet ERO)
13	variable	voir ci-dessous	ERO_NEXT_CONTEXT (sous objets ERO)
14	8	adresse IPv4	PREVIOUS_HOP_IPv4 (adresse du nœud)
15	20	adresse IPv6	PREVIOUS_HOP_IPv6 (adresse du nœud)
16	8	adresse IPv4	INCOMING_IPv4 (adresse d'interface)
17	20	adresse IPv6	INCOMING_IPv6 (adresse d'interface)
18	12	composite	INCOMING_IF_INDEX (indice d'interface)
19	variable	voir ci-dessous	INCOMING_DOWN_LABEL (étiquette GMPLS)
20	variable	voir ci-dessous	INCOMING_UP_LABEL (étiquette GMPLS)
21	8	voir ci-dessous	REPORTING_NODE_ID (identifiant de routeur)
22	x	voir ci-dessous	REPORTING_OSPF_AREA (identifiant de zone)
23	x	voir ci-dessous	REPORTING_ISIS_AREA (identifiant de zone)
24	8	voir ci-dessous	REPORTING_AS (système autonome)
25	variable	voir ci-dessous	PROPOSED_ERO (sous objets ERO)
26	variable	voir ci-dessous	NODE_EXCLUSIONS (liste de nœuds)
27	variable	voir ci-dessous	LINK_EXCLUSIONS (liste d'interfaces)

Pour les types 1, 2, et 3 le format du champ Valeur est déjà défini dans la [RFC3471].

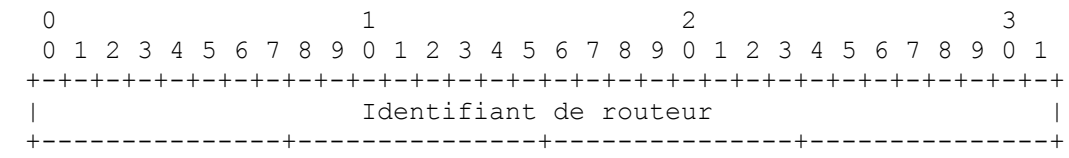
Pour les types 14 et 16, le format du champ Valeur est le même que pour le type 1.

Pour les types 15 et 17, le format du champ Valeur est le même que pour le type 2.

Pour le type 18, le format du champ Valeur est le même que pour le type 3.

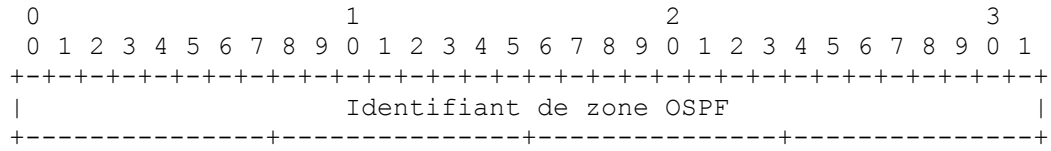
Pour les types 6, 7, 19, et 20, le champ Longueur est variable et le champ Valeur est une étiquette comme définie dans la [RFC3471]. Comme avec toutes les utilisations d'étiquettes, on suppose que tout nœud qui peut traiter les informations d'étiquette connaît la syntaxe et la sémantique de l'étiquette d'après le contexte. Noter que toutes les TLV sont bourrées de zéros jusqu'à un multiple de quatre octets afin que si une étiquette n'est pas elle-même un multiple de quatre octets, il n'y ait pas d'ambiguïté sur le bourrage à zéro des bits de queue grâce à la connaissance du contexte.

Pour les types 8 et 21, le champ Valeur a le format suivant :



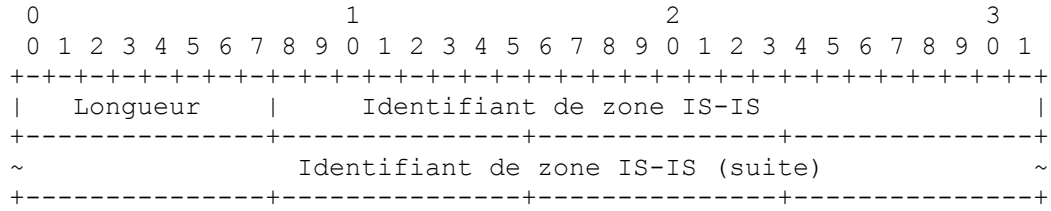
Identifiant de routeur : 32 bits. C'est l'identifant de routeur TE (type de TLV 8) ou l'identifiant de routeur (type de TLV 21) utilisé pour identifier le nœud au sein de l'IGP.

Pour les types 9 et 22, le champ Valeur a le format :



Identifiant de zone OSPF : identifiant de zone de 4 octets pour le nœud. Il identifie la zone où la défaillance s'est produite.

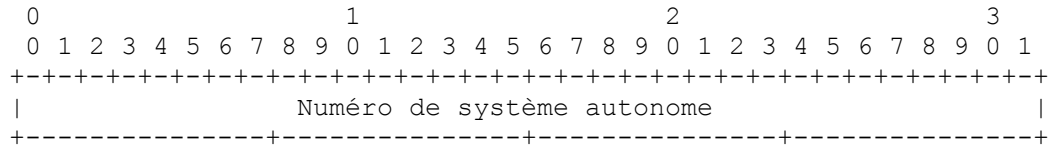
Pour les types 10 et 23, le champ Valeur a le format :



Longueur : longueur réelle (non bourrée) de l'identifiant de zone IS-IS en octets. Les valeurs valides sont de 1 à 13 inclus.

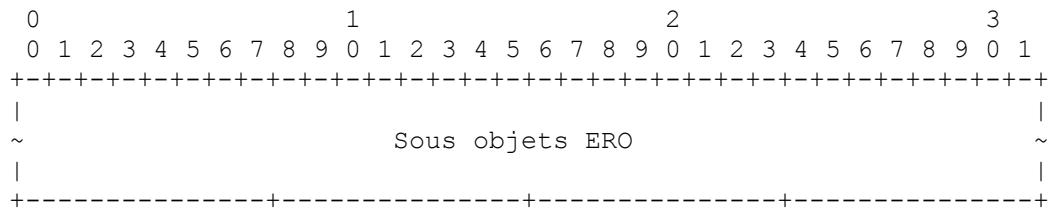
Identifiant de zone IS-IS : identifiant de zone IS-IS de longueur variable. Bourré avec des zéros en queue sur une limite de quatre octets.

Pour les types 11 et 24, le champ Valeur a le format :



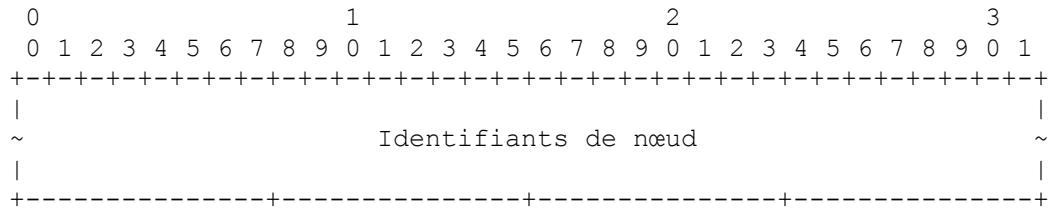
Numéro de système autonome : 32 bits. Numéro du système autonome associé. Noter que si les numéros d'AS de 16 bits sont utilisés, les bits de moindre poids (de 16 à 31) devraient être utilisés et les bits de poids fort (de 0 à 15) devraient être réglés à zéro.

Pour les types 12, 13, et 25, le champ Valeur a le format suivant :



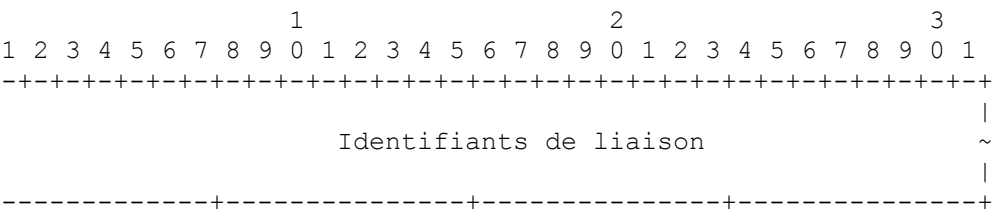
Sous objets ERO : séquence de sous objets Objet de chemin explicite (ERO, *Explicit Route Object*). Tout sous objet ERO est permis qu'il soit défini dans la [RFC3209], la [RFC3473], ou d'autres documents. Noter que les sous objets ERO contiennent leurr propres types et longueurs.

Pour le type 26, le champ Valeur a le format :



Identifiants de nœud : séquence de TLV comme définies ici des types 1, 2, ou 8 qui indiquent les nœuds en aval qui ont déjà participé à des tentatives de retour arrière et ont été déclarés inutilisables pour la tentative actuelle d'établissement de LSP. Noter qu'un identifiant d'interface peut être utilisé pour identifier un nœud.

Pour le type 27, le champ Valeur a le format :



Identifiants de liaison : séquence de TLV comme définies ici du même format que les TLV de type 1, 2 ou 3 qui indiquent les interfaces entrantes des nœuds en aval qui ont déjà participé à des tentatives de retour arrière et ont été déclarées inutilisables pour la tentative actuelle d'établissement de LSP.

6.3 Directives pour l'utilisation des TLV IF_ID ERROR_SPEC

6.3.1 Principes généraux

Si le retour arrière n'est pas utilisé, l'inclusion d'un objet IF_ID ERROR_SPEC dans les messages PathErr, ResvErr, et Notify suit les règles de traitement définies dans les [RFC3473] et [RFC4201]. Un envoyeur PEUT inclure des TLV supplémentaires des types 6 à 27 pour rapporter des informations de retour arrière à des fins d'information/surveillance.

Si le retour arrière est utilisé, l'envoyeur d'un message PathErr, ResvErr, ou Notify DOIT utiliser l'objet IF_ID ERROR_SPEC et DOIT inclure au moins une des TLV dans la gamme de 1 à 3 comme décrites dans les [RFC3473], [RFC4201], et le paragraphe précédent. Des TLV supplémentaires DEVRAIENT aussi être incluses pour rapporter plus d'informations. Le paragraphe suivant donne des avis sur les TLV qui devraient être utilisées dans différentes circonstances, et quelles TLV doivent être prises en charge par les LSR.

Noter que toutes ces TLV supplémentaires sont facultatives et PEUVENT être omises. L'inclusion de TLV facultatives DEVRAIT être effectuée lorsque le faire facilite les rapports d'erreur et le retour arrière. Les TLV entrent dans trois catégories : celles qui sont essentielles pour rapporter l'erreur, celles qui fournissent des informations supplémentaires qui sont ou peuvent être fondamentales pour l'utilisation du retour arrière, et celles qui fournissent des informations supplémentaires qui peuvent être utilies pour le retour arrière dans certaines circonstances.

Noter que tous les LSR DOIVENT être prêts à recevoir et transmettre toute TLV conformément à la [RFC3473]. Cela inclut les TLV de type 4 ou 5 comme défini dans la [RFC3473] et rendus obsolètes par la [RFC4201]. Il n'est cependant pas exigé qu'un LSR traite activement des TLV définies dans la [RFC3473]. Un LSR qui propose d'effectuer un réacheminement de retour arrière DEVRAIT prendre en charge la réception et le traitement de toutes les TLV de retour arrière fondamentales, et il est RECOMMANDÉ de prendre en charge la réception et le traitement des TV dr retour arrière supplémentaires.

On devrait noter, cependant, que certaines hypothèses sur les TLV qui vont être utilisées PEUVENT être faites sur la base de scénarios de déploiement. Par exemple, un routeur qui est déployé dans un réseau d'une seule zone n'a pas besoin de prendre en charge la réception et le traitement des TLV des types 22 et 23. Ces TLV pourraient être insérées dans un objet IF_ID ERROR_SPEC, mais n'auraient pas besoin d'être traitées par le receveur d'un message PathErr.

6.3.2 TLV de rapport d'erreur

Les TLV de rapport d'erreur sont celles dans la gamme de 1 à 3. (Noter que les TLV obsolètes 4 et 5 peuvrent être considérées être dans cette catégorie, mais NE DEVRAIENT PAS être utilisées.)

Comme noté précédemment, quand des informations de retour arrière sont rapportées, l'objet IF_ID ERROR_SPEC DOIT être utilisé. Quand l'objet IF_ID ERROR_SPEC est utilisé, au moins une des TLV dans la gamme de 1 à 3 DOIT être présente. Le choix de la TLV à utiliser va dépendre des circonstances de l'erreur et des capacités de l'appareil. Par exemple, un appareil qui ne prend pas en charge IPv6 n'a pas besoin de la capacité de créer une TLV de type 2. Noter cependant qu'un tel appareil DOIT quand même être prêt à recevoir et traiter toutes les TLV de rapport d'erreur.

6.3.3 TLV fondamentales de retour arrière

Beaucoup de TLV rapportent la ressource spécifique qui est défaillante. Par exemple, une TLV de type 1 peut être utilisée pour rapporter que la tentative d'établissement a été bloquée par une certaine forme de défaillance de ressource sur une interface spécifique identifiée par l'adresse IP fournie. Les TLV dans cette catégorie sont de 1 à 11, mais les TLV 4 et 5 peuvent être considérées comme exclues de cette catégorie car elles sont obsolètes.

Ces TLV DEVRAIENT être fournies chaque fois que le nœud qui détecte et rapporte la défaillance avec des informations de retour arrière a l'information disponible. (Noter que certaines de ces TLV DOIVENT être incluses comme décrit dans les deux paragraphes précédents.)

Les TLV de type 8, 9, 10, et 11 PEUVENT cependant être omises en accord avec la politique locale et la pertinence des informations.

6.3.4 TLV supplémentaires de retour arrière

Certaines TLV aident à localiser la faute dans le contexte du chemin du LSP qui a été établi. Les TLV des types 12, 13, 14, et 15 aident à établir le contexte de l'erreur dans la portée d'un chemin explicite qui a des bonds lâches ou des nœuds abstraits non précis. Les informations de contexte d'ERO ne sont pas toujours une exigence, mais un nœud peut remarquer qu'il est un membre du prochain bond dans l'ERO (comme un nœud abstrait lâche ou non spécifique) et en déduire que son voisin en amont peut avoir choisi le chemin en utilisant l'acheminement de prochain bond. Dans ce cas, fournir le contexte d'ERO va être utile pour que le nœud en amont effectue le réacheminement.

Noter que la distinction entre les TLV 12 et 13 est la distinction entre "ceci est le bond que j'ai essayé de réaliser quand j'ai échoué" et "ceci est le prochain bond que j'essayais d'atteindre quand j'ai eu une défaillance".

Les nœuds rapporteurs DEVRAIENT aussi fournir des TLV dans la gamme de 12 à 20 quand c'est approprié pour rapporter l'erreur. Les nœuds rapporteurs PEUVENT aussi fournir des TLV dans la gamme de 21 à 27.

Noter que pour décider si une TLV dans la gamme de 12 à 20 "est appropriée", le nœud rapporteur devrait considérer entre autres choses, si les informations sont pertinentes pour la cause de la défaillance. Par exemple, quand une interconnexion échoue, ce peut être que l'interface sortante est en faute, et dans ce cas seule l'interface (par exemple, TLV de type 1) a besoin d'être rapportée, mais si le problème est que l'interface entrante ne peut pas être connectée à l'interface sortante à cause de limitations d'interconnexion temporaires ou permanentes, le nœud devrait aussi inclure une référence à l'interface entrante (par exemple, TLV de type 16).

Quatre TLV (21, 22, 23, et 24) permettent de s'étendre sur la localisation du nœud qui fait rapport. Ces TLV ne vont pas être incluses si les informations ne sont pas utiles dans le système local, mais pourraient être ajoutées par les ABR qui relayent l'erreur. Noter que l'identifiant du nœud rapporteur (TLV 21) n'a pas besoin d'être inclus si l'adresse IP du nœud rapporteur, comme indiquée dans la ERROR_SPEC elle-même, est suffisante pour identifier pleinement le nœud.

Les trois dernières TLV (25, 26, et 27) fournissent des informations supplémentaires pour les points de calcul. Le nœud rapporteur (ou un nœud qui transmet l'erreur) PEUT faire des suggestions sur la façon dont l'erreur aurait pu être évitée, par exemple, en fournissant un ERO partiel qui causerait la réussite de l'établissement du LSP si il était utilisé. Lorsque l'erreur est propagée en retour en amont et lorsque l'acheminement de retour arrière est tenté et échoue, il est avantageux de collecter la liste des nœuds et liaisons défaillants afin qu'ils ne soient pas inclus dans les calculs suivants effectués aux nœuds en amont. Cette liste peut aussi être factorisée en exclusions de chemins [RFC4874].

Noter qu'il n'y a pas d'exigence d'ordre pour les TLV dans la spécification d'erreur IF_ID, et aucune implication ne devrait être tirée de l'ordre des TLV dans une spécification d'erreur IF_ID reçue.

La décision des types précis de TLV qu'un nœud rapporteur inclut dépend des capacités spécifiques du nœud, et sort du domaine d'application du présent document.

6.3.5 Groupement des TLV par localisation de défaillance

Plus de conseils sur l'inclusion des TLV de retour arrière peuvent être donnés en groupant les TLV en accord avec la localisation de la défaillance et le contexte dans lesquel elle est rapportée. Par exemple, une TLV qui rapporte un

identifiant de zone aurait seulement besoin d'être incluse lorsque le rapport d'erreur de retour arrière transite par une limite de zone.

Défaillance de ressource :
6 DOWNSTREAM_LABEL
7 UPSTREAM_LABEL
Défaillance d'interface :
1 IPv4
2 IPv6
3 IF_INDEX
4 COMPONENT_IF_DOWNSTREAM (obsolète)
5 COMPONENT_IF_UPSTREAM (obsolète)
12 ERO_CONTEXT
13 ERO_NEXT_CONTEXT
14 PREVIOUS_HOP_IPv4
15 PREVIOUS_HOP_IPv6
16 INCOMING_IPv4
17 INCOMING_IPv6
18 INCOMING_IF_INDEX
19 INCOMING_DOWN_LABEL
20 INCOMING_UP_LABEL
Défaillance de nœud :
8 NODE_ID
21 REPORTING_NODE_ID
Défaillance de zone :
9 OSPF_AREA
10 ISIS_AREA
22 REPORTING_OSPF_AREA
23 REPORTING_ISIS_AREA
25 PROPOSED_ERO
26 NODE_EXCLUSIONS
27 LINK_EXCLUSIONS
Défaillance d'AS :
11 AUTONOMOUS_SYSTEM
24 REPORTING_AS

Bien que la discussion de l'agrégation des informations de retour arrière sorte du domaine d'application de ce document, on devrait noter que ce sujet est en relation étroite avec les informations présentées ici. L'agrégation est discutée plus en détails au paragraphe 6.4.5.

6.3.6 Identification de chemin de remplacement

Aucun nouvel objet n'est utilisé pour distinguer entre les messages Path/Resv pour un LSP de remplacement. Donc, le LSP de remplacement utilise les mêmes objets SESSION et SENDER_TEMPLATE/FILTER_SPEC que ceux utilisés pour le LSP initial en réacheminement.

6.4 Action à réception des informations de retour arrière

6.4.1 Tentatives de réacheminement

Comme décrit à la Section 2, un nœud qui reçoit des informations de retour arrière dans un PathErr doit d'abord vérifier si il est permis d'effectuer un réacheminement. C'est indiqué par les fanions Réacheminement dans l'objet LSP_ATTRIBUTES durant une demande d'établissement de LSP.

Si il n'est pas permis à un nœud d'effectuer de réacheminement, il devrait transmettre le message PathErr, ou si il est l'entrée, rapporter le LSP comme étant défaillant.

Si le réacheminement est permis, le nœud devrait tentr de calculer un chemin pour la destination en utilisant le chemin explicite original (reçu) et exclure le nœud/liaison défaillant/bloqué. Le nouveau chemin devrait être ajouté à une demande

d'établissement de LSP comme chemin explicite et signalé.

Les LSR qui effectuent le réacheminement de retour arrière devraient mémoriser toutes les informations de retour arrière reçues pour un LSP jusqu'à ce que le LSP soit bien établi ou jusqu'à ce que le nœud abandonne ses tentatives de réacheminement de LSP. Sur la prochaine tentative de calcul de chemin de réacheminement de retour arrière, le LSR devrait exclure tous les nœuds, liaisons et ressources défaillants rapportés des tentatives précédentes.

C'est une décision de la mise en œuvre que les informations de retour arrière soient éliminées immédiatement après un établissement réussi de LSP ou conservées pendant un certain temps en cas de défaillance du LSP.

6.4.2 Identifiants de localisation de liaisons ou nœuds bloqués

Afin de calculer un chemin de remplacement par un réacheminement de retour arrière, il est nécessaire d'identifier les liaisons ou nœuds bloqués et leur localisation. L'identifiant commun de chaque liaison ou nœud dans un réseau MPLS devrait être spécifié. Des identifiants indépendants du protocole et dépendants du protocole peuvent tous deux être spécifiés. Bien qu'un identifiant général qui soit indépendant des autres protocoles soit préférable, il y a quelques restrictions sur son utilisation qui sont décrites dans le paragraphe suivant.

Dans les protocoles d'état de liaison comme OSPF et IS-IS, chaque liaison et nœud dans un réseau peut être identifié de façon univoque, par exemple, par le contexte d'un identifiant de routeur TE et l'identifiant de liaison. Si la topologie et les informations de ressources obtenues des annonces OSPF sont utilisées pour calculer un chemin fondé sur la contrainte, la localisation d'un blocage peut être représentée par de tels identifiants.

Note que quand les identifiants de liaison spécifiques du protocole d'acheminement sont utilisés, le fanion Réacheminement sur la demande d'établissement de LSP doit avoir été établi pour montrer la prise en charge du réacheminement de frontière ou fondé sur le segment.

Dans le présent document, on spécifie des identifiants de liaison et de nœud spécifiques du protocole d'acheminement pour OSPFv2, OSPFv3, et IS-IS pour IPv4 et IPv6. Ces identifiants ne peuvent être utilisés que si le réacheminement fondé sur le segment est pris en charge, comme indiqué par le fanion Comportement d'acheminement sur la demande d'établissement de LSP.

6.4.3 Localisation des erreurs au sein des nœuds lâches ou abstraits

Le chemin explicite sur la demande originale d'établissement de LSP peut contenir un nœud lâche ou abstrait. Dans ce cas, les informations de retour arrière peuvent se référer à des liaisons ou nœuds qui n'étaient pas dans le chemin explicite original.

Afin de calculer un nouveau chemin, le point de réparation peut avoir besoin d'identifier la paire de bonds (ou nœuds) dans le chemin explicite entre lesquels l'erreur/blocage s'est produit.

Pour aider à cela, les informations de retour arrière rapportent les deux bonds supérieurs du chemin explicite tels que reçus au nœud qui fait le rapport. Le premier bond va probablement identifier le nœud ou la liaison, le second bond va identifier un "prochain" bond à partir du chemin explicite original.

6.4.4 Échec de réacheminement

Quand un nœud ne peut pas, ou choisit de ne pas effectuer de réacheminement de retour arrière, il doit transmettre le message PathErr plus loin en amont.

Cependant, quand un nœud était chargé d'étendre ou de remplacer le chemin explicite lorsque l'établissement de LSP a été traité, il DOIT mettre à jour les informations de retour arrière par rapport au chemin explicite qu'il a reçu. C'est seulement si ceci est fait que les nœuds en amont auront une chance d'un acheminement réussi contournant le problème.

6.4.5 Agrégation des informations de retour arrière

Quand une erreur de blocage d'établissement ou une erreur dans un LSP établi se produit et que des informations de retour arrière sont envoyées dans un message de notification d'erreur, un nœud en amont peut choisir de tenter un réacheminemen

de retour arrièret. Si cette tentative de réacheminement du nœud échoue, le nœud va accumuler un ensemble d'informations de défaillance. Quand le nœud abandonne, il DOIT propager le mesage de défaillance plus loin en amont et inclure les informations de retour arrière quand il le fait.

Inclure une liste complète de toutes les défaillances qui se sont produites à cause de multiples défaillances de retour arrière par plusieurs LSR de point de réparation en aval pourrait conduire à ce que trop d'informations soient signalées en utilisant les extensions de protocole décrites dans le présent document. Un mécanisme de compression pour ces informations est disponible en utilisant les TLV 26 et 27. Ces TLV permettent une accumulation plus concise des informations de défaillance lorsque les défaillances de retour arrière sont propagées en amont.

L'agrégation peut impliquer de rapporter toutes les liaisons depuis un nœud comme inutilisables en mettant un fanion indiquant que le nœud est inutilisable, en mettant un fanion indiquant qu'un ABR est inutilisable quand il n'y a pas de chemin disponible en aval, ou en incluant une TLV de type 9 qui résulte en l'exclusion de la zone entière, et ainsi de suite. Les détails de comment l'agrégation des informations de retour arrière est effectuée sortent du domaine d'application de ce document.

6.5 Notification des erreurs

6.5.1 Traitement de ResvErr

Comme décrit ci-dessus, une défaillance d'allocation de ressource pour RSVP-TE peut survenir sur le chemin inverse quand le message Resv est en cours de traitement. Dans ce cas, il est encore utile de retourner les informations de retour arrière reçues au LSR d'entrée. Cependant, quand le LSR de sortie reçoit le message ResvErr, selon la [RFC2205] il a encore l'option de produire à nouveau le Resv avec des exigences de ressources différentes (mais pas sur un chemin de remplacement).

Quand un ResvErr portant des informations de retour arrière est reçu à un LSR de sortie, celui-ci PEUT ignorer cet objet et effectuer les mêmes actions qu'il aurait effectuées pour tout autre ResvErr. Cependant, si le LSR de sortie prend en charge les extensions de retour arrière définies dans le présent document, et après l'échec de toutes les procédures de récupération locale, il DEVRAIT générer un message PathErr portant les informations de retour arrière et les envoyer au LSR d'entrée.

Si un ResvErr rapporte sur plus d'un objet FILTER_SPEC (parce que le Resv portait plus d'une FILTER_SPEC) un seul ensemble d'informations de retour arrière devrait alors être présent dans le ResvErr et il devrait s'appliquer à toutes les FILTER_SPEC portées. Dans ce cas, il peut être nécessaire, conformément à la [RFC2205] de générer plus d'un message PathErr.

6.5.2 Traitement du message Notify

La [RFC3473] définit le message Notify pour améliorer le rapport d'erreurs dans les réseaux RSVP-TE. Ce message n'est pas destiné à remplacer les messages PathErr et ResvErr. Le message Notify est envoyé aux adresses demandées sur les messages Path et Resv. Ces adresses pourraient (mais ce n'est pas une obligation) identifier les LSR, respectivement d'entrée et de sortie.

Quand une erreur de réseau se produit, comme la défaillance d'un matériel de liaison, les LSR qui détectent l'erreur PEUVENT envoyer des messages Notify aux adresses demandées. Le type d'erreur qui cause l'envoi d'un message Notify est un détail de mise en œuvre.

En cas d'une défaillance, un LSR qui prend en charge la [RFC3473] et les extensions de retour arrière définies dans le présent document PEUT choisir d'envoyer un message Notify portant des informations de retour arrière.Cela assurerait un rapport plus rapide de l'erreur aux LSR d'entrée et/ou de sortie.

6.6 Valeurs d'erreur

Les valeurs d'erreur pour le code d'erreur "Échec de contrôle d'admission" sont définies dans la [RFC2205]. Les valeurs d'erreur pour le code d'erreur "Problème d'acheminement" sont définies dans les [RFC3209] et [RFC3473].

Une nouvelle valeur d'erreur est définie pour le code d'erreur "Problème d'acheminement". "Limite de réacheminement dépassée" indique que le réacheminement a échoué parce que le nombre de tentatives de réacheminement de retour arrière a dépasssé un seuil prédéterminé à un certain LSR.

6.7 Rétro compatibilité

Il est reconnu que tous les nœuds dans un réseau RSVP-TE ne vont pas prendre en charge les extensions définies dans le présent document. Il est important qu'un LSR qui ne prend pas en charge ces extensions puisse continuer de traiter un message PathErr, ResvErr, ou Notify même si il porte la nouvelle information IF_ID ERROR_SPEC définie (TLV).

Le présent document n'introduit aucun problème de rétro compatibilité pourvu que les mises en œuvre existantes se conforment aux règles de traitement de TLV définies dans les [RFC3471] et [RFC3473].

7. Considérations sur la récupération de LSP

La récupération de LSP est effectuée pour récupérer un LSP établi quand se produit une défaillance le long du chemin. Dans le cas de récupération de LSP, les extensions pour le réacheminement de retour arrière expliquées ci-dessus peuvent être appliquées pour améliorer les performances. Cette section donne un exemple d'application des extensions ci-dessus à la récupération de LSP. Le but de cet exemple est de donner une vue d'ensemble générale de la façon dont cela pourrait fonctionner, et non de donner une procédure détaillée pour la récupération de LSP.

Bien qu'il y ait plusieurs techniques pour la récupération de LSP, cette section explique le cas de récupération de LSP à la demande, qui tente d'établir un nouveau LSP à la demande après la détection de la défaillance d'un LSP.

7.1. En amont de la faute

Quand un LSR détecte une faute sur une liaison ou un nœud adjacent vers l'aval, un message PathErr est envoyé en amont. Dans GMPLS, l'objet ERROR_SPEC peut porter un fanion d'indication Path_State_Remove *(suppression d'état de chemin)*. Chaque LSR qui reçoit le message libère alors le LSP correspondant. (Noter que si l'indication de retrait d'état n'est pas présente dans le message PathErr, le nœud d'entrée DOIT produire un message PathTear pour causer la libération des ressources.) Si le LSP défaillant doit être récupéré à un LSR en amont, la spécification d'erreur IF_ID qui inclut les informations de localisation de la liaison ou nœud défaillant est incluse dans le message PathErr. Le LSR d'entrée, de bordure de zone intermédiaire, ou tout point de réparation permis par les fanions Réacheminement, qui reçoit le message PathErr peut terminer le message et effectuer ensuite l'acheminement de remplacement.

Dans un réseau plat, quand le LSR d'entrée reçoit le message PathErr avec les TLV IF_ID ERROR_SPEC, il calcule un chemin de remplacement contournant la liaison ou le nœud bloqué qui satisfasse aux garanties de QS. Si un chemin de remplacement est trouvé, un nouveau message Path est envoyé sur ce chemin vers le LSR de sortie.

Dans un réseau segmenté en zones, les procédures suivantes peuvent être utilisées. Comme expliqué au paragraphe 5.4, le comportement de récupération de LSP est indiqué dans le champ Fanions de l'objet LSP_ATTRIBUTES du message Path. Si les fanions indiquent "réacheminement de bout en bout", le message PathErr est retourné tout le long du chemin jusqu'au LSR d'entrée, qui peut alors produire un nouveau message Path sur un autre chemin, ce qui est la même procédure que dans le cas du réseau plat ci-dessus.

Si le champ Fanions indique un réacheminement de frontière, le LSR de bordure de zone d'entrée PEUT terminer le message PathErr et ensuite effectuer un acheminement de remplacement au sein de la zone pour laquelle le LSR de bordure de zone est le LSR d'entrée.

Si le champ Fanions indique un réacheminement fondé sur le segment, tout nœud PEUT appliquer les procédures décrites ci-dessus pour le réacheminement de frontière.

7.2 En aval de la faute

Ce paragraphe ne s'applique qu'aux erreurs qui surviennent après l'établissement d'un LSP. Noter qu'un LSR qui génère un PathErr avec le fanion Path_State_Remove DEVRAIT aussi envoyer un PathTear en aval pour nettoyer le LSP.

Un nœud qui détecte une faute et est en aval de la faute PEUT envoyer un message PathErr et/ou Notify contenant une spécification d'erreur IF_ID qui inclut les informations de localisation de la liaison ou nœud défaillant, et PEUT envoyer un PathTear pour nettoyer le LSP à tous les autres nœuds en aval.

Cependant, si le style de réservation pour le LSP est partagé explicite (SE, *Shared Explicit*) le LSR qui détecte PEUT choisir de ne pas envoyer de PathTear -- cela laisse en place l'état du LSP en aval et facilite la réparation en mode faire avant de casser du LSP en réutilisant les ressources ce l'aval. Noter que si le nœud qui détecte n'envoie pas de PathTear immédiatement, l'état non utilisé va arriver en fin de temporisation en accord avec les règles normales de la [RFC2205].

À un point de fusion bien connu, un ABR ou un ASBR, une décision similaire pourrait aussi être prise afin de mieux faciliter une réparation faite avant la cassure. Dans ce cas, un PathTear reçu pourrait être "absorbé" et non propagé plus loin en aval pour un LSP qui a une réservation de style SE. Noter cependant que ceci est une divergence par rapport au protocole et pourrait sévèrement impacter la suppression normale des LSP.

8. Considérations relatives à l'IANA

8.1 Codes d'erreur

L'IANA tient un registre appelé "Paramètres RSVP" avec un sous registre appelé "Codes d'erreur et sous codes d'erreur définis mondialement". Ce sous registre inclut le code d'erreur RSVP-TE "Problème d'acheminement" qui est défini dans la [RFC3209].

L'IANA a alloué une nouvelle valeur d'erreur pour le code d'erreur "Problème d'acheminement" comme suit :

22 Limite de réacheminement dépassée.

8.2 TLV IF_ID_ERROR_SPEC

Les valeurs de type de TLV IF_ID_ERROR_SPEC définies dans la [RFC3471] sont tenues par l'IANA dans le sous registre "Types d'identifiant d'interface" du registre "Paramètres de signalisation GMPLS".

L'IANA a fait de nouvelles allocations à partir de ce sous registre pour les nouveaux types de TLV définis au paragraphe 6.2 du présent document.

8.3 Objets LSP_ATTRIBUTES

L'IANA tient un registre "Paramètres RSVP TE" avec un sous registre "Fanions d'attributs". L'IANA a fait trois nouvelles allocations dans ce registre selon la liste du paragraphe 5.4.

Ces bits sont définis pour être inclus dans la TLV Attributs de LSP de l'objet LSP_ATTRIBUTES. Les valeurs indiquées ont été attribuées par l'IANA.

9. Considérations sur la sécurité

Le modèle de confiance RSVP-TE suppose que les voisins et homologues RSVP-TE se font mutuellement confiance pour échanger des messages légitimes et non malveillants. Cette hypothèse est nécessaire pour que le protocole de signalisation puisse fonctionner.

Noter que ce modèle de confiance est supposé être en cascade. C'est-à-dire que si un LSR fait confiance à ses voisins, il étend sa confiance à tous les LSR à qui son voisin fait confiance. Cela signifie que le modèle de confiance est généralement appliqué à travers tout le réseau pour créer un domaine de confiance.

L'authentification de l'identité d'un voisin est déjà une disposition standard de RSVP-TE, comme l'est la protection des messages contre l'altération et l'usurpation. On se réfèrera aux [RFC2205], [RFC3209], et [RFC3473] pour une description des considérations de sécurité applicables. Ces considérations et mécanismes sont applicables aux échanges de messages bond par bond (comme utilisés pour la propagation du retour arrière sur les messages PathErr) et les échanges de messages dirigés (comme utilisés pour la propagation du retour arrière sur les messages Notify).

La gestion de clés peut aussi être utilisée avec RSVP-TE pour aider à protéger contre l'usurpation d'identité et la falsification du contenu du message. Cela exige la maintenance, l'échange, et la configuration de clés sur chaque LSR.

Noter qu'une telle maintenance peut être particulièrement onéreuse pour les opérateurs, donc, il est important de limiter le nombre de clés tout en s'assurant du niveau de sécurité requis.

Le présent document n'introduit aucun élément de protocole ou échange de messages qui change le fonctionnement de la sécurité de RSVP-TE.

Cependant, on devrait noter que le retour arrière est envisagé comme un mécanisme inter domaines, et à ce titre, il est probable que les informations de retour arrière sont échangées sur des frontières de domaine de confiance. Dans ces cas, il est attendu que les informations provenant de l'intérieur d'un domaine voisin vont être de peu, ou pas du tout, de valeur pour le nœud qui effectue le réacheminement de retour arrière et vont être ignorées. En tous cas, il est très probable que le domaine rapporteur aura appliqué une forme d'agrégation des informations afin de préserver la confidentialité de sa topologie de réseau.

La question d'une attaque directe d'un domaine contre un autre domaine est possible et les administrateurs de domaine devraient appliquer des politiques de protection de leurs domaines contre les résultats de tentatives par un autre domaine de de perturbation des LSP en leur permettant de les établir avant de les rapporter comme défaillants. Globalement, on s'attend à ce que des accords commerciaux entre des domaines de confiance fournissent un certain degré de protection.

Une menace plus sérieuse peut se présenter si un domaine rapporte que ni lui ni son voisin en aval ne peut fournir un chemin pour la destination. Un tel rapport pourrait être bogué en ce que le domaine rapporteur pourrait n'avoir pas donné au domaine en aval une chance de tenter de fournir un chemin. Noter que le même problème ne se présente pas pour les nœuds au sein d'un domaine à cause du modèle de confiance. Ce type de comportement malveillant est difficile à surmonter, mais peut être détecté par l'utilisation de demandes de calcul de chemin indirectes envoyées directement au domaine faussement rapporté en utilisant des mécanismes comme l'élément de calcul de chemin de la [RFC4655].

Noter qu'un document séparé décrivant les considérations de sécurité inter domaines MPLS et GMPLS va être produit.

Finalement, on notera que alors que les extensions de ce document n'introduisent pas de nouveaux trous de sécurité dans les protocoles, si un utilisateur malveillant devait obtenir l'accès du protocole au réseau, les informations de retour arrière pourraient être utilisées pour empêcher l'établissement de LSP valides. Donc, les caractéristiques de sécurité existantes disponibles dans RSVP-TE devraient être examinées avec attention par tous les développeurs et DEVRAIENT être rendues disponibles par toutes les mises en œuvre qui offrent le retour arrière. Noter que la mise en œuvre de seuils de tentatives de réacheminement est aussi particulièrement utile dans ce contexte.

10. Remerciements

Nous remercions Juha Heinanen et Srinivas Makam de leur relecture et de leurs commentaires, et Zhi-Wei Lin pour la manifestation de ses opinions. Merci aussi à John Drake pour nous avoir encouragé à ressusciter le présent document et considérer l'utilisation de l'objet IF_ID ERROR SPEC. Merci pour son accueil et sa relecture très serrée à Dimitri Papadimitriou.
Stephen Shew a fait d'utiles commentaires d'éclaircissements par le processus de liaison avec l'lUIT-T.
Simon Marshall-Unitt a fait des contributions au présent document.
La relecture SecDir a été fournie par Tero Kivinen. Merci à Ross Callon pour les discussions utiles sur la prioritisation de tentatives de réacheminement de retour arrière.

11. Références

11.1 Références normatives

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

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

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

[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)

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

11.2 Références pour information

[ASH1] G. Ash, Recommandations UIT-T E.360.1 à E.360.7, "Acheminement de qualité de service et méthodes d'ingénierie du trafic en rapport pour les réseaux multi services fondés sur IP, ATM, et TDM", mai 2002.

[PNNI] ATM Forum, "Private Network-Network Interface Specification Version 1.0 (PNNI 1.0)", <af-pnni-0055.000>, mai 1996.

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

[RFC3469] V. Sharma et F. Hellstrand, éd., "Cadre pour la récupération fondée sur la commutation d'étiquettes multi-protocoles (MPLS)", février 2003. *(Information)*

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

[RFC4201] K. Kompella et autres, "Faisceaux de liaisons dans l'ingénierie du trafic MPLS", octobre 2005. *(P.S.)*

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

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

Appendice A. Expérience de retour arrière dans les réseaux fondés sur TDM

L'expérience de l'utilisation des messages de libération dans les réseaux fondés sur TDM pour les besoins de réparation analogue et de réacheminement a fourni des lignes directrices.

On peut utiliser la réception d'un message de libération avec une valeur de cause (CV, *Cause Value*) indiquant "liaison encombrée" pour déclencher une tentative de réacheminement au nœud d'origine. Cependant, cela conduit parfois à des problèmes.

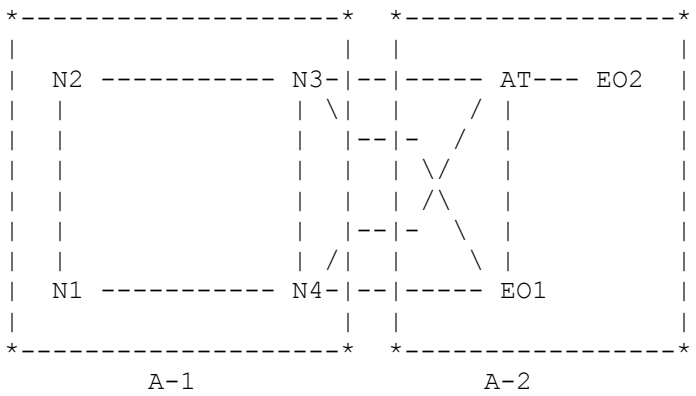


Figure 1 : Exemple de topologie de réseau

La Figure 1 illustre quatre exemples fondés sur les expériences d'un fournisseur de services par rapport au retour arrière (c'est-à-dire, une indication explicite) contre une indication implicite par une libération avec CV. Dans cet exemple, N1, N2, N3, et N4 sont situés dans une zone (A-1), et AT, EO1, et EO2 sont dans une autre zone (A-2).

Noter que deux zones distinctes sont utilisées dans cet exemple pour exposer clairement les problèmes. En fait, les questions ne sont pas limitées aux réseaux multi zones, mais surviennent chaque fois que le calcul de chemin est réparti dans le réseau, par exemple, lorsque des chemins lâches, des chemins d'AS, ou des domaines de calcul de chemin sont utilisés.

1. Une demande de connexion du nœud N1 à EO1 peut acheminer à N4 et ensuite trouver "tous les circuits occupés". N4 retourne un message de libération à N1 avec CV34 indiquant que tous les circuits sont occupés. Normalement, un nœud comme N1 est programmé à bloquer une demande de connexion quand il reçoit un CV34, bien qu'il y ait de bonnes raisons d'essayer d'acheminer autrement la demande de connexion via N2 et N3. Certains fournisseurs de services ont mis en œuvre une technique appelée avance de chemin (RA, *Route Advance*) où si un nœud qui est capable de RA reçoit un message de libération avec CV34, il va utiliser cela comme une indication implicite de réacheminement et essayer de trouver un chemin de remplacement pour la demande de connexion, si possible. Dans cet exemple, le chemin de remplacement N1-N2-N3-EO1 peut être essayé et pourrait bien réussir.

2. Supposons qu'une demande de connexion aille de N2 à N3 pour AT tout en essayant d'atteindre EO2 et soit bloquée à la liaison AT-EO2. Le nœud AT retourne un CV34 et avec RA, N2 peut essayer de réacheminer N2-N1-N4-AT-EO2, mais bien sûr cela échoue encore. Le problème est que N2 ne comprend pas où ce blocage se produit sur la base du CV34, et dans ce cas, il n'y a rien pour poursuivre l'acheminement de remplacement.

3. Cependant, dans un autre cas d'une demande de connexion de N2 à E02, supposons que la liaison N3-AT soit bloquée. Dans ce cas, N3 devrait retourner des informations de retour arrière (et pas de CV34) afin que N2 puisse être le chemin de remplacement pour N1-N4-AT-EO2, qui peut bien réussir.

4. Dans un dernier exemple, pour une demande de connexion de EO1 à N2, EO1 essaye d'abord d'acheminer la demande de connexion directement à N3. Cependant, le nœud N3 peut rejeter la demande de connexion même si il y a de la bande passante disponible sur la liaison N3-EO1 (peut-être pour des considérations de priorité d'acheminement, par exemple, réserver de la bande passante pour des demandes de connexion de priorité élevée). Cependant, quand N3 retourne le CV34 dans le message de libération, EO1 bloque la demande de connexion (une réponse normale à CV34 en particulier si E01-N4 est déjà connu pour être bloqué) plutôt que d'essayer un chemin de remplacement par AT-N3-N2, qui pourrait réussir. Si N3 retourne des informations de retour arrière, EO1 pourrait répondre en essayant le chemin de remplacement. Il est certain qu'avec l'échange de topologie, comme dans OSPF, le LSR d'entrée pourrait déduire la condition de réacheminement. Cependant, la convergence des informations d'acheminement est normalement plus lente que le temps attendu d'établissement de LSP. Une des raisons du retour arrière est d'éviter les frais généraux de l'arrosage de la bande passante de liaison disponible, et d'utiliser plus efficacement les informations d'état local pour diriger l'acheminement de remplacement sur le LSR d'entrée.

[ASH1] montre comment l'acheminement selon l'événement peut juste utiliser le retour arrière, et non l'arrosage de la bande passante de liaison disponible, pour décider du chemin de réacheminement dans le réseau par des "modèles d'apprentissage". Réduire cet arrosage réduit les frais généraux et peut conduire la capacité de prendre en charge de plus grandes tailles d'AS.

Donc, l'acheminement de remplacement devrait être indiqué de façon explicite (comme dans les exemples 3 et 4) et le mieux est de connaître les informations suivantes séparément :
a) où le blocage/encombrement s'est produit (comme dans les exemples 1-2), et
b) si l'acheminement de remplacement "devrait" être tenté même si il n'y a pas de "blocage" (comme dans l'exemple 4).

Adresse des auteurs

Adrian Farrel
Old Dog Consulting
téléphone : +44 (0) 1978 860944
mél : adrian@olddog.co.uk

Arun Satyanarayana
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
téléphone : +1 408 853-3206

Atsushi Iwata
NEC Corporation
System Platforms Research Laboratories
1753 Shimonumabe Nakahara-ku,
Kawasaki, Kanagawa, 211-8666, JAPAN

mél : asatyana@cisco.com téléphone : +81-(44)-396-2744
mél : a-iwata@ah.jp.nec.com

Norihito Fujita
NEC Corporation
System Platforms Research Laboratories
1753 Shimonumabe Nakahara-ku,
Kawasaki, Kanagawa, 211-8666, JAPAN
mél : n-fujita@bk.jp.nec.com

Gerald R. Ash
AT&T
mél : gash5107@yahoo.com

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2007)

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

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

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

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

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

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