Groupe de travail Réseau
Request for Comments : 4426
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Lang, Sonos, Inc.
B. Rajagopalan, Microsoft
D. Papadimitriou, Alcatel
mars 2006

Spécification fonctionnelle de récupération dans la commutation d'étiquette multi protocoles généralisée (GMPLS)

Résumé
Le présent document présente une description fonctionnelle des extensions de protocole nécessaires pour prendre en charge la récupération fondée sur la commutation d'étiquette multi protocole généralisée (GMPLS, *Generalized Multi-Protocol Label Switching*) (c'est-à-dire la protection et la restauration). Les formats et mécanismes spécifiques du protocole seront décrits dans des documents d'accompagnement.

Table des matières

1. Introduction

Une exigence pour le développement d'un plan de contrôle commun pour les équipements de commutation optique et électronique est qu'il doit y avoir des mécanismes de signalisation, d'acheminement, et de gestion de liaison qui prennent en charge la récupération de défaillance du plan des données. Dans le présent document, le terme "récupération" est utilisé de façon générique pour noter à la fois la protection et la restauration ; les termes spécifiques de "protection" et de "restauration" ne sont utilisés que quand une différentiation est requise. La distinction subtile entre protection et

restauration est faite sur la base de l'allocation de ressources durant la période de récupération (voir la [RFC4427]).

Un chemin à commutation d'étiquettes (LSP, *label-switched path*) peut être soumis à récupération sur le segment local (portée), et/ou de bout en bout. La protection de la portée locale se réfère à la protection de la liaison (et donc de tous les LSP marqués comme exigés pour la protection de portée et acheminés sur la liaison) entre deux commutateurs voisins. La protection de segment se réfère à la récupération d'un segment de LSP (c'est-à-dire, un SNC dans la terminologie de l'UIT-T) entre deux nœuds, c'est-à-dire, les nœuds frontières du segment. La protection de bout en bout se réfère à la protection d'un LSP entier de l'accès d'entrée à l'accès de sortie. Les modèles de récupération de bout en bout discutés dans le présent document s'appliquent à la protection de segment où la source et la destination se réfèrent au segment protégé plutôt qu'au LSP entier. Plusieurs niveaux de récupération peuvent être utilisés concurremment par un seul LSP pour ajouter de la résilience ; cependant, l'interaction entre niveaux affecte chaque direction du LSP et résulte en ce que les deux directions du LSP sont commutées à une nouvelle portée, segment, ou chemin de bout en bout.

Sauf mention contraire, toutes les références à une "liaison" dans ce document indiquent une liaison bidirectionnelle (qui peut être réalisée par une paire de liaisons unidirectionnelles).

Considérons le flux de messages de plan de contrôle durant l'établissement d'un LSP. Ce flux de messages procède d'un nœud initiateur (ou source) à un nœud de terminaison (ou destination) via une séquence de nœuds intermédiaires. Un nœud le long du LSP est dit être "en amont" d'un autre nœud si le premier intervient d'abord dans la séquence. Le dernier nœud est dit être "en aval" du premier nœud. C'est-à-dire qu'un nœud "amont" est plus proche du nœud initiateur qu'un nœud plus "en aval". Sauf mention contraire, toutes les références à "en amont" et "en aval" sont en termes de flux de messages du plan de contrôle.

Le flux de trafic de données est défini de l'entrée (nœud source) à la sortie (nœud de destination). Noter que pour les LSP bidirectionnels, il y a deux flux de plan de données différents, un pour chaque direction du LSP. Ce document présente une description fonctionnelle de protocole pour prendre en charge la récupération fondée sur la commutation d'étiquettes multi protocoles généralisée (GMPLS, *Generalized Multi-Protocol Label Switching*) (c'est-à-dire, protection et restauration). Les formats, codages, et mécanismes spécifiques de protocole seront décrits dans des documents d'accompagnement.

1.1 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] et référencée aussi dans la [RFC4427].

2. Protection de portée

Considérons une liaison (active) i entre deux nœuds A et B. Il y a deux modèles fondamentaux pour la protection de portée. Le premier est appelé la protection 1+1. Dans ce modèle, une liaison dédiée j est pré-allouée pour protéger la liaison i. Le trafic du LSP est ponté en permanence sur les deux liaisons i et j au nœud d'entrée, et le nœud de sortie choisit le signal (c'est-à-dire, le trafic normal) provenant de i ou j, sur la base d'une fonction de sélection (par exemple, qualité du signal). Dans la protection de portée unidirectionnelle 1+1 (paragraphe 2.1) chaque nœud A et B agit de façon autonome pour choisir le signal provenant de la liaison active i ou de la liaison de protection j. Dans la protection de portée bidirectionnelle 1+1 (paragraphe 2.2) les deux nœuds A et B coordonnent la fonction de sélection de telle façon qu'ils choisissent le signal provenant de la même liaison, i ou j.

Dans le second modèle, un ensemble de N liaisons actives sont protégées par un ensemble de M liaisons, généralement avec $M \leq N$. Une défaillance dans une des N liaisons actives résulte en ce que le trafic est commuté sur une des M liaisons disponibles. C'est normalement un processus en trois étapes : d'abord, la défaillance du plan de données est détectée au nœud de sortie et rapportée (notification) puis une liaison de protection est choisie, et finalement, les LSP sur la liaison défaillante sont déplacés sur la liaison de protection. Si la réversion est supportée, une quatrième étape est incluse, c'est-à-dire, le retour du trafic à la liaison active (quand la liaison active a récupéré de la défaillance). La protection de portée 1:1 est décrite au paragraphe 2.3. Le paragraphe 2.4, décrit la protection de portée M:N, où $M \leq N$.

2.1 Protection unidirectionnelle 1+1 dédiée

Supposons qu'un LSP bidirectionnel soit acheminé sur la liaison i entre deux nœuds A et B. Avec la protection unidirectionnelle 1+1, une liaison dédiée j est pré-allouée pour protéger la liaison active i. Le trafic du LSP est ponté en permanence sur les deux liaisons au nœud d'entrée, et le nœud de sortie choisit le trafic normal à partir d'une des liaisons, i ou j. Si un nœud (A ou B) détecte une défaillance d'une portée, il invoque de façon autonome un processus pour recevoir le trafic provenant de la portée de protection. Donc, il est possible que le nœud A choisisse le signal provenant de la liaison i dans la direction de B à A du LSP, et que le nœud B choisisse le signal provenant de la liaison j dans la direction de A à B.

La fonctionnalité suivante est exigée pour la protection de portée unidirectionnelle 1+1 :

- Acheminement : une seule liaison TE englobant à la fois les liaisons actives et de protection DEVRAIT être annoncée avec un type de protection de liaison "dédiée 1+1", avec les paramètres de bande passante pour la liaison active. Lorsque les ressources sont consommées/libérées, les paramètres de bande passante de la liaison TE sont ajustés en conséquence. Le codage du type de protection de liaison et les paramètres de bande passante dans IS-IS sont spécifiés dans la [RFC4205]. Le codage de ces informations dans OSPF est spécifié dans la [RFC4203].

- Signalisation : l'objet/TLV Protection de liaison DEVRAIT être utilisé pour demander la protection de liaison "dédiée 1+1" pour ce LSP. Cet objet/TLV est défini dans la [RFC3471]. Si l'objet/TLV Protection de liaison n'est pas utilisé, le choix de la liaison est une affaire de politique locale. Aucune signalisation supplémentaire n'est requise quand une reprise sur défaillance se produit.

- Gestion de liaison : les deux nœuds DOIVENT avoir une vue cohérente de l'association de protection de liaison pour les portées. Cela peut être fait en utilisant le protocole de gestion de liaison (LMP, *Link Management Protocol*) [RFC4204], ou si LMP n'est pas utilisé, cela DOIT être configuré manuellement.

2.2 Protection bidirectionnelle 1+1 dédiée

Supposons qu'un LSP bidirectionnel soit acheminé sur une liaison i entre deux nœuds A et B. Avec la protection bidirectionnelle 1+1, une liaison dédiée j est pré-allouée pour protéger la liaison active i. Le trafic du LSP est dupliqué en permanence sur les deux liaisons, et dans des conditions normales, le trafic provenant de la liaison i est reçu par les nœuds A et B (dans les directions appropriées). Une défaillance affectant la liaison i résulte en ce que A et B commutent tous les deux le trafic sur la liaison j dans les directions respectives. Noter qu'une forme de signalisation est requise pour assurer que A et B commencent tous deux à recevoir le trafic provenant de la liaison de protection.

Les étapes de base de la protection de portée 1+1 bidirectionnelle sont les suivantes :

1. Si un nœud (A ou B) détecte la défaillance de la liaison active (ou une dégradation de la qualité du signal sur la liaison active) il DEVRAIT commencer à recevoir sur la liaison de protection et envoyer un message Demande de commutation *(Switchover Request)* de façon fiable à l'autre nœud (B ou A, respectivement). Ce message DEVRAIT indiquer l'identité de la liaison active défaillante et fournir les autres informations pertinentes.

2. À réception du message Demande de commutation, un nœud DOIT commencer à recevoir de la liaison de protection et envoyer un message Réponse de commutation à l'autre nœud (A ou B, respectivement). Parce que les deux portées active/protection sont exposées à l'acheminement et à la signalisation comme une seule liaison, la commutation DEVRAIT être transparente à l'acheminement et la signalisation.

La fonctionnalité suivante est requise pour le protection de portée 1+1 bidirectionnelle :
- Les procédures d'acheminement sont les mêmes que dans le 1+1 unidirectionnel.
- Les procédures de signalisation sont les mêmes que dans le 1+1 unidirectionnel.
- En plus des procédures décrites dans 1+1 (unidirectionnel), un message Demande de commutation DOIT être utilisé pour signaler la demande de commutation. Cela peut être fait en utilisant LMP [RFC4204]. Noter que des mécanismes fondés sur GMPLS PEUVENT n'être pas nécessaires quand la technologie de portée sous-jacente (transport) fournit un tel mécanisme.

2.3 Protection dédiée 1:1 avec trafic supplémentaire

Considérons deux nœuds adjacents, A et B. Sous la protection 1:1, une liaison dédiée j entre A et B est pré-allouée pour protéger la liaison active i. La liaison j peut être en train de porter du trafic supplémentaire (préemptable). Une défaillance affectant la liaison i a pour résultat que le ou les LSP correspondants sont restaurés sur la liaison j. Le trafic supplémentaire

acheminé sur la liaison j peut devoir être préempté pour traiter les LSP qui doivent être restaurés.

Une fois qu'une faute est isolée/localisée, le ou les LSP affectés doivent être déplacés sur la liaison de protection. Le processus de déplacement d'un LSP d'une liaison (active) défaillante à une liaison de protection doit être initié par un des nœuds, A ou B. On se réfère à ce nœud comme au "maître". L'autre nœud est appelé "l'esclave". La détermination du maître et de l'esclave peut se fonder sur des informations configurées ou sur des exigences spécifiques du protocole.

Les étapes de base de la protection de portée 1:1 dédiées (en ignorant la réversion) sont les suivantes :

1. Si le maître détecte/localise un événement de défaillance de liaison, il invoque un processus pour allouer la liaison de protection au ou aux LSP affectés.

2. Si l'esclave détecte un événement de défaillance de liaison, il informe le maître de la défaillance en utilisant un message Indication de défaillance. Le maître invoque alors la même procédure qu'en (1) pour déplacer les LSP sur la liaison de protection. Si la liaison de protection porte du trafic supplémentaire, l'esclave arrête d'utiliser la portée pour le trafic supplémentaire.

3. Une fois que la procédure de protection de portée est invoquée chez le maître, il demande à l'esclave de commuter le ou les LSP affectés sur la liaison de protection. Avant cela, si la liaison de protection porte du trafic supplémentaire, le maître arrête d'utiliser la portée pour ce trafic (c'est-à-dire, le trafic est éliminé par le maître et n'est pas transmis dans ou de la liaison de protection).

4. L'esclave envoie un accusé de réception au maître. Avant cela, l'esclave arrête d'utiliser la liaison de protection pour le trafic supplémentaire (c'est-à-dire, le trafic est éliminé par l'esclave et n'est pas transmis dans ou de la liaison de protection). Il commence alors à envoyer le trafic normal sur la liaison de protection choisie.

5. Quand le maître reçoit l'accusé de réception, il commence à envoyer et recevoir le trafic normal sur la nouvelle liaison. La commutation du ou des LSP est donc achevée.

Note : Bien que ce mécanisme implique plus d'élimination de trafic que nécessaire, il est préféré aux possibles mauvaises connexions durant le processus de récupération.

D'après la description ci-dessus, il est clair que la protection de portée 1:1 peut exiger jusqu'à trois messages de signalisation pour chaque portée défaillante : un message Indication de défaillance, un message Demande de commutation de LSP, et un message Réponse de commutation de LSP. De plus, il est possible de commuter plusieurs LSP de la portée active à la portée de protection simultanément.

Les fonctions suivantes sont exigées pour la protection de portée dédiée 1:1 :

- La préemption DOIT être prise en charge pour s'accommoder du trafic supplémentaire.

- Acheminement : Une seule liaison TE englobant les deux liaisons active et de protection est annoncée avec un type de protection de liaison "dédiée 1:1". Si du trafic supplémentaire est pris en charge sur la liaison de protection, alors les paramètres de bande passante pour la liaison de protection DOIVENT aussi être annoncés. La différentiation entre la bande passante pour les liaisons active et de protection est faite en utilisant les mécanismes de priorité. En d'autres termes, le réseau DOIT être configuré de telle sorte que la bande passante de priorité X ou inférieure soit considérée comme du trafic supplémentaire.
  Si il y a une défaillance sur la liaison active, le trafic normal est alors commuté à la liaison de protection, préemptant le trafic supplémentaire si nécessaire. La bande passante pour la liaison de protection DOIT être ajustée en conséquence.

- Signalisation : pour établir un LSP sur la liaison active, l'objet/TLV Protection de liaison indiquant "dédiée 1:1" DEVRAIT être inclus dans le message de demande de signalisation pour ce LSP. Pour établir un LSP sur la liaison de protection, la priorité appropriée (indiquant Trafic supplémentaire) DEVRAIT être utilisée pour ce LSP. Ces objet/TLV sont définis dans la [RFC3471]. Si l'objet/TLV Protection de liaison n'est pas utilisé, le choix de la liaison est une affaire de politique locale.

- Gestion de liaison : les deux nœuds DOIVENT avoir une vue cohérente de l'association de liaison pour les portées. Cela peut être fait en utilisant LMP [RFC4204] ou via configuration manuelle.

- Quand une défaillance de liaison est détectée chez l'esclave, un message Indication de défaillance DOIT être envoyé au maître informant le nœud de la défaillance de liaison.

2.4 Protection partagée M:N

La protection partagée M:N est décrite par rapport aux deux nœuds voisins, A et B. Le scénario considéré est le suivant :

- À tout moment, il y a deux ensembles de liaisons entre A et B, c'est-à-dire, un ensemble actif de N liaisons (bidirectionnelles) portant le trafic soumis à protection et un ensemble de protection de M liaisons (bidirectionnelles). Une liaison de protection peut porter du trafic supplémentaire. Il n'y a pas de relation a priori entre les deux ensembles de liaisons, mais la valeur de M et N PEUT être pré-configurée. Les liaisons spécifiques dans l'ensemble de protection PEUVENT être pré-configurées pour être physiquement diverses pour éviter la possibilité d'événements de défaillance affectant une large proportion des liaisons (ainsi que les liaisons actives).

- Quand une liaison dans l'ensemble actif est affectée par une défaillance, le trafic normal est dérouté sur une liaison de l'ensemble de protection, si une telle liaison est disponible. Noter qu'une telle liaison peut être en train de porter plus d'un LSP, par exemple, une liaison OC-192 portant quatre LSP STS-48.

- Plus d'une liaison de l'ensemble actif peut être affectée par le même événement de défaillance. Dans ce cas, il peut ne pas y avoir un nombre adéquat de liaisons pour accommoder tout le trafic affecté porté par les liaisons actives défaillantes. L'ensemble des liaisons actives affectées qui sont en fait restaurées sur les liaisons de protection disponibles est alors soumis aux politiques (par exemple, sur la base des priorités relatives du trafic actif). Ces politiques ne sont pas spécifiées dans ce document.

- Quand le trafic normal doit être dérouté d'une liaison défaillante dans l'ensemble actif à une liaison de protection, la décision de quelle liaison de protection est choisie est toujours prise par un des nœuds, A ou B. Ce nœud est considéré comme le "maître" et il est exigé que tous deux appliquent toutes les politiques et choisissent la liaison spécifiée pour dérouter le trafic actif. L'autre nœud est considéré comme "esclave". La détermination du maître et de l'esclave PEUT être fondée sur des informations configurées, des exigences spécifiques du protocole, ou par suite d'une procédure de découverte de voisin.

- Les événements de défaillance sont détectés par les mécanismes de couche transport, si disponibles (par exemple, le signal d'indication d'alarme/indication de défaut distant (AIS, *Alarm Indication Signal*/(RDI, *Remote Defect Indication*) SONET). Comme les liaisons bidirectionnelles sont formées par une paire de liaisons unidirectionnelles, une défaillance dans la liaison de A à B est normalement détectée par B, et une défaillance dans la direction opposée est détectée par A. Il est possible qu'une défaillance affecte simultanément les deux directions de la liaison bidirectionnelle. Dans ce cas, A et B vont concurremment détecter les défaillances, dans la direction B à A et dans la direction A à B, respectivement.

Les étapes de base de la protection M:N (en ignorant la réversion) sont les suivantes :

1. Si le maître détecte une défaillance d'une liaison active, il invoque de façon autonome un processus pour allouer une liaison de protection au trafic affecté.

2. Si l'esclave détecte une défaillance d'une liaison active, il DOIT informer le maître de la défaillance en utilisant un message Indication de défaillance. Le maître invoque alors la même procédure que ci-dessus pour allouer une liaison de protection. (Il est possible que le maître ait lui-même détecté la même défaillance, par exemple, une défaillance affectant simultanément les deux directions d'une liaison.)

3. Une fois que le maître a déterminé l'identité de la liaison de protection, il l'indique à l'esclave et demande la commutation du trafic (en utilisant un message "Demande de commutation"). Avant cela, si la liaison de protection porte du trafic supplémentaire, le maître arrête d'utiliser la liaison pour ce trafic (c'est-à-dire, le trafic est éliminé par le maître et n'est pas transmis dans ou hors de la liaison de protection).

4. L'esclave renvoie un message "Réponse de commutation" au maître. Avant cela, si la liaison de protection choisie porte du trafic qui pourrait être préempté, l'esclave arrête d'utiliser la liaison pour ce trafic (c'est-à-dire, le trafic est éliminé par l'esclave et n'est pas transmis dans ou hors de la liaison de protection). Il commence alors à envoyer le trafic normal sur la liaison de protection choisie.

5. Quand le maître reçoit la réponse de commutation, il commence à envoyer et recevoir le trafic qui était précédemment porté sur la liaison maintenant défaillante sur la nouvelle liaison.

Note : Bien que ce mécanisme implique plus d'élimination de trafic que nécessaire, il est préféré aux possibles mauvaises

connexions durant le processus de récupération.

D'après la description ci-dessus, il est clair que la restauration de portée M:N (impliquant la récupération du LSP local) PEUT exiger jusqu'à trois messages pour chaque liaison active commutée : un message Indication de défaillance, un message Demande de commutation, et un message Réponse de commutation.

Les fonctions suivantes sont nécessaires pour la restauration de portée M:N :

- La préemption DOIT être supportée pour s'accommoder du trafic supplémentaire.

- Acheminement : une seule liaison TE englobant les deux ensembles de liaisons actif et de protection devrait être annoncée avec un type de protection de liaison "M:N partagé". Si du trafic supplémentaire est pris en charge sur un ensemble de liaisons, alors les paramètres de bande passante de l'ensemble de liaisons DOIVENT aussi être annoncés. La différentiation entre la bande passante pour les liaisons actives et de protection est faite en utilisant les mécanismes de priorité.
  Si il y a une défaillance sur une liaison active, le ou les LSP affectés DOIVENT alors être commutés sur une liaison de protection, en préemptant le trafic supplémentaire si nécessaire. La bande passante pour la liaison de protection DOIT être ajustée en conséquence.

- Signalisation : pour établir un LSP sur la liaison active, l'objet/TLV Protection de liaison indiquant "M:N partagé" DEVRAIT être inclus dans le message de demande de signalisation pour ce LSP. Pour établir un LSP sur la liaison de protection, la propriété appropriée (indiquant du trafic supplémentaire) DEVRAIT être utilisée. Ces objets/TLV sont définis dans la [RFC3471]. Si l'objet/TLV Protection de liaison n'est pas utilisé, le choix de la liaison est l'affaire de la politique locale.

- Pour la gestion de liaison, les deux nœuds DOIVENT avoir une vue cohérente de l'association de protection de liaison pour les liaisons. Cela peut être fait en utilisant LMP [RFC4204] ou via configuration manuelle.

2.5 Messages

Les messages suivants sont utilisés dans les procédures de protection de portée locale.

Ces messages DEVRAIENT être livrés de façon fiable. Donc, les mécanismes de protocole utilisés pour livrer ces messages DEVRAIENT fournir le séquençage, l'accusé de réception, et la retransmission. Le protocole DEVRAIT aussi traiter les situations où le ou les messages ne peuvent pas être livrés.

Les messages décrits dans les sous paragraphes suivants sont abstraits ; leur format et codage vont être décrits dans des documents séparés.

2.5.1 Message Indication de défaillance

Ce message est envoyé de l'esclave au maître pour indiquer l'identité d'une ou plusieurs liaisons actives défaillantes. Ce message PEUT n'être pas nécessaire quand la technologie de plan de transport fournit elle même une telle notification.

Le nombre de liaisons incluses dans le message dépend du nombre de défaillances détectées au sein d'une fenêtre de temps par le nœud envoyeur. Un nœud PEUT choisir d'envoyer des messages Indication de défaillance séparés dans le but d'achever la récupération pour une certaine liaison dans des contraintes de temps spécifiques de la mise en œuvre.

2.5.2 Message Demande de commutation

Dans la protection de portée bidirectionnelle 1+1, ce message est utilisé pour coordonner la fonction de sélection aux deux nœuds. Ce message est généré au nœud qui détecte la défaillance.

Dans la protection de portée dédiée 1:1 et M:N partagée, ce message est utilisé comme une demande de commutation de LSP. Ce message est envoyé (de façon fiable) du nœud maître au nœud esclave pour indiquer que le ou les LSP sur la liaison active (défaillante) peuvent être commutés sur une liaison de protection disponible. Si il en est ainsi, l'identifiant de la liaison de protection, ainsi que les étiquettes de LSP (si nécessaire) DOIVENT être indiqués. Ces identifiants DOIVENT être cohérents avec ceux utilisés dans la signalisation GMPLS.

Une liaison active peut porter plusieurs LSP. Comme le trafic normal porté sur la liaison active est commuté à la liaison de protection, il est possible que les LSP sur la liaison active soient transposés sur la liaison de protection sans re-signaler chaque LSP individuel. Par exemple, si la mise en faisceau de liaisons [RFC4201] est utilisée lorsque les liaisons actives et de protection sont transposées en liaisons composantes, et si les étiquettes sont les mêmes sur les liaisons active et de protection, il est possible de changer les liaisons composantes sans qu'il soit besoin de re-signaler chaque LSP individuel. Facultativement, les étiquettes PEUVENT devoir être explicitement coordonnées entre les deux nœuds. Dans ce cas, le message Demande de commutation DEVRAIT porter les nouvelles transpositions d'étiquettes.

Le maître peut n'être pas capable de trouver une liaison pour accommoder toutes les liaisons actives défaillantes. Donc, si ce message est généré en réponse à un message Indication de défaillance provenant de l'esclave, alors l'ensemble des liaisons défaillantes du message PEUT être un sous ensemble des liaisons reçues dans le message Indication de défaillance. Selon les contraintes de temps, le maître peut commuter le trafic normal de l'ensemble de liaisons défaillantes sur de plus petits lots. Donc, un seul message Indication de défaillance PEUT résulter en l'envoi par le maître de plus d'un message Demande de commutation au même nœud esclave.

2.5.3 Message Réponse de commutation

Ce message est envoyé (de façon fiable) de l'esclave au maître pour indiquer l'achèvement (ou la défaillance) de la commutation chez l'esclave. Dans ce message, l'esclave PEUT indiquer qu'il ne peut pas commuter sur la liaison libre correspondante pour une raison quelconque. Dans ce cas, le maître et l'esclave notifient à l'utilisateur (opérateur) l'échec de la commutation. Une notification de la défaillance PEUT aussi être utilisée comme déclencheur d'une récupération de bout en bout.

2.6. Prévention des connexions non voulues

Une connexion non voulue se produit quand du trafic provenant d' une mauvaise source est livré à un receveur. Cela DOIT être empêché durant la commutation de protection. Ceci est principalement un souci quand la liaison de protection est utilisée pour porter du trafic supplémentaire. Dans ce cas, on DOIT s'assurer que le trafic du LSP commuté de la liaison active (défaillante) à la liaison de protection n'est pas livré au receveur du trafic préempté. Donc, dans le flux de messages décrit ci-dessus, le nœud maître DOIT déconnecter (tout) le trafic préempté sur la liaison de protection choisie avant d'envoyer la demande de commutation. Le nœud esclave DOIT aussi déconnecter le trafic préempté avant d'envoyer la réponse de commutation. De plus, le nœud maître DEVRAIT commencer à recevoir le trafic pour le LSP protégé provenant de la liaison de protection. Finalement, le nœud maître DEVRAIT commencer d'envoyer le trafic protégé sur la liaison de protection à réception de la réponse de commutation.

3. Protection et restauration (de chemin) de bout en bout

La protection et la restauration de chemin de bout en bout se réfère à la récupération d'un LSP entier de l'initiateur à la terminaison. Supposons que le chemin principal d'un LSP soit acheminé depuis l'initiateur (Nœud A) à la terminaison (Nœud B) par un ensemble de nœuds intermédiaires.

Les paragraphes qui suivent décrivent les trois schémas de protection de bout en bout proposés précédemment et les étapes fonctionnelles nécessaires pour les mettre en œuvre.

3.1 Protection unidirectionnelle 1+1

Un chemin dédié de remplacement, disjoint des ressources est pré-établi pour protéger le LSP. Le trafic est simultanément envoyé sur les deux chemins et reçu d'un des chemins fonctionnels par les nœuds d'extrémité A et B.

Aucune signalisation explicite n'est impliquée par ce mode de protection.

3.2 Protection bidirectionnelle 1+1

Un chemin dédié de remplacement, disjoint des ressources est pré-établi pour protéger le LSP. Le trafic est simultanément envoyé sur les deux chemins ; dans les conditions normales, le trafic provenant du chemin actif est reçu par les nœuds A et B (dans les directions appropriées). Une défaillance affectant le chemin actif résulte en ce que A et B commutent tous deux le trafic sur le chemin de protection dans les directions respectives.

Noter que cela exige la coordination entre les nœuds d'extrémité pour commuter sur le chemin de protection.

Les étapes de base dans la protection bidirectionnelle de chemin 1+1 sont les suivantes :

o Détection de défaillance : il y a deux possibilités pour cela.
1. Un nœud dans le chemin actif détecte un événement de défaillance. Ce nœud DOIT envoyer un message Indication de défaillance vers le nœud d'extrémité amont ou/et aval du LSP (nœud A ou B). Ce message PEUT être transmis le long du chemin actif ou acheminé sur un chemin différent si le réseau a une intelligence d'acheminement générale.
   Les mécanismes fournis par le plan de transport des données PEUVENT aussi être utilisés pour cela, si disponibles.
2. Les nœuds d'extrémité (A ou B) détectent eux-mêmes la défaillance (par exemple, perte du signal).

o Commutation : les actions prises quand un nœud d'extrémité détecte une défaillance dans le chemin actif sont les suivantes : commencer à recevoir depuis le chemin de protection ; en même temps, envoyer un message Demande de commutation à l'autre nœud d'extrémité pour activer la commutation à l'autre extrémité.

L'action prise quand un nœud d'extrémité reçoit un message Demande de commutation est la suivante : commencer à recevoir depuis le chemin de protection ; en même temps, envoyer un message Réponse de commutation à l'autre nœud d'extrémité.

Les mécanismes GMPLS de signalisation PEUVENT être utilisés pour signaler (de façon fiable) le message Indication de défaillance, ainsi que les messages Demande et Réponse de commutation. Ces messages PEUVENT être transmis le long du chemin de protection si aucune autre intelligence d'acheminement n'est disponible dans le réseau.

3.2.1 Identifiants

Identifiant de LSP : identifiant unique pour chaque LSP. L'identifiant de LSP est dans la portée de l'identifiant de source et de l'identifiant de destination.

Identifiant de source : identifiant de la source (par exemple, une adresse IP).

Identifiant de destination : identifiant de la destination (par exemple, une adresse IP).

3.2.2 Informations de nœuds

Chaque nœud qui est sur le chemin actif ou de protection d'un LSP DOIT avoir connaissance de l'identifiant de LSP. Si le réseau ne fournit pas d'intelligence d'acheminement, des informations sur les nœuds PEUVENT aussi inclure les nœuds précédents et suivants dans le LSP afin que les messages relatifs à la restauration puissent être transmis correctement. Quand le réseau fournit une intelligence générale d'acheminement, les messages PEUVENT être transmis le long de chemins autres que celui du LSP.

Aux nœuds de point d'extrémité, les chemins actif et de protection DOIVENT être associés. L'association de ces chemins PEUT être provisionnée en utilisant la signalisation ou elle PEUT être configurée quand le provisionnement de LSP n'implique pas de signalisation (par exemple, le provisionnement par un système de gestion). Les informations relatives à l'association DOIVENT rester jusqu'à ce que le LSP soit explicitement dé-provisionné.

3.2.3 Message Indication de défaillance de bout en bout

Ce message est envoyé (de façon fiable) par un nœud intermédiaire vers la source d'un LSP. Par exemple, un tel nœud pourrait avoir tenté une protection de portée locale et échoué. Ce message PEUT n'être pas nécessaire si la couche de transport des données fournit des mécanismes pour la notification de défaillance de LSP par les points d'extrémité (c'est-à-dire, si les points d'extrémité du LSP sont colocalisés avec un domaine correspondant de maintenance/récupération de données (de transport)).

Considérons un nœud qui détecte une défaillance de liaison. Le nœud DOIT déterminer l'identité de tous les LSP qui sont affectés par la défaillance de la liaison et envoyer un message Indication de défaillance de bout en bout à la source de chaque LSP. Pour des raisons d'adaptabilité, les messages Indication de défaillance PEUVENT contenir l'identité et l'état de plusieurs LSP plutôt que d'un seul. Chaque nœud intermédiaire qui reçoit un tel message DOIT le transmettre au prochain nœud approprié afin que le message atteigne finalement le LSP source. Cependant, il n'est pas exigé que le flux de

messages s'écoule vers la source le long du même chemin que le LSP défaillant. De plus, si un nœud intermédiaire génère lui-même un message Indication de défaillance, il DEVRAIT y avoir un mécanisme pour supprimer toutes les sources sauf une des messages Indication de défaillance. Finalement, le message Indication de défaillance DOIT être envoyé de façon fiable du nœud qui détecte la défaillance au LSP source. La fiabilité PEUT être réalisée, par exemple, en retransmettant le message jusqu'à la réception d'un accusé de réception. Cependant, la retransmission des messages Indication de défaillance NE DEVRAIT PAS causer d'autres éliminations de messages. Cela PEUT être réalisé par une configuration appropriée et l'utilisation de mécanismes de contrôle d'encombrement et de flux.

3.2.4 Message Accusé de réception de défaillance de bout en bout

Ce message est envoyé par le nœud source pour accuser réception d'un message Indication de défaillance de bout en bout. Ce message est envoyé à l'origine du message Indication de défaillance. Le message Accusé de réception DEVRAIT être envoyé pour chaque message Indication de défaillance reçu. Chaque nœud intermédiaire qui reçoit le message Accusé de réception de défaillance DOIT le transmettre vers la destination du message. Cependant, il n'est pas exigé que ce message s'écoule vers la destination le long du même chemin que le LSP défaillant.

Ce message PEUT n'être pas nécessaire si d'autres moyens de s'assurer de la livraison fiable du message sont utilisés.

3.2.5 Message Demande de commutation de bout en bout

Ce message est généré par le nœud source qui reçoit une indication de défaillance dans un LSP. Il est envoyé à la destination du LSP, et il porte l'identifiant du LSP à restaurer. Le message Demande de commutation de bout en bout DOIT être envoyé de façon fiable de la source à la destination du LSP.

3.2.6 Message Réponse de commutation de bout en bout

Ce message est envoyé par le nœud de destination qui reçoit un message Demande de commutation de bout en bout vers la source du LSP. Ce message DEVRAIT identifier le LSP sur lequel se fait la commutation. Ce message DOIT être transmis en réponse à chaque message Demande de commutation de bout en bout reçu et PEUT indiquer un résultat positif ou négatif.

3.3 Restauration en maillage partagé

La restauration en maillage partagé se réfère aux schémas dans lesquels les chemins de protection pour plusieurs LSP partagent des ressources communes de liaison et de nœud. Dans ces schémas, la capacité de protection est pré-réservée, c'est-à-dire, la capacité de liaison est allouée pour protéger un ou plusieurs LSP, mais une action explicite est exigée pour instancier une protection de LSP spécifique. Cela exige la signalisation de restauration le long du chemin de protection. Normalement, la capacité de protection est seulement partagée entre les LSP dont les chemins actifs sont physiquement divers. Ce critère peut être appliqué quand il y a un provisionnement du chemin de protection. Précisément, des messages de signalisation relatifs au provisionnement peuvent porter des informations sur le chemin actif aux nœuds le long du chemin de protection. Cela peut être utilisé comme contrôle d'admission d'appel pour accepter/rejeter des connexions le long du chemin de protection sur la base de l'identification des ressources utilisées pour le chemin principal.

Donc, la restauration en maillage partagé est conçue pour protéger un LSP après un seul événement de défaillance, c'est-à-dire, une défaillance qui affecte le chemin actif d'au plus un LSP partageant la capacité de protection. Il est possible qu'un chemin de protection ne puisse pas réussir à être activé quand plusieurs événements concurrents de défaillance se produisent. Dans ce cas, la capacité de restauration en maillage partagé peut être revendiquée par plus d'un LSP défaillant et le chemin de protection peut être activé seulement pour l'un d'eux (au plus).

Pour mettre en œuvre la restauration en maillage partagé, l'identifiant et les informations de nœuds relatives à la signalisation le long du chemin de contrôle sont tels que définis pour la protection 1+1 aux paragraphes 3.2.1 et 3.2.2. De plus, chaque nœud DOIT aussi garder les informations (locales) nécessaires pour établir le plan de données du chemin de protection. Ces informations DOIVENT indiquer les ressources locales à allouer, le tissu d'interconnexions à établir pour activer le chemin, etc. La nature précise de ces informations va dépendre du type de nœud et de LSP (le document de signalisation GMPLS décrit les différents types de commutateurs [RFC3471]). Elle va aussi dépendre de si les informations sont de granularité fine ou grossière. Par exemple, des informations de granularité fine vont indiquer la pré-sélection de tous les détails relevant de l'activation du chemin de protection, comme la liaison sortante, les étiquettes, etc. Les informations de granularité grossière vont par ailleurs permettre que certains détails soient déterminés durant l'activation du

chemin de protection. Par exemple, les ressources de protection peuvent être présélectionnées au niveau d'une liaison TE, tandis que la sélection de la liaison composante spécifique et d'étiquette se produit durant l'activation du chemin de protection.

Alors que la spécification plus grossière permet une certaine souplesse dans le choix de la ressource précise à activer, elle ajoute aussi de la complexité dans la prise de décision et la signalisation durant la phase critique en temps de la restauration. De plus, les procédures pour l'allocation de la bande passante aux chemins de protection DOIVENT tenir compte des ressources totales d'une liaison TE afin que les exigences de survie à une seule défaillance soient satisfaites.

3.3.1 Message Indication et Accusé de réception de défaillance de bout en bout

Les procédures et messages d'indication et d'accusé de réception de défaillance de bout en bout sont comme défini aux paragraphes 3.2.3 et 3.2.4.

3.3.2 Message Demande de commutation de bout en bout

Ce message est généré par le nœud source qui reçoit une indication de défaillance dans un LSP. Il est envoyé à la destination du LSP le long du chemin de protection, et il identifie le LSP à restaurer. Si un nœud intermédiaire est incapable d'établir des interconnexions pour le chemin de protection, il est alors souhaitable qu'aucun autre nœud dans le chemin n'établisse d'interconnexions pour le chemin. Cela permettrait que des chemins de restauration à maillage partagé soient utilisés efficacement.

Le message Commutation de bout en bout DOIT être envoyé de façon fiable de la source à la destination du LSP le long du chemin de protection.

3.3.3 Message Réponse de commutation de bout en bout

Ce message est envoyé par le nœud de destination qui reçoit un message Demande de commutation de bout en bout vers la source du LSP, le long du chemin de protection. Ce message DEVRAIT identifier le LSP qui va être commuté. Avant d'activer la bande passante secondaire à chaque bond le long du chemin, le trafic supplémentaire (si il est utilisé) DOIT être éliminé et non transmis.

Ce message DOIT être transmis en réponse à chaque message Demande de commutation de bout en bout reçu.

4. Réversion et autres procédures administratives

La réversion se réfère au processus de restitution d'un LSP au chemin actif original après qu'une défaillance est supprimée et que le chemin est réparé. La réversion s'applique aux LSP de portée locale et de chemin protégé de bout en bout. La réversion est désirée pour les raisons suivantes. D'abord, le chemin de protection peut n'être pas optimal en comparaison du chemin actif du point de vue de l'acheminement et de la consommation de ressources. Ensuite, déplacer un LSP sur son chemin actif permet que les ressources de protection soient utilisées pour protéger les autres LSP. La réversion a l'inconvénient de causer une seconde interruption de service. L'utilisation de la réversion est une option de l'opérateur. La réversion implique qu'un chemin actif reste alloué au LSP qui était originellement acheminé sur lui, même après une défaillance. Il est important d'avoir des mécanismes qui permettent d'effectuer la réversion avec une interruption minimale de service pour le consommateur. Cela peut être réalisé en utilisant une approche de "pontage et commutation" (souvent appelée "faire avant la cassure").

Les étapes de base impliquées dans le pontage et commutation sont les suivantes :

1. le nœud source commence le processus en "pontant" le trafic normal sur les deux chemins (ou liaisons dans le cas de la protection de portée) actif et de protection.

2. Une fois achevé le processus de pontage, le nœud source envoie un message Demande de pontage et commutation à la destination, identifiant le LSP et les autres informations nécessaires pour effectuer la réversion. À réception de ce message, la destination choisit le trafic provenant du chemin actif. En même temps, il ponte le trafic transmis sur les deux chemins actif et de protection.

3. La destination envoie alors un message Réponse de pontage et commutation à la source pour confirmer l'achèvement de l'opération.

4. Quand la source reçoit ce message, elle commute pour recevoir du chemin actif, et arrête de transmettre le trafic sur le chemin de protection. La source envoie alors un message Pontage et commutation achevés à la destination pour confirmer que le LSP a été restauré.

5. À réception de ce message, la destination arrête de transmettre le long du chemin de protection et désactive le LSP le long de ce chemin. La procédure de désactivation devrait supprimer les interconnexions le long du chemin de protection (et libérer les ressources pour être utilisées à restaurer d'autres défaillances).

Les procédures administratives autres que la réversion incluent la capacité de forcer une commutation (de actif à protection ou vice versa) et de verrouiller la commutation, c'est-à-dire, empêcher administrativement un LSP de passer de actif à protection. Ces conditions administratives doivent être prises en charge par la signalisation.

5. Discussion

5.1 Priorités de LSP durant la protection

Dans la protection de portée, un événement de défaillance pourrait affecter plus d'une liaison active et il pourrait y avoir moins de liaisons de protection que le nombre de liaisons actives défaillantes. De plus, une liaison active peut contenir plusieurs LSP de priorités variées. Dans ce scénario, une décision doit être prise sur quelles liaisons actives (et donc LSP) devraient être protégées. Cette décision PEUT être fondée sur les priorités de LSP.

En général, un nœud peut détecter les défaillances en séquence, c'est-à-dire, toutes les liaisons actives défaillantes peuvent n'être pas détectées simultanément, mais seulement à la suite les une des autres. Dans ce cas, comme selon les procédures de signalisation proposées, les LSP sur une liaison active PEUVENT être commutés sur une certaine liaison de protection, mais une autre défaillance (d'une liaison active portant des LSP de priorité supérieure) peut être détectée peu après. Dans ce cas, les nouveaux LSP peut expulser ceux précédemment commutés sur la liaison de protection.

Dans le cas de restauration en maillage partagé de bout en bout, les priorités PEUVENT être mises en œuvre pour allouer des ressources de liaison partagées sous plusieurs scénarios de défaillance. Comme décrit au paragraphe 3.3, plus d'un LSP peut revendiquer des ressources partagées sous plusieurs scénarios de défaillance. Si de telles ressources sont d'abord allouées à un LSP de priorité inférieure, elles PEUVENT devoir être réclamées et allouées à un LSP de priorité supérieure.

6. Considérations sur la sécurité

Un certain nombre de menaces pour la sécurité PEUVENT être rencontrées suite à l'échange de messages et informations, comme précisé dans ce document. Des exemples incluent l'interception, l'usurpation d'identité, la modification, et la répétition des messages de contrôle. Donc, les exigences de sécurité suivantes sont applicables aux mécanismes de ce document.

- La signalisation DOIT être capable d’assurer l'authentification, l'intégrité, et la protection contre les attaques en répétition.

- La confidentialité et la protection de la vie privée ne sont pas exigées. Seule l'authentification est requise pour assurer que les messages de signalisation sont originaires du bon endroit et n'ont pas été modifiés dans le transit.

- La protection de l'identité des points d'extrémité du plan de données (dans les messages Indication de défaillance) n'est pas exigée.

Les conséquences d'une protection mal sécurisée peuvent augmenter le risque de déclenchement d'actions de récupération suite à de faux messages Indication de défaillance, incluant des identifiants de LSP qui ne sont pas défaillants. Des telles informations pourraient ensuite déclencher l'initiation de "fausses" actions de récupération alors qu'il n'y a pas de raison de le faire. De plus, si l'identification du LSP est altérée à partir d'un message Indication de défaillance, les actions de récupération vont impliquer des nœuds pour lesquels les LSP n’indiquent aucune condition de défaillance ou pour lesquels aucun message Indication de défaillance n'a été reçu. Les conséquences de telles actions ne sont pas prévisibles et PEUVENT conduire à la désynchronisation entre le plan de contrôle et le plan de données, ainsi qu'augmenter le risque de

mauvaises connexions. De plus, les conséquences d'une protection mal appliquée peuvent augmenter le risque de mauvaise connexion. En particulier, quand du trafic supplémentaire est impliqué, il est aisément possible de livrer le mauvais trafic à la mauvaise destination. De même, une intrusion qui établit ce qui paraît être un LSP de protection valide et cause en fait une faute peut être capable de dérouter le trafic.

De plus, l'altération d'un échange d'informations d'acheminement peut aussi avoir un effet sur l'ingénierie du trafic. Donc, tous les mécanismes utilisés pour sécuriser et authentifier la transmission des informations d'acheminement DEVRAIENT être appliqués dans le présent contexte.

7. Contributeurs

Ce document a été produit par de nombreuses personnes de l'équipe de conception Protection et Restauration du groupe de travail CCAMP. Les auteurs suivants ont contribué au présent document:

Deborah Brungard (AT&T)
200 S. Laurel Ave.
Middletown, NJ 07748, USA
mél : dbrungard@att.com

Sudheer Dharanikota
mél : sudheer@ieee.org

Guangzhi Li (AT&T)
180 Park Avenue,
Florham Park, NJ 07932,
mél: gli@research.att.com

Jonathan P. Lang (Sonos)
223 East De La Guerra Street
Santa Barbara, CA 93101,
mél : jplang@ieee.org

Dimitri Papadimitriou (Alcatel)
Francis Wellesplein, 1
B-2018 Antwerpen, Belgium
dimitri.papadimitriou@alcatel.be

Eric Mannie
eric_mannie@hotmail.com

Bala Rajagopalan
Microsoft India Development
Hyderabad, India
balar@microsoft.com

Yakov Rekhter (Juniper)
1194 N. Mathilda Avenue
Sunnyvale, CA 94089, USA
mél : yakov@juniper.net

8. Références

8.1 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)

[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.)*

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

[RFC4203] K. Kompella et autres, "Extensions OSPF pour la prise en charge de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. (*MàJ* RFC3630) *(P.S.)*

[RFC4204] J. Lang, éd., "Protocole de gestion de liaison (LMP)", octobre 2005. *(P.S.)*

[RFC4205] K. Kompella et Y. Rekhter, éd., "Extensions de système intermédiaire à système intermédiaire (IS-IS) pour la prise en charge de la commutation généralisée d'étiquettes multiprotocoles (GMPLS)", octobre 2005. (*Obsolète, voir* RFC5307) *(MàJ* RFC3784)

8.2 Références pour information

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

[RFC4427] E. Mannie et autres, "Terminologie de récupération (protection et restauration) pour le protocole généralisé de commutation d'étiquettes multiprotocoles (GMPLS)", mars 2006. *(Information)*

Adresse des éditeurs

Jonathan P. Lang
Sonos, Inc.
223 East De La Guerra Street
Santa Barbara, CA 93101
mél : jplang@ieee.org

Bala Rajagopalan
Microsoft India Development Center
Hyderabad, India
téléphone : +91-40-5502-7423
mél : balar@microsoft.com

Dimitri Papadimitriou
Alcatel
Francis Wellesplein, 1
B-2018 Antwerpen, Belgium
téléphone : +32 3 240-8491
mél : dimitri.papadimitriou@alcatel.be

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.