Groupe de travail Réseau
Request for Comments : 3479
Catégorie : En cours de normalisation

A. Farrel, éditeur, Movaz Networks, Inc.
février 2003
Traduction Claude Brière de L'Isle

Tolérance aux fautes pour le protocole de distribution d'étiquettes (LDP)

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

Note de l'IESG
La présente spécification comporte des procédures pour la détection des défaillances et la reprise sur une connexion TCP qui porte du trafic MPLS de contrôle de LDP, afin qu'il puisse être commuté sur une nouvelle connexion TCP. Elle ne fournit pas une approche générale de l'utilisation de plusieurs connexions TCP pour assurer cette sorte de tolérance aux fautes. Il manque à la spécification des lignes directrices adéquates pour le choix des valeurs des temporisateurs et des réessais se rapportant aux procédures de tolérance aux fautes de la connexion TCP. La spécification ne devrait pas servir de modèle pour la conception de connexions TCP tolérantes aux fautes pour un document futur, et les utilisateurs sont invités à vérifier très attentivement les configurations fondées sur la présente spécification qui pourraient subir des problèmes tels que des reprises prématurées sur défaillance.

Résumé
Les systèmes de protocole de commutation d'étiquettes multiprotocoles (MPLS) seront utilisés dans les cœurs de réseau où les temps d'arrêt de système doivent être tenus à un minimum absolu. De nombreux routeurs de commutation d'étiquettes (LSR, *Label Switching Router*) MPLS peuvent donc exploiter des matériels ou logiciels tolérants aux fautes (FT, *Fault Tolerant*) pour fournir une haute disponibilité des cœurs de réseau.

Les détails de la façon dont la tolérance aux fautes est réalisée pour les divers composants d'un LSR FT, y compris de protocole de distribution d'étiquettes (LDP, *Label Distribution Protocol*) de matériel de commutation et de TCP, sont spécifiques de la mise en œuvre. Le présent document identifie les questions qui dans la spécification de LDP [RFC3036] rendent difficile de mettre en œuvre un LSR FT en utilisant les protocoles de LDP actuels, et définit des améliorations à la spécification de LDP pour faciliter de telles mises en œuvre de LSR FT.

Les questions et les extensions décrites ici sont également applicables à la [RFC3212] "Établissement de LSP fondé sur la contrainte en utilisant LDP" (CR-LDP).

Table des matières

1. Conventions et terminologie utilisée dans le document

Les définitions des mots clés et des termes applicables à LDP et à CR-LDP sont hérités des [RFC3036] et [RFC3212].

Le terme "étiquette FT" est introduit dans le présent document pour indiquer une étiquette pour laquelle une opération tolérante aux fautes est utilisée. Une "étiquette non FT" n'est pas tolérante aux fautes et est traitée comme spécifié dans la [RFC3036].

Le terme "étiquette FT à numéro de séquence" est utilisé pour indiquer une étiquette FT qui est sécurisée en utilisant le numéro de séquence du TLV Protection FT décrit dans ce document.

Le terme "étiquette FT vérifiable-pointable" est utilisé pour indiquer une étiquette FT qui est sécurisée en utilisant les techniques de vérification-pointage décrites dans ce document.

Les extensions à LDP spécifiées dans ce document sont collectivement désignées comme "améliorations LDP FT".

Dans le contexte de ce document, "vérification-pointage" se réfère à un processus d'échange de messages qui confirme la réception et le traitement (ou la mémorisation sécurisée) de messages spécifiques du protocole.

Lorsque on parle des bits individuels dans le champ Fanion FT de 16 bits, les mots "bit" et "fanion" sont utilisés de façon interchangeable.

Dans les exemples cités, la notation suivante est utilisée : Ln : un LSP, par exemple L1.
Pn : un homologue LDP, par exemple P1.

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

2. Auteurs contributeurs

Le présent document est un travail collectif de plusieurs individus sur une période de plusieurs années. Le texte et le contenu de ce document ont été fournis par les contributions de l'éditeur et des co-auteurs énumérés à la section 15,

3. Introduction

Une forte disponibilité est normalement revendiquée par les fabricants d'équipements lorsque leur matériel réalise des niveaux de disponibilité d'au moins 99,999 % (cinq 9). Pour la mettre en œuvre, l'équipement doit être capable de récupérer de défaillances locales de matériel et logiciel par un processus connu sous le nom de tolérance aux fautes (FT).

L'approche usuelle de la FT implique de fournir des copies de sauvegarde du matériel et/ou logiciel. Lorsque une copie primaire est fautive, le traitement est basculé sur la copie de sauvegarde. Ce processus, appelé reprise sur défaillance, devrait résulter en une interruption minimale du plan de données.

Dans un système FT, les ressources de sauvegarde sont parfois provisionnées une pour une (1:1), parfois une pour plusieurs (1:n) et occasionnellement de plusieurs à plusieurs (m:n). Quel que soit le provisionnement de sauvegarde pratiqué, le système doit commuter automatiquement sur la sauvegarde en cas de défaillance du primaire, et l'état du logiciel et du matériel dans la sauvegarde doit être réglé de façon à dupliquer l'état du principal au moment de la défaillance.

3.1 Tolérance aux fautes pour MPLS

MPLS est une technologie qui sera utilisée dans les cœurs de réseaux où les temps d'arrêt du système doivent être gardés à un minimum absolu. De nombreux LSR MPLS peuvent donc exploiter des matériels ou logiciels FT pour fournir une forte disponibilité des cœurs de réseau.

Afin de fournir la forte disponibilité, un système MPLS a besoin d'être capable de survivre à diverses fautes avec une interruption minimale du plan des données, y compris les types de fautes suivants :
- défaillance/changement à chaud de la connexion physique entre les LSR,
- défaillance/changement à chaud du mode de commutation dans un LSR,
- défaillance de la pile TCP ou LDP dans un LSR,
- mise à niveau du logiciel dans les piles TCP ou LDP dans un LSR.

Les deux premiers exemples de fautes cités ci-dessus restent confinés au plan des données. De telles fautes peuvent être traitées en fournissant la redondance du plan des données qui est transparente au fonctionnement de LDP dans le plan des données. Les deux derniers types d'exemple de faute exigent une action dans le plan de contrôle pour récupérer de la faute sans interruption du trafic dans le plan des données. C'est possible parce que de nombreuses architectures récentes de routeur séparent le plan de contrôle de celui des données de sorte que la transmission puisse continuer sans être affectée par l'action de récupération dans le plan de contrôle.

3.2 Problèmes de LDP

LDP utilise TCP pour fournir des connexions fiables entre les LSR sur lesquels ils échangent des messages du protocole pour distribuer les étiquettes et établir les LSP. Une paire de LSR qui ont une telle connexion est appelée des homologues LDP.

TCP permet à LDP de supporter un transfert fiable des messages du protocole. Cela signifie que certains des messages n'ont pas besoin de recevoir des accusés de réception (par exemple, les libérations d'étiquettes).

LDP est défini de telle sorte que si la connexion TCP échoue, le LSR devrait immédiatement supprimer les LSP associés à la session entre les homologues LDP, et libérer toutes les étiquettes et ressources allouées à ces LSP.

Il est bien connu qu'il est difficile de fournir une mise en œuvre de TCP tolérante aux fautes. Le faire peut impliquer de faire des copies de toutes les données envoyées et reçues. C'est un problème qui est familier aux mises en œuvre des autres applications de TCP telles que BGP.

Durant les reprises sur défaillance qui affectent les piles TCP ou LDP, la connexion TCP peut être perdue. La récupération à partir de cette position est rendue pire par le fait que les messages de contrôle LDP peuvent avoir été perdus durant la défaillance de la connexion. Comme ces messages restent non confirmés, il est possible que le LSP ou les informations d'état soient perdus.

Le présent document décrit une solution qui implique :
- la négociation entre les homologues LDP de l'intention de prendre en charge les extensions à LDP qui facilitent la récupération des défaillances sans perte des LSP,
- la sélection de la survie de FT sur la base du LSP/étiquette,
- l'accusé de réception des messages LDP pour s'assurer qu'une prise de contact complète est effectuée sur ces messages fréquemment (comme message par message) ou moins fréquemment comme en vérification-pointage,
- la sollicitation d'accusés de réception à jour (vérification-pointage) des messages LDP précédents pour s'assurer que l'état actuel est purgé sur le disque/NVRAM, avec une option supplémentaire qui permet à un partenaire LDP de demander que l'état soit purgé dans les deux directions si la fermeture en douceur est demandée,
- de produire à nouveau les messages perdus après une reprise sur défaillance afin de s'assurer que l'état de LSP/étiquette est correctement récupéré après la reconnexion de la session LDP.

Les problèmes et les objectifs décrits ci-dessus sont également applicables au CR-LDP.

Les autres objectifs de ce document sont :
- d'offrir la rétro-compatibilité avec les LSR qui ne mettent pas en œuvre ces extensions à LDP,
- de préserver les règles de protocole existantes décrites dans la [RFC3036] pour le traitement des messages dupliqués inattendus et pour le traitement des messages inattendus qui se réfèrent à des LSP/étiquettes inconnus,
- d'éviter des solutions de rafraîchissement d'état plein (telles que celles qui sont présentes dans RSVP : voir les [RFC2205], [RFC2961], [RFC3209] et [RFC3478]) qu'elles soient continues, ou limitées à la récupération post reprise.

Noter que le présent document se concentre sur la préservation de l'état de l'étiquette pour les étiquettes échangées entre une paire de LSR adjacents lorsque la connexion TCP entre ces LSR est perdue. C'est une exigence pour le fonctionnement tolérant aux fautes des LSP, mais une pleine mise en œuvre de la protection de bout en bout pour les LSP exige que cela soit combiné avec d'autres techniques qui sortent du domaine d'application du présent document.

En particulier, ce document n'essaye pas de décrire comment modifier l'acheminement d'un LSP ou les ressources allouées à une étiquette ou à un LSP, qui est couvert par la [RFC3214]. Le présent document ne traite pas non plus de la façon de fournir une commutation automatique de protection de couche 2 ou 3 pour une étiquette ou un LSP, qui fait l'objet d'études distinctes.

La présente spécification n'empêche pas une mise en œuvre de tenter (ni n'exige d'elle qu'elle tente) d'utiliser le comportement FT décrit ici pour récupérer d'une défaillance préemptive d'une connexion sur un système non FT due à, par exemple, une défaillance partielle de système. Noter cependant qu'il y a des problèmes potentiels – qui sont trop nombreux pour qu'on en fasse la liste ici – dont la probabilité que la même défaillance se reproduise immédiatement lors du traitement des données restaurées n'est pas le moindre.

4. Vue d'ensemble des améliorations à LDP FT

Les améliorations à LDP FT consistent en les principaux éléments suivants, qui sont décrits plus en détails dans les sections qui suivent.
- La présence d'un TLV Session FT sur le message LDP Initialisation indique qu'un LSR accepte certaine forme de protection ou récupération en cas de défaillance de la session. Un bit fanion au sein de ce TLV (le bit S) indique que le LSR accepte les améliorations LDP FT sur cette session. Un autre fanion (le bit C) indique que les procédures de vérification-pointage sont à utiliser.
- Un fanion Reconnexion FT dans le TLV Session FT (le bit R) indique si un LSR a préservé l'état d'étiquette FT à travers une défaillance de la connexion TCP.
- Une Temporisation de reconnexion FT, échangée dans le message Initialisation LDP, qui indique la durée maximale pendant laquelle les LSR homologues vont préserver l'état d'étiquette FT après la défaillance d'une connexion TCP.
- Un TLV Protection FT utilisé pour identifier les opérations qui affectent les étiquettes LDP. Tous les messages LDP qui portent le TLV Protection FT ont besoin d'être sécurisés (par exemple, NVRAM) et d'accuser réception des envois des homologues LDP afin que l'état puisse être correctement récupéré pour les numéros de séquence des étiquettes FT après la reconnexion de session LDP.

Noter que la mise en œuvre au sein d'un système FT est laissée ouverte par ce document. Une mise en œuvre pourrait

choisir de sécuriser des messages entiers qui se rapportent aux étiquettes FT à numéro de séquence, ou elle pourrait ne sécuriser que les informations d'état pertinentes.

- Une annonce d'adresse peut aussi être sécurisée par l'utilisation du TLV Protection FT. Cela active la récupération après la reconnexion de la session LDP sans qu'il soit besoin de réannoncer ce qui peut être un très grand nombre d'adresses.

- Le TLV Protection FT peut aussi être utilisé sur le message Garder-en-vie pour purger les accusés de réception de toutes les opérations FT antérieures. Cela active une vérification-pointage pour une récupération future, soit à mi-session soit avant une fermeture en douceur d'une session LDP. Cette procédure peut aussi être utilisée pour vérifier-pointer toutes les opérations (c'est-à-dire aussi bien FT que non FT) pour une récupération future.

4.1 Établissement d'une session LDP FT

Pour que les extensions à LDP [RFC3036] décrites dans le présent document puissent être utilisées avec succès sur une session LDP entre une paire d'homologues LDP, ils DOIVENT négocier que les améliorations FT à LDP sont à utiliser sur la session LDP.

Cela est fait sur l'échange de messages Initialisation LDP en utilisant un nouveau TLV Session FT. La présence de ce TLV indique que l'homologue veut prendre en charge une certaine forme de protection ou un traitement de récupération. Le bit S au sein de ce TLV indique que l'homologue veut prendre en charge les améliorations FT à LDP sur cette session LDP. Le bit C indique que l'homologue veut prendre en charge la fonction de vérification-pointage décrite dans le présent document. Les bits S et C peuvent être établis indépendamment l'un de l'autre.

Les améliorations FT à LDP pertinentes DOIVENT être prises en charge sur une session LDP si les deux homologues LDP incluent un TLV Session FT dans le message Initialisation LDP et ont le même réglage des bits S ou C.

Si l'un ou l'autre des homologues LDP n'inclut pas dans le message Initialisation LDP le TLV Session FT, ou si il n'y a pas correspondance des bits S et C entre les homologues, les améliorations FT à LDP NE DOIVENT PAS être utilisées durant cette session LDP. L'utilisation dans ces cas des améliorations FT à LDP par un homologue LDP envoyeur DOIT être interprétée par l'homologue LDP receveur comme une erreur sérieuse de protocole causant la terminaison de la session.

Un LSR PEUT présenter un comportement FT/non FT différent sur des connexions TCP différentes, même si ces connexions sont des instanciations successives de la session LDP entre les mêmes homologues LDP.

4.1.1 Interopération avec les LSR non FT

Le TLV Session FT sur le message Initialisation LDP porte le bit U. Si un LSR ne prend pas en charge un des mécanismes de protection ou récupération, il ignorera ce TLV. Comme de tels partenaires n'incluent pas non plus le TLV Session FT, aucune session LDP pour de tels LSR n'utilisera les améliorations FT à LDP.

Le reste de ce document suppose que les sessions LDP dont il est question sont entre des LSR qui prennent en charge les améliorations FT à LDP, sauf mention contraire explicite.

4.2 Défaillance de connexion TCP

4.2.1 Détection des défaillance de connexion TCP

Les défaillances de connexion TCP peuvent être détectées et rapportées au composant LDP de diverses façons. Celles-ci devraient être traitées de la même façon par le composant LDP.
- Indication du composant de gestion qu'une connexion TCP ou une ressource sous-jacente n'est plus active.
- Notification par un composant de gestion de matériel de la défaillance d'une interface.
- Fin de temporisation de garde en vie de prises.
- Défaillance envoyée par les prises.
- Nouvelle prise (entrante) ouverte.
- Fin de temporisation de protocole LDP.

4.2.2 Traitement LDP sur défaillance de connexion

Si les améliorations FT à LDP ne sont pas utilisées sur une session LDP, l'action des homologues LDP en cas de défaillance de la connexion TCP est celle spécifiée dans la [RFC3036].

Toutes les informations d'état et ressources associées à des étiquettes non FT DOIVENT être libérées en cas de défaillance de la connexion TCP, incluant la déprogrammation de l'étiquette non FT des matériels de commutation. Ceci est équivalent au comportement spécifié dans la [RFC3036].

Si les améliorations FT à LDP sont utilisées dans une session LDP, les deux homologues LDP DEVRAIENT préserver les informations d'état et les ressources associées aux étiquettes FT échangées dans la session LDP. Les deux homologues LDP DEVRAIENT utiliser un temporisateur pour libérer les informations d'état et ressources préservées associées aux étiquettes FT si la connexion TCP n'est pas restaurée dans un laps de temps raisonnable. Le comportement à l'expiration de ce temporisateur est équivalent au comportement sur défaillance de session LDP décrit dans la [RFC3036].

La temporisation de reconnexion FT que chaque LDP entend appliquer à la session LDP est portée dans le TLV Session FT sur les messages Initialisation LDP. Les deux homologues LDP DOIVENT utiliser la valeur qui correspond au plus faible intervalle de temporisation des deux valeurs de temporisation proposées à partir de l'échange Initialisation LDP, où une valeur de zéro est traitée comme un infini positif.

4.3 Transmission des données durant une défaillance de connexion TCP

Un LSR qui met en œuvre les améliorations FT à LDP DEVRAIT préserver la programmation du matériel de commutation à travers une reprise sur défaillance. Cela assure que la transmission des données n'est pas affectée par l'état de la connexion TCP entre les LSR.

La possibilité de perte de certains paquets de données fait partie intégrante du processus FT de reprise sur défaillance dans certaines configurations de matériels. Si la perte de données n'est pas acceptable pour l'application qui utilise le réseau MPLS, les améliorations FT à LDP décrites dans le présent document NE DEVRAIENT PAS être utilisées.

4.4 Reconnexion de session LDP FT

Lorsque une nouvelle connexion TCP est établie, les homologues LDP DOIVENT échanger des messages Initialisation LDP. Lorsque une nouvelle connexion TCP est établie après une défaillance, les homologues LDP DOIVENT rééchanger des messages Initialisation LDP.

Si un homologue LDP inclut le TLV Session FT avec le bit S établi dans le message Initialisation LDP pour la nouvelle instance de session LDP, il DOIT aussi établir le fanion Reconnecter FT selon qu'il a été capable de préserver l'état d'étiquette. Le fanion Reconnecter FT est porté dans le TLV Session FT.

Si un homologue LDP a préservé toutes les informations d'état pour une instance précédente de la session LDP, il DEVRAIT alors régler le fanion Reconnecter FT à 1 dans le TLV Session FT. Autrement, il DOIT régler le fanion Reconnecter FT à 0.

Si l'un des homologues LDP règle le fanion Reconnecter FT à 0, ou omet le TLV Session FT, les deux homologues LDP DOIVENT libérer toutes les informations d'état et ressources associées à l'instance précédente de la session LDP entre les mêmes homologues LDP, y compris l'état d'étiquette FT et les adresses. Cela assure que les ressources du réseau ne sont pas perdues de façon permanente par un LSR si son homologue LDP est forcé de subir un démarrage à froid.

Si un homologue LDP change un paramètre de la session (par exemple, les limites de l'espace d'étiquettes) par rapport à l'instance précédente, la nature de toute étiquette préservée peut avoir changé. En particulier, les étiquettes allouées précédemment peuvent être maintenant hors gamme. Pour cette raison, la reconnexion de session DOIT utiliser les mêmes paramètres que ceux qui étaient utilisés dans la session avant la défaillance. Si un homologue LDP remarque que les paramètres ont été changés par l'autre homologue, il DEVRAIT envoyer un message Notification avec le code d'état 'Paramètres de session FT changés'.

Si les deux homologues LDP règlent le fanion Reconnecter FT à 1, les deux homologues LDP DOIVENT utiliser les procédures indiquées dans ce document pour achever toutes les opérations d'étiquette sur les étiquettes FT à numéro de séquence qui ont été interrompues par la défaillance de la session LDP.

Si un homologue LDP reçoit un message Initialisation LDP avec le fanion Reconnecter FT établi avant qu'il envoie son

propre message Initialisation, mais si il n'a conservé aucune information sur la précédente version de la session, il DOIT répondre par un message Initialisation avec le fanion Reconnecter FT à zéro. Si un homologue LDP reçoit un message Initialisation LDP avec le fanion Reconnecter FT établi en réponse à un message Initialisation qu'il a envoyé avec le fanion Reconnecter FT à zéro, il DOIT agir comme si aucun état n'avait été conservé par l'un et l'autre homologue sur la session.

4.5 Fonctionnement sur les étiquettes FT

Les opérations d'étiquette sur les étiquettes FT à numéro de séquence sont rendues tolérantes aux fautes en fournissant un accusé de réception de tous les messages LDP qui affectent les étiquettes FT à numéro de séquence. Les accusés de réception sont réalisés au moyen de numéros de séquence sur ces messages LDP.

Les échanges de messages utilisés pour réaliser l'accusé de réception des opérations d'étiquettes et les procédures utilisées pour achever les opérations d'étiquettes interrompues sont détaillées à la section 5, "Fonctionnement FT".

En utilisant ces accusés de réception et procédures, il n'est pas nécessaire que les homologues LDP effectuent une resynchronisation complète de l'état pour toutes les étiquettes FT à numéro de séquence, sur reconnexion de la session LDP entre les homologues LDP ou sur une programmation préalable.

4.6 Vérification-pointage

La vérification-pointage est un dispositif utile qui permet aux nœuds de réduire la quantité de traitement dont ils ont besoin pour accuser réception des messages LDP. Le bit C dans le TLV Session FT est utilisé pour indiquer que la vérification-pointage est prise en charge.

Dans le fonctionnement normal des étiquettes FT à numéro de séquence, les accusés de réception peuvent être différés durant le traitement normal et envoyé seulement de façon périodique. La vérification-pointage peut être utilisée pour purger les accusés de réception provenant d'un homologue en incluant un numéro de séquence sur un message Garder-en-vie demandant l'accusé de réception de ce message et de tous les messages précédents. Dans ce cas, toutes les étiquettes FT à numéro de séquence sont des étiquettes FT vérifiables-pointables.

Si le bit S n'a pas fait l'objet d'un accord, la vérification-pointage peut quand même être utilisée. Dans ce cas, il est utilisé pour accuser réception de tous les messages échangés entre les homologues, et toutes les étiquettes sont des étiquettes FT vérifiables-pointables.

Cela offre une approche dans laquelle il n'est pas nécessaire d'envoyer des accusés de réception à chaque message ou même fréquemment, mais où ils sont seulement envoyés comme vérification-pointage en réponse aux demandes portées dans les messages Garder-en-vie. Une telle approche peut être considérée comme optimale dans les systèmes qui ne présentent pas un très haut degré de changement au fil du temps (comme des LDP de session ciblés) et qui sont prêts à risquer une perte d'état pour les plus récents échanges LDP. Les systèmes plus dynamiques (comme les sessions de découverte LDP) vont plus probablement vouloir accuser plus récemment réception des changements d'état afin que la quantité maximum d'état puisse être préservée lors d'une défaillance.

Noter qu'une importante considération de ce document est que les nœuds qui accusent réception des messages un à un, les nœuds qui diffèrent les accusés de réception, et les nœuds qui s'appuient sur la vérification-pointage, devraient tous interopérer sans interruption, et sans négociation de protocole en dehors de l'initialisation de session.

Un exposé plus détaillé de ce dispositif est fourni à la section 5, "Fonctionnement FT".

4.6.1 Terminaison en douceur

Un dispositif qui s'appuie sur la vérification-pointage est la terminaison en douceur.

Dans certains cas, comme une reprise contrôlée sur défaillance ou une mise à niveau de logiciel, il est possible à un nœud de savoir à l'avance qu'il va terminer sa session avec un homologue.

Dans ces cas, le nœud qui a l'intention de mettre fin à la session peut purger les accusés de réception en utilisant une demande de vérification-pointage comme décrit ci-dessus. L'envoyeur NE DEVRAIT PLUS envoyer d'autres étiquettes ou de messages en rapport avec l'adresse après avoir demandé la vérification-pointage de fermeture afin de préserver l'intégrité de son état sauvegardé.

Ceci ne vaut, cependant, que pour les accusés de réception dans une direction, et le nœud qui va terminer exige aussi la vérification qu'il a sécurisé tous les états envoyés par son homologue. Ceci est réalisé par une prise de contact en trois phases de la vérification-pointage qui est demandée par un TLV supplémentaire (le TLV Bouchon *(Cork)*) dans le message Garder-en-vie.

Un exposé plus détaillé de ce dispositif figure à la section 5, "Fonctionnement FT".

4.7 Épuisement et réapprovisionnement de l'espace d'étiquettes

Lorsque un homologue LDP est incapable de satisfaire un message Demande d'étiquette parce qu'il n'a plus d'étiquette disponible, il envoie un message Notification qui porte le code d'état 'Pas de ressource d'étiquette'. Cela prévient l'homologue LDP demandeur que les messages Demande d'étiquette suivants vont probablement échouer pour la même raison. Ce message n'a pas besoin d'être acquitté pour les besoins de FT car les messages Demande d'étiquette envoyés après une récupération de session vont recevoir la même réponse. Cependant, l'homologue LDP qui reçoit une notification 'Pas de ressource d'étiquette' cesse d'envoyer des messages Demande d'étiquette jusqu'à ce qu'il reçoive un message de notification 'Ressources d'étiquettes disponibles'. Comme cette notification non sollicitée peut être perdue lors d'une défaillance de session, elle peut être protégée en utilisant les procédures décrites dans ce document.

Une autre approche permet qu'une mise en œuvre puisse toujours supposer que les étiquettes sont disponibles lorsque une session est rétablie. Dans ce cas, il est possible qu'elle puisse éliminer les informations de 'Pas de ressource d'étiquette' de la précédente instance de la session et puisse envoyer au moment du rétablissement de la session un lot de messages LDP qui vont échouer et dont il pourrait savoir qu'ils vont échouer.

Noter que l'envoyeur d'un message de notification 'Ressources d'étiquettes disponibles' peut choisir si il ajoute un numéro de séquence exigeant un accusé de réception. À l'inverse, le receveur du message de notification 'Ressources d'étiquettes disponibles' peut choisir d'accuser réception du message sans réellement sauvegarder aucun état.

C'est un choix de la mise en œuvre rendu possible en rendant facultatifs les paramètres FT sur le message Notification. Les mises en œuvre vont pleinement interopérer si elle prennent des approches opposées, mais des messages LDP supplémentaires peuvent être envoyés inutilement à la récupération de la session.

4.8 LSP tunnelés

Les procédures décrites dans le présent document peuvent être appliquées aux LSP qui sont des tunnels et aux LSP qui sont portés par des tunnels. On rappelle que les LSP tunnelés sont gérés par une seule session LDP qui fonctionne de bout en bout, alors que le tunnel est géré par une session LDP différente pour chaque bond le long du chemin. Néanmoins, une coupure dans une des sessions qui gèrent le tunnel va vraisemblablement correspondre à une coupure de la session qui gère le LSP tunnelé. C'est certainement le cas lorsque les échanges LDP partagent une liaison en échec, mais ce n'est pas nécessairement le cas si les messages LDP ont été acheminés le long d'un chemin qui est différent de celui du tunnel, ou si la défaillance dans le tunnel est causée par une défaillance de logiciel LDP à un LSR de transit.

Afin de préserver le chemin de transmission d'un LSP tunnelé, le chemin de transmission du tunnel lui-même doit être préservé. Cela signifie que le tunnel ne doit pas être éliminé si il y a une défaillance de session le long de son chemin. Pour réaliser cela, les échanges d'étiquettes entre chaque paire d'homologues LDP le long du chemin du tunnel doivent utiliser une des procédures de ce document ou de la [RFC3478].

Il est parfaitement acceptable de mêler les procédures de redémarrage utilisées pour le tunnel et pour le LSP tunnelé. Par exemple, le tunnel pourrait être établi en utilisant juste la vérification-pointage parce que c'est un LSP stable, mais les LSP tunnelés pourraient utiliser les procédures FT complètes afin qu'ils puissent retrouver un état actif.

Enfin, il est permis de porter des LSP tunnelés qui n'ont pas de protection FT dans un LSP qui a la protection FT.

5. Fonctionnement FT

Une fois qu'une session LDP FT a été établie, en utilisant le bit S dans le TLV Session FT sur le message Initialisation de session comme décrit au paragraphe 4.1, "Établissement d'une session LDP FT", les deux homologues LDP DOIVENT appliquer les procédures décrites dans la présente section pour les échanges de message LDP FT.

Si la session LDP a été négociée pour ne pas utiliser les améliorations FT à LDP, ces procédures NE DOIVENT PAS être utilisées.

5.1 Messages FT LDP

5.1.1 Messages Étiquettes FT à numéro de séquence

Une étiquette est identifiée comme étant une étiquette FT à numéro de séquence si la demande d'étiquette initiale ou le message Transposition d'étiquette se rapportant à cette étiquette porte le TLV Protection FT.

C'est une option de mise en œuvre valide de marquer toutes les étiquettes comme étiquettes FT à numéro de séquence. Cela peut, bien sûr, être une option préférée des mises en œuvre qui souhaitent utiliser des messages Garder-en-vie qui portent le TLV Protection FT pour réaliser des sauvegardes périodiques de l'état de transmission d'étiquettes complet.

Si une étiquette est une étiquette FT à numéro de séquence, tous les messages LDP qui affectent cette étiquette DOIVENT porter le TLV Protection FT afin que l'état de l'étiquette puisse être récupéré après une défaillance de la session LDP.

Une autre option valide est de n'avoir aucune étiquette comme étiquette FT à numéro de séquence. Dans ce cas, la vérification-pointage utilisant le message Garder-en-vie s'applique à tous les messages échangés sur la session.

5.1.1.1 Portée des étiquettes FT

La portée de l'état FT/non FT d'une étiquette est limitée à l'échange de messages LDP entre une paire d'homologues LDP.

En contrôle ordonné, lorsque le message est transmis vers l'aval ou vers l'amont, le TLV peut être présent ou absent selon les exigences du LSR qui envoie le message.

Si un espace d'étiquettes aux dimensions de la plate-forme est utilisé pour les étiquettes FT, une valeur d'étiquette FT NE DOIT PAS être réutilisée jusqu'à ce que tous les homologues FT LDP auxquels les étiquettes ont été passées aient accusé réception du retrait de l'étiquette FT, soit par un échange explicite RETRAIT D'ÉTIQUETTE/LIBÉRATION D'ÉTIQUETTE, soit implicitement si la session LDP est reconnectée après défaillance mais sans que le fanion Reconnexion FT soit établi. Dans le cas où une session n'est pas rétablie dans le délai de la temporisation de reconnexion, une étiquette PEUT devenir disponible à la réutilisation si elle n'est plus utilisée sur une autre session.

5.1.2 Messages Adresse FT

Si une session LDP utilise les améliorations FT à LDP, les deux homologues LDP DOIVENT sécuriser les messages Adresse et Retrait d'adresse en utilisant les ACK de fonctionnement FT, comme décrit ci-dessous. Cela évite toute ambiguïté sur la question de savoir si une adresse est encore valide après la reconnexion de la session LDP.

Si un LSR détermine qu'un message Adresse envoyé sur une instance précédente d'une session LDP récupérée n'est plus valide, il DOIT explicitement produire un Retrait d'adresse pour cette adresse lorsque la session est reconnectée.

Si le fanion Reconnexion FT n'est pas établi par les deux homologues LDP à la reconnexion d'une session LDP (c'est-à-dire, si l'état n'a pas été préservé) les deux homologues LDP DOIVENT considérer que toutes les adresses ont été retirées. Les homologues LDP DEVRAIENT produire de nouveaux messages Adresse pour toutes leurs adresses valides, comme spécifié dans la [RFC3036].

5.1.3 Notifications de ressources d'étiquettes disponibles

Dans LDP, il est possible qu'un LSR aval n'ait pas d'étiquette disponible pour répondre à une demande d'étiquette. Dans ce cas, comme spécifié dans la RFC3036, le LSR aval doit répondre par un message Notification – Pas de ressources d'étiquette. Le LSR amont cesse alors de réclamer de nouvelles étiquettes jusqu'à ce qu'il reçoive un message Notification - Ressources d'étiquettes disponibles du LSR aval.

Lorsque les extensions FT sont utilisées sur une session, les mises en œuvre peuvent choisir de sécuriser ou non l'état de ressource d'étiquette de leur homologue. Ce choix a un impact sur le nombre de messages LDP qui vont être incorrectement acheminés à un homologue aux ressources épuisées au moment du rétablissement de session, mais cela n'a pas d'autre impact sur l'interopérabilité.

Pour une pleine préservation d'état :

- Le LSR aval doit préserver l'état de disponibilité des étiquettes à travers une reprise sur défaillance afin qu'il se

souvienne d'envoyer une Notification - Ressources d'étiquettes disponibles lorsque les ressources deviennent disponibles.
- Le LSR amont doit se rappeler de l'état de disponibilité des étiquettes à travers la reprise afin qu'il puisse optimiser de ne pas envoyer de demande d'étiquette lors de la reprise.
- Le LSR aval doit utiliser les numéros de séquence sur la Notification - Ressources d'étiquettes disponibles afin qu'il puisse vérifier que le LSR A a reçu le message et supprimer son état sécurisé, ou renvoyer le message si le LSR A récupère sans l'avoir reçu.

Cependant, les options suivantes existent aussi :
- Le LSR aval peut choisir de ne pas inclure un numéro de séquence sur une Notification - Ressources d'étiquettes disponibles. Cela signifie qu'au rétablissement de session, il ne sait pas ce que son homologue pense de l'état des ressources, parce que la notification peut avoir été livrée ou non. Une telle mise en œuvre DOIT commencer les sessions récupérées en envoyant une Notification - Ressources d'étiquettes disponibles supplémentaire pour réinitialiser son homologue.
- Le nœud amont peut choisir de ne pas sécuriser les informations sur l'état des ressource de son homologue. Il accuserait réception de la Notification - Ressources d'étiquettes disponibles, mais ne sauvegarderait pas les informations. Une telle mise en œuvre DOIT supposer que l'état des ressources de son homologue a été réinitialisé à Ressources d'étiquettes disponibles lorsque la session a été rétablie.

Si le fanion Reconnexion FT n'est pas établi par les deux homologues LDP à la reconnexion d'une session LDP (c'est-à-dire, si l'état n'a pas été préservé) les deux homologues LDP DOIVENT considérer que l'état de disponibilité des étiquettes a été réinitialisé comme si la session avait été établie pour la première fois.

5.2 Accusés de réception du fonctionnement FT

La prise de contact des messages FT LDP est achevée par l'utilisation d'accusés de réception *(ACK)*. La corrélation entre le message original et le ACK se fait au moyen du numéro de séquence FT contenu dans le TLV Protection FT, et il est repassé dans le TLV ACK FT. Le TLV ACK FT peut être porté dans tout message LDP envoyé sur la connexion TCP entre les homologues LDP.

Un homologue LDP tient un numéro de séquence FT séparé pour chaque session LDP à laquelle il participe. Le numéro de séquence FT est incrémenté de un pour chaque message FT LDP (c'est-à-dire, qui contient le TLV Protection FT) produit par ce LSR sur la session FT LDP avec laquelle est associé le numéro de séquence FT.

Lorsque un homologue LDP reçoit un message qui contient le TLV Protection FT, il DOIT prendre des mesures pour sécuriser ce message (ou les informations d'état qui découlent du traitement du message). Une fois que le message est sécurisé, il DOIT être acquitté *(recevoir un ACK)*. Cependant, il n'est pas exigé du LSR qu'il envoie cet ACK immédiatement.

Les ACK peuvent être accumulés pour réduire le flux de messages entre les homologues LDP. Par exemple, si un LSR a reçu des messages FT LDP avec les numéros de séquence 1, 2, 3, 4, il pourrait envoyer un seul ACK avec le numéro de séquence 4 pour en accuser réception, sécurisant tous ces messages. Il n'y a aucune raison dans le protocole qui empêcherait le nombre d'accusés de réception accumulés, ou le délai pendant lequel un ACK est différé, de devenir relativement grand.

Les ACK NE DOIVENT PAS être envoyés hors séquence, car ceci est incompatible avec l'usage des ACK accumulés. Les ACK dupliqués (c'est à dire deux messages successifs qui accusent réception du même numéro de séquence) sont acceptables.

Si un homologue LDP découvre que son espace de numéro de séquence pour une session spécifique est plein de numéros de séquence non acquittés (parce que son partenaire de session n'en a pas accusé réception à temps) il ne peut pas allouer un nouveau numéro de séquence pour un autre message FT LPD. Il DEVRAIT envoyer un message Notification avec le code d'état 'Numéros de séquence FT épuisés'.

5.3 Préservation de l'état FT

Si les améliorations FT à LDP sont utilisées dans une session LDP, chaque homologue LDP NE DEVRAIT PAS libérer les informations d'état et les ressources associées aux étiquettes FT échangées dans cette session LDP lors de la défaillance de la connexion TCP. Ceci est contraire à la [RFC3036], mais permet aux opérations sur les étiquettes FT d'être menées à bien après la reconnexion de la connexion TCP.

Les deux homologues LDP d'une session LDP qui utilisent les améliorations FT à LDP DEVRAIENT préserver l'état des informations et ressources qu'ils détiennent pour cette session LDP comme décrit ci-dessous.

- Un homologue LDP amont DEVRAIT libérer les ressources (en particulier de bande passante) associées à l'étiquette FT à numéro de séquence lorsque il initie un message Libération d'étiquette ou Interruption d'étiquette pour l'étiquette. L'homologue LDP amont DOIT préserver les informations d'état pour l'étiquette FT à numéro de séquence, même si il libère les ressources associées à l'étiquette, car il peut avoir besoin de refaire l'opération d'étiquette si la connexion TCP est interrompue.

- Un homologue LDP amont DOIT libérer les informations d'état et les ressources associées à une étiquette FT à numéro de séquence lorsque il reçoit un accusé de réception à un message Libération d'étiquette ou Interruption d'étiquette qu'il a envoyé pour l'étiquette, ou lorsque il envoie un message Libération d'étiquette en réponse à un message Retrait d'étiquette reçu de l'homologue LDP aval.

- Un homologue LDP aval NE DEVRAIT PAS libérer les ressources associées à une étiquette FT à numéro de séquence lorsque il envoie un message Retrait d'étiquette pour l'étiquette car il n'a pas encore reçu confirmation que l'homologue LDP amont a cessé d'envoyer des données utilisant l'étiquette. L'homologue LDP aval NE DOIT PAS libérer les informations d'état qu'il détient pour l'étiquette car il peut encore avoir besoin de refaire l'opération d'étiquette si la connexion TCP est interrompue.

- Un homologue LDP aval DOIT libérer les ressources et informations d'état associée à une étiquette FT à numéro de séquence lorsque il reçoit un accusé de réception à un message Retrait d'étiquette pour l'étiquette.

- Lorsque la temporisation de reconnexion FT arrive à expiration, un LSR DEVRAIT libérer toutes les informations d'état et ressources provenant des instances précédentes de la session LDP défaillante (permanente).

- L'un ou l'autre homologue LDP PEUT choisir de libérer les informations d'état sur la base de sa connaissance interne de la perte d'intégrité des informations d'état ou de l'incapacité de mettre en attente (ou en file d'attente) les opérations LDP durant une défaillance TCP (comme décrit au paragraphe 5.4.1, "Fonctionnement LDP durant une défaillance TCP"). C'est-à-dire que l'homologue n'est pas obligé d'attendre toute la durée de la temporisation de reconnexion FT avant de libérer l'état ; la temporisation donne une limite supérieure à la persistance d'état. Cependant, au cas où un homologue libère l'état avant l'expiration de la temporisation de reconnexion, il NE DOIT PAS réutiliser une étiquette qui était utilisée dans la session jusqu'à l'expiration de la temporisation de reconnexion.

- Lorsque un LSR reçoit un TLV État avec le bit E établi dans le code d'état, ce qui cause la fermeture de la connexion TCP, le LSR DOIT libérer toutes les informations d'état et ressources associées à la session. Ce comportement est obligatoire parce qu'il est impossible au LSR de prédire l'état précis et le comportement futur du LSR partenaire qui a établi le bit E sans connaissance de la mise en œuvre de ce LSR partenaire.

  Noter que le code d'état 'Fermeture temporaire' n'a pas le bit E établi, et PEUT être utilisé durant des opérations de maintenance ou de mise à niveau pour indiquer que le LSR a l'intention de préserver l'état à travers une clôture et rétablissement de la session TCP.

- Si un LSR détermine qu'il doit libérer l'état d'une seule étiquette FT durant une défaillance de la connexion TCP sur laquelle cette étiquette a été échangée, il DOIT libérer tous les états pour toutes les étiquettes de la session LDP.

La libération des informations d'état et ressources associées à des étiquettes non FT est décrite dans la [RFC3036].

Noter qu'une Libération d'étiquette et l'accusé de réception à un Retrait d'étiquette peut être reçue par un LSR aval dans n'importe quel ordre. Le LSR aval PEUT libérer ses ressources à réception du premier message et DOIT libérer ses ressources à réception du second message.

5.4 Procédure FT après défaillance TCP

Lorsque un LSR découvre ou est notifié d'une défaillance de connexion TCP, il DEVRAIT lancer un temporisateur de reconnexion FT pour permettre une période de reconnexion de la connexion TCP entre les homologues LDP.

La valeur par défaut RECOMMANDÉE pour ce temporisateur est de 5 secondes. Durant cette période, la défaillance doit être détectée et faire l'objet d'un rapport, un nouveau matériel peut devoir être activé, l'état de logiciel peut devoir être examiné, et une nouvelle session TCP doit être établie.

Une fois que la connexion TCP entre les homologues LDP a échoué, le LSR actif DEVRAIT tenter de rétablir la connexion TCP. Les mécanismes, temporisateurs, et compteurs d'essais pour le rétablissement de la connexion TCP sont au choix de la mise en œuvre. Il est RECOMMANDÉ que toute tentative de rétablissement de la connexion prenne en compte le traitement de reprise sur défaillance nécessaire chez le LSR, la nature du réseau entre les homologues LDP, et la temporisation de reconnexion FT choisie sur la précédente instance de connexion TCP (s'il en est une).

Si la connexion TCP ne peut pas être rétablie dans la période de temporisation de reconnexion FT, le LSR qui détecte cette fin de temporisation DEVRAIT libérer tous les états préservés pour la session LDP défaillante. Si la connexion TCP est ensuite rétablie (par exemple, après un autre échange de Hello pour établir une nouvelle session LDP) le LSR DOIT régler le fanion Reconnexion FT à 0 si il a libéré les informations d'état préservées lors de cet événement de fin de temporisation.

Si la connexion TCP est bien rétablie dans le délai de la temporisation de reconnexion FT, les deux homologues DOIVENT reprendre les opérations LDP qui ont été interrompues par la défaillance de la connexion TCP (c'est-à-dire, qui n'ont pas eu d'accusé de réception par suite de la défaillance). Cette procédure est décrite au paragraphe 5.5, "Procédure FT après reconnexion TCP".

Le temporisateur de garde pour une session FT LDP (voir au paragraphe 2.5.5 de la [RFC3036]) DEVRAIT être ignoré pendant que le temporisateur de reconnexion FT court. Le temporisateur de garde DEVRAIT être relancé lorsque la connexion TCP est rétablie.

5.4.1 Opérations FT LDP durant une défaillance TCP

Lorsque les améliorations FT à LDP sont utilisées pour une session LDP, il est possible à un LSR de déterminer qu'il a besoin d'envoyer un message LDP à un homologue LDP, mais que la connexion TCP pour cet homologue est actuellement morte. Ces opérations d'étiquettes affectent l'état des étiquettes FT préservées pour la connexion TCP défaillante, de sorte qu'il est important que les changements d'état soient passés à l'homologue LDP lorsque la connexion TCP est restaurée.

Si un LSR détermine qu'il a besoin de produire une nouvelle opération FT LDP à un homologue LDP avec lequel la connexion TCP est actuellement défaillante, il DOIT mettre l'opération en attente (par exemple, sur une file d'attente) et achever cette opération avec l'homologue LDP lorsque la connexion TCP est restaurée, sauf si l'opération d'étiquette est outrepassée par une opération supplémentaire suivante durant la défaillance de connexion TCP (voir au paragraphe 5.5, "Procédure FT après reconnexion TCP").

Si, durant la défaillance de TCP, un LSR détermine qu'il ne peut pas attendre une opération qui ne peut simplement échouer (par exemple, une opération de retrait, de libération, ou d'interruption d'étiquette) il NE DOIT PAS tenter de rétablir la précédente session LDP. Le LSR DOIT se comporter comme si le temporisateur de reconnexion était arrivé à expiration et libérer toutes les informations d'état qui concernent l'homologue LDP. Un LSR peut être incapable (ou ne pas vouloir) attendre des opérations ; par exemple, si une transition majeure d'acheminement se produit pendant que TCP était inopérant entre les homologues LDP, il pourrait en résulter un nombre excessivement grand d'opérations FT LDP. Un LSR qui libère les états avant l'expiration de la temporisation de reconnexion NE DOIT PAS réutiliser les étiquettes qui étaient utilisées sur la session jusqu'à l'expiration de la temporisation de reconnexion.

Dans le fonctionnement ordonné, les opérations FT LDP reçues qui ne peuvent pas être correctement transmises à cause d'une défaillance de connexion TCP PEUVENT être traitées immédiatement (pourvu qu'un état suffisant soit conservé pour transmettre l'opération d'étiquette) ou mises en attente de traitement lorsque la connexion TCP en cours est restaurée et que l'opération peut être correctement transmise vers l'amont ou vers l'aval. Les opérations sur les étiquettes FT NE DEVRAIENT PAS échouer durant une défaillance de session TCP.

Il est RECOMMANDÉ que les opérations de demande d'étiquette pour de nouvelles étiquettes FT ne soient pas mises en attente pendant le rétablissement de la connexion TCP qui attend d'être récupérés au moment où le LSR détermine qu'il a besoin d'envoyer le message Demande d'étiquette. De telles opérations de demande d'étiquette DEVRAIENT plutôt être mises en échec et, si nécessaire, un message Notification contenant le code d'état 'Pas de session LDP' devrait être envoyé en amont.

Les demandes d'étiquette pour de nouvelles étiquettes non FT DOIVENT être rejetées durant une défaillance de connexion TCP, comme spécifié dans la [RFC3036].

5.5 Procédure FT après reconnexion TCP

La prise de contact d'opération FT décrite ci-dessus signifie que tous les changements d'état pour les étiquettes FT à

numéro de séquence et les messages Adresse sont confirmés ou reproductibles à chaque LSR.

Si la connexion TCP entre homologues LDP échoue mais est reconnectée dans le délai de la temporisation de reconnexion FT, et si les deux LSR ont indiqué qu'ils veulent rétablir la précédente session LDP, les deux homologues LDP sur la connexion DOIVENT achever toutes les opérations d'étiquette pour les étiquettes FT à numéro de séquence qui ont été interrompues par la défaillance et la reconnexion de la connexion TCP.

Les procédures pour la temporisation de reconnexion FT PEUVENT avoir été invoquées en résultat de ce que l'un ou l'autre des homologues LDP se trouve incapable (ou ne veut pas) d'attendre des opérations qui se sont produites pendant la défaillance TCP (comme décrit au paragraphe 5.4.1, "Opérations LDP durant une défaillance TCP").

Si, pour une raison quelconque, un LSR a été incapable d'attendre des opérations par rapport à un homologue LDP, comme décrit au paragraphe 5.4.1, "Opérations LDP durant une défaillance TCP", le LSR DOIT régler le fanion Reconnexion FT à 0 à la reconnexion de cet homologue LDP pour indiquer qu'aucun état FT n'a été préservé.

Les opérations d'étiquettes sont achevées en utilisant la procédure suivante.

5.5.1 Réémission de messages FT

À la restauration de la connexion TCP entre homologues LDP, tous les messages LDP pour les étiquettes FT à numéro de séquence qui ont été perdus à cause de la défaillance de la connexion TCP sont réémis. L'homologue LDP qui reçoit un message réémis traite le message comme si il le recevait pour la première fois.

Les combinaisons de messages "zéro net" n'ont pas besoin d'être réémises après le rétablissement de la connexion TCP entre homologues LDP. Cela conduit aux règles suivantes pour la réémission des messages qui n'ont pas reçu d'accusé de réception de la part de l'homologue LDP sur l'échange Initialisation LDP après la reconnexion de la session TCP.

- Un message Demande d'étiquette DOIT être réémis sauf si un message Interruption d'étiquette devait être réémis pour la même étiquette FT à numéro de séquence.

- Un message Transposition d'étiquette DOIT être réémis sauf si un message Retrait d'étiquette devrait être réémis pour la même étiquette FT à numéro de séquence.

- Tous les autres messages de la session LDP qui ont été envoyés et sont portés dans le TLV Protection FT DOIVENT être réémis si un accusé de réception n'a pas été reçu précédemment.

Toutes les opérations d'étiquette FT qui ont été mise en attente (voir au paragraphe 5.4.1, "Opérations LDP durant une défaillance TCP") durant la défaillance de la connexion TCP DOIVENT aussi être réémises au rétablissement de la session LDP, excepté lorsque elles font partie d'une combinaison de messages "zéro net" selon les règles ci-dessus.

La détermination des opérations d'étiquette FT "zéro net" selon les règles ci-dessus PEUT être effectuée sur des messages mis en attente avant le rétablissement de la connexion TCP afin d'optimiser l'usage des ressources de file d'attente. Les messages qui ont été envoyés à l'homologue LDP avant la défaillance de la connexion TCP, ou les messages en attente qui étaient appariés avec eux, NE DOIVENT PAS être soumis à une telle optimisation jusqu'à ce qu'un TLV ACK FT soit reçu de l'homologue LDP. Cet ACK permet au LSR d'identifier quels messages ont été reçus par l'homologue LDP avant la défaillance de la connexion TCP.

6. Procédures de vérification-pointage

La vérification-pointage peut être choisie indépendamment des procédures FT décrites ci-dessus en utilisant le bit C dans le TLV Session FT sur le message Initialisation de session. Noter, cependant, que la vérification-pointage fait partie intégrante des procédures FT. L'établissement des bits S et C bit va réaliser la même fonction que le seul établissement du bit S.

Si le bit C est établi, mais si le bit S ne l'est pas, aucune étiquette n'est une étiquette FT à numéro de séquence. Toutes les étiquettes sont alors des étiquettes FT vérifiables-pointables. La vérification-pointage est utilisée pour synchroniser tous les échanges d'étiquette. Aucun message, à part la demande et l'accusé de réception de vérification-pointage, ne porte un numéro de séquence actif. (Noter que le message Initialisation de session peut porter un numéro de séquence pour confirmer que la vérification-pointage est toujours en place).

C'est une affaire de mise en œuvre de décider de l'ordre des messages reçus et des demandes de vérification-pointage pour

s'assurer que les accusés de réception de vérification-pointage sont sécurisés.

Si les bits S et C sont tous deux établis, ou si seul le bit S est établi, la vérification-pointage ne s'applique qu'aux étiquettes FT à numéro de séquence et aux messages Adresse.

L'ensemble de tous les messages vérifiés-pointés de cette façon est appelé messages vérifiables-pointables.

6.1 Vérification-pointage avec le message Garder-en-vie

Si un LSR reçoit un TLV Protection FT sur un message Garder-en-vie, c'est une demande de purger les accusés de réception pour tous les messages vérifiables-pointables reçus précédemment sur la session.

Aussitôt que le LSR a terminé de sécuriser les messages vérifiables-pointables (ou les changements d'état qui en sont la conséquence) reçus avant le Garder-en-vie, il DOIT envoyer un accusé de réception au numéro de séquence du message Garder-en-vie.

Dans le cas où les procédures FT sont utilisées et où les accusés de réception ont été mémorisés, cela peut survenir immédiatement à la réception du Garder-en-vie.

Un exemple de flux de message qui montre cette utilisation du message Garder-en-vie pour effectuer une vérification-pointage périodique de l'état est donné au paragraphe 9.2, "Utilisation de la vérification-pointage avec les procédures FT".

Un exemple de flux de message montrant l'utilisation de la vérification-pointage sans les procédures FT est donné au paragraphe 9.5, "Vérification-pointage sans les procédures FT".

6.2 Repos *(Quiesce)* et Garder-en-vie *(Keepalive)*

Si le message Garder-en-vie contient aussi le TLV Bouchon FT, cela indique que l'homologue LSR souhaite mettre la session au repos avant un redémarrage en douceur.

Il est RECOMMANDÉ qu'à réception d'un Garder-en-vie avec le TLV Bouchon FT, un LSR devrait cesser d'envoyer d'autres étiquettes ou messages en rapport avec les adresses sur la session jusqu'à ce qu'il ait été déconnecté et reconnecté, autres que les messages générés durant le traitement et la sécurisation des messages qui n'ont pas eu d'accusé de réception précédemment reçus de l'homologue qui demande le repos. Il devrait aussi tenter d'achever ce traitement et retourner un Garder-en-vie avec le TLV ACK FT aussitôt que possible afin de permettre de placer la session en repos.

Un exemple de message qui montre cette utilisation du TLV Bouchon FT pour réaliser une prise de contact en trois phases de synchronisation d'état entre deux homologues LDP est donné au paragraphe 9.4, "Fermeture temporaire avec procédures FT de vérification-pointage".

7. Changements aux messages existants

7.1 Message d'initialisation LDP

Les améliorations FT à LDP ajoutent les paramètres facultatifs suivants à un message Initialisation LDP :

Paramètre facultatif	Longueur	Valeur
TLV Session FT	4	voir ci-dessous
TLV ACK FT	4	voir ci-dessous

Le codage de ces TLV se trouve à la Section 8, "Nouveaux champs et valeurs".

TLV Session FT
Si présent, il spécifie le comportement FT de la session LDP.

TLV ACK FT
Si présent, il spécifie le dernier message FT que l'homologue LDP qui envoie a été capable de sécuriser avant la défaillance de l'instance précédente de la session LDP. Ce TLV n'est présent que si le fanion Reconnexion FT est établi dans le TLV

Session FT, auquel cas, ce TLV DOIT être présent.

7.2 Messages LDP Garder-en-vie

Les améliorations FT à LDP ajoutent les paramètres facultatifs suivants à un message LDP Garder-en-vie :

Paramètre facultatif	Longueur	Valeur
TLV Protection FT	4	voir ci-dessous
TLV Bouchon FT	0	voir ci-dessous
TLV ACK FT	4	voir ci-dessous

Le codage de ces TLV se trouve à la Section 8, "Nouveaux champs et valeurs".

TLV Protection FT
Si présent, il spécifie le numéro de séquence FT pour les messages LDP. Lorsque présent sur un message Garder-en-vie, cela indique une purge sollicitée des accusés de réception à tous les messages LDP précédents qui contenaient des numéros de séquence et produits par l'envoyeur du Garder-en-vie de la même session.

TLV Bouchon FT
Indique que le LSR distant souhaite mettre au repos la session LDP. Voir à la Section 5, "Fonctionnement FT", l'action recommandée dans de tels cas.

TLV ACK FT
Si présent, il spécifie le plus récent message FT que l'homologue LDP envoyeur a été capable de sécuriser.

7.3 Autres messages de session LDP

Les améliorations FT à LDP ajoutent les paramètres facultatifs suivants à tous les autres types de message qui s'écoulent dans une session LDP après le message Initialisation LDP

Paramètre facultatif	Longueur	Valeur
TLV Protection FT	4	voir ci-dessous
TLV ACK FT	4	voir ci-dessous

Le codage de ces TLV se trouve à la Section 8, "Nouveaux champs et valeurs".

TLV Protection FT
Si présent, il spécifie le numéro de séquence FT pour le messages LDP.

FT ACK TLV
Si présent, il identifie les plus récents messages FT LDP dont l'homologue LDP envoyeur a accusé réception.

8. Nouveaux champs et valeurs

8.1 Codes d'état

Les nouveaux codes d'état suivants sont définis pour indiquer diverses conditions spécifiques des améliorations FT à LDP. Ces codes d'état sont portés dans le TLV État d'un message Notification.

La colonne "E" est le réglage exigé du bit E de code d'état ; la colonne "Données d'état" est la valeur du champ de 30 bits Données d'état dans le TLV Code d'état.

Noter que le réglage du bit F du code d'état est à la discrétion du LSR qui génère le TLV État. Cependant, il est RECOMMANDÉ que le bit F ne soit pas établi dans les messages Notification qui contiennent des codes d'état sauf 'Pas de session LDP' parce que la duplication des messages DEVRAIT être restreinte à un comportement par bond.

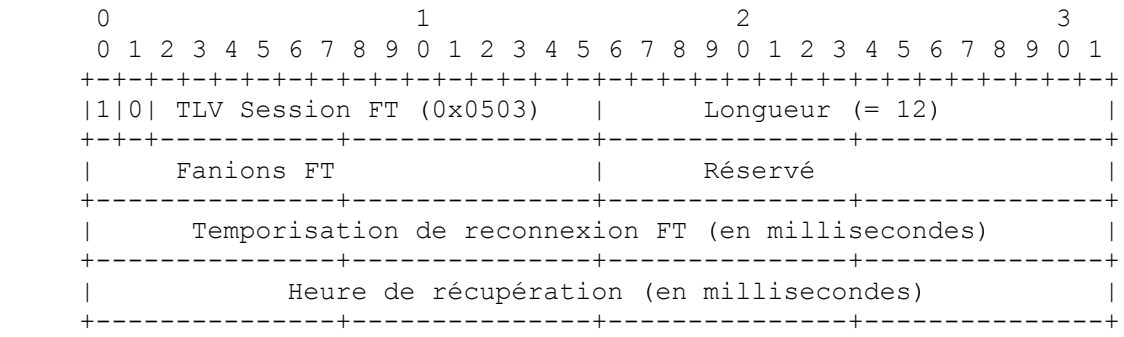
Code d'état	E	Données d'état
Pas de session LDP	0	0x0000001A
Numéro de séquence FT zéro	1	0x0000001B
TLV inattendu/ Session non FT	1	0x0000001C
TLV inattendu / Étiquette non FT	1	0x0000001D
TLV Protection FT manquant	1	0x0000001E
Erreur de séquence d'ACK FT	1	0x0000001F
Fermeture temporaire	0	0x00000020
Numéros de séquence FT épuisés	1	0x00000021
Paramètres de session FT changés	1	0x00000022
TLV Bouchon FT inattendu	1	0x00000023

Le code d'état de 'Fermeture temporaire' DEVRAIT être utilisé à la place du code d'état 'Fermeture' (qui a le bit E établi) si le LSR qui ferme souhaite informer son homologue LDP qu'il s'attend à être capable de préserver l'état des étiquettes FT et reprendre du service avant l'arrivée à expiration du temporisateur de reconnexion FT.

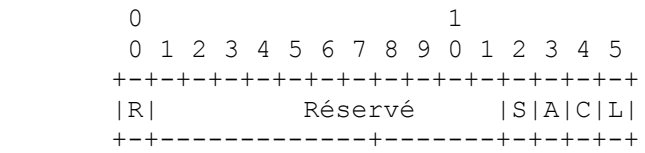
8.2 TLV de session FT

Les homologues LDP peuvent négocier si la session LDP entre eux prend en charge les extensions FT en utilisant un nouveau paramètre FACULTATIF, le TLV Session FT, sur les messages Initialisation LDP.

Le TLV Session FT est codé comme suit.



Fanions FT
C'est un champ de 16 bits qui indique divers attributs que FT accepte sur cette session LDP. Ce champ est formaté comme suit :



R : fanion Reconnexion FT.
Réglé à 1 si le LSR envoyeur a préservé l'état et les ressources pour toutes les étiquettes FT depuis la précédente session LDP entre les mêmes homologues LDP, et est autrement réglé à 0. Voir au paragraphe 5.4, "Procédures FT après défaillance TCP" les détails sur la façon d'utiliser ce fanion.
Si le fanion Reconnexion FT est établi, le LSR envoyeur DOIT inclure un TLV ACK FT dans le message Initialisation LDP.

S : Fanion Sauvegarder l'état.
Réglé à 1 si l'utilisation du TLV Protection FT est acceptée sur les messages autres que Garder-en-vie utilisés pour la vérification-pointage (voir le bit C). C'est-à-dire que le bit S indique qu'une étiquette de la session peut être une étiquette FT à numéro de séquence.

A : Protection de toutes les étiquettes exigée
Réglé à 1 si toutes les étiquettes de la session DOIVENT être traitées comme des étiquette FT à numéro de séquences. Cela retire d'un nœud l'option de traiter certaines étiquettes comme des étiquettes FT et certaines autres comme non FT.
Passer ces informations peut être considéré comme utile pour un homologue car cela peut lui permettre d'optimiser son traitement.

Le bit A n'a de signification que si le bit S est établi.

C : Fanion Vérification-pointage.
Réglé à 1 pour indiquer que les procédures de vérification-pointage de ce document sont utilisées.
Si le bit S est aussi réglé à 1, le bit C indique alors que la vérification-pointage ne s'applique qu'aux étiquettes FT à numéro de séquence.
Si le bit S est réglé à 0 (zéro) le bit C indique alors que la vérification-pointage s'applique à toutes les étiquettes – toutes les étiquettes sont des étiquettes FT vérifiables-pointables.

L : Fanion Appris du réseau.
Réglé à 1 si les procédures de récupération de fautes de la [RFC3478] sont à utiliser pour réapprendre l'état de la part du réseau.
Il n'est pas valide pour tous les bits S, C et L d'être à zéro.
Il n'est pas valide que les bits L et soit S, soit C, soient tous deux établis à 1.

Tous les autres bits de ce champ sont actuellement réservés et DEVRAIENT être réglés à zéro à l'émission et ignorés à réception.

Le tableau suivant résume le réglage de ces bits.

S	**A**	**C**	**L**	**Commentaire**
0	x	0	0	Invalide
0	0	0	1	Voir la [RFC3478]
0	1	0	1	Invalide
0	x	1	0	Vérification-pointage de toutes les étiquettes
0	x	1	1	Invalide
1	0	0	0	FT complet sur les étiquettes choisies
1	1	0	0	FT complet sur les étiquettes choisies
1	x	0	1	Invalide
1	x	1	0	Même chose que (S=1, A=x, C=0, L=0)
1	x	1	1	Invalide

Temporisation de reconnexion FT
Si le bit S ou le bit C est établi dans le champ Fanions FT, cela indique le moment où le LSR envoyeur va préserver l'état et les ressources pour les étiquettes FT échangées sur la précédente instance d'une session FT LDP qui a récemment connu une défaillance. La temporisation est codée comme entier non signé de 32 bits en nombre de millisecondes.

Une valeur de zéro dans ce champ signifie que le LSR envoyeur va préserver l'état et les ressources indéfiniment.

Voir au paragraphe 4.4 les détails de la façon dont ce champ est utilisé.

Si le bit L est réglé à 1 dans le champ Fanions FT, la signification de ce champ est définie dans la [RFC3478].

Heure de récupération
L'heure de récupération n'a de signification que si le bit L est établi dans Fanions FT. Sa signification est définie dans la [RFC3478].

8.3 TLV Protection FT

Les homologues LDP utilisent le TLV Protection FT pour indiquer qu'un message LDP contient une opération d'étiquette FT.

Le TLV Protection FT NE DOIT PAS être utilisé dans les messages qui s'écoulent sur une session LDP qui ne prend pas en charge les améliorations FT à LDP. Sa présence dans de tels messages DEVRA être traitée comme une erreur de protocole par l'homologue LDP receveur qui DEVRAIT envoyer un message Notification avec le code d'état 'TLV Session non FT inattendu'. Les LSR qui ne reconnaissent pas ce TLV DEVRAIENT répondre par un message Notification avec le code d'état 'TLV inconnu'.

Le TLV Protection FT PEUT être porté dans des messages LDP transportés dans la session LDP après l'échange initial de messages Initialisation LDP. En particulier, ce TLV PEUT facultativement être présent dans les messages suivants :
- messages Demande d'étiquette en mode distribution vers l'aval à la demande,

- messages Transposition d'étiquette en mode distribution vers l'aval non sollicitée,
- messages Garder-en-vie utilisés pour demander la purge des accusés de réception de tous les précédents messages qui contenaient ce TLV.

Si une étiquette doit être une étiquette FT à numéro de séquence, le TLV Protection DOIT alors être présent :
- dans le message Demande d'étiquette en mode de distribution vers l'aval à la demande,
- dans le message Transposition d'étiquette en mode distribution vers l'aval non sollicitée,
- dans tous les messages suivants qui concernent cette étiquette.

Ici, 'messages suivants qui concernent cette étiquette' signifie tout message dont le TLV Étiquette spécifie cette étiquette ou dont le TLV Identifiant de message de demande d'étiquette spécifie le message initial de demande d'étiquette.

Si une étiquette n'est pas destinée à être une étiquette FT à numéro de séquence, le TLV Protection NE DOIT alors PAS être présent, dans aucun des messages qui se rapportent à l'étiquette. La présence du TLV FT dans un message qui se rapporte à une étiquette non FT DEVRA être traitée comme erreur de protocole par l'homologue LDP receveur qui DEVRAIT envoyer un message Notification avec le code d'état 'TLV Étiquette non FT inattendu'.

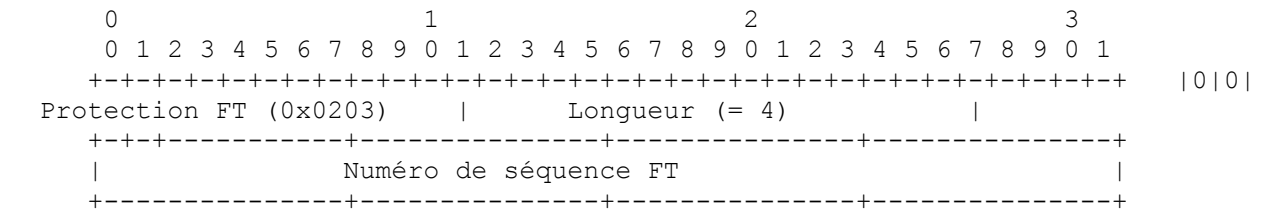
Lorsque un message Retrait d'étiquette ou Libération d'étiquette contient seulement un TLV FEC et n'identifie pas une seule étiquette spécifique, le TLV FT devrait être inclus dans le message si une étiquette affectée par le message est une étiquette FT à numéro de séquence. Si il y a un doute sur la nécessité de la présence d'un TLV FT, il est RECOMMANDÉ que l'envoyeur ajoute le TLV.

Lorsque un homologue LDP reçoit un message Retrait d'étiquette ou Libération d'étiquette qui contient seulement une FEC, il DEVRA accepter le TLV FT si il est présent, sans considération de l'état FT des étiquettes qu'il affecte.

Si une session LDP est une session FT comme déterminé par la présence du TLV Session FT, avec le bit S établi dans les messages Initialisation LDP, le TLV Protection FT DOIT être présent sur tous les messages Adresse de la session.

Si la session est une session FT, le TLV Protection FT peut aussi être facultativement présent :
- dans les messages Notification de la session qui ont le code d'état 'Ressources d'étiquette disponibles',
- dans les messages Garder-en-vie.

Le TLV Protection FT est codé comme suit.



Numéro de séquence FT
C'est le numéro de séquence pour cette opération d'étiquette FT à numéro de séquence. Le numéro de séquence est codé comme entier non signé de 32 bits. La valeur initiale de ce champ pour une nouvelle session LDP est 0x00000001 et est incrémentée de un à chaque message FT LDP produit par le LSR envoyeur sur cette session LDP. Ce champ peut revenir de 0xFFFFFFFF à 0x00000001.

Ce champ DOIT être remis à 0x00000001 si l'un ou l'autre homologue LDP ne règle pas le fanion Reconnexion FT lors du rétablissement de la connexion TCP.

Voir au paragraphe 5.2, "Accusés de réception du fonctionnement FT" les détails de la façon dont ce champ est utilisé.

L'utilisation particulière de 0x00000000 est discutée au paragraphe 8.4, "TLV ACK FT" ci-dessous.

Si un LSR reçoit un TLV Protection FT sur une session qui n'accepte pas les améliorations FT à LDP, il DEVRAIT envoyer un message Notification à son homologue LDP contenant le code d'état 'TLV inattendu, session non FT'. Les LSR qui ne reconnaissent pas ce TLV DEVRAIENT répondre par un message Notification avec le code d'état 'TLV inconnu'.

Si un LSR reçoit un TLV Protection FT sur une opération qui affecte une étiquette dont il pense qu'elle est une étiquette non FT, il DEVRAIT envoyer un message Notification à son homologue LDP contenant le code d'état 'TLV inattendu, étiquette non FT'.

Si un LSR reçoit un message sans le TLV Protection FT qui affecte une étiquette dont il pense qu'elle est une étiquette FT à numéro de séquence, il DEVRAIT envoyer un message Notification à son homologue LDP contenant le code d'état 'TLV Protection FT manquant'.

Si un LSR reçoit un TLV Protection FT contenant un numéro de séquence FT de zéro, il DEVRAIT envoyer un message Notification à son homologue LDP contenant le code d'état 'Numéro de séquence FT de zéro'.

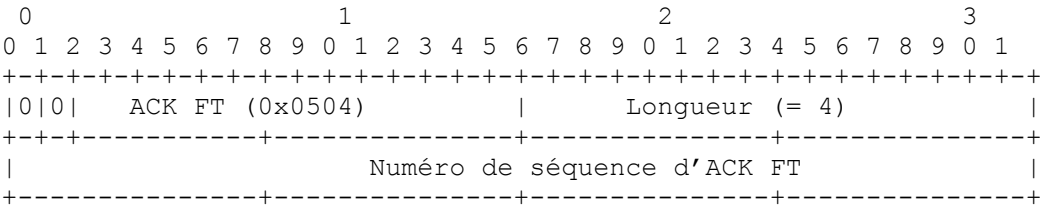
8.4 TLV ACK FT

Les homologues LDP utilisent le TLV ACK FT pour accuser réception des opérations d'étiquette FT.

Le TLV ACK FT NE DOIT PAS être utilisé dans les messages qui s'écoulent dans une session LDP qui ne prend pas en charge les améliorations FT à LDP. Sa présence dans de tels messages DEVRA être traitée comme une erreur de protocole par l'homologue LDP receveur.

Le TLV ACK FT PEUT être présent dans tous messages LDP échangés dans une session LDP après les messages Initialisation LDP initiaux. Il est RECOMMANDÉ que le TLV ACK FT soit inclus dans tous les messages FT Garder-en-vie afin de s'assurer que les homologues LDP n'entassent pas un gros arriéré d'informations d'état non acquitté.

Le TLV ACK FT est codé comme suit .



Numéro de séquence d'ACK FT
Numéro de séquence du plus récent message Étiquette FT que l'homologue LDP envoyeur a reçu de l'homologue LDP receveur et sécurisé contre la défaillance de la session LDP. Il n'est pas nécessaire que l'homologue envoyeur ait complètement traité le message avant d'en accuser réception. Par exemple, un LSR PEUT accuser réception d'un message Demande d'étiquette aussitôt qu'il a sécurisé l'enregistrement du message, sans attendre qu'il puisse envoyer le message Transposition d'étiquette en réponse.

Les ACK sont cumulatifs. La réception d'un message LDP contenant un TLV ACK FT avec un numéro de séquence d'ACK FT de 12 est traité comme accusé de réception de tous les messages de 1 à 12 inclus (en supposant que la session LDP a commencé au numéro de séquence 1).

Ce champ DOIT être réglé à 0 si le LSR qui envoie le TLV ACK FT n'a pas reçu d'opération Étiquette FT sur cette session LDP. Ceci s'applique aux sessions LDP, aux nouveaux homologues LDP ou après qu'un LSR a déterminé qu'il doit abandonner tous les états pour une connexion TCP défaillante.

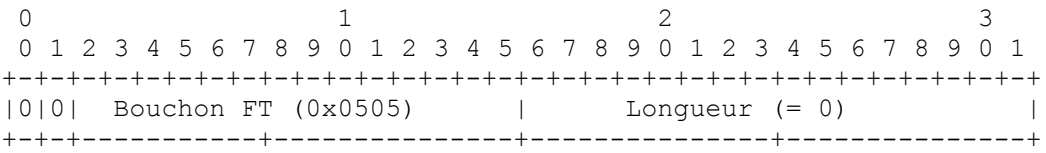
Voir au paragraphe 5.2, "Accusés de réception du fonctionnement FT" les détails de l'utilisation de ce champ.

Si un LSR reçoit un TLV ACK FT qui contient un numéro de séquence d'ACK FT qui est inférieur au numéro de séquence d'ACK FT reçu précédemment (en se souvenant de tenir compte du retour à zéro) il DEVRAIT envoyer un message Notification à son homologue LDP contenant le code d'état 'Erreur de numéro de séquence d'ACK FT'.

8.5 TLV Bouchon FT

Les homologues LDP utilisent le TLV Bouchon FT *(FT Cork)* sur les messages FT Garder-en-vie pour indiquer qu'ils souhaitent mettre au repos la session LDP avant une fermeture contrôlée et redémarrage, par exemple, durant une mise à niveau du logiciel de plan de contrôle.

Le TLV Bouchon FT est codé comme suit :



À réception d'un message Garder-en-vie avec le TLV Bouchon FT et le TLV Protection FT, un LSR DEVRAIT effectuer les actions suivantes :

- Traiter et sécuriser tous les messages provenant du LSR homologue qui ont des numéros de séquence inférieurs (en tenant compte du retour à zéro) à celui contenu dans le TLV Protection FT du message Garder-en-vie.

- Renvoyer à l'homologue un message Garder-en-vie contenant le TLV Bouchon FT et le TLV ACK FT spécifiant le numéro de séquence de l'accusé de réception FT égal à celui du message Garder-en-vie original (c'est-à-dire, accusant réception de tous les messages jusqu'à ce moment).

- Si ce LSR n'a pas encore reçu un ACK FT pour tous les messages qu'il a envoyé contenant le TLV Protection FT, inclure alors aussi un TLV Protection FT dans le message Garder-en-vie envoyé au LSR homologue. Cela indique à l'homologue distant que le LSR local a sauvegardé l'état avant de passer au repos mais qu'il attend toujours la confirmation que l'homologue distant a sauvegardé l'état.

- Cesser d'envoyer d'autres messages de changement d'état sur cette session LDP jusqu'à ce qu'elle ait été déconnectée et récupérée.

À réception d'un message Garder-en-vie avec le TLV Bouchon FT et un TLV ACK FT qui accuse réception des Garder-en-vie envoyés précédemment qui portaient le TLV Bouchon FT, un LSR sait que la mise au repos est achevée. Si le Garder-en-vie reçu porte aussi le TLV Protection FT, le LSR doit répondre par un autre Garder-en-vie pour achever la prise de contact en trois phases. Il DEVRAIT envoyer maintenant un message Notification "Fermeture temporaire", déconnecter la session TCP et effectuer les actions exigées par le plan de contrôle pour la fermeture de cette session.

Un exemple d'une telle prise de contact en trois phases pour une fermeture contrôlée figure au paragraphe 9.4, "Fermeture temporaire avec procédures FT et vérification-pointage".

Si un LSR reçoit un message qui n'a pas pu porter le TLV Bouchon FT, ou si le TLV Bouchon FT est utilisé dans un message Garder-en-vie sans que soit présent le TLV Protection FT ou le TLV ACK FT, il DEVRAIT envoyer un message Notification à son homologue LDP contenant le code d'état 'TLV Bouchon FT inattendu' .

9. Exemples d'utilisation

Considérons deux homologues LDP, P1 et P2, qui mettent en œuvre LDP sur une connexion TCP qui les connecte entre eux, et les flux de messages indiqués ci-dessous.

Les paramètres montrés sur chaque message ci-dessous sont les suivants :

message (étiquette, numéro de séquence d'envoyeur FT, numéro d'accusé de réception FT)

Un "-" pour le numéro d'accusé de réception FT signifie que le TLV ACK FT n'est pas inclus dans ce message.
Un "n/a" signifie que le paramètre en question n'est pas applicable à ce type de message.

Dans les diagrammes ci-dessous, le temps s'écoule du haut en bas. La position relative de chaque message montre quand il est transmis. Voir les notes pour la description du moment où chaque message est reçu, sécurisé pour FT ou traité.

9.1 Défaillance et récupération de session – Procédures FT

notes	**P1**		**P2**
(1)	Demande d'étiquette(L1,27,-)	---------->	
	Demande d'étiquette(L2,28,-)	---------->	
(2)	Demande d'étiquette(L3,93,27)	<----------	
(3)			Demande d'étiquette(L1,123,-) ---------->
			Demande d'étiquette(L2,124,-) ---------->

```
(4)                                  <----------------------  Transposition d'étiquette(L1,57,-)
     <------------  Transposition d'étiquette(L1,94,28)
(5)                                  <--------------------------  Transposition d'étiquette(L2,58,-)
     <------------  Transposition d'étiquette(L2,95,-)
(6)  Adresse(n/a,29,-)                    --------------------------->
(7)  Demande d'étiquette(L4,30,-)         --------------------------->
(8)  Garder-en-vie(n/a,-,94)              --------------------------->
(9)   <------------  Interruption d'étiquette(L3,96,-)
(10)                 ======  Session TCP perdue ======
                          :
(11)                      :              <--------------------------  Retrait d'étiquette(L1,59,-)
                          :
                          :
(12)                 === Session TCP restaurée ===
     Initialisation LDP(n/a,n/a,94)       --------------------------->
     <--------------  Initialisation LDP(n/a,n/a,29)
(13) Demande d'étiquette(L4,30,-)  --------------------------->
(14) <--------------  Transposition d'étiquette(L2,95,-)
     <--------------  Interruption d'étiquette(L3,96,30)
(15) <--------------  Retrait d'étiquette(L1,97,-)
```

Notes :

(1) Suppose que la session LDP a déjà été initialisée. P1 produit deux nouvelles demandes d'étiquette en utilisant les prochains numéros de séquence.

(2) P2 produit une demande d'étiquette à P1. Au moment de l'envoi de cette demande, P2 a sécurisé la réception de la demande d'étiquette pour L1 de P1, de sorte qu'il inclut un ACK pour ce message.

(3) P2 traite les demandes d'étiquette pour L1 et L2 et les transmet vers l'aval. Les détails du traitement en aval ne sont pas montrés sur le diagramme.

(4) P2 reçoit une Transposition d'étiquette de l'aval pour L1, qu'il transmet à P1. Il inclut un ACK à la demande d'étiquette pour L2, car ce message a maintenant été sécurisé et traité.

(5) P2 reçoit la transposition d'étiquette pour L2, qu'il transmet à P1. Cette fois, il n'inclut pas de ACK car il n'a pas reçu d'autre message de P1.

(6) Pendant ce temps, P1 envoie un nouveau message Adresse à P2.

(7) P1 envoie aussi une quatrième Demande d'étiquette à P2.

(8) P1 envoie un message Garder-en-vie à P2, dans lequel il inclut un ACK pour la transposition d'étiquette pour L1, qui est le dernier message que P1 a reçu et sécurisé au moment où le Garder-en-vie est envoyé.

(9) P2 produit une Interruption d'étiquette pour L3.

(10) À ce moment, la session TCP se termine.

(11) Pendant que la session TCP est morte, P2 reçoit un message Retrait d'étiquette pour L1, qu'il met en file d'attente.

(12) La session TCP est reconnectée et P1 et P2 échangent des messages Initialisation LDP sur la session récupérée, qui incluent des ACK pour le dernier message que chaque homologue a reçu et sécurisé avant la défaillance.

(13) À partir de l'échange Initialisation LDP, P1 détermine qu'il doit réémettre la demande d'étiquette pour L4.

(14) De même, P2 détermine qu'il doit réémettre la Transposition d'étiquette pour L2 et l'Interruption d'étiquette.

(15) P2 produit à P1 le Retrait d'étiquette mis en file d'attente.

9.2 Utilisation de la vérification-pointage avec procédures FT

```
notes      P1                                                    P2
(1)   Demande d'étiquette(L1,27,-)  ---------------------------->
      Demande d'étiquette(L2,28,-)  ---------------------------->
(2)   <-----------------  Demande d'étiquette(L3,93,-)
(3)                                                  Demande d'étiquette(L1,123,-)  ---------------------------->
                                                     Demande d'étiquette(L2,124,-)  ---------------------------->
(4)                                <--------------------------  Transposition d'étiquette(L1,57,-)
      <------------------ Transposition d'étiquette(L1,94,-)
(5)                                <--------------------------  Transposition d'étiquette(L2,58,-)
      <------------------ Transposition d'étiquette(L2,95,-)
(6)   Adresse(n/a,29,-)             ---------------------------->
(7)   Demande d'étiquette(L4,30,-)  ---------------------------->
(8)   Garder-en-vie(n/a,31,-)       ---------------------------->
(9)   <---------------------------- Garder-en-vie(n/a,-,31)
(10)                               <--------------------------  Garder-en-vie(n/a,59,124)
(11)                                                 Garder-en-vie(n/a,-,59) ---------------------------->
```

Notes :
Les notes (1) à (7) sont les mêmes que celles de l'exemple précédent excepté la note qu'aucun accusé de réception n'est porté sur les messages de direction inverse. Cela signifie qu'à la note (8) il y a des accusés de réception différés dans les deux directions sur les deux liaisons.

(8) P1 souhaite synchroniser l'état avec P2. Il envoie un message Garder-en-vie contenant un TLV Protection FT avec le numéro de séquence 31. Comme il n'est pas intéressé par la perception de P2 de l'état qu'il a mémorisé, il n'inclut pas de TLV ACK FT.

(9) P2 répond tout de suite par un Garder-en-vie qui accuse réception du numéro de séquence sur le Garder-en-vie reçu. Cela dit à P1 que P2 a préservé tous les états/messages précédemment reçus dans cette session.

(10) Le nœud aval souhaite synchroniser son état avec P2. Il envoie un message Garder-en-vie contenant un TLV Protection FT avec le numéro de séquence 59. P3 saisit aussi cette opportunité pour se mettre à jour de ses accusés de réception avec P2 en incluant un TLV ACK FT qui accuse réception jusqu'au numéro de séquence 124.

(11) P2 répond tout de suite avec un Garder-en-vie qui accuse réception du numéro de séquence sur le Garder-en-vie reçu.

9.3 Fermeture temporaire avec procédures FT

```
notes      P1                                                    P2
(1)   Demande d'étiquette(L1,27,-) ---------------------------->
      Demande d'étiquette(L2,28,-) ---------------------------->
(2)   <------------------ Demande d'étiquette(L3,93,27)
(3)                                                  Demande d'étiquette(L1,123,-) ---------------------------->
                                                     Demande d'étiquette(L2,124,-)  ---------------------------->
(4)                                <--------------------------  Transposition d'étiquette(L1,57,-)
      <------------------ Transposition d'étiquette(L1,94,28)
(5)                                <--------------------------  Transposition d'étiquette(L2,58,-)
      <------------------ Transposition d'étiquette(L2,95,-)
(6)   Adresse(n/a,29,-) ---------------------------->
(7)   Demande d'étiquette(L4,30,-) ---------------------------->
(8)   Garder-en-vie(n/a,-,94)  ---------------------------->
(9)   <-------------------  Interruption d'étiquette(L3,96,-)
(10)  Notification(Fermeture temporaire) ---------------------------->
                  ===== Session TCP fermée =====
                      :
(11)                  :                <--------------------------  Retrait d'étiquette(L1,59,-)
                      :
                      :
                  ===== Session TCP restaurée =====
(12)  Initialisation LDP(n/a,n/a,94) ---------------------------->
      <------------------  Initialisation LDP(n/a,n/a,29)
(13)  Demande d'étiquette(L4,30,-) ---------------------------->
(14)  <------------------Transposition d'étiquette(L2,95,-)
```

```
        <---------------- Interruption d'étiquette(L3,96,30)
(15)    <---------------- Retrait d'étiquette(L1,97,-)
```

Notes :Les notes sont les mêmes que dans l'exemple précédent excepté ce qui suit :

(10) P1 a besoin de mettre à niveau le logiciel ou matériel sur lequel il fonctionne. Il produit un message Notification pour terminer la session LDP, mais règle le code d'état à 'Fermeture temporaire' pour informer P2 que ce n'est pas une erreur fatale, et P2 devrait conserver l'état FT. La connexion TCP peut aussi avoir une défaillance durant la période où la session LDP est morte (auquel cas, elle devra être rétablie) mais il est aussi possible que la connexion TCP soit préservée.

9.4 Fermeture temporaire avec procédures FT et vérification-pointage

```
notes  P1                                                    P2
(1)      Demande d'étiquette(L1,27,-) ------------------------->
         Demande d'étiquette(L2,28,-) ------------------------->
(2)      <---------------- Demande d'étiquette(L3,93,-)
                                                  Demande d'étiquette(L1,123,-) ------------------------->
                                                  Demande d'étiquette(L2,124,-) ------------------------->
                                        <-------------------------- Transposition d'étiquette(L1,57,-)
(3)      <---------------- Transposition d'étiquette(L1,94,-)
                                        <-------------------------- Transposition d'étiquette(L2,58,-)
         <---------------- Transposition d'étiquette(L2,95,-)
(4)      Adresse(n/a,29,-) ------------------------->
(5)      Demande d'étiquette(L4,30,-) ------------------------->
(6)      Garder-en-vie(n/a,31,95) * avec TLV Bouchon FT * ------------------------->
(7)      <---------------- Interruption d'étiquette(L3,96,-)
(8)      <---------------- Garder-en-vie(n/a,97,31) * avec TLV Bouchon FT *
(9)      Garder-en-vie(n/a,-,97) * avec TLV Bouchon FT * ------------------------->
(10)     Notification(Fermeture temporaire) ------------------------->
                      ===== Fermeture de session TCP =====
                  :
                  :                   <-------------------------- Retrait d'étiquette(L1,59,-)
                  :
                  :
                    =====  Session TCP restaurée =====
(11)     Initialisation LDPt(n/a,n/a,96) ------------------------->
         <---------------- Initialisation LDP(n/a,n/a,31)
         <---------------- Retrait d'étiquette(L1,97,-)
```

Notes :

Cet exemple opère à peu près comme le précédent. Cependant, en (1), (2), (3), (4) et (5) aucun accusé de réception n'est fait.

En (6), P1 détermine qu'une fermeture en douceur est nécessaire et envoie un Garder-en-vie qui accuse réception de tous les messages reçus précédemment et contenant lui-même un numéro de TLV Protection FT et le TLV Bouchon FT.

En (7) le Interruption d'étiquette croise ce Garder-en-vie, de sorte que en (8) P2 envoie un Garder-en-vie qui accuse réception de tous les messages reçus jusqu'alors, mais inclut aussi les TLV Protection FT et Bouchon FT pour indiquer qu'il y a encore des messages qui demandent à être acquittés.

P1 est alors capable d'achever la prise de contact en trois phases en (9) et de clore la session TCP en (10).

À la récupération en (11), il n'y a pas de message à renvoyer parce que les Garder-en-vie ont purgé les accusés de réception. Le seul message envoyé après la récupération est le Retrait d'étiquette qui a été mis en attente durant l'arrêt de la session TCP.

9.5 Procédures de vérification-pointage sans FT

```
notes  P1                                                    P2
(1)      Demande d'étiquette(L1) ------------------------->
(2)      <---------------- Demande d'étiquette(L2)
                                                  Demande d'étiquette(L1) ------------------------->
                                        <-------------------------- Transposition d'étiquette(L1)
(3)      <---------------- Transposition d'étiquette(L1)
```

```
(4)   Garder-en-vie(n/a,12,-) ---------------------------->
(5)   Demande d'étiquette(L3) ---------------------------->
(6)   <---------------------- Garder-en-vie(n/a,-,12)
                                                          Demande d'étiquette(L3) ---------------------------->
                                          <-------------------------- Transposition d'étiquette(L3)
(7)   <---------------------- Transposition d'étiquette(L3)
                  ===== Défaillance de session TCP =====
                  :
                  :
                  :
                  ===== Session TCP restaurée =====
(8)   Initialisation LDP(n/a,n/a,23) ---------------------------->
      <---------------------- Initialisation LDP(n/a,n/a,12)
(9)   Demande d'étiquette(L3) ---------------------------->
                                                          Demande d'étiquette(L3) ---------------------------->
                                          <-------------------------- Transposition d'étiquette(L3)
(10)  <---------------------- Transposition d'étiquette(L3)
(11)  <---------------------- Demande d'étiquette(L2)
```

Notes :
(1), (2) et (3) montrent la distribution d'étiquettes sans numéro de séquence FT.
(4) Demande de vérification-pointage de P1. Elle porte le numéro de séquence de la demande de vérification-pointage.
(5) P1 commence immédiatement une nouvelle demande de distribution d'étiquettes.
(6) P2 confirme qu'il a sécurisé toutes les transactions précédentes.
(7) La distribution d'étiquettes suivante (non acquittées) se termine.
(8) La session échoue et est redémarrée. Les messages Initialisation confirment les numéros de séquence de la vérification-pointage sécurisée.
(9) P1 recommence la demande de distribution d'étiquettes non acquittée.
(10) P2 recommence une demande de distribution d'étiquettes non acquittée.

9.6 Fermeture en douceur avec vérification-pointage mais pas de procédures FT

```
notes P1                                                  P2
(1)   Demande d'étiquette(L1) ---------------------------->
(2)   ---------------------- Demande d'étiquette(L2)
                                                          Demande d'étiquette(L1) ---------------------------->
                                          <-------------------------- Transposition d'étiquette(L1)
(3)   <---------------------- Transposition d'étiquette(L1)
(4)   Garder-en-vie(n/a,12,23) * avec TLV Bouchon FT * ---------------------------->
(5)               :
                  :
                  :
(6)   <---------------------- Garder-en-vie(n/a,24,12) * avec TLV Bouchon FT *
(7)   Garder-en-vie(n/a,-,24) * avec TLV Bouchon FT * ---------------------------->
(8)   Notification(Fermeture temporaire) ---------------------------->
                  ===== Session TCP défaillante =====
                  :
                  :
                  :
                  ===== Session TCP restaurée =====
(9)   Initialisation LDP(n/a,n/a,24) ---------------------------->
      <---------------------- Initialisation LDP(n/a,n/a,12)
(10)  Demande d'étiquette(L3) ---------------------------->
                                                          Demande d'étiquette(L3) ---------------------------->
                                          <-------------------------- Transposition d'étiquette(L3)
(11)  <---------------------- Transposition d'étiquette(L3)
(12)  Transposition d'étiquette(L2) ---------------------------->
```

Notes :
(1), (2) et (3) montrent la distribution d'étiquettes sans numéro de séquence FT.
(4) Demande de vérification-pointage de P1. Elle porte le numéro de séquence de la demande de vérification-pointage et

un TLV Bouchon.
(5) P1 a envoyé un TLV Bouchon et passe au repos.
(6) P2 confirme la vérification-pointage et continue la prise de contact à trois phases en incluant lui-même un TLV Bouchon.
(7) P1 achève la prise de contact à trois phases. Toutes les opérations ont maintenant été vérifiées-pointées et la session est au repos.
(8) La session est fermée en douceur.
(9) La session est reprise et les homologues échangent les numéros de séquence des dernières vérifications-pointages sécurisées.
(10) P1 commence une nouvelle demande de distribution d'étiquettes.
(11) P1 continue à traiter une demande de distribution d'étiquettes reçue précédemment.

10. Considérations pour la sécurité

Les améliorations FT à LDP héritent de considérations pour la sécurité similaires à celles exposées dans la [RFC3036].

Les améliorations FT à LDP permettent le rétablissement d'une connexion TCP entre homologues LDP sans un rééchange complet des attributs des étiquettes établies, ce qui rend les LSR qui mettent en œuvre les extensions spécifiée dans ce document vulnérables à des attaques supplémentaires de déni de service :

- Un intrus peut se faire passer pour un homologue LDP afin de forcer une défaillance et reconnexion de la connexion TCP, mais où l'intrus ne règle pas le fanion Reconnexion FT à la reconnexion. Cela force la libération de toutes les étiquettes FT.
- De même, un intrus pourrait au rétablissement de la session TCP régler le fanion Reconnexion FT sans préserver l'état et les ressources pour les étiquettes FT.
- Un intrus pourrait intercepter le trafic entre homologues LDP et outrepasser le réglage du fanion Étiquette FT pour qu'il soit 0 pour toutes les étiquettes.

Toutes ces attaques peuvent être contrées par l'utilisation d'un schéma d'authentification entre homologues LDP, tel que le schéma fondé sur MD5 présenté dans la [RFC3036].

Les autres schémas d'authentification pour les homologues LDP sortent du domaine d'application du présent document, mais pourraient être déployés pour fournir une sécurité améliorée aux mises en œuvre de LDP et des améliorations FT à LDP.

Comme avec LDP, un problème de sécurité peut exister si une mise en œuvre de LDP continue d'utiliser des étiquettes après l'expiration de la session qui a causé leur première utilisation. Cela peut venir de ce que le LSR amont détecte la défaillance de la session après que le LSR aval a libéré et réutilisé l'étiquette. Le problème est très évident avec l'espace d'étiquette aux dimensions de la plate-forme et pourrait résulter et une mauvaise transmission des données à d'autres destinations que celles prévues et il est concevable que ces comportements puissent être délibérément exploités pour obtenir des services sans autorisation ou pour dénier les services aux autres.

Dans le présent document, la validité de la session peut être étendue par la temporisation de reconnexion FT, et la session peut être rétablie dans cette période. Après l'expiration de la temporisation de reconnexion, la session doit être considérée comme ayant échoué et les mêmes problèmes de sécurité que décrits ci-dessus s'appliquent.

Cependant, le LSR aval peut déclarer la session morte avant l'expiration de la temporisation de reconnexion. Cela augmente la période durant laquelle le LSR aval pourra réallouer l'étiquette alors que le LSR amont continue de transmettre des données en se servant de l'ancienne utilisation de l'étiquette. Pour réduire la portée de ce problème, le présent document exige que les étiquettes ne soient pas réutilisées jusqu'à l'expiration de la temporisation de reconnexion.

Un autre problème peut se rencontrer si les étiquettes sont réutilisées avant l'expiration de la temporisation de reconnexion FT, mais ceci est interdit par le présent document.

La question de la réutilisation des étiquettes s'étend aux étiquettes gérées à travers d'autres mécanismes incluant la configuration directe à travers des applications de gestion et la distribution par d'autres protocoles de distribution d'étiquettes. La prévention de ce problème peut être conçue comme une question de mise en œuvre (voir ci-dessous) mais manquer à le reconnaître pourrait résulter en la mauvaise transmission des données entre des LSP établis en utilisant d'autres mécanismes et ceux récupérés en utilisant les méthodes décrites dans le présent document.

11. Notes de mise en œuvre

11.1 Prise en charge de récupération FT sur les LSR non FT

Afin de tirer pleinement parti des capacités FT des LSR dans le réseau, il se peut qu'un LSR qui ne contient pas lui-même la capacité de récupérer de fautes d'un matériel ou logiciel local ait quand même besoin de prendre en charge les améliorations FT à LDP décrites dans ce document.

Considérons un LSR, P1, qui serait un homologue LDP d'un LSR pleinement tolérant aux fautes, P2. Si P2 rencontre une faute dans le matériel ou logiciel qui dessert une session LDP entre P1 et P2, il peut faire échouer la connexion TCP entre les homologues. Lorsque la connexion est récupérée, les LSP/étiquettes entre P1 et P2 ne peuvent être récupérées que si les deux LSR appliquent les procédures de récupération FT à la session LDP.

11.2 Logique de génération d'ACK

Les ACK FT DEVRAIENT être retournés au LSR envoyeur aussitôt qu'il est praticable afin d'éviter de construire une grosse quantité de changements d'état non acquittés au LSR. Cependant, des accusés de réceptions immédiats un à un seraient un gâchis inutile de bande passante.

Une stratégie de mise en œuvre possible pour l'envoi des ACK aux messages LDP FT serait la suivante :
- Un LSR sécurise les messages reçus dans l'ordre et garde trace des numéros de séquence du plus récent message sécurisé, Sr.
- Sur chaque Garder-en-vie LDP qu'envoie le LSR, il attache un TLV ACK FT mentionnant Sr.
- Facultativement, le LSR peut attacher un TLV ACK FT à tout autre message LDP envoyé entre les messages Garder-en-vie si, par exemple, Sr a augmenté de plus que la valeur seuil depuis le dernier ACK envoyé.

Cette mise en œuvre combine l'avantage pour la bande passante d'accumuler les ACK tout en les fournissant à temps.

11.2.1 Logique de génération d'accusé de réception lors de l'utilisation de la vérification-pointage

Si la vérification-pointage est utilisée, les LSR n'ont pas besoin de se soucier d'envoyer des ACK à temps.

Les vérifications-pointages sont des sollicitations d'accusés de réception portées comme numéros de séquence dans un TLV Protection FT sur un message Garder-en-vie. De telles demandes de vérification-pointage pourraient être issues d'un temporisateur, après une quantité de changements significative, ou avant la fermeture contrôlée d'une session.

L'utilisation de la vérification-pointage peut considérablement simplifier une mise en œuvre car elle n'a pas besoin de garder trace des numéros de séquence de tous les messages LDP reçus. Elle doit, cependant, encore s'assurer que tous les messages reçus (ou les changements d'état qui en découlent) sont sécurisés avant d'accuser réception du numéro de séquence dans le Garder-en-vie.

Cette approche peut être considérée comme optimale dans les systèmes qui n'affichent pas un fort degré de changement dans le temps (comme des sessions LDP ciblées) et qui sont prêts à risquer des pertes d'état pour les échanges LDP les plus récents. Les systèmes plus dynamiques (comme les sessions de découverte LDP) vont plus probablement vouloir accuser réception des changements d'état plus fréquemment afin que la quantité maximum d'état puisse être préservée en cas de défaillance.

11.3 Interactions avec les autres mécanismes de distribution d'étiquettes

De nombreux LSR LDP fonctionnent aussi avec d'autres mécanismes de distribution d'étiquettes. Cela inclut des interfaces de gestion pour la configuration de transpositions statiques d'étiquettes, d'autres instances distinctes de LDP, et d'autres protocoles de distribution d'étiquettes. Ce dernier exemple inclut le protocole de distribution d'étiquettes d'ingénierie du trafic qui est utilisé pour construire des tunnels à travers lesquels les LSP LDP sont établis.

Comme avec la réutilisation des étiquettes individuelles par LDP au sein d'un système LDP qui redémarre, il faut faire attention à empêcher les étiquettes qui doivent être conservées par une session LDP qui redémarre ou par un composant de protocole , d'être utilisées par un autre mécanisme de distribution d'étiquettes car cela peut compromettre la sécurité des données, en autres choses.

Il appartient aux mises en œuvre d'éviter ce problème en utilisant des techniques telles qu'un composant commun de gestion d'étiquettes ou des espaces segmentés d'étiquettes.

12. Remerciements

Le travail de ce document se fonde sur les idées exprimées sur LDP par les auteurs de la [RFC3036].

Le schéma ACK utilisé dans ce document s'inspire de la proposition de David Ward et John Scudder de redémarrage des sessions BGP qui est maintenant incluse dans la [RFC4724].

Les auteurs tiennent à remercier de leur relecture attentive et de leurs commentaires Nick Weeds, Piers Finlayson, Tim Harrison, Duncan Archer, Peter Ashwood-Smith, Bob Thomas, S. Manikantan, Adam Sheppard, Alan Davey, Sitekhar Hussain et Loa Andersson.

13. Considérations de propriété intellectuelle

14. Références

14.1 Références normatives

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. *(Remplace* RFC1602, RFC1871) (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378)

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

[RFC3036] L. Andersson et autres, "Spécification de LDP", janvier 2001. *(Rendue obsolète par la RFC5036)*

[RFC3478] M. Leelanivas, Y. Rekhter, R. Aggarwal, "Mécanisme de redémarrage en douceur pour le protocole de distribution d'étiquettes", février 2003. *(P.S.)*

14.2 Références pour information

[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) *(P.S.)*

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

[RFC3209] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan et G. Swallow, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (Mise à jour par RFC3936, RFC4420, RFC4874, RFC5151, RFC5420)

[RFC3212] B. Jamoussi et autres, "Établissement de LSP fondé sur la contrainte avec LDP", janvier 2002. (*MàJ par* RFC3468) *(P.S.)*

[RFC3214] J. Ash et autres, "Modification de LSP avec les CR-LDP", janvier 2002. *(P.S.)*

[RFC4724] S. Sangli et autres, "Mécanisme de redémarrage en douceur pour BGP", janvier 2007. *(P.S.)*

15. Adresse des auteurs

Adrian Farrel (editor)
Movaz Networks, Inc.
7926 Jones Branch Drive, Suite 615
McLean, VA 22102
USA
téléphone : +1 703-847-1867
mél : afarrel@movaz.com

Paul Brittain
Data Connection Ltd.
Windsor House, Pepper Street,
Chester, Cheshire
CH1 1DF, UK
téléphone : +44-(0)20-8366-1177
mél : pjb@dataconnection.com

Philip Matthews
Hyperchip
1800 Rene-Levesque Blvd W
Montreal, Quebec H3H 2H2
Canada
téléphone : +1 514-906-4965
mél : pmatthews@hyperchip.com

Eric Gray
mél : ewgray@GraIyMage.com

Jack Shaio
Vivace Networks
2730 Orchard Parkway
San Jose, CA 95134
téléphone : +1 408 432 7623
mél : jack.shaio@vivacenetworks.com

Toby Smith
Laurel Networks, Inc.
1300 Omega Drive
Pittsburgh, PA 15205
USA
mél : tob@laurelnetworks.com

Andrew G. Malis
Vivace Networks
2730 Orchard Parkway
San Jose, CA 95134
téléphone : +1 408 383 7223
mél : andy.malis@vivacenetworks.com

16. Déclaration de droits de reproduction

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