Groupe de travail Réseau E. Mannie, éditeur
Request for Comments : 3945
Catégorie : Sur la voie de la normalisation octobre 2004
Traduction Claude Brière de L'Isle

Architecture de la commutation d'étiquettes multi protocoles généralisée (GMPLS)

Statut de ce mémoire

Notice de copyright

Résumé

Les futurs réseaux de données et de transmission consisteront en éléments tels que routeurs, commutateurs, systèmes de multiplexage par répartition en longueur d'onde à haute densité (DWDM, *Dense Wavelength Division Multiplexing*) multiplexeurs d'insertion/extraction (ADM, *Add/Drop Multiplex*) brasseurs photoniques (PXC, *photonic cross-connect*) brasseurs optiques (OXC, *optical cross-connect*) etc., qui vont utiliser la commutation d'étiquette multi protocoles généralisée (GMPLS) pour provisionner dynamiquement des ressources et pour assurer la survie du réseau en utilisant les techniques de protection et de restauration.

Le présent document décrit l'architecture de GMPLS. GMPLS étend MPLS pour englober la commutation à division temporelle (par exemple, SONET/SDH, PDH, G.709) en longueur d'onde (lambdas) et spatiale (par exemple, d'accès ou fibre entrant à accès ou fibre sortant). GMPLS se concentre sur le plan de contrôle de ces trois couches car chacune d'elles peut utiliser des données ou plans de transmission physiquement divers. L'intention est de couvrir les deux parties signalisation et acheminement de ce plan de contrôle.

Table des Matières

1. Introduction

L'architecture décrite dans le présent document couvre les principaux éléments de construction nécessaires pour bâtir un plan de contrôle cohérent pour plusieurs couches de commutation. Elle n'exerce pas de contrainte sur la façon dont ces couches travaillent ensemble. Des modèles différents peuvent être appliqués, par exemple, recouvrement, augmenté ou intégré. De plus, chaque paire de couches contiguës peut collaborer de différentes façons, résultant en un certain nombre de combinaisons possibles, à la discrétion des fabricants et des opérateurs.

Cette architecture sépare clairement le plan de contrôle et le plan de transmission. De plus, elle sépare aussi clairement le plan de contrôle en deux parties, le plan de signalisation contenant les protocoles de signalisation et le plan d'acheminement contenant les protocoles d'acheminement.

Le présent document est une généralisation de l'architecture de commutation d'étiquettes multi protocoles (MPLS, *Multi-Protocol Label Switching*) [RFC3031], et il peut dans certains cas différer légèrement de cette architecture car on prend

maintenant en considération des plans de transmission non fondés sur le paquet. Il n'est pas dans les intentions du présent document de décrire les concepts qui sont déjà décrits dans l'architecture MPLS actuelle. Son but est de décrire les concepts spécifiques de MPLS généralisé (GMPLS).

Cependant, certains des concepts expliqués ici ne font pas partie de l'architecture MPLS actuelle et sont applicables à la fois à MPLS et à GMPLS (c'est-à-dire, la mise en faisceaux de liaisons, les liaisons non numérotées, la hiérarchie des LSP). Comme ces concepts ont été introduits avec GMPLS et comme ils sont d'une importance capitale pour un réseau GMPLS opérationnel, ils seront exposés ici.

L'organisation du reste du présent document est comme suit. On commence par une introduction de GMPLS. On présente ensuite les éléments de construction spécifiques de GMPLS et on explique comment ils peuvent être combinés ensemble pour bâtir un réseau GMPLS opérationnel. Les détails spécifiques des différents éléments de construction se trouvent dans les documents correspondants.

1.1 Acronymes et abréviations

AS *(Autonomous System)* = système autonome
BGP *(Border Gateway Protocol)* = protocole de passerelle frontière
CR-LDP *(Constraint-based Routing LDP)* = protocole de distribution d'étiquettes fondé sur la contrainte
CSPF *(Constrained Shortest Path First)* = chemin le plus court en premier obligé
DWDM *(Dense Wavelength Division Multiplexing)* = multiplexage par répartition en longueur d'onde à haute densité ;
FA *(Forwarding Adjacency)* = adjacence de transmission
GMPLS = commutation multi protocoles avec étiquetage généralisé des flux
IGP *(Interior Gateway Protocol)* = protocole de passerelle intérieure
LDP *(Label Distribution Protocol)* = protocole de distribution d'étiquettes
LMP *(Link Management Protocol)* = protocole de gestion de liaisons
LSA *(Link State Advertisement)* = avis d'état de liaison
LSR *(label switched router)* = routeur à commutation d'étiquettes
LSP *(Label Switched Path)* = chemin commuté par étiquettes
MIB *(Management Information Base)* = base de données d'informations de gestion
MPLS *(multi-protocol label switching)* = commutation multi protocoles par étiquetage
NMS *(network management system)* = système de gestion de réseau
OXC *(Optical Cross-Connect)* = brasseur optique
PXC *(photonic cross-connect)* = brasseur photonique
RSVP *(Resource ReserVation Protocol)* = protocle de réservation de ressources
SDH *(synchronous digital hierarchy)* = hiérarchie numérique synchrone ;
SONET *(Synchronous Optical NETwork)* = réseau optique synchrone
STM(-N) (*Synchronous Transport Module (-N)*) = module de transport synchrone de niveau N
STS(-N) *(Synchronous Transport Signal-Level N)* = signal de niveau N de transport synchrone
TDM *(Time Division Multiplexing)* = multiplexage par répartition dans le temps
TE *(Traffic Engineering)* = ingénierie du trafic

1.2 Multiples types de commutation et hiérarchies de transmission

La commutation multi protocoles par étiquetage généralisé (GMPLS, *Generalized MPLS*) diffère de la MPLS traditionnelle en ce qu'elle prend en charge plusieurs types de commutation, c'est-à-dire, avec l'ajout de la prise en charge de la commutation de TDM, lambda, et fibre (accès). La prise en charge de types supplémentaires de commutation a conduit GMPLS à étendre certaines fonctions de base du MPLS traditionnel, et dans certains cas, à ajouter des fonctionnalités. Ces changements et ajouts ont un impact sur les propriétés de base de LSP : comment les étiquettes sont demandées et communiquées, la nature unidirectionnelle des LSP, comment les erreurs sont propagées, et les informations fournies pour synchroniser les LSR d'entrée et de sortie.

L'architecture MPLS [RFC3031] a été définie pour prendre en charge la transmission de données fondée sur une étiquette. Dans cette architecture, les routeurs de commutation d'étiquettes (LSR, *Label Switching Router*) sont supposés avoir un plan de transmission qui est capable de (a) reconnaître les limites de paquet ou de cellule, et (b) traiter les en-têtes de paquet (pour les LSR capables de reconnaître les limites de paquet) ou les en-têtes de cellule (pour les LSR capables de reconnaître les limites de cellule).

L'architecture MPLS d'origine est étendue ici pour y inclure les LSR dont le plan de transmission ne reconnaît ni les limites de paquet ni les limites de cellule, et donc, ne peuvent pas transmettre de données sur la base des informations portées dans les en-têtes de paquet ou de cellule. Précisément, de tels LSR incluent des appareils où la décision de commutation est

fondée sur les créneaux temporels, les longueurs d'onde, ou les accès physiques. Donc, le nouvel ensemble de LSR, ou plus précisément les interfaces sur ces LSR, peut être subdivisé en les classes suivantes :

1. Interfaces capables de commutation de paquet (PSC, *Packet Switch Capable*) :
   Interfaces qui reconnaissent les limites de paquet et peuvent transmettre des données sur la base du contenu de l'en-tête de paquet. Les exemples incluent des interfaces sur des routeurs qui transmettent des données sur la base du contenu de l'en-tête IP et des interfaces sur des routeurs qui commutent les données sur la base du contenu de l'en-tête MPLS "shim".

2. Interfaces capables de commutation de couche 2 (L2SC, *Layer-2 Switch Capable*) :
   Interfaces qui reconnaissent les limites de trame/cellule et peuvent commuter les données sur la base du contenu de la trame/en-tête de cellule. Les exemples incluent des interfaces sur les ponts Ethernet qui commutent les données sur la base du contenu de l'en-tête MAC et des interfaces sur les LSR ATM qui transmettent les données sur la base du VPI/VCI ATM.

3. Interfaces capables de multiplexage dans le temps (TDM, *Time-Division Multiplex*) :
   Interfaces qui commutent les données sur la base de l'intervalle de temps des données dans un cycle répété. Un exemple d'une telle interface est celui d'un brasseur SONET/SDH, un multiplexeur de terminal (TM), ou un multiplexeur à insertion extraction (ADM, *Add-Drop Multiplexe*r). D'autres exemples incluent des interfaces fournissant des capacités TDM G.709 ("enveloppeur numérique") et les interfaces PDH.

4. Interfaces capables de commutation lambda (LSC, *Lambda Switch Capable*) :
   Interfaces qui commutent les données sur la base de la longueur d'onde sur laquelle les données sont reçues. Un exemple d'une telle interface est celui d'un brasseur photonique (PXC, *Photonic Cross-Connect*) ou d'un brasseur optique (OPX, *Optical Cross-Connect*) qui peut fonctionner au niveau d'une longueur d'onde individuelle. Des exemples supplémentaires incluent des interfaces PXC qui peuvent fonctionner au niveau d'un groupe de longueurs d'onde, c'est-à-dire, une bande de fréquence, et des interfaces G.709 qui fournissent des capacités optiques.

5. Interfaces capables de commutation de fibre (FSC, *Fiber-Switch Capable*) :
   Interfaces qui commutent les données sur la base de la position des données dans les espaces physiques (réels). Un exemple d'une telle interface est celui d'un PXC ou OXC qui peut fonctionner au niveau d'une seule fibre ou de plusieurs.

Un circuit peut seulement être établi entre, ou à travers, des interfaces de même type. Selon la technologie particulière utilisée pour chaque interface, des noms de circuit différents peuvent être utilisés, par exemple, circuit SDH, piste optique, chemin de la lumière, etc. Dans le contexte de GMPLS, tous ces circuits sont appelés d'un nom commun : chemin commuté par étiquettes (LSP, *Label Switched Path*).

Le concept de LSP incorporé (LSP dans un LSP) déjà disponible dans le MPLS traditionnel, facilite la construction d'une hiérarchie de transmission, c'est-à-dire, une hiérarchie de LSP. Cette hiérarchie de LSP peut se produire sur la même interface, ou entre des interfaces différentes.

Par exemple, une hiérarchie peut être construite si une interface est capable de multiplexer plusieurs LSP de la même technologie (couche) par exemple, un LSP SONET/SDH d'ordre inférieur (par exemple, VT2/VC-12) incorporé dans un LSP SONET/SDH d'ordre supérieur (par exemple, STS-3c/VC-4). Plusieurs niveaux d'incorporation de signal (LSP) sont définis dans la hiérarchie de multiplexage SONET/SDH.

L'incorporation peut aussi se produire entre des types d'interface. Au sommet de la hiérarchie sont les interfaces FSC, suivies par les interfaces LSC, suivies par les interfaces TDM, suivies par L2SC, et suivies par les interfaces PSC. De cette façon, un LSP qui commence et se termine sur une interface PSC peut être incorporé (avec d'autres LSP) dans un LSP qui commence et se termine sur une interface L2SC. Ce LSP, à son tour, peut être incorporé (avec d'autres LSP) dans un LSP qui commence et se termine sur une interface TDM. À son tour, ce LSP peut être incorporé (avec d'autres LSP) dans un LSP qui commence et se termine sur une interface LSC, qui à son tour peut être incorporée (avec d'autres LSP) dans un LSP qui commence et se termine sur une interface FSC.

1.3 Extension du plan de contrôle MPLS

L'établissement de LSP qui s'étendent seulement sur des interfaces capables de commutation par paquet (PSC) ou de commutation de couche 2 (L2SC) est défini pour les plans de contrôle originaux MPLS et/ou MPLS-TE. GMPLS étend ces plans de contrôle pour prendre en charge chacune des cinq classes d'interfaces (c'est-à-dire, couches) définies dans le paragraphe précédent.

Noter que le plan de contrôle GMPLS prend en charge un modèle de recouvrement, un modèle augmenté, et un modèle d'homologue (intégré). À court terme, GMPLS paraît convenir parfaitement pour contrôler chaque couche indépendamment. Cette approche élégante va faciliter le futur déploiement d'autres modèles.

Le plan de contrôle GMPLS est fait de plusieurs blocs de construction, comme décrit plus en détails dans les sections suivantes. Ces éléments de construction se fondent sur les protocoles bien connus de signalisation et d'acheminement qui ont été étendus et/ou modifiés pour prendre en charge GMPLS. Ils utilisent des adresses IPv4 et/ou IPv6. Un seul nouveau protocole spécialisé est nécessaire pour prendre en charge le fonctionnement de GMPLS, un protocole de signalisation pour la gestion des liaisons [RFC4204].

GMPLS se fonde bien sûr sur les extensions d'ingénierie du trafic (TE, *Traffic Engineering*) à MPLS, autrement dit,. MPLS-TE [RFC2702]. Cela, parce que la plupart des technologies qui peuvent être utilisées en dessous du niveau de PSC exigent de l'ingénierie du trafic. Le placement des LSP à ces niveaux exige en général de prendre en compte plusieurs contraintes (comme le tramage, la bande passante, la capacité de protection, etc.) et de court-circuiter l'algorithme traditionnel du plus court chemin en premier (SPF, *Shortest-Path First*). Noter, cependant, que ceci n'est pas obligatoire et que dans certains cas l'acheminement SPF peut s'appliquer.

Afin de faciliter l'acheminement SPF fondé sur la contrainte des LSP, les nœuds qui effectuent l'établissement de LSP ont besoin de plus d'informations sur les liaisons dans le réseau que n'en fournissent les protocoles standard d'acheminement intra domaine. Ces attributs TE sont distribués en utilisant des mécanismes de transport déjà disponibles dans les IGP (par exemple, l'arrosage) et qui sont pris en compte par l'algorithme d'acheminement de LSP. L'optimisation des chemins de LSP peut aussi exiger des simulations externes utilisant des heuristiques qui servent d'entrées pour le calcul du chemin réel et le processus d'établissement de LSP.

Par définition, une liaison TE est une représentation dans les annonces d'état de liaison IS-IS/OSPF et dans la base de données d'état de liaison de certaines ressources physiques, et de leurs propriétés, entre deux nœuds GMPLS. Les liaisons TE sont utilisées par le plan de contrôle GMPLS (acheminement et signalisation) pour établir les LSP.

Des extensions aux protocoles et algorithmes traditionnels d'acheminement sont nécessaires pour coder uniformément et porter les informations de liaisons TE, et les chemins explicites (par exemple, chemins de source) sont exigés dans la signalisation. De plus, la signalisation doit maintenant être capable de transporter les paramètres de circuit (LSP) exigés comme la bande passante, le type de signal, la protection désirée et/ou la restauration, la position dans un multiplex particulier, etc. La plupart de ces extensions ont déjà été définies pour l'ingénierie du trafic PSC et L2SC avec MPLS. GMPLS définit principalement des extensions supplémentaires pour l'ingénierie du trafic TDM, LSC, et FSC. Quelques éléments sont spécifiques de la technologie.

Donc, GMPLS étend les deux protocoles de signalisation définis pour la signalisation MPLS-TE, c'est-à-dire, RSVP-TE [RFC3209] et CR-LDP [RFC3212]. Cependant, GMPLS ne spécifie pas lequel de ces deux protocoles de signalisation doit être utilisé. C'est le rôle des fabricants et des opérateurs d'évaluer les deux solutions possibles dans leur propre intérêt.

Comme la signalisation GMPLS se fonde sur RSVP-TE et CR-LDP, elle rend obligatoire une allocation et distribution d'étiquettes vers l'aval à la demande, avec un contrôle initié par l'entrée. La rétention libérale d'étiquette est normalement utilisée, mais le mode de rétention d'étiquette prudent pourrait aussi être utilisé.

De plus, il n'y a pas de restriction sur la stratégie d'allocation d'étiquette, qui peut être pilotée par la demande/signalisation (évidente pour les technologies de commutation de circuits) pilotée par le trafic/données, ou même pilotée par la topologie. Il n'y a pas non plus de restriction sur le choix du chemin ; l'acheminement explicite est normalement utilisé (strict ou lâche) mais l'acheminement bond par bond pourrait aussi être utilisé.

GMPLS étend aussi deux protocoles traditionnels d'acheminement d'état de liaison intra domaine déjà étendus pour les besoins de l'ingénierie du trafic, c'est-à-dire, OSPF-TE [RFC3630] et IS-IS-TE [RFC3784]. Cependant, si l'acheminement explicite (de source) est utilisé, les algorithmes d'acheminement utilisés par ces protocoles n'ont plus besoin d'être normalisés. Les extensions pour l'acheminement inter domaines (par exemple, BGP) feront l'objet d'études ultérieures.

L'utilisation de technologies comme le multiplexage par répartition en longueur d'onde à haute densité (DWDM, *Dense Wavelength Division Multiplexing*) implique qu'on peut avoir maintenant un très grand nombre de liaisons parallèles entre deux nœuds directement adjacents (des centaines de longueurs d'onde, ou même des milliers de longueurs d'onde si on utilise plusieurs fibres). Un tel nombre de liaisons n'était pas envisagé à l'origine pour un plan de contrôle IP ou MPLS, mais pas exclu. Quelques légères adaptations de ce plan de contrôle sont donc nécessaires si on veut mieux le réutiliser dans le contexte GMPLS.

Par exemple, le modèle traditionnel d'acheminement IP suppose l'établissement d'une adjacence d'acheminement sur chaque liaison connectant deux nœuds adjacents. Cela ne s'adapte pas bien à de si grands nombres d'adjacences. Chaque

nœud doit maintenir une par une chacune de ses adjacences, et les informations d'acheminement d'état de liaison doivent être diffusées dans tout le réseau.

On a introduit le concept de faisceau de liaisons pour résoudre ce problème. De plus, la configuration et le contrôle manuel de ces liaisons, même si elles sont non numérotées, devient impraticable. Le protocole de gestion de liaison (LMP, *Link Management Protocol*) a été spécifié pour résoudre ces questions.

LMP fonctionne entre nœuds adjacents du plan de données et est utilisé pour gérer les liaisons d'ingénierie du trafic. Précisément, LMP fournit des mécanismes pou maintenir la connexité du canal de contrôle (maintenance du canal de contrôle IP) vérifier la connexité physique des liaisons porteuses de données (vérification de liaison) corréler les informations de propriété de la liaison (corrélation de propriété de liaison) et gérer les défaillances de liaison (localisation de faute et notification de faute). Une caractéristique unique de LMP est qu'il est capable de localiser des fautes dans des réseaux opaques aussi bien que transparents (c'est-à-dire, indépendamment du schéma de codage et du débit binaire utilisés pour les données).

LMP est défini dans le contexte de GMPLS, mais est spécifié indépendamment de la spécification de signalisation GMPLS car c'est un protocole local qui fonctionne entre les nœuds adjacents du plan de données.

Par conséquent, LMP peut être utilisé dans d'autres contextes avec des protocoles de signalisation non GMPLS.

Les protocoles de signalisation et d'acheminement MPLS exigent au moins un canal bidirectionnel pour communiquer même si deux nœuds adjacents sont connectés par des liaisons unidirectionnelles. Plusieurs canaux de contrôle peuvent être utilisés. LMP peut être utilisé pour établir, maintenir et gérer ces canaux de contrôle.

GMPLS ne spécifie pas comment ces canaux de contrôle doivent être mis en œuvre, mais GMPLS exige qu'IP transporte sur eux les protocoles de signalisation et d'acheminement. Les canaux de contrôle peuvent être dans la bande ou hors bande, et plusieurs solutions peuvent être utilisées pour porter IP. Noter aussi qu'un type de message LMP (le message Test) est utilisé dans la bande dans le plan des données et ne peut pas être transporté sur IP, mais c'est un cas particulier, nécessaire pour vérifier la connexité dans le plan des données.

1.4 Extensions clé de GMPLS pour MPLS-TE

On précise ici certaines extensions clés apportées par GMPLS à MPLS-TE. Certaines ont l'avantage majeur de GMPLS de contrôler les couches TDM, LSC et FSC.

- Dans MPLS-TE, les liaisons traversées par un LSP peuvent inclure un entrelaçage de liaisons avec des codages d'étiquette hétérogènes (par exemple, des liaisons entre routeurs, des liaisons entre routeurs et LSR ATM, et des liaisons entre des LSR ATM. GMPLS étend cela en incluant des liaisons où l'étiquette est codée comme intervalle de temps, ou longueur d'onde, ou une position dans l'espace physique (réel).

- Dans MPLS-TE, un LSP qui porte IP doit commencer et finir sur un routeur. GMPLS étend ceci en exigeant qu'un LSP commence et finisse sur des types d'interfaces similaires.

- Le type d'une charge utile qui peut être portée dans GMPLS par un LSP est étendu pour permettre que de telles charges utiles soient SONET/SDH, G.709, Ethernet 1 Gbit/s ou 10 Gbit/s, etc.

- L'utilisation des adjacences de transmission (FA, *Forwarding Adjacencies*) donne un mécanisme qui peut améliorer l'utilisation de la bande passante, lorsque l'allocation de bande passante peut être effectuée seulement en unités discrètes. Cela offre aussi un mécanisme pour agréger l'état de transmission, permettant donc de réduire le nombre d'étiquettes exigées.

- GMPLS permet qu'un nœud en amont suggère une étiquette afin de réduire la latence d'établissement. Cette suggestion peut être outrepassée par un nœud aval mais dans certains cas, au prix d'un temps plus long d'établissement de LSP.

- GMPLS étend la notion de restriction de la gamme d'étiquettes que peut choisir un nœud aval. Dans GMPLS, un nœud amont peut restreindre les étiquettes pour un LSP le long d'un seul bond ou pour le chemin entier de LSP. Cette disposition est utile dans les réseaux photoniques où la conversion de longueur d'onde peut n'être pas disponible.

- Alors que les LSP traditionnels fondés sur TE (et même fondés sur LDP) sont unidirectionnels, GMPLS prend en charge l'établissement de LSP bidirectionnels.

- GMPLS prend en charge la terminaison d'un LSP sur un accès de sortie spécifique, c'est-à-dire, le choix de l'accès du côté de destination.

- GMPLS avec RSVP-TE prend en charge un mécanisme spécifique de RSVP pour une notification rapide des défaillances.

Noter aussi quelques autres différences clés entre MPLS-TE et GMPLS :

- Pour les interfaces TDM, LSC et FSC, l'allocation de bande passante pour un LSP peut être effectuée seulement en unités discrètes.

- On s'attend à avoir beaucoup moins d'étiquettes sur les liaisons TDM, LSC ou FSC que sur les liaisons PSC ou L2SC, parce que ces dernières sont des étiquettes physiques au lieu d'étiquettes logiques.

2. Modèle d'acheminement et d'adressage

GMPLS se fonde sur les modèles d'acheminement et d'adressage IP. Cela suppose que les adresses IPv4 et/ou IPv6 sont utilisées pour identifier les interfaces mais aussi que les protocoles d'acheminement IP traditionnels (distribués) sont réutilisés. Bien sûr, la découverte de la topologie et de l'état des ressources de toutes les liaisons dans un domaine d'acheminement est réalisée via ces protocoles d'acheminement.

Comme les plans de contrôle et de données sont découplés dans GMPLS, les voisins du plan de contrôle (c'est-à-dire, les voisins appris par IGP) peuvent n'être pas des voisins du plan des données. Donc, des mécanismes comme LMP sont nécessaires pour associer les liaisons TE aux nœuds voisins.

Les adresses IP ne sont pas seulement utilisées pour identifier les interfaces des hôtes et routeurs IP, mais plus généralement pour identifier toutes les interfaces PSC et non PSC. De même, les protocoles d'acheminement IP sont utilisés pour trouver des chemins pour les datagrammes IP avec un algorithme SPF ; ils sont aussi utilisés pour trouver des chemins pour les circuits non PSC en utilisant un algorithme CSPF.

Cependant, des mécanismes supplémentaires sont nécessaires pour augmenter l'adaptabilité de ces modèles et pour traiter les exigences spécifiques de l'ingénierie du trafic de couches non PSC. Ces mécanismes seront présentés ci-dessous.

Réutiliser des protocoles d'acheminement IP existants permet que des couches non PSC tirent parti de tous les développements valables qui ont eu lieu depuis des années d'acheminement IP, en particulier, dans le contexte de l'acheminement intra domaine (acheminement d'état de liaison) et inter domaine (acheminement de politique).

Dans un modèle à recouvrement, chaque couche non PSC particulière peut être vue comme un ensemble de systèmes autonomes (AS, *Autonomous System*) interconnectés de façon arbitraire. De même que dans l'acheminement IP traditionnel, chaque AS est géré par une seule autorité administrative. Par exemple, un AS peut être un réseau SONET/SDH géré par un seul opérateur. L'ensemble des AS interconnectés peut être vu comme des inter réseaux SONET/SDH.

L'échange des informations d'acheminement entre les AS peut être fait via un protocole d'acheminement inter domaines comme BGP-4. Il y a évidemment une valeur énorme à réutiliser les facilités d'acheminement de politiques bien connues fournies par BGP dans un contexte non PSC. Les extensions à l'ingénierie du trafic BGP (BGP-TE) dans le contexte de couches non PSC feront l'objet d'études ultérieures.

Chaque AS peut être subdivisé en différents domaines d'acheminement, et chacun peut fonctionner avec un protocole d'acheminement intra domaine différent. À son tour, chaque domaine d'acheminement peut être divisé en zones.

Un domaine d'acheminement est fait de nœuds à capacité GMPLS (c'est-à-dire, un appareil réseau qui comporte une entité GMPLS). Ces nœuds peuvent être soit des nœuds de bordure (c'est-à-dire, des hôtes, des LSR d'entrée ou de sortie) soit des LSR internes. Un exemple d'hôte non PSC est un multiplexeur terminal (TM, *Terminal Multiplexer*) SONET/SDH. Un autre exemple est une carte d'interface SONET/SDH au sein d'un routeur IP ou d'un commutateur ATM.

Noter que l'ingénierie du trafic dans l'intra domaine exige l'utilisation de protocoles d'acheminement de l'état de liaison comme OSPF ou IS-IS.

GMPLS définit des extensions à ces protocoles. Ces extensions sont nécessaires pour disséminer les caractéristiques dynamiques et statiques spécifiques de TDM, LSC et FSC qui se rapportent aux nœuds et aux liaisons. On met l'accent sur l'ingénierie du trafic intra zone. Cependant, on examine aussi l'ingénierie du trafic inter zone.

2.1 Adressage de couches PSC et non PSC

Le fait que les adresses IPv4 et/ou IPv6 soient utilisées n'implique pas du tout qu'elles devraient être allouées dans le même espace d'adressage que les adresses IPv4 et/ou IPv6 publiques utilisées pour l'Internet. Les adresses IP privées peuvent être utilisées si il n'est pas exigé qu'elles soient échangées avec un autre opérateur ; les adresses IP publiques sont alors exigées. Bien sûr, si on utilise un modèle intégré, deux couches pourraient partager le même espace d'adressage. Finalement, les liaisons TE peuvent être "sous numérotées" c'est-à-dire, ne pas avoir d'adresse IP, au cas où des adresses IP ne sont pas disponibles, ou si les frais généraux de leur gestion sont considérés comme trop élevés.

Noter qu'il y a un avantage à utiliser les adresses Internet publiques IPv4 et/ou IPv6 pour des couches non PSC si un modèle intégré est prévu avec la couche IP.

Si on considère les améliorations d'adaptabilité proposées au paragraphe suivant, les espaces d'adressage IPv4 (32 bits) et IPv6 (128 bits) sont tous deux plus que suffisants pour s'accommoder de toute couche non PSC. On peut raisonnablement s'attendre à avoir beaucoup moins d'appareils non PSC (par exemple, des nœuds SONET/SDH) qu'il n'y a aujourd'hui d'hôtes et routeurs IP.

2.2 Améliorations de l'adaptabilité de GMPLS

Les couches TDM, LSC et FSC introduisent de nouvelles contraintes sur ces modèles d'adressage et d'acheminement IP car plusieurs centaines de liaisons physiques parallèles (par exemple, des longueurs d'onde) peuvent maintenant connecter deux nœuds. La plupart des opérateurs ont déjà aujourd'hui plusieurs dizaines de longueurs d'onde par fibre entre deux nœuds. La nouvelle génération de systèmes DWDM permettra plusieurs centaines de longueurs d'onde par fibre.

Il devient assez peu pratique d'associer une adresse IP à chaque extrémité de chaque liaison physique, pour représenter chaque liaison comme une adjacence d'acheminement séparée, et d'annoncer et entretenir les états des liaisons pour chacune de ces liaisons. Dans ce but, GMPLS améliore les modèles d'acheminement et d'adressage MPLS pour augmenter leur adaptabilité.

Deux mécanismes facultatifs peuvent être utilisés pour augmenter l'adaptabilité de l'adressage et de l'acheminement : les liaisons non numérotées et le faisceau de liaisons. Ces deux mécanismes peuvent aussi être combinés. Ils exigent des extensions aux protocoles de signalisation (RSVP-TE et CR-LDP) et d'acheminement (OSPF-TE et IS-IS-TE).

2.3 Extensions d'ingénierie du trafic aux protocoles d'acheminement IP

Traditionnellement, une liaison TE est annoncée comme une adjonction à une liaison "régulière" OSPF ou IS-IS, c'est-à-dire, une adjacence est apportée à la liaison. Lorsque la liaison est activée, les propriétés régulières IGP de la liaison (fondamentalement, la métrique SPF) et les propriétés TE de la liaison sont alors toutes deux annoncées.

Cependant, GMPLS remet en question cette notion de trois façons :
- D'abord, les liaisons qui sont non PSC peuvent avoir quand même les propriétés de TE ; cependant, une adjacence SPF ne pourrait pas être activée directement sur de telles liaisons.
- Ensuite, un LSP peut être annoncé comme liaison TE point à point dans le protocole d'acheminement, c'est-à-dire, comme une adjacence de transmission (FA, *Forwarding Adjacency*) ; donc, une liaison TE annoncée n'a plus besoin d'être entre deux voisins OSPF directs. Les adjacences de transmission (FA) sont décrites plus en détails à la Section 8.
- Enfin un certain nombre de liaisons peuvent être annoncées comme une seule liaison TE (par exemple, pour une meilleure adaptabilité) donc là encore il n'y a plus d'association biunivoque d'une adjacence régulière et d'une liaison TE.

Donc, nous avons une notion plus générale d'une liaison TE. Une liaison TE est une liaison logique qui a des propriétés de TE. Certaines de ces propriétés peuvent être configurées sur le LSR annonceur, d'autres peuvent être obtenues d'autres LSR au moyen d'un certain protocole, et d'autres encore peuvent être déduites du ou des composants de la liaison TE.

Une importante propriété de TE d'une liaison TE se rapporte à la bande passante prise en compte pour cette liaison. GMPLS va définir différentes règles de prise en compte pour différentes couches non PSC. Les attributs génériques de bande passante sont cependant définis par les extensions d'acheminement TE et par GMPLS, comme la bande passante non réservée, la bande passante maximum réservable et la bande passante maximum de LSP.

Dans un environnement dynamique, on s'attend à avoir de fréquents changements d'informations de prise en compte de bande passante. Une politique souple de déclenchement de mise à jour d'état de liaison sur la base de seuils de bande passante et de mécanisme de refroidissement de liaison peut être mise en œuvre.

Les propriétés TE associées à une liaison devraient aussi capturer les caractéristiques relatives à la protection et la restauration. Par exemple, une protection partagée peut être combinée de façon élégante avec la mise en faisceaux. La protection et la restauration sont des mécanismes principalement génériques aussi applicables à MPLS. On s'attend à ce qu'ils soient d'abord développés pour MPLS et ensuite généralisés à GMPLS.

Une liaison TE entre une paire de LSR n'implique pas l'existence d'une adjacence IGP entre ces LSR. Une liaison TE doit aussi avoir des moyens permettant au LSR annonceur de savoir s'il est en vie (par exemple, en utilisant les hellos LMP). Lorsque un LSR sait qu'une liaison TE est active, et qu'il peut déterminer les propriétés TE de la liaison TE, le LSR peut alors annoncer cette liaison à ses voisins OSPF ou IS-IS améliorés GMPLS en utilisant les objets/TLV TE. On appelle les interfaces sur lesquelles sont établies les adjacences OSPF ou IS-IS améliorées GMPLS des "canaux de contrôle".

3. Liaisons non numérotées

Les liaisons (ou interfaces) non numérotées sont des liaisons (ou interfaces) qui n'ont pas d'adresse IP. Utiliser de telles liaisons implique deux capacités : celle de spécifier les liaisons non numérotées dans la signalisation TE de MPLS, et celle de porter (TE) les informations sur les liaisons non numérotées dans les extensions TE IGP de IS-IS-TE et OSPF-TE.

A. La capacité de spécifier les liaisons non numérotées dans la signalisation TE de MPLS exige des extensions à RSVP-TE [RFC3477] et à CR-LDP [RFC3480]. La signalisation TE de MPLS ne fournit pas de prise en charge pour les liaisons non numérotées, parce qu'elle n'a pas de moyen d'indiquer une liaison non numérotée dans son objet/TLV Chemin explicite (ER, *Explicit Route*) et son objet Chemin enregistré (RR, *Registered Route*) (il n'y a pas de tel TLV pour CR-LDP). GMPLS définit de simples extensions pour indiquer une liaison non numérotée dans ces deux objets/TLV, en utilisant un nouveau sous objet/sous TLV Identifiant d'interface non numérotée.

   Comme les liaisons non numérotées ne sont pas identifiées par une adresse IP, pour les besoins de TE MPLS chaque extrémité a besoin d'un autre identifiant, local, pour le LSR auquel appartient la liaison. Les LSR aux deux points d'extrémité d'une liaison non numérotée s'échangent les identifiants qu'ils allouent à la liaison. L'échange des identifiants peut se faire par configuration, au moyen d'un protocole comme LMP ([RFC4204]), au moyen de RSVP-TE/CR-LDP (en particulier dans le cas d'une liaison qui est une adjacence de transmission, voir ci-dessous) ou au moyen d'extensions IS-IS ou OSPF ([RFC4205], [RFC4203]).

   Considérons une liaison (non numérotée) entre les LSR A et B. Le LSR A choisit un identifiant pour cette liaison. Ainsi fait le LSR B. Du point de vue de A, on se réfère à l'identifiant que A a alloué à la liaison comme "identifiant local de liaison" (ou juste "identifiant local") et à l'identifiant que B a alloué à la liaison comme "identifiant de liaison distante" (ou juste "identifiant distant"). De même, du point de vue de B, l'identifiant que B a alloué à la liaison est l'identifiant local, et l'identifiant que A a alloué à la liaison est l'identifiant distant.

   Le nouveau sous objet/sous TLV Identifiant d'interface non numérotée pour l'objet/TLV ER contient l'identifiant de routeur du LSR à l'extrémité amont de la liaison non numérotée et l'identifiant local de liaison par rapport à ce LSR amont.

   Le nouveau sous objet Identifiant d'interface non numérotée pour l'objet RR contient l'identifiant local de liaison par rapport au LSR qui l'ajoute dans l'objet RR.

B. La capacité de porter les informations (TE) sur les liaisons non numérotées dans les extensions TE IGP exige de nouveaux sous TLV pour le TLV d'accessibilité IS étendue défini dans IS-IS-TE et pour le LSA TE (qui est un LSA opaque) défini dans OSPF-TE. On définit un sous TLV Identifiant de liaison locale et un sous TLV Identifiant de liaison distante.

3.1 Adjacences de transmission non numérotées

Si un LSR qui génère un LSP annonce ce LSP comme une adjacence de transmission (FA) non numérotée dans IS-IS ou OSPF, ou si le LSR utilise cette FA comme une liaison composante non numérotée d'un faisceau de liaisons, le LSR doit allouer un identifiant d'interface à cette FA. Si le LSP est bidirectionnel, l'extrémité de queue fait la même chose et alloue un identifiant d'interface à la FA inverse.

La signalisation a été améliorée pour porter l'identifiant d'interface d'une FA dans le nouvel objet/TLV Identifiant d'interface de tunnel de LSP. Cet objet/TLV contient l'identifiant de routeur (du LSR qui le génère) et l'identifiant d'interface. Il est appelé l'identifiant d'interface de transmission quand il apparaît dans un message Path/REQUEST, et il est appelé l'identifiant d'interface inverse quand il apparaît dans le message Resv/MAPPING.

4. Mise en faisceau de liaisons

Le concept de faisceau de liaisons est essentiel dans certains réseaux qui emploient le plan de contrôle GMPLS comme défini dans la [RFC4201]. Un exemple typique en est un réseau optique maillé où les interconnexions optiques adjacentes (LSR) sont connectées par plusieurs centaines de longueurs d'ondes parallèles. Dans ce réseau, considérons l'application de protocoles d'acheminement à état de liaison, comme OSPF ou IS-IS, avec les extensions convenables pour la découverte de ressources et le calcul dynamique du chemin. Chaque longueur d'onde doit être annoncée séparément pour être utilisée, sauf si la mise en faisceau de liaison est utilisée.

Lorsque une paire de LSR est connectée par plusieurs liaisons, il est possible d'annoncer plusieurs de ces liaisons (ou toutes) comme une seule liaison dans OSPF et/ou IS-IS. Ce processus est appelé mise en faisceau de liaison, ou juste mise en faisceau *(bundling)*. La liaison logique résultante est appelée un faisceau de liaisons car ses liaisons physiques sont appelées liaisons composantes (et sont identifiées par les indices d'interface).

Le résultat est qu'une combinaison de trois identifiants (en faisceau) identifiant de liaison, identifiant de liaison composante, étiquette) est suffisante pour identifier sans ambiguïté les ressources appropriées utilisées par un LSP.

L'objet de la mise en faisceau de liaison est d'améliorer l'adaptabilité de l'acheminement en réduisant la quantité d'informations qui doivent être traitées par OSPF et/ou IS-IS. Cette réduction est accomplie en effectuant une agrégation/abstraction d'informations. Comme avec toute autre agrégation/abstraction d'informations, il en résulte une perte de certaines informations. Pour limiter la quantité de pertes, on doit restreindre le type des informations qui peuvent être agrégées/abstraites.

4.1 Restrictions à la mise en faisceau

Les restrictions suivantes sont exigées pour la mise en faisceau de liaisons. Toutes les liaisons composantes d'un faisceau doivent commencer et se terminer sur la même paire de LSR; et partager des caractéristiques ou propriétés communes définies dans les [RFC3630] et [RFC3784], c'est-à-dire, elles doivent avoir :
- le même type de liaison (c'est-à-dire, point à point ou multi accès),
- la même métrique TE (c'est-à-dire, un coût administratif),
- le même ensemble de classes de ressources à chaque extrémité des liaisons (c'est-à-dire, les couleurs).

Noter qu'une adjacence de transmission peut aussi être une liaison composante. En fait, un faisceau peut consister en un mélange de liaisons point à point et de FA, mais toutes partageant des propriétés communes.

4.2 Considérations d'acheminement pour la mise en faisceau

Une liaison en faisceau est juste une autre sorte de liaison TE comme celles définies par la [RFC4202]. La vie de la liaison en faisceau est déterminée par la vie de chacune de ses liaisons composantes. Une liaison en faisceau est en vie lorsque au moins une de ses liaisons composantes est en vie. La vivacité d'une liaison composante peut être déterminée par plusieurs moyens : des hellos IS-IS ou OSPF sur la liaison composante, ou un Hello RSVP (bond local), ou des hellos LMP (liaison locale), ou par des indications de couche 1 ou 2.

Noter que (conformément à la spécification RSVP-TE [RFC3209]) le mécanisme Hello RSVP est destiné à être utilisé lorsque la notification des défaillances de couche liaison n'est pas disponible et que des liaisons non numérotées ne sont pas utilisées, ou lorsque les mécanismes de détection de défaillance fournis par la couche de liaison ne sont pas suffisants pour détecter en temps utile la défaillance du nœud.

Une fois qu'il est déterminé qu'une liaison en faisceau est en vie, elle peut être annoncée comme liaison TE et les informations TE peuvent être répandues. Si des hellos IS-IS/OSPF sont lancés sur les liaisons composantes, l'arrosage IS-IS/OSPF peut être restreint à juste une des liaisons composantes.

Noter que l'annonce d'une liaison (en faisceau) TE entre une paire de LSR n'implique pas qu'il y ait une adjacence IGP entre ces LSR qui sont juste associés à cette liaison. En fait, dans certains cas une liaison TE entre une paire de LSR

pourrait être annoncée même si il n'y a pas du tout d'adjacence IGP entre les LSR (par exemple, lorsque la liaison TE est une FA).

Former une liaison en faisceau consiste à agréger les paramètres TE identiques de chaque liaison composante individuelle pour produire des paramètres TE agrégés. Une liaison TE comme défini par la [RFC4202] a de nombreux paramètres ; les règles d'agrégation adéquates doivent être définies pour chacune.

Certains paramètres peuvent être les sommes de caractéristiques composantes telles que bande passante non réservée et bande passante maximum réservable. Les informations de bande passante sont une partie importante de l'annonce de faisceau et elles doivent être clairement définies quand est faite une abstraction.

Un nœud GMPLS avec des liaisons en faisceau doit appliquer le contrôle d'admission liaison composante par liaison composante.

4.3 Considérations de signalisation

Normalement, un chemin explicite d'un LSP (par exemple, contenu dans un objet/TLV Chemin explicite) va choisir la liaison en faisceau à utiliser pour le LSP, mais pas la ou les liaisons composantes. Cela parce que les informations sur la liaison en faisceau sont diffusées mais pas les informations sur les liaisons composantes.

Le choix de la liaison composante à utiliser est toujours fait par le nœud amont. Si le LSP est bidirectionnel, le nœud amont choisit une liaison composante dans chaque direction.

Trois mécanismes sont possibles pour indiquer ce choix au nœud aval.

4.3.1 Mécanisme 1 : Indication implicite

Ce mécanisme exige que chaque liaison composante ait un canal de signalisation dédié (par exemple, la liaison est une liaison Sonet/SDH utilisant le DCC pour la signalisation dans la bande). Le nœud amont dit au receveur quelle liaison composante utiliser en envoyant le message sur le canal de signalisation dédié choisi de la liaison composante. Noter que ce canal de signalisation peut être dans la bande ou hors bande. Dans ce dernier cas, l'association entre le canal de signalisation et cette liaison composante doit être explicitement configuré.

4.3.2 Mécanisme 2 : Indication explicite par identifiant d'interface numérotée

Ce mécanisme exige que la liaison composante ait une adresse IP distante unique. Le nœud amont indique le choix de la liaison composante en incluant un nouveau TLV objet/IF_ID IF_ID RSVP_HOP portant une adresse IPv4 ou IPv6 dans le message de demande de chemin/étiquette (voir respectivement la [RFC3473]/[RFC3472]). Pour un LSP bidirectionnel, une liaison composante est fournie pour chaque direction par le nœud amont.

Ce mécanisme n'exige pas que chaque liaison composante ait son propre canal de contrôle. En fait, il n'exige même pas que toute la liaison (en faisceau) ait son propre canal de contrôle.

4.3.3 Mécanisme 3 : Indication explicite par identifiant d'interface non numérotée

Avec ce mécanisme, chaque liaison composante qui est non numérotée reçoit un identifiant d'interface unique (une valeur de 32 bits). Le nœud amont indique le choix de la liaison composante en incluant un nouveau TLV objet/IF_ID IF_ID RSVP_HOP dans le message de demande de chemin/étiquette (voir respectivement la [RFC3473]/[RFC3472]).

Cet objet/TLV porte l'identifiant d'interface de composante dans la direction aval pour un LSP unidirectionnel, et de plus, l'identifiant d'interface de composante dans la direction amont pour un LSP bidirectionnel.

Les deux LSR à chaque extrémité de la liaison en faisceau échangent ces identifiants. Échanger les identifiants peut être réalisé par configuration, au moyen d'un protocole comme LMP (solution préférée) au moyen de RSVP-TE/CR-LDP (en particulier dans le cas où une liaison composante est une adjacence de transmission) ou au moyen des extensions IS-IS ou OSPF.

Ce mécanisme n'exige pas que chaque liaison composante ait son propre canal de contrôle. En fait, il n'a même pas besoin que la liaison (en faisceau) toute entière ait son propre canal de contrôle.

4.4 Faisceaux de liaisons non numérotées

Une liaison en faisceau peut elle-même être numérotée ou non numérotée indépendamment de si les liaisons composantes sont numérotées ou non. Ceci affecte la façon dont la liaison en faisceau est annoncée dans IS-IS/OSPF et le format des objets de chemin explicites (ERO, *Explicit Route Object*) de LSP qui traversent la liaison en faisceau. De plus, les identifiants d'interfaces non numérotées pour toutes les liaisons sortantes non numérotées d'un certain LSR (que ce soient des liaisons composantes, des adjacences de transmission ou des liaisons en faisceau) doivent être uniques dans le contexte de ce LSR.

4.5 Formation de faisceaux de liaisons

La règle générale pour les liaisons composantes en faisceau est de placer ces liaisons qui sont corrélées d'une certaine manière dans le même faisceau. Si les liaisons peuvent être corrélées sur la base de plusieurs propriétés, alors la mise en faisceau peut être appliquée de façon séquentielle sur la base de ces propriétés. Par exemple, les liaisons peuvent être d'abord groupées sur la base de la première propriété. Chacun de ces groupes peut ensuite être divisé en plus petits groupes sur la base de la seconde propriété et ainsi de suite. Le principe majeur suivi dans ce processus est que les propriétés des faisceaux résultants devraient pouvoir être résumées de façon concise. La mise en faisceau peut être faite automatiquement ou par configuration. La mise en faisceau automatique de liaisons peut appliquer les règles de mise en faisceau à la suite pour produire des faisceaux.

Par exemple, la première propriété sur laquelle les liaisons composantes peuvent être corrélées pourrait être la capacité de commutation d'interface [RFC4202], la seconde propriété pourrait être le codage [RFC4202], la troisième propriété pourrait être le poids administratif (coût), la quatrième propriété pourrait être la classe de ressource et finalement, les liaisons peuvent être corrélées sur la base d'une autre métrique comme les groupes de liaisons à risques partagés (SRLG, *Shared Risk Link Group*).

Lorsque on achemine sur un chemin de remplacement pour des besoins de protection, le principe général suivi est que ce chemin de remplacement n'est pas acheminé sur une liaison appartenant à un SRLG qui relève d'une liaison du chemin principal. Donc, la règle à suivre est de grouper les liaisons appartenant exactement au même ensemble de SRLG.

Ce type de sous division séquentielle peut résulter en un certain nombre de faisceaux entre deux nœuds adjacents. En pratique, cependant, les propriétés de la liaison ne peuvent pas être très hétérogènes entre les liaisons composantes entre deux nœuds adjacents. Donc, le nombre de faisceaux ne peut pas en pratique être très élevé.

5. Relations avec l'UNI

L'interface entre un nœud bordure GMPLS et un LSR GMPLS sur le côté réseau peut être appelée une interface usager réseau (UNI, *User to Network Interface*), tandis que l'interface entre deux LSR côté réseau peut être appelée une interface réseau à réseau (NNI, *Network to Network Interface*).

GMPLS ne spécifie pas séparément une UNI et une NNI. Les nœuds bordures sont connectés aux LSR sur le côté réseau, et ces LSR sont à leur tour connectés entre eux. Bien sûr, le comportement d'un nœud bordure n'est pas exactement le même que celui d'un LSR sur le côté réseau. Noter aussi q'un nœud bordure peut appliquer un protocole d'acheminement, cependant on s'attend dans la plupart des cas qu'il ne le fasse pas (voir aussi au paragraphe 5.2 et la section sur la signalisation avec un chemin explicite).

Conceptuellement, une différence entre UNI et NNI a un sens si les deux interfaces utilisent des protocoles complètement différents, ou si elles utilisent les mêmes protocoles mais avec des différences marquantes. Dans le premier cas, des protocoles séparés sont souvent définis successivement, avec plus ou moins de succès.

L'approche GMPLS consistait à construire un modèle cohérent dès le début, en considérant les deux interfaces UNI et NNI en même temps [RFC4208]. À cette fin, très peu de particularités spécifiques de l'UNI ont été ignorées dès le départ. GMPLS a été amélioré pour prendre en charge de telles particularités de l'UNI spécifiées par d'autres organes de normalisation (voir ci-après).

5.1 Relations avec l'UNI OIF

Ce paragraphe n'est là que pour faire référence au travail sur OIF en relation avec GMPLS. La spécification OIF UNI actuelle [OIF-UNI] définit une interface entre un équipement client SONET/SDH et un réseau SONET/SDH, chacun

appartenant à une autorité administrative distincte. Il est conçu pour un modèle à recouvrement. L'UNI OIF définit des mécanismes supplémentaires par dessus GMPLS pour l'UNI.

Par exemple, la procédure de découverte de service OIF est un précurseur pour obtenir des services d'UNI. La découverte de service permet à un client de déterminer les paramètres statiques de l'interconnexion avec le réseau, incluant le protocole de signalisation d'UNI, le type d'enchaînement, le niveau de transparence ainsi que le type de diversité (nœud, liaison, SRLG) pris en charge par le réseau.

Comme l'interface OIF UNI actuelle ne couvre pas les réseaux photoniques, l'enveloppe numérique G.709, etc., c'est dans cette perspective un sous ensemble de l'architecture GMPLS à l'UNI.

5.2 Accessibilité à travers l'UNI

Ce paragraphe expose le choix d'un chemin explicite par un nœud bordure. Le choix du premier LSR par un nœud bordure connecté à plusieurs LSR fait partie de ce problème.

Un nœud bordure (hôte ou LSR) peut participer plus ou moins profondément à l'acheminement GMPLS. Quatre différents modèles d'acheminement peuvent être pris en charge à l'UNI : fondé sur la configuration, homologue à homologue partiel, écoute silencieuse et homologue à homologue complet.

- Fondé sur la configuration : ce modèle d'acheminement exige une configuration manuelle ou automatique du nœud bordure avec une liste de LSR voisins triés par ordre de préférence. La configuration automatique peut être réalisée en utilisant DHCP par exemple. Aucune information d'acheminement n'est échangée à l'UNI, excepté peut-être la liste ordonnée des LSR. Les seules informations d'acheminement utilisées par le nœud bordure sont cette liste. Le nœud bordure envoie par défaut une demande de LSP au LSR préféré. Les redirections ICMP pourraient être envoyées par ce LSR pour rediriger certaines demandes de LSP à un autre LSR connecté au nœud bordure. GMPLS n'empêche pas ce modèle.

- Homologue à homologue partiel : des informations d'acheminement limitées (principalement d'accessibilité) peuvent être échangées à travers l'UNI en utilisant certaines extensions dans le plan de signalisation. Les informations d'accessibilité échangées à l'UNI peuvent être utilisées pour initier des décisions spécifiques du nœud bordure sur le réseau. GMPLS n'a aujourd'hui aucune capacité de prendre en charge ce modèle.

- Écoute silencieuse : le nœud bordure peut écouter en silence les protocoles d'acheminement et prendre des décisions d'acheminement sur la base des informations obtenues. Un nœud bordure reçoit les informations d'acheminement complètes, incluant les extensions d'ingénierie du trafic. Un LSR devrait transmettre de façon transparente toutes les PDU d'acheminement au nœud bordure. Un nœud bordure peut alors calculer un chemin explicite complet en prenant en considération toutes les informations d'acheminement de bout en bout. GMPLS n'empêche pas ce modèle.

- Homologue à homologue complet : en plus de l'écoute silencieuse, le nœud bordure participe à l'acheminement, établit des adjacences avec ses voisins et annonce les LSA. Ceci n'est utile que si il y a un avantage pour les nœuds bordures de s'annoncer les informations d'ingénierie du trafic. GMPLS n'interdit pas ce modèle.

6. Gestion de liaison

Dans le contexte de GMPLS, une paire de nœuds (par exemple, un commutateur photonique) peut être connectée par des dizaines de fibres, et chaque fibre peut être utilisée pour transmettre des centaines de longueurs d'onde si DWDM est utilisé. Plusieurs fibres et/ou plusieurs longueurs d'onde peuvent aussi être combinées en un ou plusieurs faisceaux de liaisons pour des besoins d'acheminement. De plus, pour permettre la communication entre les nœuds pour l'acheminement, la signalisation, et la gestion de la liaison, des canaux de contrôle doivent être établis entre une paire de nœuds.

La gestion de liaison est une collection de procédures utiles entre des nœuds adjacents qui fournissent des services locaux comme la gestion des canaux de contrôle, la vérification de la connectivité des liaisons, la corrélation des propriétés de la liaison, et la gestion des fautes. Le protocole de gestion de liaison (LMP, *Link Management Protocol*) [RFC4204] a été défini pour assurer ces opérations. LMP a été initié dans le contexte de GMPLS mais est une boîte à outils générique qui peut aussi être utilisée dans d'autres contextes.

Dans GMPLS, les canaux de contrôle entre deux nœuds adjacents ne sont plus obligés d'utiliser le même support physique que les liaisons de données entre ces nœuds. De plus, les canaux de contrôle qui sont utilisés pour échanger les

informations de plan de contrôle GMPLS existent indépendamment des liaisons qu'elles gèrent. Donc, LMP a été conçu pour gérer les liaisons de données, indépendamment des capacités de terminaison de ces liaisons de données.

Les procédures de gestion des canaux de contrôle et de corrélation des propriétés de liaison sont obligatoires selon LMP. Les procédures de vérification de connectivité et de gestion des fautes sont facultatives.

6.1 Canal de contrôle et gestion de canal de contrôle

La gestion des canaux de contrôle LMP est utilisée pour établir et entretenir des canaux de contrôle entre nœuds. Les canaux de contrôle existent indépendamment des liaisons TE, et peuvent être utilisés pour échanger des informations de plan de contrôle MPLS telles que de signalisation, d'acheminement, et de gestion de liaison.

Une "adjacence LMP" est formée entre deux nœuds qui prennent en charge les mêmes capacités LMP. Plusieurs des canaux de contrôle peuvent être actifs simultanément pour chaque adjacence. Un canal de contrôle peut être soit explicitement configuré, soit automatiquement choisi, cependant, LMP suppose actuellement que les canaux de contrôle sont explicitement configurés alors que la configuration des capacités du canal de contrôle peut être négociée dynamiquement.

Pour les besoins de LMP, la mise en œuvre exacte du canal de contrôle est laissée inspécifiée. Le ou les canaux de contrôle entre deux nœuds adjacents ne sont plus obligés d'utiliser le même support physique que les liaisons qui portent les données entre ces nœuds. Par exemple, un canal de contrôle pourrait utiliser une longueur d'onde ou fibre séparée, une liaison Ethernet, ou un tunnel IP à travers un réseau de gestion séparé.

Permettre que le ou les canaux de contrôle entre deux nœuds soient physiquement différents des liaisons associées qui portent les données a pour conséquence que la santé d'un canal de contrôle n'est pas nécessairement corrélée à la santé des liaisons porteuses de données, et vice-versa. Donc, de nouveaux mécanismes ont été développés dans LMP pour gérer les liaisons, à la fois en termes de provisionnement de liaison et en termes d'isolement de faute.

LMP ne spécifie pas le mécanisme de transport de signalisation utilisé dans le canal de contrôle, cependant il déclare que les messages transportés sur un canal de contrôle doivent être codés en IP. De plus, comme les messages sont codés en IP, le codage de niveau liaison ne fait pas partie de LMP. Un identifiant de canal de contrôle (CCId, *Control Channel Identifier*) entier de 32 bits non à zéro est alloué à chaque direction d'un canal de contrôle.

Chaque canal de contrôle négocie individuellement ses paramètres de canal de contrôle et entretient la connexité en utilisant un protocole de Hello rapide. Ce dernier est requis si des mécanismes de niveau inférieur ne sont pas disponibles pour détecter les défaillances de liaison.

Le protocole Hello de LMP est destiné à être un mécanisme léger de garde en vie qui va réagir rapidement aux défaillances du canal de contrôle afin que les Hello IGP ne soient pas perdus et que les adjacences d'état de liaison associées ne soient pas supprimées sans nécessité.

Le protocole Hello comporte deux phases : une phase de négociation et une phase de garde en vie. La phase de négociation permet la négociation de certains paramètres de base du protocole Hello, comme la fréquence de Hello. La phase de garde en vie consiste en un échange rapide de messages Hello bidirectionnels légers.

Si un groupe de canaux de contrôle partage une paire de nœuds commune et prend en charge les mêmes capacités de LMP, les messages de canal de contrôle LMP (sauf les messages Configuration, et les Hello) peuvent alors être transmis sur tout canal de contrôle actif sans coordination entre nœud local et distant.

Pour LMP, il est essentiel qu'au moins un canal de contrôle soit toujours disponible. En cas de défaillance du canal de contrôle, il est possible d'utiliser un canal de contrôle actif de remplacement sans coordination.

6.2 Corrélation de propriété de liaison

Au titre de LMP est défini un échange de corrélation de propriétés de liaison. L'échange est utilisé pour agréger plusieurs liaisons porteuses de données (c'est-à-dire, des liaisons composantes) en une liaison en faisceau et pour échanger, corréler, ou changer les paramètres de liaison TE. L'échange de corrélation de propriétés de liaison peut être fait à tout moment quand une liaison est active et pas dans le processus de vérification (voir le paragraphe suivant).

Il permet, par exemple, l'ajout de liaisons composantes à un faisceau de liaisons, de changer la bande passante minimum/maximum réservable d'une liaison, de changer les identifiants d'accès, ou de changer les identifiants d'une composante d'un faisceau. Ce mécanisme est pris en charge par un échange de messages de résumé de liaison.

6.3 Vérification de la connexité de liaison

La vérification de la connexité de liaison est une procédure facultative qui peut être utilisée pour vérifier la connexité physique des liaisons porteuses de données ainsi que pour échanger les identifiants de liaison qui sont utilisés dans la signalisation GMPLS.

Cette procédure devrait être effectuée initialement lors du premier établissement d'une liaison porteuse de données, et ensuite, sur une base périodique pour toutes les liaisons porteuses de données non allouées (libres).

La procédure de vérification consiste à envoyer des messages Test dans la bande sur les liaisons porteuses de données. Cela exige que les liaisons non allouées soient opaques ; cependant, plusieurs degrés d'opacité (par exemple, examiner les octets de surdébit, qui terminent la charge utile, etc.) et donc différents mécanismes pour transporter les messages Test, sont spécifiés. Noter que le message Test est le seul message LMP qui soit transmis sur la liaison porteuse de données, et que les messages Hello continuent d'être échangés sur le canal de contrôle durant la processus de vérification de la liaison. Les liaisons porteuses de données sont vérifiées dans la direction d'émission car elles sont unidirectionnelles. À ce titre, il est possible pour les nœuds LMP du voisinage d'échanger les messages Test simultanément dans les deux directions.

Pour initier la procédure de vérification de liaison, un nœud doit d'abord notifier au nœud adjacent qu'il va commencer à envoyer des messages Test sur une certaine liaison porteuse de données, ou sur les liaisons composantes d'une certaine liaison en faisceau. Le nœud doit aussi indiquer le nombre de liaisons porteuses de données qui sont à vérifier, l'intervalle auquel les messages Test seront envoyés, le schéma de codage, les mécanismes de transport qui sont acceptés, le débit de données pour les messages Test ; et, dans le cas où les liaisons porteuses de données correspondent à des fibres, la longueur d'onde sur laquelle les messages Test seront transmis. De plus, les identifiants locaux et distants de la liaison en faisceau sont transmis à ce moment pour effectuer l'association de la liaison composante avec les identifiants de la liaison en faisceau.

6.4 Gestion des fautes

La gestion des fautes est une exigence importante du point de vue du fonctionnement. La gestion des fautes inclut généralement la détection, la localisation et la notification des fautes. Lorsque survient une défaillance et qu'elle est détectée (détection) un opérateur a besoin de savoir exactement où elle se produit (localisation) et un nœud source peut avoir besoin d'une notification afin d'entreprendre certaines actions (notification).

Noter que la localisation de faute peut aussi être utilisée pour prendre en charge certains mécanismes spécifiques (locaux) de protection/restauration.

Dans les nouvelles technologies comme la commutation photonique transparente, aucune méthode n'est actuellement définie pour localiser une faute, et le mécanisme par lequel les informations de faute sont propagées doit être envoyé "hors bande" (via le plan de contrôle).

LMP fournit une procédure de localisation de faute qui peut être utilisée pour localiser rapidement les défaillances de liaison, en notifiant une faute au nœud amont de cette faute (c'est-à-dire, par une procédure de notification de faute).

Un voisin LMP vers l'aval qui détecte une défaillances de liaison de données va envoyer un message LMP à son voisin amont pour lui notifier la défaillance. Lorsque un nœud amont reçoit une notification de défaillance, il peut corréler la défaillance avec les accès d'entrée correspondants pour déterminer si la défaillance est entre les deux nœuds. Une fois la défaillance localisée, le protocole de signalisation peut être utilisé pour initier les procédures de protection/restauration de liaison ou chemin.

6.5 LMP pour systèmes de ligne optique DWDM

Dans un environnement tout optique, LMP se focalise sur les communications d'homologue à homologue (par exemple, OXC à OXC). Une grande quantité d'informations sur une liaison entre deux OXC est connue par le système de ligne optique (OLS, *Optical Line System*) ou le multiplexeur de terminal WDM. Exposer ces informations au plan de contrôle peut améliorer l'utilisation du réseau en réduisant la configuration manuelle requise, et en améliorant grandement la détection et la récupération de faute.

LMP-WDM [RFC4209] définit les extensions à LMP pour l'utilisation entre un OXC et un OLS. Ces extensions sont destinées à satisfaire les exigences d'interface de liaison optique décrites dans la [RFC4258].

La détection de faute est particulièrement un problème lorsque le réseau utilise des brasseurs photoniques tout optique (PXC, *photonic cross-connect)*). Une fois qu'une connexion est établie, les PXC ont seulement une visibilité limitée de la santé de la connexion. Bien que le PXC soit tout optique, les OLS à longue portée terminent normalement des canaux par des moyens électriques et les régénèrent par des moyens optiques. Cela donne une opportunité de surveiller la santé d'un canal entre des PXC. LMP-WDM peut alors être utilisé par l'OLS pour fournir ces informations au PXC.

En plus des informations de liaison connues de l'OLS qui sont échangées par LMP-WDM, des informations connues de l'OXC peuvent aussi être échangées avec l'OLS par LMP-WDM. Ces informations sont utiles pour alerter le système de gestion et la surveillance de liaison (par exemple, la surveillance de trace). La gestion d'alerte est importante parce que l'état administratif d'une connexion, connue de l'OXC (par exemple, ces informations peuvent être apprises de l'objet AdminStatus de la signalisation GMPLS [RFC3471]), peut être utilisé pour supprimer les alarmes parasites. Par exemple, l'OXC peut savoir qu'une connexion est "active", "morte", dans un mode "essai", ou en cours de suppression ("suppression-en-cours"). L'OXC peut utiliser ces informations pour inhiber le rapport d'alarme provenant de l'OLS lorsque une connexion est "morte", "en essai", ou en cours de suppression.

Il est important de noter qu'un OXC peut échanger avec un ou plusieurs OLS et un OLS peut échanger avec un ou plusieurs OXC. Bien qu'il y aient de nombreuses similarités entre une session LMP d'OXC-OXC et une session LMP OXC-OLS, en particulier pour la gestion de contrôle et la vérification de liaison, il y a aussi quelques différences. Ces différences peuvent principalement être attribuées à la nature d'une liaison OXC-OLS, et à l'objet des sessions LMP OXC-OLS. Les liaisons OXC-OXC peuvent être utilisées pour donner une base pour la signalisation GMPLS et l'acheminement à la couche optique. Les informations échangées sur les sessions LMP-WDM sont utilisées pour augmenter les connaissances sur les liaisons entre les OXC.

Afin que les informations échangées sur les sessions LMP OXC-OLS soient utilisées par la session OXC-OXC, les informations doivent être coordonnées par l'OXC. Cependant, les sessions LMP OXC-OXC et les sessions LMP OXC-OLS fonctionnent indépendamment et doivent être entretenues séparément. Une exigence critique du fonctionnement d'une session LMP OXC-OLS est la capacité de l'OLS à rendre une liaison de données transparente lorsque elle ne fait pas la procédure de vérification. Cela parce que la même liaison de données peut être vérifiée entre OXC-OLS et entre OXC-OXC. La procédure de vérification de LMP est utilisée pour coordonner la procédure d'essai (et donc la transparence/opacité des liaisons de données). Pour maintenir l'indépendance entre les sessions, il doit être possible pour les sessions LMP de s'activer dans n'importe quel ordre. En particulier, il doit être possible pour une session LMP OXC-OXC de s'activer sans qu'une session LMP OXC-OLS soit activée, et vice-versa.

7. Signalisation généralisée

La signalisation GMPLS étend certaines fonctions de base de la signalisation RSVP-TE et CR-LDP et, dans certains cas, ajoute des fonctionnalités. Ces changements et ajouts ont un impact sur les propriétés de base de LSP : comment les étiquettes sont demandées et communiquées, la nature unidirectionnelle des LSP, comment les erreurs sont propagées, et les informations fournies pour synchroniser l'entrée et la sortie.

Le cœur de la spécification de la signalisation GMPLS est disponible en trois parties :
1. Une description fonctionnelle de la signalisation [RFC3471].
2. les extensions RSVP-TE [RFC3473].
3. les extensions CR-LDP [RFC3472].

De plus, des parties indépendantes sont disponibles par technologie :
1. Extensions GMPLS pour les commandes SONET et SDH [RFC3946].
2. Extensions GMPLS pour les commandes G.709 [RFC4328].

Le profil MPLS suivant exprimé en termes de caractéristiques MPLS [RFC3031] s'applique à GMPLS :
- Allocation et distribution d'étiquette vers l'aval à la demande.
- Contrôle ordonné à l'initiative de l'entrée.
- Mode de rétention d'étiquette libéral (normal) ou prudent (facultatif).
- Stratégie d'allocation d'étiquette piloté par la demande, le trafic/données, ou la topologie.
- Acheminement explicite (normal), ou acheminement bond par bond.

La signalisation GMPLS définit les nouveaux blocs de construction suivants par dessus MPLS-TE :
1. Un nouveau format générique de demande d'étiquette.

2. Des étiquettes pour les interfaces TDM, LSC et FSC, appelées de façon générique "étiquettes généralisées.
3. La prise en charge de la commutation de longueur d'onde.
4. La suggestion d'étiquette par l'amont pour les besoins d'optimisation (par exemple, la latence).
5. La restriction d'étiquette par l'amont pour prendre en charge de contraintes optiques.
6. L'établissement de LSP bidirectionnel avec résolution de conflit.
7. Des extensions de notification rapide de défaillance.
8. Des informations de protection actuellement focalisées sur la protection de la liaison, plus l'indication du LSP principal et secondaire.
9. Acheminement explicite avec contrôle d'étiquette explicite pour un degré de contrôle fin.
10. Des paramètres de trafic spécifiques par technologie.
11. Traitement du statut administratif du LSP.
12. Séparation du canal de contrôle.

Ces blocs de construction seront décrits plus en détails plus loin. Une spécification complète se trouve dans les documents correspondants.

Noter que GMPLS est très générique et a de nombreuses options. Seuls les blocs 1, 2 et 10 sont obligatoires, et seulement dans le format spécifique qui est nécessaire. Normalement, les blocs 6 et 9 devraient être mis en œuvre. Les blocs 3, 4, 5, 7, 8, 11 et 12 sont facultatifs.

Un réseau typique à commutation SONET/SDH mettrait en œuvre les blocs de construction 1, 2 (l'étiquette SONET/SDH) 6, 9, 10 et 11. Les blocs 7 et 8 sont facultatifs car la protection peut être réalisée en utilisant les octets supplémentaires SONET/SDH.

Un réseau typique à commutation de longueur d'onde mettrait en œuvre les blocs de construction 1, 2 (le format générique) 4, 5, 6, 7, 8, 9 et 11. Le bloc 3 n'est nécessaire que dans le cas particulier de commutation de longueur d'onde.

Un réseau typique de commutation sur fibre mettrait en œuvre les blocs de construction 1, 2 (le format générique) 6, 7, 8, 9 et 11.

Un réseau MPLS-IP typique ne mettrait en œuvre aucun de ces blocs, car l'absence du bloc 1 indiquerait un MPLS-IP régulier. Noter cependant que les blocs de construction 1 et 8 peuvent être utilisés aussi pour signaler MPLS-IP. Dans ce cas, le réseau MPLS-IP peut bénéficier du type de protection de la liaison (non disponible en CR-LDP, une forme très basique étant disponible dans RSVP-TE). Le bloc 2 est ici une étiquette MPLS régulière et aucun nouveau format n'est nécessaire.

GMPLS ne spécifie aucun profil pour les mises en œuvre de RSVP-TE et CR-LDP qui ont à prendre en charge GMPLS - sauf pour ce qui est directement en rapport avec les procédures GMPLS. Il appartient au fabricant de décider quels sont les éléments et procédures facultatifs de RSVP-TE et CR-LDP qui ont besoin d'être mis en œuvre. Certains éléments MPLS-TE facultatifs peuvent être utiles pour les couches TDM, LSC et FSC, par exemple les priorités d'établissement et de garde qui sont héritées de MPLS-TE.

7.1 Généralités : comment demander un LSP

Un LSP TDM, LSC ou FSC est établi en envoyant un message Demande d'étiquette/chemin vers l'aval à la destination. Ce message contient une demande d'étiquette généralisée avec le type de LSP (c'est-à-dire, la couche concernée) et son type de charge utile. Un objet de chemin explicite (ERO, *Explicit Route Object*) est aussi normalement ajouté au message, mais ceci peut être ajouté et/ou complété par le premier LSR ou celui par défaut.

La bande passante demandée est codée dans l'objet RSVP-TE SENDER_TSPEC, ou dans le TLV Paramètres de trafic CR-LDP. Des paramètres spécifiques pour une certaine technologie sont donnés dans ces paramètres de trafic, comme le type de signal, l'enchaînement et/ou la transparence pour un LSP SONET/SDH. Pour certaines autres technologies, il pourrait y avoir juste un paramètre de bande passante indiquant la bande passante comme une valeur à virgule flottante.

La protection locale demandée par liaison peut être demandée en utilisant l'objet/TLV Information de protection. La protection LSP de bout en bout fera l'objet d'études ultérieures et est introduite dans la section protection/restauration de LSP (voir plus loin).

Si le LSP est bidirectionnel, une étiquette amont est aussi spécifiée dans le message Demande de chemin/étiquette. Cette étiquette sera celle à utiliser dans la direction amont.

De plus, une étiquette suggérée, une étiquette établie et une étiquette de longueur d'onde peuvent aussi être incluses dans le message. Les autres opérations sont définies dans MPLS-TE.

Le nœud aval va renvoyer un message Transposition de réservation/étiquette incluant un objet/TLV étiquette généralisée qui peut contenir plusieurs étiquettes généralisées. Par exemple, si un signal SONET/SDH enchaîné est demandé, plusieurs étiquettes peuvent être retournées.

En cas d'enchaînement virtuel SONET/SDH, une liste d'étiquettes est retournée. Chaque étiquette identifiant un élément du signal virtuel enchaîné. Ceci limite l'enchaînement virtuel à rester au sein d'une seule liaison (composante).

En cas de tout type d'enchaînement SONET/SDH contigu, une seule étiquette est retournée. Cette étiquette est le plus faible signal du signal enchaîné contigu (selon un ordre spécifié dans la [RFC3946]).

En cas de "multiplication" SONET/SDH, c'est-à-dire, de co-acheminement de circuits du même type mais sans enchaînement et tous appartenant au même LSP, la liste explicitement ordonnée de tous les signaux qui prennent part au LSP est retournée.

7.2 Demande d'étiquette généralisée

La demande d'étiquette généralisée est un nouvel objet/TLV à ajouter dans un message Chemin RSVP-TE au lieu de la demande d'étiquette régulière, ou dans un message Demande CR-LDP en plus des TLV déjà existants. Une seule demande d'étiquette peut être utilisée par message, de sorte qu'un seul LSP peut être demandé à un instant donné par message de signalisation.

La demande d'étiquette généralisée donne trois caractéristiques majeures (paramètres) requises pour la prise en charge du LSP demandé : le type de codage de LSP, le type de commutation qui doit être utilisée et le type de charge utile de LSP appelé PID généralisé (G-PID).

Le type de codage de LSP indique le type de codage qui sera utilisé avec les données associées au LSP, c'est-à-dire, le type de technologie considérée. Par exemple, il peut être SDH, SONET, Ethernet, ANSI PDH, etc. Il représente la nature du LSP, et non la nature des liaisons que le LSP traverse. Ceci est utilisé bond par bond par chaque nœud.

Une liaison peut prendre en charge un ensemble de formats de codage, où prendre en charge signifie qu'une liaison est capable de porter et commuter un signal de un ou plusieurs de ces formats de codage. Le type de commutation indique ensuite le type de commutation qui devrait être effectuée sur une certaine liaison pour ce LSP. Ces informations sont nécessaires pour les liaisons qui annoncent plus d'un type de capacité de commutation.

Les nœuds doivent vérifier que le type indiqué dans le type de commutation est pris en charge sur l'interface entrante correspondante ; autrement, le nœud doit générer un message de notification avec une indication de "problème d'acheminement/type de commutation".

Le type de charge utile de LSP (G-PID) identifie la charge utile portée par le LSP, c'est-à-dire, un identifiant de la couche client de ce LSP. Pour certaines technologies, il indique aussi la transposition utilisée par la couche client, par exemple, la transposition d'octet synchrone de E1. Ceci doit être interprété conformément au type de codage de LSP et est utilisé par les nœuds aux points d'extrémité du LSP pour savoir à quelle couche client une demande est destinée, et dans certains cas par le pénultièmes bond.

Les autres paramètres spécifiques de technologies ne sont pas transportés dans la demande d'étiquette généralisée mais dans les paramètres de trafic spécifiques de la technologie comme expliqué ci-après. Actuellement, deux ensembles de paramètres de trafic sont définis, un pour SONET/SDH et un pour G.709.

Noter qu'on s'attend à ce que des paramètres de trafic spécifiques soient définis à l'avenir pour la commutation photonique (toute optique).

7.3 Paramètres de trafic SONET/SDH

Les paramètres de trafic GMPLS SONET/SDH [RFC3946] spécifient un ensemble de capacités puissantes pour SONET [ANSI-T1.105] et SDH [ITUT-G.707].

Le premier paramètre de trafic spécifie le type de signal SONET/SDH élémentaire que comporte le LSP demandé, par exemple, VC-11, VT6, VC-4, STS-3c, etc. Plusieurs transformations peuvent alors être appliquées successivement sur le signal élémentaire pour construire le signal final demandé réellement pour le LSP.

Ces transformations sont l'enchaînement contigu, l'enchaînement virtuel, la transparence et la multiplication. Chacune est facultative. Elles doivent être appliquées strictement dans l'ordre suivant :

- En premier, l'enchaînement contigu peut être facultativement appliqué au signal élémentaire, résultant en un signal à enchaînement contigu.

- En second, l'enchaînement virtuel peut être facultativement appliqué soit directement sur le signal élémentaire, soit sur le signal à enchaînement contigu obtenu de la phase précédente.

- En troisième, une certaine transparence peut être facultativement spécifiée lors de la demande d'une trame comme signal plutôt que comme contenant. Plusieurs paquetages de transparence sont définis.

- Quatrièmement, une multiplication peut être facultativement appliquée soit directement sur le signal élémentaire, soit sur le signal à enchaînement contigu obtenu de la première phase, soit du signal à enchaînement virtuel obtenu de la seconde phase, soit de ces signaux combinés avec une certaine transparence.

Pour RSVP-TE, les paramètres de trafic SONET/SDH sont portés dans une nouvelle SENDER_TSPEC et FLOWSPEC. Le même format est utilisé pour les deux. Il n'y a pas d'Adspec associée à la SENDER_TSPEC, elle est omise ou on utilise une valeur par défaut. Le contenu de l'objet FLOWSPEC reçu dans un message Resv devrait être identique au contenu de la SENDER_TSPEC du message Chemin correspondant. En d'autres termes, il n'est pas permis au receveur de changer les valeurs des paramètres de trafic. Cependant, un certain niveau de négociation peut être réalisé comme expliqué dans la [RFC3946].

Pour CR-LDP, les paramètres de trafic SONET/SDH sont simplement portés dans un nouveau TLV.

Noter qu'on peut trouver un exposé général sur SONET/SDH et GMPLS dans la [RFC4257].

7.4 Paramètres de trafic G.709

Dit simplement, un réseau fondé sur [ITUT-G.709] se décompose en deux couches majeures : une couche optique (c'est-à-dire, faite de longueurs d'onde) et une couche numérique. Ces deux couches sont divisées en sous couches et la commutation se fait dans deux sous couches spécifiques : à la couche optique OCh (Optical Channel) et à la couche électrique d'unités de données du canal optique ODU (Optical channel Data Unit). La notation ODUk est utilisée pour noter les ODU aux différentes bandes passantes.

Les paramètres de trafic GMPLS G.709 [RFC4328] spécifient un ensemble de capacités puissantes pour les réseaux UIT-T G.709.

Le premier paramètre de trafic spécifie le type du signal élémentaire G.709 qui comporte le LSP demandé, par exemple, ODU1, OCh à 40 Gbit/s, etc. Plusieurs transformations peuvent alors être appliquées successivement au signal élémentaire pour construire le signal final réellement demandé pour le LSP.

Les transformations sont l'enchaînement virtuel et la multiplication. Chacune de ces transformations est facultative. Elles doivent être appliquées strictement dans l'ordre suivant :
- D'abord, l'enchaînement virtuel peut être facultativement appliqué directement au signal élémentaire,
- Ensuite, une multiplication peut être facultativement appliquée, soit directement sur le signal élémentaire, soit sur le signal à enchaînement virtuel obtenu de la première phase.

Des paramètres de trafic de multiplexage d'ODUk supplémentaires permettent d'indiquer une transposition d'ODUk (ODUj dans ODUk) pour une demande de LSP de multiplexage d'ODUk. G.709 prend en charge les capacités de multiplexage suivantes : ODUj dans ODUk (k > j) et ODU1 avec multiplexage ODU2 dans ODU3.

Pour RSVP-TE, les paramètres de trafic G.709 sont portés dans de nouvelles SENDER-TSPEC et FLOWSPEC. Le même format est utilisé pour les deux. Il n'y a pas d'Adspec associée à la SENDER_TSPEC, elle est omise ou une valeur par défaut est utilisée. Le contenu de l'objet FLOWSPEC reçu dans un message Resv devrait être identique au contenu de la SENDER_TSPEC du message Chemin correspondant.

Pour CR-LDP, les paramètres de trafic G.709 sont simplement portés dans un nouveau TLV.

7.5 Codage de bande passante

Certaines technologies qui n'ont pas (encore) de paramètres de trafic spécifiques exigent juste un codage de bande passante transporté sous une forme générique. La largeur de bande est portée dans un chiffre de 32 bits en format IEEE à virgule flottante (l'unité est l'octet/s). Les valeurs sont portées d'une manière spécifique du protocole. Pour les LSP qui ne sont pas par paquet, il est utile de définir des valeurs discrètes pour identifier la bande passante du LSP.

On devrait noter que ce codage de bande passante ne s'applique pas à SONET/SDH et G.709, pour lesquels les paramètres de trafic définissent pleinement le signal SONET/SDH ou G.709 demandé.

La bande passante est codée dans le champ Débit de crête de données *(Peak Data Rate)* des objets Int-Serv pour RSVP-TE dans les objets SENDER_TSPEC et FLOWSPEC et dans les champs Débit de crête de données et Débit de données obligé du TLV Paramètres de trafic de CR-LDP.

7.6 Étiquette généralisée

L'étiquette généralisée étend l'étiquette MPLS traditionnelle en permettant la représentation non seulement des étiquettes qui voyagent dans la bande avec les paquets de données associés, mais aussi des étiquettes (virtuelles) qui identifient des intervalles de temps, des longueurs d'onde, ou des positions multiplexées de division d'espace.

Par exemple, l'étiquette généralisée peut identifier (a) une seule fibre dans un faisceau, (b) une seule bande d'onde dans une fibre, (c) une seule longueur d'onde au sein d'une bande d'onde (ou fibre), ou (d) un ensemble d'intervalles de temps au sein d'une longueur d'onde (ou fibre). Ce peut aussi être une étiquette générique MPLS, une étiquette de relais de trame, ou une étiquette ATM (VCI/VPI). Le format d'une étiquette peut être aussi simple qu'une valeur d'entier comme une étiquette de longueur d'onde ou peut être plus élaborée comme une étiquette SONET/SDH ou G.709.

SDH et SONET définissent chacun une structure de multiplexage. Ces structures de multiplexage seront utilisées comme des arborescences de dénomination pour créer des étiquettes uniques. Une telle étiquette identifiera la position exacte (intervalle de temps) d'un signal dans une structure de multiplexage. Comme la structure de multiplexage SONET peut être vue comme un sous ensemble de la structure de multiplexage SDH, le même format d'étiquette est utilisé pour SDH et SONET. Un concept similaire est appliqué pour construire une étiquette à la couche ODU G.709.

Comme les nœuds qui envoient et reçoivent l'étiquette généralisée savent quelle sorte de liaison ils utilisent, l'étiquette généralisée n'identifie pas son type. À la place, les nœuds sont supposés savoir d'après le contexte quel type d'étiquette attendre.

Une étiquette généralisée porte seulement un seul niveau d'étiquette c'est-à-dire, il n'est pas hiérarchique. Lorsque plusieurs niveaux d'étiquettes (des LSP au sein de LSP) sont exigés, chaque LSP doit être établi séparément.

7.7 Commutation de gamme d'ondes

Un cas particulier de commutation de longueur d'onde est la commutation de bande d'onde. Une bande d'onde représente un ensemble de longueurs d'onde contiguës, qui peuvent être commutées en une nouvelle bande d'ondes. Pour des raisons d'optimisation, il peut être souhaitable pour un brasseur photonique de commuter optiquement plusieurs longueurs d'onde comme une unité. Cela peut réduire la distorsion sur les longueurs d'onde individuelles et peut permettre une séparation plus serrée des longueurs d'onde individuelles. une étiquette de bande d'onde est définie comme prenant en charge ce cas particulier.

La commutation de bande d'onde introduit naturellement un autre niveau de hiérarchie d'étiquettes et à ce titre la bande d'onde est traitée de la même façon que toutes les autres étiquettes de couche supérieure sont traitées. Pour autant que les protocoles MPLS soient concernés, il y a peu de différences entre une étiquette de bande d'onde et une étiquette de longueur d'onde. L'exception est que sémantiquement, la bande d'onde peut être subdivisée en longueurs d'onde tandis que la longueur d'onde peut seulement être subdivisée en étiquettes multiplexées en temps, ou statistiquement.

Dans le contexte de la commutation de bande d'onde, l'étiquette généralisée utilisée pour indiquer une bande d'ondes contient trois champs, un identifiant de bande d'ondes, une étiquette de début et une étiquette de fin. Les étiquettes de début et de fin sont du point de vue de l'envoyeur des identifiants de canal qui identifient respectivement, la plus faible valeur de longueur d'onde et la plus forte valeur de longueur d'onde qui constituent la bande d'ondes.

7.8 Suggestion d'étiquette par l'amont

GMPLS permet qu'une étiquette soit facultativement suggérée par un nœud amont. Cette suggestion peut être outrepassée par un nœud aval mais dans certains cas, au prix du coût d'un temps d'établissement de LSP plus élevé. L'étiquette suggérée est valable quand on établi des LSP à travers certaines sortes d'équipements optiques où il y a peut-être un délai plus long (en termes électriques) pour la configuration de la fabrique de commutation. Par exemple, des micro miroirs peuvent devoir être élevés ou déplacés, et ce mouvement physique et l'amortissement subséquent prennent du temps. Si les étiquettes et donc la fabrique de commutation sont configurées dans la direction inverse (la norme), le message Resv/MAPPING peut devoir être différé de dixièmes de millisecondes par bond afin d'établir un chemin de transmission utilisable. Cela peut être important pour des besoins de restauration lorsque les LSP de remplacement peuvent avoir besoin d'être établis rapidement par suite d'une défaillance du réseau.

7.9 Restriction d'étiquette par l'amont

Un nœud amont peut facultativement restreindre (limiter) le choix d'étiquette d'un nœud aval à un ensemble d'étiquettes acceptables. Donner des listes et/ou des gammes d'étiquettes inclusives (acceptables) ou exclusives (inacceptables) dans un ensemble d'étiquettes assure cette restriction. Si elle n'est pas appliquée, toutes les étiquettes de la gamme d'étiquettes valides peuvent être utilisées. Il y a au moins quatre cas où une restriction d'étiquette est utile dans le domaine "optique".

Cas 1 : l'équipement terminal est seulement capable de transmettre et recevoir sur un petit ensemble spécifique de longueurs d'onde/bandes d'ondes.

Cas 2 : il y a une séquence d'interfaces qui ne peuvent pas prendre en charge la conversion de longueurs d'ondes et exige que les mêmes longueurs d'ondes soient utilisées de bout en bout sur une séquence de bonds, ou même un chemin entier.

Cas 3 : il est souhaitable de limiter la quantité de conversion de longueurs d'ondes à effectuer pour réduire la distorsion sur les signaux optiques.

Cas 4 : les deux extrémités d'une liaison supportent des ensembles différents de longueurs d'onde.

Le receveur d'un ensemble d'étiquettes doit restreindre son choix d'étiquettes à une de celles de l'ensemble d'étiquettes. Un ensemble d'étiquettes peut être présent à travers plusieurs bonds. Dans ce cas, chaque nœud génère son propre ensemble d'étiquettes sortant, éventuellement sur la base de l'ensemble d'étiquette entrant et les capacités du matériel du nœud. Ce cas est supposé être la norme pour les nœuds avec des interfaces incapables de conversion.

7.10 LSP bidirectionnel

GMPLS permet l'établissement de LSP bidirectionnels symétriques (pas de LSP asymétriques). Un LSP symétrique bidirectionnel a les mêmes exigences d'ingénierie du trafic, incluant le partage de sort, la protection et la restauration, les LSR, et les exigences de ressources (par exemple, latence et gigue) dans chaque direction.

Dans le reste de ce paragraphe, le terme "initiateur" est utilisé pour se référer à un nœud qui commence d'établissement d'un LSP ; le terme de "terminus" est utilisé pour se référer au nœud qui est la cible du LSP. Pour un LSP bidirectionnel, il y a seulement un initiateur et un terminus.

Normalement, pour établir un LSP bidirectionnel lorsque on utilise RSVP-TE [RFC3209] ou CR-LDP [RFC3212] deux chemins unidirectionnels doivent être établis indépendamment. Cette approche présente les inconvénients suivants :

1. La latence d'établissement du LSP bidirectionnel est égale à un temps d'aller retour de la signalisation plus un délai de transit de la signalisation initiateur-terminus. Cela étend non seulement la latence d'établissement pour l'établissement réussi de LSP, mais aussi le pire cas de latence pour découvrir un LSP non réussi jusqu'à deux fois le délai de transit d'initiateur à terminus. Ces délais sont particulièrement significatifs pour les LSP établis pour des besoins de restauration.
2. Le surdébit de contrôle est deux fois celui d'un LSP unidirectionnel. C'est parce que des messages de contrôle séparés (par exemple, Path et Resv) doivent être générés pour les deux segments du LSP bidirectionnel.
3. Parce que les ressources sont établies dans des segments séparés, le choix de chemin est compliqué. Il y a aussi une compétition potentielle supplémentaire pour les conditions d'allocation de ressources, qui diminue la probabilité globale de réussite de l'établissement de la connexion bidirectionnelle.
4. Il est plus difficile de fournir une interface nette pour un équipement SONET/SDH qui puisse s'appuyer sur des chemins bond par bond bidirectionnels pour la commutation de protection. Noter que les équipements existants SONET/SDH transmettent les informations de contrôle dans la bande avec les données.

5. Les LSP optiques bidirectionnels (ou chemins optiques) sont vus somme une exigence pour de nombreux fournisseurs de service de réseau optique.

Avec les LSP bidirectionnels, les deux chemins de données vers l'amont et vers l'aval, c'est-à-dire, de l'initiateur au terminus et du terminus à l'initiateur, sont établis en utilisant un seul ensemble de messages de signalisation. Cela réduit la latence d'établissement à essentiellement un temps d'aller-retour d'initiateur-terminus plus le temps de traitement, et limite le surdébit de contrôle au même nombre de messages qu'un LSP unidirectionnel.

Pour les LSP bidirectionnels, deux étiquettes doivent être allouées. L'établissement de LSP bidirectionnel est indiqué par la présence d'une étiquette amont dans le message de signalisation approprié.

7.11 Résolution de conflit entre LSP bidirectionnels

Un conflit pour les étiquettes peut survenir entre deux demandes d'établissement de LSP bidirectionnel voyageant dans des directions opposées. Ce conflit survient lorsque les deux côtés allouent les mêmes ressources (accès) au même moment. La signalisation GMPLS définit une procédure pour résoudre ce conflit : le nœud qui a le l'identifiant le plus élevé gagne le conflit. Pour réduire la probabilité de conflit, des mécanismes sont aussi suggérés.

7.12 Notification rapide de défaillance

GMPLS définit plusieurs extensions de signalisation qui permettent l'envoi de notifications de défaillances et autres événements aux nœuds responsables de la restauration des LSP défaillants, et du traitement des erreurs.

1. Ensemble d'étiquettes acceptable pour notification sur erreur d'étiquette :
   Il y a des cas dans le MPLS traditionnel et dans GMPLS qui résultent en un message d'erreur contenant une indication "Valeur d'étiquette inacceptable". Lorsque ces cas se produisent, il peut être utile pour le nœud qui génère le message d'erreur d'indiquer quelles étiquettes seraient acceptables. Pour couvrir ce cas, GMPLS introduit la capacité de porter de telles informations via le "Ensemble d'étiquettes acceptables". Un ensemble d'étiquettes acceptable est porté dans les messages d'erreur spécifiques du protocole approprié. Le format d'un ensemble d'étiquettes acceptables est identique à celui de l'ensemble d'étiquettes.

2. Envoi de notification :
   Les extensions à RSVP-TE permettent l'envoi de notifications de défaillances et autres événements à des nœuds déterminés. Pour CR-LDP, il n'y a actuellement pas de mécanisme similaire. La première extension identifie où les notifications d'événement sont à envoyer. La seconde assure un envoi général de notification d'événement avec un message Notify. De telles extensions peuvent être utilisées par des mécanismes de restauration rapide. Les notifications peuvent être demandées dans les deux directions vers l'amont et vers l'aval.
   Le message Notify est un mécanisme de notification généralisée qui diffère des messages d'erreur actuellement définis en ce qu'il peut être "ciblé" vers un nœud autre que le voisin immédiat en amont ou en aval. Le message Notify ne remplace pas les messages d'erreur existants. Le message Notify peut être envoyé soit (a) normalement, et alors des nœuds non cibles transmettent juste le message Notify au nœud cible, comme dans le traitement ResvConf de la [RFC2205] ; soit (b) encapsulé dans un nouvel en-tête IP dont la destination est égale à l'adresse IP cible.

3. Suppression plus rapide des états intermédiaires :
   Optimisation spécifique de RSVP qui permet dans certains cas une suppression plus rapide des états intermédiaires. Cette extension est utilisée avec des mécanismes spécifiques de RSVP.

7.13 Protection de liaison

Les informations de protection sont portées dans le nouvel objet/TLV facultatif Informations de protection. Il indique actuellement la protection de liaison désirée pour chaque liaison d'un LSP. Si un type de protection particulier, c'est-à-dire, 1+1, ou 1:N, est demandé, une demande de connexion n'est alors traitée que si le type de protection désiré peut être honoré. Noter que GMPLS annonce les capacités de protection d'une liaison dans les protocoles d'acheminement. Les algorithmes de calcul de chemin peuvent considérer ces informations lors du calcul de chemin pour établir les LSP.

Les informations de protection indiquent aussi si le LSP est principal ou secondaire. Un LSP secondaire est une sauvegarde d'un LSP principal. Les ressources d'un LSP secondaire ne sont normalement pas utilisées tant que le LSP principal n'a pas de défaillance, mais elles peuvent être utilisées par d'autres LSP jusqu'à ce que le LSP principal se replie sur le LSP secondaire. À ce moment, tout LSP qui utilise les ressources pour le LSP secondaire doit être préempté.

Six types de protection de liaison sont actuellement définis comme des fanions individuels et peuvent être combinés: améliorés, dédiés 1+1, dédiés 1:1, partagés, non protégés, extra trafic. Voir au paragraphe 7.1 de la [RFC3471] une définition précise de chacun d'eux.

7.14 Acheminement et contrôle d'étiquette explicites

En utilisant un chemin explicite, le chemin pris par un LSP peut être contrôlé plus ou moins précisément. Normalement, le nœud à l'extrémité de tête d'un LSP trouve un chemin explicite et construit un objet/TLV Chemin explicite (ERO/ER) qui contient ce chemin. Éventuellement, le nœud bordure ne construit pas de chemin explicite, et transmet juste une demande de signalisation à un LSR voisin par défaut (comme le ferait un hôte IP/MPLS). Par exemple, un chemin explicite pourrait être ajouté à un message de signalisation par le premier nœud commutant, au nom du nœud bordure. Noter aussi qu'un chemin explicite est altéré par les LSP intermédiaires durant sa progression vers la destination.

Le chemin explicite est à l'origine défini par MPLS-TE comme une liste de nœuds abstraits (c'est-à-dire, des groupes de nœuds) le long du chemin explicite. Chaque nœud abstrait peut être un préfixe d'adresse IPv4, un préfixe d'adresse' IPv6, ou un numéro d'AS. Cette capacité permet au générateur du chemin explicite d'avoir des informations incomplètes sur les détails du chemin. Dans le cas le plus simple, un nœud abstrait peut être une adresse IP complète (32 bits) qui identifie un nœud spécifique (appelé un nœud abstrait simple).

MPLS-TE permet des nœuds abstraits strict et lâches. Le chemin entre un nœud strict et son nœud précédent doit inclure seulement des nœuds réseau provenant du nœud strict et de son nœud abstrait précédent. Le chemin entre un nœud lâche et son nœud abstrait précédent peut inclure d'autres nœuds réseau qui ne font pas partie du nœud lâche ou de son nœud abstrait précédent.

Ce chemin explicite a été étendu pour inclure des numéros d'interface comme nœuds abstraits pour prendre en charge des interfaces non numérotées, et a été encore étendu par GMPLS pour inclure des étiquettes comme nœuds abstraits. Avoir des étiquettes dans un chemin explicite est une caractéristique importante qui permet de contrôler le placement d'un LSP avec une granularité très fine. Ceci sera très probablement utilisé pour les liaisons TDM, LSC et FSC.

En particulier, le contrôle explicite d'étiquette dans le chemin explicite permet la terminaison d'un LSP sur un accès sortant particulier d'un nœud de sortie. Bien sûr, un sous objet/TLV d'étiquette doit suivre un sous objet/TLV contenant l'adresse IP, ou l'identifiant d'interface (en cas d'une interface non numérotée) associé à la liaison sur laquelle il va être utilisé.

Ceci peut aussi être utilisé lorsque il est désirable de "lier" deux LSP ensemble, c'est-à-dire, lorsque la queue du premier LSP serait "épissée" dans la tête du second LSP.

Lorsque il est utilisé avec un algorithme d'optimisation, il peut fournir des chemins explicites très détaillés, incluant l'étiquette (intervalle de temps) à utiliser sur une liaison, afin de minimiser la fragmentation du multiplex SONET/SDH sur l'interface correspondante.

7.15 Enregistrement de chemin

Afin d'améliorer la fiabilité et la gérabilité des LSP à établir, le concept d'enregistrement de chemin a été introduit dans RSVP-TE pour fonctionner comme :

- D'abord un mécanisme de détection de boucle pour découvrir des boucles d'acheminement de couche 3, ou des boucles inhérentes au chemin explicite (ce mécanisme est strictement exclusif de l'utilisation d'objets d'acheminement explicite).

- Ensuite un mécanisme d'enregistrement de chemin collecte les informations de chemin détaillées et à jour bond par bond durant le processus d'établissement du LSP. Ce mécanisme fournit des informations précieuses aux nœuds de source et de destination. Tout changement d'acheminement intermédiaire au moment de l'établissement, en cas d'acheminement explicite lâche, sera rapporté.

- Enfin, un chemin enregistré peut être utilisé comme entrée pour un chemin explicite. Ceci est utile si un nœud source reçoit le chemin enregistré d'un nœud de destination et l'applique comme un chemin explicite afin de "baliser le chemin".

Dans l'architecture GMPLS, seules les secondes et troisièmes fonctions sont principalement applicables pour les couches TDM, LSC et FSC.

7.16 Modification et réacheminement de LSP

La modification et le réacheminement de LSP sont deux caractéristiques déjà disponibles dans MPLS-TE. GMPLS n'ajoute rien de nouveau. Un réacheminement élégant est possible avec le concept de "couture avant cassure" par lequel un vieux chemin est toujours utilisé alors qu'un nouveau chemin est établi en évitant une double réservation de ressources. Ensuite, le nœud qui effectue le réacheminement peut basculer sur le nouveau chemin et clore l'ancien. Cette caractéristique est prise en charge avec RSVP-TE (en utilisant des filtres explicites partagés) et CR-LDP (en utilisant le fanion d'indicateur d'action).

La modification de LSP consiste à changer certains paramètres de LSP, mais normalement sans changer le chemin. Elle est prise en charge en utilisant le même mécanisme que le réacheminement. Cependant, la sémantique de la modification de LSP va différer d'une technologie à l'autre. Par exemple, des études complémentaires sont nécessaires pour comprendre l'impact du changement dynamique de certaines caractéristiques de circuits SONET/SDH comme la bande passante, le type de protection, la transparence, l'enchaînement, etc..

7.17 Traitement de l'état administratif de LSP

GMPLS fournit la capacité facultative d'indiquer l'état administratif d'un LSP en utilisant un nouvel objet/TLV État administratif. Les informations d'état administratif sont généralement utilisées de deux façons. Dans le premier usage, l'objet/TLV État administratif est porté dans un message Demande de chemin/étiquette ou Transposition de réservation/étiquette pour indique l'état administratif d'un LSP. Dans cet usage, les informations d'état administratif indiquent l'état du LSP, ce qui inclut "actif" ou "mort", si il est en mode "essai", et si la suppression est en cours.

Sur la base de cet état administratif, un nœud peut prendre des décisions locales, comme d'inhiber les alarmes qui rapportent quand un LSP est dans les états "mort" ou "en essai", ou rapporter des alarmes associées à la connexion à une priorité égale ou inférieure à "N'affecte pas le service".

Il est possible que certains nœuds le long d'un LSP ne prennent pas en charge l'objet/TLV État administratif. Dans le cas d'un nœud qui ne prend pas en charge le transit, l'objet va passer non modifié à travers le nœud et le traitement normal peut continuer.

Dans certaines circonstances, en particulier dans les réseaux optiques, il est utile de régler l'état administratif d'un LSP à "en cours de suppression" avant de le supprimer afin d'éviter la génération d'alarmes sans utilité. Le LSR d'entrée précède la suppression d'un LSP en insérant un objet/TLV État administratif approprié dans un message de demande de chemin/étiquette (avec le fanion indicateur d'action de modification réglé à modifier). Les LSR de transit traitent l'objet/TLV État administratif et le transmettent. Le LSR de sortie répond dans un message Transposition de réservation/étiquette (avec le fanion d'indicateur d'action de modification réglé à modifier) avec l'objet État administratif. À réception de ce message et objet, le nœud d'entrée envoie un message PathTear/Release vers l'aval pour supprimer le LSP et le traitement normal RSVP-TE/CR-LDP a lieu.

Dans le second usage, l'objet/TLV État administratif est porté dans un message Transposition de notification/étiquette (avec le fanion d'indication d'action de modification réglé à modifier) pour demander que le nœud d'entrée change l'état administratif d'un LSP. Cela permet aux nœuds intermédiaires et de sortie de déclencher le réglage de l'état administratif. En particulier, cela permet aux LSR intermédiaires ou de sortie de demander la libération d'un LSP initié par le nœud d'entrée.

7.18 Séparation du canal de contrôle

Dans GMPLS, un canal de contrôle est séparé du canal de données. Bien sûr, le canal de contrôle peut être mis en œuvre complètement hors bande pour diverses raisons, par exemple, lorsque le canal de données ne peut pas porter les informations de contrôle dans la bande. Cette question a même été introduite à l'origine dans MPLS dans le contexte des faisceaux de liaisons.

Dans le MPLS traditionnel, il y a une association implicite biunivoque d'un canal de contrôle à un canal de données. Lorsque une telle association est présente, aucune information supplémentaire ou particulière n'est requise pour associer une transaction d'établissement d'un LSP particulier avec un certain canal de données.

Autrement, il est nécessaire de convoyer des informations supplémentaires dans la signalisation pour identifier le canal de données particulier qui est contrôlé. GMPLS prend en charge l'identification explicite de canal de données en fournissant les informations d'identification d'interface. GMPLS permet l'utilisation d'un certain nombre de schémas d'identification d'interface incluant des adresses IPv4 ou IPv6, des indices d'interface (pour les interfaces non numérotées) et d'interfaces de composantes (pour des interfaces en faisceaux) ; les interfaces en faisceau non numérotées sont aussi acceptées.

Le choix de l'interface de données à utiliser est toujours fait par l'envoyeur du message Demande de chemin/étiquette, et indiqué en incluant l'identifiant d'interface du canal de données dans le message en utilisant un nouveau TLV sous type/interface d'objet RSVP_HOP.

Pour les LSP bidirectionnels, l'envoyeur choisit l'interface de données dans chaque direction. Dans tous les cas sauf la mise en faisceau, l'interface amont est impliquée par l'interface aval. Pour la mise en faisceau, l'envoyeur de la demande Chemin/étiquette identifie explicitement l'interface composante utilisée dans chaque direction. Le nouvel objet/TLV est utilisé dans le message Transposition de Réservation/étiquette pour indiquer l'usage par le nœud aval de la ou des interfaces indiquées.

Le nouvel objet/TLV peut contenir une liste de TLV incorporés, dont chacun peut être une adresse IPv4, une adresse IPv6, un indice d'interface, un identifiant d'interface de composante aval ou un identifiant d'interface de composante amont. Dans les trois derniers cas, le TLV incorporé contient lui-même une adresse IP plus un identifiant d'interface, l'adresse IP utilisée pour identifier l'identifiant d'interface (il peut être par exemple l'identifiant de routeur).

Il y a des cas où il est utile d'indiquer une interface spécifique associée à une erreur. On définit les objets RSVP IF_ID ERROR_SPEC pour prendre en charge ces cas.

8. Adjacences de transmission

Pour améliorer l'adaptabilité de MPLS TE (et donc de GMPLS) il peut être utile d'agréger plusieurs LSP TE à l'intérieur d'un plus gros LSP TE. Les nœuds intermédiaires voient seulement le LSP externe. Ils n'ont pas à entretenir d'états de transmission pour chaque LSP interne, moins de messages de signalisation doivent être échangés et le LSP externe peut être d'une certaine manière protégé au lieu (ou en plus) des LSP internes. Ceci peut augmenter considérablement l'adaptabilité de la signalisation.

L'agrégation est réalisée par (a) la création par un LSR d'un LSP TE, (b) la formation par le LSR d'une adjacence de transmission à partir de ce LSP (en annonçant de LSP comme une liaison d'ingénierie de trafic (TE) dans IS-IS/OSPF), (c) en permettant que d'autres LSR utilisent les adjacences de transmission pour leur calcul de chemin, et (d) l'incorporation de LSP générés par d'autres LSR dans ce LSP (par exemple, en utilisant la construction de piles d'étiquettes dans le cas de IP).

ISIS/OSPF écoule les informations sur les "adjacences de transmission" (FA) tout comme il écoule les informations sur toutes les autres liaisons. Par suite de cet arrosage, un LSR a dans sa base de données d'états de liaison TE les informations non seulement sur les liaisons conventionnelles, mais aussi sur les FA.

Un LSR, lorsque il effectue le calcul de chemin, utilise non seulement les liaisons conventionnelles, mais aussi les FA. Une fois qu'un chemin est calculé, le LSR utilise RSVP-TE/CR-LDP pour établir les liens d'étiquette le long du chemin. Les FA ont besoin d'une simple extension pour les protocoles de signalisation et d'acheminement.

8.1 Adjacences d'acheminement et de transmission

Les adjacences de transmission peuvent être représentées comme des liaisons non numérotée ou numérotées. Une FA peut aussi être un faisceau de LSP entre deux nœuds.

Les FA sont annoncées comme des liaisons TE GMPLS comme celles définies dans la [RFC4206]. Les liaisons TE GMPLS sont annoncées dans OSPF et IS-IS comme défini dans les [RFC4203] et [RFC4205]. Ces deux dernières spécifications améliorent les [RFC3630] et [RFC3784] qui définissent une liaison TE de base.

Lorsque une FA est créée de façon dynamique, ses attributs TE sont hérités de la FA-LSP qui a induit leur création. La [RFC4206] spécifie comment chaque paramètre TE de la FA est hérité de la FA-LSP. Noter que la bande passante de la FA doit être au moins aussi grosse que la FA-LSP qui l'a induite, mais peut être plus grosse si seules des bandes passantes discrètes sont disponibles pour la FA-LSP. En général, pour des adjacence de transmission provisionnées de façon dynamique, des mécanismes fondés sur la politique peuvent être nécessaires pour associer les attributs aux adjacences de transmission.

Une annonce de FA pourrait contenir des informations sur le chemin pris par le FA-LSP associé à cette FA. D'autres LSR peuvent utiliser ces informations pour le calcul de chemin. Ces informations sont portées dans un nouveau TLV OSPF et IS-IS appelé le TLV de chemin.

Il est possible que les informations de chemin sous-jacentes puissent changer au fil du temps, via des mises à jour de configuration, ou des modifications de chemin, résultant en le changement de ce TLV.

Si les adjacences de transmission sont mises en faisceau (via la mise en faisceau de liaisons) et si la liaison en faisceau résultante porte un TLV de chemin, le chemin sous-jacent suivi par chacune des FA-LSP qui forment les liaisons composantes doit être le même.

Il est prévu que les adjacences de transmission ne seront pas utilisées pour établir des relations d'homologue à homologue IS-IS/OSPF entre les routeurs aux extrémités de l'adjacence.

La hiérarchie de LSP pourrait exister aussi bien avec les modèles d'homologue qu'avec ceux de recouvrement. Avec le modèle d'homologue, la hiérarchie de LSP est réalisée via les FA et un LSP est à la fois créé et utilisé comme une liaison TE par exactement la même instance du plan de contrôle. Créer les hiérarchies de LSP avec des recouvrements n'implique pas le concept de FA. Avec le modèle de recouvrement, un LSP créé (et entretenu) par une instance du plan de contrôle GMPLS est utilisé comme une liaison TE par une autre instance du plan de contrôle GMPLS. De plus, les nœuds qui utilisent une liaison TE sont supposés avoir une adjacence d'acheminement et de signalisation.

8.2 Aspects de signalisation

Pour les besoins du traitement de chemin explicite dans un message Chemin/Demande d'un LSP qui doit être tunnelé sur une adjacence de transmission, un LSR à l'extrémité de tête de la FA-LSP voit le LSR à la fin de cette FA-LSP comme adjacente (un bond IP plus loin).

8.3 Cascade d'adjacences de transmission

Avec un modèle intégré, plusieurs couches sont contrôlées en utilisant les mêmes protocoles d'acheminement et de signalisation. Un réseau peut alors avoir des liaisons avec des capacités de multiplexage/démultiplexage différentes. Par exemple, un nœud peut être capable de multiplexer/démultiplexer des paquets individuels sur une certaine liaison, et peut être capable de multiplexer/démultiplexer des canaux au sein d'une charge utile SONET sur d'autres liaisons.

Un nouveau sous TLV OSPF et IS-IS a été défini pour annoncer la capacité de multiplexage de chaque interface : PSC, L2SC, TDM, LSC ou FSC. Ce sous TLV est appelé le sous TLV Descripteur de capacité de commutation d'interface, qui complète les sous TLV définis dans les [RFC4203] et [RFC4205]. Les informations portées dans ce sous TLV sont utilisées pour construire les régions de LSP, et déterminer les limites des régions.

Le calcul de chemin peut prendre en compte les limites de région lors du calcul d'un chemin pour un LSP. Par exemple, le calcul de chemin peut restreindre le chemin pris par un LSP aux seules liaisons dont la capacité de multiplexage/démultiplexage est PSC. Lorsque un LSP a besoin de franchir une limite de région, il peut déclencher l'établissement d'une FA à la couche sous-jacente (c'est-à-dire, la couche L2SC). Cela peut déclencher une cascade de FA entre les couches avec l'ordre évident suivant : L2SC, puis TDM, puis LSC, et finalement FSC.

9. Adjacences d'acheminement et de signalisation

Par définition, deux nœuds ont une adjacence d'acheminement (IS-IS/OSPF) si ils sont voisins dans le sens IS-IS/OSPF.

Par définition, deux nœuds ont une adjacence de signalisation (RSVP-TE/CR-LDP) si ils sont voisins dans le sens RSVP-TE/CR-LDP. Les nœuds A et B sont des voisins RSVP-TE si ils échangent directement des messages RSVP-TE (Path/Resv) (par exemple, comme décrit aux paragraphes 7.1.1 et 7.1.2 de la [RFC4206]). Les relations de voisinage incluent les échanges de Hello RSVP-TE.

Par définition, une adjacence de transmission (FA) est une liaison TE entre deux nœuds GMPLS dont le chemin transite par une ou plusieurs autres nœuds (G)MPLS dans la même instance du plan de contrôle (G)MPLS. Si deux nœuds ont une ou plusieurs liaisons TE non FA entre elles, ces deux nœuds sont supposés (bien que ce ne soit pas exigé) avoir une adjacence d'acheminement. Si deux nœuds n'ont pas de liaison TE non FA entre eux, il est supposé (mais pas exigé) que ces deux nœuds n'ont pas d'adjacence d'acheminement. Pour dire ce qui est évident, si les liaisons TE entre deux nœuds sont utilisées pour établir des LSP, les deux nœuds doivent avoir une adjacence de signalisation.

Si on veut établir une adjacence d'acheminement et/ou de signalisation entre deux nœuds, il doit y avoir un chemin IP entre eux. Ce chemin IP peut être, par exemple, une liaison TE avec une capacité de commutation d'interface de PSC, quelque

chose qui ressemble à une liaison IP (par exemple, un tunnel GRE, ou un LSP (bidirectionnel) avec une capacité de commutation d'interface de PSC).

Une liaison TE peut n'être pas capable d'être utilisée directement pour entretenir des adjacences d'acheminement et/ou de signalisation. Cela parce que les adjacences d'acheminement et de signalisation GMPLS exigent d'échanger des données sur la base de la trame ou du paquet, et qu'une liaison TE (par exemple, une liaison entre des OXC) peut n'être pas capable d'échanger des données sur la base du paquet. Dans ce cas, les adjacences d'acheminement et de signalisation sont entretenues via un ensemble d'un ou plusieurs canaux de contrôle (voir la [RFC4204]).

Deux nœuds peuvent avoir une liaison TE entre eux même si ils n'ont pas d'adjacence d'acheminement. Naturellement, chaque nœud doit faire fonctionner OSPF/IS-IS avec les extensions GMPLS afin que cette liaison TE soit annoncée. Plus précisément, le nœud a besoin de faire fonctionner les extensions GMPLS pour les liaisons TE avec une capacité de commutation d'interface (voir la [RFC4202]) autre que PSC. De plus, ce nœud doit faire fonctionner les extensions GMPLS ou MPLS pour les liaisons TE avec une capacité de commutation d'interface de PSC.

Les mécanismes pour la séparation de canal de contrôle [RFC3471] devraient être utilisés (même si le chemin IP entre deux nœuds est une liaison TE). C'est-à-dire, la signalisation RSVP-TE/CR-LDP devrait utiliser l'objet Interface_ID (IF_ID) pour spécifier une liaison TE particulière lors de l'établissement d'un LSP.

Le chemin IP pourrait consister en plusieurs bonds IP. Dans ce cas, les mécanismes des paragraphes 7.1.1 et 7.1.2 de la [RFC4206] devraient être utilisés (en plus de la séparation du canal de contrôle).

10. Traitement par défaut du plan de contrôle

Deux types majeurs de fautes peuvent impacter un plan de contrôle. Le premier, appelé faute de canal de contrôle, est relatif au cas où la communication de contrôle est perdue entre deux nœuds voisins. Si le canal de contrôle est incorporé dans le canal de données, la procédure de récupération du canal de données devrait résoudre le problème. Si le canal de contrôle est indépendant du canal de données, des procédures supplémentaires sont nécessaires pour récupérer.

Le second, appelé faute nodale, est relatif au cas où le nœud perd son état de contrôle (par exemple, après un redémarrage) mais ne perd pas son état de transmission de données.

Dans les réseaux de transport, de tels types de faute de plan de contrôle ne devraient pas avoir d'impact de service sur les connections existantes. Dans ces circonstances, il doit exister un mécanisme pour détecter une défaillance de la communication de contrôle et une procédure de restauration doit garantir l'intégrité de connexion aux deux extrémités du canal de contrôle.

Pour une faute de canal de contrôle, une fois que la communication est restaurée, les protocoles d'acheminement sont naturellement capables de récupérer mais les protocoles de signalisation sous-jacents doivent indiquer que les nœuds ont conservé leur état à travers la défaillance. Le protocole de signalisation doit aussi assurer que tout changement d'état qui a été instancié durant la défaillance est synchronisé entre les nœuds.

Pour une faute nodale, le plan de contrôle d'un nœud redémarre et perd la plupart de ses informations d'état. Dans ce cas, les nœuds amont et aval doivent tous deux synchroniser leurs informations d'état avec le nœud redémarré. Pour que toute resynchronisation se produise, le nœud qui effectue le redémarrage va avoir besoin de préserver certaines informations, comme sa transposition des étiquettes entrantes en sortantes.

Ces questions sont traitées de façon spécifique par les protocoles, voir les [RFC3473], [RFC3472], [RFC4203] et [RFC4205]. Noter que ces cas ne s'appliquent que quand il y a des mécanismes pour détecter les défaillances de canal de données indépendantes des défaillances du canal de contrôle.

La tolérance aux fautes dans le LDP ([RFC3479]) spécifie les procédures pour récupérer d'une défaillance du canal de contrôle. La [RFC3473] spécifie comment récupérer à la fois d'une défaillance du canal de contrôle et d'un nœud.

11. Protection et restauration de LSP

Cette section discute des questions de protection et de restauration (P&R) pour les LSP GMPLS. Elle est guidée par les exigences mentionnées dans la [RFC3386] et certains des principes établis dans la [RFC3469]. Elle sera améliorée, lorsque plus de mécanismes de P&R GMPLS seront définis. La portée de cette section est précisée comme suit :

- Cette section n'est applicable que lorsque une faute qui impacte des LSP survient dans le plan données/transport. La Section 10 s'occupe du traitement des fautes du plan de contrôle pour les fautes des nœuds et du canal de contrôle.
- Elle se focalise sur les P&R aux couches TDM, LSC et FSC. Il y a des exigences de P&R spécifiques de ces couches qui ne sont pas présentes à la couche PSC.
- Elle se concentre sur les P&R intra zone par opposition aux P&R inter zones et même inter domaines. Noter que les P&R peuvent même être plus restrictives, par exemple, pour une collection d'équipements d'utilisateur, ou une collection d'équipements de mêmes capacités, dans une seule zone d'acheminement.
- Elle se focalise sur les P&R intra couche (hiérarchie horizontale comme défini dans la [RFC3386]) par opposition aux P&R inter couches (hiérarchie verticale).
- Les mécanismes de P&R sont en général conçus pour traiter des défaillances individuelles, qui rendent nécessaire la diversité de SRLG. La récupération de défaillances multiples exige des études complémentaires.
- Les topologies de maillage et d'anneau sont toutes deux prises en charge.

Dans ce qui suit, on suppose que :
- les appareils TDM, LSC et FSC engagent plus généralement des ressources de récupération d'une façon qui n'est pas au mieux. Les ressources de récupération sont soit allouées (donc utilisées) ou au moins réservées logiquement (qu'elles soient utilisées ou non par du trafic supplémentaire préemptable mais indisponible de toutes façons pour du trafic de travail régulier).
- Les mécanismes de P&R partagés sont précieux pour les opérateurs afin de maximiser l'utilisation du réseau.
- L'envoi du trafic préemptable excédentaire sur les ressources de récupération est un dispositif valable pour les opérateurs.

11.1 Intensification de la protection à travers les domaines et les couches

Pour décrire l'architecture de P&R, on doit considérer deux dimensions de hiérarchie [RFC3386] :

- Une hiérarchie horizontale consistant en plusieurs domaines P&R, qui est importante dans un schéma de protection fondé sur le LSP. La portée de P&R peut s'étendre sur une liaison (ou portée) un domaine administratif ou un sous réseau, un LSP entier. Un domaine administratif peut consister en un seul domaine P&R ou un enchaînement de plusieurs plus petits domaines P&R. L'opérateur peut configurer des domaines P&R, sur la base des exigences du consommateur, et sur les contraintes de la topologie du réseau et de l'ingénierie du trafic.

- Une hiérarchie verticale consistant en plusieurs couches de P&R avec diverses granularités (flux de paquets, traces STS, chemins lumineux, fibres, etc.). En l'absence de coordination P&R adéquate, une faute peut se propager d'un niveau à l'autre au sein d'une hiérarchie P&R. Cela peut conduire à des "collisions" et des actions de récupération simultanées peuvent conduire à des conditions de conflit, une utilisation de ressources réduite, ou des instabilités [MANCHESTER]. Donc, une stratégie cohérente d'escalade est nécessaire pour coordonner la récupération à travers les domaines et les couches. Le fait que GMPLS puisse être utilisé à différentes couches pourrait simplifier cette coordination. Il y a deux types de stratégies d'escalade : du bas vers le haut et du haut vers le bas. L'approche de bas en haut suppose que les schémas de récupération de "niveau inférieur" sont plus efficaces. Donc, on peut inhiber ou tenir à distance une P&R de niveau supérieur. L'approche de haut en bas tente de servir le P&R aux niveaux supérieurs avant d'invoquer le P&R de "niveau inférieur". La P&R de couche supérieure est sélective du service, et permet un réacheminement "par CoS" ou "par LSP".

Les accords de niveau de service (SLA, *Service Level Agreement*) entre opérateurs de réseau et leurs clients sont nécessaires pour déterminer les échelonnements temporaires nécessaires pour la P&R à chaque couche et domaine.

11.2 Transposition des services en ressources de protection et récupération

Le choix d'un schéma de P&R est un compromis entre utilisation du réseau (coût) et durée d'interruption de service. À la lumière de ce compromis, les fournisseurs de service réseau sont supposés prendre en charge différentes offres ou niveaux de service.

On peut classer les LSP en un petit ensemble de niveaux de service. Entre autres choses, ces niveaux de service définissent les caractéristiques de fiabilité du LSP. Le niveau de service associé à un certain LSP est transposé en un ou plusieurs schémas de P&R durant l'établissement du LSP. Un avantage de cette transposition est que un LSP peut utiliser différents schémas de P&R dans différents segments d'un réseau (par exemple, certaines liaisons peuvent être protégées sur leur portée, tandis que d'autres segments du LSP peuvent utiliser une protection en anneau). Ces détails seront probablement spécifiques du fournisseur de service.

Une solution de remplacement à l'utilisation de niveaux de service est qu'une application spécifie l'ensemble de mécanismes spécifiques de P&R à utiliser lors de l'établissement du LSP. Cela permet une plus grande souplesse dans l'utilisation des différents mécanismes pour satisfaire les exigences de l'application.

Un moyen de différenciation entre ces niveaux de service est le temps d'interruption du service en cas de défaillance du réseau, qui est défini comme la durée entre le moment où se produit la défaillance et celui où la connexité est rétablie. Le choix du niveau de service (ou schéma de P&R) devrait être dicté par les exigences de service des différentes applications.

11.3 Classification des caractéristiques de mécanisme de protection et récupération

La figure qui suit donne une classification des types de provisionnement possibles de LSP de récupération, et des niveaux de sur réservation qui sont possibles pour eux.

```
                        +-Calculé à la demande +-Établi à la demande +-Ressources pré allouées
Provisionnement de LSP  |                      |                     |
  de récupération      -+-Précalculé           +-Préétabli           +-Ressources allouées à la demande

                         +--- Dédié (1:1, 1+1)
                         |
                         +--- Partagé (1:N, anneau, maillage partagé)
                         |
Niveau de surréservation--+--- Au mieux
```

11.4 Différentes étapes de protection et récupération

La récupération d'une faute ou d'une dégradation du réseau a lieu à différentes étapes, comme exposé dans la [RFC3469], incluant la détection de faute, la localisation de faute, la notification, la récupération (c'est-à-dire, la P&R elle-même) et l'inversion du trafic (c'est-à-dire, le retour du trafic au LSP fonctionnel d'origine ou à un nouveau).

- La détection de faute dépend de la technologie et de la mise en œuvre. En général, les défaillances sont détectées par des mécanismes de couche inférieure (par exemple, SONET/SDH, perte de lumière (LOL, *Loss-of-Light*)). Lorsque un nœud détecte une défaillance, une alarme peut être renvoyée à une entité GMPLS, qui va prendre les actions appropriées, ou l'alarme peut être propagée à la couche inférieure (par exemple, AIS SONET/SDH).

- La localisation de faute peut être faite avec l'aide de GMPLS, par exemple, en utilisant LMP pour la localisation de faute (voir le paragraphe 6.4).

- La notification de faute peut aussi être réalisée par GMPLS, par exemple, en utilisant la notification GMPLS RSVP-TE/CR-LDP (voir le paragraphe 7.12).

- Cette section se focalise sur les différents mécanismes disponibles pour la récupération et l'inversion du trafic une fois que la détection de faute, la localisation et la notification ont eu lieu.

11.5 Stratégies de récupération

Les techniques P&R de réseau peuvent être divisées en protection et restauration. Dans la protection, les ressources entre les points d'extrémité de protection sont établis avant la défaillance, et la connexité après la défaillance est réalisée simplement par une commutation effectuée aux points d'extrémité de protection. À l'opposé, la restauration utilise la signalisation après la défaillance pour allouer les ressources le long du chemin de récupération.

- La protection vise des délais de réaction extrêmement rapides et peut s'appuyer sur l'utilisation de champs de contrôle de surdébit pour réaliser la coordination de point d'extrémité. La protection pour les réseaux SONET/SDH est décrite dans [ITUT-G.841] et [ANSI-T1.105]. Les mécanismes de protection peuvent être encore classés par le niveau de redondance et de partage.

- Les mécanismes de restauration s'appuient sur les protocoles de signalisation pour coordonner les actions de commutation durant la récupération, et peuvent impliquer un simple reprovisionnement, c'est-à-dire, de signaler seulement au moment de la récupération ; ou une présignalisation, c'est-à-dire, signaler avant la récupération.

De plus, la P&R peut être appliquée en local ou de bout en bout. Dans l'approche locale, la P&R se focalise sur la proximité locale de la faute afin de réduire le délai de restauration du service. Dans l'approche de bout en bout, le LSP générateur et les nœuds de terminaison contrôlent la récupération.

En utilisant ces stratégies, les mécanismes de récupération suivants peuvent être définis.

11.6 Mécanismes de récupération : schémas de protection

Noter que les schémas de protection sont généralement définis dans des technologies spécifiques, mais cela n'empêche pas d'autres solutions.

- Protection de liaison 1+1 : deux ressources pré provisionnées sont utilisées en parallèle. Par exemple, les données sont transmises simultanément sur deux liaisons parallèles et un choix est fait au nœud receveur de la meilleure source (voir aussi la [RFC4426]).

- Protection de liaison 1:N : les ressources de travail et de protection (N de travail, 1 de sauvegarde) sont pré provisionnées. Si une ressource de travail a une défaillance, les données sont commutées sur la ressource de protection, en utilisant un mécanisme de coordination (par exemple, dans les octets de surdébit). Plus généralement, N ressources de travail et M ressources de protection peuvent être allouées pour M:N protection de liaison (voir aussi la [RFC4426]).

- Protection améliorée : divers mécanismes comme des anneaux de protection peuvent être utilisés pour améliorer le niveau de protection au delà de la simple défaillance de liaison pour inclure la capacité de contourner la défaillance d'un nœud ou plusieurs défaillances de liaison dans une certaine portée, sur la base d'une topologie pré établie des ressources de protection (note : aucune référence disponible au moment de cette publication).

- Protection de LSP 1+1 : une transmission de données simultanée sur les LSP de travail et de protection et la sélection de l'extrémité de queue peuvent être appliquées (voir aussi la [RFC4426]).

11.7 Mécanismes de récupération : schémas de restauration

Grâce à l'utilisation d'un plan de contrôle réparti comme GMPLS, la restauration est possible en quelques dixièmes de millisecondes. Il est beaucoup plus difficile de la réaliser lorsque seul un système de gestion de réseau (NMS) est utilisé et elle peut seulement être faite dans ce cas en plusieurs secondes.

- Restauration de LSP de bout en bout avec reprovisionnement : un chemin de restauration de bout en bout est établi après la défaillance. Le chemin de restauration peut être calculé de façon dynamique après la défaillance, ou pré calculé avant (souvent durant l'établissement du LSP). Il est important de noter qu'aucune signalisation n'est utilisée le long du chemin de restauration avant la défaillance, et aucune bande passante de restauration n'est réservée. Par conséquent, il n'est pas garanti qu'un certain chemin de restauration soit disponible quand une défaillance se produit. Donc, on peut avoir à "rétro pédaler" à la recherche d'un chemin disponible.

- Restauration de LSP de bout en bout avec réservation de bande passante de récupération pré signalée et pas de pré sélection d'étiquette : un chemin de restauration de bout en bout est pré calculé avant la défaillance et un message de signalisation est envoyé le long de ce chemin pré sélectionné pour réserver de la bande passante, mais les étiquettes ne sont pas choisies (voir aussi la [RFC4426]). Les ressources réservées sur chaque liaison d'un chemin de restauration peuvent être partagées entre différents LSP de travail qui ne sont pas supposés faillir simultanément. Les politiques de nœud locales peuvent être appliquées pour définir le degré de partage de capacité entre des défaillances indépendantes. À détection d'une défaillance, la signalisation de LSP est initiée le long du chemin de restauration pour choisir les étiquettes, et pour initier les interconnexions appropriées.

- Restauration de LSP de bout en bout avec réservation de bande passante de récupération pré signalée et pré sélection d'étiquette : un chemin de restauration de bout en bout est pré calculé avant la défaillance et une procédure de signalisation est initiée le long de ce chemin pré sélectionné sur lequel la bande passante est réservée et les étiquettes sont choisies (voir aussi la [RFC4426]). Les ressources réservées sur chaque liaison peuvent être partagées entre différents LSP de travail qui ne sont pas supposés faillir simultanément. Dans les réseaux fondés sur les technologies TDM, LSC et FSC, la signalisation de LSP est utilisée après la détection de défaillance pour établir les interconnexions aux commutateurs intermédiaires sur le chemin de restauration en utilisant les étiquettes pré sélectionnées.

- Restauration de LSP local : les approches ci-dessus peuvent être appliquées sur une base locale plutôt que de bout en bout, afin de réduire le temps de récupération (note : aucune référence disponible au moment de la publication).

11.8 Critères de choix de schéma

Ce paragraphe expose les critères qui pourraient être utilisés par l'opérateur afin de faire un choix parmi les divers mécanismes de P&R.

- Robustesse : en général, moins il y a de pré planification du chemin de restauration, plus le schéma de restauration est robuste à diverses défaillances, pourvu que les ressources adéquates soient disponibles. Les schémas de restauration avec des chemins pré planifiés ne seront pas capables de récupérer de défaillances réseau qui affectent simultanément les deux chemins de travail et de restauration. Donc, ces chemins devraient idéalement être choisis comme aussi disjoints que possible (c'est-à-dire, SRLG et nœud disjoints) afin q'aucun événement de défaillance seul ne puisse affecter les deux chemins. Le risque d'une défaillance simultanée des deux chemins peut être réduit par un nouveau calcul du chemin de restauration chaque fois qu'il s'y produit une défaillance. La pré sélection d'une étiquette donne moins de souplesse pour les divers scénarios de défaillance que pas de pré sélection d'étiquette. Si il se produit des défaillances qui affectent deux LSP qui partagent une étiquette à un nœud commun le long de leurs chemins de restauration, un seul de ces LSP peut alors être récupéré, sauf si l'allocation d'étiquette est changée. La robustesse d'un schéma de restauration est aussi déterminé par la quantité de bande passante de restauration réservée – lorsque la quantité de partage de bande passante de restauration augmente (la bande passante réservée diminue) le schéma de restauration devient moins robuste aux défaillances. Les schémas de restauration avec réservation de bande passante pré signalée (avec ou sans pré sélection d'étiquette) peuvent réserver la bande passante adéquate pour assurer la récupération de tout ensemble d'événement de défaillance spécifique, comme toute défaillance de SRLG unique, toutes doubles défaillances de SRLG, etc.. Il est clair qu'une plus grande capacité de restauration est allouée si un niveau de récupération de défaillance supérieur est exigé. Donc, le niveau de protection du réseau est déterminé par la politique qui définit la quantité de bande passante de restauration réservée.

- Délai de récupération : en général, plus il y a de pré planification du chemin de restauration, plus le schéma de P&R est rapide. Les schémas de protection récupèrent généralement plus vite que les schémas de restauration. La restauration avec réservation de bande passante pré signalée est probablement (significativement) plus rapide que la restauration de chemin avec réapprovisionnement, en particulier à cause de l'élimination de tout rétropédalage. La restauration locale sera généralement plus rapide que les schémas de bout en bout. Les objectifs de temps de récupération pour la commutation de protection SONET/SDH (non inclus le délai de détection de la défaillance) sont spécifiés dans [ITUT-G.841] à 50 ms, prenant en compte les contraintes de distance, de nombre de connexions impliquées, et dans le cas de protection améliorée d'anneau, le nombre de nœuds dans l'anneau. Les objectifs de temps de récupération pour les mécanismes de restauration sont définis dans un autre document [RFC3386].

- Partage de ressource : la protection 1+1 et 1:N de liaison et LSP exige des chemins de récupération dédiés avec une capacité limitée de partager les ressources : 1+1 ne permet pas de partage, 1:N permet un peu de partage des ressources de protection et de prise en charge de trafic supplémentaire (préemptable). La souplesse est limitée à cause des restrictions topologiques, par exemple, topologie d'anneau fixe pour les schémas traditionnels de protection améliorée. Le degré de partage que permettent les schémas de restauration parmi plusieurs défaillances indépendantes est directement dicté par la taille du réservoir de restauration. Dans les schémas de restauration avec réapprovisionnement, un réservoir de capacité de restauration peut être défini à partir duquel tous les chemins de restauration sont choisis après la défaillance. Donc, le degré de partage est défini par la quantité de capacité de restauration disponible. En restauration avec réservation de bande passante pré signalée, la capacité de restauration réservée est déterminée par les politiques locale de réservation de bande passante. Dans tous les schémas de restauration, des ressources préemptables peuvent utiliser la capacité de restauration résiduelle quand cette capacité n'est pas utilisée pour la récupération de défaillance.

12. Gestion de réseau

Les fournisseurs de service (SP, *Service Provider*) utilisent intensivement la gestion de réseau pour configurer, surveiller ou provisionner divers appareils dans leur réseau. Il est important de noter qu'un équipement de SP peut être distribué à travers des sites géographiquement séparés, ce qui rend la gestion répartie encore plus importants. Le fournisseur de service devrait utiliser le système NMS et les protocoles de gestion standard comme SNMP (voir les [RFC3410], [RFC3411] et [RFC3416]) et les modules de MIB pertinents comme interfaces standard pour configurer, surveiller et provisionner les appareils aux diverses localisations. Le fournisseur de service peut aussi souhaiter utiliser l'interface de ligne de commande (CLI, *command line interface*) fournie par les fabricants avec leurs appareils. Cependant, ceci n'est pas une solution standard ou recommandée parce qu'il n'y a pas de langage ou interface de CLI standard, d'où il résulte dans un réseau N différents CLI avec des appareils de N différents fabricants. Dans le contexte de GMPLS, il est extrêmement important que les interfaces standard aux appareils du SP (par exemple, SNMP) existent à cause de la nature de la technologie elle-même. Comme GMPLS comporte de nombreuses couches différentes de technologies de plan de contrôle et de plan des données,

il est important pour les interfaces de gestion dans ce domaine d'être assez souples pour permettre au gestionnaire de gérer facilement GMPLS, et d'une façon standard.

12.1 Systèmes de gestion de réseau (NMS)

Le système NMS devrait conserver les informations collectives sur chaque appareil au sein du système. Noter que le système NMS peut en fait être composé de plusieurs applications réparties (c'est-à-dire, des agrégateurs d'alarmes, des consoles de configuration, des applications d'interrogation, etc.) qui constituent collectivement le NMS du SP. De cette façon, il peut prendre des décisions d'approvisionnement et de maintenance avec la pleine connaissance du réseau entier du SP. Les informations de configuration ou de provisionnement (c'est-à-dire, les demandes de nouveaux services) pourraient être entrées dans le NMS et ensuite distribuées via SNMP aux appareils distants. Donc, rendre la tâche de gestion du SP beaucoup plus compacte et facile plutôt que d'avoir à gérer chaque appareil individuellement (c'est-à-dire, via la CLI).

La sécurité et le contrôle d'accès peuvent être réalisés en utilisant le modèle de sécurité fondé sur l'utilisateur(USM, *User-based Security Model*) de SNMPv3 [RFC3414] et le modèle de contrôle d'accès fondé sur la vue (VCAM, *View-based Access Control Model*) [RFC3415]. Cette approche peut être très efficacement utilisée au sein du réseau d'un SP, car le SP a l'accès et le contrôle sur tous les appareils dans son domaine. Des MIB normalisées devront être développées avant que cette approche puisse être utilisée partout pour provisionner, configurer et surveiller les appareils dans des réseaux non hétérogènes ou à travers les frontières de réseau de SP.

12.2 Base de données d'informations de gestion (MIB)

Dans le contexte de GMPLS, il est extrêmement important qu'il existe des interfaces standard aux appareils à cause de la nature de la technologie elle-même. Comme GMPLS comporte de nombreuses couches de technologie de plan de contrôle différentes, il est important pour les modules de MIB SNMP dans ce domaine d'être assez souples pour permettre au gestionnaire de gérer le plan de contrôle entier. Cela devrait être fait en utilisant des modules de MIB qui puissent coopérer (c'est-à-dire, une création coordonnée de rangées chez l'agent) ou des modules de MIB plus généraux qui agrègent certaines des actions désirées et repoussent les détails jusqu'aux appareils. Il est important de noter que dans certaines circonstances, il peut être nécessaire de dupliquer un petit sous ensemble d'objets gérables dans de nouveaux modules de MIB pour faciliter la gestion. Le contrôle de certaines parties de GMPLS peut aussi être réalisé en utilisant des interfaces de MIB existantes (c'est-à-dire, la MIB SONET existante) ou en en utilisant d'autres, distinctes, qui sont encore à définir. Les modules de MIB peuvent avoir été précédemment définis dans l'IETF ou l'UIT. Les modules de MIB actuels peuvent devoir être étendus pour faciliter certaines des nouvelles fonctionnalités désirées par GMPLS. Dans ces cas, le groupe de travail devrait étudier de nouvelles versions de ces modules de MIB afin que ces extensions puissent être ajoutées.

12.3 Outils

Comme dans les réseaux traditionnels, des outils standard tels que traceroute [RFC1393] et ping [RFC2151] sont nécessaires pour déboguer et surveiller les performances des réseaux GMPLS, et principalement pour la technologie du plan de contrôle, qui vont imiter la topologie du plan des données. De plus, de tels outils fournissent des informations sur l'accessibilité des réseaux. Les protocoles de contrôle de GMPLS auront besoin d'exposer certains éléments d'information afin que ces outils fonctionnent correctement et fournissent des informations en rapport avec GMPLS. Ces outils devraient être disponibles via la CLI. Ces outils devraient aussi être disponibles pour l'invocation à distance via l'interface SNMP [RFC2925].

12.4 Corrélation des fautes entre plusieurs couches

Du fait de la nature de GMPLS, et que des couches potentielles peuvent être impliquées dans le contrôle et la transmission des informations de données et de contrôle de GMPLS, il est nécessaire qu'une faute dans une couche soit passée aux couches adjacentes supérieure et inférieure pour leur notifier la faute. Cependant, du fait de la nature de ces nombreuses couches, il est possible, et même probable, que des centaines ou même des milliers de notifications peuvent devoir passer entre les couches. Ceci est indésirable pour plusieurs raisons. D'abord, ces notifications vont surcharger l'appareil. Ensuite, si le ou les appareils sont programmés pour émettre des notifications SNMP [RFC3417] le grand nombre de notifications que l'appareil peut tenter d'émettre peut alors surcharger le réseau avec une tempête de notifications. De plus, même si l'appareil émet les notifications, le NMS qui doit traiter ces notifications sera lui aussi surchargé ou va traiter des informations redondantes. C'est à dire que si 1000 interfaces à la couche B sont empilées au dessus d'une seule interface en dessous à la couche A, et si l'interface en A tombe en panne, les interfaces à la couche B ne devraient pas émettre de notifications. À la place, l'interface de la couche A devrait émettre une seule notification. Le NMS qui reçoit cette notification devrait être capable de corréler le fait que cette interface en a de nombreuses autres empilées au dessus d'elle, et prendre les actions appropriées, si nécessaire.

Les appareils qui prennent en charge GMPLS devraient fournir des mécanismes pour agréger, résumer, activer et désactiver les notifications inter couches pour les raisons décrites ci-dessus. Dans le contexte des modules de MIB SNMP, tous les modules de MIB qui sont utilisés par GMPLS doivent fournir des objets d'activation/désactivation pour tous les objets de notification. De plus, ces MIB doivent aussi fournir des objets ou fonctionnalités de résumé de notification (comme décrit ci-dessus). Les systèmes NMS et les outils standard qui traitent les notifications ou gardent trace de nombreuses couches sur un certain appareil doivent être capables de traiter à tout moment la grande quantité d'informations qui peuvent éventuellement être émises par les appareils du réseau qui fonctionnent avec GMPLS.

13. Considérations sur la sécurité

GMPLS définit une architecture de plan de contrôle pour plusieurs technologies et types d'éléments de réseau. En général, comme les LSP établis en utilisant GMPLS peuvent porter de gros volumes de données et consommer des ressources significatives du réseau, des mécanismes de sécurité sont requis pour sauvegarder le réseau sous-jacent contre les attaques sur le plan de contrôle et/ou l'utilisation non autorisée des ressources de transport des données. Le plan de contrôle GMPLS devrait donc inclure des mécanismes qui empêchent ou minimisent le risque que des attaquants soient capables d'injecter du trafic de contrôle et/ou de l'espionner. Ces risques dépendent du niveau de confiance entre les nœuds qui échangent des messages de contrôle GMPLS, ainsi que de la réalisation et des caractéristiques physiques du canal de contrôle. Par exemple, un canal de contrôle dans la bande sur fibre, sur des octets SONET/SDH redondants est, en général, considéré moins vulnérable qu'un canal de contrôle sur un réseau IP hors bande.

Les mécanismes de sécurité peuvent assurer l'authentification et la confidentialité. L'authentification peut assurer la vérification de l'origine, de l'intégrité du message, et la protection contre la répétition, tandis que la confidentialité assure qu'un tiers ne peut pas déchiffrer le contenu d'un message. Dans les situations où le déploiement de GMPLS exige principalement l'authentification, les mécanismes respectifs d'authentification des protocoles composants de GMPLS peuvent être utilisés (voir les [RFC2747], [RFC3036], [RFC2385] et [RFC4204]). De plus, la suite de protocoles IPsec (voir les [RFC2402], [RFC2406] et [RFC2409]) peut être utilisée pour assurer l'authentification, la confidentialité ou les deux, pour un canal de contrôle GMPLS. IPsec offre donc les avantages d'une protection combinée pour tous les protocoles composants de GMPLS ainsi que la gestion de clés.

Une question en rapport est celle de l'autorisation de demandes de ressources par des nœuds à capacité GMPLS. L'autorisation détermine si certaine partie, qu'on suppose déjà authentifiée, a un droit d'accès aux ressources demandées. Cette détermination est normalement une affaire de contrôle de politique locale [RFC2753], par exemple en établissant les limites sur la bande passante totale disponible pour une certaine partie en présence de compétition pour les ressources. De telles politiques peuvent devenir assez complexes lorsque le nombre d'usagers, de types de ressources et de sophistication des règles d'autorisation augmente.

Après l'authentification des demandes, les éléments de contrôle devraient leur être confrontés par rapport à la politique d'autorisation locale. Ces éléments de contrôle doivent être capables de prendre des décisions sur la base de l'identité du demandeur, telle que vérifiée cryptographiquement et/ou topologiquement. Par exemple, des décisions peuvent dépendre de si l'interface à travers laquelle la demande est faite est inter ou intra domaine. L'utilisation des politiques d'autorisation locales appropriées peut aider à limiter l'impact des failles de sécurité dans les parties distantes d'un réseau.

Finalement, on notera que GMPLS n'introduit par lui-même aucune nouvelle considération de sécurité pour la signalisation MPLS-TE actuelle (RSVP-TE, CR-LDP), pour les protocoles d'acheminement actuels (OSPF-TE, IS-IS-TE) ou pour les protocoles de gestion de réseau (SNMP).

14. Remerciements

Le présent document est le fruit du travail de nombreux auteurs et consiste en la composition d'un certain nombre de documents antérieurs dans ce domaine.

Tous mes remerciement à Ben Mack-Crane (Tellabs) pour les utiles discussions sur SONET/SDH. Merci aussi à Pedro Falcao, Alexandre Geyssens, Michael Moelants, Xavier Neerdaels, et Philippe Noel de Ebone pour leur avis technique et leur soutien sur SONET/SDH et optique. Enfin, tous mes remerciements à Krishna Mitra (consultant), Curtis Villamizar (Avici), Ron Bonica (WorldCom), et Bert Wijnen (Lucent) pour leur effort de révision de la Section 12.

15. Références

15.1 Références normatives

[RFC3031] E. Rosen, A. Viswanathan, R. Callon, "Architecture de commutation d'étiquettes multi protocoles", janvier 2001. *(P.S.)* (*MàJ par la* RFC6790)

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

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

[RFC3471] L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : description fonctionnelle de la signalisation", janvier 2003. (*MàJ par* RFC4201, RFC4328, RFC4872) *(P.S.)*

[RFC3472] P. Ashwood-Smith et L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : extensions au protocole de distribution d'étiquettes acheminées sur la base des contraintes de signalisation (CR-LDP)", janvier 2003. (*MàJ par* RFC3468, RFC4201) *(P.S.)*

[RFC3473] L. Berger, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", janvier 2003. *(P.S., MàJ par 4003, 4201, 4420, 4783, 4784, 4873, 4974, 5063, 5151,* RFC6780))

15.2 Références pour information

[ANSI-T1.105] "Synchronous Optical Network (SONET): Basic Description Including Multiplex Structure, Rates, And Formats," ANSI T1.105, 2000.

[ITUT-G.707] Recommandation UIT-T G.707, "Interface de nœud de réseau pour la hiérarchie numérique synchrone", octobre 2000.

[ITUT-G.709] Recommandation UIT-T G.709, "Interface pour le réseau de transport optique" version 1.0 (et Amendement 1) février 2001 (et octobre 2001).

[ITUT-G.841] Recommandation UIT-T G.841, "Types et caractéristiques des architectures de protection de réseau SDH", octobre 1998.

[MANCHESTER] J. Manchester, P. Bonenfant and C. Newton, "The Evolution of Transport Network Survivability," IEEE Communications Magazine, août 1999.

[OIF-UNI] The Optical Internetworking Forum, "User Network Interface (UNI) 1.0 Signaling Specification - Implementation Agreement OIF-UNI-01.0," octobre 2001.

[RFC1393] G. Malkin, "Traceroute en utilisant une option IP", janvier 1993. *(Historique, voir la* RFC6814)

[RFC2151] G. Kessler, S. Shepard, "Les bases des outils et utilitaires de l'Internet et de TCP/IP", juin 1997. (FYI0030) *(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, RFC6780))

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S.* ; *MàJ par la* RFC6691 *;Remplacée par* RFC5925).

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

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

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

[RFC2753] R. Yavatkar, D. Pendarakis, R. Guerin, "Cadre pour le contrôle d'admission fondé sur la politique", janvier 2000. *(Info.)*

[RFC2925] K. White, "Définitions des objets gérés pour les opérations de Ping à distance, Traceroute, et Lookup", septembre 2000. (*Obsolète, voir* RFC4560) *(P.S.)*

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

[RFC3386] W. Lai, éd., D. McDysan, éd., "Hiérarchie de réseau et résilience multicouche", novembre 2002. *(Information)*

[RFC3410] J. Case et autres, "Introduction et déclarations d'applicabilité pour le cadre de gestion standard de l'Internet", décembre 2002. *(Information)*

[RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "Architecture de description des cadres de gestion du protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* RFC5343) (STD0062)

[RFC3414] U. Blumenthal, B. Wijnen, "Modèle de sécurité fondée sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau (SNMPv3)", décembre 2002. (STD0062)

[RFC3415] B. Wijnen, R. Presuhn, K. McCloghrie, "Modèle de contrôle d'accès fondé sur la vue (VACM) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC3416] R. Presuhn, éd., "Version 2 des opérations de protocole pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC3417] R. Presuhn, éd. "Transpositions de transport pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* RFC4789) (STD0062)

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

[RFC3477] K. Kompella, Y. Rekhter, "Signalisation des liaisons non numérotées dans le protocole de réservation de ressource – ingénierie du trafic (RSVP-TE)", janvier 2003. *(P.S.)*

[RFC3479] A. Farrel, éd., "Tolérance aux fautes dans le protocole de distribution d'étiquettes (LDP)", février 2003. *(P.S.)*

[RFC3480] K. Kompella, Y. Rekhter, A. Kullberg, "Signalisation des liaisons non numérotées dans le protocole de distribution d'étiquettes acheminées sur la base des contraintes de signalisation (CR-LDP)", février 2003. *(P.S.)*

[RFC3630] D. Katz, K. Kompella et D. Yeung, "Extensions d'ingénierie de trafic à OSPF version 2", septembre 2003.

[RFC3784] H. Smit, T. Li, "Extensions de système intermédiaire à système intermédiaire (IS-IS) pour l'ingénierie du trafic (TE)", juin 2004. (*Obsolète, voir* RFC5305) (*MàJ par* RFC4205) *(Information)*

[RFC3946] E. Mannie, D. Papadimitriou, "Extensions de commutation d'étiquettes multi-protocoles généralisée (GMPLS) pour le contrôle de réseau optique synchrone (SONET) et de hiérarchie numérique synchrone (SDH)", octobre 2004. (*Obsolète, voir* RFC4606) *(P.S.)*

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

RFC4202] K. Kompella et autres, "Extensions d'acheminement pour la prise en charge de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

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

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

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

[RFC4206] K. Kompella, Y. Rekhter, "Hiérarchie de chemins commutés par étiquettes (LSP) avec l'ingénierie de trafic (TE) de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

[RFC4208] G. Swallow et autres, "Interface usager-réseau (UNI) de commutation généralisée d'étiquettes multiprotocoles (GMPLS) : prise en charge du protocole de réservation de ressource - ingénierie du trafic (RSVP-TE) pour le modèle de recouvrement", octobre 2005. *(P.S.)*

[RFC4209] A. Fredette et J. Lang, éd., "Protocole de gestion de liaison (LMP) pour les systèmes de lignes optiques en multiplexage par répartition en longueur d'onde à haute densité", octobre 2005. *(P.S., MàJ par* RFC 6898*)*

[RFC4257] G. Bernstein et autres, "Cadre du contrôle fondé sur la commutation généralisée d'étiquettes multiprotocoles (GMPLS) de réseaux en hiérarchie numérique synchrone/réseautage optique synchrone (SDH/SONET)", décembre 2005. *(Information)*

[RFC4258] D. Brungard, éd., "Exigences pour l'acheminement de la commutation généralisée d'étiquettes multiprotocoles (GMPLS) pour les réseaux optiques à commutation automatique (ASON)", novembre 2005. *(Information)*

[RFC4328] D. Papadimitriou, éd,. "Extensions de signalisation de commutation généralisée d'étiquettes multiprotocoles (GMPLS) pour la commande des réseaux de transport optiques G.709", janvier 2006. (*MàJ* RFC3471) *(P.S.)*

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

16. Contributeurs

Peter Ashwood-Smith
Nortel
P.O. Box 3511 Station C,
Ottawa, ON K1Y 4H7, Canada
mél : petera@nortelnetworks.com

Eric Mannie
Consult
Phone: +32 2 648-5023
Mobile: +32 (0)495-221775
mél : eric_mannie@hotmail.com

Daniel O. Awduche
Consult
mél : awduche@awduche.com

Thomas D. Nadeau
Cisco
250 Apollo Drive
Chelmsford, MA 01824, USA
mél : tnadeau@cisco.com

Ayan Banerjee
Calient
5853 Rue Ferrari
San Jose, CA 95138, USA
mél : abanerjee@calient.net

Lyndon Ong
Ciena
10480 Ridgeview Ct
Cupertino, CA 95014, USA
mél : lyong@ciena.com

Debashis Basak
Accelight
70 Abele Road, Bldg.1200
Bridgeville, PA 15017, USA
mél : dbasak@accelight.com

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

Lou Berger
Movaz
7926 Jones Branch Drive
MCLean VA, 22102, USA
mél : lberger@movaz.com

Dimitrios Pendarakis
Tellium
2 Crescent Place, P.O. Box 901
Oceanport, NJ 07757-0901, USA
mél : dpendarakis@tellium.com

Greg Bernstein
Grotto
mél : gregb@grotto-networking.com

Bala Rajagopalan
Tellium
2 Crescent Place, P.O. Box 901
Oceanport, NJ 07757-0901, USA
mél : braja@tellium.com

Yakov Rekhter

Juniper
1194 N. Mathilda Ave.
Sunnyvale, CA 94089, USA
mél: yakov@juniper.net

Sudheer Dharanikota

Consult
mél : sudheer@ieee.org

John Drake
Calient
5853 Rue Ferrari
San Jose, CA 95138, USA
mél : jdrake@calient.net

Debanjan Saha
Tellium
2 Crescent Place
Oceanport, NJ 07757-0901, USA
mél : dsaha@tellium.com

Yanhe Fan
Axiowave
200 Nickerson Road
Marlborough, MA 01752, USA
mél : yfan@axiowave.com

Hal Sandick
Shepard M.S.
2401 Dakota Street
Durham, NC 27705, USA
mél : sandick@nc.rr.com

Don Fedyk
Nortel
600 Technology Park Drive
Billerica, MA 01821, USA
mél : dwfedyk@nortelnetworks.com

Vishal Sharma
Metanoia
1600 Villa Street, Unit 352
Mountain View, CA 94041, USA
mél : v.sharma@ieee.org

Gert Grammel
Alcatel
Lorenzstrasse, 10
70435 Stuttgart, Germany
mél : gert.grammel@alcatel.de

George Swallow
Cisco
250 Apollo Drive
Chelmsford, MA 01824, USA
mél : swallow@cisco.com

Dan Guo
Turin
1415 N. McDowell Blvd,
Petaluma, CA 95454, USA
mél : dguo@turinnetworks.com

Z. Bo Tang
Tellium
2 Crescent Place, P.O. Box 901
Oceanport, NJ 07757-0901, USA
mél : btang@tellium.com

Kireeti Kompella
Juniper
1194 N. Mathilda Ave.
Sunnyvale, CA 94089, USA
mél : kireeti@juniper.net

Jennifer Yates
AT&T
180 Park Avenue
Florham Park, NJ 07932, USA
mél : jyates@research.att.com

Alan Kullberg
NetPlane
888 Washington
St.Dedham, MA 02026, USA
mél : akullber@netplane.com

George R. Young
Edgeflow
329 March Road
Ottawa, Ontario, K2K 2E1, Canada
mél : george.young@edgeflow.com

Jonathan P. Lang
Rincon Networks
mél : jplang@ieee.org

John Yu
Hammerhead Systems
640 Clyde Court
Mountain View, CA 94043, USA
mél : john@hammerheadsystems.com

Alex Zinin
Alcatel
1420 North McDowell Ave
Petaluma, CA 94954, USA
mél : alex.zinin@alcatel.com

Fong Liaw
Solas Research
Solas Research, LLC
mél : fongliaw@yahoo.com

17. Adresse de l'auteur

Eric Mannie (Consultant)
Avenue de la Folle Chanson, 2
B-1050 Brussels, Belgique
téléphone : +32 2 648-5023
mobile : +32 (0)495-221775
mél : eric_mannie@hotmail.com

Déclaration complète de droits de reproduction

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