Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8077
STD 84
RFC rendues obsolètes : 4447, 6723
Catégorie : Norme
ISSN: 2070-1721

L. Martini, éditeur, Cisco
G. Heron, éditeur, Cisco
février 2017

Traduction Claude Brière de L'Isle

Établissement et maintenance de pseudo filaires avec le protocole de distribution d'étiquettes (LDP)

Résumé
Les services de couche 2 (comme le relais de trame, le mode de transfert asynchrone, et Ethernet) peuvent être émulés sur un cœur de réseau MPLS en encapsulant les unités de données de protocole (PDU, *Protocol Data Unit*) de couche 2 et en les transmettant ensuite sur des pseudo filaires (PW, *pseudo filaire*). Il est aussi possible d'utiliser des pseudo filaires pour fournir des émulations de circuit de réseau optique à bas débit à multiplexage par division dans le temps et synchrones sur un réseau à capacité MPLS. Le présent document spécifie un protocole pour établir et maintenir les pseudo filaires, en utilisant des extensions au protocole de distribution d'étiquettes (LDP, *Label Distribution Protocol*). Les procédures pour encapsuler les PDU de couche 2 sont spécifiées dans d'autres documents.

Ce document est une réécriture de la RFC 4447 pour sa publication comme norme de l'Internet.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc8077.

Table des matières

1. Introduction

Les [RFC4619], [RFC4717], [RFC4618], et [RFC4448] expliquent comment encapsuler une unité de données de protocole (PDU, *Protocol Data Unit*) de couche 2 pour transmission sur un réseau à capacité MPLS. Ces documents spécifient qu'un "en-tête de pseudo filaire", consistant en un champ de démultiplexeur, va être ajouté devant la PDU encapsulée. Le champ démultiplexeur de pseudo filaire est ajouté avant la transmission d'un paquet sur un pseudo filaire. Quand le paquet arrive au point d'extrémité distant du pseudo filaire, le démultiplexeur est ce qui permet au receveur d'identifier le pseudo filaire particulier sur lequel le paquet est arrivé. Pour transmettre le paquet d'un point d'extrémité de pseudo filaire à un autre, le paquet peut avoir besoin de voyager à travers un "tunnel de réseau à commutation de paquets" (PSN, *Packet Switched Network*) ; cela va exiger qu'un en-tête supplémentaire soit ajouté devant le paquet.

Les [RFC4842] et [RFC4553] spécifient deux méthodes pour transporter des signaux numériques de multiplexage à division dans le temps (TDM, *time-division multiplexing*) (émulation de circuit TDM) sur un réseau à capacité MPLS en mode paquet. Le système de transmission pour les signaux TDM en mode circuit est le réseau optique synchrone (SONET, *Synchronous Optical Network*) [ANSI] / hiérarchie numérique synchrone (SDH, *Synchronous Digital Hierarchy*) [G.707]. Pour prendre en charge le trafic TDM, qui inclut des services vocaux, de données, et de liaisons louées privées, les pseudo filaires doivent émuler les caractéristiques de circuit des charges utiles SONET/SDH. Les signaux et charges utiles TDM sont encapsulées pour transmission sur les pseudo filaires. Un démultiplexeur pseudo filaire et un en-tête de tunnel PSN sont ajoutés devant cette encapsulation.

La [RFC4553] décrit les méthodes pour transporter les signaux numériques de multiplexage à répartition dans le temps (TDM, *time-division multiplexing*) à bas débit (émulation de circuit TDM) sur des PSN, tandis que la [RFC4842] décrit de façon similaire le transport de TDM à haut débit (SONET/SDH). Pour prendre en charge le trafic TDM, les pseudo filaires doivent émuler les caractéristiques de circuit des signaux T1, E1, T3, E3, SONET, ou SDH originaux. La [RFC4553] fait cela en encapsulant une quantité arbitraire mais constante de données de TDM dans chaque paquet, et les autres méthodes encapsulent les structures de TDM.

Dans ce document, on spécifie l'utilisation du protocole de distribution d'étiquettes MPLS (LDP, *Label Distribution Protocol*) [RFC5036] comme protocole pour établir et maintenir les pseudo filaires. En particulier, on définit de nouvelles TLV, des éléments de classe d'équivalence de transmission (FEC, *Forwarding Equivalence Class*) des paramètres, et des codes pour LDP, qui permettent à LDP d'identifier les pseudo filaires et de signaler les attributs de pseudo filaires. On

spécifie comment un point d'extrémité de pseudo filaire utilise ces TLV dans LDP pour lier une valeur de champ de démultiplexeur à un pseudo filaire et comment il informe le point d'extrémité distant de ce lien. On spécifie aussi les procédures pour rapporter les changements d'état de pseudo filaire, pour passer des informations supplémentaires sur le pseudo filaire comme nécessaire, et pour libérer les liens. Ces procédures sont destinées à être indépendantes de la version sous-jacente de IP utilisée pour la signalisation de LDP.

Dans le protocole spécifié ici, le champ démultiplexeur de pseudo filaire est une étiquette MPLS. Donc, les paquets qui sont transmis d'une extrémité du pseudo filaire à l'autre sont des paquets MPLS, qui doivent être transmis à travers un tunnel MPLS. Cependant, si les points d'extrémité du pseudo filaire sont immédiatement adjacents et si le comportement de saut d'avant-dernier bond est utilisé, le tunnel MPLS peut n'être pas nécessaire. Toute sorte de tunnel de PSN peut être utilisée, pour autant qu'il soit possible de transmettre les paquets MPLS à travers lui. Le tunnel de PSN peut lui-même être un LSP MPLS, ou toute autre sorte de tunnel qui peut porter des paquets MPLS. Les procédures pour établir et maintenir les tunnels MPLS sortent du domaine d'application de ce document.

Le présent document traite seulement de l'établissement et de la maintenance des pseudo filaires point à point. Ni les pseudo filaires point à multipoints ni multipoints à point ne sont discutés.

Les questions relatives à la qualité de service ne sont pas discutées dans le présent document.

Les deux figures suivantes décrivent les modèles de référence qui sont déduits de la [RFC3985] pour prendre en charge les services d'émulation de PW.

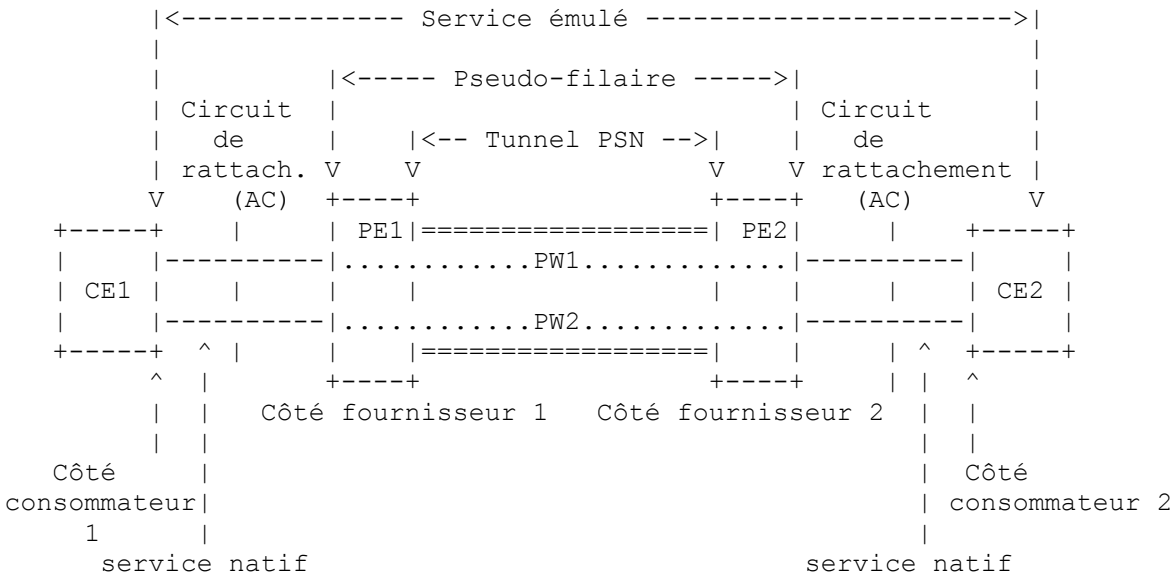


Figure 1 : Modèle de référence PWE3

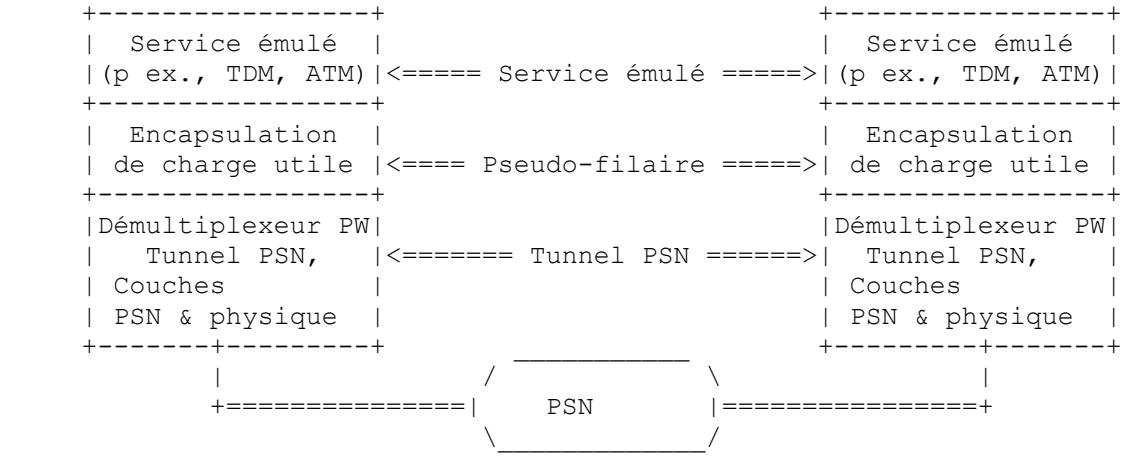


Figure 2 : Modèle de référence de pile de protocole PWE3

Pour les besoins de ce document, PE1 (Bord fournisseur 1) va être défini comme routeur d'entrée, et PE2 comme routeur de sortie. Une PDU de couche 2 va être reçue à PE1, encapsulée à PE1, transportée et désencapsulée à PE2, et transmise de PE2.

2. Changements par rapport à la RFC 4447

Les changements dans le présent document sont principalement des corrections mineures d'orthographe et de grammaire, ou des précisions du texte, qui n'ont pas été notées comme errata à la[RFC4447] ou trouvées par les éditeurs.

De plus, le paragraphe 7.3 ("Renégociation du mot de contrôle par le message de demande d'étiquette") a été ajouté, rendant obsolète la [RFC6723]. Le diagramme des procédures de traitement du bit C a aussi été supprimé. Une note a été ajoutée au paragraphe 6.3.2 pour préciser que le bit C fait partie de la classe d'équivalence de transmission (FEC).

Une référence a aussi été ajoutée à la [RFC7358] pour indiquer l'utilisation du mode non sollicité vers l'aval pour distribuer les liens d'étiquette FEC de PW, indépendamment du mode négocié d'annonce d'étiquette de la session LDP.

3. Spécification des exigences

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

4. Étiquette de pseudo filaire

Supposons qu'on désire transporter des PDU de couche 2 du LSR PE1 d'entrée au LSR PE2 de sortie, à travers un réseau à capacité MPLS interposé. On suppose qu'il y a un tunnel MPLS de PE1 à PE2. C'est-à-dire, on suppose que PE1 peut causer la livraison d'un paquet à PE2 en encapsulant le paquet dans un "en-tête de tunnel MPLS" et envoyer le résultat à une de ses adjacences. Le tunnel MPLS est un chemin à commutation d'étiquettes (LSP, *Label Switched Path*) MPLS ; donc, mettre une encapsulation de tunnel MPLS revient à pousser une étiquette MPLS.

On présuppose qu'un grand nombre de pseudo filaires peuvent être portés à travers un seul tunnel MPLS. Donc, il n'est jamais nécessaire de conserver l'état dans le cœur de réseau pour des pseudo filaires individuels. On ne présuppose pas que les tunnels MPLS sont en point à point ; bien que les pseudo filaires soient en point à point, les tunnels MPLS peuvent être multipoints à point. On ne présuppose pas que PE2 va même être capable de déterminer le tunnel MPLS à travers lequel un paquet reçu a été transmis. (Par exemple, si le tunnel MPLS est un LSP et que le saut de l'avant-dernier bond est utilisé, quand le paquet arrive à PE2, il ne va pas contenir d'informations identifiant le tunnel.)

Quand PE2 reçoit un paquet sur un pseudo filaire, il doit être capable de déterminer que le paquet a en fait été reçu sur un pseudo filaire, et il doit être capable d'associer ce paquet à un pseudo filaire particulier. PE2 est capable de faire cela en examinant l'étiquette MPLS qui sert de champ de démultiplexeur pseudo filaire montré à la Figure 2. On appelle cette étiquette une "étiquette de PW".

Quand PE1 envoie une PDU de couche 2 à PE2, il crée un paquet MPLS en ajoutant l'étiquette de PW au paquet, créant donc la première entrée de la pile d'étiquettes. Si le tunnel de PSN est un LSP MPLS, le PE1 pousse une autre étiquette (l'étiquette de tunnel) sur le paquet comme seconde entrée de la pile d'étiquettes. L'étiquette de PW n'est pas encore visible tant que le paquet MPLS n'a pas atteint PE2. Le traitement du paquet par PE2 se fonde sur l'étiquette de PW.

Si la charge utile du paquet MPLS est, par exemple, une PDU ATM de couche d'adaptation 5 (AAL5) l'étiquette de PW va généralement correspondre à un circuit virtuel (VC, *Virtual Circuit*) ATM particulier chez PE2. C'est-à-dire que PE2 doit être capable de déduire de l'étiquette de PW l'interface sortante et la valeur de l'identifiant de circuit virtuel/identifiant de chemin virtuel (VPI/VCI, *Virtual Path Identifier/Virtual Circuit Identifier*) pour la PDU AAL5. Si la charge utile est une PDU de relais de trame, PE2 a alors besoin d'être capable de déduire de l'étiquette de PW l'interface sortante et la valeur d'identifiant de connexion de liaison de données (DLCI, *Data Link Connection Identifier*). Si la charge utile est une trame

Ethernet, PE2 a alors besoin d'être capable de déduire de l'étiquette de PW l'interface sortante, et peut-être l'identifiant de VLAN. Ce processus est unidirectionnel et va être répété indépendamment pour une opération bidirectionnelle. Quand on utilise l'élément de FEC PWid, il est EXIGÉ que le même identifiant de PW et le même type de PW soient alloués pour un certain circuit dans les deux directions. L'identifiant de groupe (voir ci-dessous) NE DOIT PAS être obligé de correspondre dans les deux directions. La trame transportée PEUT être modifiée quand elle atteint le routeur de sortie. Si l'en-tête de la trame de couche 2 transportée est modifiée, ceci DOIT être fait seulement au LSR de sortie. Noter que l'étiquette de PW doit toujours être au fond de la pile d'étiquettes du paquet, et les étiquettes DOIVENT être allouées à partir de l'espace d'étiquette de la plate-forme.

Le présent document ne spécifie pas de méthode de distribution d'étiquette de tunnel MPLS ni d'aucune autre étiquette qui peut apparaître au dessus de l'étiquette de PW sur la pile. Toute méthode acceptable de distribution d'étiquette MPLS conviendra. Le présent document spécifie un protocole pour allouer et distribuer les étiquettes de PW. Ce protocole est LDP, étendu comme spécifié dans la suite de ce document. Une session LDP doit être établie entre les points d'extrémité du pseudo filaire. LDP DOIT échanger les liens d'étiquette de FEC de PW en mode non sollicité vers l'aval, indépendamment du mode d'annonce d'étiquettes négocié de la session LDP conformément aux spécifications de la [RFC7358]. Le mode LDP de "rétention libérale d'étiquette" DEVRAIT être utilisé. Cependant, toutes les procédures LDP qui sont spécifiées dans la [RFC5036] et qui sont aussi applicables à la présente spécification de protocole DOIVENT être mises en œuvre.

Le présent document exige qu'un LSR receveur DOIT répondre à un message de demande d'étiquette avec soit une transposition d'étiquette pour l'étiquette demandée, soit un message Notification qui indique pourquoi il ne peut pas satisfaire la demande. Ces procédures sont spécifiées dans la [RFC5036], aux paragraphes 3.5.7 ("Message Transposition d'étiquette") et 3.5.8 ("Message Demande d'étiquette"). Noter que l'envoi de ces réponses est une exigence plus stricte que celle spécifiée dans la [RFC5036], mais ces messages de réponse sont EXIGÉS pour assurer un fonctionnement correct de ce protocole.

En plus du protocole spécifié ici, l'allocation statique des étiquettes de PW peut être utilisée, et les mises en œuvre du présent protocole DEVRAIENT prendre en charge l'allocation statique. L'encapsulation de PW est toujours symétrique dans les deux directions de trafic avec un PW spécifique, que le PW utilise ou non un plan de contrôle LDP.

Le présent document spécifie toutes les procédures nécessaires pour établir et maintenir les pseudo filaires nécessaires à la prise en charge de services "non commutés" en point à point, où chaque point d'extrémité du pseudo filaire est provisionné avec l'identité de l'autre point d'extrémité. Il y a aussi des mécanismes de protocole qui sont spécifiés ici qui peuvent être utilisés pour prendre en charge des services commutés et d'autres modèles de provisionnement. Cependant, l'utilisation des mécanismes de protocole pour prendre en charge ces autres modèles et services n'est pas décrite dans le présent document.

5. Détails spécifiques des services émulés particuliers

5.1 Transport IP de couche 2

Ce mode porte les paquets IP sur un pseudo filaire. L'encapsulation utilisée est conforme à la [RFC3032]. Le mot de contrôle de PW PEUT être inséré entre la pile d'étiquettes MPLS et la charge utile IP. L'encapsulation des paquets IP à transmettre sur le circuit de rattachement est spécifique de la mise en œuvre, et fait partie de la fonction de traitement du service natif (NSP, *native service processing*) [RFC3985], et sort du domaine d'application de ce document.

6. LDP

Les liens d'étiquette de PW sont distribués en utilisant le mode LDP non sollicité vers l'aval décrit dans la [RFC5036]. Les appareils côté fournisseur (PE, *Provider Edge*) vont établir une session LDP en utilisant le mécanisme de découverte étendue décrit aux paragraphes 2.4.2 et 2.5 de la [RFC5036].

Un message LDP Transposition d'étiquette contient une TLV FEC, une TLV Étiquette, et zéro, une, ou plusieurs TLV Paramètres facultatifs.

La TLV FEC est utilisée pour indiquer la signification de l'étiquette. Dans le contexte courant, la TLV FEC va être utilisée pour identifier le pseudo filaire particulier auquel est liée une certaine étiquette. Dans la présente spécification, on définit deux nouvelles TLV FEC à utiliser pour identifier les pseudo filaires. Quand on établit un pseudo filaire particulier, une seule de ces TLV FEC est utilisée. Celle à utiliser va dépendre du service particulier à émuler et du modèle de

provisionnement particulier pris en charge.

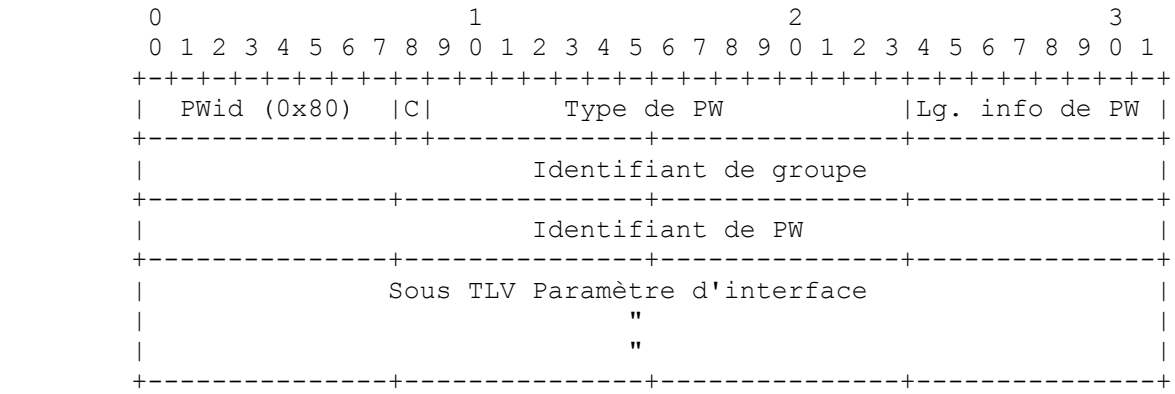
LDP permet que chaque TLV FEC consiste en un ensemble d'éléments de FEC. Pour établir et maintenir les pseudo filaires, chaque TLV FEC DOIT cependant contenir exactement un élément de FEC.

La spécification LDP de base a plusieurs sortes de TLV d'étiquettes, incluant la TLV Étiquette générique, comme spécifié au paragraphe 3.4.2.1 de la [RFC5036]. Pour établir et maintenir les pseudo filaires, la TLV Étiquette générique DOIT être utilisée.

6.1 Élément de FEC PWid

L'élément de FEC PWid peut être utilisé chaque fois que les deux points d'extrémité du pseudo filaire ont été provisionnés avec le même identifiant de 32 bits pour le pseudo filaire.

À cette fin, un nouveau type d'élément de FEC est défini. Le type d'élément de FEC est 0x80 et est défini comme suit :



- Bit Mot de contrôle (C)

Le bit C est utilisé comme fanion de présence d'un mot de contrôle comme suit :
C = 1 : le mot de contrôle est présent sur ce PW.
C = 0 : aucun mot de contrôle n'est présent sur ce PW.
Voir d'autres explications à la Section 7 ("Mot de contrôle").

- Type de PW : quantité de 15 bits contenant une valeur qui représente le type de PW. Les valeurs allouées sont spécifiées dans "Allocations de l'IANA pour l'émulation de pseudo filaire bord à bord (PWE3)" [RFC4446].

- Longueur d'informations de PW : Longueur du champ Identifiant de PW et du champ Sous TLV Paramètre d'interface en octets. Si cette valeur est 0, elle fait alors référence à tous les PW qui utilisent l'identifiant de groupe spécifié, et aucun identifiant de PW, ni de sous TLV Paramètre d'interface, n'est présent.

- Identifiant de groupe : valeur arbitraire de 32 bits qui représente un groupe de PW qui est utilisé pour créer des groupes dans l'espace de PW. L'identifiant de groupe est destiné à être utilisé comme indice d'accès ou indice de tunnel virtuel. Pour simplifier la configuration, un identifiant de groupe de PW particulier en entrée pourrait faire partie d'un identifiant de groupe alloué au tunnel virtuel pour le transport au routeur de sortie. L'identifiant de groupe est très utile pour envoyer des messages de notification de suppression d'étiquettes de caractère générique ou d'état de caractère générique de PW à des PE distants lors d'une défaillance d'accès physique.

- Identifiant de PW : identifiant de connexion non zéro, de 32 bits qui avec le type de PW identifie un PW particulier. Noter que l'identifiant de PW et le type de PW DOIVENT être les mêmes aux deux points d'extrémité.

- Sous TLV Paramètre d'interface : cette TLV de longueur variable est utilisée pour fournir des paramètres spécifiques de l'interface, comme la MTU du circuit de rattachement.

Noter que la sous TLV Paramètre d'interface fait partie de la FEC, les règles de LDP rendent impossible de changer les paramètres d'interface une fois que le pseudo filaire a été établi. Donc, le champ Paramètres d'interface ne doit pas être utilisé pour passer des informations, comme les informations d'état, qui peuvent changer durant la vie du pseudo filaire. Les

TLV Paramètres facultatifs devraient être utilisées à cette fin.

En utilisant la FEC PWid, chaque point d'extrémité du pseudo filaire initie indépendamment l'établissement d'un LSP unidirectionnel. Un LSP sortant et un LSP entrant sont liés ensemble dans un seul pseudo filaire si ils ont le même identifiant et type de PW.

6.2 Élément de FEC PWid généralisé

L'élément de FEC PWid peut être utilisé si une valeur unique de 32 bits a été allouée au PW et si chaque point d'extrémité a été provisionné avec cette valeur. L'élément de FEC PWid généralisé exige que les points d'extrémité de PW soient identifiés de façon univoque ; le PW lui-même est identifié comme une paire de points d'extrémité. De plus, les identifiants de point d'extrémité sont structurés pour prendre en charge les applications où l'identité de points d'extrémité distants doit être auto-découverte plutôt que configurée statiquement.

Le type de l'élément de FEC PWid généralisé est 0x81.

L'élément de FEC PWid généralisé ne contient rien de correspondant à l'identifiant de groupe de l'élément de FEC PWid. La fonction d'identifiant de groupe est fournie par une TLV LDP facultative séparée, la TLV Identifiant de groupe de PW, décrite au paragraphe 6.2.2.2. Le champ Paramètres d'interface de l'élément de FEC PWid est aussi absent ; sa fonction est remplacée par la TLV facultative Paramètres d'interface de PW, décrite au paragraphe 6.2.2.1.

6.2.1 Identifiants de rattachement

Comme discuté dans la [RFC3985], un pseudo filaire peut être vu comme connectant deux "émetteurs". Le protocole utilisé pour établir un pseudo filaire doit permettre à l'émetteur à une extrémité d'un pseudo filaire d'identifier l'émetteur à l'autre extrémité. On utilise le terme d'identifiant de rattachement (AI, *Attachment Identifier*) pour se référer au champ qu'utilise le protocole pour identifier les émetteurs. Dans la FEC PWid, le champ PWid sert d'AI. Dans ce paragraphe, on spécifie une forme d'AI plus générale qui est structurée et de longueur variable.

Chaque émetteur dans un PE doit être associé à un AI, par configuration ou par un algorithme. L'AI doit être unique dans le contexte du routeur de PE dans lequel réside l'émetteur. La combinaison <adresse IP de routeur PE, AI> doit être unique au monde.

Il est souvent pratique de voir un ensemble d'émetteurs comme des membres d'un "groupe" particulier, où les PW peuvent seulement être établis parmi les membres d'un groupe. Dans ce cas, il est pratique d'identifier les émetteurs par rapport au groupe, de sorte qu'un AI va consister en un identifiant de groupe de rattachement (AGI, *Attachment Group Identifier*) plus un identifiant individuel de rattachement (AII, *Attachment Individual Identifier*).

Un identifiant de groupe de rattachement peut être vu comme un identifiant de VPN, ou de VLAN, un attribut qui est partagé par tous les PW de rattachement (ou de leurs réservoirs) à qui il est permis d'être connectés.

Les détails de la façon de construire les champs AGI et AII qui identifient les points d'extrémité de pseudo filaire sortent du domaine d'application de la présente spécification. Différentes applications de pseudo filaire, et différents modèles de provisionnement, vont exiger différentes sortes de champs AGI et AII. La spécification de chacune de ces applications et/ou modèle doit inclure les règles pour construire les champs AGI et AII.

Comme discuté précédemment, un pseudo filaire (bidirectionnel) consiste en une paire de LSP unidirectionnels, un dans chaque direction. Si un pseudo filaire particulier connecte PE1 à PE2, la direction du PW de PE1 à PE2 peut être identifiée comme :

<PE1, <AGI, AII1>, PE2, <AGI, AII2>>,

et la direction du PW de PE2 à PE1 peut être identifiée par :

<PE2, <AGI, AII2>, PE1, <AGI, AII1>>.

Noter que le AGI doit être le même aux deux points d'extrémité, mais le AII va en général être différent à chaque point d'extrémité. Donc, du point de vue d'un PE particulier, chaque pseudo filaire a un AII local ou "AII de source", et un AII

distant ou "AII cible". Le protocole d'établissement de pseudo filaire peut porter ces trois quantités :
- Identifiant de groupe de rattachement (AGI, *Attachment Group Identifier*)
- Identifiant individuel de rattachement de source (SAII, *Source Attachment Individual Identifier*)
- Identifiant individuel de rattachement cible (TAII, *Target Attachment Individual Identifier*)

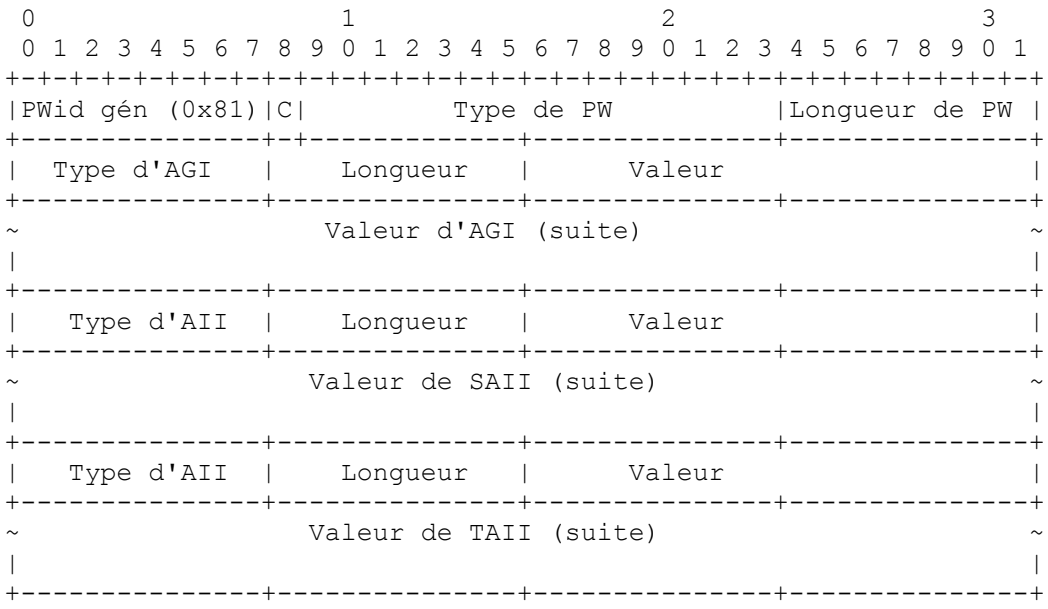
Si l'AGI est non nul, alors l'AI de source (SAI) consiste en l'AGI avec le SAII, et l'AI cible (TAI) consiste en le TAII avec l'AGI. Si l'AGI est nul, alors le SAII et le TAII sont respectivement le SAI et le TAI.

L'interprétation du SAI et du TAI est une affaire locale aux points d'extrémité respectifs.

L'association de deux LSP unidirectionnels dans un seul pseudo filaire bidirectionnel dépend du SAI et du TAI. Chaque application et/ou modèle de provisionnement qui utilise la FEC de PWid généralisé doit spécifier les règles pour effectuer cette association.

6.2.2 Codage de l'élément de FEC PWid généralisé

Le type d'élément de FEC 0x81 est utilisé. L'élément de FEC est codé comme suit :



Le présent document ne spécifie pas les valeurs des champs de type d'AII et d'AGI ; la spécification des valeurs de champ de type à utiliser pour une application particulière fait partie de la spécification de cette application. L'IANA a alloué ces valeurs en utilisant la méthode définie dans la [RFC4446].

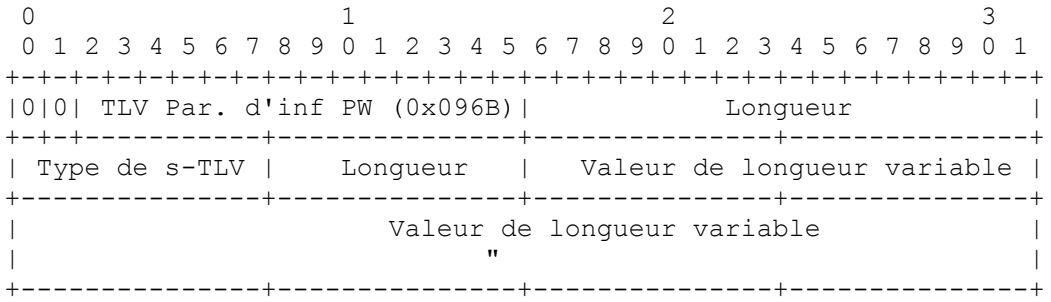
SAII, TAII, et AGI sont simplement portés comme des chaînes d'octets. L'octet Longueur spécifie la taille du champ Valeur. La chaîne nulle peut être envoyée en réglant l'octet Longueur à 0. Si une application particulière n'a pas besoin de tous ces trois sous éléments, elle DOIT envoyer tous les sous éléments mais régler Longueur à 0 pour les sous éléments non utilisés.

Le champ Longueur de PW contient la longueur de SAII, TAII, et AGI, combinés en octets. Si cette valeur est 0, elle fait alors référence à tous les PW qui utilisent l'identifiant de groupe spécifique (spécifié dans le TLV ID de groupe de PW). Dans ce cas, il n'y a pas d'autre champ Élément de FEC (AGI, SAII, etc.) présent, ni de TLV Paramètres d'interface de PW.

Noter que l'interprétation d'un champ particulier comme AGI, SAII, ou TAII dépend de l'ordre de son occurrence. Le champ Type identifie le type de l'AGI, SAII, ou TAII. Quand on compare deux occurrences d'un AGI (ou SAII ou TAII) les deux occurrences sont considérées comme identiques si les champs Type, Longueur, et Valeur de l'un sont identiques, respectivement, à ceux de l'autre.

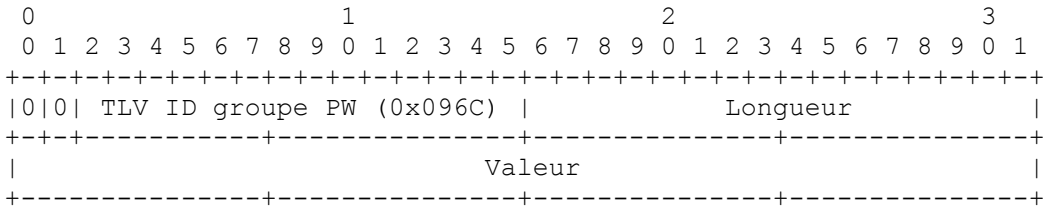
6.2.2.1 TLV Paramètres d'interface de pseudo filaire

Cette TLV DOIT seulement être utilisée pour l'envoi de la FEC PWid généralisée. Elle spécifie des paramètres spécifiques de l'interface. Les paramètres spécifiques, lorsque applicables, DOIVENT être utilisés pour valider que les PE et les accès d'entrée et de sortie aux bordures du circuit ont les capacités nécessaires pour interopérer les uns avec les autres.



Une description plus détaillée de ce champ se trouve au paragraphe 6.4 ("Sous TLV Paramètre d'interface").

6.2.2.2 TLV Identifiant de groupe de pseudo filaire



L'identifiant de groupe de PW est une valeur arbitraire de 32 bits qui représente un groupe arbitraire de PW. Il est utilisé pour créer des PW de groupe ; par exemple, un identifiant de groupe de PW peut être utilisé comme indice d'accès et être alloué à tous les PW qui conduisent à cet accès. L'utilisation de l'identifiant de groupe de PW permet à un PE d'envoyer des retraits d'étiquettes "génériques", ou des messages Notification d'état "génériques", aux PE distants lors d'une défaillance d'accès physique.

Note : L'identifiant de groupe de PW est différent de l'identifiant de groupe de rattachement et n'a pas de relation avec lui.

La TLV Identifiant de groupe de PW ne fait pas partie de la FEC et ne sera pas annoncée sauf dans l'annonce de FEC du PW. Le PE annonceur PEUT utiliser la sémantique de retrait générique, mais les PE distants DOIVENT mettre en œuvre la prise en charge des messages génériques. Cette TLV DOIT seulement être utilisée pour l'envoi de FEC de PWid généralisé.

Pour produire une commande générique (état ou retrait) :
- Régler la longueur d'informations de PW à 0 dans l'élément FEC de PWid généralisé.
- Envoyer seulement la TLV Identifiant de groupe de PW avec la FEC (aucun AGI/SAII/TAII n'est envoyé).

6.2.3 Procédures de signalisation

Afin que PE1 commence à signaler à PE2, PE1 doit connaître l'adresse du PE2 distant et un TAI. Cette information peut avoir été configurée chez PE1, ou elle peut avoir été apprise de façon dynamique via une procédure d'auto découverte.

Le PE de sortie (PE1), qui a connaissance du PE d'entrée, initie l'établissement en envoyant un message Transposition d'étiquette au PE d'entrée (PE2). Le message Transposition d'étiquette contient la TLV FEC, portant l'élément de FEC PWid généralisée (type 0x81). L'élément de FEC PWid généralisée contient les informations d'AGI, SAII, et TAII.

Ensuite, quand PE2 reçoit un tel message Transposition d'étiquette, PE2 interprète le message comme une demande d'établissement d'un PW dont le point d'extrémité (à PE2) est le transmetteur identifié par le TAI. Du point de vue du protocole de signalisation, comment exactement PE2 transpose les AI en transmetteurs est une affaire locale. Dans certains modèles de provisionnement de service filaire privé virtuel (VPWS, *Virtual Private Wire Service*) le TAI pourrait, par exemple, être une chaîne qui identifie un circuit de rattachement particulier, comme "ATM3VPI4VCI5", ou il pourrait, par

exemple, être une chaîne comme "Fred", qui est associée par configuration à un circuit de rattachement particulier. Dans le service de LAN privé virtuel (VPLS, *Virtual Private LAN Service*) l'AGI pourrait être un identifiant de VPN, identifiant une instance de VPLS particulière.

Si PE2 ne peut pas transposer le TAI en un de ses transmetteurs, il envoie un message Libération d'étiquette à PE1, avec un code d'état de "TAI non alloué/non reconnu", et le traitement du message Transposition d'étiquette est achevé.

La TLV FEC envoyée dans un message Libération d'étiquette est la même que la TLV FEC reçue dans le message Transposition d'étiquette qui est libéré (mais sans la TLV Paramètre d'interface). Plus généralement, la TLV FEC est la même dans tous les messages LDP qui se rapportent au même PW. Dans un message Libération d'étiquette, cela signifie que le SAII est l'AII de l'homologue distant et que le TAII est l'AII local de l'envoyeur.

Si le message Transposition d'étiquette a un TAI valide, PE2 doit décider s'il l'accepte. Les procédures pour le faire vont dépendre du type particulier de transmetteur identifié par le TAI. Bien sûr, le message Transposition d'étiquette peut être rejeté à cause de conditions d'erreur LDP standard comme précisé dans la [RFC5036].

Si PE2 décide d'accepter le message Transposition d'étiquette, il doit alors s'assurer qu'un PW LSP est établi dans la direction opposée (PE1-->PE2). Si il a déjà signalé le PW LSP correspondant dans cette direction, rien de plus n'a à être fait. Autrement, il doit initier une telle signalisation en envoyant un message Transposition d'étiquette à PE1. Ceci est très similaire au message Transposition d'étiquette que PE2 a reçu, mais le SAI et le TAI sont inversés.

Donc, un PW bidirectionnel consiste en deux LSP, où la FEC de l'un a le SAII et le TAII inversés par rapport à la FEC de l'autre.

6.3 Signalisation de l'état de pseudo filaire

6.3.1 Utilisation des messages de transposition d'étiquette

Les PE DOIVENT envoyer des messages Transposition d'étiquette à leurs homologues aussitôt que le PW est configuré et activé administrativement, sans considération de l'état du circuit de rattachement. L'étiquette de PW ne devrait pas être supprimée sauf si l'opérateur configure administrativement la fermeture du pseudo filaire(ou si la configuration de PW est entièrement supprimée). En utilisant les procédures mentionnées dans ce paragraphe, une simple méthode de retrait d'étiquette PEUT aussi être prise en charge comme un moyen traditionnel de signaler l'état de PW et l'état d'AC. Dans tous les cas, si le lien d'étiquette à PW n'est pas disponible, le PW DOIT être considéré comme étant dans l'état mort.

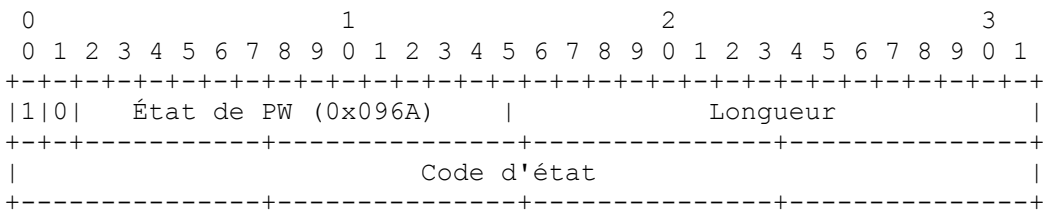
Une fois que les procédures de négociation d'état de PW sont achevées, si elles résultent en l'utilisation de la méthode de retrait d'étiquette pour la communication d'état de PW, et si cette méthode n'est pas prise en charge par un des PE, celui-ci doit alors envoyer un message Libération d'étiquette à son homologue avec l'erreur "Retrait d'étiquette de méthode d'état de PW non prise en charge".

Si la méthode de retrait d'étiquette pour la communication d'état de PW est choisie pour le PW, elle va résulter en l'annonce du message Transposition d'étiquette seulement si le circuit de rattachement est actif. Les procédures de signalement d'état de PW décrites dans ce paragraphe DOIVENT être entièrement mises en œuvre.

6.3.2 Signalisation d'état de pseudo filaire

Les appareils PE utilisent une TLV LDP pour indiquer l'état à leurs homologues distants. Cette TLV État de PW contient plus d'informations que le simple message Suppression d'étiquette.

Le format de la TLV État de PW est :

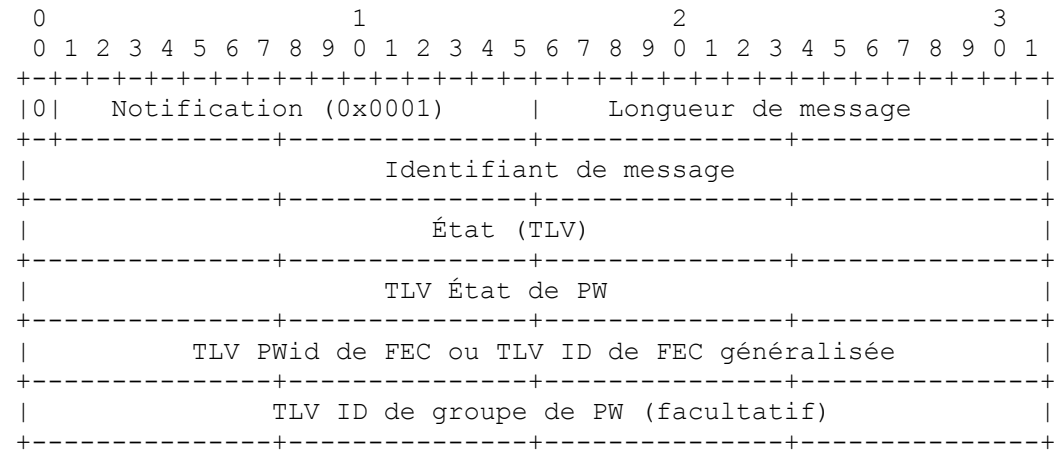


Le code d'état est un champ de 4 octets comme spécifié dans "Allocations de l'IANA pour l'émulation de pseudo filaire bord à bord (PWE3)" [RFC4446].

Le champ Longueur spécifie la longueur du champ Code d'état en octets (égal à 4).

Chaque bit dans le champ Code d'état peut être réglé individuellement pour indiquer plus d'une seule défaillance à la fois. Chaque faute peut être supprimée par l'envoi d'un message Notification approprié dans lequel le bit respectif est à zéro. La présence du bit inférieur (PW non transmetteur) agit seulement comme indication générique de défaillance quand il y a un événement de rupture de liaison pour laquelle aucun des autres bits ne s'applique.

La TLV État est transportée au PW homologue distant via le message Notification LDP comme décrit dans la [RFC5036]. Le format du message Notification pour porter l'état de PW est le suivant :



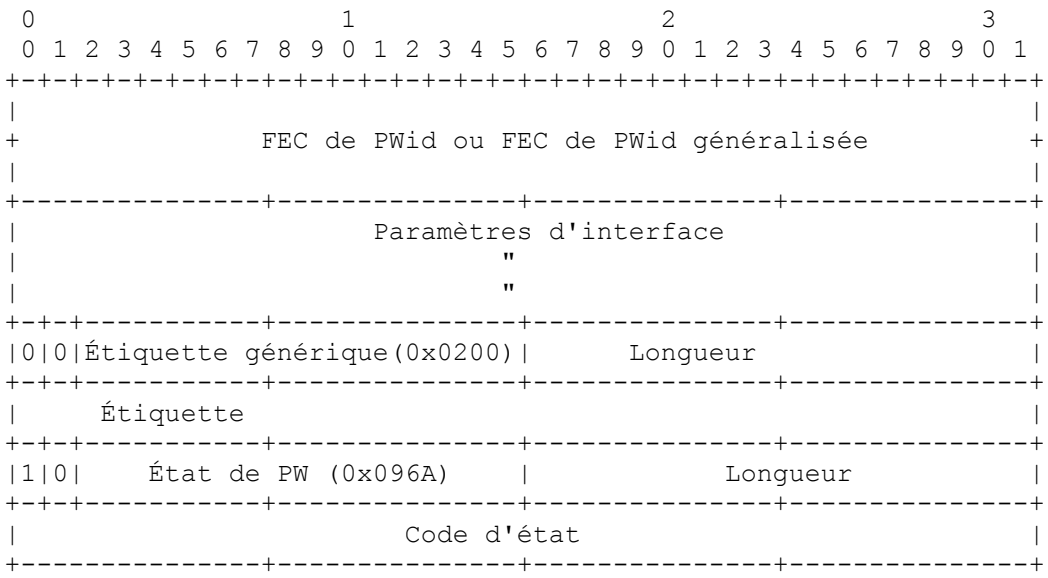
Le code d'état de TLV État est réglé à 0x00000028, "État de PW", pour indiquer que l'état de PW suit. Comme cette notification ne se réfère à aucun message particulier, le champ Identifiant de message est réglé à 0.

La TLV FEC de PW NE DEVRAIT PAS inclure de sous TLV Paramètre d'interface, car elles sont ignorées dans le contexte de ce message. Cependant, la TLV FEC de PW DOIT inclure le bit C, lorsque applicable, car il fait partie de la FEC. Quand le circuit de rattachement d'un PE rencontre une erreur, l'utilisation du message Notification de PW permet au PE d'envoyer un seul message d'état "générique", en utilisant une TLV FEC de PW avec seulement l'identifiant de groupe établi pour noter ce changement d'état pour toutes les connexions de PW affectées. Ce message d'état contient soit la TLV FEC de PW avec seulement l'identifiant de groupe établi, soit la TLV FEC généralisée avec seulement la TLV Identifiant de groupe de PW.

Comme mentionné ci-dessus, le champ Identifiant de groupe de l'élément de FEC PWid, ou la TLV identifiant de groupe de PW utilisé avec l'élément FEC PWid généralisé, peut être utilisé pour envoyer une notification d'état pour tous les ensembles arbitraires de PW. Cette procédure est FACULTATIVE, et si elle est mise en œuvre, le message Notification LDP devrait être comme suit : si l'élément FEC de PWid est utilisé, le champ Longueur des informations de PW est réglé à 0, le champ Identifiant de PW n'est pas présent, et les sous TLV Paramètre d'interface ne sont pas présents. Si l'élément FEC généralisée est utilisé, AGI, SAII, et TAII ne sont pas présents, le champ Longueur des informations de PW est réglé à 0, la TLV Identifiant de groupe de PW est incluse, et la TLV Paramètres d'interface de PW est omise. Pour les besoins du présent document, ceci est appelé la "procédure de notification générique d'état de PW", et il est EXIGÉ de tous les PE qui mettent en œuvre ce concept qu'ils acceptent un tel message de notification, mais ils ne sont pas obligés de l'envoyer.

6.3.3 Procédures de négociation d'état de pseudo filaire

Quand un PW est établi pour la première fois, les PE DOIVENT tenter de négocier l'usage de la TLV État de PW. Ceci est réalisé comme suit : un PE qui prend en charge la TLV État de PW DOIT l'inclure dans le message Transposition d'étiquette initial à la suite des sous TLV FEC de PW et Paramètres d'interface. La TLV État de PW va alors être utilisée pour la durée de vie du pseudo filaire. C'est ce qui est montré dans le diagramme suivant :



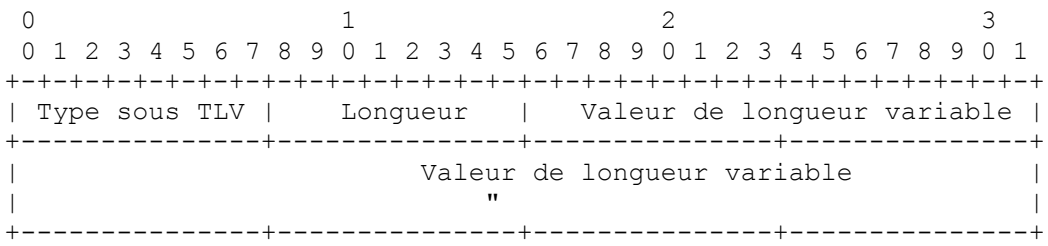
Si une TLV État de PW est incluse dans le message Transposition d'étiquette initial pour un PW, alors si le message Transposition d'étiquette provenant du PE distant pour ce PW n'inclut pas de TLV État de PW, ou si le PE distant ne prend pas en charge la TLV État de PW, le PW va revenir à la méthode de retrait d'étiquette de signalement d'état de PW. Noter que si la TLV État de PW n'est pas prise en charge par l'homologue distant, l'homologue va automatiquement l'ignorer, car le bit I (ignorer) est établi dans la TLV. La TLV État de PW ne va donc pas être présente dans l'annonce de FEC correspondante venant de l'homologue LDP distant, ce qui résulte exactement en le comportement ci-dessus.

Si la TLV État de PW n'est pas présente à la suite de la TLV FEC dans le message Transposition d'étiquette de PW initial reçu par un PE, alors la TLV État de PW ne va pas être utilisée, et les deux PE qui prennent en charge le pseudo filaire vont revenir à la procédure de retrait d'étiquette pour signaler les changements d'état.

Si le processus de négociation résulte en l'usage de la TLV État de PW, alors l'état réel du PW est déterminé par la TLV État de PW qui a été envoyée dans le message Transposition d'étiquette de PW initial. Les mises à jour ultérieures de l'état d'un PW sont portées dans les messages Notification.

6.4 Sous TLV Paramètre d'interface

Ce champ spécifie les paramètres spécifiques de l'interface. Quand il est applicable, il DOIT être utilisé pour valider que les PE et les accès d'entrée et de sortie dans les bordures du circuit ont les capacités nécessaires pour interopérer les uns avec les autres. La structure des champs est définie comme suit :



Le champ Longueur est défini comme la longueur du paramètre d'interface incluant les champs Type de sous TLV et Longueur eux-mêmes. Le traitement des paramètres d'interface devrait se poursuivre quand des paramètres d'interface inconnus sont rencontrés, et ils DOIVENT être ignorés en silence.

Les valeurs de type de sous TLV Paramètre d'interface sont spécifiées dans "Allocations de l'IANA pour l'émulation de pseudo filaire bord à bord (PWE3)" [RFC4446].

- Type de sous TLV MTU d'interface : Valeur de 2 octets qui indique la MTU en octets. C'est l'unité maximum de transmission, excluant les frais généraux d'encapsulation, de l'interface de sortie de paquets qui va transmettre la PDU

désencapsulée reçue du réseau à capacité MPLS. Ce paramètre n'est applicable qu'aux PW qui transportent des paquets et il est EXIGÉ pour ces types de PW. Si ce paramètre ne correspond pas dans les deux directions d'un PW spécifique, ce PW NE DOIT PAS être activé.

- Type de sous TLV facultative de chaîne de description d'interface : Cette chaîne arbitraire, et FACULTATIVE, de description d'interface est utilisée pour envoyer une chaîne administrative lisible par l'homme décrivant l'interface au PE distant. Ce paramètre est FACULTATIF et est applicable à tous les types de PW. La longueur de la chaîne du paramètre de description d'interface est variable et peut être de 0 à 80 octets. Le texte lisible par l'homme DOIT être fourni dans le jeu de caractères UTF-8 en utilisant le langage par défaut [RFC2277].

6.5 Procédures de retrait d'étiquette LDP

Comme mentionnée précédemment, le champ Identifiant de groupe de l'élément FEC de PWid, ou TLV Identifiant de groupe de PW utilisé avec l'élément FEC de PWid généralisé, peut être utilisé pour retirer toutes les étiquettes de PW associées à un groupe de PW particulier. Cette procédure est FACULTATIVE, et si elle est mise en œuvre, le message Suppression d'étiquette LDP devrait être comme suit : si l'élément FEC de PWid est utilisé, le champ Longueur des informations de PW est réglé à 0, le champ Identifiant de PW n'est pas présent, les sous TLV Paramètre d'interface ne sont pas présents, et la TLV Étiquette n'est pas présente. Si l'élément FEC généralisée est utilisé, AGI, SAII, et TAII ne sont pas présents, le champ Longueur des informations de PW est réglé à 0, la TLV Identifiant de groupe de PW est incluse, la TLV Paramètre d'interface de PW n'est pas présente, et la TLV Étiquette n'est pas présente. Pour les besoins du présent document, ceci est appelé la "procédure de retrait générique", et il est EXIGÉ de tous les PE qui mettent en œuvre ce concept qu'ils acceptent de tels messages de retrait, mais ils ne sont pas obligés de les envoyer. Noter que la TLV Identifiant de groupe de PW ne s'applique qu'aux PW qui utilisent l'élément d'identifiant de FEC généralisée, tandis que l'identifiant de groupe s'applique à l'élément de FEC PWid.

Les sous TLV ou TLV Paramètre d'interface, NE DOIVENT PAS être présentes dans un message de retrait d'étiquette de PW LDP ou Libération d'étiquette. Un message Libération d'étiquette générique DOIT seulement inclure la TLV Identifiant de groupe ou Identifiant de groupe de PW. Un message Libération d'étiquette initié par un routeur PE doit toujours inclure l'identifiant de PW.

7. Mot de contrôle

7.1 Types de PW pour lesquels le mot de contrôle est EXIGÉ

Les messages Transposition d'étiquette qui sont envoyés afin d'établir ces PW DOIVENT avoir C=1. Quand un message Transposition d'étiquette pour un PW d'un de ces types est reçu et que C=0, un message Libération d'étiquette DOIT être envoyé, avec un code d'état "Bit C illégal". Dans ce cas, le PW ne sera pas activé.

7.2 Types de PW pour lesquels le mot de contrôle N'EST PAS obligatoire

Si un système est capable d'envoyer et recevoir le mot de contrôle sur des types de PW pour lesquels le mot de contrôle n'est pas obligatoire, alors chacun de ces points d'extrémité de PW DOIT être configurable avec un paramètre qui spécifie si l'utilisation du mot de contrôle est PRÉFERÉE ou NON PRÉFÉRÉE. Pour chaque PW, il DOIT y avoir une valeur par défaut de ce paramètre. La présente spécification NE déclare PAS quelle valeur par défaut ce devrait être.

Si un système N'est PAS capable d'envoyer et recevoir le mot de contrôle sur les types de PW pour lesquels le mot de contrôle n'est pas obligatoire, il se comporte alors exactement comme si il était configuré pour l'utilisation NON PRÉFÉRÉE du mot de contrôle.

Si un message Transposition d'étiquette pour le PW a déjà été reçu mais si aucun message Transposition d'étiquette pour le PW n'a encore été vu, la procédure est alors comme suit :

i. Si le message Transposition d'étiquette reçu a C=0, envoyer un message Transposition d'étiquette avec C=0 ; le mot de contrôle n'est pas utilisé.
ii. Si le message Transposition d'étiquette reçu a C=1, et si le PW est configuré en local de telle façon que l'utilisation du mot de contrôle est préférée, envoyer alors un message Transposition d'étiquette avec C=1; le mot de contrôle est utilisé.
iii. Si le message Transposition d'étiquette reçu a C=1, et si le PW est configuré en local de telle façon que l'utilisation du mot de contrôle n'est pas préférée ou que le mot de contrôle n'est pas pris en charge, agir alors comme si aucun message Transposition d'étiquette n'avait été reçu pour le PW (c'est-à-dire, passer au paragraphe suivant).

Si un message Transposition d'étiquette pour le PW n'a pas déjà été reçu (ou si le message Transposition d'étiquette reçu a C=1 et si la configuration locale dit que l'utilisation du mot de contrôle n'est pas préférée ou si le mot de contrôle n'est pas pris en charge) alors envoyer un message Transposition d'étiquette dans lequel le bit C est réglé à correspondre à la préférence configurée localement pour l'utilisation du mot de contrôle. (C'est-à-dire, C=1 si la configuration locale est de préférer le mot de contrôle, et C=0 si la configuration locale est de préférer ne pas utiliser de mot de contrôle ou si le mot de contrôle n'est pas pris en charge).

L'action suivante dépend du message de contrôle qui est reçu ensuite pour ce PW. Les possibilités sont :

i. Un message Transposition d'étiquette avec la même valeur de bit C que spécifiée dans le message Transposition d'étiquette qui a été envoyé. L'établissement de PW est maintenant achevé, et le mot de contrôle est utilisé si C=1 mais n'est pas utilisé si C=0.
ii. Un message Transposition d'étiquette avec C=1, mais le message Transposition d'étiquette envoyé avait C=0. Dans ce cas, ignorer le message Transposition d'étiquette reçu et continuer d'attendre le prochain message de contrôle pour le PW.
iii. Un message Transposition d'étiquette avec C=0, mais le message Transposition d'étiquette envoyé avait C=1. Dans ce cas, envoyer un message Suppression d'étiquette avec un code d'état "Bit C erroné", suivi par un message Transposition d'étiquette qui a C=0. L'établissement de PW est maintenant achevé, et le mot de contrôle n'est pas utilisé.
iv. Un message Suppression d'étiquette avec le code d'état "Mauvais bit C". Le traiter comme un message Suppression d'étiquette normal, mais ne pas répondre. Continuer d'attendre le prochain message de contrôle pour le PW.

Si à tout moment après la réception d'un message Transposition d'étiquette, un retrait ou une libération d'étiquette correspondant est reçu, l'action effectuée est la même que pour tout message Retrait ou Libération d'étiquette qui pourrait être reçu à tout moment.

Si les deux points d'extrémité préfèrent utiliser le mot de contrôle, cette procédure va faire qu'il sera utilisé. Si l'un au l'autre point d'extrémité préfère ne pas utiliser le mot de contrôle ou ne prend pas en charge le mot de contrôle, cette procédure va faire qu'il ne sera pas utilisé. Si un point d'extrémité préfère utiliser le mot de contrôle mais pas l'autre, celui qui préfère ne pas l'utiliser n'a pas de protocole supplémentaire à exécuter ; il attend juste un message Transposition d'étiquette qui a C=0.

7.3 Renégociation du mot de contrôle par le message Demande d'étiquette

Il est possible qu'après que la procédure de négociation du bit C de PW décrite ci-dessus est achevée, le PE local PE soit re-provisionné avec une préférence différente de mot de contrôle. Donc, une fois que les procédures de négociation de mot de contrôle sont achevées, la procédure peut être redémarrée comme suit :

i. Si le PE local a envoyé précédemment un message Transposition d'étiquette, il DOIT envoyer un message Suppression d'étiquette au PE distant et attendre jusqu'à ce qu'il reçoive un message Libération d'étiquette du PE distant.
ii. Le PE local DOIT envoyer un message Libération d'étiquette au PE distant pour l'étiquette spécifique associée à la FEC qui a annoncé ce PW spécifique. Note : les étapes mentionnées ci-dessus de message Libération d'étiquette et de message Suppression d'étiquette ne sont pas obligées d'être exécutées dans une séquence spécifique.
iii. Le PE local DOIT envoyer un message de demande d'étiquette au PE homologue et ensuite DOIT attendre de recevoir un message Transposition d'étiquette contenant la préférence configurée actuellement définie du PE distant sur l'utilisation du mot de contrôle.

Une fois que le PE distant a réussi à traiter le message Suppression d'étiquette et les messages Libération d'étiquette, il va réinitialiser l'automate à états de négociation du bit C et son utilisation du mot de contrôle avec la préférence configurée en local.

À partir de ce point, le PE local et le PE distant vont suivre les procédures de négociation de bit C définies au paragraphe précédent.

Le processus de renégociation de bit C NE DEVRAIT PAS être interrompu avant son achèvement, car des résultats imprévisibles pourraient survenir.

7.4 Considérations de séquençage

Dans le cas où le routeur considère le champ Numéro de séquence dans le mot de contrôle, il est important de noter les détails suivants sur l'annonce des étiquettes.

7.4.1 Annonces d'étiquettes

Après qu'une étiquette a été retirée par le routeur de sortie et/ou libérée par le routeur d'entrée, on doit faire attention de ne pas annoncer (réutiliser) la même étiquette libérée jusqu'à ce que le routeur de sortie puisse être raisonnablement certain que de vieux paquets contenant l'étiquette libérée ne persistent pas dans le réseau à capacité MPLS.

Cette précaution est nécessaire pour empêcher le routeur d'imposition de redémarrer la transmission de paquets avec un numéro de séquence de 1 quand il reçoit un message Transposition d'étiquette qui lie la même FEC à la même étiquette si il y a encore d'anciens paquets dans le réseau avec un numéro de séquence entre 1 et 32768. Par exemple, si il y a un paquet avec un numéro de séquence de n, où n est dans l'intervalle [1, 32768] voyageant dans le réseau, il serait possible que le routeur de disposition reçoive ce paquet après qu'il ait ré-annoncé l'étiquette. Comme l'étiquette a été libérée par le routeur d'imposition, le routeur de disposition DEVRAIT s'attendre à ce que le prochain paquet arrive avec un numéro de séquence de 1. La réception d'un paquet avec un numéro de séquence égal à n va avoir pour résultat que n paquets pourraient être rejetés par le routeur de disposition jusqu'à ce que le routeur d'imposition impose un numéro de séquence de n+1 dans un paquet. Les méthodes possibles pour éviter cela sont que le routeur de disposition annonce toujours une étiquette de PW différente, ou que le routeur de disposition attende un délai suffisant avant de tenter de ré-annoncer une étiquette récemment libérée. Cela ne pose de problème que quand le traitement du numéro de séquence est activé chez le routeur de disposition.

7.4.2 Libération d'étiquette

Dans les situations où le routeur d'imposition veut redémarrer la transmission des paquets avec le numéro de séquence 1, le routeur devra 1) envoyer au routeur de disposition un message Libération d'étiquette, et 2) envoyer au routeur de disposition un message de demande d'étiquette. Quand le séquençage est pris en charge, l'annonce d'une étiquette de PW en réponse à un message de demande d'étiquette DOIT aussi considérer les questions discutées au paragraphe 7.4.1 ("Annonces d'étiquette").

8. Considérations relatives à l'IANA

8.1 Type de TLV LDP

Le présent document utilise plusieurs nouveaux types de TLV LDP ; l'IANA tient déjà un registre intitulé "Espace de noms de type de TLV", défini par la RFC 5036. Les valeurs suivantes ont été allouées dans ledit registre :

Type de TLV	Description
0x096A	TLV État de PW
0x096B	TLV Paramètres d'interface de PW
0x096C	TLV Identifiant de groupe de PW

8.2 Codes d'état LDP

Le présent document utilise plusieurs nouveaux codes d'état de LDP ; l'IANA tient déjà un registre intitulé "Espace de noms de codes d'état", défini par la RFC 5036. Les valeurs suivantes ont été allouées :

Gamme/valeur	E	Description	Référence
0x00000024	0	Bit C illégal	[RFC8077]
0x00000025	0	Mauvais bit C	[RFC8077]
0x00000026	0	Débit binaire incompatible	[RFC8077]
0x00000027	0	Mauvaise configuration de CEP-TDM	[RFC8077]
0x00000028	0	État de PW	[RFC8077]
0x00000029	0	TAI non alloué/non reconnu	[RFC8077]
0x0000002A	0	Erreur générique de mauvaise configuration	[RFC8077]
0x0000002B	0	Retrait d'étiquette de méthode d'état de PW non prise en charge	[RFC8077]

8.3 Espace de noms Type de FEC

Le présent document utilise deux nouveaux types d'élément de FEC, 0x80 et 0x81, dans le registre "Espace de noms de type de classe d'équivalence de transmission (FEC)" pour le protocole de distribution d'étiquettes (LDP) [RFC5036].

9. Considérations sur la sécurité

Le présent document spécifie les extensions à LDP qui sont nécessaires pour établir et maintenir des pseudo filaires. L'objet de l'établissement de pseudo filaires est de permettre aux trames de couche 2 d'être encapsulées dans MPLS et transmises d'une extrémité d'un pseudo filaire à l'autre. Donc, on traite les considérations de sécurité pour à la fois le plan des données et le plan de contrôle.

9.1 Sécurité du plan des données

À l'égard de la sécurité du plan des données, les domaines suivants doivent être considérés :
- inspection de PDU MPLS
- usurpation de PDU MPLS
- altération de PDU MPLS
- sécurité du protocole de PSN MPLS
- sécurité de circuit d'accès
- prévention du déni de service sur les routeurs PE

Quand un PSN MPLS est utilisé pour fournir le service de pseudo filaire, on comprend que la sécurité doit être au moins égale à celle des réseaux actuellement déployés de protocole de couche 2 native que la combinaison de réseau MPLS/PW émule. Cela signifie que le réseau à capacité MPLS DEVRAIT être isolé de l'insertion de paquets provenant de l'extérieur de telle façon qu'il NE DEVRAIT PAS être possible d'insérer directement un paquet MPLS dans le réseau. Pour empêcher l'insertion involontaire de paquet, il est aussi important d'empêcher l'accès physique non autorisé au PSN, ainsi que l'accès administratif non autorisé aux éléments de réseau individuels.

Comme mentionné ci-dessus, un réseau à capacité MPLS ne devrait pas accepter des paquets MPLS provenant de ses interfaces externes (c'est-à-dire, les interfaces aux appareils côté consommateur (CE) ou aux réseaux d'autres fournisseurs) sauf si l'étiquette supérieure du paquet a été légitimement distribuée au système duquel le paquet est reçu. Si l'interface entrante du paquet conduit à un fournisseur de services différent (plutôt qu'à un client) une relation de confiance appropriée doit aussi être présente, incluant la confiance que l'autre fournisseur de service fournit aussi des mesures de sécurité appropriées.

Les trois principaux problèmes de sécurité rencontrés dans l'utilisation d'un réseau à capacité MPLS pour transporter des PW sont l'usurpation, l'altération, et l'inspection. En premier lieu, il y a une possibilité que le PE qui reçoit des PDU de PW obtienne une PDU qui paraît être du PE qui transmet le PW dans le PSN mais n'a en fait pas été transmise par le PE à l'origine du PW. (C'est-à-dire que les encapsulations spécifiées ne permettent pas par elles mêmes au désencapsuleur d'authentifier l'encapsuleur.) Un second problème est la possibilité que la PDU de PW soit altérée entre le moment où elle entre dans le PSN et le moment où elle quitte le PSN (c'est-à-dire, les encapsulations spécifiées n'assurent pas par elles-mêmes au désencapsuleur l'intégrité du paquet.) Un troisième problème est la possibilité que le contenu d'une PDU soit vu pendant que la PDU est en transit à travers le PSN (c'est-à-dire, la spécification des encapsulations n'assure pas la confidentialité.) L'importance de ces problèmes dans la pratique dépend des exigences de sécurité des applications dont le trafic est envoyé à travers le tunnel et du niveau de sécurité du PSN lui-même.

9.2 Sécurité du plan de contrôle

Les considérations générales de sécurité à l'égard de l'utilisation de LDP sont spécifiées à la Section 5 de la [RFC5036]. Ces considérations s'appliquent aussi au cas où LDP est utilisé pour établir des pseudo filaires.

Un pseudo filaire connecte deux circuits de rattachement. Il est important de s'assurer que les connexions LDP ne sont pas acceptées arbitrairement de n'importe où, ou autrement un circuit de rattachement local pourrait être connecté à un circuit de rattachement distant arbitraire. Donc, une demande de session LDP entrante NE DOIT PAS être acceptée si son adresse IP de source n'est pas connue comme étant la source d'un homologue LDP "éligible". L'ensemble des homologues éligibles pourrait être pré configuré (soit comme une liste d'adresses IP soit comme une liste de combinaisons d'adresse/gabarit) ou il

pourrait être découvert de façon dynamique via un protocole d'auto découverte qui soit lui-même de confiance. (Évidemment, si le protocole d'auto découverte n'est pas de confiance, l'ensemble d'homologues éligibles qu'il produit ne pourra pas être de confiance.)

Même si une demande de connexion LDP apparaît comme venant d'un homologue éligible, son adresse de source peut avoir été usurpée. Donc, des moyens d'empêcher l'usurpation d'adresse de source doivent être mis en place. Par exemple, si tous les homologues éligibles sont dans le même réseau, le filtrage d'adresse de source aux routeurs de bordure de ce réseau pourrait éliminer la possibilité d'usurpation d'adresse de source.

L'option de clé d'authentification MD5 de LDP, décrite au paragraphe 2.9 de la [RFC5036], DOIT être mise en œuvre, et pour un degré de sécurité supérieur, elle doit être utilisée. Cela assure l'intégrité et l'authentification des messages LDP et élimine la possibilité d'usurpation d'adresse de source. L'utilisation de l'option MD5 n'assure pas la confidentialité, mais la confidentialité des messages de contrôle LDP n'est généralement pas considérée comme importante. Comme l'option MD5 s'appuie sur la configuration de clés pré-partagées, elle ne donne pas beaucoup de protection contre les attaques en répétition. De plus, sa dépendance aux clés pré-partagées peut rendre très difficile de la déployer quand l'ensemble de voisins éligibles est déterminé par un protocole d'auto-configuration.

Quand l'élément de FEC PWid généralisée est utilisé, il est possible qu'un homologue LDP particulier puisse être un des homologues LDP éligibles mais qu'il ne soit pas le bon à connecter au circuit de rattachement particulier identifié par l'instance particulière d'élément de FEC PWid généralisée. Cependant, étant donné que l'homologue est connu pour être un des homologues éligibles (comme discuté ci-dessus) cela va être le résultat d'une erreur de configuration plutôt qu'un problème de sécurité. Néanmoins, il peut être conseillé à un PE d'associer chacun de ses circuits de rattachement local à un ensemble d'homologues éligibles plutôt que d'avoir juste un seul ensemble d'homologues éligibles associé au PE comme un tout.

10. Interopérabilité et déploiement

Le paragraphe 2.2 de la [RFC6410] spécifie quatre exigences qu'une norme de l'Internet doit respecter. Cette section documente comment le présent document satisfait ces exigences.

La technologie de pseudo filaire a été déployée pour la première fois en 2001 et a été largement déployée par de nombreux transporteurs. La [RFC7079] documente les résultats d'une enquête sur les mises en œuvre de PW avec une attention particulière sur l'usage du mot de contrôle. [EANTC] documente un essai public d'interopérabilité sur plusieurs fabricants d'équipements MPLS et de transporteurs Ethernet, qui incluait des essais de pseudo filaires Ethernet, ATM, et TDM.

Les errata sur la [RFC4447] sont généralement de nature rédactionnelle et ont été traités dans le présent document.

Toutes les caractéristiques de la présente spécification ont été mis en œuvre par plusieurs fabricants.

Aucune revendication d'IPR n'a été faite à l'IETF concernant le présent document, les RFC 4447 ou 6723, ou sur les projets Internet qui ont résulté en les RFC 4447 et 6723.

11. Références

11.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, DOI 10.17487/RFC2119, mars 1997, DOI 10.17487/RFC2119. *(MàJ par* RFC8174)

[RFC3032] E. Rosen et autres, "Codage de pile d'étiquettes MPLS", janvier 2001, DOI 10.17487/RFC3032.

[RFC4446] L. Martini, "Allocations de l'IANA pour l'émulation de bord à bord pseudo filaire (PWE3)", avril 2006. (BCP0116)

[RFC5036] L. Andersson, I. Minei et B. Thomas, éditeurs, "Spécification de LDP", janvier 2001, DOI 10.17487/RFC5036. (*Remplace* RFC3036) (*MàJ par les* RFC6720 , RFC6790, RFC7552,) *(D.S)*

[RFC7358] K. Raza, et autres,"Discipline d'annonce d'étiquette pour les classes d'équivalence de transmission LDP", octobre 2014, DOI 10.17487/RFC7358. *(P.S., MàJ RFC* 3212, 4447, 5036, 5918, 6388, 7140)

11.2 Références pour information

[ANSI] American National Standards Institute, "Telecommunications - Synchronous Optical Network (SONET) - Basic Description Including Multiplex Structures, Rates, and Formats", ANSI T1.105, octobre 1995.

[EANTC] European Advanced Networking Test Center, "MPLS and Carrier Ethernet: Service - Connect - Transport. Public Multi-Vendor Interoperability Test", février 2009.

[G.707] Recommandation UIT-T G.707, "Interface de nœud réseau pour la hiérarchie numérique synchrone (SDH)", mai 1996.

[RFC2277] H. Alvestrand, "Politique de l'IETF en matière de jeux de caractères et de langages", BCP 18, janvier 1998, DOI 10.17487/RFC2227.

[RFC4447] L. Martini et autres, "Établissement et maintenance de pseudo filaires avec le protocole de distribution d'étiquettes", avril 2006, DOI 10.17487/RFC4447. *(P.S. ; Remplacé par* RFC8077 STD 84)

[RFC4448] L. Martini et autres, "Méthodes d'encapsulation pour le transport d'Ethernet sur des réseaux MPLS", avril 2006, DOI 10.17487/RFC4448. *(P.S. ; MàJ par* RFC8469)

[RFC4553] A. Vainshtein et autres, "Multiplexage de paquet à répartition dans le temps ignorant la structure (SAToP)", juin 2006, DOI 10.17487/RFC4553. (*P.S.)*

[RFC4618] L. Martini et autres, "Méthodes d'encapsulation pour le transport du contrôle de liaisons de données en PPP/haut-niveau (HDLC) sur réseaux MPLS", septembre 2006, DOI 10.17487/RFC4618. *(P.S.)*

[RFC4619] L. Martini et autres, "Méthodes d'encapsulation pour le transport de relais de trame sur les réseaux de commutation d'étiquettes multiprotocoles (MPLS)", septembre 2006, DOI 10.17487/RFC4619. *(P.S.)*

[RFC4717] L. Martini et autres, "Méthodes d'encapsulation pour le transport de mode de transfert asynchrone (ATM) sur réseaux MPLS", décembre 2006, DOI 10.17487/RFC4717. *(P.S.)*

[RFC4842] A. Malis et autres, "Émulation de circuit sur paquet (CEP) en réseau optique synchrone/hiérarchie numérique synchrone (SONET/SDH)", avril 2007, DOI 10.17487/RFC4842. *(Remplacé par* RFC5143) *(P.S.)*

[RFC6410] R. Housley, D. Crocker, E. Burger, "Réduction de la voie de la normalisation à deux niveaux de maturité", octobre 2011, DOI 10.17487/RFC6410. (*MàJ la* RFC2026) (BCP009)

[RFC6723] L. Jin, et autres, "Mise à jour du mécanisme de négociation du mot de contrôle de pseudo fil", septembre 2012, DOI 10.17487/RFC6723. (*MàJ les* RFC4447, RFC6073) *(P.S. ; Remplacé par* RFC8077 STD 84)

[RFC7079] N. Del Regno, A. Malis, "Résultats de l'enquête sur la mise en œuvre de pseudo câblage (PW) et de connexité de circuit virtuel (VCCV)", novembre 2013, DOI 10.17487/RFC7079. *(Information)*

Remerciements

Les auteurs souhaitent remercier de leurs contributions Vach Kompella, Vanson Lim, Wei Luo, Himanshu Shah, et Nick Weeds. Ils remercient de leur contribution les auteurs de la RFC 6723, dont le travail a été incorporé dans le présent document : Lizhong Jin, Raymond Key, Simon Delord, Tom Nadeau, et Sami Boutros.

Contributeurs

Les personnes suivantes ont été les auteurs ou auteurs contributeurs de la RFC 4447. Ils sont mentionnés ici en

reconnaissance de leur travail sur ce document.

Nasser El-Aawar
Level 3 Communications, LLC.
1025 Eldorado Blvd.
Broomfield, CO 80021
United States of America
mél : nna@level3.net

Eric C. Rosen
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
United States of America
mél : erosen@cisco.com

Dan Tappan
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
United States of America
mél : tappan@cisco.com

Toby Smith
Google
6425 Penn Ave. #700
Pittsburgh, PA 15206
United States of America
mél : tob@google.com

Dimitri Vlachos
Riverbed Technology
mél : dimitri@riverbed.com

Jayakumar Jayakumar
Cisco Systems Inc.
3800 Zanker Road, MS-SJ02/2
San Jose, CA 95134
United States of America
mél : jjayakum@cisco.com

Alex Hamilton,
Cisco Systems Inc.
485 East Tasman Drive, MS-SJC07/3
San Jose, CA 95134
United States of America
mél : tahamilt@cisco.com

Steve Vogelsang
ECI Telecom
Omega Corporate Center
1300 Omega Drive
Pittsburgh, PA 15205
mél : stephen.vogelsang@ecitele.com

John Shirron
ECI Telecom
Omega Corporate Center
1300 Omega Drive
Pittsburgh, PA 15205
mél : john.shirron@ecitele.com

Andrew G. Malis
Verizon
60 Sylvan Rd.
Waltham, MA 02451
United States of America
mél : andrew.g.malis@verizon.com

Vinai Sirkay
Reliance Infocomm
Dhirubai Ambani Knowledge City
Navi Mumbai 400 709
India
mél : vinai@sirkay.com

Vasile Radoaca
Nortel Networks
600 Technology Park
Billerica MA 01821
United States of America
mél : vasile@nortelnetworks.com

Chris Liljenstolpe
149 Santa Monica Way
San Francisco, CA 94127
United States of America
mél : ietf@cdl.asgaard.org

Dave Cooper
Global Crossing
960 Hamlin Court
Sunnyvale, CA 94089
United States of America
mél : dcooper@gblx.net

Kireeti Kompella
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089
United States of America
mél : kireeti@juniper.net

Adresse des éditeurs

Luca Martini
Cisco Systems, Inc.
1899 Wynkoop Street, Suite 600
Denver, CO 80202
United States of America
mél : lmartini@monoski.com

Giles Heron
Cisco Systems
10 New Square
Bedfont Lakes, Feltham
Middlesex
TW14 8HA
United Kingdom
mél : giheron@cisco.com