Groupe de travail Réseau
Request for Comments : 1990
RFC rendue obsolète : 1717
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

K. Sklower, University of California, Berkeley
B. Lloyd, G. McGregor, Lloyd Internetworking
D. Carr, Newbridge Networks Corporation
T. Coradetti, Sidewalk Software
août 1996

Protocole PPP multiliaison (MP)

Statut du présent mémoire
Le présent mémoire définit un protocole expérimental pour la communauté Internet. Il ne spécifie en aucune façon une norme Internet. Il invite à discussion et suggestions pour son amélioration. La distribution de ce mémo n'est pas limitée.

Résumé
Le présent document propose une méthode pour séparer, recombiner et mettre en séquence les datagrammes à travers des liaisons de données logiques multiples. Ce travail était à l'origine motivé par le désir d'exploiter plusieurs canaux support en RNIS, mais il est également applicable à toute situation dans laquelle plusieurs liaisons PPP connectent deux systèmes, y compris des liaisons asynchrones. Ceci est réalisé au moyen de nouvelles options et protocoles PPP [2].

Les différences entre la spécification PPP multiliaison actuelle (RFC 1717) et le présent mémo sont expliquées à la Section 11. Tout système mettant en œuvre les contraintes supplémentaires exigées par le présent mémoire sera compatible en amont avec les mises en œuvre conformes à la RFC 1717.

Remerciements
Les auteurs souhaitent remercier tout particulièrement Fred Baker de ACC, Craig Fox de Network Systems, Gerry Meyer de Spider Systems, Dan Brennan de Penril Datability Networks, Vernon Schryver de SGI (pour la discussion très complète sur le bourrage) et les membres des groupes de travail IP sur grands réseaux de données publics et Extensions PPP, pour les très utiles discussions sur le sujet.

Table des matières

1 Introduction

1.1 Exposé des motifs

Le débit de base et le débit primaire du RNIS offrent tous deux la possibilité d'ouvrir plusieurs canaux simultanés entre des systèmes, ce qui donne aux utilisateurs de la bande passante supplémentaire à la demande (pour un surcoût). Les propositions précédentes pour la transmission des protocoles Internet sur RNIS ont fixé comme objectif la capacité à utiliser cette facilité (par exemple, Leifer et al., [1]).

Des propositions ont été formulées pour assurer la synchronisation entre plusieurs flux au niveau binaire (les propositions BONDING) ; de telles caractéristiques ne sont pas encore très largement déployées, et elles pourraient exiger des matériels supplémentaires pour le système d'extrémité. Et donc il peut être utile d'avoir une solution purement logicielle, ou tout au moins une disposition intermédiaire.

Il y a d'autres instances où la bande passante à la demande peut être exploitée, comme l'utilisation d'une ligne téléphonique asynchrone à 28 800 baud pour sécuriser une ligne louée synchrone, ou d'ouvrir des SVC X.25 supplémentaires lorsque la taille de fenêtre est limitée à deux par un accord international.

Les algorithmes les plus simples possibles d'alternance des paquets entre les canaux sur la base de l'espace disponible (qu'on pourrait appeler l'algorithme du guichet bancaire automatique) peuvent avoir des effets secondaires indésirables du fait du réarragement des paquets.

Au moyen d'un en-tête de séquençage de quatre octets et de règles de synchronisation simples, on peut partager les paquets entre des circuits virtuels parallèles entre les systèmes d'une façon telle que l'ordre des paquets ne soit pas changé, ou tout au moins, que la probabilité que cela arrive soit réduite.

1.2. Description fonctionnelle

La méthode exposée ici est similaire à celle du protocole multiliaison décrit dans la norme ISO 7776 [4], mais offre la capacité supplémentaire de partager et recombiner les paquets, réduisant ainsi le délai de latence, et avec un potentiel d'augmentation de l'unité de réception maximale (MRU) effective. De plus, il n'y a pas ici d'exigence de fonctionnement avec accusé de réception de la couche de liaison, bien que cela soit autorisé en option.

Multiliaison se fonde sur une négociation de l'option LCP qui permet à un système d'indiquer à ses homologues qu'il est capable de combiner plusieurs liaisons physiques en un "faisceau". C'est seulement dans des conditions exceptionnelles qu'une paire de systèmes exigera le fonctionnement de plus d'un faisceau pour les connecter.

Multiliaison est négocié durant la négociation initiale de l'option LCP. Un système indique à son homologue qu'il souhaite faire une multiliaison en envoyant l'option multiliaison au titre de la négociation initiale de l'option LCP. Cette négociation indique trois choses :

1. Le système offrant l'option est capable de combiner plusieurs liaisons physiques en une seule liaison logique ;

2. Le système est capable de recevoir des unités de données de protocole (PDU) de couche supérieure fragmentées en utilisant l'en-tête multiliaison (décrit plus loin) et de ré assembler les fragments dans la PDU d'origine pour le traitement ;

3. Le système est capable de recevoir des PDU de N octets de taille où N est spécifié au titre de l'option même si N est plus grand que l'unité de réception maximale (MRU) pour une seule liaison physique.

Une fois réussie la négociation de la multiliaison, le système d'envoi a toute liberté pour expédier des PDU enchâssées et/ou fragmentées avec l'en-tête multiliaison.

1.3 Conventions

Les conventions de langage suivantes sont utilisées dans les éléments de spécification du présent document :
DOIT ou OBLIGATOIRE – l'élément est une exigence absolue de la spécification.
DEVRAIT ou RECOMMANDE – l'élément devrait généralement être suivi sauf circonstances exceptionnelles.

PEUT ou FACULTATIF – l'élément est vraiment facultatif et peut être suivi ou ignoré selon les besoins de la mise en œuvre.

2. Généralités

Pour établir des communications sur une liaison point à point, chaque extrémité de la liaison PPP doit d'abord envoyer des paquets LCP pour configurer la liaison des données durant la phase d'établissement de liaison. Après l'établissement de la liaison, PPP fournit une phase d'authentification dans laquelle les protocoles d'authentification peuvent être utilisés pour déterminer les identifiants associés à chaque système connecté par la liaison.

L'objectif d'une opération multiliaison est de coordonner plusieurs liaisons indépendantes entre une paire fixe de systèmes, fournissant une liaison virtuelle avec une plus grande bande passante que celle d'aucun de ses membres constitutifs. La liaison agrégée, ou faisceau, est nommé par la paire des identifiants des deux systèmes connectés par les liaisons. Un identifiant de système peut inclure des informations fournies par l'authentification PPP [3] et des informations fournies par la négociation LCP. Les liaisons en faisceau peuvent être différentes liaisons physiques, comme dans des lignes asynchrones multiples, mais peuvent aussi être des instances de liaisons multiplexées, comme du RNIS, du X.25 ou du relais de trame. Les liaisons peuvent aussi être de différentes sortes, comme un appariement de liaisons téléphoniques asynchrones avec des lignes louées synchrones.

On suggère que le fonctionnement multiliaison soit modélisé comme une entité virtuelle PPP de couche liaison des données dans laquelle les paquets reçus sur différentes entités physiques de couche liaison sont identifiés comme appartenant à un protocole réseau PPP distinct (le protocole multiliaison, ou MP) et recombinés et mis en séquence conformément aux informations présentes dans un en-tête de fragmentation multiliaison. Tous les paquets reçus sur des liaisons identifiées comme appartenant à un arrangement multiliaison sont présentées à la même machine de traitement de protocole de couche réseau, qu'ils aient des en-tête multiliaison ou non.

Les paquets à transmettre en utilisant les procédures multiliaison sont incorporés conformément aux règles de PPP dans lesquelles les options suivantes seront à configurer manuellement :

Pas de transposition de caractère de contrôle asynchrone
Pas de numéro magique
Pas de surveillance de qualité de liaison
Compression d'adresse et de champ de contrôle
Compression de champ de protocole
Pas de trames composées
Pas de bourrage auto-décrit

Selon les règles spécifiées dans la RFC1661, cela signifie qu'une mise en œuvre DOIT accepter les paquets ré assemblés avec et sans zéros en tête présents dans le champ Protocole du paquet réassemblé. Bien qu'il soit explicitement interdit ci-dessous d'inclure les champs Adresse et Contrôle (habituellement, les deux octets FF 03) dans le tissu à fragmenter, il est d'une bonne pratique de programmation défensive d'accepter le paquet de toutes façons, en ignorant les deux octets s'ils sont présents, car c'est ce que spécifie la RFC1661.

Par politesse pour les mises en œuvre qui fonctionnent mieux en présence d'un verrouillage assuré, il est suggéré de déterminer lors de la création d'un faisceau si on doit transmettre les zéros figurant en tête en examinant si PFC a été négocié sur la première liaison admise dans un faisceau. Cette détermination devrait rester en vigueur tant que perdure un faisceau.

Bien sûr, il est permis aux liaisons individuelles d'avoir différents réglages pour ces options. Comme décrit ci-dessous, les liaisons membres DEVRAIENT négocier le bourrage auto-décrit, même si les paquets pré-fragmentés NE DOIVENT PAS avoir de bourrage. Comme le mode Compression de champ de protocole sur la liaison membre permet à un système expéditeur d'inclure ou non à sa discrétion un octet de tête de zéro, c'est un mécanisme de remplacement pour générer des paquets de longueur égale.

Les négociations LCP ne sont pas permises sur le faisceau lui-même. Une mise en œuvre NE DOIT PAS transmettre de paquets de demande-de-configuration LCP, ni rejet-, accusé-de-réception, non-accusé-de-réception, demande–de-terminaison, ou accusé-de-réception via la procédure multiliaison, et une mise en œuvre les recevant DOIT les supprimer en silence. (Par "suppression en silence" on veut dire de ne pas générer de paquets PPP en réponse ; une mise en œuvre est libre de générer une entrée de registre pour enregistrer la réception du paquet inattendu). A l'opposé, d'autres paquets LCP qui ont des fonctions de contrôle non associées au changement des réglages par défaut pour le faisceau lui-même sont permis. Une mise en oeuvre PEUT transmettre des paquets LCP Rejet-de-code, Rejet-de-protocole, Demande-d'écho, Réponse-d'écho et Demande-de-suppression.

L'unité MTU effective pour l'entité de liaison logique est négociée via une option LCP. Il importe peu que les paquets de protocole de contrôle réseau soient incorporés dans des en-têtes multiliaison ou non, ou même de savoir sur quelle liaison ils sont envoyés, du moment que cette liaison s'identifie comme appartenant à un arrangement multiliaison.

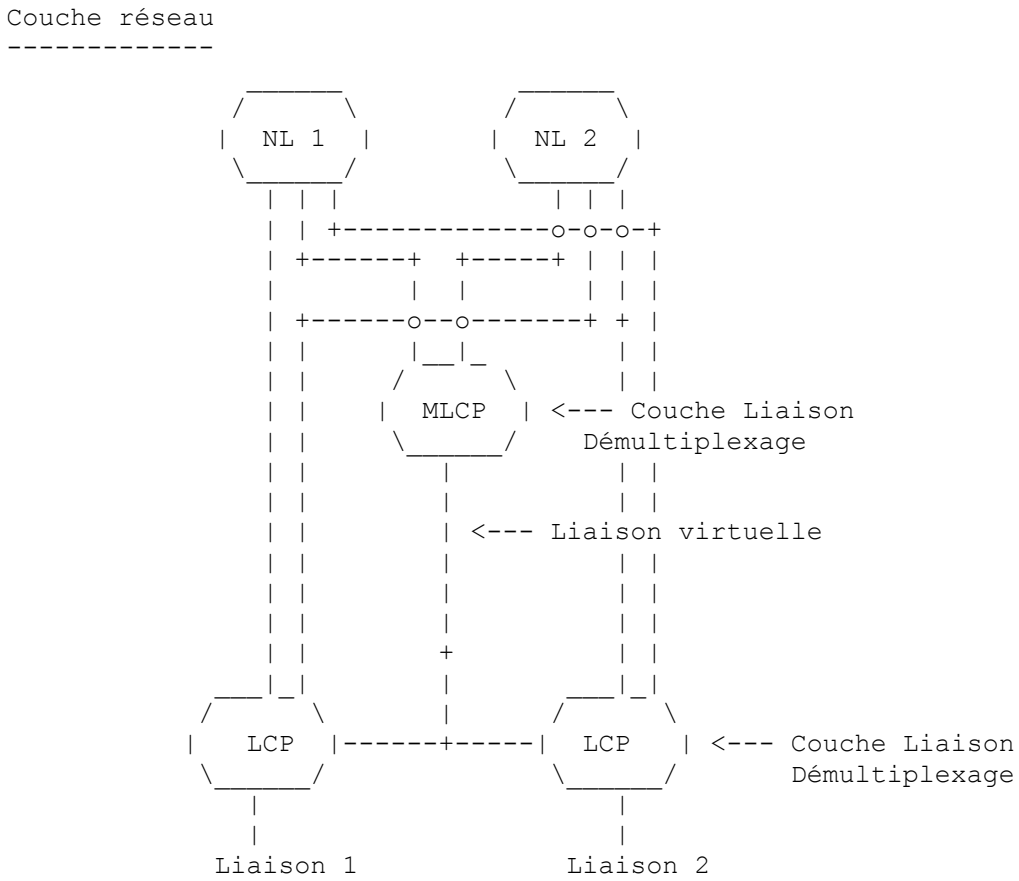
Noter que les protocoles réseau qui ne sont pas envoyés à l'aide d'en-têtes multiliaison ne peuvent pas être mis en séquence. (Et par conséquent, ne seront pas délivrés d'une façon convenable).

Par exemple, considérons le cas de la Figure 1. La liaison 1 a négocié les couches réseau NL 1, NL 2, et MP entre deux systèmes. Les deux systèmes négocient alors MP sur la liaison 2.

Les trames reçues sur la liaison 1 sont démultiplexées à la couche de liaison des données conformément à l'identifiant de protocole réseau PPP et peuvent être envoyées à NL 1, NL 2, ou MP. La liaison 2 acceptera des trames avec tous les identifiants de protocole réseau qu'accepte la liaison 1.

Les trames reçues par MP sont ensuite démultiplexées à la couche réseau conformément à l'identifiant de protocole réseau PPP et envoyées à NL 1 ou NL 2. Toute trame reçue par MP pour tout autre protocole de couche réseau sera rejetée en utilisant le mécanisme de rejet de protocole normal.

Figure 1. Vue d'ensemble du multiliaison



3. Formats de paquet

La présente section décrit la disposition des fragments individuels, qui sont les "paquets" dans le protocole multiliaison. Les paquets de protocole réseau sont d'abord incorporés (mais non mis en trame) conformément aux procédures PPP normales, et les grands paquets sont coupés en plusieurs segments dimensionnée de façon appropriée pour les différentes liaisons physiques. Bien que ce soit par ailleurs permis par les spécifications PPP, les mises en œuvre NE DOIVENT PAS inclure le champ Adresse et Contrôle dans l'entité logique à fragmenter. Un nouvel en-tête PPP, comportant l'identifiant de protocole multiliaison et l'en-tête multiliaison, est inséré avant chaque section. (Et donc le premier fragment d'un paquet multiliaison en PPP aura deux en-têtes, un pour le fragment, suivi par l'en-tête pour le paquet lui-même.)

Les systèmes qui mettent en œuvre la procédure multiliaison ne sont pas obligés de fragmenter les petits paquets. Il n'est pas non plus exigé que les segments soient de taille égale, ou que les paquets soient fractionnés du tout. Une stratégie possible pour s'accommoder de liaisons membres ayant des débits de transmission différents serait de diviser les paquets en segments proportionnels aux débits de transmission. Une autre stratégie pourrait être de les diviser en nombreux fragments égaux et de distribuer plusieurs fragments par liaison, leur nombre étant proportionnel aux vitesses relatives des liaisons.

Les fragments multiliaison PPP sont incorporés en utilisant l'identifiant de protocole 0x00-0x3d. À la suite de l'identifiant de protocole se trouve un en-tête de quatre octets qui contient un numéro de séquence et deux champs d'un bit qui indiquent que le fragment commence ou termine un paquet. Après la négociation d'une option LCP PPP supplémentaire, l'en-tête de quatre octets peut facultativement être remplacé par un en-tête de deux octets avec seulement un espace de séquence de 12 bits. La compression d'Adresse & Contrôle et d'ID de protocole est supposée être activée. Les fragments individuels auront donc le format suivant :

Figure 2 : Format de fragment à numéro de séquence long

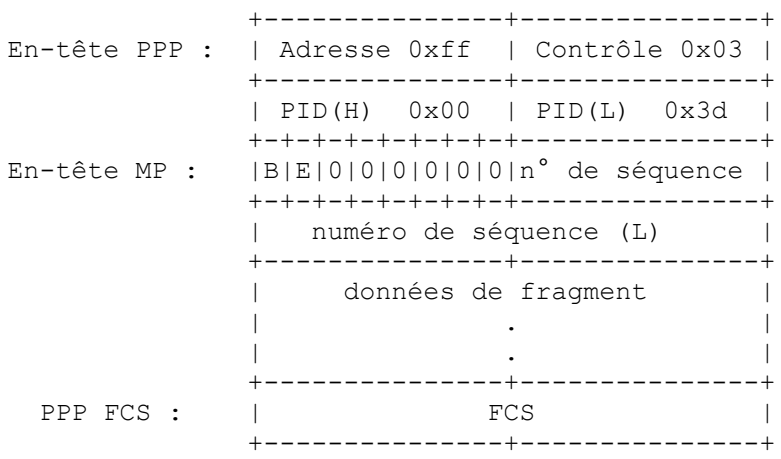
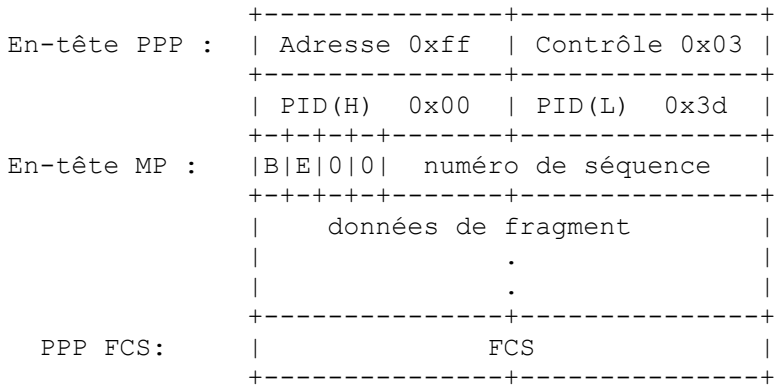


Figure 3 : Format de fragment à numéro de séquence court



Le bit de début *[(B)eginning]* de fragment est un champ d'un bit mis à 1 sur le premier fragment provenant d'un paquet PPP et mis à 0 pour tous les autres du même paquet PPP.

Le bit de fin *[(E)nding]* de fragment est un champ d'un bit mis à 1 sur le dernier fragment et mis à 0 pour tous les autres fragments. Un fragment peut avoir les deux bits de fragment (B)eginning et (E)nding mis à 1.

Le champ de séquence est un nombre de 24 bits ou de 12 bits qui est incrémenté pour chaque fragment transmis. Par défaut, le champ de séquence est long de 24 bits, mais il peut être négocié à seulement 12 bits avec une option de configuration LCP décrite ci-dessous.

Entre le bit de fin *[(E)nding]* de fragment et le numéro de séquence se trouve un champ réservé, dont l'utilisation n'est pas définie actuellement, qui DOIT être mis à zéro. Il est long de 2 bits lorsque l'utilisation des numéros de séquence courts a été négociée, et de 6 bits autrement.

Dans ce protocole multiliaison, une seule structure de réassemblage est associée au faisceau. Les en-têtes multiliaison sont interprétés dans le contexte de cette structure.

Le champ FCS indiqué dans le diagramme est hérité du mécanisme de tramage normal provenant de la liaison membre sur laquelle le paquet est transmis. Il n'y a pas de FCS distinct appliqué au paquet reconstitué comme un tout s'il est transmis dans plus d'un fragment.

3.1 Considérations sur le bourrage

Les systèmes qui prennent en charge le protocole multiliaison DEVRAIENT mettre en œuvre le bourrage auto-décrit. Un système qui met en œuvre le bourrage auto-décrit va par définition inclure l'option bourrage dans ses Demandes-de-configuration LCP initiales, ou (pour éviter le délai d'un Rejet-de-configuration) inclure l'option bourrage après réception d'un NAK contenant l'option.

Un système qui doit faire un bourrage sur ses propres émissions mais qui n'utilise pas le bourrage auto-décrit lorsqu'il n'utilise pas le multiliaison PEUT continuer à ne pas utiliser le bourrage auto-décrit s'il s'assure par un choix très soigneux des longueurs de fragment que seuls les fragments de fin des paquets sont bourrés. Un système NE DOIT PAS ajouter de bourrage à un paquet qui ne peut pas être reconnu comme bourré par l'homologue. Les fragments non terminaux NE DOIVENT PAS être bourrés avec du matériel en queue par toute autre méthode que le bourrage auto-décrit.

Un système DOIT s'assurer que le bourrage auto-décrit tel que décrit dans la RFC 1570 [11] est négocié sur la liaison individuelle avant de transmettre aucun paquet de données multiliaison s'il devait bourrer des fragments non-terminaux ou s'il devait utiliser des protocoles réseau ou de compression qui sont vulnérables au bourrage, comme décrit dans la RFC 1570. Si nécessaire, le système qui ajoute le bourrage DOIT utiliser le NAK-de-configuration de LCP pour obtenir une Demande-de-configuration pour le bourrage auto-décrit de la part de son homologue.

Noter que les Demandes-de-configuration de LCP peuvent être envoyées à tout moment sur toute liaison, et que l'homologue répondra toujours avec son propre Demande-de-configuration. Un système qui pratique le bourrage sur ses transmissions mais n'utilise pas de protocole autre que multiliaison qui soit vulnérable au bourrage PEUT utiliser un délai pour s'assurer que l'homologue a fait une Demande-de-configuration pour le bourrage auto-décrit jusqu'à ce qu'il lui paraisse désirable de négocier l'utilisation de multiliaison lui-même. Cela permet l'interopérabilité d'un système qui pratique le bourrage avec des homologues plus anciens qui ne prennent en charge ni multiliaison ni bourrage auto-décrit.

4 Espace de mémoire tampon contre perte de fragment

Dans une procédure multiliaison, un canal peut être retardé par rapport aux autres canaux du faisceau. Cela peut conduire à déranger l'ordre des fragments, accroissant par là la difficulté de détecter la perte d'un fragment. L'estimation de l'espace nécessaire pour la mise en mémoire tampon sur le récepteur en est rendue plus compliquée. Dans la présente section, nous exposons une technique de déclaration de perte d'un fragment, dans l'intention de minimiser la quantité d'espace de mémoire tampon nécessaire, en commençant par minimiser le nombre de pertes de paquet disponibles.

4.1 Détection de perte de fragment

Sur chaque liaison membre d'un faisceau, l'expéditeur DOIT transmettre les fragments avec des numéros de séquence strictement croissants (modulo la taille de l'espace de la séquence). Cette exigence prend en charge une stratégie du récepteur consistant à détecter les fragments perdus sur la base de la comparaison des numéros de séquence. Le numéro de séquence n'est pas remis à zéro à chaque nouveau paquet PPP, et un numéro de séquence est consommé même pour les fragments qui contiennent un paquet PPP entier, c'est-à-dire, un paquet dans lequel les bits de début *[(B)eginning]* et de fin *[(E)nding]* sont établis.

Une mise en œuvre DOIT mettre à zéro le numéro de séquence du premier fragment transmis d'un faisceau nouvellement construit. (Joindre une liaison secondaire à un faisceau existant est invisible pour le protocole, et une mise en œuvre NE DOIT PAS remettre le numéro de séquence à zéro dans cette situation).

Le récepteur garde trace des numéros de séquence entrants sur chaque liaison du faisceau et surveille le minimum actuel du numéro de séquence le plus récent parmi toutes les liaisons membres du faisceau (appelons le M). Le récepteur détecte la fin d'un paquet lorsqu'il reçoit un fragment portant le bit de fin *[(E)nding]*. Le réassemblage du paquet est terminé si tous les numéros de séquence jusqu'à ce fragment ont été reçus.

Un fragment perdu est détecté lorsque M avance au-delà du numéro de séquence d'un fragment portant un bit de fin *[(E)nding]* d'un paquet qui n'a pas été complètement réassemblé (c'est-à-dire, que tous les numéros de séquence entre le

fragment portant le bit de début et le fragment portant le bit de fin n'ont pas été reçus). Cela est causé par la règle des numéros de séquence croissants sur le faisceau. Tout numéro de séquence ainsi détecté est supposé correspondre à un fragment perdu.

Une mise en œuvre DOIT supposer que si un fragment porte un bit de début, le fragment précédemment numéroté portait un bit de fin. Si donc un paquet qui porte le bit de fin est perdu, et si le paquet dont le numéro de fragment est M contient un bit de début, la mise en œuvre DOIT supprimer les fragments pour tous les paquets non assemblés jusqu'à M-1, mais NE DEVRAIT PAS supprimer les fragments portant le nouveau bit de début sur ce seul fondement.

La détection d'un fragment perdu, dont le numéro de séquence a été déduit comme étant U, cause la suppression par le récepteur de tous les fragments jusqu'au fragment ayant le plus faible numéro de fragment avec un bit de fin (qui peut être déduit) supérieur ou égal à U. Cependant, la quantité M peut sauter au milieu d'une chaîne de paquets ayant été complétés avec succès.

Les fragments peuvent être perdus par suite de la corruption de paquets individuels ou d'une perte catastrophique de la liaison (qui peut ne survenir que dans une seule direction). La précédente version du protocole multiliaison ne rend obligatoire aucune procédure spécifique pour la détection de liaisons défaillantes. Le dispositif de gestion de la qualité de liaison PPP, ou la production périodique de demandes d'écho LCP, pourrait être utilisé pour ce faire.

Les expéditeurs DEVRAIENT éviter de conserver des liaisons membres inactives, afin de maximiser la détection précoce des fragments perdus par le récepteur, car la valeur de M n'est pas incrémentée sur les liaisons inactives. Pour éviter les liaisons inactives, les expéditeurs DEVRAIENT faire tourner le trafic parmi les liaisons membres s'il n'y a pas un trafic suffisant pour déborder la capacité d'une liaison.

La perte du fragment final d'une transmission peut causer le calage du récepteur jusqu'à l'arrivée de nouveaux paquets. La probabilité que cela arrive peut être diminuée en envoyant un fragment nul à chaque liaison membre d'un faisceau qui autrement deviendrait inactive immédiatement après avoir transmis un fragment portant le bit de fin. Un fragment nul est un fragment qui consiste seulement en un en-tête multiliaison portant à la fois le bit de début et le bit de fin (c'est-à-dire, qui n'a pas de charge utile). Les mises en œuvre concernées par le problème soit de perdre de la bande passante soit d'augmenter le coût des paquets ne sont pas obligées d'envoyer des fragments nuls et peuvent choisir de différer leur envoi jusqu'à l'arrivée à expiration d'un temporisateur, avec l'augmentation marginale possible de calages plus longs au récepteur. Le récepteur DEVRAIT mettre en œuvre un type de temporisateur d'inactivité de liaison pour se protéger contre des calages de durée indéfinie.

La règle de l'augmentation du numéro de séquence liaison par liaison interdit la réallocation à une liaison active des fragments en file d'attente derrière une liaison défaillante, pratique qui n'est pas inhabituelle pour les mises en œuvres de multiliaison ISO sur LAPB [4].

4.2 Exigences d'espace de mémoire tampon

Aucune quantité de mémoire tampon ne peut garantir une détection correcte de la perte de fragment, car un homologue adverse peut retenir un fragment sur un canal et envoyer des quantités arbitraires sur les autres. Pour le cas habituel où tous les canaux transmettent, on peut aussi montrer qu'il y a une quantité minimum en dessous de laquelle on ne peut pas détecter correctement la perte de paquet. La quantité dépend du délai relatif entre les canaux, (D[canal-i,canal-j]), du débit de données de chaque canal, R[c], de la taille maximum de fragment permise sur chaque canal, F[c], et de la quantité totale de mémoire tampon que l'émetteur a alloué parmi les canaux.

Lorsqu'on utilise PPP, le délai entre les canaux pourrait être estimé en utilisant la demande d'écho LCP et les paquets de réponse d'écho. (Dans le cas de liaisons ayant des débits de transmission différents, le temps d'aller-retour pourrait être réglé pour en tenir compte.) Le décalage pour chaque canal est défini comme la bande passante fois le délai pour ce canal par rapport au canal qui a le plus long délai, S[c] = R[c] * D[c,c-pire]. (S[c-pire] sera zéro, bien sûr !)

Une situation qui pourrait exacerber le biais des numéros de séquence serait celle dans laquelle un trafic est soumis à des salves extrêmes (permettant à presque tous les canaux d'en écouler) et où l'émetteur mettrait d'abord en file d'attente autant de paquets numérotés consécutivement sur une liaison qu'il le peut, puis de mettre en file d'attente le lot suivant sur une seconde liaison, et ainsi de suite. Comme les émetteurs doivent être capables de mettre en mémoire tampon au moins un fragment de taille maximum pour chaque liaison (et qu'il vont habituellement en mettre au moins deux en mémoire) un récepteur qui alloue moins que S[1] + S[2] + ... + S[N] + F[1] + ... + F[N] courra le risque de faire de mauvaises hypothèses sur les pertes de paquet, et donc, il DEVRAIT allouer au moins deux fois cela.

5 Extensions du protocole de commande de liaison PPP

Si on souhaite un fonctionnement fiable de multiliaison, la transmission PPP fiable [6] (essentiellement par l'utilisation de LAPB de l'ISO) DOIT être négociée préalablement à l'utilisation du protocole multiliaison sur chaque liaison membre.

Qu'une livraison fiable soit utilisée ou non sur les liaisons membres, une mise en oeuvre DOIT présenter un signal aux protocoles NCP tournant sur l'arrangement multiliaison comme quoi une perte est survenue.

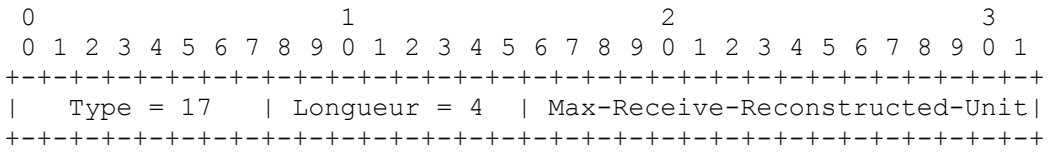
La compression peut être utilisée séparément sur chaque liaison membre, ou tourner sur le faisceau (comme une liaison de groupe logique). L'utilisation de plusieurs flux de compression au-dessous du faisceau (c'est-à-dire sur chaque liaison séparément) est indiquée en faisant tourner le protocole de commande de compression [5] mais avec un ID de protocole PPP de remplacement.

5.1 Types d'option de configuration

Le protocole multiliaison introduit l'utilisation d'options de configuration LCP supplémentaires :
Unité reconstruite de réception multiliaison maximum
Format d'en-tête de numéro de séquence multiliaison court
Discriminant de point d'extrémité.

5.1.1 Option LCP MRRU multiliaison

Figure 4 : Option LCP MRRU multiliaison



La présence de cette option LCP indique que le système qui l'envoie met en œuvre le protocole multiliaison PPP. Si elle n'est pas rejetée, le système va interpréter tous les paquets reçus sur cette liaison comme pouvant être traités par une machine de protocole commune avec tout autre paquet reçu du même homologue sur toute autre liaison sur laquelle cette option a été acceptée.

Le champ d'unité maximum de reconstruction reçue (MRRU, *Max-Receive-Reconstructed-Unit*) est de deux octets, et il spécifie le nombre maximum d'octets dans les champs d'information des paquets réassemblés. Un système DOIT être capable de recevoir la totalité des 1500 octets de champ d'information de tout paquet PPP réassemblé, bien qu'il PUISSE essayer de négocier un valeur plus petite ou plus grande. Le nombre 1500 qui figure ici provient de la spécification de l'option LCP de MRU dans PPP ; si cette exigence devait changer dans une future version de la RFC 1661, les mêmes règles s'appliqueraient ici.

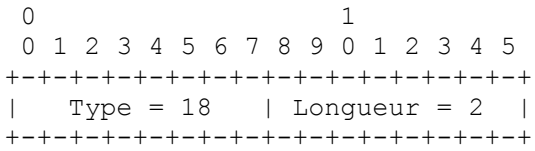
Un système DOIT inclure l'option MRU de LCP dans toute négociation LCP destinée à créer un faisceau ou à se joindre à un faisceau existant. Si l'option MRRU de LCP est offerte sur une liaison qui est destinée à se joindre à un faisceau existant, un système DOIT offrir la même valeur d'unité maximum de reconstruction reçue que précédemment négocié pour le faisceau.

Un système NE DOIT PAS envoyer de paquet multiliaison sur une liaison à moins que son homologue n'ait offert l'option LCP MMRU et que le système n'ait envoyé d'accusé de réception de configuration durant la plus récente négociation LCP sur cette liaison. Un système PEUT inclure l'option LCP MMRU dans un configure-NAK, si son homologue ne l'a pas offert (jusqu'à ce que, conformément aux règles PPP, l'homologue envoie un Rejet-de-configuration).

Note : La valeur de MRRU portée dans cette option correspond à la MRU du faisceau lorsque conçue comme une entité PPP ; mais les règles pour l'option MRRU multiliaison sont différentes de l'option MRU de LCP, car des valeurs DOIVENT être proposées dans chaque négociation LCP, et la confirmation de cette option est exigée avant l'interprétation multiliaison.

5.1.2 Option de format d'en-tête de numéro de séquence court

Figure 5 : Option de format d'en-tête de numéro de séquence court

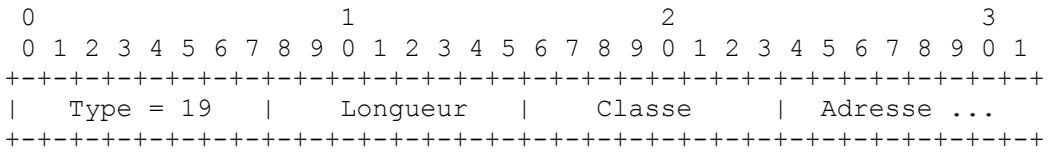


Cette option informe l'homologue que la mise en œuvre souhaite recevoir des fragments avec des numéros de séquence courts, de 12 bits. Lorsqu'un système homologue envoie un accusé de réception de configuration de cette option, il DOIT transmettre tous les paquets multiliaison sur toutes les liaisons du faisceau avec des numéros de séquence de 12 bits ou envoyer un Rejet-de-configuration de cette option. Si des numéros de séquence de 12 bits sont souhaités, cette option DOIT être négociée lors de la création du faisceau, et elle DOIT être explicitement incluse dans chaque demande de configuration LCP proposée par un système lorsqu'il entend inclure cette liaison dans un faisceau existant en utilisant des numéros de séquence à 12 bits. Si cette option n'est jamais négociée durant la vie d'un faisceau, les numéros de séquence sont longs de 24 bits.

Une mise en œuvre qui souhaite transmettre des fragments multiliaison avec des numéros de séquence courts PEUT inclure le numéro de séquence multiliaison court dans un configure-NAK pour demander que l'homologue réponde par une demande de réception de numéros de séquence courts. L'homologue n'est pas obligé de répondre par l'option.

5.1.3 Option de discriminant de point d'extrémité

Figure 7 : Option de discriminant de point d'extrémité



L'option de discriminant de point d'extrémité représente l'identification du système qui transmet le paquet. Cette option indique à un système que l'homologue sur cette liaison pourrait être le même que l'homologue sur une autre liaison existante. Si l'option distingue cet homologue de tous les autres, un nouveau faisceau DOIT être établi à partir de la liaison sur laquelle s'effectue la négociation. Si cette option correspond à la classe et adresse d'un homologue sur une liaison existante, la nouvelle liaison DOIT être jointe au faisceau qui contient la liaison avec l'homologue correspondant, ou DOIT établir un nouveau faisceau, en fonction de l'arbre de décision montré ci-dessous de (1) à (4).

Pour se joindre en toute sécurité à un faisceau existant, on doit utiliser un protocole d'authentification PPP [3] pour obtenir des informations authentifiées de la part de l'homologue afin d'empêcher qu'un homologue hostile ne se joigne à un faisceau existant en présentant une option de discriminant falsifiée.

Cette option n'est pas exigée pour le fonctionnement multiliaison. Si un système ne reçoit pas l'option MRRU multiliaison, mais reçoit l'option de discriminant de point d'extrémité, et qu'il n'y a pas de configuration manuelle qui fournisse d'informations extérieures, la mise en œuvre NE DOIT PAS supposer sur cette seule base que le fonctionnement multiliaison est demandé.

Comme il n'y a pas d'exigence d'authentification, il y a quatre ensembles de scénarios :

(1) Pas d'authentification, pas de discriminant :
Toute nouvelle liaison DOIT se joindre à un faisceau, sauf si une configuration manuelle en décide autrement. Il est aussi permis d'avoir plus d'un faisceau configuré manuellement pour connecter deux systèmes donnés.

(2) Discriminant, pas d'authentification :
Correspondance de discriminant -> DOIT se joindre au faisceau correspondant,
Pas de correspondance de discriminant -> DOIT établir un nouveau faisceau.

(3) Pas de discriminant, authentification :
Correspondance d'authentification -> DOIT se joindre au faisceau correspondant,
Pas de correspondance d'authentification -> DOIT établir un nouveau faisceau.

(4) Discriminant, authentification :
Correspondance de discriminant et d'authentification -> DOIT se joindre au faisceau,
Pas de correspondance de discriminant -> DOIT établir un nouveau faisceau,
Pas de correspondance d'authentification -> DOIT établir un nouveau faisceau.

L'option comporte une Classe qui sélectionne un espace d'adresse d'identifiant et une Adresse qui sélectionne un identifiant unique au sein de l'espace d'adresse de classe.

Cet identifiant est censé se référer à l'équipement mécanique associé au système de transmission. Pour certaines classes, l'unicité de l'identifiant est globale et n'est pas bornée par la portée d'un domaine administratif particulier. Au sein de chaque classe, l'unicité des valeurs d'adresse est contrôlée par une politique dépendante de la classe pour l'allocation des valeurs.

Chaque point d'extrémité peut choisir sans restriction une classe d'identifiant. Comme l'objectif est de détecter les discordances entre points d'extrémité supposés à tort être semblables, la discordance sur la seule classe est suffisante. Bien qu'aucune classe ne soit recommandée, les classes qui ont des valeurs universellement uniques sont préférées.

La prise en charge de cette option n'est pas exigée, ni de la part du système, ni de la part de l'homologue. Si l'option n'est pas présente dans une Demande-de-configuration, le système NE DOIT PAS générer un Configure-Nak de cette option pour quelque raison que ce soit ; il DEVRAIT à la place se comporter comme s'il avait reçu l'option avec Classe = 0, Adresse = 0. Si un système reçoit un Configure-Nak ou Configure-Reject de cette option, il DOIT la retirer de toute Demande-de-configuration supplémentaire.

La taille est déterminée à partir du champ Longueur de l'élément. Pour certaines classes, la longueur est fixée, pour d'autres, la longueur est variable. L'option est invalide si le champ Longueur indique une taille inférieure au minimum pour la classe.

Une mise en œuvre PEUT utiliser le discriminant de point d'extrémité pour localiser les enregistrements d'administration ou d'authentification dans une base de données locale. Une telle utilisation de cette option est accessoire par rapport à son objet et elle est déconseillée lorsqu'un protocole PPP d'authentification [3] peut être utilisé à la place. Comme certaines classes permettent à l'homologue de générer des valeurs aléatoires ou allouées localement, l'utilisation de cette option comme clé de base de données exige un accord préalable avec les administrateurs homologues.

La spécification des sous champs est la suivante :
Type : 19 = pour le discriminant de point d'extrémité
Longueur : 3 + longueur de l'adresse
Classe : Le champ Classe a un octet et indique l'espace d'adresse d'identifiant. Les valeurs les plus à jour du champ Classe de discriminant de point d'extrémité LCP sont spécifiées dans la plus récente RFC "Numéros alloués" [7]. Les valeurs courantes sont allouées comme suit :

0 Classe nulle
1 Adresse allouée localement
2 Adresse de protocole Internet (IP)
3 Adresse MAC IEEE 802.1 allouée mondialement
4 Bloc de numéro magique PPP
5 Numéro d'annuaire de réseau public commuté

Adresse : Le champ Adresse est de un ou plusieurs octets et indique l'adresse d'identifiant au sein de la classe choisie. La longueur et le contenu dépendent de la valeur de la Classe comme suit :

Classe 0 – Classe nulle
Longueur maximale : 0
Contenu : Cette classe est la valeur par défaut si l'option n'est pas présente dans une Demande-de-configuration reçue.

Classe 1 – Adresse allouée localement
Longueur maximale : 20
Contenu : Cette classe est définie pour permettre une allocation locale dans le cas où l'utilisation des classes globalement uniques n'est pas possible. On suggère l'utilisation d'un numéro de série d'appareil. L'utilisation de cette classe est déconseillée car l'unicité n'est pas garantie.

Classe 2 – Adresse de protocole Internet (IP)
Longueur fixée : 4
Contenu : Une adresse dans cette classe contient une adresse d'hôte IP comme défini en [8].

Classe 3 - Adresse MAC IEEE 802.1 allouée mondialement
Longueur fixée : 6
Contenu : Une adresse dans cette classe contient une adresse MAC IEEE 802.1 MAC en format canonique (802.3) [9]. L'adresse DOIT avoir le bit d'allocation mondial/local libre et DOIT avoir le bit multidiffusion/spécifique libre. Les adresses MAC allouées localement devraient être représentées en utilisant la Classe 1.

Classe 4 – Bloc de numéro magique PPP
Longueur maximale : 20
Contenu : Ce n'est pas une adresse mais un bloc de 1 à 5 numéros magiques PPP de 32 bits enchaînés, comme défini en [2]. Cette classe sert à la génération automatique d'une valeur vraisemblablement unique, mais sans garantie. Le même bloc DOIT être utilisé de façon continue par un point d'extrémité pendant toute période durant laquelle au moins une liaison est dans l'état ouvert LCP. L'utilisation de cette classe est déconseillée.

Noter que les numéros magiques PPP sont utilisés dans [2] pour détecter des bouclages inattendus d'une liaison entre un point d'extrémité et elle-même. Il y a une faible probabilité que deux points d'extrémité distincts génèrent des numéros magiques correspondants. Cette probabilité est réduite de façon géométrique lorsque la négociation LCP est répétée à la recherche de la discordance désirée, si un homologue peut générer des numéros magiques non corrélés.

Tels qu'ils sont utilisés ici, les numéros magiques servent à déterminer si deux liaisons proviennent en fait du même point d'extrémité homologue ou de deux points d'extrémités distincts. Les numéros correspondent toujours lorsqu'il n'y a qu'un seul point d'extrémité. Il y a une probabilité faible que les numéros correspondent même s'il y a deux points d'extrémité. Pour obtenir la même assurance qu'il n'y a pas une fausse correspondance que pour la détection de bouclage LCP, on peut combiner en un seul bloc plusieurs numéros magiques non corrélés.

Classe 5 – Numéro d'annuaire de réseau public commuté
Longueur maximale : 15
Contenu : Une adresse de cette classe contient une séquence d'octets telle que définie par I.331 (E.164) qui représente un numéro de téléphone international susceptible d'être utilisé pour accéder au point d'extrémité via le réseau téléphonique public commuté [10].

6 Lancement de l'utilisation d'en-tête multiliaison

Lorsque l'utilisation du protocole multiliaison a été négociée sur une liaison (disons Y), et que la liaison est ajoutée à un faisceau qui contient actuellement une seule liaison existante (disons X), un système DOIT transmettre un paquet incorporé multiliaison sur X avant de transmettre tout paquet incorporé multiliaison sur Y.

Comme des liaisons peuvent être ajoutées et retirées d'un faisceau sans détruire l'état qui lui est associé, le fragment devrait se voir allouer le numéro de fragment approprié (le suivant). Comme noté plus haut, le premier fragment transmis dans la vie d'un faisceau est le fragment de numéro 0.

7 Fermeture des liaisons membres

Les liaisons membres peuvent être terminées en conformité avec les procédures LCP PPP normales en utilisant les paquets LCP Demande-de-fin et Accusé-de-réception-de-fin sur cette liaison membre. Comme on suppose que ces liaisons membres ne réarrangent pas les paquets, la réception d'un accusé-de-réception-de-fin est suffisante pour supposer que tout paquet de protocole multiliaison qui lui est antérieur ne court pas de risque de perte particulier.

La réception d'une Demande-de-fin LCP sur une liaison ne termine pas la procédure sur les liaisons restantes.

Tant qu'une liaison membre est active sur le faisceau, l'état PPP persiste pour le faisceau comme entité distincte. Cependant, si il n'y a qu'une liaison unique dans le faisceau, et que toutes les autres liaisons ont été fermées volontairement (avec Accusé-de-réception-de-fin), une mise en œuvre PEUT cesser d'utiliser des en-têtes multiliaison.

Si la procédure multiliaison est utilisée conjointement avec la transmission PPP fiable, et qu'une liaison membre n'est pas fermée volontairement, la mise en œuvre devrait s'attendre à recevoir des paquets qui violent la règle de croissance des numéros de séquence.

8 Interaction avec les autres protocoles

Dans le cas habituel, LCP et le protocole de contrôle d'authentification seront négociés sur chaque liaison membre. Les protocoles réseau eux-mêmes et les échanges de commandes associés devraient normalement avoir été effectués une seule fois sur le faisceau.

Dans certains cas, il peut être souhaitable que certains protocoles réseau soient exemptés des exigences de séquencement, et si les tailles de MRU de la liaison ne causent pas de fragmentation, ces protocoles peuvent être envoyés directement sur les liaisons membres.

Bien qu'explicitement déconseillé ci-dessus, si on souhaite que plusieurs liaisons membres connectent deux mises en œuvre, avec un séquencement indépendant des deux ensembles de protocoles, mais si on ne souhaite pas bloquer l'un à l'aide de l'autre, on pourrait décrire deux procédures multiliaison en allouant plusieurs identifiants de point d'extrémité à un système donné. Chaque liaison membre devrait cependant n'appartenir qu'à un seul faisceau. On pourrait penser à un routeur physique qui hébergerait deux mises en œuvre séparées logiquement, chacune d'elles étant configurée indépendamment.

Une solution plus simple serait d'avoir une liaison qui refuse de se joindre au faisceau, en envoyant un Rejet-de-configuration en réponse à l'option LCP multiliaison.

9 Considérations sur la sécurité

Le fonctionnement de ce protocole n'est ni plus ni moins sûr que le fonctionnement des protocoles d'authentification PPP [3]. Le lecteur est invité à s'y reporter pour toute précision.

10 Références

[1] Leifer, D., Sheldon, S., and B. Gorsline, "A Subnetwork Control Protocol for ISDN Circuit-Switching", (non publiée), mars 1991.

[2] W. Simpson, éditeur, "Protocole point à point (PPP)", RFC1661 , STD 51, juillet 1994. *(MàJ par la RFC 2153)*

[3] B. Lloyd et W. Simpson, "Protocoles d'authentification PPP", RFC1334 , octobre 1992. *(Remplacée par RFC1994)*

[4] International Organisation for Standardization, "HDLC - Description of the X.25 LAPB-Compatible DTE Data Link Procedures", International Standard 7776, 1988

[5] D. Rand, "Protocole de contrôle de compression en PPP (CCP)", RFC1962, juin 1996.

[6] D. Rand, éditeur, "Transmission fiable en PPP", RFC1663, juillet 1994. *(P.S.)*

[7] J. Reynolds et J. Postel, "Numéros alloués", RFC1700, STD 2, octobre 1994. *(Historique)*

[8] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet DARPA", RFC0791, STD 5, septembre 1981.

[9] Institute of Electrical and Electronics Engineers, Inc., "IEEE Local and Metropolitan Area Networks: Overview and Architecture", IEEE Std. 802-1990, 1990.

[10] The International Telegraph and Telephone Consultative Committee (CCITT), "Numbering Plan for the ISDN Area", Recommendation I.331 (E.164), 1988.

[11] W. Simpson, "Extensions LCP pour PPP", RFC1570, janvier 1994. *(P.S., MàJ par 2484)*

11 Différences par rapport à la RFC 1717

La présente section expose les différences par rapport à la RFC 1717. Des restrictions s'appliquent aux mises en œuvre qui n'existaient pas dans la RFC 1717 ; les systèmes qui suivent ces restrictions sont pleinement interopérables avec les systèmes conformes à la RFC 1717.

11.1 Négociation de multiliaison, en soi

La RFC1717 permet l'utilisation des options de format court d'en-tête de numéro de séquence (SSNHF, *Short Sequence Number Header Format*) ou d'unité maximum de réception reconstruite (MRRU, *Maximum Reconstructed Receive Unit*) par elles-mêmes pour indiquer l'intention de négocier multiliaison. La présente spécification interdit l'utilisation de

l'option SSNHF par elle-même ; mais elle permet l'utilisation des deux options ensemble. Toute mise en œuvre qui se conforme par ailleurs à la RFC1717 et respecte aussi cette restriction interopérera avec toute mise en œuvre de la RFC1717.

11.2 Numéro de séquence initial défini

La présente spécification exige que le premier numéro de séquence transmis après que la liaison virtuelle a atteint l'état ouvert soit 0.

11.3 Valeur par défaut du MRRU

La présente spécification retire la valeur par défaut pour le MRRU, (car il doit toujours être négocié avec une valeur), et elle spécifie qu'une mise en œuvre doit prendre en charge une MRRU avec la même valeur que la taille de MRU par défaut pour PPP.

11.4 Interdiction du Config-Nak d'EID

La présente spécification interdit l'accusé de réception négatif de configuration d'un EID pour quelque raison que ce soit.

11.5 Uniformité d'espace de séquence

La présente spécification exige que soit employé le même format de numéro de séquence sur toutes les liaisons d'un faisceau.

11.6 Début et fin d'utilisation des en-têtes multiliaison

Le présent mémoire spécifie comment on devrait commencer l'utilisation des en-têtes multiliaison lors de l'ajout d'une liaison, et dans quelles circonstances l'arrêt de leur utilisation est sûr.

11.7 Configuration manuelle et allocation de faisceau

Le document permet explicitement que plusieurs faisceaux soient configurés manuellement en l'absence à la fois de discriminant de point d'extrémité et de toute forme d'authentification.

12 Adresse des auteurs

Keith Sklower
Computer Science Department
384 Soda Hall, Mail Stop 1776
University of California
Berkeley, CA 94720-1776
téléphone : (510) 642-9587
mél : sklower@CS.Berkeley.EDU

Brian Lloyd
Lloyd Internetworking
3031 Alhambra Drive
Cameron Park, CA 95682

téléphone : (916) 676-1147
mél l: brian@lloyd.com

Glenn McGregor
Lloyd Internetworking
3031 Alhambra Drive
Cameron Park, CA 95682

téléphone : (916) 676-1147
mél : glenn@lloyd.com

Dave Carr
Newbridge Networks Corporation
600 March Road
P.O. Box 13600
Kanata, Ontario,
Canada, K2K 2E6
téléphone : (613) 591-3600
mél : dcarr@Newbridge.COM

Tom Coradetti
Sidewalk Software
1190 Josephine Road
Roseville, MN 55113

téléphone : (612) 490 7856
mél : 70761.1664@compuserve.com