Groupe de travail Réseau
Request for Comments : 1661
STD : 51
RFC rendue obsolète : 1548
Catégorie : Norme

W. Simpson, éditeur
Daydreamer
juillet 1994

Traduction Claude Brière de L'Isle

Protocole point à point (PPP)

Résumé
Le protocole point à point (PPP, *Point-to-Point Protocol*) fournit une méthode normalisée pour le transport de datagrammes multi-protocoles sur des liaisons point à point. PPP comporte trois composants principaux :

1. une méthode d'encapsulation des datagrammes multi-protocoles,
2. un protocole de commande de liaison (LCP, *Link Control Protocol*) pour établir, configurer et vérifier la connexion de la liaison de données,
3. une famille de protocoles de commande de réseau (NCP, *Network Control Protocol*) pour établir et configurer différents protocoles de couche réseau.

Le présent document définit l'organisation et la méthodologie de PPP, et l'encapsulation PPP, avec un mécanisme de négociation d'option extensible qui est capable de négocier un riche assortiment de paramètres de configuration et fournit des fonctions de gestion supplémentaires. Le protocole PPP de commande de liaison (LCP) est décrit selon ce mécanisme.

Table des matières

1. Introduction

Le protocole point à point a été conçu pour les liaisons simples qui transportent des paquets entre deux homologues. Ces liaisons permettent un fonctionnement bidirectionnel simultané, et sont supposées livrer les paquets dans l'ordre. L'intention est que PPP fournisse une solution commune pour la connexion facile d'hôtes, ponts et routeurs très divers [RFC1547].

Encapsulation
L'encapsulation PPP permet le multiplexage simultané de différents protocoles de couche réseau sur la même liaison. L'encapsulation PPP a été conçue avec soin pour conserver la compatibilité avec les matériels de prise en charge les plus largement utilisés.

Seuls huit octets supplémentaires sont nécessaires pour former l'encapsulation lorsque elle est utilisée dans les trames de style HDLC par défaut. Dans les environnements où la bande passante est un bien précieux, l'encapsulation et le tramage peuvent être raccourcis à 2 ou 4 octets.

Pour la prise en charge de mises en œuvre à grande vitesse, l'encapsulation par défaut utilise seulement des champs simples, dont un seul doit être examiné pour le démultiplexage. Les champs d'en-tête et d'informations par défaut se terminent sur des limites de 32 bits, et l'en-queue peut être bourré jusqu'à une limite fixée arbitrairement.

Protocole de contrôle de liaison
Afin d'être suffisamment adaptable pour être portable dans une grande variété d'environnements, PPP fournit un protocole de contrôle de liaison (LCP, *Link Control Protocol*). Le LCP est utilisé pour un accord automatique sur les options de format d'encapsulation, traiter la variation des limites de taille des paquets, détecter une liaison en boucle et d'autres erreurs courantes de mauvaise configuration, et pour terminer la liaison. Les autres facilités facultatives fournies sont l'authentification de l'identité de ses homologues sur la liaison, et la détermination des moments où une liaison fonctionne correctement et de ceux où elle est défaillante.

Protocoles de contrôle de réseau
Les liaisons en point à point tendent à exacerber de nombreux problèmes de la famille actuelle des protocoles réseau. Par exemple, l'allocation et la gestion des adresses IP, qui est un problème même dans les environnements de LAN, est particulièrement difficile sur les liaisons à commutation de circuit en point à point (comme les serveurs à modem à numérotation). Ces problèmes sont traités par une famille de protocoles de contrôle de réseau (NCP, *Network Control Protocol*) dont chacun gère les besoins spécifiques imposés par leurs protocoles de couche réseau respectifs. Ces NCP sont définis dans les documents d'accompagnement.

Configuration
Il est prévu que les liaisons PPP soient faciles à configurer. Par conception, la norme traite par défaut toutes les configurations courantes. Une mise en œuvre peut spécifier des améliorations à la configuration par défaut, qui sont automatiquement communiquées à l'homologue sans intervention d'un opérateur. Finalement, l'opérateur peut explicitement configurer pour la liaison des options qui permettent à celle-ci de fonctionner dans des environnements qui lui auraient autrement été impossibles.

Cette auto configuration est mise en œuvre grâce à un mécanisme de négociation d'extension d'options, par lequel chaque extrémité de la liaison décrit à l'autre ses capacités et exigences. Bien que le mécanisme de négociation d'option décrit dans le présent document soit spécifié dans les termes du protocole de contrôle de liaison (LCP) ces mêmes facilités sont conçues pour être utilisées par les autres protocoles de contrôle, en particulier ceux de la famille des NCP.

1.1 Spécification des exigences

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules :

DOIT Ce mot, ou l'adjectif "exigé", signifie que la définition est une exigence absolue de la spécification.

NE DOIT PAS Cette phrase signifie que la définition est une interdiction absolue de la spécification.

DEVRAIT Ce mot, ou l'adjectif "recommandé", signifie qu'il peut exister des raisons valides dans des circonstances particulières pour ignorer cet élément, mais toutes leurs implications doivent être comprises et soigneusement soupesées avant de choisir une voie différente.

PEUT Ce mot, ou l'adjectif "facultatif", signifie que cet élément fait partie d'un ensemble permis de solutions de remplacement. Une mise en œuvre qui n'inclut pas cette option DOIT être prête à interopérer avec d'autres mises en œuvres qui incluent bien l'option.

1.2 Terminologie

Le présent document utilise fréquemment les termes suivants :

datagramme C'est l'unité de transmission à la couche réseau (comme IP). Un datagramme peut être encapsulé dans un ou plusieurs paquets passés à la couche de liaison des données.

trame C'est l'unité de transmission à la couche de liaison des données. Une trame peut inclure un en-tête et/ou un en-queue, ainsi qu'un certain nombre d'unités de données.

paquet Unité de base de l'encapsulation, passé par l'interface entre la couche réseau et la couche de liaison des données. Un paquet est normalement transposé sur une trame ; les exceptions sont lorsque on effectue une fragmentation à la couche de liaison des données, ou lorsque plusieurs paquets sont incorporés dans une seule trame.

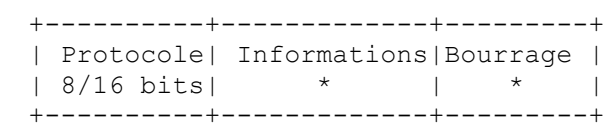
homologue C'est l'autre extrémité de la liaison point à point.

éliminer en silence La mise en œuvre élimine le paquet sans autre traitement. La mise en œuvre DEVRAIT donner la possibilité d'inscrire l'erreur dans le journal d'événements, en incluant le contenu du paquet éliminé en silence, et DEVRAIT enregistrer l'événement dans un compteur de statistiques.

2. Encapsulation PPP

L'encapsulation PPP est utilisée pour rendre sans ambiguïté les datagrammes multi-protocoles. Cette encapsulation exige que le tramage indique le début et la fin de l'encapsulation. Les méthodes de fourniture du tramage sont spécifiées dans les documents d'accompagnement.

Le schéma ci-dessous résume l'encapsulation PPP. Les champs sont transmis de gauche à droite.



Champ Protocole
Il comporte un ou deux octets, et sa valeur identifie le datagramme encapsulé dans le champ Information du paquet. Le champ est transmis et reçu avec l'octet de poids fort en premier.

La structure de ce champ est cohérente avec le mécanisme d'extension de la norme ISO 3309 pour les champs d'adresse. Toutes les valeurs de Protocole DOIVENT être impaires ; le bit de moindre poids de l'octet de moindre poids DOIT être égal à "1". Aussi, tout Protocole DOIT être alloué de telle sorte que le bit de moindre poids de l'octet de poids fort soit égal à "0". Les trames reçues qui ne se conforment pas à ces règles DOIVENT être traitées comme ayant un Protocole non reconnu.

Les valeurs du champ Protocole dans la gamme "0***" à "3***" identifient le protocole de couche réseau des paquets spécifiques, et les valeurs dans la gamme "8***" à "b***" identifient les paquets qui appartiennent aux protocoles de contrôle de réseau (NCP, *Network Control Protocol*) associés, s'il en est.

Les valeurs du champ Protocole dans la gamme "4***" à "7***" sont utilisées pour les protocoles à faible volume de trafic qui n'ont pas de NCP associé. Les valeurs de champ Protocole dans la gamme "c***" à "f***" identifient les paquets comme étant des protocoles de contrôle de couche de liaison (comme LCP).

Les valeurs à jour du champ Protocole sont spécifiées dans la plus récente version des "Numéros alloués" [RFC1700]. La présente spécification réserve les valeurs suivantes :

Valeur (en hexadécimal)	**Nom du protocole**
0001	Protocole de bourrage
0003 à 001f	réservé (transparence inefficace)
007d	réservé (Control Escape)
00cf	réservé (PPP NLPID)
00ff	réservé (compression inefficace)
8001 à 801f	non utilisé
807d	non utilisé
80cf	non utilisé
80ff	non utilisé
c021	Protocole de contrôle de liaison
c023	Protocole d'authentification de mot de passe
c025	Rapport de qualité de liaison
c223	Protocole d'authentification à prise de contact par mise au défi

Les développeurs de nouveaux protocoles DOIVENT obtenir un numéro auprès de l'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) à IANA@isi.edu.

Champ Information
Il est de zéro, un ou plusieurs octets. Le champ Information contient le datagramme pour le protocole spécifié dans le champ Protocole.

La longueur maximum du champ Information, y compris le bourrage, mais non compris le champ Protocole, est appelée l'unité de réception maximum (MRU, *Maximum Receive Unit*) qui a par défaut 1500 octets. Par négociation, les mises en œuvre de PPP qui y consentent peuvent utiliser d'autres valeurs pour la MRU.

Bourrage
À l'émission, le champ Information PEUT être bourré avec un nombre arbitraire d'octets jusqu'à la MRU. Il est de la responsabilité de chaque protocole de distinguer les octets de bourrage des informations réelles.

3. Fonctionnement de la liaison PPP

3.1 Généralités

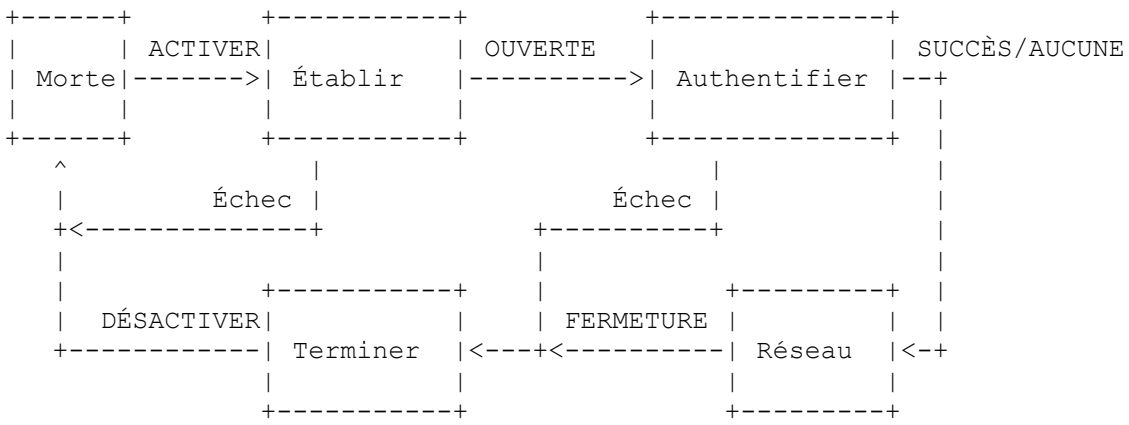
Pour établir des communications sur une liaison point à point, chaque extrémité de la liaison PPP DOIT d'abord envoyer des paquets de LCP pour configurer et essayer la liaison de données. Après l'établissement de la liaison, l'homologue PEUT être authentifié.

Ensuite, PPP DOIT envoyer des paquets NCP pour choisir et configurer un ou plusieurs protocoles de couche réseau. Une fois que le protocole de couche réseau choisi a été configuré, les datagrammes provenant de chaque protocole de couche réseau peuvent être envoyés sur la liaison.

La liaison va rester configurée pour des communications jusqu'à ce que des paquets LCP ou NCP explicites closent la liaison, ou jusqu'à ce que survienne quelque événement externe (l'arrivée à expiration d'un temporisateur d'inactivité ou une intervention de l'administrateur du réseau).

3.2 Diagramme de phase

Dans le processus de configuration, maintenance et terminaison de la liaison point à point, la liaison PPP passe par plusieurs phases distinctes qui sont spécifiées dans le diagramme d'état simplifié suivant :



Toutes les transitions ne sont pas spécifiées dans ce diagramme. La sémantique développée dans les paragraphes qui suivent DOIT être respectée.

3.3 Liaison morte (couche physique pas prête)

La liaison commence et se termine nécessairement par cette phase. Lorsque un événement externe (comme une détection de porteuse ou une configuration de l'administrateur du réseau) indique que la couche physique est prête à être utilisée, PPP va procéder à la phase d'établissement de la liaison.

Durant cette phase, l'automate LCP (décrit plus loin) va être dans l'état Initial ou Débutant. La transition à la phase établissement de liaison va signaler un événement ACTIVER *(UP)* à l'automate LCP.

Note de mise en œuvre : Normalement une liaison va retourner à cette phase automatiquement après la déconnexion d'un modem. Dans le cas d'une liaison matérielle, cette phase peut être extrêmement courte – simplement assez longue pour détecter la présence de l'appareil.

3.4 Phase d'établissement de la liaison

Le protocole de contrôle de liaison (LCP, *Link Control Protocol*) est utilisé pour établir la connexion par un échange de paquets Configure. Cet échange est terminé, et on passe dans l'état LCP Ouvert, une fois qu'un paquet Accusé de réception de configuration *(Configure-Ack)* (décrit plus loin) a été à la fois envoyé et reçu.

Toutes les options Configuration sont supposées être à leur valeur par défaut sauf si elles ont été altérées par l'échange de configuration. Voir un exposé plus détaillé sur les options de configuration LCP à la section 6.

Il est important de noter que seules les options de configuration qui sont indépendantes des protocoles particuliers de couche réseau sont configurées par LCP. La configuration des protocoles individuels de couche réseau est traitée par des protocoles de commande réseau (NCP, *Network Control Protocol*) distincts durant la phase de protocole de couche réseau.

Tout paquet non LCP reçu durant cette phase DOIT être éliminé en silence.

La réception d'une demande de configuration *(Configure-Request)* LCP provoque un retour à la phase d'établissement de liaison depuis la phase Protocole de couche réseau ou depuis la phase Authentification.

3.5 Phase d'authentification

Il peut être souhaitable sur certaines liaisons d'exiger d'un homologue qu'il s'authentifie avant de permettre l'échange de paquets de couche réseau.

Par défaut, l'authentification n'est pas obligatoire. Si une mise en œuvre désire que l'homologue s'authentifie avec un protocole d'authentification spécifique, il DOIT alors demander l'usage de ce protocole d'authentification durant la phase d'établissement de liaison.

L'authentification DEVRAIT avoir lieu aussitôt que possible après l'établissement de la liaison. Cependant, la détermination de la qualité de la liaison PEUT survenir en même temps. Une mise en œuvre NE DOIT PAS permettre que l'échange de paquets de détermination de la qualité de la liaison retarde indéfiniment l'authentification.

L'avancement de la phase Authentification à la phase Protocole de couche réseau NE DOIT PAS survenir tant que l'authentification n'est pas terminée. Si l'authentification échoue, l'authentificateur DEVRAIT procéder à la place à la phase Terminaison de liaison.

Seuls les paquets de protocole de contrôle de liaison, de protocole d'authentification, et de surveillance de la qualité sont permis durant cette phase. Tous les autres paquets reçus durant cette phase DOIVENT être éliminés en silence.

Notes de mise en œuvre : Une mise en œuvre NE DEVRAIT PAS faire échouer l'authentification pour une simple expiration de temporisation ou un manque de réponse. L'authentification DEVRAIT permettre une méthode de retransmission, et ne passer à la phase Terminaison de liaison qu'après qu'un certain nombre de tentatives d'authentification a été dépassé.

La mise en œuvre chargée de commencer la phase Terminaison de liaison est celle qui a refusé l'authentification à son homologue.

3.6 Phase de protocole de couche réseau

Une fois que PPP a fini les phases précédentes, chaque protocole de couche réseau (comme IP, IPX, ou AppleTalk) DOIT être configuré séparément par le protocole de contrôle réseau (NCP) approprié.

Chaque NCP PEUT être Ouvert et Fermé à tout moment.

Note de mise en œuvre : Comme une mise en œuvre peut initialement utiliser une durée significative pour la détermination de qualité de la liaison, les mises en œuvre DEVRAIENT éviter les temporisations fixes lors de l'attente de la configuration d'un NCP par leurs homologues.

Après qu'un NCP a atteint l'état Ouvert, PPP va porter les paquets correspondants de protocole de couche réseau. Tout paquet de protocole de couche réseau pris en charge reçu alors que le NCP correspondant n'est pas dans l'état Ouvert DOIT être éliminé en silence.

Note de mise en œuvre : Lorsque le LCP est dans l'état Ouvert, tout paquet de protocole qui n'est pas pris en charge par la mise en œuvre DOIT être retourné dans un Rejet de protocole (décrit plus loin). Seuls les protocoles qui sont pris en charge sont éliminés en silence.

Durant cette phase, le trafic de la liaison consiste en toutes combinaisons possibles de paquets LCP, NCP, et de protocole de couche réseau.

3.7 Phase de terminaison de la liaison

PPP peut terminer la liaison à tout moment. Cela peut survenir à cause de la perte de la porteuse, d'un échec d'authentification, d'un échec de qualité de liaison, de l'expiration d'un temporisateur de période d'inactivité, ou de la fermeture administrative de la liaison. Un LCP est utilisé pour clore la liaison par un échange de paquets Terminer. Lorsque la liaison se ferme, PPP informe les protocoles de couche liaison afin qu'ils puissent prendre les actions appropriées.
Après l'échange des paquets Terminer, la mise en œuvre DEVRAIT signaler à la couche physique de se déconnecter afin de mettre en application la terminaison de la liaison, en particulier dans le cas d'un échec de l'authentification. L'envoyeur de la Demande-de-terminer DEVRAIT se déconnecter après réception d'un Accusé-de-terminaison, ou après l'expiration du compteur Redémarrer. Le receveur d'une Demande-de-terminer DEVRAIT attendre que l'homologue se déconnecte, et NE DOIT PAS se déconnecter tant qu'au moins une temporisation de Redémarrer ne s'est pas passée après l'envoi d'un Accusé-de-terminaison. PPP DEVRAIT passer à la phase Liaison morte.

Tout paquet non LCP reçu durant cette phase DOIT être éliminé en silence.

Note de mise en œuvre : La fermeture de la liaison par le LCP est suffisante. Il n'est pas besoin que chaque NCP envoie une débauche de paquets Terminer. À l'inverse, le fait qu'un NCP ait fermé n'est pas une raison suffisante pour causer la terminaison de la liaison PPP, même si ce NCP était le seul actuellement dans l'état Ouvert.

4. L'automate de négociation d'option

L'automate à états finis est défini par des événements, des actions et des transitions d'état. Les événements incluent la

réception de commandes externes telles que Ouverture et Clôture, l'expiration du temporisateur de Redémarrage, et la réception des paquets provenant d'un homologue. Les actions incluent le lancement du temporisateur de redémarrage et la transmission de paquets à l'homologue.

Certains types de paquets – Non-accusé-de-configuration et Rejet-de-configuration, ou Rejet-de-code et Rejet-de-protocole, ou Demandes-d'écho, Réponse-d'écho et Demande-d'élimination – ne sont pas différenciés dans les descriptions de l'automate. Comme on le décrira plus loin, ces paquets servent bien des fonctions différentes. Cependant, ils causent toujours les mêmes transitions.

Événements	Actions
Up = la couche inférieure est active	tlu = This-Layer-Up *(cette couche est active)*
Down = la couche inférieur est morte	tld = This-Layer-Down *(cette couche est morte)*
Open = ouverture administrative	tls = This-Layer-Started *(cette couche a commencé)*
Close= clôture administrative	tlf = This-Layer-Finished *(cette couche est finie)*
TO+ = Temporisation avec compteur > 0	irc = Initialize-Restart-Count *(initialiser le compteur de redémarrage)*
TO- = Temporisation avec compteur expiré	zrc = Zero-Restart-Count *(compte sans redémarrage)*
RCR+ = Demande de configuration reçue (bonne)	scr = Send-Configure-Request *(envoyer demande de configuration)*
RCR- = Demande de configuration reçue (mauvaise)	
RCA = Acquittement de configuration reçu	sca = Send-Configure-Ack *(envoi d'acquittement de configuration)*
RCN = Non-acqu/Rejet de config. reçu	scn = Send-Configure-Nak/Rej *(envoi de non acqu/rejet de configuration)*
RTR = Demande de terminaison reçue	str = Send-Terminate-Request *(envoi de demande de terminaison)*
RTA = Reçu-acquit-terminaison	sta = Send-Terminate-Ack *(envoi d'acquittement de terminaison)*
RUC = Reçu-code-inconnu	scj = Send-Code-Reject *(envoi de rejet de code)*
RXJ+ = Code-rejet-reçu (permis) ou Rejet-de-protocole-reçu	
RXJ- = Code-Rejet-reçu (catastrophique) ou Rejet-de-protocole-reçu	
RXR = Receive-Echo-Request	ser = Send-Echo-Reply *(envoi de réponse d'écho)*
ou Réponse-d'écho-reçue	
ou Demande-d'élimination-reçue	

4.1 Tableau de transition d'état

Le tableau qui suit donne la totalité des états de transition. Les états sont indiqués horizontalement, et les événements se lisent verticalement. Les transitions d'état et les actions sont représentées sous la forme action/nouvel-état. Plusieurs actions sont séparées par des virgules, et peuvent continuer sur les lignes suivantes si nécessaire ; plusieurs actions peuvent être mises en œuvre dans n'importe quel ordre. L'état peut être suivi d'une lettre, qui indique une note d'explication. Un tiret ('-') indique une transition illégale.

État	**0**	**1**	**2**	**3**	**4**	**5**
Événements	Initial	Débute	Clos	Arrêté	Fermant	Arrêtant
Up	2	irc,scr/6	-	-	-	-
Down	-	-	0	tls/1	0	1
Open	tls/1	1	irc,scr/6	3r	5r	5r
Close	0	tlf/0	2	2	4	4
TO+	-	-	-	-	str/4	str/5
TO-	-	-	-	-	tlf/2	tlf/3
RCR+	-	-	sta/2 irc,scr,sca/8	4	5	
RCR-	-	-	sta/2 irc,scr,scn/6	4	5	
RCA	-	-	sta/2	sta/3	4	5
RCN	-	-	sta/2	sta/3	4	5
RTR	-	-	sta/2	sta/3	sta/4	sta/5
RTA	-	-	2	3	tlf/2	tlf/3
RUC	-	-	scj/2	scj/3	scj/4	scj/5
RXJ+	-	-	2	3	4	5
RXJ-	-	-	tlf/2	tlf/3	tlf/2	tlf/3
RXR	-	-	2	3	4	5

État	6	7	8	9
Événements	Dem-envoyée	Acq-Reçu	Acq-Envoyé	Ouvert
Up	-	-	-	-
Down	1	1	1	tld/1
Open	6	7	8	9r
Close	irc,str/4	irc,str/4	irc,str/4	tld,irc,str/4
TO+	scr/6	scr/6	scr/8	-
TO-	tlf/3p	tlf/3p	tlf/3p	-
RCR+	sca/8	sca,tlu/9	sca/8	tld,scr,sca/8
RCR-	scn/6	scn/7	scn/6	tld,scr,scn/6
RCA	irc/7	scr/6x	irc,tlu/9	tld,scr/6x
RCN	irc,scr/6	scr/6x	irc,scr/8	tld,scr/6x
RTR	sta/6	sta/6	sta/6	tld,zrc,sta/5
RTA	6	6	8	tld,scr/6
RUC	scj/6	scj/7	scj/8	scj/9
RXJ+	6	6	8	9
RXJ-	tlf/3	tlf/3	tlf/3	tld,irc,str/5
RXR	6	7	8	ser/9

Les états dans lesquels le temporisateur de redémarrage fonctionne sont identifiables par la présence des événements TO. Seules les actions Envoyer-demande-de-configuration, Envoyer-demande-de-fin et Compte-de-redémarrage-à-zéro démarrent ou redémarrent avec le temporisateur de redémarrage. Le temporisateur de redémarrage est arrêté lors d'une transition de tout état dans lequel le temporisateur fonctionne à un état où le temporisateur ne fonctionne pas.

Les événements et actions sont définis conformément à une architecture de passage de message plutôt qu'une architecture de signalisation. Si une action est désirée pour contrôler des signaux spécifiques (tels que DTR) des actions supplémentaires seront vraisemblablement nécessaires.

[p] Option passive ; voir l'exposé sur l'état Arrêté.
[r] Option Redémarrage ; voir l'exposé sur l'événement Open.
[x] Connexion croisée ; voir l'exposé sur l'événement RCA.

4.2 États

Ci-après figure une description plus détaillée de chacun des états de l'automate.

Initial
Dans l'état Initial, la couche inférieure est indisponible (Morte), et aucun Open n'est survenu. Le temporisateur de redémarrage ne fonctionne pas dans l'état Initial.

Débute *(Starting)*
L'état Débute est la contrepartie Ouverte de l'état Initial. Une ouverture administrative a été initiée, mais la couche inférieure est toujours indisponible (Morte). Le temporisateur de redémarrage ne fonctionne pas dans l'état Débute.

Lorsque la couche inférieure devient disponible (active) une Demande de configuration est envoyée.

Clos
Dans l'état Clos, la liaison est disponible (Active), mais un Open n'est pas arrivé. Le temporisateur Redémarrage ne fonctionne pas dans l'état Clos.

À réception des paquets Demande-de-configuration, un Acq-de-terminaison est envoyé. Les Acq-de-terminaison sont éliminés en silence pour éviter de créer une boucle.

Arrêté
L'état Arrêté est la contrepartie Ouverte de l'état Clos. On y entre lorsque l'automate attend un événement Down après l'action Cette-couche-est-finie, ou après l'envoi d'un Acq-de-terminaison. Le temporisateur de redémarrage ne fonctionne pas dans l'état Arrêté.

À réception de paquets Demande-de-configuration, une réponse appropriée est envoyée. À réception d'autres paquets, un Acq-de-terminaison est envoyé. Les Acq-de-terminaison sont éliminés en silence pour éviter de créer une boucle.

Raison :
L'état arrêté est un état de jonction pour la terminaison de liaison, l'échec de configuration de liaison, et d'autres modes d'échec de l'automate. Ces états potentiellement séparés ont été combinés.

Il y a une concurrence entre la réponse d'événement Down (à partir de l'action Cette-couche-est-finie) et l'événement Demande-de-configuration-reçue (RCR). Lorsque une Demande-de-configuration arrive avant l'événement Down, celui-ci va prendre le pas en faisant retourner l'automate à l'état Début. Cela empêche les attaques par répétition.

Option de mise en œuvre :
Après l'échec de l'homologue à répondre aux demandes de configuration, une mise en œuvre PEUT attendre passivement que l'homologue envoie des demandes de configuration. Dans ce cas, l'action Cette-couche-est-finie n'est pas utilisée pour l'événement TO- dans les états Req-Sent, Ack-Rcvd et Ack-Sent.

Cette option est utile pour les circuits spécialisés, ou les circuits qui n'ont pas de signaux d'état disponibles, mais NE DEVRAIT PAS être utilisée pour les circuits commutés.

+Fermant *(Closing)*
Dans l'état Fermant est faite une tentative de terminaison de la connexion. Une Demande-de-terminaison a été envoyée et le temporisateur de redémarrage fonctionne, mais un Acq-de-terminaison n'a pas encore été reçu.

À réception d'un Acq-de-terminaison, on entre dans l'état Clos. À l'expiration du temporisateur de redémarrage, une nouvelle Demande-de-terminaison est transmise, et le temporisateur de redémarrage est relancé. Après l'expiration Max-Terminate fois du temporisateur de redémarrage, on entre dans l'état Clos.

Arrêtant *(Stopping)*
L'état Arrêtant est la contrepartie Ouverte de l'état Fermant. Une Demande-de-terminaison a été envoyée et le temporisateur de redémarrage fonctionne, mais un Acq-de-terminaison n'a pas encore été reçu.

Raison :
L'état Arrêtant donne une opportunité bien définie de terminer une liaison avant de permettre du trafic nouveau. Après la terminaison de la liaison, une nouvelle configuration peut s'établir via les états Arrêté ou Débute.

Demande-envoyée *(Request-Sent)*
Dans l'état Demande-envoyée est faite une tentative de configuration de la connexion. Une Demande-de-configuration a été envoyée et le temporisateur de redémarrage fonctionne, mais un Acq-de-configuration n'a pas encore été reçu ni envoyé.

Acq-reçu *(Ack-Received)*
Dans l'état Acq-reçu, une Demande-de-configuration a été envoyée et un Configure-Acq a été reçu. Le temporisateur de redémarrage fonctionne toujours, car un Configure-Acq n'a pas encore été envoyé.

Acq-envoyé *(Ack-Sent)*
Dans l'état Acq-envoyé, une Demande-de-configuration et un Configure-Acq ont tous deux été envoyés, mais un Configure-Acq n'a pas encore été reçu. Le temporisateur de redémarrage fonctionne, car un Configure-Acq n'a pas encore été reçu.

Ouvet
Dans l'état Ouvert, un Configure-Acq a été à la fois envoyé et reçu. Le temporisateur de redémarrage ne fonctionne pas.

En entrant dans l'état Ouvert, la mise en œuvre DEVRAIT signaler aux couches supérieures qu'elle est maintenant Up. À l'inverse, en quittant l'état Ouvert, la mise en œuvre DEVRAIT signaler aux couches supérieures qu'elle est maintenant Down.

4.3 Événements

Dans l'automate, les transitions et les actions sont causées par des événements.

Up
Cet événement survient lorsque une couche inférieure indique qu'elle est prête à porter des paquets.

Normalement, cet événement est utilisé par un traitement de modem ou par un processus d'appel, ou par quelque autre couplage de la liaison PPP au support physique, pour signaler au LCP que la liaison entre dans la phase Établissement de liaison.

Il peut aussi être utilisé par le LCP pour signaler à chaque NCP que la liaison entre dans la phase Protocole de couche réseau. C'est à dire que l'action This-Layer-Up de la part du LCP déclanche l'événement Up dans le NCP.

Down
Cet événement survient lorsque une couche inférieure indique qu'elle n'est plus prête à porter des paquets.

Normalement, cet événement est utilisé par un traitement de modem ou un processus d'appel, ou par quelque autre couplage de la liaison PPP au support physique pour signaler au LCP que la liaison entre dans la phase Liaison morte.

Il peut aussi être utilisé par le LCP pour signaler à chaque NCP que la liaison quitte la phase Protocole de couche réseau. C'est à dire que l'action This-Layer-Down de la part du LCP déclanche l'événement Down dans le NCP.

Open
Cet événement indique que la liaison est disponible du point de vue administratif pour le trafic ; c'est à dire que l'administrateur du réseau (un homme ou un programme) a indiqué qu'il est permis que la liaison soit Open. Lorsque survient cet événement, et si la liaison n'est pas dans l'état Ouvert, l'automate tente d'envoyer des paquets de configuration à l'homologue.

Si l'automate n'est pas capable de commencer la configuration (la couche inférieure est Down, ou un événement Close précédent ne s'est pas achevé) l'établissement de la liaison est automatiquement retardé.

Lorsque est reçue une Demande de terminaison; ou lorsque surviennent d'autres événements qui causent l'indisponibilité de la liaison, l'automate va passer à un état où la liaison est prête à se rouvrir. Aucune intervention administrative supplémentaire n'est nécessaire.

Option de mise en œuvre :
L'expérience a montré que les usagers vont exécuter une commande Open supplémentaire lorsque ils veulent renégocier la liaison. Cela peut indiquer que de nouvelles valeurs sont à négocier.

Comme ce n'est pas la signification de l'événement Open, il est suggéré que lorsque une commande d'utilisateur Open est exécutée dans les états Ouvert, Fermant, Arrêtant, ou Arrêté, la mise en œuvre produise un événement Down, immédiatement suivi par un événement Up. Il faut faire attention que l'intervention d'un événement Down ne puisse pas provenir d'une autre source.

Le Down suivi d'un Up va causer une renégociation ordonnée de la liaison, en passant par les états Débute et Demande-envoyée. Cela va causer la renégociation de la liaison, sans aucun effet collatéral dommageable.

Close
Cet événement indique que la liaison n'est pas disponible pour le trafic ; c'est-à-dire que l'administrateur du réseau (homme ou programme) a indiqué que la liaison n'est pas autorisée à être Ouverte. Lorsque cet événement survient, et lorsque la liaison n'est pas dans l'état Clos, l'automate tente de terminer la connexion. Les tentatives suivantes de reconfigurer la liaison sont refusées jusqu'à ce que survienne un nouvel événement Open.

Note de mise en œuvre :
Lorsque l'authentification échoue, la liaison DEVRAIT être terminée, pour empêcher une attaque par répétition et de déni de service aux autres usagers. Comme la liaison est administrativement disponible (par définition) cela peut être réalisé en simulant un événement Close au LCP, immédiatement suivi par un événement Open. Il faut veiller à ce que l'intervention d'un événement Close ne puisse pas survenir d'une autre source.

Le Close suivi par un Open causera une terminaison ordonnée de la liaison, en progressant par les états Fermant jusqu'à Arrêtant, et l'action Cette-couche-est-finie peut déconnecter la liaison. L'automate attend dans l'état Arrêté ou Débute la prochaine tentative de connexion.

Fin de temporisation *(Timeout)* (TO+, TO-)
Cet événement indique l'expiration du temporisateur de redémarrage. Le temporisateur de redémarrage est utilisé pour mesurer le temps de réponse aux paquets Demande-de-configuration et Demande-de-terminaison.
L'événement TO+ indique que le compteur de redémarrage continue d'être supérieur à zéro, ce qui déclanche la retransmission du paquet Demande-de-configuration ou Demande-de-terminaison correspondant.
L'événement TO- indique que le compteur de redémarrage n'est plus supérieur à zéro, et qu'aucun autre paquet ne doit être retransmis.

Demande-de-configuration-reçue (RCR+, RCR-)
Cet événement survient lorsque un paquet Demande-de-configuration est reçu de l'homologue. Le paquet Demande-de-configuration indique le désir d'ouvrir une connexion et peut spécifier des options Configuration. Le paquet Demande-de-configuration est plus complètement décrit dans un paragraphe ultérieur.

L'événement RCR+ indique que la Demande-de-configuration était acceptable, et déclanche la transmission d'un Configure-Ack correspondant.

L'événement RCR- indique la Demande-de-configuration n'était pas acceptable, et déclanche la transmission d'un Configure-Nak ou Configure-Reject correspondant.

Note de mise en œuvre :
Ces événements peuvent survenir sur une connexion qui est déjà dans l'état Ouvert. La mise en œuvre DOIT être prête à renégocier immédiatement les options de configuration.

Receive-Configure-Ack (RCA)
Cet événement survient lorsque un paquet Configure-Ack valide est reçu de l'homologue. Le paquet Configure-Ack est une réponse positive à un paquet Demande-de-configuration. Un paquet hors séquence ou invalide pour une autre cause est éliminé en silence.

Note de mise en œuvre :
Comme le paquet correct a déjà été reçu avant qu'on atteigne les états Ack-Rcvd ou Ouvert, il est extrêmement peu vraisemblable qu'un tel autre paquet arrive. Comme spécifié, tous les paquets Ack/Nak/Rej invalides sont éliminés en silence, et n'affectent pas les transitions de l'automate. Cependant, il n'est pas impossible qu'un paquet correctement formé arrive par une connexion croisée au même moment. Il est plus vraisemblable que ce sera le résultat d'une erreur de mise en œuvre. Au minimum, cet événement DEVRAIT être enregistré dans le journal.

Receive-Configure-Nak/Rej (RCN)
Cet événement survient lorsque un paquet valide Configure-Nak ou Configure-Reject est reçu de l'homologue. Les paquets Configure-Nak et Configure-Reject sont des réponses négatives à un paquet Demande-de-configuration. Un paquet hors séquence ou invalide par ailleurs est éliminé en silence.

Note de mise en œuvre :
Bien que le Configure-Nak et le Configure-Reject causent la même transition d'état dans l'automate, ces paquets ont des effets significativement différents sur l'option de configuration envoyée dans le paquet Demande-de-configuration résultant.

Demande-de-terminaison-reçue (RTR)
Cet événement survient lorsque un paquet Demande-de-terminaison est reçu. Le paquet Demande-de-terminaison indique le désir de l'homologue de clore la connexion.

Note de mise en œuvre :
Cet événement n'est pas identique à l'événement Close (voir ci-dessus) et n'outrepasse pas les commandes Open de l'administrateur de réseau local. La mise en œuvre DOIT être prête à recevoir une nouvelle Demande-de-configuration sans intervention de l'administrateur de réseau.

Receive-Terminate-Ack (RTA)
Cet événement survient lorsque un paquet Terminate-Ack est reçu de l'homologue. Le paquet Terminate-Ack est habituellement une réponse à un paquet Demande-de-terminaison. Le paquet Terminate-Ack peut aussi indiquer que l'homologue est dans les états Fermé ou Arrêté, et qu'il sert à resynchroniser la configuration de la liaison.

Receive-Unknown-Code (RUC)
Cet événement survient lorsque un paquet non interprétable est reçu de l'homologue. Un paquet Code-Reject est envoyé en réponse.

Receive-Code-Reject, Receive-Protocol-Reject (RXJ+,RXJ-)
Cet événement survient lorsque un paquet Code-Reject ou Protocol-Reject est reçu de l'homologue.

L'événement RXJ+ survient lorsque la valeur rejetée est acceptable, comme un Code-Reject d'un code étendu, ou un Protocol-Reject d'un NCP. Il rentre dans le cadre d'un fonctionnement normal. La mise en œuvre DOIT arrêter d'envoyer le type de paquet en cause.

L'événement RXJ- survient lorsque la valeur rejetée est catastrophique, telle qu'un Code-Reject d'une Demande-de-configuration, ou un Protocol-Reject de LCP ! Cet événement communique une erreur irrécupérable qui met fin à la connexion.

Receive-Echo-Request, Receive-Echo-Reply, Receive-Discard-Request (RXR)
Cet événement survient lorsque un paquet Echo-Request, Echo-Reply ou Discard-Request est reçu de l'homologue. Le paquet Echo-Reply est une réponse à un paquet Echo-Request. Il n'y a pas de réponse à un paquet Echo-Reply ou Discard-Request.

4.4 Actions

Les actions dans l'automate sont causées par des événements et indiquent normalement la transmission de paquets et/ou le début ou l'arrêt du temporisateur de redémarrage.

Événement illégal (-)
Cela indique un événement qui ne peut pas survenir dans un automate correctement mis en œuvre. La mise en œuvre a une erreur interne, qui devrait être rapportée et enregistrée dans le journal. Aucune transition n'intervient, et la mise en œuvre NE DEVRAIT PAS faire un redémarrage ou être gelée.

This-Layer-Up (tlu)
Cette action indique aux couches supérieures que l'automate entre dans l'état Ouvert.
Normalement, cette action est utilisée par le LCP pour signaler l'événement Up à un NCP, un protocole d'authentification, ou un protocole de qualité de liaison, ou PEUT être utilisé par un NCP pour indiquer que la liaison est disponible pour son trafic de couche réseau.

This-Layer-Down (tld)
Cette action indique aux couches supérieures que l'automate quitte l'état Ouvert.
Normalement, cette action est utilisée par le LCP pour signaler l'événement Down à un NCP, un protocole d'authentification, ou un protocole de qualité de liaison, ou PEUT être utilisé par un NCP pour indiquer que la liaison n'est plus disponible pour ce trafic de couche réseau.

This-Layer-Started (tls)
Cette action indique aux couches inférieures que l'automate entre dans l'état Débute, et que la couche inférieure est nécessaire pour la liaison. La couche inférieure DEVRAIT répondre par un événement Up lorsque la couche inférieure est disponible.
Le résultat de cette action est très dépendant de la mise en œuvre.

This-Layer-Finished (tlf)
Cette action indique aux couches inférieures que l'automate entre dans les états Initial, Clos ou Arrêté, et que la couche inférieure n'est plus nécessaire à la liaison. La couche inférieure DEVRAIT répondre par un événement Down lorsque la couche inférieure se termine. Normalement, cette action PEUT être utilisée par le LCP pour avancer à la phase Liaison morte, ou PEUT être utilisée par un NCP pour indiquer au LCP que la liaison peut se terminer lorsque il n'y a pas d'autre NCP ouvert.
Le résultat de cette action est très dépendant de la mise en œuvre.

Initialize-Restart-Count (irc)
Cette action règle le compteur de redémarrage à la valeur appropriée (Max-Terminate ou Max-Configure). Le compteur est décrémenté pour chaque transmission, y compris la première.

Note de mise en œuvre :
En plus du réglage du compteur de redémarrage, la mise en œuvre DOIT régler la période de temporisation à la valeur initiale lorsque le retard de temporisateur de redémarrage est utilisé.

Zero-Restart-Count (zrc)
Cette action règle le compteur de redémarrage à zéro.

Note de mise en œuvre :
Cette action permet au FSA de marquer une pause avant de procéder à l'état final désiré, permettant au trafic d'être traité par l'homologue. En plus de la mise à zéro du compteur de redémarrage, la mise en œuvre DOIT régler la période de temporisation à une valeur appropriée.

Send-Demande-de-configuration (scr)
Un paquet Demande-de-configuration est transmis. Cela indique le désir d'ouvrir une connexion avec un ensemble spécifié d'options de configuration. Le temporisateur de redémarrage est lancé lorsque le paquet Demande-de-configuration est transmis, pour se prémunir contre la perte de paquet. Le compteur de redémarrage est décrémenté à chaque fois qu'est envoyé une Demande-de-configuration.

Send-Configure-Ack (sca)
Un paquet Configure-Ack est transmis. Cela accuse réception d'un paquet Demande-de-configuration avec un ensemble acceptable d'options de configuration.

Send-Configure-Nak (scn)
Un paquet Configure-Nak ou Configure-Reject est transmis, selon le cas approprié. Cette réponse négative rapporte la réception d'un paquet Demande-de-configuration avec un ensemble non acceptable d'options de configuration.

Les paquets Configure-Nak sont utilisés pour refuser une valeur d'option de configuration, et pour suggérer une nouvelle valeur acceptable. Les paquets Configure-Reject sont utilisés pour refuser toute négociation sur une option de configuration, normalement parce qu'elle n'est pas reconnue ou mise en œuvre. L'utilisation de Configure-Nak plutôt que Configure-Reject est décrite plus en détails à la section 5 sur les formats de paquet LCP.

Envoi-demande-de-terminaison (str)
Un paquet Demande-de-terminaison est transmis. Cela indique le désir de clore une connexion. Le temporisateur de redémarrage est lancé lorsque le paquet Demande-de-terminaison est transmis, pour se garder contre la perte de paquet. Le compteur de redémarrage est décrémenté chaque fois qu'une Demande-de-terminaison est envoyée.

Send-Terminate-Ack (sta)
Un paquet Terminate-Ack est transmis. Cela accuse réception d'un paquet Demande-de-terminaison ou autrement, sert à la synchronisation des automates.

Send-Code-Reject (scj)
Un paquet Code-Reject est transmis. Cela indique la réception d'un type de paquet inconnu.

Send-Echo-Reply (ser)
Un paquet Echo-Reply est transmis. Cela accuse réception d'un paquet Echo-Request.

4.5 Éviter les boucles

Le protocole fait une tentative raisonnable pour éviter les boucles de négociation d'option de configuration. Cependant, le protocole NE garantit PAS que des boucles ne puissent se produire. Comme avec toute négociation, il est possible de configurer deux mises en œuvre de PPP avec des politiques contradictoires qui ne vont jamais converger. Il est aussi possible de configurer des politiques qui convergent bien, mais qui prennent un temps significatif pour le faire. Les mises en œuvre devraient avoir cela présent à l'esprit et DEVRAIENT développer des mécanismes de détection de boucle ou des temporisations au niveau supérieur.

4.6 Compteurs et temporisateurs

Temporisateur de redémarrage
L'automate utilise un temporisateur spécial. Le temporisateur de redémarrage est utilisé pour limiter les transmissions de paquets Demande-de-configuration et Demande-de-terminaison. L'expiration du temporisateur de redémarrage cause un événement de fin de temporisation, et la retransmission du paquet Demande-de-configuration ou Demande-de-terminaison correspondant. Le temporisateur de redémarrage DOIT être configurable, mais DEVRAIT par défaut être réglé à trois (3) secondes.

Note de mise en œuvre :
Le temporisateur de redémarrage DEVRAIT être fondé sur la vitesse de la liaison. La valeur par défaut est conçue pour les liaisons à basse vitesse (2 400 à 9 600 bit/s) et forte latence de commutation (les lignes téléphoniques normales). Les liaisons à plus grande vitesse, ou les liaisons avec faible latence de commutation, DEVRAIENT avoir des temps de retransmission réduits en proportion.
Au lieu d'une valeur constante, le temporisateur de redémarrage PEUT commencer à une faible valeur initiale et augmenter jusqu'à la valeur finale configurée. Chaque valeur successive inférieure à la valeur finale DEVRAIT être au moins deux fois la valeur précédente. La valeur initiale DEVRAIT être assez grande pour tenir compte de la taille des paquets, deux fois le délai d'aller-retour pour la transmission à la vitesse de la liaison, et au moins 100 millisecondes additionnelles pour permettre à l'homologue de traiter les paquets avant de répondre. Certains circuits ajoutent 200

autres millisecondes de délai de satellite. Les temps d'aller-retour pour les modems qui fonctionnent à 14 400 bit/s ont été mesurés dans la gamme de 160 à plus de 600 millisecondes.

Max-Terminate
Il y a un compteur de redémarrage exigé pour les Demande-de-terminaison. Max-Terminate indique le nombre de paquets Demande-de-terminaison envoyés sans recevoir de Terminate-Ack avant de supposer que l'homologue est incapable de répondre. Max-Terminate DOIT être configurable, mais DEVRAIT être de deux (2) transmissions par défaut.

Max-Configure
Un compteur similaire est recommandé pour les Demande-de-configuration. Max-Configure indique le nombre de paquets Demande-de-configuration envoyés sans recevoir un Configure-Ack, Configure-Nak ou Configure-Reject valide avant de supposer que l'homologue est incapable de répondre. Max-Configure DOIT être configurable, mais DEVRAIT par défaut être de dix (10) transmissions.

Max-Failure
Un compteur particulier est recommandé pour Configure-Nak. Max-Failure indique le nombre de paquets Configure-Nak envoyés sans envoi d'un Configure-Ack avant de supposer que la configuration ne converge pas. Tout autre paquet Configure-Nak pour les options demandées par l'homologue est converti en paquet Configure-Reject, et les options désirées en local ne sont plus ajoutées. Max-Failure DOIT être configurable, mais DEVRAIT être de cinq (5) transmissions par défaut.

5. Formats de paquet LCP

Il y a trois classes de paquets LCP :

1. Les paquets de configuration de liaison sont utilisés pour établir et configurer une liaison (Demande-de-configuration, Configure-Ack, Configure-Nak et Configure-Rejet).

2. Les paquets de terminaison de liaison qui sont utilisés pour terminer une liaison (Demande-de-terminaison et Terminate-Ack).

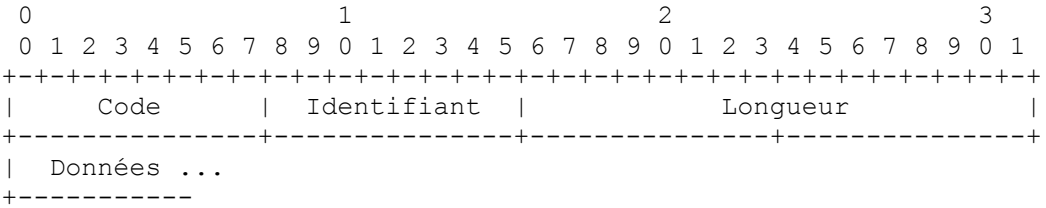
3. Les paquets de maintenance de liaison, utilisés pour gérer et déboguer une liaison (Code-Rejet, Protocol-Rejet, Echo-Request, Echo-Reply, et Discard-Request).

Pour faire simple, il n'y a pas de champ Version dans le paquet LCP. Une mise en œuvre de LCP qui fonctionne correctement va toujours répondre aux protocoles et codes inconnus par un paquet LCP facilement reconnaissable, fournissant ainsi un mécanisme déterministe de repli pour les mises en œuvre d'autres versions.

Sans considérer quelles options de configuration sont activées, tous les paquets LCP Configuration de liaison, Terminaison de liaison, et Code-Rejet (codes 1 à 7) sont toujours envoyés comme si aucune option de configuration n'était négociée. En particulier, chaque option de configuration spécifie une valeur par défaut. Cela assure que de tels paquets LCP sont toujours reconnaissables, même lorsque une extrémité de la liaison croit à tord que la liaison est ouverte.

Exactement un paquet LCP est encapsulé dans le champ Information PPP, où le champ Protocole PPP indique le type hex c021 (Protocole de contrôle de liaison).

Un résumé du format du paquet Protocole de contrôle de liaison est montré ci-dessous. Les champs sont émis de gauche à droite.



Code
Le champ Code fait un octet, et identifie le type de paquet LCP. Lorsque un paquet est reçu avec un champ Code inconnu, un paquet Code-Rejet est transmis.

Les valeurs à jour du champ Code LCP sont spécifiées dans la plus récente version des "Numéros alloués" [RFC1700]. Le présent document concerne les valeurs suivantes :

1 Demande-de-configuration
2 Configure-Ack
3 Configure-Nak
4 Configure-Rejet
5 Demande-de-terminaison
6 Terminate-Ack
7 Code-Rejet
8 Protocol-Rejet
9 Echo-Request
10 Echo-Reply
11 Discard-Request

Identifiant
Le champ Identifiant fait un octet, et aide à faire correspondre les demandes et les réponses. Lorsque un paquet est reçu avec un champ Identifiant invalide, le paquet est éliminé en silence sans affecter l'automate.

Longueur
Le champ Longueur fait deux octets, et indique la longueur du paquet LCP, y compris les champs Code, Identifiant, Longueur et Données. La longueur NE DOIT PAS excéder la MRU de la liaison.

Les octets en dehors de la gamme du champ Longueur sont traités comme du bourrage et sont ignorés à réception. Lorsque un paquet est reçu avec un champ Longueur invalide, le paquet est éliminé en silence sans affecter l'automate.

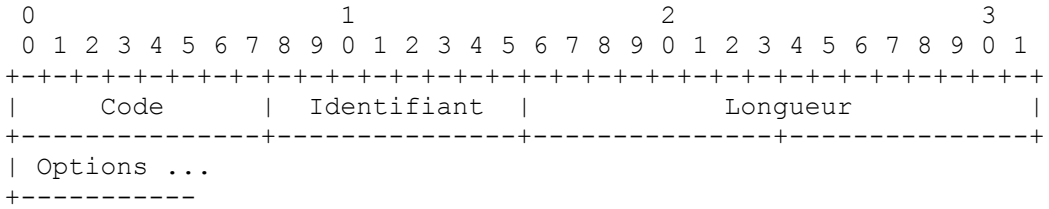
Données
Le champ Données fait zéro, un ou plusieurs octets, comme indiqué par le champ Longueur. Le format du champ Données est déterminé par le champ Code.

5.1 Demande-de-configuration

Description
Une mise en œuvre qui souhaite ouvrir une connexion DOIT transmettre une Demande-de-configuration. Le champ Options est rempli avec tout changement désiré aux valeurs par défaut de la liaison. Les options de configuration NE DEVRAIENT PAS être incluses avec des valeurs par défaut.

À réception d'une Demande-de-configuration, une réponse appropriée DOIT être transmise.

Un résumé du format du paquet Demande-de-configuration est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 1 pour Demande-de-configuration.

Identifiant
Le champ Identifiant DOIT être changé chaque fois que le contenu du champ Options change, et chaque fois que une réponse valide a été reçue pour une demande précédente. Pour la retransmissions, l'identifiant PEUT rester inchangé.

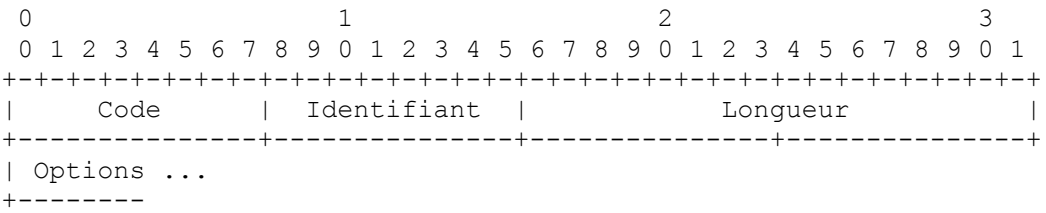
Options
Le champ Options est de longueur variable, et contient la liste de zéro, une ou plusieurs options de configuration que l'envoyeur désire négocier. Toutes les options de configuration sont toujours négociées simultanément. Le format des options de configuration est décrit plus en détails à la section 6.

5.2 Configure-Ack

Description
Si chaque option de configuration reçue dans une Demande-de-configuration est reconnaissable et si toutes les valeurs sont acceptables, alors la mise en œuvre DOIT transmettre un Configure-Ack. Les options de configuration acquittées NE DOIVENT PAS être réordonnées ou modifiées de quelque façon que ce soit.

À réception d'un Configure-Ack, le champ Identifiant DOIT correspondre à celui du dernier Demande-de-configuration transmis. De plus, les options de configuration dans un Configure-Ack DOIVENT exactement correspondre à celles de la dernière Demande-de-configuration transmise. Les paquets invalides sont éliminés en silence.

Un résumé du format de paquet Configure-Ack est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 2 pour Configure-Ack.

Identifiant
Le champ Identifiant est une copie du champ Identifiant de la Demande-de-configuration qui a causé ce Configure-Ack.

Options
Le champ Options est de longueur variable, et contient la liste de zéro, une ou plusieurs options de configuration dont l'envoyeur accuse réception. Toutes les options de configuration sont toujours acquittées simultanément.

5.3 Configure-Nak

Description
Si chaque instance des options de configuration reçues est reconnaissable, mais si certaines valeurs ne sont pas acceptables, la mise en œuvre DOIT alors transmettre un Configure-Nak. Le champ Options est rempli avec les seules options de configuration inacceptables dans la Demande-de-configuration. Toutes les options de configuration acceptables sont sorties du Configure-Nak, mais autrement, les options de configuration de la Demande-de-configuration NE DOIVENT PAS être réordonnées.

Les options qui n'ont pas de champ de valeur (options booléennes) DOIVENT utiliser plutôt la réponse Configure-Rejet.

Chaque option de configuration qui est admise en une seule instance DOIT être modifiée en une valeur acceptable pour l'envoyeur du Configure-Nak. La valeur par défaut PEUT être utilisée quand elle diffère de la valeur demandée.

Lorsque un type particulier d'option de configuration peut être énuméré plus d'une fois avec des valeurs différentes, le Configure-Nak DOIT inclure une liste de toutes les valeurs qui pour cette option sont acceptables pour l'envoyeur du Configure-Nak. Cela inclut les valeurs acceptables qui étaient présentes dans la Demande-de-configuration.

Finalement, une mise en œuvre peut être configurée pour demander la négociation d'une option de configuration spécifique. Si cette option ne figure pas sur la liste, cette option PEUT alors être ajoutée à la liste des options de configuration qui font l'objet du non accusé de réception, afin d'inviter l'homologue à inclure cette option dans son prochain paquet Demande-de-configuration. Tout champ de valeur pour l'option DOIT indiquer les valeurs acceptables pour l'envoyeur du Configure-Nak.

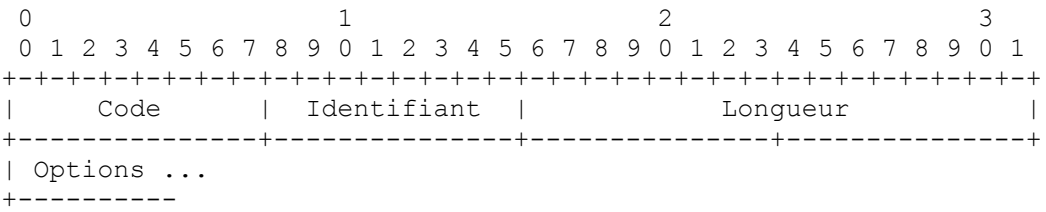
À réception d'un Configure-Nak, le champ Identifiant DOIT correspondre à celui de la dernière Demande-de-configuration transmise. Les paquets invalides sont éliminés en silence.

La réception d'un Configure-Nak valide indique que quand une nouvelle Demande-de-configuration sera envoyée, les options de configuration POURRONT être modifiées comme spécifié dans le Configure-Nak. Lorsque plusieurs instances d'une option de configuration sont présentes, l'homologue DEVRAIT choisir une seule valeur à inclure dans son prochain paquet Demande-de-configuration.

Certaines options de configuration ont une longueur variable. Comme l'option qui a fait l'objet du non accusé de réception

a été modifiée par l'homologue, la mise en œuvre DOIT être capable de traiter une longueur d'option qui est différente de celle de la Demande-de-configuration d'origine.

Un résumé du format de paquet Configure-Nak est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 3 pour Configure-Nak.
Identifiant
Le champ Identifiant est une copie du champ Identifiant de la Demande-de-configuration qui a causé ce Configure-Nak.

Options
Le champ Options est de longueur variable, et contient la liste de zéro, une ou plusieurs options de configuration dont l'envoyeur fait un accusé de réception négatif. Toutes les options de configuration sont non acquittées simultanément.

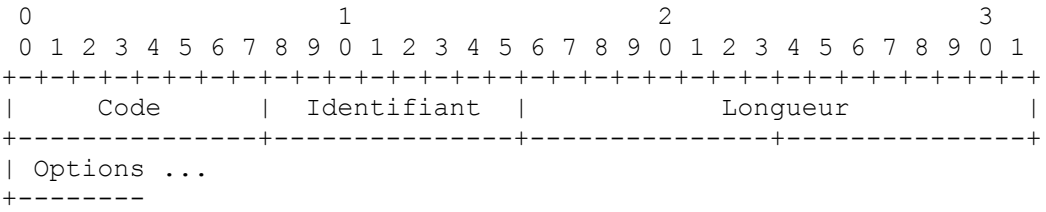
5.4 Configure-Rejet

Description
Si certaines options de configuration reçues dans une Demande-de-configuration ne sont pas reconnaissables ou ne sont pas acceptables pour la négociation (comme configuré par un administrateur de réseau) la mise en œuvre DOIT alors transmettre un Configure-Rejet. Le champ Options est rempli avec les seules options de configuration inacceptables de la Demande-de-configuration. Toutes les options de configuration reconnaissables et négociables sont retirées de la Configure-Rejet, mais autrement, les options de configuration NE DOIVENT PAS être réordonnées ou modifiées de quelque façon que ce soit.

À réception d'un Configure-Rejet, le champ Identifiant DOIT correspondre à celui de la dernière Demande-de-configuration transmise. De plus, les options de configuration dans un Configure-Rejet DOIVENT être un sous-ensemble de celles du dernier Demande-de-configuration transmis. Les paquets invalides sont éliminés en silence.

La réception d'un Configure-Rejet valide indique que quand une nouvelle Demande-de-configuration est envoyée, elle NE DOIT inclure aucune des options de configuration énumérées dans le Configure-Rejet.

Un résumé du format de paquet Configure-Rejet est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 4 pour Configure-Rejet.

Identifiant
Le champ Identifiant est une copie du champ Identifiant de la Demande-de-configuration qui a causé ce Configure-Rejet.

Options
Le champ Options est de longueur variable, et contient la liste de zéro, une ou plusieurs options de configuration que l'envoyeur rejette. Toutes les options de configuration sont toujours rejetées simultanément.

5.5 Demande-de-terminaison et Terminate-Ack

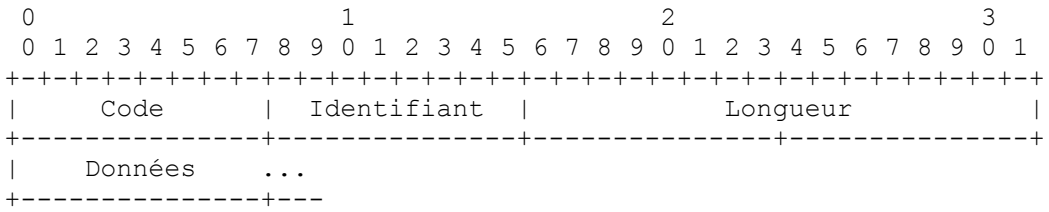
Description
LCP inclut des codes Demande-de-terminaison et Terminate-Ack afin de fournir un mécanisme pour clore une connexion.

Une mise en œuvre qui souhaite clore une connexion DEVRAIT transmettre une Demande-de-terminaison. Les paquets de Demande-de-terminaison DEVRAIENT continuer d'être envoyés jusqu'à ce que le Terminate-Ack soit reçu, que la couche inférieure indique qu'elle a fermé, ou qu'un nombre suffisamment grand ait été transmis pour qu'il y ait une certitude raisonnable que l'homologue soit déconnecté.

À réception d'une Demande-de-terminaison, un Terminate-Ack DOIT être transmis.

La réception d'un Terminate-Ack non sollicité indique que l'homologue est dans l'état Clos ou Arrêté, ou autrement a besoin d'une renégociation.

Un résumé du format des paquets Demande-de-terminaison et Terminate-Ack est donné ci-dessous. Les champs sont émis de gauche à droite.



Code
5 pour Demande-de-terminaison;
6 pour Terminate-Ack.

Identifiant
À l'émission, le champ Identifiant DOIT être changé chaque fois que le contenu du champ Données change, et chaque fois qu'une réponse valide a été reçue pour une demande précédente. Pour les retransmissions, l'identifiant PEUT rester inchangé.

À réception, le champ Identifiant de la Demande-de-terminaison est copié dans le champ Identifiant du paquet Terminate-Ack.

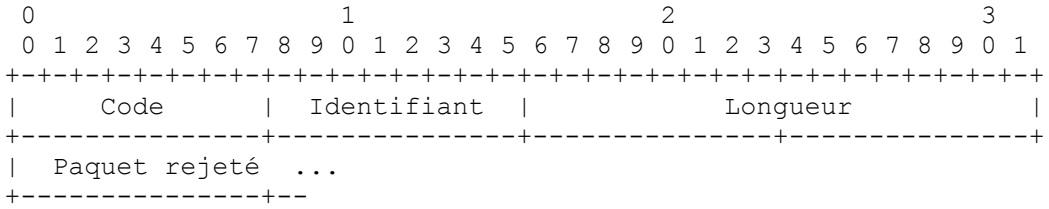
Données
Le champ Données est de zéro, un ou plusieurs octets, et contient des données non interprétées à utiliser par l'envoyeur. Les données peuvent consister en toute valeur binaire. La fin du champ est indiquée par la Longueur.

5.6 Code-Rejet

Description
La réception d'un paquet LCP qui a un code inconnu indique que l'homologue fonctionne avec une version différente. Cela DOIT être rapporté à l'envoyeur du code inconnu par la transmission d'un Code-Rejet.

À réception du Code-Rejet d'un code qui est fondamental pour cette version du protocole, la mise en œuvre DEVRAIT rapporter le problème et abandonner la connexion, car il est peu vraisemblable que la situation puisse être rectifiée automatiquement.

Un résumé du format de paquet Code-Rejet est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 7 pour Code-Rejet.

Identifiant
Le champ Identifiant DOIT être changé pour chaque Code-Rejet envoyé.

Paquet-rejeté
Le champ Paquet-rejeté contient une copie du paquet LCP qui est rejeté. Il commence par le champ Informations, et ne comporte aucun en-tête de couche de liaison des données ni de séquence de contrôle de trame (FCS, *Frame Check Sequence)*. Le paquet rejeté DOIT être tronqué pour se conformer à la MRU établie de l'homologue.

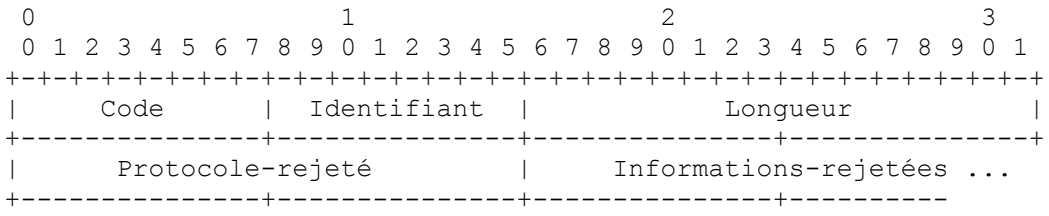
5.7 Protocol-Rejet

Description
La réception d'un paquet PPP avec un champ Protocole inconnu indique que l'homologue tente d'utiliser un protocole qui n'est pas pris en charge. Cela survient habituellement lorsque l'homologue tente de configurer un nouveau protocole. Si l'automate LCP est dans l'état Ouvert, cela DOIT alors être rapporté à l'homologue en transmettant un Protocol-Rejet.

À réception d'un Protocol-Rejet, la mise en œuvre DOIT arrêter d'envoyer des paquets du protocole indiqué à la première opportunité.

Les paquets Protocol-Rejet peuvent seulement être envoyés dans l'état LCP Ouvert. Les paquets Protocol-Rejet reçus dans tout état autre que l'état LCP Ouvert DEVRAIENT être éliminés en silence.

Un résumé du format de paquet Protocol-Rejet est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 8 pour Protocol-Rejet.

Identifiant
Le champ Identifiant DOIT être changé pour chaque Protocol-Rejet envoyé.

Protocole-rejeté
Le champ Protocole-rejeté fait deux octets, et contient le champ Protocole PPP du paquet qui est rejeté.

Informations-rejetées
Le champ Informations-rejetées contient une copie du paquet qui est rejeté. Il commence par le champ Information, et n'inclut aucun en-tête de couche de liaison des données ni de FCS. Informations-rejetées DOIT être tronqué pour se conformer à la MRU établie de l'homologue.

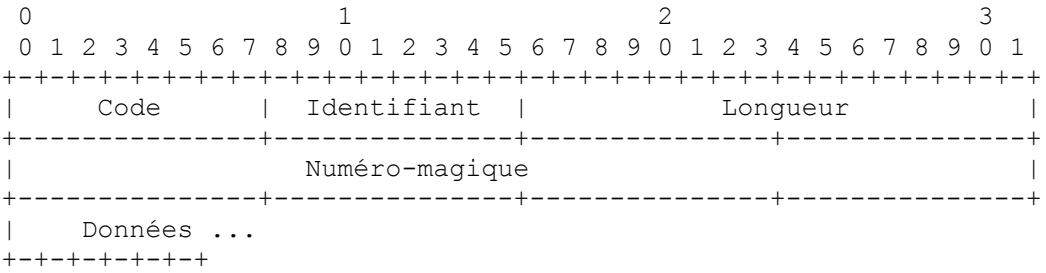
5.8 Echo-Request et Echo-Reply

Description
LCP inclut les codes Echo-Request et Echo-Reply afin de fournir un mécanisme de mise en boucle de couche de liaison des données à utiliser dans les deux sens de la liaison. Cela est utile pour aider au débogage, à la détermination de la qualité de la liaison, à l'essai des performances, et pour de nombreuses autres fonctions.

À réception d'une Echo-Request dans l'état LCP Ouvert, une Echo-Reply DOIT être transmise.

Les paquets Echo-Request et Echo-Reply DOIVENT être envoyés seulement dans l'état LCP Ouvert. Les paquets Echo-Request et Echo-Reply reçus dans tout autre état que LCP Ouvert DEVRAIENT être éliminés en silence.

Un résumé des formats de paquet de Echo-Request et Echo-Reply est donné ci-dessous. Les champs sont émis de gauche à droite.



Code :
9 pour Echo-Request;
10 pour Echo-Reply.

Identifiant
En émission, le champ Identifiant DOIT être changé chaque fois que le contenu du champ Données change, et chaque fois qu'une réponse valide a été reçue pour une demande précédente. Pour les retransmissions, l'identifiant PEUT rester inchangé.

À réception, le champ Identifiant de la Echo-Request est copié dans le champ Identifiant du paquet Echo-Reply.

Numéro-magique
Le champ Numéro-magique fait quatre octets, et aide à détecter les liaisons qui sont en condition de mise en boucle. Tant que l'option de configuration Numéro-magique n'a pas réussi à être négociée, le Numéro-magique DOIT être transmis à zéro. Voir des explications complémentaires dans l'option de configuration Numéro-magique.

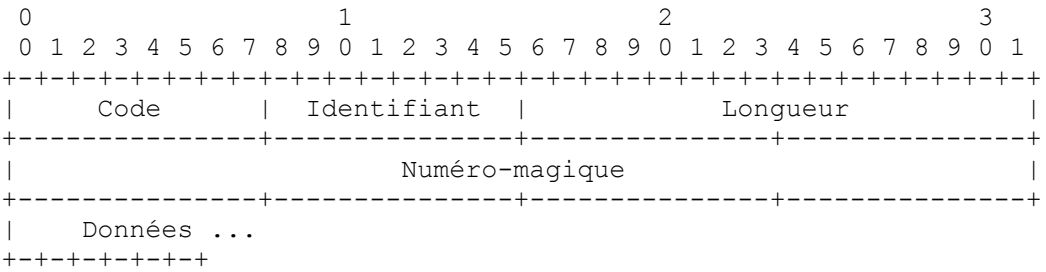
Données
Le champ Données fait zéro, un ou plusieurs octets, et contient des données non interprétées à utiliser par l'envoyeur. Les données peuvent consister en toute valeur binaire. La fin du champ est indiquée par la Longueur.

5.9 Discard-Request

Description
LCP inclut un code Discard-Request afin de fournir un mécanisme de collecteur de couche de liaison des données à utiliser pour essayer la direction local à distant de la liaison. Cela est utile comme aide au débogage, à l'essai des performances, et pour de nombreuses autres fonctions.

Les paquets Discard-Request DOIVENT n'être envoyés que dans l'état LCP Ouvert. À réception, le receveur DOIT éliminer en silence tout Discard-Request qu'il reçoit.

Un résumé du format de paquet Discard-Request est donné ci-dessous. Les champs sont émis de gauche à droite.



Code : 11 pour Discard-Request.

Identifiant
Le champ Identifiant DOIT être changé pour chaque Discard-Request envoyé.

Numéro-magique
Le champ Numéro-magique fait quatre octets, et aide à détecter les liaisons qui sont en condition de mise en boucle. Tant que l'option de configuration Numéro-magique n'a pas réussi à être négociée, le Numéro-magique DOIT être transmis à zéro. Voir des explications complémentaires dans l'option de configuration Numéro-magique au paragraphe 6.4.

Données
Le champ Données fait zéro, un ou plusieurs octets, et contient des données non interprétées à utiliser par l'envoyeur. Les données peuvent consister en toute valeur binaire. La fin du champ est indiquée par la Longueur.

6. Options de configuration de LCP

Les options de configuration LCP permettent la négociation de modifications aux caractéristiques par défaut d'une liaison point à point. Si une option de configuration n'est pas incluse dans un paquet Demande-de-configuration, la valeur par défaut est supposée pour cette option de configuration.

Certaines options de configuration PEUVENT être citées plus d'une fois. L'effet de cela est spécifique de l'option de configuration, et est spécifié par chaque description d'option de configuration. (Aucune des options de configuration de la présente spécification ne peut être citée plus d'une fois.)

La fin de la liste des options de configuration est indiquée par le champ Longueur du paquet LCP.

Sauf spécification contraire, toutes les options de configuration s'appliquent en mode semi-duplex ; normalement, dans la direction de réception de la liaison du point de vue de l'envoyeur de la Demande-de-configuration.

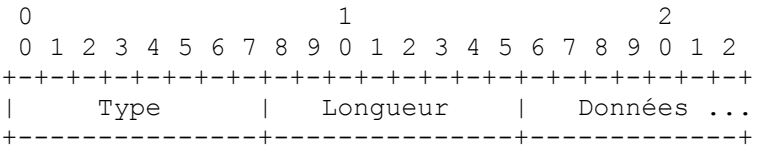
Philosophie du concept
Les options indiquent des capacités ou exigences supplémentaires de la mise en œuvre qui demande l'option. Une mise en œuvre qui ne comprend aucune option DEVRAIT interopérer avec une qui met en œuvre toutes les options.

Une valeur par défaut est spécifiée pour chaque option, ce qui permet à la liaison de fonctionner correctement sans négociation de l'option, quoique peut-être avec des performances sous optimales.

Sauf lorsque c'est explicitement spécifié, l'accusé de réception d'une option n'exige pas que l'homologue prenne d'autres mesures que celles prévues par défaut.

Il n'est pas nécessaire d'envoyer les valeurs par défaut pour les options dans une Demande-de-configuration.

Un résumé du format d'option de configuration est donné ci-dessous. Les champs sont émis de gauche à droite.



Type
Le champ Type fait un octet, et indique le type de l'option de configuration. Les valeurs à jour du champ Type d'option LCP sont spécifiées dans la plus récente version des "Numéros alloués" [RFC1700].
Le présent document concerne les valeurs suivantes :

0 Réservé
1 Unité de réception maximum
3 Protocole d'authentification
4 Protocole de qualité
5 Numéro magique
7 Compression du champ Protocole
8 Compression du champ Adresse et Contrôle

Longueur
Le champ Longueur fait un octet, et indique la longueur de cette option de configuration incluant les champs Type, Longueur et Données.
Si une option de configuration négociable est reçue dans une Demande-de-configuration, mais avec une longueur invalide ou non reconnue, un Configure-Nak DEVRAIT être transmis qui comporte l'option de configuration désirée avec des champs Longueur et Données appropriés.

Données
Le champ Données fait zéro, un ou plusieurs octets, et contient des informations spécifiques de l'option de configuration. Le format et la longueur du champ Données est déterminé par les champs Type et Longueur.

Lorsque le champ Données est indiqué par la longueur comme s'étendant au delà de la fin du champ Information, le paquet entier est éliminé en silence sans affecter l'automate.

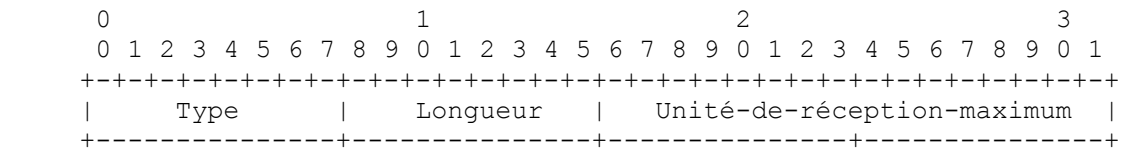
6.1 Unité de réception maximum (MRU)

Description
Cette option de configuration peut être envoyée pour informer l'homologue que la mise en œuvre peut recevoir de plus gros paquets, ou pour demander que l'homologue envoie de plus petits paquets.

La valeur par défaut est 1500 octets. Si des paquets plus petits sont demandés, une mise en œuvre DOIT cependant toujours être capable de recevoir le plein champ d'informations de 1500 octets pour le cas où la synchronisation de la liaison serait perdue.

Note de mise en œuvre :
Cette option est utilisée pour indiquer les capacités d'une mise en œuvre. L'homologue n'est pas obligé de maximiser l'utilisation de la capacité. Par exemple, lorsque une MRU est indiquée à 2048 octets, l'homologue n'est pas obligé d'envoyer tous les paquets avec 2048 octets. L'homologue n'a pas besoin de Configure-Nak pour indiquer qu'il va envoyer seulement de plus petits paquets,car la mise en œuvre va toujours exiger la prise en charge d'au moins 1500 octets.

Un résumé du format de l'option de configuration Unité de réception maximum est donné ci-dessous. Les champs sont émis de gauche à droite.



Type : 1
Longueur : 4

Unité-de-réception-maximum
Le champ Unité-de-réception-maximum fait deux octets, et spécifie le nombre maximum d'octets dans les champs Information et Bourrage. Il n'inclut pas le tramage, le champ Protocole, la FCS, ni aucun bits ou octets de transparence.

6.2 Protocole d'authentification

Description
Sur certaines liaisons, il peut être désirable d'exiger d'un homologue qu'il s'authentifie avant de lui permettre d'échanger des paquets de protocole de couche réseau.

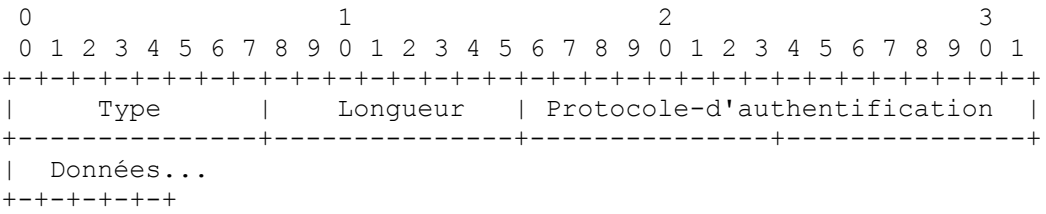
Cette option de configuration fournit une méthode de négociation de l'utilisation d'un protocole spécifique pour l'authentification. Par défaut, l'authentification n'est pas exigée.

Une mise en œuvre NE DOIT PAS inclure plusieurs options de configuration Protocole d'authentification dans ses paquets Demande-de-configuration. Il DEVRAIT plutôt tenter de configurer d'abord le protocole le plus souhaitable. Si ce protocole reçoit un Non accusé de réception, la mise en œuvre DEVRAIT alors tenter le protocole le plus désirable suivant dans la prochaine Demande-de-configuration.

La mise en œuvre qui envoie la Demande-de-configuration indique qu'elle attend une authentification de la part de son homologue. Si une mise en œuvre envoie un Configure-Ack, elle est alors d'accord pour s'authentifier avec le protocole spécifié. Une mise en œuvre qui reçoit un Configure-Ack DEVRAIT s'attendre à ce que l'homologue s'authentifie avec le protocole ayant fait l'objet de l'accusé de réception.

Il n'y a pas d'exigence que l'authentification soit bidirectionnelle ou que le même protocole soit utilisé dans les deux directions. Il est parfaitement acceptable que des protocoles différents soient utilisés dans chaque direction. Cela va, bien sûr, dépendre des protocoles spécifiques négociés.

Un résumé du format de l'option de configuration Protocole d'authentification est donné ci-dessous. Les champs sont émis de gauche à droite.



Type : 3
Longueur : ≥ 4

Protocole-d'authentification
Le champ Protocole-d'authentification fait deux octets, et indique le protocole d'authentification désiré. Les valeurs pour ce champ sont toujours les mêmes que celles du champ Protocole PPP pour le même protocole d'authentification .

Les valeurs à jour pour le champ Protocole d'authentification sont spécifiées dans la plus récente version des "Numéros alloués" [RFC1700]. Les valeurs allouées actuellement sont les suivantes :

Valeur (en hex)	Protocole
c023	Protocole d'authentification de mot de passe
c223	Protocole d'authentification par mise en cause de la prise de contact

Données
Le champ Données est de zéro, un ou plusieurs octets, et contient des données supplémentaires selon ce qui est déterminé par le protocole concerné.

6.3 Protocole de qualité

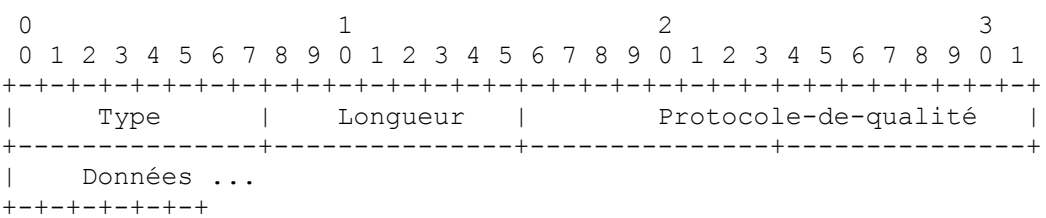
Description
Sur certaines liaisons, il peut être désirable de déterminer quand, et souvent comment, la liaison abandonne des données. Ce processus est appelé surveillance de la qualité de la liaison.

Cette option de configuration donne une méthode pour négocier l'utilisation d'un protocole spécifique pour la surveillance de la qualité de la liaison. Par défaut, la surveillance de la qualité de la liaison est désactivée.

La mise en œuvre qui envoie la Demande-de-configuration indique qu'elle s'attend à recevoir des informations de surveillance de la part de son homologue. Si une mise en œuvre envoie un Configure-Ack, elle est alors d'accord pour envoyer le protocole spécifié. Une mise en œuvre qui reçoit un Configure-Ack DEVRAIT s'attendre à ce que l'homologue envoie le protocole qui a fait l'objet de l'accusé de réception.

Il n'est pas exigé que la surveillance de qualité soit bidirectionnelle ou que le même protocole soit utilisé dans les deux directions. Il est parfaitement acceptable que des protocoles différents soient utilisés dans chaque direction. Cela va bien sûr, dépendre des protocoles spécifiques négociés.

Un résumé du format de l'option de configuration Protocole-de-qualité est donné ci-dessous. Les champs sont émis de gauche à droite.



Type : 4
Longueur : ≥ 4

Protocole-de-qualité
Le champ Protocole-de-qualité fait deux octets, et indique le protocole de surveillance de la qualité de liaison désiré. Les valeurs pour ce champ sont toujours les mêmes que les valeurs du champ Protocole PPP pour le même protocole de

surveillance.

Les valeurs à jour du champ Protocole-de-qualité sont spécifiées dans la plus récente version des "Numéros alloués" [RFC1700]. Les valeurs actuelles sont allouées comme suit :

Valeur (en hex)	Protocole
c025	Rapport de qualité de liaison

Données
Le champ Données fait zéro, un ou plusieurs octets, et contient des données supplémentaires selon ce qui est déterminé par le protocole concerné.

6.4 Numéro-magique

Description
Cette option de configuration donne une méthode pour détecter les liaisons mises en boucle et autres anomalies de couche de liaison des données. Cette option de configuration PEUT être exigée par certaines autres options de configuration telles que l'option de configuration Protocole-de-qualité. Par défaut, le Numéro-magique n'est pas négocié, et zéro est inséré lorsque un Numéro-magique pourrait autrement être utilisé.

Avant que cette option de configuration ne soit demandée, une mise en œuvre DOIT choisir son Numéro-magique. Il est recommandé que le Numéro-magique soit choisi de la façon la plus aléatoire possible afin de garantir avec une très forte probabilité qu'une mise en œuvre va arriver à un nombre univoque. Une bonne façon de choisir un nombre aléatoire univoque est de commencer par un germe univoque. Les sources d'unicité suggérées incluent des numéros de série de machine, des adresses d'autres matériels réseau, l'heure, etc. Des germes de nombre aléatoire particulièrement bons sont des mesures précises de l'heure de survenance d'événements physiques comme la réception de paquets sur d'autres réseaux connectés, l'heure de réponse d'un serveur, ou la vitesse de frappe d'un utilisateur humain. Il est aussi suggéré qu'autant de sources que possible soient utilisées simultanément.

Lorsque une Demande-de-configuration est reçue avec une option de configuration Numéro-magique, le Numéro-magique reçu est comparé au Numéro-magique de la dernière Demande-de-configuration envoyée à l'homologue. Si les deux Numéro-magique sont différents, la liaison n'est pas en boucle, et le Numéro-magique DEVRAIT être acquitté. Si les deux Numéro-magique sont égaux, il est alors possible, mais non certain, que la liaison soit mise en boucle et que cette Demande-de-configuration soit en fait celle qui vient d'être envoyée. Pour déterminer cela, un Configure-Nak DOIT être envoyé en spécifiant une valeur de numéro magique différente. Une nouvelle Demande-de-configuration NE DEVRAIT PAS être envoyée à l'homologue jusqu'à ce que le traitement normal cause son envoi (c'est-à-dire, jusqu'à ce qu'un Configure-Nak soit reçu ou que le temporisateur de redémarrage arrive à expiration).

La réception d'un Configure-Nak avec un Numéro-magique différent de celui du dernier Configure-Nak envoyé à l'homologue prouve que la liaison n'est pas mise en boucle, et indique un Numéro-magique unique. Si le Numéro-magique est égal à celui envoyé dans le dernier Configure-Nak envoyé, la possibilité d'une liaison en boucle augmente, et un nouveau Numéro-magique DOIT être choisi. Dans l'un et l'autre cas, une nouvelle Demande-de-configuration DEVRAIT être envoyée avec le nouveau Numéro-magique.

Si la liaison est bien en boucle, cette séquence (transmission d'une Demande-de-configuration, réception d'une Demande-de-configuration, transmission d'un Configure-Nak, réception d'un Configure-Nak) va se répéter sans fin. Si la liaison n'est pas en boucle, cette séquence peut survenir plusieurs fois, mais il est extrêmement peu vraisemblable qu'elle se produise de façon répétée. Il est plus vraisemblable que le Numéro-magique choisi à l'une ou l'autre extrémité va rapidement diverger, terminant ainsi la séquence. Le tableau suivant montre la probabilité d'une collision en supposant que les deux extrémités de la liaison choisissent des numéros magiques avec une distribution parfaitement uniforme :

Nombre de collisions	Probabilité
1	1/2**32 = 2,3 E-10
2	1/2**32**2 = 5,4 E-20
3	1/2**32**3 = 1,3 E-29

De bonnes sources d'unicité ou d'aléa sont nécessaires pour que survienne cette divergence. Si on ne peut pas trouver une bonne source d'unicité, il est recommandé que cette option de configuration ne soit pas activée ; les Demande-de-configuration qui ont l'option NE DEVRAIENT PAS être transmises et toutes les options de configuration Numéro-magique que l'homologue envoie DEVRAIENT être soit acquittées, soit rejetées. Dans ce cas, les liaisons en boucle ne peuvent pas être détectées fiablement par la mise en œuvre, bien qu'elles puissent encore être détectables par l'homologue.

Si une mise en œuvre transmet effectivement une Demande-de-configuration avec une option de configuration Numéro-magique, elle NE DOIT PAS répondre alors par un Configure-Rejet lorsque elle reçoit une Demande-de-configuration avec une option de configuration Numéro-magique. C'est-à-dire que si une mise en œuvre désire utiliser les numéros magiques, elle DOIT alors aussi permettre à son homologue de le faire. Si une mise en œuvre reçoit bien un Configure-Rejet en réponse à une Demande-de-configuration, cela ne peut que vouloir dire que la liaison n'est pas en boucle, et que son homologue ne va pas utiliser de numéro magique. Dans ce cas, une mise en œuvre DEVRAIT agir comme si la négociation avait réussi (comme si elle avait à la place reçu un Configure-Ack).

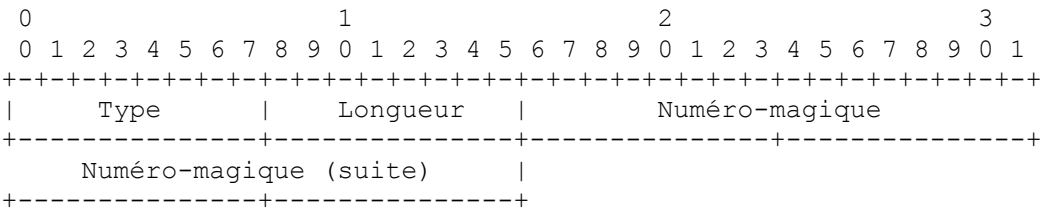
Le Numéro-magique peut aussi être utilisé pour détecter les liaisons en boucle durant le fonctionnement normal, aussi bien que durant une négociation d'option de configuration. Tous les paquets LCP Echo-Request, Echo-Reply, et Discard-Request ont un champ Numéro-magique. Si la négociation de Numéro-magique a réussi, une mise en œuvre DOIT transmettre ces paquets avec le champ Numéro-magique réglé au numéro magique négocié.

Le champ Numéro-magique de ces paquets DEVRAIT être inspecté à réception. Tous les champs Numéro-magique reçus DOIVENT être égaux à zéro ou au numéro magique unique de l'homologue, selon que l'homologue a négocié ou non un numéro magique.

La réception d'un champ Numéro-magique égal au numéro magique local négocié indique une liaison en boucle. La réception d'un numéro magique autre que le numéro magique local négocié, que le numéro magique négocié de l'homologue, ou zéro si l'homologue n'en a pas négocié un, indique une liaison qui a été (mal) configurée pour des communications avec un homologue différent.

Les procédures pour récupérer de l'un ou l'autre cas ne sont pas spécifiées, et peuvent varier d'une mise en œuvre à l'autre. Une procédure assez pessimiste est de supposer un événement de mort du LCP. Un autre événement Open va lancer le processus de rétablissement de la liaison, qui ne pourra s'achever qu'avec la fin de la condition de mise en boucle, et la réussite de la négociation de numéros magiques. Une procédure plus optimiste (dans le cas d'une liaison en boucle) est de commencer à transmettre des paquets LCP Echo-Request jusqu'à ce qu'une Echo-Reply appropriée soit reçue, ce qui indique la fin de la condition de bouclage.

Un résumé du format de l'option de configuration Numéro-magique est donné ci-dessous. Les champs sont émis de gauche à droite.



Type : 5
Longueur : 6

Numéro-magique
Le champ Numéro-magique fait quatre octets, et indique un nombre qui a une forte probabilité d'être univoque pour une extrémité de la liaison. Un numéro magique de zéro est illégal et DOIT toujours recevoir un Non-Accusé-de-réception, si il n'a pas été directement rejeté.

6.5 Compression du champ Protocole (PFC)

Description
Cette option de configuration donne une méthode de négociation de la compression du champ Protocole PPP. Par défaut, toutes les mises en œuvre DOIVENT transmettre les paquets avec des champs Protocole PPP de deux octets.

Les numéros de champ Protocole PPP sont choisis de telle façon que certaines valeurs puissent être compressées sous la forme d'un seul octet qu'on peut clairement distinguer de la forme à deux octets. Cette option de configuration est envoyée pour informer l'homologue que la mise en œuvre peut recevoir de tels champs Protocole d'un seul octet.

Comme on l'a mentionné précédemment, le champ Protocole utilise un mécanisme d'extension en cohérence avec le mécanisme d'extension ISO 3309 pour le champ Adresse ; le bit de moindre poids (LSB, *Least Significant Bit*) de chaque octet est utilisé pour indiquer l'extension du champ Protocole. Un "0" binaire comme LSB indique que le champ Protocole se continue avec l'octet suivant. La présence d'un "1" binaire comme LSB marque le dernier octet du champ Protocole.

Noter que tout nombre d'octets "0" peut être placé devant le champ, et va toujours indiquer la même valeur (considérer les deux représentations binaires de 3, 00000011 et 00000000 00000011).

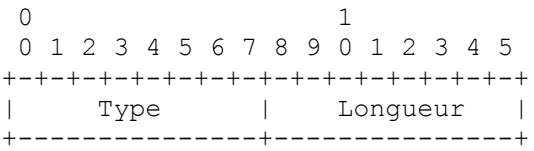
Lorsque on utilise des liaisons à faible débit, il est souhaitable de préserver la bande passante en envoyant aussi peu de données redondantes que possible. L'option de configuration de compression du champ Protocole permet un compromis entre simplicité de la mise en œuvre et efficacité de la bande passante. Si il est négocié avec succès, le mécanisme d'extension ISO 3309 peut être utilisé pour compresser le champ Protocole à un octet au lieu de deux. La grande majorité des paquets est compressible car les protocoles de données reçoivent normalement des valeurs de champ Protocole inférieures à 256.

Les champs Protocole compressés NE DOIVENT PAS être transmis si cette option de configuration n'a pas été négociée. Lorsque elle est négociée, les mises en œuvre de PPP DOIVENT accepter les paquets PPP avec des champs Protocole aussi bien à deux octets qu'à un seul, et NE DOIVENT PAS faire de distinction entre eux.

Le champ Protocole n'est jamais compressé lors de l'envoi d'un paquet LCP. Cette règle garantit une reconnaissance non ambiguë des paquets LCP.

Lorsque un champ Protocole est compressé, le champ FCS de la couche de liaison des données est calculé sur la trame compressée, et non sur la trame originale non compressée.

On donne ci-dessous un résumé du format de l'option de configuration Compression du champ Protocole. Les champs sont émis de gauche à droite.



Type : 7
Longueur : 2

6.6 Compression du champ Adresse-et-Contrôle (ACFC)

Description
Cette option de configuration donne une méthode de négociation de la compression des champs Adresse et Contrôle de la couche de liaison des données. Par défaut, toutes les mises en œuvre DOIVENT transmettre les trames avec les champs Adresse et Contrôle appropriés au tramage de la liaison.

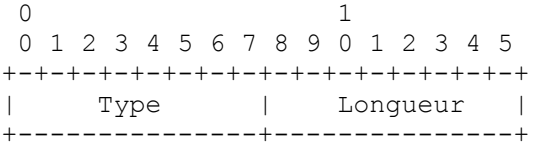
Comme ces champs ont normalement des valeurs constantes pour les liaisons en point à point, ils sont facilement compressés. Cette option de configuration est envoyée pour informer l'homologue que la mise en œuvre peut recevoir des champs Adresse et Contrôle compressés.

Si une trame compressée est reçue alors que la compression de champ Adresse et Contrôle n'a pas encore été négociée, la mise en œuvre PEUT éliminer la trame en silence.

Les champs Adresse et Contrôle NE DOIVENT PAS être compressés lors de l'envoi de tout paquet LCP. Cette règle garantit une reconnaissance non ambiguë des paquets LCP.

Lorsque les champs Adresse et Contrôle sont compressés, le champ FCS de couche de liaison des données est calculé sur la trame compressée, et non sur la trame originale non compressée.

On donne ci-dessous un résumé du format de l'option de configuration Compression de champ d'adresse et de contrôle. Les champs sont émis de gauche à droite.



Type : 8
Longueur : 2

7. Considérations pour la sécurité

Les questions de sécurité sont brièvement abordées dans les paragraphes concernant la phase d'authentification, l'événement Close, et l'option de configuration du protocole d'authentification.

8. Références

[RFC1547] D. Perkins, "Exigences pour une norme de protocole point à point Internet", , décembre 1993. *(Information)*

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir http://www.iana.org/numbers.html)*

9. Remerciements

Le présent document a été produit par le groupe de travail Protocole point à point de l'équipe d'ingénierie de l'Internet (IETF). Les commentaires devraient être envoyés à la liste de diffusion ietf-ppp@merit.edu.

Beaucoup du texte de ce document est tiré des exigences du groupe de travail [RFC1547]; et des RFC1171 & 1172, par Drew Perkins lorsqu'il était à l'Université Carnegie Mellon, et par Russ Hobby de l'Université de Californie à Davis.

William Simpson était principalement chargé d'introduire une terminologie et une philosophie cohérentes, et de la révision de la conception des automates de phase et de négociation d'état.

De nombreuses personnes ont passé un temps significatif à aider au développement du protocole point à point. La liste complète de ces gens est trop longue pour la donner ici, mais les personnes suivantes méritent des remerciements particuliers : Rick Adams, Ken Adelman, Fred Baker, Mike Ballard, Craig Fox, Karl Fox, Phill Gross, Kory Hamzeh, l'ancien président du groupe de travail Russ Hobby, David Kaufman, l'ancien président du groupe de travail Steve Knowles, Mark Lewis, l'ancien président du groupe de travail Brian Lloyd, John LoVerso, Bill Melohn, Mike Patton, l'ancien président du groupe de travail Drew Perkins, Greg Satz, John Shriver, Vernon Schryver, et Asher Waldfogel.

Des remerciements particuliers à Morning Star Technologies pour la fourniture des ressources de calcul et la prise en charge de l'accès réseau pour la rédaction de la présente spécification.

Adresse du président

Le groupe de travail peut être contacté via son président actuel :

Fred Baker
Advanced Computer Communications315 Bollay Drive
Santa Barbara, California 93117
fbaker@acc.com

Adresse de l'éditeur

Les questions sur le présent mémoire peuvent aussi être adressées à :

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071
Bill.Simpson@um.cc.umich.edu
bsimpson@MorningStar.com