www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

rfc1661

RFC : 1661
Remplace: 1548
Statut: Standard

Le Protocole Point-à-Point (PPP)

Edition originale : W. Simpson / Juillet 1994
Traduction : V.G. Frémaux / EISTI / Janvier 1998

Notes de traduction

Ce document est une traduction conforme et intégrale, sans omission ni rajout, du texte original de la norme. Par mesure de cohérence avec d'autres documents pouvant faire référence au présent, et non encore traduits, les abréviations de termes explicités ou de noms symboliques n'ont pas été (ou du moins pratiquement pas) modifiées, ce qui peut paraître un petit peu confus lorsque seules ces abréviations sont utilisées. Néanmoins, ce choix permettra de se reporter à cette version lorsque vous rencontrerez ces abréviations dans d'autres RFC traitant d'aspects similaires ou associés.

Statut de ce mémo

Ce document constitue une définition de standard pour un protocole de communication point à point pour la communauté Internet, et admet discussion et suggestions pour son amélioration. Reportez vous à l'édition en cours de la définition des protocoles Internet "Internet Official Protocol Standards" (STD 1) pour connaître le dernier état de ce protocole. La distribution du présent est libre.

Contexte

Le protocole Point à Point (PPP) propose une méthode standard pour le transport de datagrammes multi-protocoles sur une liaison simple point à point. PPP comprend trois composants principaux:

Une méthode pour encapsuler les datagrammes de plusieurs protocoles.

Un protocole de contrôle du lien "Link Control Protocol" (LCP) destiné à établir, configurer, et tester la liaison de données.

Une famille de protocoles de contrôle de réseau "Network Control Protocols" (NCPs) pour l'établissement et la configuration de plusieurs protocoles de la couche "réseau".

Ce document définit l'organisation et les méthodes utilisées par PPP, ainsi que l'encapsulation effectuée par ce protocole, un mécanisme extensible de négociation d'options capable de négocier une large gamme de paramètres de configuration et apportant des fonctions étendues de gestion. Le protocole PPP Link Control Protocol (LCP) est décrit dans le contexte de ce mécanisme.

Table des Matières

1. Introduction
   Encapsulation
   Protocole de contrôle de liaison (Link Control Protocol)
   Protocole de gestion réseau (Network Control Protocol)
   Configuration
 1.1. Note sur la sémantique
 1.2. Terminologie
2. Encapsulation PPP

Champ protocole
Champ Information
Bourrage
3. Fonctionnement d'une liaison PPP
3.1. Vue d'ensemble
3.2. Diagramme d'états
3.3. "Link Dead" (couche physique non prête)
3.4. Etablissement
3.5. Authentification
3.6. Phase de négociation réseau
3.7. Fermeture de liaison
4. L'automate de négociation d'options
4.1. Table de transition d'états
4.2. Etats
Initial
Démarrage (Starting)
Fermé (Closed)
Arrêté (Stopped)
Fermeture en cours (Closing)
Arrêt en cours (Stopping)
Connexion-demandée (Request-Sent)
Connexion-Acquittée (Ack-Received)
Aquittement-connexion (Ack-Sent)
Ouvert (Opened)
4.3. Evénements
Up
Down
Ouverture (Open)
Fermeture (Close)
Temporisation (TO+,TO-)
Requête-Configuration-Reçue (RCR+,RCR-)
Acquitement-Configuration-Reçue (RCA)
Configuration-NonAcquittée/Rejetée-Reçue (RCN)
Requête-Fermeture-Reçue (RTR)
Acquittement-Fermeture-Reçue (RTA)
Code-Inconnu-Reçu (RUC)
Code-Rejeté-Reçu, Protocole-Rejeté-Reçu (RXJ+,RXJ-)
Requête-Echo-Reçu, Réponse-Echo-Reçu, Requête-Elimination-Reçu. (RXR)
4.4. Actions
Evénement-Illégal (-)
Ouvrir (tlu)
Fermer (tld)
Démarrer (tls)
Terminer (tlf)
Init-Compteur-Reprise (irc)
Zero-Compteur-Reprise (zrc)
Emission-Requête-Configuration (scr)
Emission-Configuration-Acquittée (sca)
Emission-Configuration-NonAcquittée (scn)
Emision-Requête-Fermeture (str)
Emission-Fermeture-Acquittée (sta)
Emission-Code-Rejeté (scj)
Emission-Réponse-Echo (ser)
4.5. Elimination de rebouclages
4.6. Compteurs et Temporisations
Temporisation de Reprise
Max-Fermeture
Max-Configuration

Max-Echec
5. Formats de paquets LCP
Code
Identificateur
Longueur
Données
5.1. Requête-Configuration
5.2. Configuration-Acquittée
5.3. Configuration-NonAcquittée
5.4. Configuration-Rejetée
5.5. Requête-Fermeture et Fermeture-Acquittée
5.6. Code-Rejeté
5.7. Protocole-Rejeté
5.8. Requête-Echo et Réponse-Echo
5.9. Requête-Elimination
6. Options de Configuration LCP
Philosophie
Type
Longueur
Données
6.1. Unité-Réception-Maximale (URM)
6.2. Protocole-Authentification
6.3. Protocole-Qualité
6.4. Nombres-Magiques
6.5. Compression-Champ-Protocole (PFC)
6.6. Compression-Adresse-et-Contrôles (ACFC)
Considérations sécuritaires
Références
Remerciements
Contact

1. Introduction

Le protocole Point-à-Point est utilisé pour des liaisons simples transportant des paquets de données entre deux éléments. Ces liens permettent une communication simultanée bidirectionnelle (full-duplex), et sont supposés transmettre des paquets dans l'ordre. PPP propose une solution commune pour un raccordement aisé d'une grande variété d'hôtes, de ponts et de routeurs [1].

Encapsulation

L'encapsulation PPP permet le multiplexage de différentes connexions protocolaires au niveau réseau simultanées sur la même liaison physique. Cette encapsulation a été conçue dans l'exigence d'une excellente compatibilité avec la plus grande variété de matériels.

Seuls 8 octets supplémentaires sont nécessaires pour accomplir l'encapsulation lorsque ce protocole est utilisé dans des trames de type HDLC. Dans des environnements dans lesquels la bande passante est une préoccupation majeure, cette encapsulation et la mise en trame peut être réduite à 2 ou 4 octets.

Pour permettre des implémentations à haute vitesse, l'encapsulation par défaut utilise des champs élémentaires, un seul d'entre eux devant être examiné pour réaliser le démultiplexage. L'en-tête par défaut et les champs d'information tombent toujours sur des limites de mots de 32-bits, la fin de message pouvant être complétée par des octets de "bourrage".

Protocole de contrôle de liaison (Link Control Protocol)

Afin d'être suffisamment souple pour pouvoir être porté dans de nombreux environnements, le protocole PPP dispose d'un protocole de contrôle de liaison (Link Control Protocol - LCP). Le LCP est utilisé pour effectuer la négociation automatique des options de format d'encapsulation, la gestion de tailles variables de

paquets, la détection d'un rebouclage de liaison ainsi que d'autres erreurs courantes de configuration, ainsi que pour gérer la rupture de liaison. Les autres fonctionnalités apportées concernent l'authentification de l'identité de l'hôte dans lequel il est implémenté, ainsi que la détection de fautes de fonctionnement sur la liaison.

Protocole de gestion réseau (Network Control Protocol)

Les liaisons Point-à-Point tendent à mettre en exergue de nombreux problèmes vis à vis de protocoles réseaux communs. Par exemple, l'assignation et la gestion des adresses IP, pouvant poser des problèmes y compris dans l'environnement limité d'un LAN, est particulièrement délicate lorsque la liaison passe par un réseau de type circuit commuté (par exemple une connexion modem via réseau téléphonique). Ces problèmes sont gérés par une famille de protocoles de gestion réseau (Network Control Protocols - NCPs), chacun traitant des aspects particuliers à la gestion de tel ou tel type de protocole de niveau réseau. Ces protocoles NCPs sont définis dans des documents associés.

Configuration

Le but des liaisons PPP est qu'elles soient facilement configurables. Du fait de leur design, les paramètres standard par défaut correspondent aux configurations les plus communes. Les implémenteurs pourront passer dans un mode amélioré, dont les paramètres seront automatiquement transmis au correspondant sans aucune intervention de l'opérateur. En fin, l'opérateur pourra configurer explicitement certaines options nécessaires au fonctionnement de la liaison dans son environnement, laquelle configuration ne pourrait être effectuée autrement.

L'auto-configuration de la liaison est implémentée grâce à un mécanisme de négociation d'options extensible, par lequel chaque extrémité de la liaison renseigne l'autre de ses possibilités et de ses contraintes propres. Bien que ce mécanisme de négociation d'options ne soit décrit dans ce document qu'en rapport avec le Link Control Protocol (LCP), les fonctionnalités en sont suffisamment générales pour pouvoir être réutilisées par d'autres protocoles de contrôle, parmi lesquels la famille des protocoles NCP.

1.1. Note sur la sémantique

Dans ce document, plusieurs mots différents sont utilisés pour exprimer la force d'une obligation ou le statut d'une recommandation. Ces mots seront souvent écrits en capitales.

DOIT, DEVRA

Ce mot, ou l'utilisation des adverbes "nécessairement" ou "obligatoirement", signifie que le comportement exprimé est une condition sine qua non à remplir pour la conformité au standard.

NE DOIT PAS

Cette expression, ou l'utilisation des adjectifs "interdit" ou "prohibé" indique une interdiction absolue du comportement décrit.

DEVRAIT

Associé à la sémantique de "recommandé", signifie qu'il peut exister des raisons valables et légitimes pour que dans certaines circonstances, le comportement décrit soit ignoré, mais que ne pas implémenter ce dernier doit être le résultat d'une analyse minutieuse des conséquences. Une implémentation complète devra se tenir à implémenter ces comportements "conseillés".

POURRAIT, POURRA

Associé à la sémantique "optionnel", signifie que ce comportement est un autorisé parmi une série d'alternatives possibles. Une implémentation qui ignore cette option DEVRA néanmoins s'attendre à interopérer avec une autre implémentation qui peut, quant à elle, l'utiliser.

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

1.2. Terminologie

Ce document utilise abondamment les termes suivants:

Datagramme

L'unité de transmission de la couche réseau (par exemple IP). Un datagramme peut être encapsulé dans un ou plusieurs paquets passés à la couche liaison.

Trame

L'unité de transmission de la couche liaison. Une trame peut comporter une en-tête et/ou une queue, et bien sûr des octets de données.

Paquet

L'unité d'encapsulation de base, passant entre la couche réseau et la couche liaison de données. Un paquet est en général associé à une trame; sauf pour les cas particuliers où une fragmentation du paquet doit être opérée, où lorsque plusieurs paquets sont insérées dans une trame unique.

Correspondant (peer)

L'autre extrémité d'une liaison point-à-point.

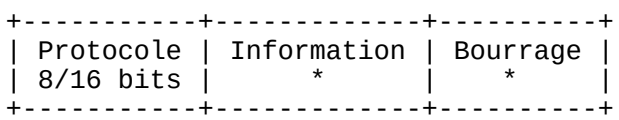
Paquets ignorés

Se dit lorsque l'implémentation élimine et détruit le paquet sans autre traitement ultérieur. L'implémentation DEVRAIT proposer la possibilité d'archiver l'erreur, y compris le contenu du paquet détruit, et DEVRAIT pouvoir établir des statistiques sur ce genre d'événements.

2. Encapsulation PPP

L'encapsulation PPP est utilisée pour lever l'ambiguïté sur des datagrammes provenant de protocoles différents. Cette encapsulation nécessite l'usage d'un tramage dont le but principale est d'indiquer le début et la fin de l'encapsulation. Des méthodes pour réaliser ce tramage sont décrites dans des documents associés au présent.

Une explicitation sommaire de l'encapsulation PPP est donnée ci-dessous. Les champs sont toujours transmis de gauche à droite.



Champ protocole

Le Protocole comprend un ou deux octets, et sa valeur identifie le datagramme encapsulé dans le champ Information du paquet. Ce champ est transmis et reçu l'octet le plus significatif en tête.

La structure de ce champ est conforme aux mécanismes définis par l'ISO 3309 pour l'extension des champs d'adresse. Tous les Protocoles DOIVENT être impairs; le bit le moins significatif de l'octet le moins significatif DOIT être égal à "1". De plus, tous les Protocoles DOIVENT être codés de sorte que le bit le moins significatif de l'octet le plus significatif soit égal à "0". Les trames reçues qui ne se conforment pas à ces règles DOIVENT être considérées comme transportant un Protocole non identifié.

Les valeurs du champ Protocole comprises dans la plage "0***" à "3***" identifient un protocole de niveau réseau de paquets spécifiques, et des valeurs entre "8***" et "b***" identifient des paquets appartenant aux Network Control Protocols (NCPs) associés, le cas échéant.

Des valeurs de champ de protocole comprises entre "4***" et "7***" sont utilisées pour des protocoles de faible trafic et ne disposant pas de NCP associé. Les valeurs entre "c***" et "f***" identifient des paquets appartenant aux Link Control Protocols (comme LCP).

Les valeurs les plus récentes établies pour ce champ Protocole sont listées dans le document "Assigned Numbers" [2]. La spécification suivante réserve les valeurs :

Valeur (en hexa)	Nom de protocole
0001	Protocole de bourrage
0003 à 001f	réservé (non transparents)
007d	réservé (Control Escape)
00cf	réservé (PPP NLPID)
00ff	réservé (non comprimables)
8001 à 801f	non utilisé
807d	non utilisé
80cf	non utilisé
80ff	non utilisé
c021	Link Control Protocol
c023	Password Authentication Protocol
c025	Link Quality Report
c223	Challenge Handshake Authentication Protocol

Les développeurs de nouveaux protocoles DOIVENT obtenir un numéro de protocole de l'Internet Assigned Numbers Authority (IANA), à IANA@isi.edu.

Champ Information

Le champ Information contient zéro octets au minimum. Il contient le datagramme du protocole spécifié dans le champ Protocole.

La longueur maximum du champ Information, y compris le bourrage, mais hors champ Protocole, est limité à l'Unité de Réception Maximale (URM), par défaut 1500 octets. Par négociation, des implémentations de PPP plus "libérales" pourront utiliser d'autres valeurs d'URM.

Bourrage

En transmission, le champ Information PEUT être complété d'un nombre arbitraire d'octets de "bourrage" dans la limite de la règle de l'URM. C'est à chaque protocole que revient le travail de dissocier les octets de bourrage de l'information utile.

3. Fonctionnement d'une liaison PPP

3.1. Vue d'ensemble

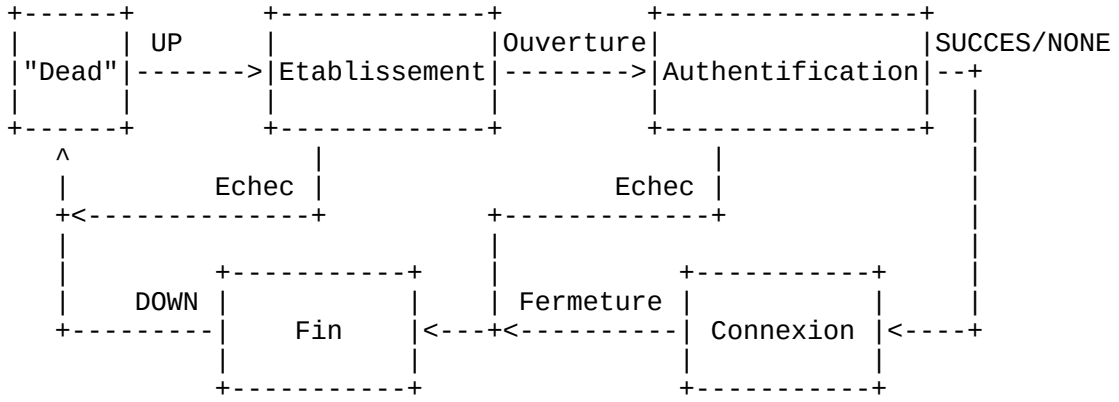
Afin d'établir une communication sur un lien point-à-point, chaque extrémité du lien PPP DOIT d'abord émettre des paquets LCP pour configurer et tester le support de liaison. Une fois la liaison établie, le correspondant POURRA être authentifié.

Ensuite, PPP DOIT envoyer des paquets NCP pour choisir et configurer un ou plusieurs protocoles réseau disponibles. Une fois que les protocoles réseau choisis ont été configurés, les datagrammes pour chacun de ces protocoles réseau peuvent être envoyés sur la liaison.

La liaison restera disponible et configurée pour la communication jusqu'à ce que des paquets LCP ou NCP ne ferment explicitement la liaison, à moins qu'un événement extérieur ne survienne (par exemple une temporisation d'inactivité, ou l'intervention de l'administrateur).

3.2. Diagramme d'états

Dans les processus de configuration, de maintien et de clôture de liaison point-à-point, le lien PPP rencontre un certain nombre d'états décrits de façon sommaire par le schéma suivant :



Toutes les transitions possibles ne sont pas explicitées dans ce diagramme. La sémantique suivante DOIT être adoptée.

3.3. "Link Dead" (couche physique non prête)

Une communication débute et se termine nécessairement dans cet état. Lorsqu'un événement extérieur (comme une détection de porteuse ou la configuration par l'administrateur réseau) indique que le niveau physique est en état pour un processus de connexion, PPP passera la liaison en phase d'établissement.

Durant cette phase, l'automate LCP (décrit plus loin) sera dans l'état Initial ou Démarrage. Le passage à l'état Etablissement sera signalée par un événement Up à l'automate LCP.

Note d'implémentation :

Typiquement, une liaison doit retomber dans cet état après toute déconnexion du modem. Dans le cas d'une liaison filaire permanente, cette état pourra n'être maintenu que pendant une très courte durée – cependant suffisamment longue pour pouvoir simuler un état repos effectif.

3.4. Etablissement

Le protocole de liaison Link Control Protocol (LCP) est utilisé pour établir la connexion grâce à l'échange de paquets de Configuration. Cet échange est totalement résolu, et l'automate LCP entre dans l'état Ouvert, lorsque des paquets d'acquittement *Configuration-Acquittée* (décrits plus loin) ont été reçus des deux côtés.

Toutes les options de Configuration sont supposées être à leur valeur par défaut avant d'être modifiées par l'échange de configuration. Voir le chapitre sur les options de configuration LCP pour plus de détails.

Il est important de noter que seules les options de configuration indépendantes de tout protocole réseau sont configurées par LCP. La configuration de chacun des protocoles réseau est réalisée via des protocoles Network Control Protocols (NCPs) spécifiques durant la phase de configuration réseau. Tout paquet non-LCP reçu pendant cette phase DOIT être ignoré.

La réception d'une requête pour configuration LCP provoque un retour à l'état d'établissement de liaison à partir de l'état de configuration réseau ou de la phase d'authentification.

3.5. Authentification

Sur certaines liaisons il peut être pertinent d'imposer une authentification du correspondant avant de permettre toute négociation protocolaire au niveau réseau.

Par défaut, l'authentification n'est pas demandée. Lorsqu'une implémentation impose que le correspondant s'authentifie à l'aide d'un protocole d'authentification particulier, alors il DOIT explicitement demander l'usage de ce protocole d'authentification pendant la phase d'établissement de la liaison.

L'authentification DEVRAIT être faite le plus tôt possible après la conclusion de la phase d'établissement. La détermination de la qualité de la liaison POURRA être réalisée dans le même temps. Toutefois, une implémentation correcte NE DOIT PAS permettre un échange de paquets de mesure de la qualité de liaison, dans le but de retarder indéfiniment le processus d'authentification.

Le passage de la phase d'authentification à la phase de négociation de protocole réseau NE DOIT PAS être accepté avant que l'authentification n'ait abouti avec succès. Si l'authentification échoue, l'authentificateur DEVRAIT plutôt entamer une phase de fermeture de liaison.

Les paquets LCP, d'authentification, et de mesure de qualité de liaison sont les seuls autorisés pendant cette phase. Tout autre forme de paquet DOIT être ignoré.

Notes d'implémentation :

Une implémentation NE DOIT PAS faire échouer un processus d'authentification sur une simple temporisation ou une absence de réponse. L'authentification DEVRAIT permettre un certain nombre de tentatives, et ne conclure à un échec seulement lorsque le nombre de tentatives maximum est "consommé".

C'est dans tous les cas l'implémentation qui a refusé d'authentifier son correspondant qui doit entamer la phase de fermeture de liaison.

3.6. Phase de négociation réseau

Une fois que PPP a achevé les procédures précédentes, chaque protocole réseau (tels qu'IP, IPX, ou AppleTalk) DOIT être configuré séparément via un protocole Network Control Protocol (NCP). Chaque NCP DEVRAIT pouvoir être Ouvert et Fermé à tout moment.

Notes d'implémentation :

Comme il se peut que certaines implémentations demandent un temps non négligeable pour mesurer la qualité de liaison, les modules PPP DEVRAIENT éviter l'utilisation de temporisations à durée fixe entre la fin de l'authentification et le début d'une négociation NCP.

Lorsqu'un NCP atteint l'état Ouvert, la liaison PPP est alors prête à véhiculer les paquets du protocole réseau associé. Tout paquet dans un protocole géré par NCPs arrivant alors que le NCP associé (ou associable) est en état fermé doit être ignoré.

Lorsque le LCP est dans son état ouvert, tout paquet protocolaire non supporté par l'implémentation DOIT être retourné à l'émetteur dans un paquet *Protocole-Rejeté* (décrit plus loin). Seuls les protocoles gérés (mais de NCP fermés) sont ignorés.

Dans cet état, le trafic sur le lien est composé de toute combinaison de paquets LCP, NCP, et datagrammes réseau.

3.7. Fermeture de liaison

PPP peut fermer la liaison à tout moment. Ceci peut survenir suite à une perte de porteuse, l'échec d'une authentification, la détection d'une qualité de liaison insuffisante, la chute d'une temporisation d'attente, ou la fermeture de la liaison du fait d'une décision humaine.

Le protocole LCP est utilisé pour procéder à la clôture de la liaison par l'échange de paquets de Clôture. Lors de la fermeture, PPP en informe tout d'abord les couches réseau afin que ces dernières puissent prendre leurs dispositions.

Après l'échange des paquets de Clôture, l'implémentation DEVRAIT signaler à la couche physique de procéder à la déconnexion physique, particulièrement utile dans le cas de l'échec d'une authentification. L'émetteur d'une Requête pour Clôture DEVRAIT se déconnecter juste après avoir reçu un acquittement de Clôture, ou au plus tard après que la temporisation de Reprise soit écoulée. Le récepteur d'une Requête pour Clôture DEVRAIT attendre la déconnexion du correspondant, et NE DOIT PAS se déconnecter pendant au

moins la durée d'une temporisation de Reprise comptée à partir de l'émission de l'acquittement de Clôture. PPP DEVRAIT passer en état "Link Dead".

Tout paquet autre que LCP reçu durant cette phase DOIT être ignoré.

Note d'implémentation :

La fermeture d'une liaison par LCP est suffisante. Les différents NCP actifs n'ont pas l'obligation d'envoyer chacun leur salve de paquets de clôture. Inversement, la rupture d'une communication réseau par un NCP n'est pas une raison suffisante pour la coupure de la liaison PPP, même s'il s'agit du dernier NCP actif sur la liaison.

4. L'automate de négociation d'options

L'automate à nombre d'états fini est défini par des événements, des actions et des transitions entre états. Les événements incluent la réception de commandes externes telles que Open et Close, la retombée de la temporisation de Reprise, et la réception de paquets via la liaison. Les actions comprennent le démarrage de la temporisation de Reprise et l'émission de paquets vers le correspondant.

Certains types de paquets -- *Configuration-NonAcquittée* et *Configuration-Rejetée*, ou *Code-Rejeté* et *Protocole-Rejeté*, ou *Requête-Echo*, *Réponse-Echo* et *Requête-Elimination* – ne sont pas différentiés dans la description de l'automate. Comme ceci sera décrit plus tard, ces paquets correspondent cependant à des usages différents. Ils génèrent cependant toujours des transitions identiques.

Evénements	**Actions**
Up = couche inférieure prête	tlu = Couche prête
Down = couche inférieure non prête	tld = Couche non prête
Open = commande administrateur Open	tls = Démarrer
Close = commande administrateur Close	tlf = Terminer
TO+ = Temporisation non expirée > 0	irc = Initialiser-Reprise
TO- = Temporisation expirée	zrc = Réinitialiser-compteur
RCR+ = Requête-Configuration-Reçue (Correcte)	scr = Emission-Requête-Configuration
RCR- = Requête-Configuration-Reçue (Incorrecte)	
RCA = Configuration-Acquittée-Reçu	sca = Emission-Configuration-Acquittée
RCN = Configuration-NonAcquittée/Rejetée-Reçu	scn = Emission-Configuration-NonAcquittée/Rejetée
RTR = Requête-Fermeture-Reçue	str = Emission-Requête-Fermeture
RTA = Fermeture-Acquittée-Reçu	sta = Emission-Fermeture-Acquittée
RUC = Code-Inconnu-Reçu	scj = Emission-Code-Rejeté
RXJ+ = Code-Rejeté-Reçu (non critique) ou Protocole-Rejeté-Reçu	
RXJ- = Code-Rejeté-Reçu (critique) ou Protocole-Rejeté-Reçu	
RXR = Requête-Echo-Reçu	ser = Emission-Echo-Réponse
RRR = Réponse-Echo-Reçu ou Requête-Elimination-Reçu	

4.1. Table de transition d'états

La table complète des transitions d'état est donnée ci-après. Les états sont indiqués horizontalement, et les événements verticalement. Les transitions entre états et les actions sont représentés sous la forme d'un couple action/nouvel-état. Des actions multiples sont séparées par des virgules, et peuvent être exprimées sur plusieurs lignes successives; les actions multiples pourront être implémentées dans n'importe quel ordre. L'état peut être suivi d'une lettre, renvoyant à une note explicative. Le tiret ('-') marque une transition illégale.

	Etat					
	0	1	2	3	4	5
Events	Initial	Starting	Closed	Stopped	Closing	Stopping
Up	2	irc,scr/6	-	-	-	-
Down	-	-	0	tls/1	0	1

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

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

	State			
Events	6 Req-Sent	7 Ack-Rcvd	8 Ack-Sent	9 Opened
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 la temporisation Reprise tourne sont identifiables par la possibilité d'événements TO. Seules les actions Emission-*Requête-Configuration*, Emission-*Requête-Fermeture* et Réinitialiser-Compteur démarrent ou redémarrent la temporisation de Reprise. La temporisation est arrêtée lors de toute transition d'un état permettant le comptage de temporisation vers un état ne la permettant pas.

Les événements et les actions sont implémentées selon une architecture d'échange de messages, plutôt que par gestion de signaux. Si l'on désire qu'une action contrôle certains signaux (par exemple DTR), des actions supplémentaires devront être définies.

[p] Option passive; voir Arrêté(Stopped).
[r] Option de redémarrage; voir l'événement ouverture.
[x] Connexion croisée; voir l'événement RCA.

4.2. Etats

Ce qui suit est une description plus détaillée de chaque état de l'automate.

Initial

Dans l'état Initial, la couche physique est indisponible (Down), et aucune demande d'ouverture n'est intervenue. La temporisation de Reprise ne tourne pas dans l'état Initial.

Démarrage (Starting)

L'état de démarrage est la réponse à une demande d'ouverture par une commande administrateur Open à partir de l'état Initial. Cet état survient dès réception de l'ordre Open, bien que la couche physique ne soit toujours pas disponible (Down). La temporisation de Reprise ne tourne pas dans cet état.
Dès que la couche physique devient prête (Up), une Requête de Configuration est émise.

Fermé (Closed)

L'état Fermé résulte d'une action de fermeture alors que le lien physique est disponible (Up), mais que le lien n'est pas dans un état opérationnel. La temporisation de Reprise ne tourne pas dans cet état.

Sur réception d'une *Requête-Configuration*, un paquet *Fermeture-Acquittée* est émis. Les paquets *Fermeture-Acquittée* sont ignorés pour éviter un fonctionnement en boucle.

Arrêté (Stopped)

L'état arrêté (Stopped) est la conséquence d'une fermeture à partir d'un état ouvert du lien. Il est atteint lorsque l'automate attend un événement Down après l'action de fermeture, ou après avoir envoyé un message Emission-*Fermeture-Acquittée*. La temporisation de Reprise ne court pas dans cet état.

Lorsqu'un paquet *Requête-Configuration* est reçu, une réponse appropriée est envoyée. La réception de tout autre paquet entraîne l'émission d'un paquet *Fermeture-Acquittée*. Ces mêmes paquets *Fermeture-Acquittée* seront ignorés en réception pour éviter de boucler le protocole.

Justification :

L'état arrêté (Stopped) est un état intermédiaire lors de la coupure d'une liaison, l'échec d'une configuration, et d'autres modes d'échec de l'automate. Ces états à priori distincts ont été combinés dans cette étape.

Il existe une concurrence temporelle entre la réponse par l'événement Down (attendu après l'action Terminer de la couche PPP) et l'apparition possible d'un événement *Requête-Configuration*-Reçue. Lorsqu'une *Requête-Configuration* arrive avant la chute de ligne (Down), ce dernier événement prévaudra et la ligne reviendra à l'état initial dès sa réception. Ceci protège le protocole contre les attaques par répétition.

Option d'implémentation :

Lorsque le distant ne parvient pas à répondre à une *Requête-Configuration* locale, l'implémentation POURRA attendre la réception d'une *Requête-Configuration* distante. Dans ce cas, l'action Terminer ne sera pas effectuée lorsque l'événement TO- survient dans les états Connexion-demandée, Connexion-Acquittée et Acquitement-connexion.

Cette option est utile dans le cas de lignes permanentes dédiées, ou circuits ne disposant pas de signalisation d'état physique de ligne, mais doit être proscrite pour des lignes câblées sur un réseau commuté.

Fermeture en cours (Closing)

En Fermeture, une tentative est faite pour fermer la connexion. Une *Requête-Fermeture* a été émise et la temporisation de Reprise tourne, l'acquittement de fermeture n'a pas encore été reçu.

En réponse à un événement *Fermeture-Acquittée*-reçu, l'automate passe en état Fermé.

Lorsque la temporisation de Reprise expire, une nouvelle *Requête-Fermeture* est émise, et la temporisation relancée. Lorsque la temporisation a expiré un nombre de fois fixé, l'automate passe alors en état Fermé.

Arrêt en cours (Stopping)

L'état Arrêt en Cours est à l'état Arrêté ce que la Fermeture en Cours est à l'état Fermé. Une *Requête-Fermeture* a été émise et la temporisation de Reprise tourne, un *Fermeture-Acquittée* n'a pas encore été reçu.

Justification :

L'état Arrêt en Cours définit parfaitement comment terminer une communication avant de permettre le passage de nouvelles données. Une fois la liaison coupée, une nouvelle configuration peut être demandée par l'état Arrêté ou Démarrage.

Connexion-demandée (Request-Sent)

Dans l'état Connexion-demandée, une configuration peut prendre place pour initialiser la liaison. Un paquet *Requête-Configuration* a été émis et la temporisation de Reprise est mise en route. Dans cet état, un paquet *Configuration-Acquittée* n'a ni été reçu, et encore moins émis.

Connexion-Acquittée (Ack-Received)

Dans l'état de Connexion-Acquittée (Ack-Received), un paquet *Requête-Configuration* a été émis et un *Configuration-Acquittée* distant reçu. La temporisation de Reprise tourne toujours, dans la mesure où le paquet local *Configuration-Acquittée* n'a pas été encore envoyé.

Aquittement-connexion (Ack-Sent)

Dans l'état d'Acquittement-Connexion, un paquet de *Requête-Configuration* et un *Configuration-Acquittée* ont tous deux été émis, mais le distant n'a toujours pas acquitté à son tour la configuration négociée. La temporisation de Reprise tourne, tant que cette réponse n'est pas parvenue au local.

Ouvert (Opened)

Dans l'état Ouvert, les acquittements de configuration ont été échangés. La temporisation de Reprise s'arrête.

Lorsque cet état est atteint par l'automate, l'implémentation DEVRAIT émettre vers la couche supérieure un événement Up. A l'inverse, lorsque cet état est quitté, l'implémentation DEVRAIT émettre un signal Down vers la couche supérieure.

4.3. Evénements

Les transitions et les actions de l'automate sont causés par des événements.

Up

Cet événement survient lorsque la couche basse de protocole est prête à transporter des paquets de données.

Typiquement, cet événement est généré par un pilote de modem, ou par toute autre interface entre PPP et un gestionnaire de média physique, pour signaler au LCP que la liaison entre dans la phase d'Etablissement.

Il sera l'occasion pour le LCP de signaler à chaque NCP que la liaison admet désormais un fonctionnement au niveau réseau., l'action Couche-Prête du LCP déclenchera les actions Up de chaque NCP.

(NdT: cette couche devenant alors la couche inférieure des NCP).

Down

Cet événement survient lorsque la couche basse de protocole n'est plus en mesure de transporter des paquets de données.

Typiquement, cet événement est généré par un pilote de modem, ou par toute autre interface entre PPP et un gestionnaire de média physique, pour signaler au LCP que la liaison entre dans un état non opérationnel.

Il sera l'occasion pour le LCP de signaler à chaque NCP que la liaison quitte le fonctionnement au niveau réseau., l'action Couche-non-Prête du LCP déclenchera les actions Down de chaque NCP.

Ouverture (Open)

Cet événement indique que la mise en œuvre de la liaison est demandée par l'administrateur humain ou une couche supérieure. Lorsqu'il apparaît, et que la liaison n'est pas déjà dans l'état Ouverte, l'automate essayera d'émettre des paquets de configuration au distant.

Si l'automate est dans l'impossibilité de commencer cette configuration (la ligne est physiquement indisponible, ou une commande Close précédente n'est pas encore totalement traitée), l'établissement de la nouvelle communication est automatiquement différé.

Lorsqu'une *Requête-Fermeture* est reçue, ou tout autre événement qui rend le lien non disponible, l'automate progressera vers un état dans lequel une réouverture de la ligne est possible. Aucune autre intervention de l'administrateur n'est nécessaire.

Option d'implémentation :

L'expérience a démontré que les utilisateurs relancent en général une nouvelle commande Open lorsqu'ils désirent renégocier la liaison. Cette action indique en général que les paramètres de la liaison sont à modifier.

Comme il ne s'agit pas de la sémantique exacte de l'événement d'Ouverture, il est suggéré que l'implémentation lance un événement Down immédiatement suivi d'un événement Up, lorsqu'une commande Open est exécutée alors que l'automate est dans l'un des états Ouvert, Fermeture en Cours, Arrêt en Cours, ou Arrêté. On prendra garde dans ce cas que l'avènement de l'événement Down ne puisse être provoqué par une autre cause.

La succession d'un Down puis d'un Up va provoquer une renégociation de la liaison, en suivant la progression passant par les états Démarrage et Connexion-demandée. La connexion est ainsi renégociée sans effets de bords notable.

Fermeture (Close)

Cet événement indique que la liaison ne doit plus véhiculer de données; en d'autre termes, l'administrateur de réseau (humain ou logiciel) a avisé que la liaison ne doit plus resté en état Ouvert. Lorsque cet événement survient, et la liaison n'est pas déjà Fermée, l'automate va tenter d'interrompre la connexion. Des tentatives ultérieures de reconfiguration de la liaison seront refusées tant qu'un nouvel événement Open n'intervient pas.

Note d'implémentation :

Lorsque une authentification échoue, la liaison DEVRAIT être coupée, pour éviter une attaque par répétition et le refus de service aux autres utilisateurs. Comme la liaison est encore administrativement disponible (par définition), ceci pourrait être accompli en simulant une commande Close donnée au LCP, immédiatement suivie d'une commande Open. On prendra garde dans ce cas que l'avènement de l'événement Close ne puisse être provoqué par une autre cause.

L'événement Close suivi d'un Open provoque une coupure normale de la ligne, progressant depuis l'état Fermeture en Cours vers l'état Arrêt en Cours, l'action Terminer entraîne la déconnexion physique de la ligne. L'automate attend alors la prochaine demande de connexion dans l'état Arrêté ou Démarrage.

Temporisation (TO+,TO-)

Cet événement indique l'expiration de la temporisation de Reprise. Cette temporisation sert à quantifier l'attente maximum d'une réponse à une *Requête-Configuration* et une *Requête-Fermeture*.

L'événement TO+ indique que le compteur de Reprise est toujours positif, ce qui provoque la réémission d'un paquet *Requête-Configuration* ou *Requête-Fermeture* suivant le cas.

L'événement TO- indique que le compteur de Reprise est passé à zéro, et aucun paquet de Requête ne doit être réémis dans ce cas.

Requête-Configuration-Reçue (RCR+,RCR-)

Cet événement survient lorsqu'un paquet *Requête-Configuration* distant est reçu. Cette *Requête-Configuration* indique que le distant souhaite ouvrir une communication et peut y spécifier des options de configuration. Le paquet *Requête-Configuration* est présenté en détail plus loin.

L'événement RCR+ indique que la *Requête-Configuration* est légitime, et déclenche la transmission d'un paquet *Configuration-Acquittée*.

L'événement RCR- indique que la *Requête-Configuration* n'est pas légitime, ou acceptable, et déclenche la transmission d'un paquet *Configuration-Rejetée* ou *Configuration-NonAcquittée*.

Note d'implémentation :

Ces événements peuvent survenir sur une connexion ouverte. L'implémentation DEVRA être préparé à renégocier immédiatement les options de configuration.

Acquitement-Configuration-Reçue (RCA)

Cet événement survient lorsqu'un paquet Configuration-Acquittée distant est reçu. Ce paquet est une réponse positive à une Requête-Configuration. Un paquet hors contexte ou invalide pour une autre raison est ignoré.

Note d'implémentation :

Dans la mesure ou des paquets conformes ont déjà été reçus avant que les états Acquitement-Configuration-Reçu ou Ouvert, il reste très peu de chances qu'un paquet non conforme arrive dans cette phase. Comme il est spécifié, tout paquet d'acquittement/non-acquittement/Rejet invalide est ignoré, et n'affecte pas les transitions de l'automate.

Cependant, il n'est pas impossible qu'un paquet pourtant correct arrive accidentellement pendant un état transitoire. Souvent, cela résultera d'une imperfection de l'implémentation. Au pire, ce cas POURRAIT être enregistré dans le rapport d'erreurs.

Configuration-NonAcquittée/Rejetée-Reçue (RCN)

Cet événement survient lorsqu'un paquet distant *Configuration-NonAcquittée* ou *Configuration-Rejetée* est reçu. Les paquets *Configuration-NonAcquittée* et *Configuration-Rejetée* constituent les réponses négatives à une *Requête-Configuration*. Un paquet hors contexte ou invalide pour une autre raison est ignoré.

Note d'implémentation :

Bien que les événements *Configuration-NonAcquittée* et *Configuration-Rejetée* cause les mêmes transitions d'état dans l'automate, ces paquets ont des effets différents quant aux options de configurations envoyées par la *Requête-Configuration* résultante.

Requête-Fermeture-Reçue (RTR)

Cet événement survient lorsqu'une *Requête-Fermeture* est arrivée du distant. La *Requête-Fermeture* indique que le distant souhaite suspendre la communication.

Note d'implémentation :

Cet événement n'a pas la même signification que la commande Close (voir ci-avant), qui impose l'émission d'une commande d'ouverture par l'administrateur local pour répondre à des sollicitations d'ouverture. L'implémentation DOIT se préparer à recevoir une nouvelle *Requête-Configuration* sans aucune autre intervention de l'administrateur local.

Acquittement-Fermeture-Reçue (RTA)

Cet événement signifie qu'un paquet *Fermeture-Acquittée* a été reçu du distant. Ce paquet est dans la plupart des cas une réponse à une *Requête-Fermeture* antérieure. Ce paquet peut aussi indiquer que le distant est dans l'état Fermé ou Arrêté, et sert dans ce cas à la resynchronisation de la configuration de la liaison.

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

Code-Inconnu-Reçu (RUC)

Cet événement est lancé lorsqu'un paquet reçu du distant ne peut être interprété. Un paquet *Code-Rejeté* est renvoyé en réponse.

Code-Rejeté-Reçu, Protocole-Rejeté-Reçu (RXJ+,RXJ-)

Cet événement signifie qu'un paquet *Code-Rejeté* ou *Protocole-Rejeté* a été reçu du distant.

L'événement RXJ+ intervient lorsque la valeur est acceptable selon le point de vue du LCP, comme pour le rejet d'un code d'extension valide, ou le rejet d'un protocole NCP. Ces événements sont dans le contexte d'in fonctionnement normal. L'implémentation DOIT arrêter d'émettre un tel type de paquet.

L'événement RXJ- intervient lorsque la valeur rejetée a une signification critique, comme le rejet d'un code de configuration, ou le rejet du protocole LCP! Cet événement indique la présence d'une erreur fatale qui provoque la fin forcée de la communication.

Requête-Echo-Reçu, Réponse-Echo-Reçu, Requête-Elimination-Reçu. (RXR)

Cet événement survient lorsqu'un paquet *Requête-Echo*, *Réponse-Echo* ou *Requête-Elimination* est reçu du distant. Le paquet *Réponse-Echo* est une réponse à un paquet *Requête-Echo*. Il n'y a pas de réponse à fournir à un paquet *Réponse-Echo* ou *Requête-Elimination*.

4.4. Actions

Les actions dans l'automate sont déclenchées par les événements et signifie typiquement la transmission de paquets et/ou le départ ou l'arrêt de la temporisation de Reprise.

Evénement-Illégal (-)

Cette action indique un événement non conforme à une implémentation correcte. L'implémentation affiche une erreur interne, laquelle devrait être signalée et archivée. Aucune transition n'est initiée, et l'implémentation NE DOIT ni se bloquer, ni être réinitialisée.

Ouvrir (tlu)

Cette action indique aux couches supérieures que l'automate entre dans l'état Ouvert. Typiquement, cette action est menée par le LCP pour lancer un événement Up vers un NCP, un protocole d'Authentification, ou le protocole de mesure de Qualité de Liaison, ou POURRAIT être menée par un NCP pour indiquer que la liaison et prête à faire transiter des données réseau.

Fermer (tld)

Cette action indique aux couches supérieures que l'automate quitte l'état Ouvert. Typiquement, cette action est menée par le LCP pour signaler la fermeture de ligne à un NCP, un protocole d'Authentification, ou le protocole de mesure de Qualité de Liaison, ou POURRAIT être menée par un NCP pour indiquer que la liaison n'est plus en mesure de faire transiter des données réseau.

Démarrer (tls)

Cette action indique aux couches inférieures que l'automate entre dans l'état Démarrage, et requiert la mise en route de celles-ci pour l'établissement de la liaison. La couche inférieure DEVRAIT répondre par un événement Up lorsque celle-ci s'est établie.

Les résultats de cette action dépendent fortement de l'implémentation.

Terminer (tlf)

Cette action indique aux couches inférieures que l'automate entre dans l'état Initial, Fermé ou Arrêté, et que le niveau de protocole inférieur n'est plus nécessaire. La couche inférieure DEVRAIT répondre par un événement Down lorsque les opérations de clôture de la couche inférieure sont achevées.

Typiquement, cette action DEVRAIT être menée par le LCP pour avancer vers la phase Link Dead, ou par un NCP pour indiquer au LCP que la liaison peut être coupée dès qu'il ne restera plus de NCP ouvert.

Les résultats de cette action dépendent fortement de l'implémentation.

Init-Compteur-Reprise (irc)

Cette action initialise le compteur de Reprise à la valeur appropriée (Max-Fermeture ou Max-Configuration). Le compteur est décrémenté à chaque transmission, y compris à la première.

Note d'implémentation :

En plus d'initialiser le compteur de Reprise, l'implémentation DOIT réinitialiser la temporisation d'attente à sa valeur initiale.

Zero-Compteur-Reprise (zrc)

Met le compteur de Reprise à zéro.

Note d'implémentation :

Cette action permet au FSA de faire une pause avant de passer à l'état final visé, permettant ainsi au trafic restant d'être traité par le distant. En plus de mettre le compteur de Reprise à zéro, l'implémentation DOIT initialiser la temporisation de Reprise à une valeur appropriée.

Emission-Requête-Configuration (scr)

Un paquet *Requête-Configuration* est émis. Il indique le désir d'établir une communication selon un ensemble d'Options de Configuration spécifié. La temporisation de Reprise est démarrée lorsque ce paquet est émis, afin de se prémunir contre une perte de celui-ci. Le compteur de Reprise est décrémenté chaque fois qu'une *Requête-Configuration* est envoyée.

Emission-Configuration-Acquittée (sca)

Un paquet *Configuration-Acquittée* est émis. Il acquitte la réception d'une *Requête-Configuration* et de son ensemble d'Options de Configuration, jugées alors acceptables.

Emission-Configuration-NonAcquittée (scn)

Un paquet *Configuration-NonAcquittée* ou *Configuration-Rejetée* est émis, selon le cas. Cette réponse négative rend compte de la réception d'une *Requête-Configuration* correcte mais dans laquelle certaines Options de Configuration sont incorrectes.

Les paquets *Configuration-NonAcquittée* sont utilisés pour refuser une valeur d'Option de Configuration, et pour en suggérer une autre, acceptable par l'appelé. Les paquets *Configuration-Rejetée* sont utilisés pour refuser toute négociation sur les Options de Configuration, en principe parce que l'option demandée est inconnue ou non implémentée. Les conditions d'utilisation des paquets *Configuration-NonAcquittée* plutôt que *Configuration-Rejetée* sont décrits plus avant dans le chapitre détaillant les formats de paquets LCP.

Emision-Requête-Fermeture (str)

Un paquet *Requête-Fermeture* est émis. Il indique le désir de clore une connexion. La temporisation de Reprise est démarrée lorsque la *Requête-Fermeture* est envoyée, pour se prémunir des pertes d'un tel paquet. Le compteur de Reprise est décrémenté à chaque émission de *Requête-Fermeture*.

Emission-Fermeture-Acquittée (sta)

Un paquet *Fermeture-Acquittée* est émis. Il rend compte de la réception d'un paquet *Requête-Fermeture* ou peut aussi servir à la synchronisation des automates.

Emission-Code-Rejeté (scj)

Un paquet *Code-Rejeté* est transmis. Il indique la réception d'un paquet non interprétable.

Emission-Réponse-Echo (ser)

Un paquet *Réponse-Echo* est transmis. Il accuse réception d'un paquet *Requête-Echo*.

4.5. Elimination de rebouclages

Le protocole est conçu de sorte à ne laisser que peu de chances à l'établissement d'une boucle protocolaire lors de la négociation d'Options de Configuration. Cependant, le protocole NE garantit PAS qu'une boucle ne puisse résulter d'une séquence particulière. Comme pour toute négociation, il n'est pas impossible de tomber sur le cas de deux implémentations de PPP aux stratégies contradictoires et pour lesquelles la négociation ne converge jamais. Il sera alors possible de changer de stratégie de négociation pour obtenir la convergence, mais cette pratique consommera nécessairement un certain temps. Les développeurs doivent garder à l'esprit ce problème et DEVRAIENT ajouter des mécanismes de détection de boucle ou un autre étage de temporisation.

4.6. Compteurs et Temporisations

Temporisation de Reprise

L'automate utilise une temporisation spéciale. La temporisation de Reprise est utilisée pour donner un cadre temporel aux échanges de paquets *Requête-Configuration* et *Requête-Fermeture*. L'expiration de la temporisation de Reprise constitue un événement TO, et provoque la retransmission de la Requête correspondante. La durée de la temporisation DOIT être configurable, mais POURRA avoir une valeur par défaut de trois (3) secondes.

Note d'implémentation :

La temporisation de Reprise DEVRAIT être adaptative selon la vitesse de transmission de la liaison. La valeur par défaut est donnée pour des liaisons lentes (2400 à 9600 bauds), et dans le cas de lignes commutées à basculement lent (lignes téléphoniques). Des lignes plus rapides, ou à commutation rapide, POURRAIENT bénéficier de délais d'attente inférieurs.

Plutôt qu'utiliser une valeur constante, la temporisation de Reprise POURRAIT être d'abord fixée à une valeur faible puis être augmentée progressivement jusqu'à sa valeur finale théorique selon une progression géométrique de facteur 2 (doublement pour chaque nouvelle valeur). La valeur initiale DEVRAIT être suffisamment grande en rapport à la taille des paquets, au moins deux fois le temps d'aller-retour d'un paquet à la vitesse de transmission nominale de la ligne, avec au moins une marge supplémentaire de 100 millisecondes pour donner au distant le temps de traiter le paquet avant de répondre. Certains circuits ajouteront une marge supplémentaire de 200 millisecondes pour un transfert "satellite". Les temps d'aller-retour pour des modems opérant à 14400 bauds sont mesurés entre environ 160 à plus de 600 millisecondes.

Max-Fermeture

Un compteur de Reprise au moins doit traiter les paquets *Requête-Fermeture*. Max-Fermeture indique le nombre de paquets *Requête-Fermeture* émis et n'ayant pas reçu de paquet *Fermeture-Acquittée* avant qu'il ait pu être établi que le distant n'est plus en état de répondre. Max-Fermeture DOIT être configurable, mais DEVRAIT proposer une valeur par défaut de deux (2) émissions.

Max-Configuration

Il est recommandé d'effectuer un compte similaire des paquets *Requête-Configuration*. Max-Configuration indique le nombre de paquets *Requête-Configuration* émis sans avoir reçu de paquet *Configuration-Acquittée*, Configuration-NonAcquittée ou Configuration-Rejetée valides avant qu'il ait pu être établi que le distant n'est plus en état de répondre. Max-Configuration DOIT être configurable, mais DEVRAIT proposer une valeur par défaut de dix (10) émissions.

Max-Echec

Un comptage des émissions de *Configuration-NonAcquittée* est nécessaire. Max-Echec donne le nombre de paquets *Configuration-NonAcquittée* émis sans avoir émis de *Configuration-Acquittée* et avant de pouvoir déterminer que les configurations ne convergent pas vers un accord probable. Tout nouveau paquet *Configuration-NonAcquittée* destiné au distant doit être converti en paquets *Configuration-Rejetée*, et les options souhaitées par le local ne sont plus transmises. Max-Echec DOIT être configurable, mais DEVRAIT proposer une valeur par défaut de cinq (5) émissions.

5. Formats de paquets LCP

Il existe trois classes de paquets LCP :

1. Les paquets de Configuration de Liaison utilisés pour établir et configurer une communication (*Requête-Configuration*, *Configuration-Acquittée*, *Configuration-NonAcquittée* et *Configuration-Rejetée*).

2. Les paquets de Fermeture de Liaison utilisés pour couper une communication (*Requête-Fermeture* et *Fermeture-Acquittée*).

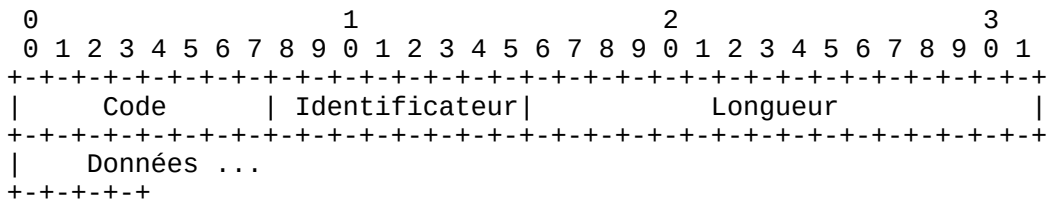
3. Les paquets de Maintenance de Liaison utilisés pour gérer et déverminer une liaison (*Code-Rejeté*, *Protocole-Rejeté*, *Requête-Echo*, *Réponse-Echo*, et *Requête-Elimination*).

Par souci de simplicité, il n'existe pas de champ de version dans les paquets LCP. Une implémentation LCP fonctionnelle correcte répondra toujours à des Protocoles et des Codes inconnus par un paquet LCP parfaitement univoque, ce qui procure un mécanisme automatique de reconnaissance de version non compatibles.

Quelles que soient les options de Configuration activées, tous les paquets LCP de Configuration, Fermeture et Rejet de Code (codes 1 à 7) seront systématiquement envoyés comme si aucune option de Configuration n'avait été négociée. En particulier, à chaque option de Configuration est attribuée une valeur par défaut. Ceci assure que tel paquet LCP restera toujours reconnaissable, même lorsqu'une extrémité de la ligne considère par erreur que la ligne est ouverte.

Un et un seul paquet LCP est encapsulé dans le champ d'information PPP, lorsque le champ Protocole du paquet PPP indique une valeur hexadécimale c021 (Link Control Protocol).

Un résumé des formats de paquets LCP est donné ci-après. Les champs sont transmis de la gauche vers la droite.



Code

Le champ Code comporte un octet, et identifie le type de paquet LCP. Lorsqu'un paquet reçu affiche un code inconnu, un paquet *Code-Rejeté* est transmis en retour.

Les valeurs de codes LCP reconnus les plus récents sont mentionnés dans la RFC "Assigned Numbers" [2]. Cette spécification donne les codes de base suivants :

1 Requête-Configuration
2 Configuration-Acquittée
3 Configuration-NonAcquittée
4 Configuration-Rejetée
5 Requête-Fermeture
6 Fermeture-Acquittée
7 Code-Rejeté
8 Protocole-Rejeté
9 Requête-Echo
10 Réponse-Echo
11 Requête-Elimination

Identificateur

Le champ Identificateur comporte un octet, et fournit un moyen d'associer requêtes et réponses. Lorsqu'un paquet présente un Identificateur invalide, il est ignoré sans affecter l'automate.

Longueur

Le champ Longueur comporte deux octets, et donne la longueur du paquet LCP, y compris l'octet de Code, d'Identificateur, le champ Longueur lui-même et le champ Données. La longueur NE DOIT PAS excéder l'URM de la liaison.

Les octets reçus en dehors de la plage définie par le champ Longueur sont traités comme des octets de bourrage et sont ignorés. Lorsqu'un paquet affiche une Longueur invalide, il est ignoré sans affecter le fonctionnement de l'automate.

Données

Le champ Données comporte zéro ou un nombre quelconque d'octets, selon l'indication du champ Longueur. Le format interne du champ Données dépend de la valeur présente dans le champ Code.

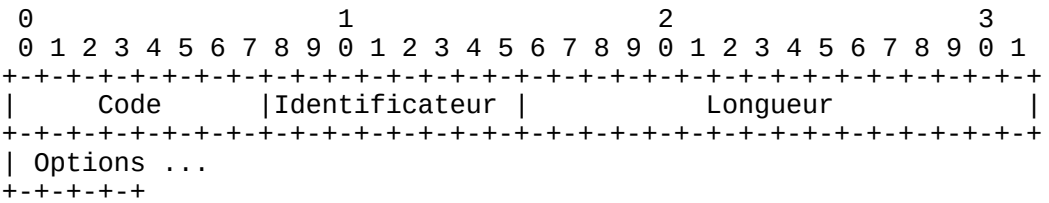
5.1. Requête-Configuration

Description

Une implémentation désireuse d'initialiser une communication DOIT transmettre une *Requête-Configuration*. Le champ d'Options est renseigné avec tous les changements à faire par rapport à la configuration par défaut. Les Options de Configuration NE DOIVENT PAS y apparaître lorsqu'elles ont leur valeur par défaut.

Sur réception d'une *Requête-Configuration*, une réponse appropriée DOIT être émise.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

Code

1 pour signifier Requête-Configuration.

Identificateur

Le champ Identificateur DOIT changer lorsque le contenu des Options change, et dans la mesure où une réponse valide a été reçu pour la requête précédente. Pour toute retransmission, l'Identificateur PEUT demeurer inchangé.

Options

Le champ d'Options est de longueur variable, et contient une liste de zéro ou plus Options de Configuration que l'émetteur désire renégocier. Toutes les Options de Configuration sont négociables simultanément. Le format des Options de Configuration est décrit dans un des chapitres suivants.

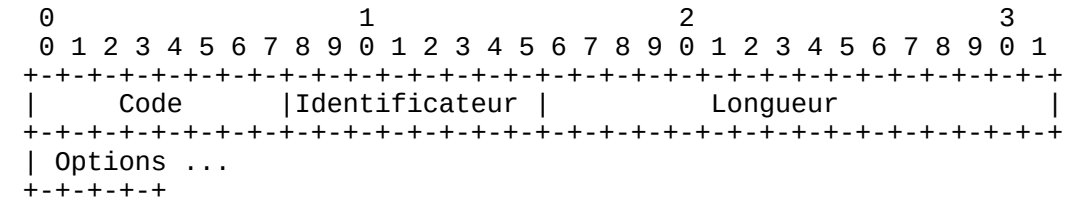
5.2. Configuration-Acquittée

Description

Si toutes les Options de Configuration reçues dans une *Requête-Configuration* est reconnaissable et toutes les valeurs valides, alors l'implémentation DOIT transmettre un paquet *Configuration-Acquittée*. La confirmation des Options de Configuration NE DOIT PAS en changer l'ordre ni les valeurs.

Sur réception d'un paquet *Configuration-Acquittée*, le champ Identificateur DOIT correspondre en valeur à celui de la dernière *Requête-Configuration* reçue. De plus, la liste d'Options de Configuration d'un paquet *Configuration-Acquittée* DOIT correspondre en tous points à celle de la *Requête-Configuration* précédente. Des paquets invalides sont ignorés.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

2 pour signifier Configuration-Acquittée.

Identificateur

Le champ Identificateur contient une copie de l'identificateur de la *Requête-Configuration* motivant l'envoi de ce paquet.

Options

Le champ d'Options varie en longueur, et contient une liste de zéro ou plus Options de Configuration à acquitter. Toutes les Options de Configuration sont toujours Acquittées collectivement.

5.3. Configuration-NonAcquittée

Description

Si toutes les instances d'Options de Configuration reçues peuvent être reconnues, mais avec pour certaines des valeurs non valides, alors l'implémentation DOIT transmettre un paquet *Configuration-NonAcquittée*. Le

champ d'Options est renseigné avec les Options de Configuration non acceptables de la requête correspondante. Toutes les Options validées doivent être filtrées dans le paquet *Configuration-NonAcquittée*, celles qui restent dans la réponse ne DEVANT PAS être changées d'ordre.

Le rejet d'Options sans champ de valeur (options booléennes) DOIT s'effectuer à l'aide de paquets *Configuration-Rejetée*.

A toute Option de Configuration dont une seule instance peut être présente DOIT être attribuée une valeur acceptable pour l'émetteur de l'accusé de réception. La valeur par défaut PEUT être utilisée, lorsque celle-ci est différente de la valeur requise par l'initiateur.

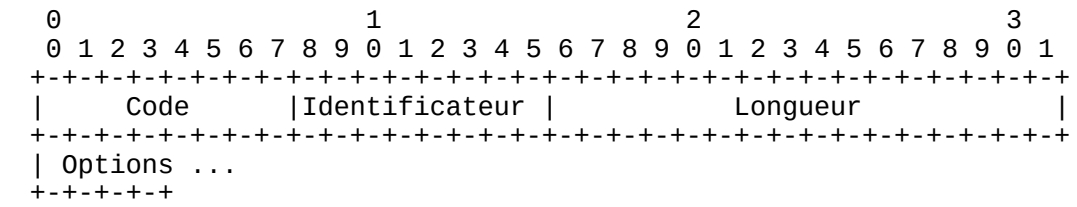
Pour toute Option de Configuration pouvant apparaître plusieurs fois avec des valeurs différentes, le paquet *Configuration-NonAcquittée* DOIT fournir une liste de toutes les valeurs acceptable par l'émetteur de l'acquittement. Cette liste inclura les valeurs acceptées présentes dans la requête.

Finalement, une implémentation peut être configurée pour requérir la négociation d'une Option de Configuration spécifique. Si cette option n'apparaît pas dans la requête, elle PEUT être ajoutée à la liste d'Options de Configuration dans l'accusé de réception, de sorte à inciter l'initiateur à spécifier cette option lors de l'émission de la Requête corrective suivante. Cette option DEVRA figurer avec toutes les valeurs acceptées par l'émetteur de l'accusé de réception.

Sur réception d'un paquet *Configuration-NonAcquittée*, le champ Identificateur DOIT contenir la même valeur que celle présente dans la dernière *Requête-Configuration*. Des paquets non valides seront ignorés.

Un paquet *Configuration-NonAcquittée* valide indique à son récepteur qu'une nouvelle *Requête-Configuration* est demandée, en indiquant les valeurs attendues et permises. Lorsqu'une Option de Configuration apparaît en plusieurs exemplaires dans l'accusé de réception, listant ainsi les valeurs permises, l'initiateur DEVRA en choisir une pour la constitution de la requête corrective suivante.

Certaines Options de Configuration sont de longueur variable. Comme l'option retournée par l'accusé a été modifiée entre temps par le distant, l'implémentation DOIT pouvoir traiter un retour d'Option de longueur différente à celle émise initialement dans la *Requête-Configuration*. Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

3 pour signifier Configuration-NonAcquittée.

Identificateur

L'identificateur doit être la copie de celui présent dans le *Requête-Configuration* à l'origine de cet accusé de réception.

Options

Le champ d'Options est de longueur variable, et contient une liste de zéro ou plus Options de Configuration dont l'émetteur accuse réception. Toutes les Options de Configuration sont traitées en une fois.

5.4. Configuration-Rejetée

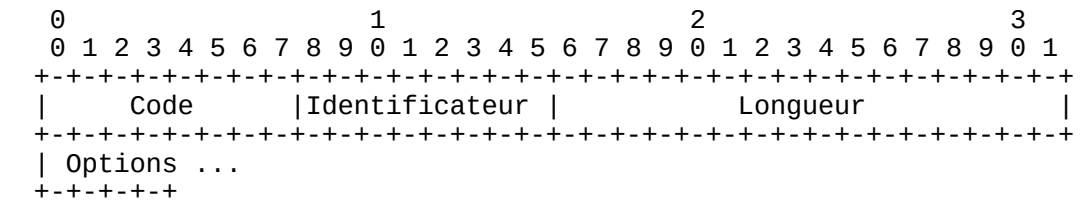
Description

Lorsque certaines Options de Configuration reçues dans une requête ne sont pas reconnaissables ou ne sont pas négociables (parce que par exemple configurées en fixe par un administrateur réseau), alors l'implémentation DOIT répondre par un paquet *Configuration-Rejetée*. Le champ d'Options est renseigné avec les seules Options de Configuration non conformes présentes dans la requête. Toutes les Options reconnues et négociables sont expurgées de la requête originale, celles qui restent ne devant en AUCUN CAS être réordonnées ni modifiées.

L'identificateur du paquet *Configuration-Rejetée*, DOIT nécessairement correspondre à celui de la requête initiale. De plus, l'ensemble des Options de Configuration figurant dans un rejet DOIT être exclusivement un sous ensemble de ceux transmis dans la requête originatrice. Les paquets non valides sont ignorés.

Un paquet *Configuration-Rejetée* indique à son récepteur que dans toute requête ultérieure corrective NE DEVRA figurer AUCUNE des Options stipulées dans le rejet.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

4 pour signifier Configuration-Rejetée.

Identificateur

L'identificateur doit être la copie de celui présent dans le *Requête-Configuration* à l'origine de cet accusé de rejet.

Options

Le champ d'Options est de longueur variable, et contient une liste de zéro ou plus Options de Configuration que l'émetteur rejette. Toutes les Options de Configuration sont rejetées en une fois.

5.5. Requête-Fermeture et Fermeture-Acquittée

Description

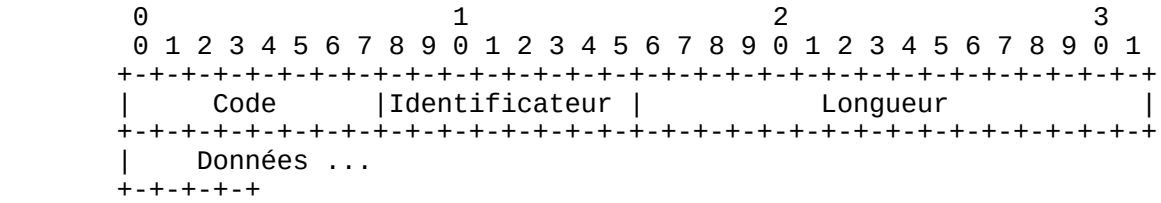
Le LCP inclue des codes particuliers de *Requête-Fermeture* et *Fermeture-Acquittée* afin d'inclure un mécanisme de clôture d'une connexion.

Une implémentation désireuse de suspendre une connexion DEVRAIT transmettre un paquet *Requête-Fermeture*. Ces paquets DEVRAIENT être émis continuellement jusqu'à réception d'un paquet *Fermeture-Acquittée*, ou jusqu'à ce que la couche inférieure ait signalé sa désactivation, ou encore jusqu'à ce que le nombre de requêtes soit suffisant pour que le distant puisse être raisonnablement considéré comme déconnecté.

Sur réception d'une *Requête-Fermeture*, un paquet *Fermeture-Acquittée* DOIT être renvoyé.

La réception d'un paquet *Fermeture-Acquittée* sans sollicitation indique que le distant est dans un des états Fermé ou Arrêté, ou réclame une renégociation de la liaison.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

5 pour signifier Requête-Fermeture;
6 pour signifier Fermeture-Acquittée.

Identificateur

Lors de l'émission, la valeur d'identification DOIT être modifiée chaque fois que le contenu du champ de données change, et dès qu'une réponse valide a été reçue pour une requête antérieure. Lors de la retransmission d'une même requête, la valeur d'identification reste inchangée.

Sur réception, la valeur d'identification de la *Requête-Fermeture* est recopiée dans le champ d'identification du paquet *Fermeture-Acquittée* émis en réponse.

Données

Le champ de Données est de longueur zéro ou plus d'octets, et contient les données non interprétées par l'émetteur. Les données peuvent être constituées de n'importe quelle séquence d'octets binaires. La fin de ce champ est donnée par calcul à l'aide du champ Longueur.

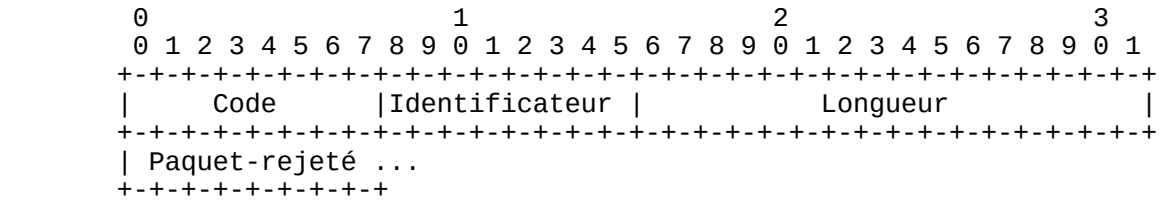
5.6. Code-Rejeté

Description

La réception d'un paquet LCP affichant un code non reconnaissable indique que le distant dispose d'une autre version de protocole que celle utilisée par le récepteur. Ceci DOIT être reporté à l'émetteur du paquet litigieux par l'émission d'un paquet *Code-Rejeté*.

Sur réception d'un rejet d'un code émis et implémentant une fonction indispensable pour la version de protocole implémentée, l'implémentation DEVRAIT signaler le problème et avorter le processus de connexion, dans la mesure où il est fortement improbable que le problème puisse être corrigé automatiquement.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

7 pour signifier Code-Rejeté.

Identificateur

La valeur d'identification DOIT changer à chaque émission d'un nouveau rejet.

Paquet-Rejeté

Le champ Paquet-Rejeté contient une copie du paquet LCP ayant été refusé. Il commence par le champ d'Information, et ne contient aucune en-tête Data Link Layer ni de FCS. Le Paquet-Rejeté DOIT être tronqué si nécessaire pour se conformer à la valeur d'URM maximale du distant.

5.7. Protocole-Rejeté

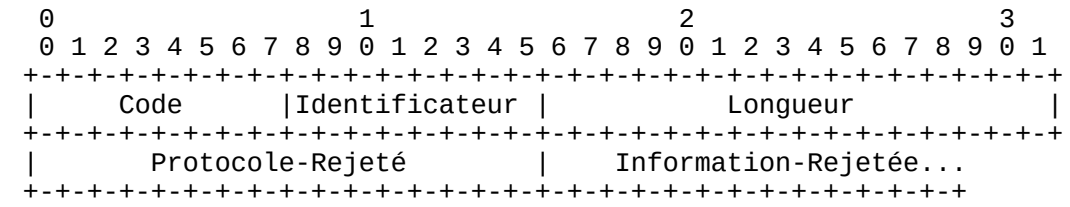
Description

La réception d'un paquet PPP dont le champ Protocole affiche une valeur inconnue indique que le distant essaie d'utiliser un protocole qui n'est pas supporté par le récepteur. Ceci peut arriver lorsque le distant essaie de configurer un nouveau protocole. Si l'automate LCP est dans l'état Ouvert, le caractère illicite de cette opération DOIT être signalé au distant par l'émission d'un paquet *Protocole-Rejeté*.

Sur réception d'un paquet *Protocole-Rejeté*, l'implémentation DOIT cesser toute émission de paquets de ce protocole aussi rapidement qu'il le peut.

Les paquets *Protocole-Rejeté* ne peuvent être émis que par un LCP en état Ouvert. Les paquets *Protocole-Rejeté* reçus lorsque le LCP est dans tout autre état que le précédent doivent être ignorés.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

8 pour signifier Protocole-Rejeté.

Identificateur

La valeur d'identification DOIT être modifiée à chaque nouveau rejet émis.

Protocole-Rejeté

Le champ Protocole-rejeté est de deux octets, et contient la copie du champ de protocole PPP du paquet refusé.

Information-Rejetée

Le champ Information-Rejetée contient une copie du paquet ayant été refusé. Il commence par le champ d'Information, et ne contient aucune en-tête Data Link Layer ni de FCS. L'Information-Rejetée DOIT être tronqué si nécessaire pour se conformer à la valeur d'URM maximale du distant.

5.8. Requête-Echo et Réponse-Echo

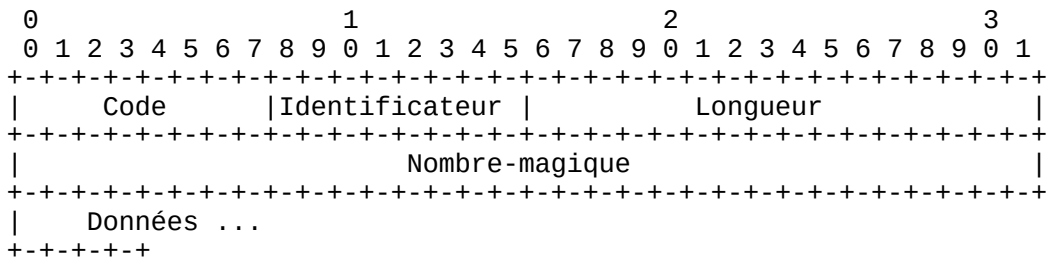
Description

Le LCP prévoit les paquets *Requête-Echo* et *Réponse-Echo* pour introduire un mécanisme de rebouclage du lien de données permettant d'implémenter des fonctions de test. Ce rebouclage permet notamment le déverminage d'un nouveau prototype d'implémentation, la mesure de la qualité de la ligne, la mesure de performances, ainsi que de nombreuses autres fonctions annexes.

Sur réception d'une *Requête-Echo* en état Ouvert, le LCP DOIT répondre par un paquet *Réponse-Echo*.

Les paquets *Requête-Echo* et *Réponse-Echo* ne DOIVENT être transmis que lorsque les LCP sont dans l'état Ouvert. Ces deux types de paquets, lorsqu'ils sont reçus dans tout autre état de l'automate, doivent être ignorés par celui-ci.

Le format de ces paquets est exprimé ci-dessous. Les champs sont transmis de gauche à droite.



Code

9 pour signifier Requête-Echo;
10 pour signifier Réponse-Echo.

Identificateur

En transmission, la valeur d'identification DOIT être changée dès que le contenu du champ de Données est modifié, ou qu'une réponse valide a été reçue pour une requête donnée. Lors des retransmissions, La valeur d'identification PEUT rester inchangée.

En réception, l'identificateur d'une *Requête-Echo* sera copié dans la *Réponse-Echo* émise en retour.

Nombre-Magique

Le Nombre-Magique a une longueur de quatre octets, et permet de détecter des liaisons en condition de rebouclage. Tant que l'Option de Configuration relative aux Nombres-Magiques n'a pas été négociée avec sucés, Le Nombre-Magique DOIT être transmis à zéro. Voir le paragraphe concernant l'Option de Configuration Nombres-Magiques pour plus de détails.

Données

Le champ de Données contient zéro ou plus d'octets, et contient des données non interprétées. Ces données peuvent constituer n'importe quelle séquence d'octets binaires. La fin de ce champ est obtenue par calcul grâce à l'indication de Longueur.

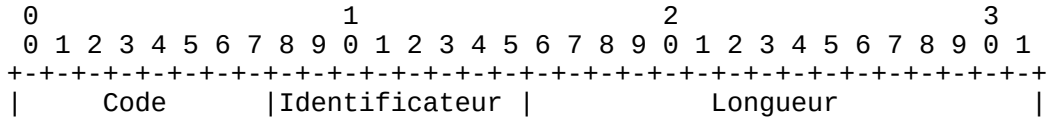
5.9. Requête-Elimination

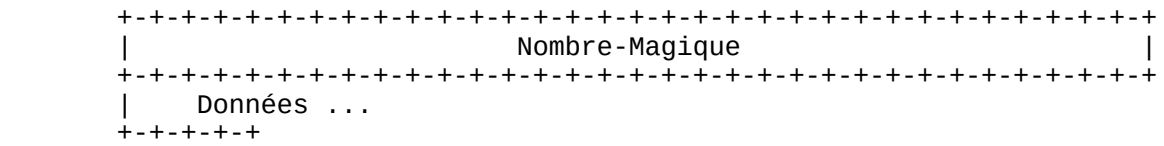
Description

Le LCP dispose d'un code de *Requête-Elimination* dans le but de fournir un mécanisme de test de la liaison de donnée dans le sens local vers distant. Ce mécanisme permet la mise en œuvre de fonctions de déverminage de nouveaux prototypes, de fonctions de mesure de performances, et d'autres fonctions accessoires.

Les paquets *Requête-Elimination* NE DOIVENT ETRE émis que par un LCP en l'état Ouvert. Sur réception, ces paquets doivent être ignorés par le récepteur.

Le format de ce paquet est exprimé ci-dessous. Les champs sont transmis de gauche à droite.





Code

11 pour signifier *Requête-Elimination*.

Identificateur

La valeur d'identification DOIT changer à chaque émission.

Nombre-Magique

Le Nombre-Magique a une longueur de quatre octets, et permet de détecter des liaisons en condition de rebouclage. Tant que l'Option de Configuration relative aux Nombres-Magiques n'a pas été négociée avec sucés, Le Nombre-Magique DOIT être transmis à zéro. Voir le paragraphe concernant l'Option de Configuration Nombres-Magiques pour plus de détails.

Données

Le champ de Données contient zéro ou plus d'octets, et contient des données non interprétées. Ces données peuvent constituer n'importe quelle séquence d'octets binaires. La fin de ce champ est obtenue par calcul grâce à l'indication de Longueur.

<A NAME="6"></A>

6. Options de Configuration LCP

Les Options de Configuration du LCP permettent la négociation de certaines modifications des valeurs par défaut des paramètres d'une liaison Point à Point. Si une Option de Configuration n'est pas mentionnée dans une *Requête-Configuration*, on suppose que c'est la valeur par défaut qui est requise pour cette Option.

Certaines Options de Configuration PEUVENT apparaître plus d'une fois. Cette possibilité est spécifique à certaines Options de Configuration, et est annoncée dans la description de chaque Option de Configuration. (aucune des Options de Configuration décrites dans ce document ne peut être mentionnée plus d'une fois).

La fin de la liste d'Options de Configuration peut être identifiée par calcul à l'aide du champ Longueur dans le paquet LCP.

Sauf mention contraire, toutes les Options de Configuration concernent une transmission "half-duplex", soit une moitié de la communication; typiquement, elles spécifient les caractéristiques attendues en réception du point de vue de l'émetteur de la Requête.

Philosophie

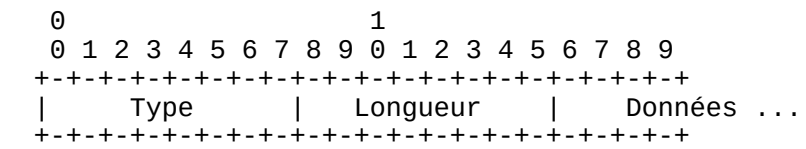
Les options indiquent soit la disponibilité soit la nécessité d'implémentation de l'option demandée par la requête. Une implémentation ne pouvant interpréter aucune option DEVRAIT néanmoins pouvoir fonctionner avec une autre qui les reconnaît toutes.

Des valeurs par défaut sont spécifiées pour chacune des options, permettant ainsi à la liaison de pouvoir s'établir sans aucune négociation, mais peut être sur un mode réduit ou non optimisé.

Sauf mention explicite, l'acquittement des options n'impose pas au distant l'utilisation d'une autre valeur que celle par défaut.

Il n'est donc pas nécessaire d'émettre les options requises avec les valeurs par défaut dans une *Requête-Configuration*.

Un prototype du format général des Options de Configuration est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type

Le champ Type est défini sur un octet, et indique le type d'Option de Configuration. Ce document liste quelques options de base établies à la construction du protocole. Les dernières Options validées sont indiquées dans la RFC "Assigned Numbers" [2]. Voici les valeurs initialement admises :

0	RESERVE
1	Unité-Réception-Maximale
3	Protocole-Authentification
4	Protocole-Qualité
5	Nombres-Magiques
7	Compression-Protocoles
8	Compression-Adresses-et-Contrôles

Longueur

Le champ Longueur est défini sur un octet, et indique la longueur de l'Option de Configuration en comptant l'octet de Type, la longueur elle-même et le champ de Données.

Si une Option de Configuration dans une *Requête-Configuration* porte un numéro valide, mais spécifie une longueur erronée ou non interprétable, un paquet *Configuration-NonAcquittée* DEVRAIT être transmis explicitant l'Option de Configuration demandée, avec sa Longueur et ses Données régulières.

Données

Le champ de Données peut transporter zéro ou un nombre quelconque d'octets, et contient des informations spécifiques à l'Option de Configuration. Le format et la longueur du champs Données est déterminé par calcul à l'aide du champ de Type et de Longueur.

Lorsque la longueur mentionnée semble prétendre que les données s'arrêtent au delà de la longueur du champ Information du paquet LCP, ce paquet entier doit être ignoré sans affecter pour autant l'automate.

6.1. Unité-Réception-Maximale (URM)

Description

Cette Option de Configuration peut être utilisée pour informer le distant que cette implémentation peut accepter des paquets plus grands que l'URM standard, ou à l'inverse pour forcer le distant à envoyer des paquets plus courts.

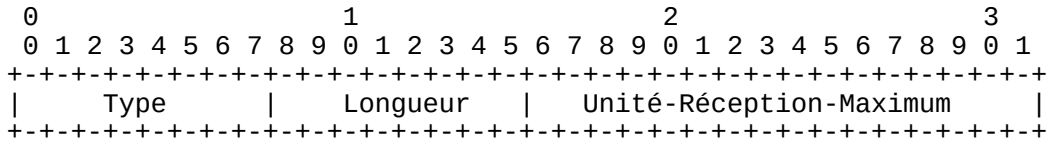
La valeur par défaut est de 1500 octets. Si des paquets plus courts sont demandés par une implémentation, celle-ci DEVRA néanmoins rester capable de recevoir des paquets de 1500 octets au cas ou la synchronisation de la ligne serait perdue.

Note d'Implémentation :

Cette option est utilisée pour indiquer une performance de l'implémentation. Le distant n'est pas tenu d'exploiter cette performance. Par exemple, lorsqu'une implémentation indique une URM de 2048 octets, le distant n'est pas obligé d'envoyer des paquets de cette taille. Le distant n'a pas non plus nécessairement à

refuser la négociation de l'option et peut librement émettre des paquets de 1500 octets, dans la mesure où toute implémentation doit au moins accepter des paquets de cette taille.

Le format de l'Option de Configuration Unité-Réception-Maximale est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type

1

Longueur

4

Unité-Réception-Maximum

Le champ Unité-Réception-Maximale est codé sur deux octets, et spécifie le nombre maximum d'octets que doit comporter un ensemble Information plus Bourrage. Il ne compte pas les octets de trame, le champ de Protocole, le FCS, ni aucun bits ou octets "transparents".

6.2. Protocole-Authentification

Description

Sur certaines liaisons, il peut être utile de demander au distant de s'authentifier avant de permettre le transit de protocoles de niveau réseau.

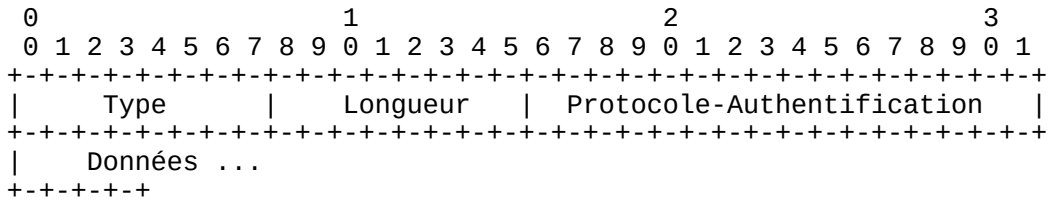
Cette Option de Configuration procure une méthode pour négocier l'usage d'un protocole d'authentification spécifique. Par défaut, aucune authentification n'est demandée.

Une implémentation NE DOIT PAS faire figurer plusieurs Options Protocole-Authentification dans ses paquets de *Requête-Configuration*. Au lieu de cela, elle DEVRAIT tenter de configurer le protocole le plus "adéquat" en premier. Si ce protocole est rejeté par la négociation, alors l'implémentation DEVRAIT tenter de négocier le protocole suivant dans l'ordre de préférence dans un nouveau paquet *Requête-Configuration*.

L'implémentation émettant la *Requête-Configuration* indique qu'il attend que le distant s'authentifie. Si le distant acquitte cette option, alors il accepte de s'authentifier avec le protocole spécifié dans la requête. Une implémentation recevant un acquittement pour cette option DEVRAIT attendre l'identification du distant en activant le protocole indiqué.

Il n'y a aucune obligation que l'authentification soit faite dans les deux sens, ni que le même protocole soit utilisé dans les deux directions pour effectuer une "reconnaissance" bilatérale. Il est tout à fait acceptable que deux protocoles distincts soient utilisés pour les deux sens d'authentification. Ceci dépendra évidemment du résultat de la négociation.

Le format pour l'Option de Configuration Protocole-Authentification est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type

3

Longueur

>= 4

Protocole-Authentification

Le champ Protocole-Authentification est décrit par deux octets, et indique le protocole d'authentification désiré. Les valeurs de ce champ sont toujours les mêmes que celles mentionnées dans le champ de protocole PPP pour ce même protocole d'authentification.

Ce document liste quelques valeurs de protocoles d'authentification établies à la construction de ce protocole. Les derniers protocoles validés sont indiqués dans la RFC "Assigned Numbers" [2]. Voici les valeurs initialement admises :

Identificateur (hexa) de Protocole

c023	PAP (protocole d'identification par mot de passe)
c223	CHAP (protocole par échange de certificats)

Données

Le champ de donnée contient zéro ou un nombre quelconque d'octets, et contient des données additionnelles selon le protocole spécifié.

6.3. Protocole-Qualité

Description

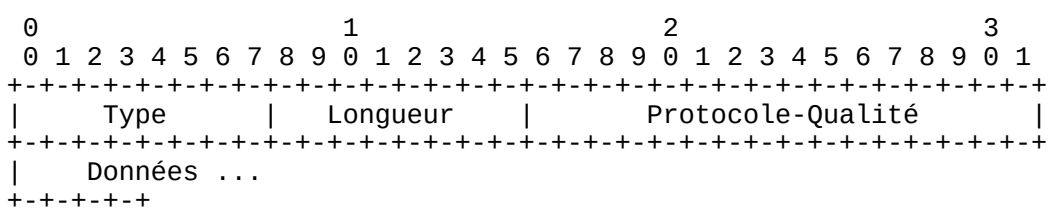
Sur certaines liaisons, il peut être souhaitable de déterminer quand, et dans quelle proportion la liaison perd des données. Ce procédé est appelé contrôle de qualité de liaison.

Cette Option de Configuration procure une méthode pour négocier l'usage d'un protocole particulier pour le contrôle de qualité de liaison. Par défaut, le contrôle de qualité de liaison est désactivé.

L'implémentation émettant la *Requête-Configuration* indique qu'elle demande au distant de lui envoyer des données pour tester la qualité de liaison. Si un distant acquitte cette option, alors il déclare accepter l'usage de ce protocole. Une implémentation recevant un acquittement pour cette option DEVRAIT attendre du distant un échange sur le protocole convenu.

Il n'y a aucune obligation que le contrôle de qualité soit fait dans les deux sens, ni que le même protocole soit utilisé dans les deux directions. Il est tout à fait acceptable que deux protocoles distincts soient utilisés pour les deux sens de la mesure. Ceci dépendra évidemment du résultat de la négociation.

Le format pour l'Option de Configuration Protocole-Qualité est donné ci-dessous. Les champs sont transmis de gauche à droite.



www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

Type

4

Longueur

>= 4

Protocole-Qualité

Le Protocole-Qualité est décrit sur deux octets, et indique le type de protocole de contrôle de qualité demandé. Les valeurs de ce champ sont toujours les mêmes que celles mentionnées dans le champ de protocole PPP pour ce même protocole de mesure.

Ce document liste quelques valeurs de protocoles de contrôle établies à la construction de ce protocole. Les derniers protocoles validés sont indiqués dans la RFC "Assigned Numbers" [2]. Voici les valeurs initialement admises :

Identificateur (hexa) de Protocole

c025 Link Quality Report

Données

Le champ de donnée contient zéro ou un nombre quelconque d'octets, et contient des données additionnelles selon le protocole spécifié.

6.4. Nombres-Magiques

Description

Cette Option de Configuration procure une méthode pour détecter des liaisons rebouclées et d'autres anomalies au niveau Liaison de Données. Cette Option de Configuration POURRA être nécessaire selon la présence ou l'absence d'autres Options de Configuration telles que l'option Protocole-Qualité. Par défaut, l'option Nombres-Magiques n'est pas négociée, et la valeur zéro doit être utilisée là où un Nombre-Magique aurait du être inscrit.

Avant de requérir cette Option de Configuration, une implémentation DOIT choisir son propre Nombre-Magique. Il est conseillé de choisir ce Nombre-Magique de la façon la plus aléatoire possible de sorte qu'il puisse être garanti avec une très forte probabilité que ce nombre soit unique pour deux implémentation en contact. Un bonne méthode pour obtenir l'unicité de ce nombre est de prendre comme base de calcul un nombre lui-même unique. Répondent à cette définition les numéros de série des machines, ou d'autres adresses matérielles dans le réseau, des horloges datées, etc. Des nombres présentant un bon facteur d'aléatoire sont obtenus par mesure précise du temps entre deux événements tels que la réception de paquets sur une autre connexion réseau, le temps de réponse d'un serveur, ou la cadence de frappe d'un utilisateur humain. Il peut être aussi suggéré de combiner plusieurs source aléatoires pour augmenter la probabilité d'unicité.

Lorsqu'une *Requête-Configuration* précise une Option de Configuration Nombres-Magiques, le Nombre-Magique reçu est comparé avec le Nombre-Magique de la dernière requête émise vers un distant. Si ces deux Nombres-Magiques sont distincts, la ligne est considérée comme non bouclée, et le Nombre-Magique DEVRAIT être acquitté. Si les deux Nombres-Magiques sont égaux, alors il est probable, mais pas certain, que la ligne est rebouclée et que la requête reçue est en fait la dernière émise. Pour s'assurer de cette éventualité, un paquet *Configuration-NonAcquittée* DOIT être émis avec une nouvelle valeur de Nombre-Magique. Une nouvelle *Requête-Configuration* NE DEVRAIT PAS être émise vers le distant tant qu'une réaction normale n'est pas obtenue (c'est à dire, un paquet *Configuration-NonAcquittée* est reçu ou la temporisation de Reprise expire).

La réception d'un paquet *Configuration-NonAcquittée* présentant un Nombre-Magique différent de celui transmis dans le dernier paquet *Configuration-NonAcquittée* émise vers le distant prouve que la liaison n'est pas bouclée, en éliminant le cas possible bien qu'improbable de Nombres-Magiques égaux par pur hasard. Si les

deux Nombres-Magiques des paquets *Configuration-NonAcquittée* sont égaux, la probabilité d'être en présence d'une boucle augmente, et un nouveau Nombre-Magique DOIT être choisi. Dans les deux cas, une nouvelle *Requête-Configuration* DEVRAIT être émise avec ce nouveau Nombre-Magique.

Si la ligne est effectivement en état rebouclé, cette séquence (transmission d'une *Requête-Configuration*, réception d'une *Requête-Configuration*, transmission d'un *Configuration-NonAcquittée*, réception d'un *Configuration-NonAcquittée*) se reproduira encore et encore. Si la ligne n'était pas bouclée, au pire cette séquence pourrait se produire un certain nombre (petit) de fois, mais aurait vraiment très peu de chance de se répéter continuellement. Selon toute attente, les Nombres-Magiques choisis des deux côtés de la liaison devraient rapidement diverger, arrêtant ainsi cette séquence. La table suivante montre la probabilité de collisions en supposant que les deux extrémités choisissent des Nombres-Magiques selon une loi de 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

Pour que cette divergence puisse survenir, il faut assurer un caractère aléatoire et unique suffisant. Si une source présentant ces qualités intrinsèques suffisantes ne peut être trouvée, il est conseillé de ne pas activer cette Option de Configuration; Des *Requête-Configuration* ne DOIVENT PAS être émises avec cette option et toute Option de Configuration Nombre-Magique émise par le distant DOIT être soit Acquittée soit rejetée. Dans ce cas, l'implémentation n'a pas la possibilité de détecter avec suffisamment d'assurance une situation de rebouclage, bien que cette dernière puisse l'être par le distant.

Si une implémentation émet effectivement une *Requête-Configuration* affichant une Option de Configuration Nombres-Magiques, alors elle de DOIT PAS répondre a une *Requête-Configuration* distante avec la même option par un paquet *Configuration-Rejetée*. En d'autres termes, si une implémentation désire utiliser l'option Nombres-Magiques, alors elle DOIT alors accepter que le distant en fasse de même. Si une implémentation reçoit un paquet *Configuration-Rejetée* en réponse à une *Requête-Configuration*, cela signifiera seulement que le lien n'est pas rebouclé, et que le distant ne désira pas utiliser les Nombres-Magiques. Dans ce cas, une implémentation DEVRAIT réagir comme si la négociation avait abouti (comme si une *Configuration-Acquittée* avait été reçue à la place).

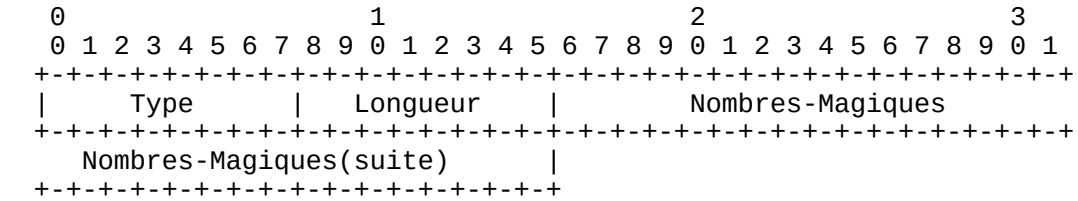
Le Nombre-Magique peut aussi être utilisé pour détecter un rebouclage de ligne pendant une phase de fonctionnement normale, en plus d'une phase de négociation d'options. Tous les paquets LCP *Requête-Echo*, *Réponse-Echo*, et *Requête-Elimination* ont un champ Nombre-Magique. Si les Nombres-Magiques ont été négociés avec sucés, une implémentation DOIT transmettre ces paquets avec le Nombre-Magique négocié.

Le champ Nombre-Magique de ces paquets DEVRAIT être testé sur réception. Tous les champs Nombres-Magiques reçus DOIVENT avoir une valeur soit nulle soit égale au Nombre-Magique unique défini pour le distant, suivant le résultat de la négociation de cette option entre les deux entités.

La réception d'un champ Nombre-Magique de valeur égale au Nombre-Magique défini par l'implémentation locale signifie la possibilité d'une liaison rebouclée. La réception d'un Nombre-Magique de valeur différente que celle négociée comme local, ou de la valeur distante, ou nulle si des valeurs n'ont pas été négociées, indique que la liaison a été mal configurée.

Les procédures pour se récupérer de l'un ou l'autre cas de figure ne sont pas précisées, et peuvent varier d'une implémentation à l'autre. Une méthode quelque peu pessimiste est d'assimiler ces situations à un événement Down du LCP. Une réouverture relancera le processus pour négocier de nouveau la liaison, processus qui ne pourra être achevé tant que perdurent les causes de rebouclage de la liaison, et tant que des Nombres-Magiques conformes n'ont pu être négociés. Une méthode plus optimiste (dans le cas d'un lien en boucle) est d'entamer la transmission de paquets *Requête-Echo* LCP jusqu'à ce que soit reçu un paquet *Réponse-Echo* conforme, indiquant de ce fait la fin d'une telle situation.

Le format pour l'Option de Configuration Nombres-Magiques est donnée ci-dessous. Les champs sont transmis de gauche à droite.



Type

5

Longueur

6

Nombres-Magiques

Le champ Nombres-Magiques est décrit sur quatre octets, et donne un nombre supposé être unique vis à vis de l'autre extrémité. Une valeur nulle est illégale et DOIT être refusée, si l'Option Nombres-Magiques n'est pas elle-même rejetée.

6.5. Compression-Champ-Protocole (PFC)

Description

Cette Option de Configuration procure une méthode pour négocier la compression du champ Protocole PPP. Par défaut, toutes les implémentations DOIVENT transmettre des paquets avec un champ Protocole PPP de deux octets.

Les valeurs pour le champ Protocole PPP sont choisis de sorte que certaines valeurs puissent être exprimées sous une forme réduite d'un octet, et de façon tout à fait univoque par rapport à leur expression en deux octets. Cette Option de Configuration est envoyée pour informer le distant que le local accepte des valeurs de Protocole compressées sur un octet.

Comme indiqué précédemment, le champ Protocole utilise un mécanisme d'extension conforme à au mécanisme de l'ISO 3309 concernant les champs d'Adresse; le bit de poids faible (LSB) de chaque octet est utilisé pour indiquer l'extension du champ Protocole. Un "0" binaire comme LSB indique que l'octet suivant code la suite du champ Protocole. Un "1" binaire comme LSB marque le dernier octet du champ Protocole. Notez qu'ainsi, un nombre quelconques d'octets nuls peuvent être placés avant le champ, indiquant toujours la même valeur (considérez les deux représentations pour la valeur 3, 00000011 et 00000000 00000011).

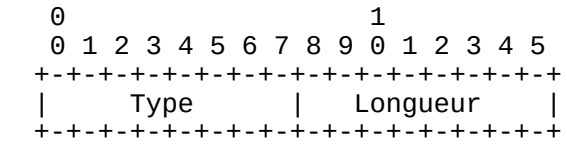
Sur des liaisons à bas débit, il est souhaitable de préserver la bande passante utile en envoyant le moins de données redondantes ou non significatives possible. L'Option de Configuration Compression-Champ-Protocole permet de privilégier tantôt simplicité d'implémentation, tantôt optimisation de la bande utile. Si la négociation se déroule avec sucés, le mécanisme d'extension ISO 3309 peut être utilisé pour compresser le champ Protocole sur un octet au lieu de deux. La grande majorité des paquets émis par la suite peuvent être compressés dans la mesure où la plupart des valeurs de protocoles utilisées sont inférieures à 256.

Des champs Protocoles ne doivent JAMAIS être compressés sauf si cette Option de Configuration a été négociée. Une fois cette option négociée, les implémentations PPP DOIVENT accepter des paquets PPP de champ Protocole à un ou deux octets, SANS distinction AUCUNE entre les deux formes.

Le champ Protocole n'est JAMAIS compressé lors de l'envoi de paquets LCP. Cette règle garantit une reconnaissance univoque des paquets LCP.

Lorsqu'un champ Protocole est compressé, le champ FCS de la couche données (Data Link Layer) est calculé sur la trame compressée, et non sur la trame originale.

Le format de l'Option de Configuration Compression-Champ-Protocole est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type

7

Longueur

2

6.6. Compression-Adresse-et-Contrôles (ACFC)

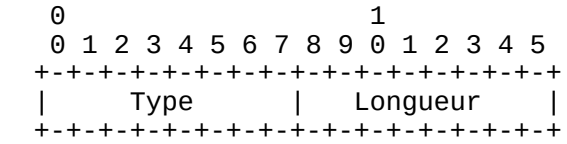
Description

Cette Option de Configuration procure une méthode pour négocier la compression des champs d'Adresse et Contrôles de la couche de données (Data Link Layer). Par défaut, toutes les implémentations DOIVENT transmettre des trames avec des champs Adresse et Contrôles appropriés à la définition de la trame correspondante.

Dans la mesure où ces données ont souvent des valeurs statiques pour des liaisons point-à-point, il est possible sans risque de les compresser. Cette Option de Configuration est envoyée pour informer le distant que l'implémentation locale peut recevoir des champs Adresse et Contrôles compressés. Si une trame compressée est reçue alors que cette option n'a pas été négociée, ces trames devront être ignorées.

Les champs Adresse et Contrôle NE DOIVENT PAS être compressés dans des paquets LCP. Cette règle permet d'assurer une reconnaissance univoque des paquets LCP. Lorsque les champs Adresse et Contrôle sont compressés, le champ FCS de la couche de données (Data Link Layer) est calculé sur la trame compressée et non sur la trame originale.

Le format de L'Option de Configuration Compression-Adresse-et-Contrôle est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type

8

Longueur

2

Considérations sécuritaires

Certains aspects concernant la sécurisation sont traités dans les sections Phase d'Authentification, Evénement Close, et Option Protocole-Authentification.

Références

[1] Perkins, D., "Requirements for an Internet Standard Point-to- Point Protocol", RFC 1547, Carnegie Mellon University, December 1993.

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

[2] Reynolds, J., and Postel, J., "Assigned Numbers", STD 2, RFC 1340, USC/Information Sciences Institute, July 1992.

Remerciements

Ce document est produit par le Point-to-Point Protocol Working Group de l'Internet Engineering Task Force (IETF). Tout commentaire doit être transmis à la mailing list ietf-ppp@merit.edu.

La majeure partie de ce texte a été tirée des spécifications du groupe de travail [1]; des RFCs 1171 & 1172, par Drew Perkins, alors à l'Université Carnegie Mellon, et par Russ Hobby de l'Université de Californie à Davis.

William Simpson est le premier à avoir introduit des principes et une terminologie conséquente; on lui doit le nouveau design des phases et états de négociation.

De nombreuses personnes ont contribué à la mise au point du Protocole Point-à-Point. La liste complète de ces personnes est trop longue, mais nous attribuons des remerciements particuliers à: Rick Adams, Ken Adelman, Fred Baker, Mike Ballard, Craig Fox, Karl Fox, Phill Gross, Kory Hamzeh, Russ Hobby, David Kaufman, Steve Knowles, Mark Lewis, Brian Lloyd, John LoVerso, Bill Melohn, Mike Patton, Drew Perkins, Greg Satz, John Shriver, Vernon Schryver, et Asher Waldfogel.

Remerciements particuliers à Morning Star Technologies pour son aide matérielle et ses accès réseau ayant permis l'établissement de cette spécification.

Contact

Le groupe de travail peut être contacté à l'adresse suivante :

Fred Baker
Advanced Computer Communications
315 Bollay Drive
Santa Barbara, California 93117

fbaker@acc.com

Toute question technique sur ce mémo peut être envoyée à :

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071

Bill.Simpson@um.cc.umich.edu
bsimpson@MorningStar.com