

Groupe de travail Réseau
Request for Comments : 3437
 Catégorie : En cours de normalisation
 Traduction Claude Brière de L'Isle

W. Palter zev.net
 W. Townsley, Cisco Systems
 décembre 2002

Extensions au protocole de tunnelage de couche deux pour la négociation du protocole de contrôle de liaison PPP

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2002). Tous droits réservés

Résumé

Le présent document définit des extensions au protocole de tunnelage de couche deux (L2TP) pour une prise en charge améliorée des options du protocole point à point (PPP) spécifiques de la liaison. Les points d'extrémité PPP ont normalement un accès direct au support physique commun qui les connecte et ont donc une connaissance détaillée du support qui est utilisé. Lorsque L2TP est utilisé, les deux homologues PPP ne sont plus directement connectés sur le même support physique. L2TP insère plutôt une connexion virtuelle sur certaines ou sur toutes les connexions PPP en tunnelant les trames PPP sur un réseau de commutation de paquets tel que IP. Dans certaines conditions, un point d'extrémité L2TP peut avoir besoin de négocier des options du protocole de contrôle de liaison PPP (LCP, *Link Control Protocol*) dans une localisation qui peut n'avoir pas accès à toutes les informations sur le support nécessaires pour une participation appropriée à la négociation LCP. Le présent document fournit un mécanisme pour communiquer les options LCP désirées entre les points d'extrémité L2TP avant la négociation PPP LCP à l'extrémité distante d'un tunnel L2TP, ainsi qu'un mécanisme pour communiquer les options LCP négociées là où réside la liaison PPP native.

Table des Matières

1. Introduction.....	1
1.1 Spécification des exigences.....	2
2. Options LCP du LAC au LNS.....	2
2.1 LCP veut des options (iccn, occn).....	2
2.2 Options permises au LCP (iccn, occn).....	3
2.3 Options LCP du LNS au LAC.....	4
3. Considérations sur la sécurité.....	4
4. Considérations relatives à l'IANA.....	5
5. Références normatives.....	5
6. Adresse des auteurs.....	5
7. Déclaration complète de droits de reproduction.....	5

1. Introduction

L2TP [RFC2661] ne donne qu'une quantité très limitée d'indications au LNS sur le type d'interface sur lequel arrive une session PPP tunnelée à un concentrateur d'accès du protocole de tunnelage de couche 2 (LAC, *L2TP Access Concentrator*). Ces informations se limitent au caractère "synchrone" ou "asynchrone", "numérique" ou "analogique" de l'interface. Ces indications donnent quelques lignes directrices lors de la négociation du LCP PPP au serveur réseau L2TP (LNS, *L2TP Network Server*), mais elles ne sont pas aussi robustes qu'elles pourraient l'être.

Le présent document définit une façon plus robuste d'informer le LAC des options LCP négociées, et donne des lignes directrices au LNS sur les limites et les valeurs que le LAC demande durant la négociation LCP. Une bonne connaissance de PPP [RFC1661] et de L2TP [RFC2661] est nécessaire pour la suite de ce document.

Le mandataire L2TP de LCP permet que des options soient négociées là où réside la liaison PPP native, circonvenant ainsi les problèmes de tableau de caractères de commande asynchrones (*ACCM, Async-Control-Character-Map*), de séquence de

contrôle de trame (FCS, *Frame Check Sequence*) de remplacement, et autres options LCP que le LNS ne saurait pas nécessairement négocier de façon appropriée sans un accès au support physique pour la connexion PPP native, le type d'interface, ou la configuration. Cependant, l'utilisation du mandataire LCP introduit aussi d'autres problèmes comme les options au sein de la négociation PPP LCP qui devraient être réglées ou ajustées par le LNS, comme le type d'authentification PPP et la MRU. Finalement, le client PPP peut réinitialiser la négociation LCP à tout moment, et sauf si le LAC examine tous les paquets de données PPP qu'il transmet, il ne saura même pas que cela se produit.

Les options LCP peuvent être classées en gros en trois catégories différentes par rapport à leur effet sur L2TP ; (1) options qui affectent le tramage d'une façon que le LAC peut avoir besoin de connaître ou traiter d'une façon spécifique (par exemple, ALT-FCS, ACCM, MRU), (2) options qui sont pour la plupart transparentes au LAC (par exemple, AUTH-TYPE), et (3) options que le LAC peut souhaiter influencer parce qu'elles dépendent du type de support (ACFC, PFC). On s'occupera plus précisément des options qui entrent dans les catégories (1) et (3).

Le présent document définit de nouvelles paires de valeurs d'attributs (AVP, *attribute value pair*) pour permettre au LAC et au LNS de communiquer des informations LCP complètes afin de réagir en conséquence. Les informations d'option LCP sont structurées de la même façon que le sont les AVP de mandataire LCP dans la [RFC2661]. Cela implique essentiellement l'encapsulation d'un paquet Demande de configuration ou Accusé de réception de configuration PPP LCP au sein d'une AVP L2TP.

1.1 Spécification des exigences

Dans ce document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules. Les mots-clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

2. Options LCP du LAC au LNS

Le LAC peut utiliser les AVP suivantes au sein d'un message ICCN ou OCCN afin d'influencer le LNS pour négocier LCP d'une manière spécifique. Si ces AVP sont acceptées par le LNS, elles devraient supplanter toute les suggestions d'options LCP impliquées par les AVP de type de support ou de type de tramage.

Ces AVP peuvent coexister avec les AVP Mandataire LCP et Authentification de mandataire (AVP mandataires) définies dans la spécification L2TP de base. Si des AVP Mandataire sont reçues, le LNS peut choisir d'accepter ces paramètres, ou de renégocier LCP avec les options suggérées par les AVP définies dans le présent document. Si le LAC souhaite forcer la négociation de LCP par le LNS, il devrait simplement omettre toutes les AVP Mandataires durant l'initialisation d'appel.

Par défaut, les AVP définies dans le présent document ne sont pas obligatoires (le bit M est réglé à zéro). Cependant, si une mise en œuvre a besoin d'appliquer fortement d'adhésion aux options définies dans les AVP, elle PEUT régler le bit M à 1, forçant ainsi l'homologue à interrompre la session si il n'accepte pas cette AVP. Ceci N'EST PAS recommandé sauf si il est connu que le résultat du fonctionnement sans ces extensions est complètement inacceptable.

Si les AVP des paragraphes 2.1 et 2.2 sont envoyées au LNS, le LAC DOIT être prêt à accepter les AVP comme définies au paragraphe 2.3.

2.1 LCP veut des options (iccn, occn)

L'AVP "LCP veut des options", type d'attribut 49, contient une liste d'options dont le LAC veut qu'elles soient négociées par le LNS.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|M|H|réservé|          Longueur          |          Identifiant de fabricant  |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|          Type d'attribut          |Demande de configuration LCP ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|          Demande de configuration LCP (suite) ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

L'identifiant de fabricant est l'identifiant de fabricant IETF de 0.

Cette AVP PEUT être cachée (le bit H PEUT être 0 ou 1).

Le bit M pour cette AVP peut être réglé à 0 ou 1. Si l'envoyeur de cette AVP ne souhaite pas établir une connexion avec un homologue qui ne comprend pas cette extension L2TP, il DEVRAIT régler le bit M à 1 ; autrement, il DOIT être réglé à 0.

Le champ Longueur (avant de cacher) de cette AVP est 6, plus la longueur de la demande de configuration de LCP.

L'AVP DEVRAIT être présente dans les messages suivants : ICCN, OCCN

La valeur Configure-Req LCP pour cette AVP est identique au champ Information d'un paquet Configure-Req PPP LCP (comme une AVP Mandataire LCP dans la [RFC2661]). Elle est envoyée du LAC au LNS, et est destinée à guider les négociations PPP LCP au LNS. Dans certains cas, chaque option individuelle PPP LCP portée dans cette AVP se transpose en une valeur désirée (par exemple, une MRU) et dans certains cas, elle se transpose en une option spécifique qu'on désire activer (par exemple, ACFC). Le LNS devrait utiliser ces suggestions lors de la construction de sa demande de configuration initiale.

Le tableau suivant définit certaines des options LCP les plus courantes qui peuvent être incluses dans cette AVP avec des indications sur la façon de les traiter au LAC et au LNS. Ce tableau est fourni pour certaines des options LCP les plus courantes ou les plus problématiques. Il n'est pas destiné à être une représentation exhaustive de toutes les options LCP disponibles.

Option voulue du LCP	Action du LAC	Action du LNS
MRU	Le LAC donne une valeur maximum	Le LNS DEVRAIT commencer la négociation LCP de valeur maximum avec cette valeur. Cependant, il PEUT réduire la MRU si nécessaire..
ACCM	Le LAC donne un gabarit	Le LNS DEVRAIT commencer la négociation LCP avec cette valeur. Le LNS peut ajouter des bits dans la négociation. .
PFC	Le LAC fournit PFC sur le type de liaison (par exemple AHDLC).	Le LNS DEVRAIT commencer la négociation de LCP si il le désire avec cette valeur.
ACFC	Le LAC fournit ACCOMP si il le désire sur ce type de liaison (par exemple, AHDLC).	Le LNS DEVRAIT commencer la négociation LCP avec cette valeur.
FCS-ALT	Le LAC indique les valeurs requises pour le type de liaison.	Le LNS DEVRAIT commencer la négociation avec cette valeur. Noter que cette valeur n'a pas de conséquence pour le LNS car FCS est supprimé au LAC, cependant certains types de support exigent cette option.

2.2 Options permises au LCP (iccn, occn)

Options permises au LCP, type d'attribut 50, contient une liste des options que le LAC va permettre de négocier au LNS.

```

      0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|M|H|réservé|   Longueur   |   Identifiant de fabricant   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type d'attribut   |   Configure-Ack LCP ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
... Configure-Ack LCP (suite) ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

L'identifiant de fabricant est l'identifiant de fabricant de l'IETF de 0.

Cette AVP PEUT être cachée (le bit H PEUT être 0 ou 1).

Le bit M pour cette AVP peut être réglé à 0 ou 1. Si l'envoyeur de cette AVP ne souhaite pas établir une connexion avec un homologue qui ne comprend pas cette extension L2TP, il DEVRAIT régler le bit M à 1 ; autrement, il DOIT être réglé à 0.

La longueur (avant de cacher) de cette AVP est 6, plus la longueur de l'accusé de réception de la demande configuration LCP.

L'AVP PEUT être présente dans les messages suivants : ICCN, OCCN

La valeur LCP Configure-Ack pour cet AVP est identique au champ Information d'un paquet de demande de configuration PPP LCP (un peu comme une AVP Mandataire LCP dans la [RFC2661]). Elle est envoyée du LAC au LNS, et est destinée à guider les négociations PPP LCP au LNS. Dans certains cas, chaque option PPP LCP individuelle portée dans cette AVP se transpose en une valeur maximum (par exemple, une MRU) tandis que dans d'autres elle se transpose en une option qui est permise par le LAC (par exemple, ACFC). Si l'option n'est pas incluse ici, le LNS peut supposer que le LAC ne comprend pas comment effectuer cette option particulière à la couche liaison (et va donc faire un Configure-Rejet pour cette option). Les informations de cette AVP devraient être utilisées lors de la construction des messages PPP Configure-Ack, Configure-Rejet et Configure-Nak.

Le tableau suivant définit certaines des options LCP les plus courantes qui peuvent être incluses dans cette AVP avec des indications sur la façon de les traiter au LAC et au LNS. Ce tableau est fourni à des fins d'illustration pour certaines des options LCP les plus courantes ou problématiques. Il n'est pas destiné à être une représentation exhaustive de toutes les options LCP disponibles.

Options permises au LCP	Action du LAC	Action du LNS
MRU	Le LAC donne une valeur maximum.	Le LNS peut accepter une réduction de MRU si demandé.
ACCM	Le LAC donne un gabarit.	Le LNS peut accepter les bits définis ici. Noter que si ACCM manque, on suppose qu'elle n'est pas applicable à ce type de liaison.
PFC	Le LAC fournit PFC si c'est permis sur ce type de liaison (par exemple, AHDLC).	Le LNS peut accepter PFC.
ACFC	Le LAC fournit ACFC si c'est permis sur ce type de liaison (par exemple, AHDLC).	Le LNS peut accepter ACFC.
FCS-ALT	Le LAC indique des valeurs valides pour le type de liaison.	La négociation de cette option est sans conséquence pour le LNS car le FCS est supprimé au LAC. Cependant, le LNS DEVRAIT n'accepter que les types FCS-ALT notés ici (plus d'une valeur peut être présente).

2.3 Options LCP du LNS au LAC

Afin de communiquer les paramètres LCP négociés du LNS au LAC, le format des deux messages existants dans la [RFC2661] est utilisé. Ce sont :

Dernière demande de configuration LCP demandée (Attribut IETF L2TP 27)

Dernière demande de configuration LCP reçue (Attribut IETF L2TP 28)

Ces AVP sont envoyées du LAC au LNS pour prendre en charge la négociation Mandataire LCP. Afin de rapporter les paramètres LCP négociés du LNS au LAC, deux messages ayant précisément le même format sont définis :

Dernière demande de configuration LCP envoyée du LNS (Attribut IETF L2TP 51)

Dernière demande de configuration LCP reçue du LNS (Attribut IETF L2TP 52)

Lorsque la négociation LCP est achevée par le LNS, un message de contrôle Set-Link-Info contenant ces AVP DOIT être envoyé. Ces AVP DOIVENT contenir le dernier paquet LCP envoyé et reçu (par rapport au LNS).

Plutôt que de simplement utiliser les vieilles valeurs d'attribut dans le message SLI, de nouveaux types d'attribut d'AVP sont définis pour ces messages du fait que certaines mises en œuvre existantes de L2TP pourraient faire des vérifications de ce qui semblerait un placement erroné de types d'AVP connus et générer une fausse condition d'erreur.

3. Considérations sur la sécurité

Aucune menace significative supplémentaire connue n'est induite par les mécanismes décrits dans le présent document.

Il définit des AVP L2TP supplémentaires qui identifient des caractéristiques de liaison et des informations d'interface d'une liaison PPP tunnelée. Si ces valeurs sont divulguées, un pirate peut avoir accès à plus d'informations sur un certain réseau ou une certaine topologie. Étant donné que ces mêmes valeurs peuvent de toutes façons être négociées sur la liaison tunnelée dans

les paquets LCP PPP, ce ne sont pas plus d'informations que celles qui sont potentiellement transmises aujourd'hui, simplement sous une forme différente.

4. Considérations relatives à l'IANA

Le présent document requiert quatre nouveaux numéros "d'attribut AVP" L2TP à allouer par l'IANA :

- 49, paragraphe 2.1, LCP veut des options
- 50, paragraphe 2.2, Options permises au LCP
- 51, paragraphe 2.3, Dernière demande de configuration LCP envoyée du LNS
- 52, paragraphe 2.3, Dernière demande de configuration LCP reçue du LNS

5. Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC1661] W. Simpson, éditeur, "[Protocole point à point](#) (PPP)", STD 51, juillet 1994. (*MàJ par la RFC2153*)
- [RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de [tunnelage de couche 2](#) (L2TP)", août 1999. (*P.S.*)

6. Adresse des auteurs

W. Mark Townsley
Cisco Systems
7025 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709
USA
mél : mark@townsley.net

Bill Palter
mél : palter.ietf@zev.net

7. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2002). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

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