

Groupe de travail Réseau
Request for Comments : 3145
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

R. Verma, Deloitte Consulting
M. Verma, 3Com Corporation
J. Carlson, Sun Microsystems
juillet 2001

Information sur la cause de déconnexion dans L2TP

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 (2001). Tous droits réservés.

Résumé

Le présent document fait une extension au protocole de tunnelage de couche 2 (L2TP, *Layer 2 Tunneling Protocol*) qui est un mécanisme pour tunneler les sessions du protocole point à point (PPP). Il manque à L2TP un mécanisme pour qu'un hôte fournisse à un autre hôte les informations de cause de déconnexion en rapport avec PPP. Ces informations, fournies par l'extension décrite dans le présent document, peuvent être utiles pour les besoins de comptabilité et de débogage.

1. Introduction

L2TP [RFC2661] définit un mécanisme d'utilité générale pour tunneler PPP sur divers supports. Par conception, il isole les opérations L2TP des détails de la session PPP qui est encapsulée par L2TP. Il y a cependant des cas où il peut être souhaitable que les informations de déconnexion spécifiques de PPP soient fournies à un hôte L2TP (concentrateur d'accès L2TP (LAC, *L2TP Access Concentrator*) ou serveur réseau L2TP (LNS, *L2TP Network Server*)) sous un format descriptif. L'absence de ces informations pose particulièrement problème lorsque le LAC et le LNS ne sont pas en la possession ou sous la gestion de la même entité.

Les codes de résultat et d'erreur définis pour L2TP spécifient seulement les informations de déconnexion spécifiques de L2TP. Le présent document fournit une paire d'attribut/valeur (AVP, *Attribute Value Pair*) supplémentaire, appelée code de cause de déconnexion PPP, qui PEUT être utilisée par un hôte L2TP pour fournir à ses homologues les informations de déconnexion spécifiques de PPP. Cette AVP devrait être utilisée en conjonction avec, et non comme remplacement, des AVP de code de résultat et d'erreur L2TP.

L'AVP de code de cause de déconnexion PPP peut aussi être utilisée pour fournir à l'utilisateur une cause de déconnexion lisible par l'homme. Cette AVP ne devrait avoir aucun effet sur le fonctionnement du tunnel ni sur le fonctionnement de la session PPP ; elle ne sert qu'à des fins d'information et d'enregistrement d'événement.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. AVP de code de cause de déconnexion PPP

L'AVP n'est valide que dans le message L2TP Notification de déconnexion d'appel (CDN, *Call-Disconnect-Notify*) et elle NE DOIT PAS être marquée Obligatoire.

L'AVP Code de cause de déconnexion PPP est codée avec l'identifiant de fabricant 0 et un Type d'attribut de code de cause de déconnexion PPP de 46. La longueur du champ Valeur DOIT être d'au moins 11 octets. Si la longueur est de plus de 11 octets, les octets supplémentaires DOIVENT contenir un texte descriptif en format UTF-8 [RFC2279] qui puisse être affiché à l'utilisateur ou dans un fichier de journalisation. Le format de l'AVP est montré ci-dessous.

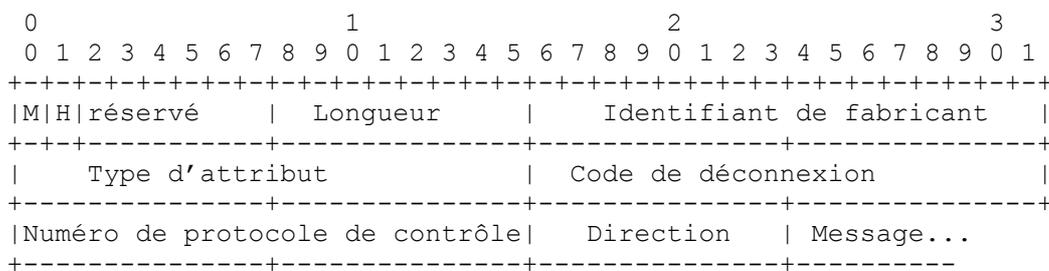


Figure 1 : AVP de code de cause de déconnexion PPP

Bit M (Obligatoire) : DOIT être 0.

Bit H (Caché) : PEUT être 1 si l'attribut est caché.

Longueur : longueur de l'attribut entier en octets, exprimé par un seul octet. La longueur DOIT être au moins 11.

Identifiant de fabricant : valeur de deux octets dans l'ordre des octets du réseau ; réglé à 0 pour indiquer que c'est un attribut alloué par l'IETF.

Type d'attribut : valeur de deux octets dans l'ordre des octets du réseau ; réglé à 46 (Code de cause de déconnexion PPP).

Code de déconnexion : valeur de deux octets dans l'ordre des octets du réseau. (Décrit à la section 3 de ce document.)

Numéro de protocole de contrôle : numéro du protocole de contrôle PPP du protocole principal connu pour avoir causé l'erreur, si il y en a une. Ce champ peut être 0 sauf mention contraire dans la description des codes de déconnexion de la section 3.

Direction : valeur d'un seul octet ; spécifie la direction dans laquelle le code de déconnexion s'applique.

Les valeurs valides de ce champ sont :

- 0 : erreur globale
- 1 : chez l'homologue
- 2 : en local
- 3-255 : réservé

Ce champ DEVRAIT être 0 sauf documenté autrement dans la description du code de déconnexion spécifique.

3. Codes de déconnexion

Cette section contient la liste des valeurs bien connues du champ Code de déconnexion dans l'AVP de code de cause de déconnexion PPP. L'IANA tiendra un registre à jour des valeurs (voir la section 5 de ce document). Ces valeurs devraient être utilisées en conjonction avec la valeur des champs Direction et Numéro de protocole de contrôle pour interpréter la condition d'erreur spécifique.

Sauf mention contraire pour un code de déconnexion spécifique, la valeur de Direction DEVRAIT être 0.

3.1 Erreurs globales

Les codes d'erreur globale, donnés dans la liste ci-dessous, sont les codes de déconnexion qui ne se rapportent pas à un protocole de contrôle PPP particulier. Le numéro de protocole de contrôle pour ces erreurs DOIT donc être réglé à 0.

- 0 pas d'information disponible.
- 1 déconnexion administrative.
- 2 renégociation du protocole de contrôle de liaison (LCP) au LNS désactivée ; le LNS attend des informations de LCP mandataire que le LAC n'a pas envoyées.
- 3 déconnexion normale ; demande de terminaison de LCP envoyée.
 - Les valeurs de Direction valides sont :
 - 1 demande de terminaison de LCP envoyée par l'homologue,
 - 2 demande de terminaison de LCP envoyée par l'hôte local.
- 4 le chiffrement obligatoire exigé par l'homologue PPP a été refusé par l'autre.
 - Les valeurs de Direction valides sont :

- 1 exigé en local ; refusé par l'homologue,
- 2 exigé par l'homologue ; refusé en local.

3.2 Erreurs de LCP

Les codes d'erreur de LCP, dont la liste est donnée ci-dessous, sont des raisons de déconnexion qui se rapportent directement à l'échec des homologues PPP à négocier des paramètres de liaison mutuellement acceptables. Le numéro de protocole de contrôle pour ces erreurs DOIT être réglé à C021 (hexadécimal pour LCP).

- 5 erreur de fin de temporisation d'automate à états finis (FSM, *Finite State Machine*). (événement PPP "TO-".)
- 6 des paquets LCP non reconnaissables ont été reçus.
- 7 échec du LCP : erreur de numéro magique ; liaison éventuellement en boucle.
- 8 échec de liaison LCP : fin de temporisation de demande d'écho.
- 9 l'homologue a un discriminateur de point d'extrémité inattendu pour un faisceau existant de multi liaison PPP (MP).
- 10 l'homologue a une MRRU inattendue pour le faisceau de MP existant.
- 11 l'homologue a une option Numéro de séquence court inattendue pour le faisceau de MP existant.
- 12 rappel obligatoire exigé par un homologue PPP a été refusé par l'autre.
Les valeurs de Direction valides sont :
 - 1 exigé en local ; refusé par l'homologue
 - 2 exigé par l'homologue ; refusé en local

3.3 Erreurs d'authentification

La liste des codes d'erreur d'authentification ci-dessous sont des raisons de déconnexion qui se rapportent directement aux échecs d'authentification entre les homologues PPP. Le numéro de protocole de contrôle pour de telles erreurs DOIT correspondre au numéro de protocole de contrôle PPP pour le protocole d'authentification utilisé.

- 13 erreur de fin de temporisation de FSM.
- 14 l'homologue a un nom authentifié inattendu pour le faisceau de MP existant.
- 15 échec d'authentification PPP : protocole d'authentification inacceptable.
Les valeurs de Direction valides sont :
 - 1 tous les protocoles d'authentification locaux ont été rejetés par l'homologue.
 - 2 tous les protocoles d'authentification demandés par l'homologue étaient inacceptables ou impossibles à mettre en œuvre en local.
- 16 échec d'authentification PPP : l'authentification a échoué (mauvais nom, mot de passe, ou secret).
Les valeurs de Direction valides sont :
 - 1 authentification de l'identité de l'homologue par le système local.
 - 2 authentification de l'identité locale par le système homologue.

3.4 Erreurs de protocole de contrôle réseau (NCP)

Les erreurs de NCP sont des raisons de déconnexion qui se rapportent directement à l'échec des homologues PPP à négocier un ensemble mutuellement acceptable de paramètres pour les protocoles réseau. Le numéro de protocole de contrôle pour de telles erreurs DEVRAIT correspondre au numéro de protocole de contrôle réseau PPP utilisé. Lorsque plusieurs protocoles réseau sont utilisés, plusieurs copies de cette AVP PEUVENT être données pour indiquer les raisons d'échec pour chaque NCP. Autrement, si une seule copie de l'AVP est donnée, le numéro de protocole de contrôle DEVRAIT correspondre au dernier (plus récent) NCP défaillant.

- 17 erreur de fin de temporisation de FSM.
- 18 aucun NCP disponible (tous désactivés ou rejetés) ; aucun NCP n'est passé à l'état Ouvert. (Le numéro de protocole de contrôle ne peut être zéro que si aucun homologue n'a de NCP activé.)
- 19 défaillance de NCP : échec à converger sur des adresses acceptables.
Les valeurs de Direction valides sont :
 - 1 trop de Configure-Nak reçus de l'homologue.
 - 2 trop de Configure-Nak envoyés à l'homologue.
- 20 défaillance de NCP : l'utilisateur n'a la permission d'utiliser aucune adresse.
Les valeurs de Direction valides sont :
 - 1 adresse de liaison locale non acceptable pour l'homologue.

- 2 adresse de liaison distante non acceptable pour le système local.

4. Notes

Cette AVP PEUT être envoyée par le LNS ou par le LAC. On s'attend généralement à ce que cette AVP soit des plus utiles dans l'envoi de notification du LNS au LAC dans le cas de tunnelage obligatoire, bien qu'il ne soit pas interdit de l'utiliser dans de tout autre cas.

Une forme restée en projet de cette AVP utilisait l'identifiant de fabricant 43 (3Com Corporation) et le type d'attribut spécifique du fabricant 46. Les mises en œuvre PEUVENT accepter les AVP qui ont ces valeurs comme équivalentes au message décrit dans le présent document, mais NE DEVRAIENT PAS émettre une AVP utilisant ces valeurs.

5. Considérations pour la sécurité

L'intégrité et la confidentialité de cette AVP s'appuient sur les mécanismes de sécurité L2TP sous-jacents. Elles sont destinées à l'enregistrement dans les journaux d'événement et aux fins de diagnostic pour le cas de défaillance de la liaison PPP et cela ne devrait pas faire peser de menace sur la sécurité du système, mais l'AVP PEUT être cachée comme décrit au paragraphe 4.3 de la [RFC2661].

L'extension définie ne fournit pas d'information qui serait utile à un attaquant. De futures extensions ne devraient pas être définies pour diminuer la sécurité. Par exemple, il est inapproprié de fournir des informations distinctives qui informeraient l'homologue qu'un certain nom d'authentification est correct, mais que le mot de passe/secret est incorrect.

6. Considérations en rapport avec l'IANA

L'IANA a alloué une valeur de type d'attribut L2TP de 46 au code de cause de déconnexion PPP défini à la Section 2.

Cet AVP inclut une valeur de code de cause, appelée "code de déconnexion". Les valeurs 0 à 20 sont décrites dans le présent document. Les valeurs 21 à 32767 (inclus) sont allouées par l'IANA sous réserve de l'approbation de l'IESG. Les valeurs 32768 à 65279 (inclus) sont allouées par l'IANA selon le principe du premier arrivé, premier servi, et sont destinées à des caractéristiques de fabricant. Les valeurs 65280 à 65535 (inclus) sont allouées pour utilisation privée ou expérimentale, et l'IANA n'a pas prévu de prendre part à leur allocation.

7. Références

- [RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de [tunnelage de couche 2](#) "L2TP"", (P.S.)
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir [RFC3629](#)*) (D.S.)

8. Remerciements

Les auteurs remercient W. Mark Townsley et Thomas Narten de leur aide et de leurs commentaires.

9. Contacts

9.1 Président du groupe de travail L2TP

W. Mark Townsley
Cisco Systems
7025 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709

mél : townsley@cisco.com

9.2 Adresse des auteurs

Rohit Verma
180 N. Stetson Avenue
Chicago IL 60601
téléphone : +1 312 374 2475
Fax : +1 312 870 2475
mél : rverma@dc.com

Madhvi Verma
3800 Golf Road
Rolling Meadows IL 60008
téléphone : +1 847 262 2987
Fax: +1 847 262 2255
mél : Madhvi_Verma@3com.com

James Carlson
Sun Microsystems
1 Network Drive MS UBUR02-212
Burlington MA 01803-2757
téléphone: +1 781 442 2084
mél : james.d.carlson@sun.com

10. Notices standard

10.1. Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2001). Tous droits réservés.

Ce document et les traductions de celui-ci peuvent être copiés et diffusés, et les travaux dérivés qui commentent ou expliquent autrement ou aident à sa mise en œuvre peuvent être préparés, copiés, publiés et distribués, partiellement ou en totalité, sans restriction d'aucune sorte, à condition que l'avis de copyright ci-dessus et ce paragraphe soit inclus sur toutes ces copies et œuvres dérivées. Toutefois, ce document lui-même ne peut être modifié en aucune façon, par exemple en supprimant le droit d'auteur ou les références à l'Internet Society ou d'autres organisations Internet, sauf si c'est nécessaire à l'élaboration des normes Internet, auquel cas les procédures pour les droits de reproduction définis dans les processus des normes pour l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet, ses successeurs ou ayants droit.

Ce document et les renseignements qu'il contient sont fournis "TELS QUELS" et l'INTERNET SOCIETY et l'INTERNET ENGINEERING TASK FORCE déclinent toute garantie, expresse ou implicite, y compris mais sans s'y limiter, toute

garantie que l'utilisation de l'information ici présente n'enfreindra aucun droit ou aucune garantie implicite de commercialisation ou d'adaptation a un objet particulier.

Remerciement

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