

Groupe de travail Réseau
Request for Comments : 3070
 Catégorie : En cours de normalisation
 Traduction Claude Brière de L'Isle

V. Rawat, ONI Systems, Inc.
 R. Tio & S. Nanji, Redback Networks, Inc.
 R. Verma, Deloitte Consulting
 février 2001

Protocole de tunnelage de couche deux (L2TP) sur relais de trame

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 protocole de tunnelage de couche deux (L2TP, *Layer Two Tunneling Protocol*) décrit un mécanisme pour tunneler les sessions en point à point (PPP). Le protocole a été conçu pour être indépendant du support sur lequel il fonctionne. La spécification de base décrit comment il devrait être mis en œuvre pour fonctionner sur le protocole de datagramme d'utilisateur (UDP, *User Datagram Protocol*) et le protocole Internet (IP). Le présent document décrit comment L2TP est mis en œuvre sur des circuits virtuels permanents (PVC, *Permanent Virtual Circuit*) et des circuits virtuels commutés (SVC, *Switched Virtual Circuit*) en relais de trame.

Applicabilité

La présente spécification est destinée aux mises en œuvre qui désirent utiliser les facilités qui sont définies pour L2TP et s'applique seulement à l'utilisation de circuits point à point en relais de trame.

1. Introduction

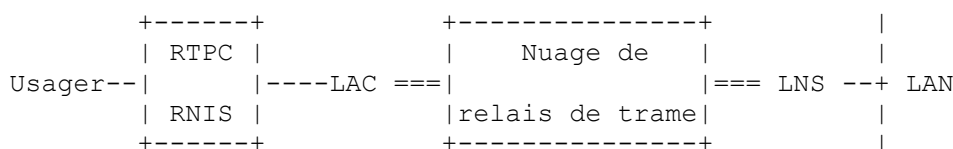
L2TP [RFC2661] définit un mécanisme à caractère général pour tunneler PPP sur divers supports. Par sa conception, il isole le fonctionnement de L2TP des détails du support sur lequel il opère. La spécification de base du protocole illustre comment L2TP peut être utilisé dans des environnements IP. Le présent document spécifie l'encapsulation de L2TP sur du relais de trame natif et traite des questions pertinentes.

2. Conventions

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

3. Généralités sur la portée du problème

Dans cette section, on décrit en termes généraux la portée du problème considéré. Topologie :



Un concentrateur d'accès L2TP (LAC, *L2TP Access Concentrator*) est un appareil rattaché au système de réseau commuté (par exemple, RTPC ou RNIS) ou colocalisé avec un système terminal PPP capable de traiter le protocole L2TP. Le LAC a seulement besoin de mettre en œuvre le support sur lequel L2TP va fonctionner pour passer le trafic à un ou plusieurs serveurs de réseau L2TP (LNS, *L2TP Network Server*). Il peut tunneler tout protocole porté dans PPP.

Le serveur de réseau L2TP (LNS) fonctionne sur toute plateforme capable de terminaison PPP. Le LNS traite le côté

serveur du protocole L2TP. L2TP est en mode connexion. Le LNS et le LAC conservent l'état pour chaque utilisateur qui est rattaché à un LAC. Une session est créée lorsque une connexion PPP de bout en bout est tentée entre un usager et le LNS. Les datagrammes qui se rapportent à une session sont envoyés sur le tunnel entre le LAC et le LNS. Un tunnel est défini par une paire LNS-LAC. Le tunnel porte les datagrammes PPP entre le LAC et le LNS.

Le protocole L2TP fonctionne à un niveau au dessus du support particulier sur lequel il est porté. Cependant, certains détails de sa connexion au support sont exigés pour permettre l'interopérabilité des mises en œuvre. L2TP sur IP/UDP est décrit dans la spécification L2TP de base [RFC2661]. Les questions relatives à L2TP sur relais de trame sont traitées dans les sections suivantes de ce document.

4. Encapsulation et format de paquet

L2TP DOIT être capable de partager un circuit virtuel (VC, *virtual circuit*) en relais de trame avec d'autres protocoles portés sur le même VC. Le format d'en-tête de relais de trame pour les paquets de données doit être défini pour identifier le protocole porté dans les paquets. Le réseau de relais de trame peut ne pas comprendre ces formats.

Tous les protocoles sur ce circuit DOIVENT encapsuler leurs paquets dans une trame Q.922. De plus, les trames doivent contenir les informations nécessaires pour identifier le protocole porté au sein de l'unité de données de protocole (PDU, *Protocol Data Unit*) de relais de trame, permettant ainsi au receveur de traiter correctement les paquets entrants.

Le format de trame pour L2TP DOIT être l'encapsulation SNAP comme définie dans la [RFC1490] et [FRF.3.1]. Le format SNAP utilise un NLPID suivi par un identifiant unique d'organisation (OUI, *Organizationally Unique Identifier*) et un identifiant de protocole (PID).

NLPID

Cet identifiant d'un seul octet donne un mécanisme permettant une identification facile du protocole. Pour L2TP, la valeur du NLPID est 0x80 qui indique la présence d'un en-tête SNAP.

OUI & PID

L'identifiant unique d'organisation de trois octets 0x00-00-5E identifie l'IANA qui administre la signification de l'identifiant de protocole (PID) 0x0007. Ils identifient ensemble un protocole distinct.

Le format des trames L2TP encapsulées en relais de trame est donné à la Figure 1.

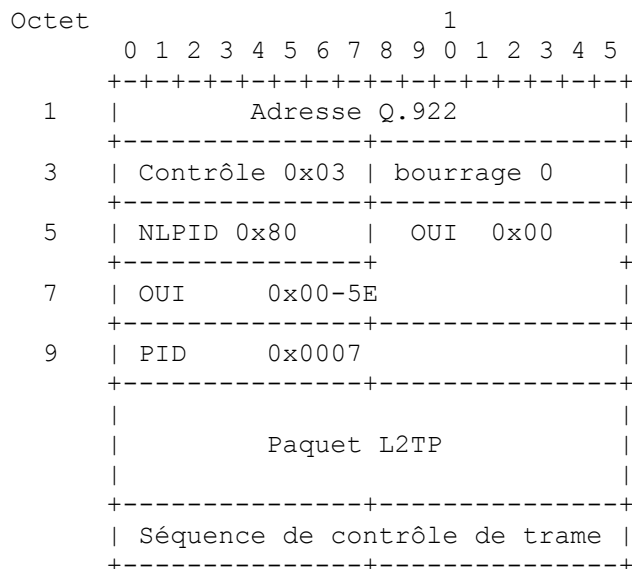


Figure 1 : Format des trames L2TP encapsulées en relais de trame

5. Considérations sur la MTU

[FRF.12] est l'accord sur la mise en œuvre de la fragmentation en relais de trame. Si la fragmentation n'est pas supportée, les deux points d'extrémité de relais de trame DOIVENT prendre en charge une taille de MTU d'au moins 1526 qui est fondée sur l'addition de la taille de Max-Receive-Unit PPP et de la taille d'en-tête PPP avec la taille d'en-tête maximum L2TP et de la taille d'en-tête de relais de trame (la taille d'en-tête PPP est la taille du champ Protocole plus les octets de tramage HDLC, qui est exigé par L2TP). Pour éviter l'élimination de paquets sur l'interface de relais de trame, la MTU par défaut de relais de trame RECOMMANDÉE est de 1564 sur la base d'une MRU PPP par défaut de 1500. Les moyens pour assurer ces réglages de MTU sont laissés à la mise en œuvre.

6. Questions de QS

En général, des mécanismes de qualité de service peuvent être fournis par des mécanismes propriétaires localisés dans le LAC ou le LNS. Les considérations de qualité de service sortent du domaine d'application du présent document.

7. Interaction relais de trame L2TP

Dans le cas de SVS en relais de trame, l'établissement de la connexion va être déclenché lorsque L2TP essaye de créer un tunnel. Les détails du mécanisme de déclenchement relèvent de la mise en œuvre. Il ne DEVRA y avoir aucun changement dans la signalisation de SVC en relais de trame à cause de L2TP. Les points d'extrémité du tunnel L2TP DOIVENT être identifiés par des adresses X.121/E.164 en cas de SVC en relais de trame. Ces adresses PEUVENT être obtenues comme points d'extrémité de tunnel pour un utilisateur comme défini dans la [RFC2868]. En cas de PVC, le circuit virtuel pour porter le trafic L2TP PEUT être configuré administrativement. Les points d'extrémité du tunnel DOIVENT être identifiés par le DLCI, alloué au PVC au moment de la configuration. Ce DLCI PEUT être obtenu comme point d'extrémité de tunnel pour un utilisateur comme défini dans la [RFC2868].

Il NE DEVRA PAS y avoir de problème de tramage entre PPP et le relais de trame. Les trames PPP reçues par le LAC de l'utilisateur distant sont débarrassées du CRC, du tramage de liaison, et des octets de transparence, encapsulées dans L2TP, et transmises sur le tunnel de relais de trame.

8. Considérations pour la sécurité

Il n'y a actuellement pas de spécification standard de la sécurité du relais de trame bien que le Forum Relais de trame travaille à un accord de confidentialité du relais de trame. À la lumière de ce travail, la question de la sécurité sera réexaminée ultérieurement pour voir si des mécanismes de protection spécifiques de L2TP sur relais de trame sont nécessaires. Dans l'intervalle, les questions de sécurité de base sont discutées dans la spécification de base de L2TP [RFC2661].

9. Remerciements

Ken Pierce (3Com Corporation) et (Rick Dynarski 3Com Corporation) ont contribué à l'édition de ce document.

10. Références

- [FRF.3.1] Multiprotocol Encapsulation Implementation Agreement, Frame Relay Forum Technical Committee, juin 1995.
- [FRF.12] Frame Relay Fragmentation Implementation Agreement, Frame Relay Forum Technical Committee, décembre 1997.
- [RFC1490] T. Bradley, C. Brown et A. Malis, "Interconnexions multi protocoles sur relais de trame", juillet 1993. (*Remplacée par la RFC2427*)
- [RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

- [RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de [tunnelage de couche 2](#) "L2TP"", (P.S.)
- [RFC2868] G. Zorn et autres, "[Attributs RADIUS](#) pour la prise en charge du protocole de tunnel", juin 2000. (*Information*)

11. Adresse des auteurs

Vipin Rawat
ONI Systems, Inc.
166 Baypointe Parkway
San Jose CA 95134
mél : vrawat@oni.com

Rene Tio
Redback Networks, Inc.
300 Holger Way
San Jose, CA 95134
mél : tor@redback.com

Rohit Verma
Deloitte Consulting
180 N. Stetson Avenue
Chicago Illinois 60601
mél : rverma@dc.com

Suhail Nanji
Redback Networks, Inc.
300 Holger Way
San Jose, CA 95134
mél : suhail@redback.com

12. 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 à un objet particulier.

Remerciement

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