Groupe de travail Réseau
Request for Comments : 4817
Catégorie : Sur la voie de la normalisation

M. Townsley, Cisco Systems
C. Pignataro, Cisco Systems
S. Wainner, Cisco Systems
T. Seely, Sprint Nextel
J. Young

Traduction Claude Brière de L'Isle
mars 2007

Encapsulation de MPLS sur protocole de tunnelage de couche 2, v.3

Résumé
Le protocole de tunnelage de couche 2, version 3 (L2TPv3, *Layer 2 Tunneling Protocol, Version 3*) définit un protocole pour tunneler divers types de charges utiles sur les réseaux IP. Le présent document définit comment porter une pile d'étiquettes MPLS et sa charge utile sur l'encapsulation de données L2TPv3. Cela permet à une application qui exige traditionnellement un réseau de cœur à capacité MPLS, d'utiliser à la place une encapsulation L2TPv3 sur un réseau IP.

Table des matières

1. Introduction

Le présent document définit comment encapsuler une pile d'étiquettes MPLS et sa charge utile dans la charge utile de tunnel L2TPv3. Après avoir défini la procédure d'encapsulation de MPLS sur L2TPv3, d'autres options d'encapsulation de MPLS sur IP, incluant IP, l'encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*), et IPsec sont discutées dans leur contexte avec MPLS sur L2TPv3 dans une section d'applicabilité. Ce document décrit seulement l'encapsulation et ne s'occupe pas de toutes les applications possibles fondées sur MPLS qui peuvent être activées sur L2TPv3.

1.1 Spécification des exigences

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules. Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT",

"NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. MPLS sur codage L2TPv3

MPLS sur L2TPv3 permet le tunnelage d'une pile MPLS [RFC3032] et sa charge utile sur un réseau IP, en utilisant l'encapsulation L2TPv3 définie dans la [RFC3931]. La pile d'étiquettes MPLS et sa charge utile sont portées dans leur intégralité suivant les en-têtes IP (IPv4 ou IPv6) et L2TPv3.

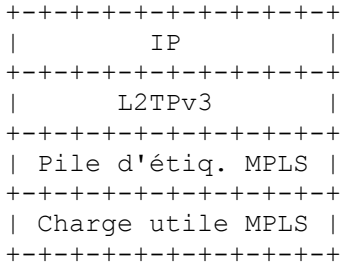

Figure 2.1 : paquet MPLS sur L2TPv3/IP

L'encapsulation L2TPv3 portant une seule entrée de pile d'étiquettes MPLS est comme suit :

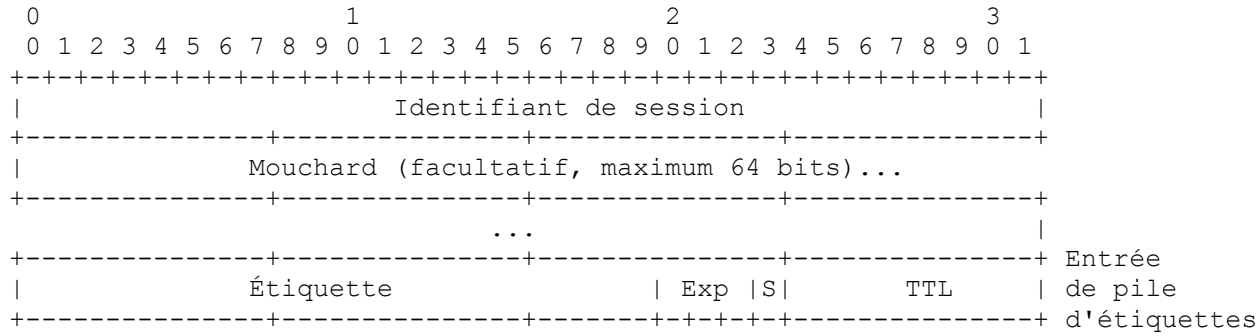

Figure 2.2 : encapsulation MPLS sur L2TPv3

Lors de l'encapsulation de MPLS sur L2TPv3, la sous couche L2TPv3 spécifique de couche 2 PEUT être présente. Elle n'est généralement pas présente ; donc, elle n'est pas incluse dans la Figure 2.2. L'identifiant de session L2TPv3 DOIT être présent. Le mouchard PEUT être présent.

Identifiant de session : c'est un champ d'identifiant de 32 bits choisi en local comme clé de recherche pour le contexte d'une session L2TP. Une session L2TP contient le contexte nécessaire pour le traitement d'un paquet L2TP reçu. Au minimum, ce contexte contient si le mouchard (décrit ci-dessous) est présent, la valeur qui lui a été allouée, la présence et le type d'une sous couche L2TPv3 spécifique de couche 2, ainsi que le type d'encapsulation tunnelé qui suit (c'est-à-dire, relais de trame, Ethernet, MPLS, etc.)

Cookie : le champ Mouchard L2TPv3 contient une valeur de longueur variable (maximum 64 bits) allouée au hasard. Il est destiné à fournir un niveau supplémentaire de garantie qu'un paquet de données a été dirigé sur la bonne session L2TP par l'identifiant de session. Alors que l'identifiant de session peut être codé et recevoir une valeur quelconque (peut-être une optimisation pour les capacités de recherche locales, une redirection dans une architecture de transmission répartie, etc.) le mouchard DOIT être choisi comme une valeur cryptographiquement aléatoire [RFC4086], avec la restriction supplémentaire qu'elle n'est pas la même qu'une valeur utilisée récemment pour un identifiant de session donné. Un mouchard bien choisi va empêcher une mauvaise direction involontaire d'un paquet égaré contenant un identifiant de session récemment réutilisé, un identifiant de session qui est sujet à la corruption de paquet, et assure une protection contre certaines attaques d'insertion de paquet malveillantes spécifiques, comme décrit plus en détails à la Section 4 du document.

Entrée de pile d'étiquettes : entrée de pile d'étiquettes MPLS comme défini dans la [RFC3032].

La sous couche facultative spécifique de couche 2 (définie dans la [RFC3931]) n'est généralement pas présente pour MPLS sur L2TPv3.

Les procédures génériques d'encapsulation IP, comme la fragmentation et les considérations de MTU, le traitement des bits de durée de vie (TTL, *Time to Live*), EXP, et codet de services différenciés (DSCP, *Differentiated Services Code Point*) etc. sont les mêmes que pour les "procédures communes" pour l'encapsulation IP de MPLS définies à la Section 5 de la [RFC4023] et ne sont pas répétées ici.

3. Allocation de l'identifiant de session L2TPv3 et du mouchard

Un peu comme une étiquette MPLS, l'identifiant de session et le mouchard L2TPv3 doivent être choisis et échangés entre les nœuds participants avant que L2TPv3 puisse fonctionner. Ces valeurs peuvent être configurées manuellement, ou distribuées via un protocole de signalisation. Le présent document s'occupe seulement de l'encapsulation de MPLS sur L2TPv3 ; donc, la méthode particulière pour allouer l'identifiant de session et le mouchard (si il est présent) sort du domaine d'application du présent document.

4. Applicabilité

Les méthodes définies dans la [RFC4023], [MPLS-IPSEC], et le présent document décrivent toutes les méthodes pour porter MPLS sur un réseau IP. Les cas où MPLS sur L2TPv3 est comparable aux autres solutions de remplacement sont discutées dans cette section.

Il est généralement plus simple d'avoir des routeurs de bordure qui refusent d'accepter un paquet MPLS que de configurer un routeur à refuser d'accepter certains paquets MPLS portés dans IP ou GRE de ou vers certaines sources ou destinations IP. Donc, l'utilisation de IP ou GRE pour porter des paquets MPLS augmente la probabilité qu'une attaque par usurpation d'étiquette MPLS réussisse. L2TPv3 fournit un niveau supplémentaire de protection contre l'usurpation d'identité de paquet avant de permettre à un paquet d'entrer sur un réseau privé virtuel (VPN, *Virtual Private Network*) (un peu comme IPsec fournit un niveau de protection supplémentaire au routeur côté fournisseur (PE, *Provider Edge*) plutôt que de s'appuyer sur des filtres de liste de contrôle d'accès (ACL, *Access Control List*)). Vérifier la valeur du mouchard L2TPv3 est similaire à une sorte d'ACL qui inspecte le contenu d'un en-tête de paquet, sauf qu'on se donne le luxe de "mettre un germe" à l'en-tête L2TPv3 avec une valeur qui est très difficile à usurper.

MPLS sur L2TPv3 peut être avantageux comparé à la [RFC4023], si :

- Deux routeurs sont déjà "adjacents" sur un tunnel L2TPv3 établi pour une autre raison, et souhaitent échanger des paquets MPLS sur cette adjacence.

- Des considérations de mise en œuvre imposent l'utilisation de MPLS sur L2TPv3. Par exemple, un appareil peut être capable de tirer parti de l'encapsulation L2TPv3 pour un traitement plus rapide ou réparti.

- La protection contre l'usurpation et l'insertion de paquet, l'intégrité du service et des ressources sont des soucis, en particulier à cause du fait qu'un tunnel IP expose potentiellement le routeur à des paquets IP falsifiés ou inappropriés provenant de sources inconnues ou non fiables. Les listes de contrôle d'accès (ACL, *Access Control List*) IP et les méthodes de numérotation peuvent être utilisées pour protéger les routeurs PE contre les sources IP non fiables, mais peuvent être sujettes à des erreurs et sont difficiles à maintenir tout le temps à tous les points de bordure. Le mouchard L2TPv3 fournit un moyen simple de valider la source d'un paquet L2TPv3 avant de permettre la poursuite du traitement. Cette validation offre un niveau supplémentaire de protection par dessus les ACL IP, et une validation que l'identifiant de session n'a pas été corrompu dans le transit ou subi une erreur de recherche interne à la réception et au traitement. Si la valeur du mouchard est allouée et distribuée automatiquement, elle est moins sujette à une erreur de l'opérateur ; et si elle est d'une nature cryptographiquement aléatoire, moins sujette à des suppositions à l'aveugle que les adresses de source IP (dans le cas ou un pirate pourrait insérer des paquets dans un cœur de réseau).

(Les deux premières déclarations d'applicabilité ci-dessus ont été tirées de la [RFC4023].)

En résumé, L2TPv3 peut fournir un équilibre entre une sécurité limitée contre les attaques d'usurpation IP offertes par la [RFC4023] et une plus grande sécurité et les frais généraux de fonctionnement et de traitement associés offerte par [MPLS-

IPSEC]. De plus, MPLS sur L2TPv3 peut être plus rapide dans certains matériels, en particulier si ce matériel est déjà optimisé pour classer les paquets L2TPv3 entrants qui portent IP tramé de diverses façons. Par exemple, IP encapsulé par une commande de liaison des données de haut niveau (HDLC, *High-Level Data Link Control*) ou le relais de trame sur L2TPv3 peuvent être équivalent en complexité à IP encapsulé par MPLS sur L2TPv3.

5. Considérations d'encombrement

Le présent document spécifie une méthode d'encapsulation pour MPLS à l'intérieur de la charge utile de tunnel L2TPv3. MPLS peut porter un certain nombre de protocoles différents comme charges utiles. Quand un flux MPLS/L2TPv3 porte du trafic fondé sur IP, le trafic agrégé est supposé accepter TCP à cause des mécanismes de contrôle d'encombrement utilisés par le trafic de charge utile. La perte de paquets va déclencher la réduction nécessaire de la charge offerte, et aucune autre action supplémentaire d'évitement d'encombrement n'est nécessaire.

Quand un flux MPLS/L2TPv3 porte du trafic de charge utile qui n'est pas connu pour accepter TCP et que le flux cours à travers un chemin non provisionné qui pourrait éventuellement devenir encombré, l'application qui utilise l'encapsulation spécifiée dans le présent document DOIT employer des mécanismes supplémentaires pour s'assurer que la charge offerte est réduite de façon appropriée durant les périodes d'encombrement. Le flux MPLS/L2TPv3 ne devrait pas excéder la bande passante moyenne que réaliserait un flux TCP à travers le même chemin de réseau et rencontrant les mêmes conditions de réseau, mesuré sur une échelle de temps raisonnable. Ce n'est pas nécessaire dans le cas d'un chemin non provisionné à travers un réseau sur provisionné, où le potentiel d'encombrement est évité par le sur provisionnement du réseau.

La comparaison avec TCP ne peut pas être spécifiée exactement mais est destinée à donner un "ordre de grandeur" de comparaison en échelle de temps et de débit. L'échelle de temps sur laquelle le débit est mesuré est le délai d'aller-retour de la connexion. Par nature, cette exigence déclare qu'il n'est pas acceptable de déployer une application utilisant l'encapsulation spécifiée dans ce document sur l'Internet au mieux, qui consomme arbitrairement la bande passante et n'est pas à armes égales avec TCP d'un ordre de grandeur. Une méthode pour déterminer une bande passante acceptable est décrite dans la [RFC3448]. D'autres méthodes existent, mais cela sort du domaine d'application du présent document.

8. Considérations sur la sécurité

Il y a trois problèmes principaux lors du transport de trafic étiqueté MPLS entre des PE en utilisant des tunnels IP. Le premier est la possibilité qu'un tiers puisse insérer des paquets dans un flux de paquets entre deux PE. Le second est qu'un tiers pourrait voir le flux de paquets entre les deux PE. Le troisième est qu'un tiers puisse altérer les paquets dans un flux entre deux PE. Les exigences de sécurité des applications dont le trafic est envoyé à travers le tunnel caractérisent dans quelle mesure ces problèmes sont significatifs. Les opérateurs peuvent utiliser plusieurs méthodes pour atténuer le risque, incluant des listes d'accès, l'authentification, le chiffrement, et la validation du contexte. Les opérateurs devraient examiner le coût de l'atténuation du risque.

La sécurité est aussi discutée au titre de l'applicabilité dans la Section 4 de ce document.

6.1 En l'absence de IPsec

Si les tunnels ne sont pas sécurisés avec IPsec, alors une autre méthode devrait être utilisée pour s'assurer que les paquets sont désencapsulés et traités par la queue du tunnel seulement si ces paquets ont été encapsulés par la tête du tunnel. Si le tunnel repose entièrement dans un seul domaine administratif, le filtrage d'adresse aux frontières peut être utilisé pour s'assurer qu'aucun paquet avec d'adresse de source IP d'un point d'extrémité de tunnel ou avec l'adresse de destination IP d'un point d'extrémité de tunnel ne peut entrer de l'extérieur dans le domaine.

Cependant, quand la tête du tunnel et la queue du tunnel ne sont pas dans le même domaine administratif, cela peut devenir difficile, et le filtrage fondé sur l'adresse de destination peut même devenir impossible si les paquets doivent traverser l'Internet public.

Parfois, seul le filtrage sur l'adresse de source (mais pas le filtrage sur l'adresse de destination) est fait aux frontières d'un domaine administratif. Si c'est le cas, le filtrage ne fournit pas de protection efficace du tout sauf si le désencapsuleur de MPLS sur L2TPv3 valide l'adresse IP de source du paquet.

De plus, les considérations sur "l'usurpation de paquet de données" du paragraphe 8.2 de la [RFC3931] et les considérations de "validation de contexte" du paragraphe Section 6.2 de ce document s'appliquent. Ces deux paragraphes soulignent les avantages du mouchard L2TPv3.

6.2 Validation de contexte

Le mouchard L2TPv3 ne fournit pas de protection via le chiffrement. Cependant, quand il est utilisé avec une valeur suffisamment aléatoire de 64 bits qui reste secrète à un attaquant hors du chemin, le mouchard L2TPv3 peut être utilisé comme une vérification simple mais efficace de la source du paquet qui est assez résistante aux attaques en force brute d'usurpation de paquet. Il allège aussi le besoin de s'appuyer seulement sur des listes de filtrage fondées sur une liste d'adresses de source IP valides, et déjoue les attaques qui pourraient bénéficier d'une usurpation d'une adresse IP de source permise. Le mouchard L2TPv3 donne un moyen de valider l'identifiant de session couramment alloué sur le flux de paquets, fournissant la protection du contexte, et peut être réputé complémentaire de la sécurisation du tunnel en utilisant IPsec. En l'absence de sécurité cryptographique sur le plan des données (comme celle fournie par IPsec) le mouchard L2TPv3 fournit une méthode simple pour valider la recherche d'identifiant de session effectuée sur chaque paquet L2TPv3. Si le mochard est suffisamment aléatoire et reste inconnu d'un attaquant (c'est-à-dire, si l'attaquant n'a pas de moyen de prédire les valeurs de mouchard ou de surveiller le trafic entre les PE) alors le mouchard fournit une mesure de protection supplémentaire contre les paquets usurpés malveillants insérés au PE sur et au dessus des ACL normales d'adresses et accès IP.

6.3 Sécurisation du tunnel avec IPsec

Les tunnels L2TPv3 peuvent aussi être sécurisés en utilisant IPsec,comme spécifié au paragraphe 4.1.3 de la [RFC3931]. IPsec peut assurer l'authentification, la protection de la confidentialité, la vérification de l'intégrité, et la protection contre la répétition. Ces fonctions peuvent être réputées nécessaires par l'opérateur. Quand on utilise IPsec, la tête du tunnel et la queue du tunnel devraient être traitées comme les points d'extrémité d'une association de sécurité. Une seule adresse IP de la tête de tunnel est utilisée comme adresse IP de source, et une seule adresse IP de la queue du tunnel est utilisée comme l'adresse IP de destination. Les moyens par lesquels chaque nœud connaît la propre adresse de l'autre sortent du domaine d'application du présent document. Cependant, si un protocole de contrôle est utilisé pour établir les tunnels, ce protocole de contrôle DOIT avoir un mécanisme d'authentification, il DOIT être utilisé quand le tunnel est établi. Si le tunnel est établi automatiquement par suite, par exemple, d'informations distribuées par BGP, alors l'utilisation du mécanisme d'authentification fondé sur le résumé de message n° 5 (MD5, *Message Digest 5*) de BGP peut servir à cette fin.

Les paquets encapsulés MPLS sur L2TPv3 devraient être considérés comme originaires de la tête du tunnel et destinés à la queue du tunnel ; le mode de transport IPsec DEVRAIT donc être utilisé.

Noter que la queue du tunnel et la tête du tunnel sont des adjacences de chemin de commutation d'étiquettes (LSP, *Label Switched Path*) (pour les adjacences de distribution d'étiquettes, voir la [RFC3031]) ce qui signifie que l'étiquette sommitale de tout paquet envoyé à travers le tunnel doit être une qui a été distribuée par la queue du tunnel à la tête du tunnel. La queue du tunnel DOIT savoir précisément quelles étiquettes elle a distribuées aux têtes de tunnel des tunnels sécurisés par IPsec. Les étiquettes de cet ensemble NE DOIVENT PAS être distribuées par la queue du tunnel à des adjacences de LSP autres que celles qui sont des têtes de tunnel de tunnels sécurisés par IPsec. Si un paquet MPLS est reçu sans encapsulation IPsec, et si son étiquette sommitale est dans cet ensemble, le paquet DOIT alors être éliminé.

La sécurisation de L2TPv3 en utilisant IPsec DOIT fournir l'authentification et la protection de l'intégrité. (Noter que l'authentification et l'intégrité fournies s'appliquent au paquet MPLS entier, incluant la pile d'étiquettes MPLS.)

Par conséquent, les mises en œuvre DOIVENT prendre en charge l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) avec chiffrement nul. ESP avec chiffrement PEUT être pris en charge si une source exige la confidentialité. Si ESP est utilisé, la queue de tunnel DOIT vérifier que l'adresse IP de source de tout paquet reçu sur une association de sécurité donnée est celle attendue.

La distribution de clés peut être faite manuellement ou automatiquement au moyen du protocole d'échange de clés Internet (IKE, *Internet Key Exchange*) [RFC2409] ou IKEv2 [RFC4306]. Le chiffrement manuel DOIT être pris en charge. Si le chiffrement automatique est mis en œuvre, IKE en mode principal avec clés pré partagées DOIT être pris en charge. Une application particulière peut augmenter cette exigence et demander la mise en œuvre du chiffrement automatique. La distribution manuelle de clés est beaucoup plus simple, mais aussi moins adaptable, que la distribution automatique de clés. Si la protection contre la répétition est estimée nécessaire pour un tunnel particulier, la distribution automatique de clés devrait être configurée.

9. Remerciements

Merci à Robert Raszuk, Clarence Filsfils, et Eric Rosen pour leur relecture de ce document. Du texte a été adopté de la [RFC4023].

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3032] E. Rosen et autres, "Codage de pile d'étiquettes MPLS", janvier 2001.

[RFC3931] J. Lau et autres, "Protocole de tunnelage de couche deux - version 3 (L2TPv3)", mars 2005. *(P.S.)*

[RFC4023] T. Worster et autres, "Encapsulation de MPLS dans IP ou encapsulation d'acheminement générique (GRE)", mars 2005. (*MàJ par* RFC5332) *(P.S.)*

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

8.2 Références pour information

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC3031] E. Rosen, A. Viswanathan, R. Callon, "Architecture de commutation d'étiquettes multi protocoles", janvier 2001. *(P.S.)* (*MàJ par la* RFC6790)

[RFC3448] M. Handley, S. Floyd, J. Padhye, J. Widmer, "Contrôle de débit convivial sur TCP (TFRC) : Spécification du protocole", janvier 2003. (*Obsolète, voir* RFC5348) *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[MPLS-IPSEC] Rosen, E., De Clercq, J., Paridaens, O., T'Joens, Y., and C. Sargor, "Architecture for the Use of PE-PE IPsec Tunnels in BGP/MPLS IP VPNs", Travail en cours, août 2005.

Adresse des auteurs

W. Mark Townsley
Cisco Systems
USA
téléphone : +1-919-392-3741
mél : mark@townsley.net

Carlos Pignataro
Cisco Systems
USA
téléphone : +1-919-392-7428
mél : cpignata@cisco.com

Scott Wainner
Cisco Systems
USA
mél : swainner@cisco.com

Ted Seely
Sprint Nextel
12502 Sunrise Valley Drive
Reston, VA 20196
USA
téléphone : +1-703-689-6425
mél : tseely@sprint.net

Jeff Young
mél : young@jsyoung.net

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient 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 le 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.

Remerciement

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