Groupe de travail Réseau
Request for Comments : 4023
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

T. Worster, Motorola, Inc
Y. Rekhter, Juniper Networks
E. Rosen, Ed., Cisco Systems, Inc.
mars 2005

Encapsulation de MPLS dans IP ou encapsulation d'acheminement générique (GRE)

Résumé
Diverses applications de MPLS font usage de piles d'étiquettes avec plusieurs entrées. Dans certains cas, il est possible de remplacer l'étiquette de niveau supérieur de la pile par une encapsulation fondée sur IP, permettant par là que l'application fonctionne sur des réseaux qui n'ont pas MPLS activé dans leurs routeurs de cœur. Le présent document spécifie deux encapsulations fondées sur IP : MPLS-dans-IP et MPLS-dans-GRE (encapsulation d'acheminement générique). Chacune d'elles est applicable dans certaines circonstances.

Table des matières

1. Motivation

Dans de nombreuses applications de MPLS, les paquets qui traversent un cœur de réseau MPLS portent des piles d'étiquettes avec plus d'une étiquette. Comme décrit au paragraphe 3.15 de la [RFC3031], chaque étiquette représente un chemin à commutation d'étiquette (LSP, *Label Switched Path*). Pour chaque LSP, il y a un routeur à commutation d'étiquettes (LSR, *Label Switching Router*) qui est le "LSP d'entrée", et un LSR qui est le "LSP de sortie". Si les LSR A et B sont respectivement le LSR d'entrée et de sortie du LSP correspondant à l'étiquette supérieure du paquet, alors A et B sont des LSR adjacents sur le LSP correspondant à la seconde étiquette du paquet (c'est-à-dire, l'étiquette immédiatement en dessous de l'étiquette supérieure).

L'objet (ou un des objets) de l'étiquette supérieure est de faire que le paquet soit livré de A à B, afin que B puisse continuer

le traitement du paquet sur la base de la seconde étiquette. Dans ce sens, l'étiquette supérieure sert d'en-tête d'encapsulation pour le reste du paquet. Dans certains cas, d'autres sortes d'en-têtes d'encapsulation peuvent remplacer l'étiquette supérieure sans perte de fonctionnalité. Par exemple, un en-tête IP ou un en-tête d'encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*) pourrait remplacer l'étiquette supérieure. Comme le paquet encapsulé serait encore un paquet MPLS, le résultat est une encapsulation MPLS-dans-IP ou MPLS-dans-GRE.

Avec ces encapsulations, il est possible que deux LSR soient adjacents sur un LSP en étant séparés par un réseau IP, même si ce réseau IP ne fournit pas MPLS.

Pour utiliserl'une ou l'autre de ces encapsulations, le LSR encapsulant doit savoir :
- l'adresse IP du LSR de désencapsulation,
- si le LSR de désencapsulation prend réellement en charge l'encapsulation particulière.

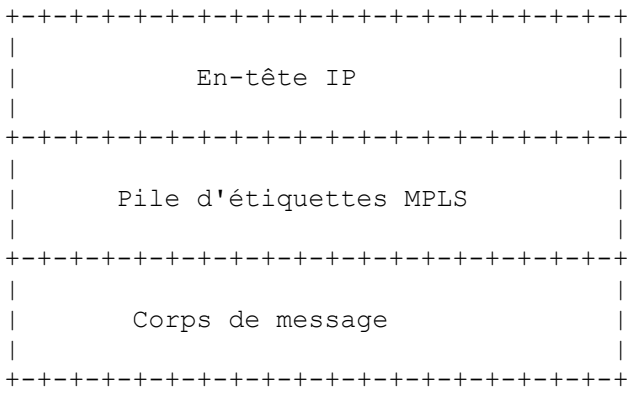
Cette connaissance peut être portée au LSR encapsulant par une configuration manuelle, ou au moyen d'un protocole de découverte. En particulier, si le tunnel est utilisé en soutien d'une application particulière et si cette application a un protocole d'établissement ou de découverte, le protocole de l'application pourrait porter cette connaissance. Les moyens de transport de cette connaissance sortent du domaine d'application du présent document.

2. Spécification des exigences

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].

3. Encapsulation dans IP

Les messages MPLS-dans-IP ont le format suivant :



En-tête IP : ce champ contient un en-tête de datagramme IPv4 ou IPv6 comme défini dans la [RFC0791] ou [RFC2460], respectivement. Les adresses de source et de destination sont réglées aux adresses des LSR respectivement d'encapsulation et de désencapsulation.

Pile d'étiquettes MPLS : ce champ contient une pile d'étiquettes MPLS comme défini dans la [RFC3032].

Corps de message : ce champ contient un corps de message MPLS.

Le champ Numéro de protocole IPv4 ou le champ Prochain en-tête IPv6 est réglé à 137, pour indiquer un paquet MPLS en envoi individuel. (L'utilisation de l'encapsulation MPLS-dans-IP pour les paquets MPLS en diffusion groupée n'est pas prise en charge par la présente spécification.)

À la suite de l'en-tête IP se trouve un paquet MPLS, comme spécifié dans la [RFC3032]. Cette encapsulation cause l'envoi des paquets MPLS à travers des "tunnels IP". Quand le point d'extrémité de réception du tunnel reçoit un paquet, il le désencapsule en retirant l'en-tête IP. Le paquet est alors traité comme un paquet MPLS reçu dont "l'étiquette entrante" [RFC3031] est l'étiquette supérieure du paquet désencapsulé.

4. Encapsulation dans GRE

L'encapsulation MPLS-dans-GRE encapsule un paquet MPLS dans GRE [RFC2784]. Le paquet consiste alors en un en-tête IP (IPv4 ou IPv6) suivi par un en-tête GRE, suivi par une pile d'étiquettes MPLS comme spécifié dans la [RFC3032]. Le champ Type de protocole dans l'en-tête GRE DOIT être réglé à la valeur d'Ethertype pour MPLS en envoi individuel (0x8847) ou en diffusion groupée (0x8848).

Cette encapsulation cause l'envoi des paquets MPLS à travers des "tunnels GRE". Quand le point d'extrémité de réception du tunnel reçoit un paquet, il désencapsule le paquet MPLS en retirant les en-têtes IP et GRE. Le paquet est ensuite traité comme un paquet MPLS reçu dont "l'étiquette entrante" [RFC3031] est l'étiquette supérieue du paquet désencapsulé.

La [RFC2784] spécifie une somme de contrôle GRE facultative, et la [RFC2890] spécifie des champs facultatifs de clé GRE et de numéro de séquence.

Ces champs facultatifs ne sont pas très utiles pour l'encapsulation MPLS-dans-GRE. Les champs Numéro de séquence et Somme de contrôle ne sont pas nécessaires car il n'y a pas de champs correspondants dans les paquets MPLS natifs qui sont tunnelés. Le champ Clé GRE n'est pas nécessaire pour le démultiplexage, car l'étiquette MPLS supérieure du paquet encapsulé est utilisé pour cela. Le champ Clé GRE est parfois considéré comme un dispositif de sécurité, fonctionnant comme un mot de passe de 32 bits en clair, mais c'est une forme de sécurité extrêmement faible. Afin (a) de faciliter les mises en œuvre à haut débit des procédures d'encapsulation/désencapsulation et (b) d'assurer l'interopérabilité, on exige que toutes les mises en œuvre soient capables de fonctionner correctement sans ces champs facultatifs.

Plus précisément, une mise en œuvre de désencapsuleur de MPLS-dans-GRE DOIT être capable de traiter correctement les paquets sans ces champs facultatifs. Elle PEUT être capable de traiter les paquets correctement avec ces champs facultatifs.

Une mise en œuvre d'encapsuleur MPLS-dans-GRE DOIT être capable de générer des paquets sans ces champs facultatifs. Elle PEUT avoir la capacité de générer des paquets avec ces champs, mais l'état par défaut DOIT être que les paquets sont générés sans ces champs. L'encapsuleur NE DOIT PAS inclure un de ces champs facultatifs sauf si il sait que le désencapsuleur peut les traiter correctement. Les méthodes pour porter ces connaissances sortent du domaine d'application de la présente spécification.

5. Procédures communes

Certaines procédures sont communes aux encapsulations MPLS-dans-IP et MPLS-dans-GRE. Dans ce qui suit, l'encapsuleur, dont l'adresse apparaît dans le champ Adresse IP de source de l'en-tête IP encapsulant, est appelé la "tête de tunnel". Le désencapsuleur, dont l'adresse apparaît dans le champ Adresse IP de destination de l'en-tête IP désencapsulant, est appelé la "queue de tunnel".

Si IPv6 est utilisé (pour MPLS-dans-IPv6 ou MPLS-dans-GRE-dans-IPv6) les procédures de la [RFC2473] sont généralement applicables.

5.1 Empêcher la fragmentation et le réassemblage

Si un paquet MPLS-dans-IP ou MPLS-dans-GRE est fragmenté (à cause d'une fragmentation IP "ordinaire") la queue de tunnel va devoir le réassembler avant que le paquet MPLS contenu puisse être désencapsulé. Quand la queue de tunnel est un routeur, cela va probablement être indésirable ; la queue de tunnel peut n'avoir pas la capacité ou les ressources pour effectuer le réassemblage au niveau de performances nécessaire.

L'autorisation de fragmentation des paquets tunnelés DOIT être configurable à la tête du tunnel. La valeur par défaut DOIT être que les paquets ne sont pas fragmentés. La valeur par défaut ne va être changée que si il est connu que la queue du tunnel peut effectuer adéquatemnt la fonction de réassemblage.

Les procédures spécifiées dans le reste de cette section ne s'appliquent que si les paquets ne sont pas fragmentés.

Évidemment, si les paquets ne sont pas à fragmenter, la tête de tunnel NE DOIT PAS fragmenter un paquet avant de l'encapsuler. Si IPv4 est utilisé, le tunnel DOIT alors établir le bit DF. Cela empêche des nœuds intermédiaires dans le

tunnel d'effectuer la fragmentation. (Si IPv6 est utilisé, les nœuds intermédiaires n'effectuent en aucun cas de fragmentation.)

La tête de tunnel DEVRAIT effectuer la découverte de la MTU de chemin ([RFC1191] pour IPv4, ou [RFC1981] pour IPv6).

La tête de tunnel DOIT tenir une "MTU de tunnel" pour chaque tunnel ; c'est le minimum de (a) une valeur configurée administrativement, et, si elle est connue, (b) la valeur de la MTU de chemin découverte moins les frais généraux d'encapsulation.

Si la tête de tunnel reçoit, pour encapsulation, un paquet MPLS dont la taille excède la MTU de tunnel, ce paquet DOIT être éliminé. Cependant, éliminer en silence de tels paquets peut causer des problèmes de fonctionnement significatifs ; le générateur des paquets va remarquer que ses données ne passent plus, mais il peut ne pas réaliser que les gros paquets causent la perte de paquets. Il peut donc continuer d'envoyer des paquets qui sont éliminés. La découverte de la MTU de chemin peut aider (si la tête de tunnel renvoie des erreurs ICMP) mais fréquemment il y a des informations insuffisantes disponibles à la tête de tunnel pour identifier correctement l'envoyeur d'origine. Pour minimiser les problèmes, il est conseillé que les MTU soient calculées de façon assez large pour éviter en pratique la fragmentation.

Dans certains cas, la tête de tunnel reçoit, pour encapsulation, un paquet IP, qu'elle encapsule d'abord dans MPLS et ensuite dans MPLS-dans-IP ou MPLS-dans-GRE. Si la source du paquet IP est accessible à partir de la tête de tunnel, et si le résultat de l'encapsulation du paquet dans MPLS serait un paquet dont la taille excède la MTU du tunnel, alors la valeur que la tête de tunnel DEVRAIT utiliser pour la fragmentation la découverte de la PMTU en dehors du tunnel est la valeur de la MTU de tunnel moins la taille de l'encapsulation MPLS. (C'est-à-dire que la valeur de la MTU de tunnel moins la taille de l'encapsulation MPLS est la MTU qui est à rapporter dans les messages ICMP.) Le paquet devra être éliminé, mais la tête de tunnel devrait envoyer à la source IP du paquet éliminé le message d'erreur ICMP approprié comme spécifié dans la [RFC1191] ou [RFC1981].

5.2 TTL ou limite de bonds

La tête de tunnel PEUT placer le TTL provenant de la pile d'étiquettes MPLS dans le champ TTL de l'en-tête IPv4 encapsulant ou dans le champ Limite de bonds de l'en-tête IPv6 encapsulant. La queue de tunnel PEUT placer le TTL provenant de l'en-tête IPv4 encapsulant ou Limite de bonds de l'en-tête IPv6 encapsulant dans le champ TTL de l'en-tête MPLS, mais seulement si cela n'augmente pas la valeur du TTL dans l'en-tête MPLS.

Si de telles modifications sont faites, et les détails de la façon de le faire va dépendre de la configuration de la queue et de la tête du tunnel.

5.3 Services différenciés

Les procédures spécifiées dans le présent document permettent qu'un LSP soit envoyé à travers un tunnel IP ou GRE. La [RFC2983] détaille un certain nombre de considérations et procédures qui doivent être appliquées pour prendre correctement en charge l'architecture de services différenciés en présence de tunnels IP-dans-IP. Ces considérations et procédures s'appliquent aussi en présence de tunnels MPLS-dans-IP ou MPLS-dans-GRE.

En conséquence, quand une tête de tunnel est sur le point d'envoyer un paquet MPLS dans un tunnel MPLS-dans-IP ou MPLS-dans-GRE, le réglage du champ DS de l'en-tête IPv4 ou IPv6 encapsulant PEUT être déterminé (au moins partiellement) par le "comportement agrégé" du paquet MPLS. Les procédures pour déterminer le comportement agrégé d'un paquet MPLS sont spécifiées dans la [RFC3270].

De même, à la queue de tunnel, le champ DS de l'en-tête IPv4 ou IPv6 encapsulant PEUT être utilisé pour déterminer le comportement agrégé du paquet MPLS encapsulé. La [RFC3270] spécifie une relation entre le comportement agrégé et la disposition suivante du paquet.

6. Applicabilité

Toutes choses égales par ailleurs, l'encapsulation MPLS-dans-IP est la plus efficace, et elle sera généralement considérée comme préférable. Il y a cependant des situations dans lesquelles l'encapsulation MPLS-dans-GRE peut être utilisée :

- Deux routeurs sont "adjacents" sur un tunnel GRE qui existe pour des raisons qui sortent du domaine d'application du présent document, et ces deux routeurs doivent envoyer des paquets MPLS sur cette adjacence. Comme tous les paquets envoyés sur cette adjacence doivent avoir une encapsulation GRE, l'encapsulation MPLS-dans-GRE est plus efficace que l'autre solution, qui serait une encapsulation MPLS-dans-IP qui serait ensuite encapsulée dans GRE.

- Des considérations de mise en œuvre peuvent imposer l'utilisation de MPLS-dans-GRE. Par exemple, un appareil pourrait n'être capable que de traiter des encapsulations GRE dans son chemin.

7. Considérations relatives à l'IANA

L'IANA a alloué le numéro de protocole IP 137 pour l'encapsulation MPLS-dans-IP, comme décrit à la Section 3. Aucune autre action de l'IANA n'est exigée. L'encapsulation MPLS-dans-GRE n'exige aucune action de la part de l'IANA.

8. Considérations sur la sécurité

Le principal problème de sécurité qui se présente quand des tunnels IP ou GRE sont utilisés est la possibilité que le point d'extrémité de réception du tunnel reçoive un paquet qui paraît provenir du tunnel, mais n'a en fait pas été mis dans le tunnel par le point d'extrémité d'émission du tunnel. (Les encapsulations spécifiées ne permettent pas par elles-mêmes au désencapsuleur d'authentifier l'encapsuleur.) Un second problème est la possibilité que le paquet soit altéré entre le moment où il entre dans le tunnel et celui où il le quitte. (Les encapsulations spécifiées n'assurent pas par elles mêmes le désencapsuleur de l'intégrité du paquet.) Un troisième problème est la possibilité que le contenu du paquet soit vu alors que le paquet est en transit dans le tunnel. (La spécification des encapsulations n'assure pas la confidentialité.) La signification de ces problèmes en pratique dépend des exigences de sécurité des applications dont le trafic est envoyé à travers le tunnel. Par exemple, l'absence de confidentialité pour les paquets tunnelés n'est pas un problème significatif si les applications qui génèrent les paquets n'exigent pas la confidentialité.

À cause des exigences de sécurité potentiellement différentes, des scénarios de déploiement, et des considérations de performances des différentes applications qui utilisent le mécanisme d'encapsulation décrit, la présente spécification définit la prise en charge de IPsec comme FACULTATIVE. Les exigences de base de mise en œuvre si IPsec est utilisé sont décrites au paragraphe 8.1. Si IPsec n'est pas mis en œuvre, des mécanismes supplémentaires peuvent devoir être utilisés et déployés. Ils sont discutés au paragraphe 8.2.

8.1 Sécuriser le tunnel avec IPsec

Tous ces problèmes de sécurité peuvent être évités si les tunnels MPLS-dans-IP ou MPLS-dans-GRE sont sécurisés avec IPsec. Les exigences de mise en œuvre définies dans cette section s'appliquent si IPsec est mis en œuvre.

Quand IPsec est utilisé, la tête de tunnel et la queue de tunnel devraient être traitées comme les points d'extrémité d'une association de sécurité. À cette fin, une seule adresse IP de la tête de tunnel va être utilisée comme adresse IP de source, et une seule adresse IP de la queue de tunnel va être utilisée comme adresse de destination IP. Les moyens par lesquels chaque nœud connaît la bonne adresse de l'autre sort du domaine d'application de ce document. Si un protocole de contrôle est utilisé pour établir les tunnels (par exemple, pour informer un point d'extrémité de tunnel de l'adresse IP de l'autre) le protocole de contrôle DOIT avoir un mécanisme d'authentification, et celui-ci 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 MD5 de BGP est satisfaisant.

Les paquets encapsulés dans MPLS-dans-IP ou MPLS-dans-GRE devraient être vus comme générés à la tête du tunnel et comme étant destinés à la queue du tunnel ; le mode transport IPsec DEVRAIT donc être utilisé.

L'en-tête IP du paquet MPLS-dans-IP devient l'en-tête IP externe du paquet résultant quand la tête de tunnel utilise le mode de transport IPsec pour sécuriser le paquet MPLS-dans-IP. Ceci est suivi par un en-tête IPsec, suivi par la pile d'étiquettes MPLS. L'en-tête IPsec doit régler le type de charge utile à MPLS en utilisant le numéro de protocole IP spécifié à la Section 3. Si le mode transport IPsec est appliqué sur un paquet MPLS-dans-GRE, l'en-tête GRE suit l'en-tête IPsec.

À la queue du tunnel, le processus de sortie d'IPsec récupère le paquet contenu dans MPLS-dans-IP/GRE. La queue de tunnel supprime alors l'en-tête IP/GRE encapsulant pour récupérer le paquet MPLS, qui est alors transmis en accord avec sa pile d'étiquettes.

Noter que la queue et la tête de tunnel sont des adjacences de LSP, ce qui signifie que l'étiquette sommitale de tout paquet envoyé à travers le tunnel doit être une de celles distribuées par la queue du tunnel à la tête du tunnel. La queue de tunnel DOIT connaître précisément quelles étiquettes elle a distribué aux têtes de tunnel des tunnels sécurisés par IPsec. Les étiquettes de cet ensemble NE DOIVENT PAS être distribuées par la queue de tunnel à des adjacences de LSP autres que celle qui sont des têtes de tunnels sécurisés par IPsec. Si un paquet MPLS est reçu sans encapsulation IPsec, et si son étiquette sommtale est dans cet ensemble, le paquet DOIT alors être éliminé.

Un tunnel MPLS-dans-IP ou MPLS-dans-GRE sécurisé par IPsec DOIT fournir l'authentification et la protection d'ntégrité. (Noter que l'authentification et l'intégrité s'appliquent au paquet MPLS entier, incluant la pile d'étiquettes MPLS.) Donc, la mise en œuvre DOIT prendre en charge ESP avec le 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 SA est celui attendu.

La distribution de clés peut être faite manuellement ou automatiquement au moyen de IKE [RFC2409]. Le chiffrement manuel DOIT être accepté. Si un chiffrement automatique est mis en œuvre, IKE en mode principal avec des clés prépartagées DOIT être pris en charge. Une application particulière peut augmenter cette exigence et demander la mise en œuvre du chiffrement automatique.

La distribution de clés manuelle est beaucoup plus simple, mais aussi moins adaptable, que la distribution de clés automatique. Donc, quelle méthode de distribution de clés est appropriée pour un tunnel particulier doit être considéré avec soin par l'administrateur (ou la paire d'administrateurs) responsable des points d'extrémité de tunnel. Si la protection contre la répétition est considérée comme nécessaire pour un tunnel, la distribution automatique de clés devrait être configurée.

Si l'encapsulation MPLS-dans-IP est utilisée, les sélecteurs associés à la SA vont être les adresses de source et de destination mentionnées ci-dessus, plus le numéro de protocole IP spécifié à la Section 3. Si on désire sécuriser plusieurs tunnels MPLS-dans-IP entre une certaine paire de nœuds séparément, chaque tunnel doit avoir une paire unique d'adresses IP.

Si l'encapsulation MPLS-dans-GRE est utilisée, les sélecteurs associés à la SA vont être les adresses de source et de destination mentionnées ci-dessus, et le numéro de protocole IP représentant GRE (47). Si on désire sécuriser plusieurs tunnels MPLS-dans-GRE entre une certaine paire de nœuds séparément, chaque tunnel doit avoir une paire unique d'adresses IP.

8.2 En l'absence de IPsec

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

Cependant, quand la tête de tunnel et la queue de 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 d'adresse de source (mais pas le filtrage d'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 d'un MPLS-dans-IP ou MPLS-dans-GRE valide l'adresse IP de source du paquet. Le présent document n'exige pas que le désencapsuleur valide l'adresse IP de source des paquets tunnelés, mais il devrait être compris que manquer à le faire présuppose qu'il y a un filtrage effectif fondé sur la destination (ou une combinaison de filtrage fondé sur la source et de filtrage fondé sur la destination) aux frontières.

9. Remerciements

La présente spécification combine des travaux antérieurs sur l'encapsulation de MPLS dans IP, par Tom Worster, Paul Doolan, Yasuhiro Katsube, Tom K. Johnson, Andrew G. Malis, et Rick Wilder, et des travaux antérieurs sur l'encapsulation de MPLS dans GRE, par Yakov Rekhter, Daniel Tappan, et Eric Rosen. Les auteurs actuels remercient tous ces auteurs de

leur contribution.

De nombreuses personnes ont fait de précieux commentaires et corrections, incluant Rahul Aggarwal, Scott Bradner, Alex Conta, Mark Duffy, Francois Le Faucheur, Allison Mankin, Thomas Narten, Pekka Savola, et Alex Zinin.

10. Références normatives

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. *(MàJ par la* RFC6633)

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", novembre 1990.

[RFC1981] J. McCann, S. Deering, J. Mogul, "Découverte de la MTU de chemin pour IP version 6", août 1996. *(D.S. ; Remplacé par* [RFC8201], STD87)

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

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

[RFC2473] A. Conta, S. Deering, "Spécification du tunnelage générique de paquet dans IPv6", décembre 1998. *(P.S.)*

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", mars 2000.

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

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

11. Références pour information

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Ob., voir* RFC4303)

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

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss, "Architecture pour services différenciés", décembre 1998. *(MàJ par* RFC3260)

[RFC2890] G. Dommety, "Extensions de clé et de numéro de séquence à GRE", septembre 2000. *(P.S.)*

[RFC2983] D. Black, "Services différenciés et tunnels", octobre 2000. *(Information)*

[RFC3260] D. Grossman, "Nouvelle terminologie et précisions pour Diffserv", avril 2002. *(Information)*

[RFC3270] F. Le Faucheur et autres, "Prise en charge des services différenciés par la commutation d'étiquettes multi-protocoles (MPLS)", mai 2002. *(P.S.)*

Adresse des auteurs

Tom Worster
Motorola, Inc.
120 Turnpike Road
Southborough, MA 01772
USA
mél ; tom.worster@motorola.com

Eric Rosen
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
mél : erosen@cisco.com

Yakov Rekhter
Juniper Networks, Inc.
1194 N. Mathilda Ave
Sunnyvale, CA 94089
USA
mél : yakov@juniper.net

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.