

Groupe de travail Réseau  
**Request for Comments : 3828**  
 Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

L-A. Larzon, Lulea University of Technology  
 M. Degermark & S. Pink, University of Arizona  
 L-E. Jonsson, Ericsson  
 G. Fairhurst, University of Aberdeen  
 juillet 2004

## Protocole léger de datagramme d'utilisateur (UDP-Lite)

### 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 (2004). Tous droits réservés

### Résumé

Le présent document décrit le protocole léger de datagramme d'utilisateur (UDP-Lite, *Lightweight User Datagram Protocol*) qui est similaire au protocole de datagramme d'utilisateur (UDP, *User Datagram Protocol*) [RFC0768], mais peut aussi servir les applications dans des environnements réseau enclins à l'erreur qui préfèrent se voir livrer des charges utiles partiellement endommagées plutôt que de les éliminer. Si ce dispositif n'est pas utilisé, UDP-Lite est sémantiquement identique à UDP.

### Table des Matières

1. Introduction.....	1
2. Terminologie.....	2
3. Description du protocole.....	2
3.1 Champs.....	3
3.2 Pseudo en-tête.....	3
3.3 Interface d'application.....	3
3.4 Interface IP.....	3
3.5 Jumbogrammes.....	4
4. Considérations sur les couches inférieures.....	4
5. Compatibilité avec UDP.....	4
6. Considérations sur la sécurité.....	5
7. Considérations relatives à l'IANA.....	5
8. Références.....	5
8.1 Références normatives.....	5
8.2 Références pour information.....	5
9. Remerciements.....	6
10. Adresse des auteurs.....	6
11. Déclaration complète de droits de reproduction.....	7

## 1. Introduction

Le présent document décrit un nouveau protocole de transport, UDP-Lite, (aussi appelé UDPLite). Ce nouveau protocole se fonde sur trois observations:

D'abord, il existe une classe d'applications qui préfèrent se voir livrer des données endommagées plutôt qu'éliminées par le réseau. Un certain nombre de codecs pour la voix et la vidéo rentrent dans cette classe (par exemple, le codec vocal AMR [RFC3267], le codec bas débit Internet [RFC3951], et les codecs vidéo résilients à l'erreur H.263+ [H.263], H.264 [H.264], et MPEG-4 [ISO-14496]). Ces codecs peuvent être conçus pour mieux faire face aux erreurs dans la charge utile qu'avec la perte de paquets entiers.

Ensuite, toutes les liaisons qui prennent en charge la transmission IP devraient utiliser une vérification forte d'intégrité de la couche de liaison (par exemple, CRC-32 [RFC-3819]), et ceci DOIT être utilisé par défaut pour le trafic IP. Lorsque la

liaison sous-jacente le prend en charge, certains types de trafic (par exemple, UDP-Lite) peuvent bénéficier d'un comportement de liaison différent qui permet de transmettre les paquets IP partiellement endommagés quand on le demande [RFC3819]. Plusieurs technologies radio (par exemple, [3GPP]) prennent en charge ce comportement de liaison lors d'un fonctionnement à un point où le coût et le délai sont suffisamment faibles. Si des liaisons enclines à l'erreur ont connaissance de la portion sensible à l'erreur d'un paquet, il est aussi possible que la liaison physique fournisse une protection supérieure pour réduire la probabilité de corruption de ces octets sensibles à l'erreur (par exemple, l'utilisation d'une correction d'erreur directe non égale).

Enfin, les couches intermédiaires (c'est-à-dire, IP et les protocoles de couche de transport) ne devraient pas empêcher les applications tolérantes à l'erreur de bien fonctionner en présence de telles liaisons. IP n'est pas un problème à cet égard, car l'en-tête IP n'a pas de somme de contrôle qui couvre la charge utile IP. Le protocole de transport généralement disponible qui convient le mieux pour ces applications est UDP, car il n'a pas de surdébit pour la retransmission de paquets erronés, pour la livraison dans l'ordre, ou la correction d'erreur. Dans IPv4 [RFC0791], la somme de contrôle UDP couvre soit le paquet entier, soit rien du tout. Dans IPv6 [RFC2460], la somme de contrôle UDP est obligatoire et ne doit pas être désactivée. L'en-tête IPv6 n'a pas de somme de contrôle d'en-tête et il était réputé nécessaire de toujours protéger les informations d'adressage IP en rendant la somme de contrôle UDP obligatoire.

Un protocole de transport conforme aux propriétés des couches de liaison et aux applications décrites ci-dessus est nécessaire [LDP99]. Le mécanisme de détection d'erreur de la couche de transport doit être capable de protéger des informations vitales telles que les en-têtes, mais aussi d'ignorer facultativement les erreurs qui sont mieux traitées par l'application. L'ensemble d'octets à vérifier par la somme de contrôle est mieux spécifié par l'application d'envoi.

UDP-Lite fournit une somme de contrôle avec une couverture partielle facultative. Lorsque on utilise cette option, un paquet est divisé en une partie sensible (couverte par la somme de contrôle) et une partie non sensible (non couverte par la somme de contrôle). Des erreurs dans la partie non sensible ne vont pas causer l'élimination du paquet par la couche de transport chez l'hôte d'extrémité receveur. Lorsque la somme de contrôle couvre le paquet entier, ce qui devrait être par défaut, UDP-Lite est sémantiquement identique à UDP.

Comparé à UDP, la somme de contrôle partielle UDP-Lite fournit une souplesse supplémentaire aux applications qui veulent définir la charge utile comme partiellement insensible aux erreurs binaires.

## 2. Terminologie

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. Description du protocole

L'en-tête UDP-Lite est montré à la Figure 1. Son format diffère de celui d'UDP en ce que le champ Longueur a été remplacé par un champ Couverture de somme de contrôle. Cela peut être fait parce que les informations sur la longueur du paquet UDP peuvent être fournies par le module IP de la même manière que pour TCP [RFC0793].

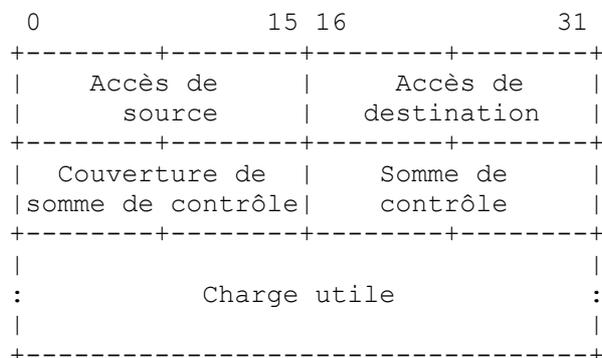


Figure 1 : Format d'en-tête UDP-Lite

### 3.1 Champs

Les champs Accès de source et Accès de destination sont définis comme dans la spécification d'UDP [RFC0768]. UDP-Lite utilise le même ensemble de valeurs de numéro d'accès qu'allouées par l'IANA pour l'usage de UDP.

Couverture de somme de contrôle est le nombre d'octets, en comptant à partir du premier octet de l'en-tête UDP-Lite, qui sont couverts par la somme de contrôle. L'en-tête UDP-Lite DOIT toujours être couvert par la somme de contrôle. En dépit de cette exigence, la couverture de somme de contrôle est exprimée en octets depuis le début de l'en-tête UDP-Lite de la même façon que pour UDP. Une couverture de somme de contrôle de zéro indique que le paquet UDP-Lite entier est couvert par la somme de contrôle. Cela signifie que la valeur du champ Couverture de somme de contrôle DOIT être 0 ou au moins 8. Un paquet UDP-Lite avec une valeur de couverture de somme de contrôle de 1 à 7 DOIT être éliminé par le receveur. Sans considération de la couverture de somme de contrôle, le champ Somme de contrôle calculé DOIT inclure un pseudo en-tête, sur la base de l'en-tête IP (voir ci-dessous). Les paquets UDP-Lite avec une couverture de somme de contrôle supérieure à la longueur IP DOIVENT aussi être éliminés.

Le champ Somme de contrôle est le complément à un sur 16 bits de la somme des compléments à un d'un pseudo en-tête des informations collectées de l'en-tête IP, du nombre d'octets spécifié par la couverture de somme de contrôle (en commençant au premier octet de l'en-tête UDP-Lite) virtuellement bourré avec un octet à zéro à la fin (si nécessaire) pour faire un multiple de deux octets [RFC1071]. Avant le calcul, le champ Somme de contrôle DOIT être réglé à zéro. Si la somme de contrôle calculée est 0, il est transmis comme tout à un (l'équivalent en arithmétique de complément à un).

Comme la somme de contrôle transmise NE DOIT PAS être toute à zéro, une application utilisant UDP-Lite qui souhaite n'avoir aucune protection de la charge utile du paquet devrait utiliser une valeur de couverture de somme de contrôle de 8. Ceci diffère de l'utilisation de UDP sur IPv4 en ce que la somme de contrôle minimale UDP-Lite couvre toujours l'en-tête de protocole UDP-Lite, qui inclut le champ Couverture de somme de contrôle.

### 3.2 Pseudo en-tête

UDP et UDP-Lite utilisent le même pseudo en-tête conceptuellement préfixé provenant de la couche IP pour la somme de contrôle. Ce pseudo en-tête est différent pour IPv4 et IPv6. Le pseudo en-tête de UDP-Lite est différent du pseudo en-tête d'UDP par un aspect : la valeur du champ Longueur du pseudo en-tête n'est pas tirée de l'en-tête UDP-Lite mais plutôt d'informations fournies par le module IP. Ce calcul est fait de la même manière que pour TCP [RFC0793], et implique que le champ Longueur du pseudo en-tête inclut l'en-tête UDP-Lite et tous les octets suivants dans la charge utile IP.

### 3.3 Interface d'application

Une interface d'application devrait permettre les mêmes opérations que pour UDP. En plus de cela, elle devrait donner à l'application envoyeuse le moyen de passer la valeur de la couverture de somme de contrôle au module UDP-Lite. Il devrait aussi y avoir un moyen de passer la valeur de la couverture de somme de contrôle à l'application receveuse, ou au moins permettre à l'application receveuse de bloquer la livraison des paquets dont la valeur de couverture est inférieure à une valeur fournie par l'application.

Il est RECOMMANDÉ que le comportement par défaut de UDP-Lite soit réglé à imiter UDP en faisant que le champ Couverture de somme de contrôle corresponde à la longueur du paquet UDP-Lite et vérifie le paquet entier. Les applications qui souhaitent définir la charge utile comme partiellement insensible aux erreurs binaires (par exemple, un codec tolérant à l'erreur qui utilise RTP [RFC3550]) devraient faire cela par une invocation explicite du système du côté de l'envoyeur. Les applications qui souhaitent recevoir des charges utiles qui ont été seulement partiellement couvertes par une somme de contrôle devraient informer le système receveur par une invocation explicite du système.

Les caractéristiques des liaisons qui forment un chemin Internet peuvent varier considérablement. Il est donc difficile de faire des hypothèses sur les niveaux ou schémas d'erreurs qui peuvent survenir dans la partie insensible à la corruption de la charge utile UDP-Lite. Les applications qui utilisent UDP-Lite ne devraient pas faire d'hypothèses concernant la correction des données reçues au delà de la position indiquée par le champ Couverture de somme de contrôle, et devraient, si nécessaire, introduire leurs propres vérifications de validité appropriées.

### 3.4 Interface IP

Comme pour UDP, le module IP doit fournir le pseudo en-tête au module de protocole UDP-Lite (appelé module UDPLite). Le pseudo en-tête UDP-Lite contient les champs Adresses IP et Protocole de l'en-tête IP, et aussi la longueur de la charge utile IP, qui est déduite du champ Longueur dans l'en-tête IP.

Le module IP envoyeur NE DOIT PAS bourrer la charge utile IP avec des octets supplémentaires, car la longueur de la charge utile UDP-Lite délivrée au receveur dépend de la longueur de la charge utile IP.

### 3.5 Jumbogrammes

Le champ Couverture de la somme de contrôle est de 16 bits et peut représenter jusqu'à une valeur de couverture de somme de contrôle de 65 535 octets. Cela permet une couverture arbitraire de somme de contrôle pour les paquets IP, sauf si ce sont des jumbogrammes. Pour les jumbogrammes, la somme de contrôle peut couvrir soit la charge utile entière (lorsque le champ Couverture de somme de contrôle a la valeur zéro) soit au plus les 65 535 octets initiaux du paquet UDP-Lite.

## 4. Considérations sur les couches inférieures

Comme UDP-Lite peut livrer des paquets avec des charges utiles endommagées à une application qui souhaite les recevoir, les trames qui portent des paquets UDP-Lite n'ont pas besoin d'être éliminées par les protocoles de couche inférieure lorsque il y a des erreurs dans la seule partie insensible. Pour une liaison qui prend en charge la détection d'erreurs partielles, le champ Couverture de somme de contrôle dans l'en-tête UDP-Lite PEUT être utilisé comme indication de si des erreurs ont besoin ou non d'être détectées. Les couches inférieures DOIVENT utiliser un mécanisme de détection d'erreur fort [RFC3819] pour détecter au moins les erreurs qui surviennent dans la partie sensible du paquet, et éliminer les paquets endommagés. La partie sensible consiste en les octets entre le premier octet de l'en-tête IP et le dernier octet identifié par le champ Couverture de somme de contrôle. La partie sensible sera donc traitée exactement de la même façon que pour un paquet UDP.

Les couches de liaison qui ne prennent pas en charge la détection d'erreur partielle convenable pour UDP-Lite, comme décrit ci-dessus, DOIVENT détecter les erreurs dans le paquet UDP-Lite entier et DOIVENT éliminer les paquets endommagés [RFC3819]. Le paquet UDP-Lite entier est donc traité exactement de la même façon qu'un paquet UDP.

On devrait noter que UDP-Lite ne va faire une différence sur une application que si la détection d'erreur partielle, sur la base de la caractéristique de somme de contrôle partielle de UDP-Lite, est aussi mise en œuvre par les couches de liaison, comme exposé ci-dessus. La détection d'erreur partielle à la couche liaison va seulement faire une différence lorsque mise en œuvre sur des liaisons enclines à l'erreur.

## 5. Compatibilité avec UDP

UDP et UDP-Lite ont une syntaxe et une sémantique similaires. Les applications conçues pour UDP peuvent donc utiliser plutôt UDP-Lite, et vont recevoir par défaut la même couverture de paquet complet. Les similarités facilitent aussi la mise en œuvre de UDP-Lite, car seules des modifications mineures sont nécessaires à une mise en œuvre UDP existante.

Il a été alloué à UDP-Lite un identifiant de protocole IP distinct, 136 (UDPLite), permettant donc à un receveur d'identifier si UDP ou UDP-Lite est utilisé. Un hôte d'extrémité de destination qui ignore UDP-Lite va, en général, retourner un message d'erreur ICMP "Protocole injoignable" ou ICMPv6 "Type de charge utile inconnu" (selon le type de protocole IP). Cette méthode simple de détection des systèmes qui ignorent UDP-Lite est le principal avantage d'avoir des identifiants de protocole séparés.

Le reste de cette section donne les raisons de l'allocation d'un identifiant de protocole séparé pour UDP-Lite, plutôt que de partager l'identifiant de protocole IP avec UDP.

Il n'y a pas de problème d'interopérabilité connu entre UDP et UDP-Lite si ils devaient partager l'identifiant de protocole avec UDP. Spécifiquement, il n'y a pas de cas où un paquet potentiellement problématique serait livré à une application qui ne s'y attend pas ; une charge utile UDP-Lite avec une couverture de somme de contrôle partielle ne peut pas être livrée à des applications UDP, et des paquets UDP qui couvrent seulement partiellement la charge utile IP ne peuvent pas être livrés à des applications qui utilisent UDP-Lite.

Cependant, si l'identifiant de protocole devait être partagé entre UDP et UDP-Lite, et si une mise en œuvre UDP-Lite se trouvait à envoyer un paquet UDP-Lite utilisant une somme de contrôle partielle à une mise en œuvre UDP, la mise en œuvre UDP éliminerait en silence le paquet, parce qu'une discordance de pseudo en-tête causerait l'échec de la somme de contrôle UDP. Ni l'application envoyeuse ni la receveuse ne serait notifiée. Des solutions potentielle pourraient être :

- 1) la signalisation explicite dans la bande de l'application (bien que n'utilisant pas l'option de couverture partielle de somme de contrôle) pour permettre à l'envoyeur d'apprendre si le receveur est ou non à capacité UDP-Lite,
- 2) l'utilisation de signalisation hors bande comme H.323, SIP, ou RTCP pour dire si le receveur a la capacité UDP-Lite.

Comme UDP-Lite a reçu son propre identifiant de protocole IP, il n'est pas nécessaire de considérer cette possibilité de livraison d'un paquet UDP-Lite à un accès UDP qui ne s'y attend pas.

## 6. Considérations sur la sécurité

L'impact de UDP-Lite sur la sécurité se rapporte à son interaction avec les mécanismes d'authentification et de chiffrement. Lorsque l'option de somme de contrôle partielle de UDP-Lite est activée, la portion non sensible d'un paquet peut changer dans le transit. Ceci est contraire à l'idée derrière la plupart des mécanismes d'authentification : l'authentification réussit si le paquet n'a pas changé dans le transit. Sauf si des mécanismes d'authentification qui ne fonctionnent que sur la partie sensible des paquets sont développés et utilisés, l'authentification va toujours échouer pour les paquets UDP-Lite lorsque la partie non sensible a été endommagée.

La vérification d'intégrité IPsec (Encapsulation de charge utile de sécurité IP (ESP) [RFC2406], ou l'en-tête d'authentification, AH [RFC2402]) est appliquée (au moins) à la charge utile entière du paquet IP. La corruption de tout bit au sein de la zone protégée va alors résulter en l'élimination du paquet UDP-Lite par le receveur IP.

Lorsque IPsec est utilisé avec le chiffrement de la charge utile ESP, une liaison ne peut pas déterminer le protocole de transport spécifique d'un paquet en cours de transmission en inspectant la charge utile du paquet IP. Dans ce cas, la liaison DOIT fournir une vérification d'intégrité standard couvrant le paquet IP entier et sa charge utile. UDP-Lite n'apporte aucun avantage dans ce cas.

Le chiffrement (par exemple, au niveau transport ou application) peut être utilisé. Si quelques bits d'un paquet chiffré sont endommagés, la transformation de déchiffrement va normalement étendre les erreurs de sorte que le paquet devient trop endommagé pour être utilisable. De nombreuses transformations de chiffrement affichent aujourd'hui ce comportement. Il existe des transformations de chiffrement, et des chiffrements de flux, qui ne causent pas de propagation d'erreurs. Noter qu'omettre une vérification d'intégrité peut, dans certaines circonstances, compromettre la confidentialité [Bellovin98]. L'utilisation appropriée des chiffrements de flux pose ses propres défis [BB01]. En particulier, un attaquant peut causer des changements prévisibles au texte source ultime, même sans être capable de déchiffrer le texte chiffré.

## 7. Considérations relatives à l'IANA

Un nouveau numéro de protocole IP, 136, a été alloué pour UDP-Lite. Le nom associé à ce numéro de protocole est "UDPLite". Cela assure la compatibilité à travers une large gamme de plateformes, car sur certaines plateformes, le caractère "-" ne peut pas faire partie d'un nom d'entité de protocole.

## 8. Références

### 8.1 Références normatives

[RFC0768] J. Postel, "Protocole de [datagramme d'utilisateur](#) (UDP)", (STD 6), 28 août 1980.

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

[RFC0793] J. Postel (éd.), "Protocole de [commande de transmission](#) – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

[RFC1071] R. Braden, D. Borman et C. Partridge, "Calcul de la [somme de contrôle Internet](#)", septembre 1988.

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

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

### 8.2 Références pour information

[3GPP] TS 23.107 V5.9.0, "Technical Specification Group Services et System Aspects; Quality of Service (QoS)

concept et architecture", Specification technique 3GPP, juin 2003.

- [Bellovin98] Bellovin, S.M., "Cryptography et the Internet", dans Proceedings of CRYPTO '98, août 1988.
- [BB01] Bellovin, S. et M. Blaze, "Cryptographic Modes of Operation for the Internet", Second NIST Workshop on Modes of Operation, août 2001.
- [ISO-14496] Norme internationale ISO/CEI 1446 (MPEG-4), "Technologies de l'information, codage des objets audiovisuels", janvier 2000.
- [H.263] Recommandation UIT-T H.263, "Codage vidéo pour communication à faible débit binaire," janvier 1998.
- [H.264] Recommandation UIT-T H.264, "Draft ITU-T Recommendation et Final Draft International Standard of Joint Video Specification", mai 2003.
- [LDP99] Larzon, L-A., Degermark, M. et S. Pink, "UDP Lite for Real-Time Multimedia Applications", Proceedings of the IEEE International Conference of Communications (ICC), 1999.
- [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. (*Obsolète, voir RFC4303*)
- [RFC3267] J. Sjöberg et autres, "Format de charge utile et format de mémorisation de fichier pour les codecs audio AMR et AMR-WB dans RTP", juin 2002. (*Obsolète, voir RFC4867*) (P.S.)
- [RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "[RTP : un protocole de transport pour les applications en temps réel](#)", STD 64, juillet 2003. (*MàJ par RFC7164, RFC7160*)
- [RFC3819] P. Karn et autres, "Conseils aux concepteurs de sous-réseaux Internet", juillet 2004. ([BCP0089](#))
- [RFC3951] S. Andersen et autres, "Codec Internet à faible débit binaire (iLBC)", décembre 2004. (*Expérimentale*)
- [RFC3984] S. Wenger et autres, "Format de charge utile RTP pour vidéo H.264", février 2005. (*P.S., Obsolète, voir RFC6184*)

## 9. Remerciements

Merci à Ghyslain Pelletier de ses commentaires techniques et rédactionnels significatifs. Merci aussi à Steven Bellovin, Elisabetta Carrara, et Mats Naslund de leur révision du chapitre des considérations sur la sécurité, et à Peter Eriksson de sa revue du langage, qui a bien amélioré la clarté du présent document.

## 10. Adresse des auteurs

Lars-Ake Larzon  
Department of CS & EE  
Lulea University of Technology  
S-971 87 Lulea, Sweden  
mél : [ln@csee.ltu.se](mailto:ln@csee.ltu.se)

Mikael Degermark  
Department of Computer Science  
The University of Arizona  
P.O. Box 210077  
Tucson, AZ 85721-0077, USA  
mél : [micke@cs.arizona.edu](mailto:micke@cs.arizona.edu)

Stephen Pink  
The University of Arizona  
P.O. Box 210077  
Tucson, AZ 85721-0077, USA  
mél : [steve@cs.arizona.edu](mailto:steve@cs.arizona.edu)

Lars-Erik Jonsson  
Ericsson AB  
Box 920  
S-971 28 Lulea, Sweden  
mél : [lars-erik.jonsson@ericsson.com](mailto:lars-erik.jonsson@ericsson.com)

Godred Fairhurst  
Department of Engineering  
University of Aberdeen  
Aberdeen, AB24 3UE, UK  
mél : [gorry@erg.abdn.ac.uk](mailto:gorry@erg.abdn.ac.uk)

## 11. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à [www.rfc-editor.org](http://www.rfc-editor.org), et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis 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.

### 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](mailto:ietf-ipr@ietf.org).

### Remerciement

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