

Groupe de travail Réseau
Request for Comments : 5291
 Catégorie : Sur la voie de la normalisation
 Traduction Claude Brière de L'Isle

E. Chen, Cisco Systems
 Y. Rekhter, Juniper Networks
 août 2008

Capacité de filtrage de chemin sortant pour BGP-4

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document définit un mécanisme fondé sur BGP qui permet à un locuteur BGP d'envoyer à son homologue BGP un ensemble de filtres de chemins sortants (ORF, *Outbound Route Filter*) que l'homologue va utiliser pour contraindre/filtrer ses mises à jour d'acheminement sortant au locuteur.

Table des matières

1. Introduction.....	1
2. Spécification des exigences.....	1
3. Filtre de chemin sortant.....	2
4. Portage des entrées d'ORF dans BGP.....	2
5. Capacité de filtrage de chemin sortant.....	4
6. Fonctionnement.....	4
7. Considérations relatives à l'IANA.....	6
8. Considérations de gestion.....	6
9. Considérations sur la sécurité.....	6
10. Remerciements.....	6
11. Références normatives.....	6
Adresse des auteurs.....	7
Déclaration complète de droits de reproduction.....	7

1. Introduction

Actuellement, il n'est pas infrequent qu'un locuteur BGP [RFC4271] reçoive, et ensuite filtre des chemins non voulus de ses homologues sur la base de sa politique locale d'acheminement. Comme la génération et la transmission des mises à jour d'acheminement par l'envoyeur, ainsi que le traitement des mises à jour d'acheminement par le receveur consomment des ressources, il peut être avantageux que la génération de telles mises à jour d'acheminements non voulus puisse être évitée d'abord.

Le présent document définit un mécanisme fondé sur BGP qui permet à un locuteur BGP d'envoyer à son homologue BGP un ensemble de filtres de chemins sortants (ORF, *Outbound Route Filter*). L'homologue va alors appliquer ces filtres, en plus de ses filtres de sortie configurés en local (si il en est) pour contraindre/filtrer ses mises à jour d'acheminement sortant vers le locuteur.

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. Filtre de chemin sortant

Le présent document utilise les termes "identifiant de famille d'adresses" (AFI, *Address Family Identifier*) et "identifiant de famille d'adresses suivante" (SAFI, *Subsequent Address Family Identifier*). Dans le contexte de ce document, la signification de ces termes est la même que dans la [RFC4760].

Conceptuellement, une entrée d'ORF est un quintuplet de la forme <AFI/SAFI, Type d'ORF, Action, Correspondance, Valeur d'ORF> ; un ORF consiste en une ou plusieurs entrées d'ORF qui ont un AFI/SAFI et type d'ORF communs. Un ORF est identifié par <AFI/SAFI, Type d'ORF>.

Le composant "AFI/SAFI" fournit un contrôle de granularité grossière en limitant l'ORF aux seuls chemins dont les informations d'accessibilité de couche réseau (NLRI, *Network Layer Reachability Information*) correspondent au composant "AFI/SAFI" de l'ORF.

Le composant "Type d'ORF" détermine le contenu de la valeur d'ORF.

Le composant "Action" contrôle le traitement de la demande d'ORF par l'homologue distant. L'action peut être une de ADD, REMOVE, REMOVE-ALL. ADD ajoute une entrée d'ORF à l'ORF chez l'homologue distant ; REMOVE supprime une entrée d'ORF précédemment installée chez l'homologue distant ; REMOVE-ALL supprime toutes les entrées précédemment installées de l'ORF spécifié chez l'homologue distant.

Le composant "Correspondance" est utilisé pour prendre en charge la granularité de la correspondance par entrée d'ORF. Il peut être PERMIS ou REFUSÉ. La sémantique de PERMIS est de demander à l'homologue de passer les mises à jour pour l'ensemble de chemins qui correspondent à l'entrée d'ORF. La sémantique de REFUSÉ est de demander à l'homologue de ne pas passer les mises à jour pour l'ensemble de chemins qui correspondent à l'entrée d'ORF.

Quand un ORF est défini, une règle de correspondance spécifique de l'ORF DOIT être spécifiée afin qu'il n'y ait pas d'ambiguïté à l'égard de l'entrée d'ORF qui est considérée comme entrée correspondante dans l'ORF quand un chemin est passé à travers l'ORF.

4. Portage des entrées d'ORF dans BGP

Les entrées d'ORF sont portées dans le message BGP ROUTE-REFRESH (*rafraîchissement de chemin*) [RFC2918].

Un locuteur BGP peut distinguer un message ROUTE-REFRESH entrant qui porte une ou plusieurs entrées d'ORF provenant d'un message ROUTE-REFRESH complet en utilisant le champ Longueur de message dans l'en-tête de message BGP.

Un seul message ROUTE-REFRESH PEUT porter plusieurs entrées d'ORF dans un ou plusieurs ORF, pour autant que toutes ces entrées partagent le même AFI/SAFI.

Du point de vue du codage, chaque entrée d'ORF consiste en une partie commune et une partie spécifique du type, comme le montrent les Figures 1 et 2.

La partie commune consiste en <AFI/SAFI, Type d'ORF, Action, Correspondance>, et est codée comme suit :

Le composant AFI/SAFI d'une entrée d'ORF est codé dans le champ AFI/SAFI du message ROUTE-REFRESH.

À la suite du composant AFI/SAFI est le champ d'un octet Quand-rafraîchir. La valeur de ce champ peut être IMMÉDIAT (0x01) ou DIFFÉRER (0x02). La sémantique de IMMÉDIAT et DIFFÉRER est discutée dans la Section 6 "Fonctionnement" de ce document.

À la suite du champ Quand-rafraîchir est une collection d'un ou plusieurs ORF, groupés par Type d'ORF.

Le composant Type d'ORF est codé comme un champ d'un octet.

Le composant "Longueur des entrées d'ORF" est un champ de deux octets qui contient la longueur totale (en octets) des entrées d'ORF qui suivent pour le type spécifié d'ORF.

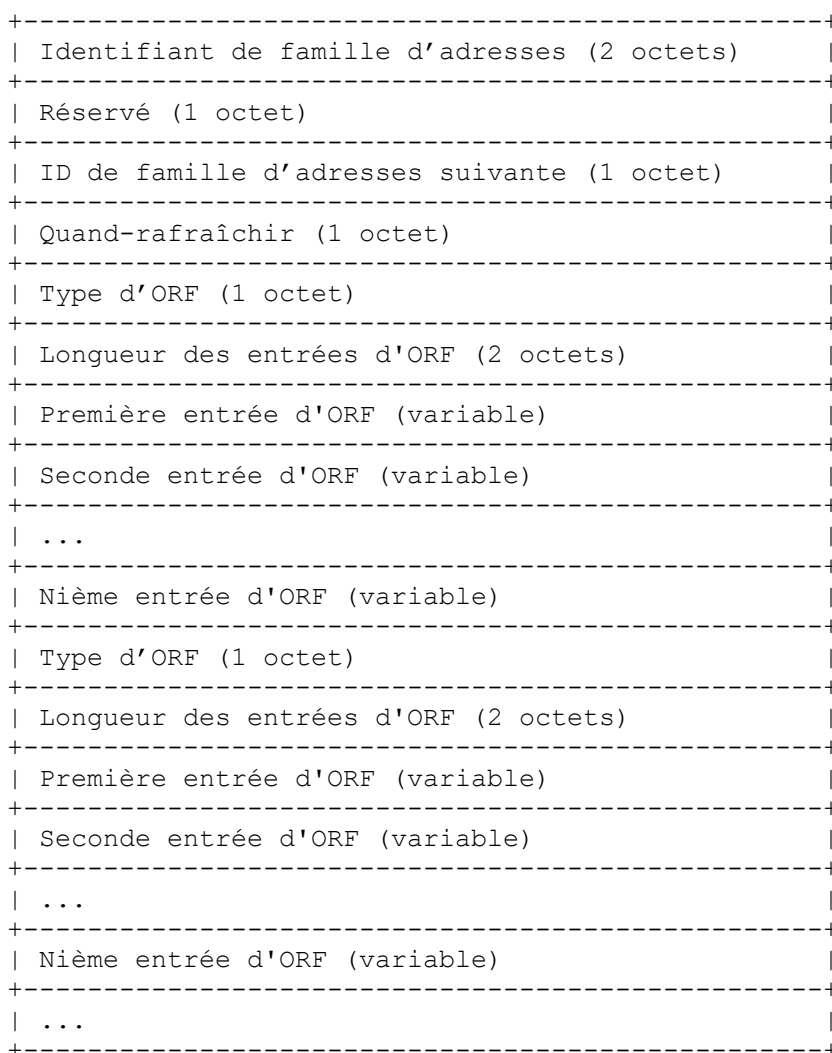


Figure 1 : Portage des entrées d'ORF dans le message ROUTE-REFRESH

Le reste des composants dans la partie commune est codé dans le premier octet de chaque entrée d'ORF (du bit de poids fort au bit de moindre poids) comme montré à la Figure 2 :

- Action est un champ de deux bits. La valeur de ce champ est 0 pour ADD, 1 pour REMOVE, et 2 pour REMOVE-ALL.
- Correspondance est un champ d'un bit. La valeur de ce champ est 0 pour PERMIS et 1 pour REFUSÉ. Ce champ n'est significatif que quand la valeur du champ Action est ADD ou REMOVE.
- Réserve est un champ de 5 bits. Il est réglé à 0 à l'émission et ignoré à réception.

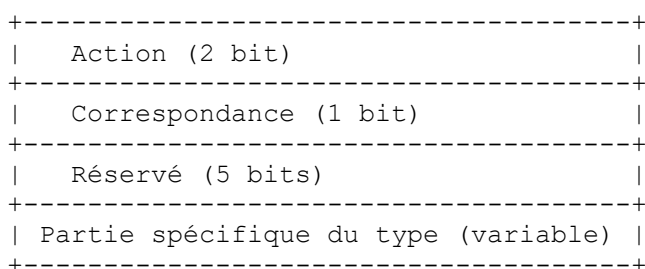


Figure 2 : Codage d'une entrée d'ORF

Quand le composant Action d'une entrée d'ORF spécifie REMOVE-ALL, l'entrée comporte seulement la partie commune.

5. Capacité de filtrage de chemin sortant

Un locuteur BGP qui veut recevoir des entrées d'ORF de son homologue, ou un locuteur BGP qui aimerait envoyer des entrées d'ORF à son homologue, annonce cela à son homologue en utilisant la capacité de filtrage de chemin sortant, comme décrit ci-dessous.

La capacité de filtrage de chemin sortant est une nouvelle capacité BGP [RFC3392] définie comme suit :

Code de capacité : 3

Longueur de capacité : variable

Valeur de capacité : une ou plusieurs des entrées montrées à la Figure 3.

```

+-----+
| Identifiant de famille d'adresses (2 octets) |
+-----+
| Réservé (1 octet) |
+-----+
| ID de famille d'adresses suivante (1 octet) |
+-----+
| Nombre de types d'ORF (1 octet) |
+-----+
| Type d'ORF (1 octet) |
+-----+
| Envoi/Réception (1 octet) |
+-----+
| ... |
+-----+
| Type d'ORF (1 octet) |
+-----+
| Envoi/Réception (1 octet) |
+-----+

```

Figure 3 : Codage de capacité de filtrage de chemin sortant

La signification et l'utilisation de ces champs est la suivante :

Identifiant de famille d'adresses (AFI) : ce champ est le même que celui utilisé dans la [RFC4760].

Identifiant de famille d'adresses suivante (SAFI) : ce champ est le même que celui utilisé dans la [RFC4760].

Nombre de types d'ORF : ce champ contient le nombre de types de filtres énumérés dans les champs suivants.

Type d'ORF : ce champ contient la valeur d'un type d'ORF.

Envoi/Réception : ce champ indique si l'expéditeur (a) veut recevoir des entrées d'ORF de son homologue (valeur 1), (b) voudrait envoyer des entrées d'ORF à son homologue (valeur 2), ou (c) les deux (valeur 3) pour le type d'ORF.

6. Fonctionnement

Un locuteur BGP qui veut recevoir des entrées d'ORF de son homologue, ou voudrait envoyer des entrées d'ORF à son homologue DEVRAIT annoncer la capacité de filtrage de chemin sortant à son homologue en utilisant l'annonce de capacités BGP [RFC3392].

Un locuteur BGP qui met en œuvre la capacité de filtrage de chemin sortant DOIT prendre en charge le message BGP ROUTE-REFRESH, comme défini dans la [RFC2918]. Un locuteur BGP qui annonce la capacité de filtrage de chemin sortant à un homologue en utilisant les annonces de capacité BGP [RFC3392] n'a pas à annoncer la capacité de rafraîchissement de chemin BGP à cet homologue.

Considérons un locuteur BGP qui annonce la capacité de filtrage de chemin sortant indiquant sa volonté de recevoir un ensemble particulier de <AFI/SAFI, Type d'ORF> de son homologue, et qui reçoit la capacité de filtrage de chemin sortant indiquant le désir de l'homologue d'envoyer un ensemble particulier de <AFI/SAFI, Type d'ORF> au locuteur. Si pour un AFI/SAFI donné l'intersection entre ces deux ensembles est non-vide, le locuteur NE DEVRAIT PAS annoncer à l'homologue de chemin avec cet AFI/SAFI avant de recevoir de l'homologue un message ROUTE-REFRESH portant ce AFI/SAFI, où le message pourrait être soit sans aucune entrée d'ORF, soit avec une ou plusieurs entrées d'ORF et le champ Quand-rafraîchir réglé à IMMÉDIAT. Si, par ailleurs, pour un AFI/SAFI donné l'intersection entre ces deux ensembles est vide, le locuteur DOIT suivre les procédures BGP normales.

Un locuteur BGP ne peut envoyer un message ROUTE-REFRESH avec une ou plusieurs entrées d'ORF à son homologue que si l'homologue annonce au locuteur la capacité de filtrage de chemin sortant indiquant sa volonté de recevoir des entrées d'ORF du locuteur, et si le locuteur annonce à l'homologue la capacité de filtrage de chemin sortant indiquant son désir d'envoyer des entrées d'ORF à l'homologue. Le message peut seulement contenir des entrées d'ORF de <AFI/SAFI, Type d'ORF> que l'homologue veut recevoir, comme annoncé au locuteur dans la capacité de filtrage de chemin sortant.

Quand un locuteur BGP reçoit un message ROUTE-REFRESH avec une ou plusieurs entrées d'ORF de son homologue, le locuteur effectue alors les actions suivantes. Si un <AFI/SAFI, Type d'ORF> porté par le message ne correspond pas au <AFI/SAFI, Type d'ORF> que le locuteur veut recevoir de l'homologue (comme annoncé à l'homologue dans la capacité de filtrage de chemin sortant) les entrées d'ORF spécifiées dans le message sont ignorées. Autrement, le locuteur modifie l'ORF spécifié reçu précédemment, conformément aux entrées d'ORF portées dans le message. Si un des champs d'une entrée d'ORF dans le message contient une valeur non reconnue, tout l'ORF spécifié reçu précédemment est supprimé.

Si le composant Action d'une entrée d'ORF est REMOVE, mais si l'ORF reçu précédemment ne contient pas l'entrée spécifiée, l'entrée d'ORF dans le message est ignorée.

Les entrées d'ORF avec REMOVE ou REMOVE-ALL ne peuvent pas supprimer les filtres de chemin sortant configurés localement.

Si le Quand-rafraîchir indique IMMÉDIAT, alors après avoir traité toutes les entrées d'ORF portées dans le message, le locuteur ré-annonce à son homologue les chemins à partir du Adj-RIB-Out associé à l'homologue qui ont le même AFI/SAFI que celui qui est porté dans le message, et en tenant compte de toutes les entrées d'ORF pour ce AFI/SAFI reçu de l'homologue. Le locuteur DOIT ré-annoncer tous les chemins qui ont été affectés par les entrées d'ORF portées dans le message, mais PEUT aussi ré-annoncer les chemins qui n'ont pas été affectés par les entrées d'ORF portées dans le message.

Si le Quand-rafraîchir indique DIFFÉRER, alors après le traitement de toutes les entrées d'ORF portées dans le message, le locuteur diffère de ré-annoncer à l'homologue les chemins provenant du Adj-RIB-Out associé à l'homologue qui ont le même AFI/SAFI que celui porté dans le message, et en tenant compte de toutes les entrées d'ORF reçues de l'homologue jusqu'à ce que le locuteur reçoive un message ROUTE-REFRESH suivant pour le même AFI/SAFI sans aucune entrée d'ORF, ou avec une ou plusieurs entrées d'ORF et Quand-rafraîchir réglé à IMMÉDIAT.

Si le locuteur reçoit de l'homologue un message ROUTE-REFRESH sans aucune entrée d'ORF, alors le locuteur envoie à l'homologue tous les chemins provenant du Adj-RIB-Out associé à l'homologue dont le AFI/SAFI est le même que celui qui est porté dans le message et en tenant compte du ou des ORF (si il en est) précédemment reçus de l'homologue.

L'ensemble d'entrées d'ORF que le locuteur envoie à l'homologue exprime la préférence locale du locuteur, que l'homologue peut ou non décider d'honorer.

Durant une seule session BGP, le locuteur PEUT passer plusieurs entrées d'ORF à l'homologue.

Après qu'un locuteur BGP a fait des changements aux entrées d'ORF précédemment envoyées à un homologue, le locuteur DOIT envoyer à l'homologue les entrées d'ORF mises à jour avec soit (a) Quand-rafraîchir réglé à IMMÉDIAT, soit (b) Quand-rafraîchir réglé à DIFFÉRER suivi par un message ROUTE-REFRESH complet. Ce dernier DOIT être utilisé par le locuteur quand il y a d'autres changements de politique (en plus des entrées d'ORF) qui exigent que l'homologue réannonce tous les chemins.

La durée de vie d'un ORF est celle de la session BGP durant laquelle l'ORF est échangé.

Un ORF est supprimé quand la dernière entrée d'ORF est supprimée (soit via REMOVE-ALL, soit via une séquence de REMOVE).

Si un chemin particulier maintenu par un locuteur BGP ne correspond pas à une des entrées d'ORF d'un ORF (non vide) associé à un homologue particulier, ce chemin NE DEVRAIT PAS être annoncé à l'homologue.

Si un locuteur BGP maintient plusieurs ORF de différents types d'ORF pour un homologue particulier, alors la décision par le locuteur d'annoncer un chemin à l'homologue est déterminée par le passage du chemin à travers chacun de ces ORF, et en combinant les résultats (combinaison des résultats de PERMIS et REFUSÉ dans un REFUSÉ).

7. Considérations relatives à l'IANA

Le présent document définit une nouvelle capacité BGP – Capacité de filtrage de chemin sortant. Le code de capacité pour la capacité de filtrage de chemin sortant est 3.

Comme spécifié dans le présent document, une entrée d'ORF contient le champ Type d'ORF pour lequel l'IANA a créé et tient maintenant un registre intitulé "Types de filtrage de chemin sortant (ORF) BGP".

L'IANA maintient et enregistre les valeurs pour le champ Type d'ORF comme suit :

- La valeur de type d'ORF de 0 est réservée.
- Les valeurs de type d'ORF de 1 à 63 seront allouées par l'IANA en utilisant soit le processus Action de normalisation défini dans la [RFC5226], soit le processus d'allocation précoce de l'IANA défini dans la [RFC4020].
- Les valeurs de type d'ORF de 64 à 127 seront allouées par l'IANA, selon la politique de "premier arrivé, premier servi" définie dans la [RFC5226].
- Les valeurs de type d'ORF de 128 à 255 sont spécifiques du fabricant, et ne seront pas allouées par l'IANA.

8. Considérations de gestion

Les objets de gestion pour les ORF BGP seront définis séparément, en dehors du présent document. Cependant, il est suggéré que les objets de gestion suivants soient définis :

L'objet Capacité ORF, qui décrit la capacité ORF échangée sur une session BGP, devrait inclure les types ORF et les valeurs Envoi/Réception annoncées et reçues pour un homologue BGP.

L'objet Entrée d'ORF devrait contenir les entrées d'ORF de chaque ORF envoyé et reçu pour un homologue BGP.

9. Considérations sur la sécurité

Cette extension à BGP ne change pas les questions de sécurité sous-jacentes de la [RFC4271].

10. Remerciements

Une partie des matériaux de ce document est adaptée d'une proposition de mises à jour sélectives par Yakov Rekhter, Kannan Varadhan, et Curtis Villamizar.

11. 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](#))

- [RFC2918] E. Chen, "[Capacité de rafraîchissement de chemin](#) pour BGP-4", septembre 2000. (*P.S.*, *MàJ par RFC7313*)
- [RFC3392] R. Chandra et J. Scudder, "Annonces de capacités avec BGP-4", novembre 2002. (*Obsolète, voir RFC5492*)
- [RFC4020] K. Kompella et A. Zinin, "Allocation précoce par l'IANA de codets pour des RFC en cours de normalisation", [BCP 100](#), février 2005. (*Remplacée par RFC7120*)
- [RFC4271] Y. Rekhter, T. Li et S. Hares, "[Protocole de routeur frontière](#) version 4 (BGP-4)", janvier 2006. (*D.S.*) (*MàJ par RFC6608, RFC8212, RFC9072*)
- [RFC4760] T. Bates, R. Chandra, D. Katz et Y. Rekhter, "[Extensions multi protocoles pour BGP-4](#)", janvier 2007.
- [RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace RFC2434 ; remplacée par RFC8126*)

Adresse des auteurs

Enke Chen
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
USA
mél: enkechen@cisco.com

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

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2008)

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, 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, le IETF TRUST 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 encloses ne viole 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.

Remerciement

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