

Groupe de travail Réseau
Request for Comments: 5642
 Catégorie : Sur la voie de la normalisation

S. Venkata, Google Inc.
 S. Harwani, Cisco Systems
 C. Pignataro, Cisco Systems
 D. McPherson, Arbor Networks
 août 2009

Traduction Claude Brière de L'Isle

Mécanisme dynamique d'échange de nom d'hôte pour OSPF

Résumé

Le présent document définit un nouveau TLV Informations de routeur OSPF (RI) qui permet aux routeurs OSPF d'arroser leurs informations de transposition de nom d'hôte en identifiant de routeur à travers un réseau OSPF pour fournir un mécanisme simple et dynamique pour que les routeurs fonctionnant avec OSPF apprennent leurs noms d'hôte symboliques, tout comme pour les routeurs qui fonctionnent avec IS-IS. Ce mécanisme est applicable à OSPFv2 et à OSPFv3.

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.

Notice de droits de reproduction

Copyright (c) 2009 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document.

Le présent document peut contenir des matériaux provenant de documents de l'IETF ou de contributions à l'IETF publiées ou rendues disponibles au public avant le 10 novembre 2008. La ou les personnes qui ont le contrôle des droits de reproduction sur tout ou partie de ces matériaux peuvent n'avoir pas accordé à l'IETF Trust le droit de permettre des modifications de ces matériaux en dehors du processus de normalisation de l'IETF. Sans l'obtention d'une licence adéquate de la part de la ou des personnes qui ont le contrôle des droits de reproduction de ces matériaux, le présent document ne peut pas être modifié en dehors du processus de normalisation de l'IETF, et des travaux dérivés ne peuvent pas être créés en dehors du processus de normalisation de l'IETF, excepté pour le formater en vue de sa publication comme RFC ou pour le traduire dans une autre langue que l'anglais.

Table des matières

1. Introduction.....	1
1.1 Spécification des exigences.....	2
2. Solutions possibles.....	2
3. Mise en œuvre.....	3
3.1 TLV Nom d'hôte dynamique.....	3
4. Considérations d'IPv6.....	4
5. Considérations sur la sécurité.....	4
6. Considérations relatives à l'IANA.....	5
7. Remerciements.....	5
8. Références.....	5
8.1 Références normatives.....	5
8.2 Références pour information.....	5
Adresse des auteurs.....	6

1. Introduction

OSPF utilise un identifiant de routeur de 32 bits pour représenter et identifier de façon univoque un nœud dans le réseau. Pour des raisons de gestion et de fonctionnement, les opérateurs de réseaux ont besoin de vérifier l'état des adjacences

OSPF, les entrées dans le tableau d'acheminement, et le contenu de la base de données d'état de liaison OSPF. Quand on cherche des informations de diagnostic, les représentations numériques des identifiants de routeur (par exemple, des représentations décimales séparées par des points ou hexadécimales) sont moins claires pour les humains que les noms symboliques.

Une façon de surmonter ce problème est de définir un tableau de transposition de nom d'hôte en identifiant de routeur sur un routeur. Cette transposition peut être utilisée bidirectionnellement (par exemple, pour trouver des noms symboliques pour les identifiants de routeur et trouver des identifiants de routeur pour les noms symboliques) ou unidirectionnellement (par exemple, pour trouver des noms d'hôte symboliques pour les identifiants de routeur). Donc, chaque routeur doit tenir un tableau avec les transpositions entre noms de routeur et identifiants de routeur.

Ces tableaux doivent contenir tous les noms et identifiants de routeur de tous les routeurs dans le réseau. Si ces tableaux de transposition sont construits par des définitions statiques, cela peut devenir un processus manuel fastidieux dans les réseaux opérationnels ; modifier ces entrées de transposition statiques quand des ajouts, suppressions, ou changements surviennent devient un processus non adaptable très enclin à l'erreur.

Le présent document analyse les solutions possibles à ce problème (Section 2) et fournit un moyen de remplir les tableaux en définissant un nouveau TLV d'information de routeur OSPF pour OSPF, le TLV Nom d'hôte dynamique (Section 3). Ce mécanisme est applicable à OSPFv2 et OSPFv3.

1.1 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].

2. Solutions possibles

Il y a plusieurs approches pour fournir un service de transposition de nom en identifiant de routeur.

Une façon de construire ce tableau de transpositions est par des définitions statiques. Le problème des définitions statiques est que l'administrateur de réseau doit mettre à jour manuellement les entrées de transposition lorsque le réseau change ; cette approche ne s'adapte pas lorsque le réseau croît, car il doit y avoir une entrée dans le tableau de transposition pour chaque routeur dans le réseau, sur chaque routeur dans le réseau. Donc, cette approche souffre de problèmes de maintenance et d'adaptabilité.

Une autre approche est d'avoir une localisation centralisée où la transposition de nom en identifiant de routeur peut être conservée. Le DNS pourrait être utilisé pour cela. Un inconvénient de cette solution centralisée est que c'est un seul point de défaillance ; et bien qu'une disponibilité améliorée du service de transposition central puisse être conçue, elle peut ne pas être capable de résoudre le nom d'hôte en cas de problèmes d'accessibilité ou dans le réseau, qui peuvent être particulièrement problématiques quand il y a des difficultés de résolution. Aussi, le temps de réponse peut être un problème avec la solution centralisée, qui peut être également problématique. Si le DNS est utilisé comme tableau de transposition centralisée, un opérateur de réseau peut désirer une transposition de nom différente de la transposition existante dans le DNS, ou de nouveaux routeurs peuvent n'être pas encore dans le DNS.

De plus, pour OSPFv3 dans les déploiements natifs IPv6, la valeur de 32 bits de l'identifiant de routeur ne va pas se transposer en les entités adressées en IPv4 dans le réseau, et le DNS ne pourra pas être résolu (Section 4).

La troisième solution que nous avons définie dans le présent document est d'utiliser le protocole lui-même pour porter la transposition de nom en identifiant de routeur dans un TLV. Les routeurs qui comprennent ce TLV peuvent l'utiliser pour créer la transposition symbolique de nom en identifiant de routeur, et les routeurs qui ne le comprennent pas peuvent simplement l'ignorer. La présente spécification fournit ces mécanismes de sémantique et transposition pour OSPFv2 et OSPFv3, en développant l'annonce d'état de liaison (LSA, *Link State Advertisement*) [RFC4970] d'informations de routeur (RI, *Router Information*) OSPF.

Si un routeur annonce une LSA de portée d'AS (autre qu'une LSA RI de TLV Nom d'hôte dynamique) ce routeur DEVRAIT annoncer une LSA RI de TLV Nom d'hôte dynamique dans la portée d'AS. Autrement, il DEVRAIT annoncer une LSA RI de TLV Nom d'hôte dynamique dans la portée de zone. Par exemple, un routeur de bordure d'AS (ASBR, *AS boundary router*) DEVRAIT envoyer un TLV Nom d'hôte dynamique de portée d'AS, tandis qu'un routeur de bordure de zone (ABR, *area boundary router*) et un routeur interne DEVRAIT envoyer un TLV Nom d'hôte dynamique de portée de zone.

La portée d'arrosage est contrôlée par le type de LSA opaque dans OSPFv2 et par les bits S1 et S2 dans OSPFv3. Pour la portée de zone, le TLV Nom d'hôte dynamique DOIT être porté au sein d'une LSA RI OSPFv2 de type 10 ou une LSA RI OSPFv3 avec le bit S1 établi et le bit S2 à zéro. Si la portée d'arrosage est le domaine d'acheminement entier (portée d'AS) le TLV Nom d'hôte dynamique DOIT être porté au sein d'une LSA RI OSPFv2 de type 11 ou une LSA RI OSPFv3 avec le bit S1 à zéro et le bit S2 établi.

3.1.2 Instances OSPF multiples

Quand une LSA d'informations de routeur OSPF incluant le TLV Nom d'hôte dynamique est annoncée dans plusieurs instances OSPF, le nom d'hôte DEVRAIT soit être préservé, soit inclure un élément de base commun. Il peut être utile pour le débogage ou d'autres fins d'allouer des instances séparées de noms d'hôte différents avec un ensemble cohérent de suffixes ou préfixes qui peuvent être associés à une instance spécifique -- en particulier, quand une instance est utilisée pour une famille d'adresses discrète ou des informations non d'acheminement.

4. Considérations d'IPv6

OSPFv2 et OSPFv3 emploient tous deux les identifiants de routeur avec une taille commune de 32 bits. Dans IPv4, les valeurs d'identifiant de routeur étaient normalement déduites automatiquement d'une adresse IPv4 configurée sur une interface de bouclage ou physique définie sur le système local ou explicitement définie au sein de la configuration de processus OSPF. Avec un plus large déploiement de IPv6, il est assez probable que les réseaux OSPF qui vont exister n'auront pas d'interface native d'adressage IPv4. Par suite, un identifiant de routeur OSPF de 32 bits va devoir être spécifié explicitement ou déduit d'une manière automatique qui évite les collisions avec d'autres routeurs OSPF au sein du domaine local d'acheminement.

Parce que cette valeur de 32 bits ne va pas se transposer en entités adressées en IPv4 dans le réseau, ni ne seront résolubles par le DNS, il est considéré qu'il est extrêmement désirable d'un point de vue opérationnel qu'un mécanisme existe pour transposer les identifiants de routeur OSPF en valeurs plus faciles à interpréter -- idéalement, des chaînes lisibles par l'homme. La présente spécification permet une fonction de transposition qui allège la charge opérationnelle qui peut autrement être introduite avec les déploiements natifs de IPv6.

5. Considérations sur la sécurité

Comme la transposition de nom d'hôte en identifiant de routeur s'appuie sur les informations fournies par les routeurs eux-mêmes, un routeur mal configuré ou compromis peut injecter de fausses informations de transposition, incluant un nom d'hôte dupliqué pour des identifiants de routeur différents. Donc, ces informations doivent être traitées avec suspicion quand, par exemple, on fait des diagnostics sur un incident de sécurité suspect.

Il y a une confusion potentielle provenant de collisions de noms si deux routeurs utilisent et annoncent le même nom d'hôte dynamique. Les conflits de noms ne sont pas cruciaux, et donc il n'y a pas de mécanisme générique de détection ou résolution de conflit dans le protocole. Cependant, un routeur qui détecte qu'un nom d'hôte reçu est le même qu'un nom local peut produire une notification ou une alerte de gestion.

L'utilisation d'un FQDN comme nom d'hôte OSPF dynamique expose potentiellement des informations géographiques ou autres informations commerciales qui peuvent être déduites du nom d'hôte quand il est envoyé en clair. OSPFv3 prend en charge la confidentialité via IPsec en mode transport (voir la [RFC4552]). OSPFv2 pourrait fonctionner sur des tunnels IPsec si la confidentialité est exigée.

Le présent document ne soulève pas d'autres nouveaux problèmes de sécurité pour OSPF. Les considérations sur la sécurité pour le protocole OSPF de base sont traitées dans les [RFC2328] et [RFC5340]. L'utilisation de l'authentification pour les protocoles d'acheminement OSPF est encouragée.

6. Considérations relatives à l'IANA

L'IANA tient le registre des "TLV d'informations de routeur OSPF" [IANA-RI]. Un type supplémentaire de TLV Informations de routeur OSPF est défini à la Section 3. Il a été alloué par l'IANA dans la gamme d'allocation d'action de normalisation [RFC4970].

Nom du registre : TLV Informations de routeur OSPF

Type	Capacités	Référence
7	Nom d'hôte dynamique OSPF	RFC 5642

7. Remerciements

Les auteurs de ce document ne prétendent pas à l'originalité des idées décrites. Le présent document adapte le format et le texte de travaux similaires faits dans IS-IS [RFC5301] (qui rend obsolète la [RFC2763]) ; nous tenons à remercier Naiming Shen et Henk Smit, auteurs de la [RFC2763].

Les auteurs remercient aussi Acee Lindem, Abhay Roy, Anton Smirnov, et Dave Ward de leurs précieux commentaires et suggestions.

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. DOI 10.17487/RFC2119, (MàJ par [RFC8174](#))
- [RFC4970] A. Lindem et autres, "Extensions à OSPF pour l'[annonce des capacités facultatives de routeur](#)", DOI 10.17487/RFC4970, juillet 2007. (P.S.)

8.2 Références pour information

- [IANA-RI] Internet Assigned Numbers Authority, "Open Shortest Path First v2 (OSPFv2) Parameters", <<http://www.iana.org>>.
- [RFC1035] P. Mockapetris, "Noms de domaines – [Mise en œuvre](#) et spécification", DOI 10.17487/RFC1035, STD 13, novembre 1987. (MàJ par [RFC1101](#), [1183](#), [1348](#), [1876](#), [1982](#), [1995](#), [1996](#), [2065](#), [2136](#), [2181](#), [2137](#), [2308](#), [2535](#), [2673](#), [2845](#), [3425](#), [3658](#), [4033](#), [4034](#), [4035](#), [4343](#), [5936](#), [5966](#), [6604](#), [7766](#), [8482](#), [8767](#))
- [RFC2181] R. Elz et R. Bush, "[Clarifications pour la spécification du DNS](#)", DOI 10.17487/RFC2181, juillet 1997. (P.S., MàJ par [RFC4035](#), [RFC2535](#), [RFC4343](#), [RFC4033](#), [RFC4034](#), [RFC5452](#), [RFC8767](#))
- [RFC2328] J. Moy, "[OSPF version 2](#)", DOI 10.17487/RFC2328, STD 54, avril 1998. (MàJ par la [RFC6549](#), [RFC8042](#), [RFC9355](#))
- [RFC2763] N. Shen, H. Smit, "Mécanisme d'échange dynamique de nom d'hôte pour IS-IS", février 2000. (*Obs, voir [RFC5301](#)*) (*Info.*)
- [RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les RFC [5890](#) et [5891](#), P.S.*)
- [RFC4552] M. Gupta, N. Melam, "[Authentification/confidentialité](#) pour OSPFv3", DOI 10.17487/RFC4552, juin 2006. (P.S.)

- [RFC5301] D. McPherson, N. Shen, "[Mécanisme d'échange dynamique de nom d'hôte](#) pour IS-IS", DOI 10.17487/RFC5301, octobre 2008. (Remplace [RFC2763](#)) (P.S.)
- [RFC5340] R. Coltun et autres, "[OSPF pour IPv6](#)", DOI 10.17487/RFC5340, juillet 2008. (P.S. ; Remplace [RFC2740](#) ; MàJ par [RFC8362](#))

Adresse des auteurs

Subbaiah Venkata

Google Inc.

mél : svenkata@google.com

URI : <http://www.google.com>

Sanjay Harwani

Cisco Systems

mél : sharwani@cisco.com

URI : <http://www.cisco.com>

Carlos Pignataro

Cisco Systems

mél : cpignata@cisco.com

URI : <http://www.cisco.com>

Danny McPherson

Arbor Networks, Inc.

mél : danny@arbor.net