Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 7526
BCP 196
RFC rendues obsolètes : 3068, 6732
Catégorie : Bonnes pratiques actuelles
ISSN : 2070-1721

O. Troan, Cisco
B. Carpenter, Univ. of Auckland

août 2015
Traduction Claude Brière de L'Isle

Bouclier DHCPv6 : protection contre les serveurs DHCPv6 félons

Résumé
L'expérience du mécanisme de transition 6à4 défini dans la RFC 3056 ("Connexion des domaines IPv6 via des nuages IPv4") a montré que le mécanisme ne convient pas pour les larges déploiements et l'utilisation dans l'Internet en mode d'envoi à la cantonade. Donc, le présent document demande que la RFC 3068 ("Préfixe d'envoi à la cantonade pour les routeurs relais 6à4") et la RFC 6732 ("Tunnels 6 à 4 gérés par le fournisseur") soient rendues obsolètes et passent au statut de Historique. Il recommande que les futurs produits ne devraient pas prendre en charge l'envoi à la cantonade 6à4 et que les déploiements existants soient revus. Il complète les lignes directrices de la RFC 6343.

Table des Matières

1. Introduction

La forme d'origine du mécanisme de transition 6à4 [RFC3056] s'appuie sur l'adressage en envoi individuel. Cependant, il a été montré que son extension spécifiée dans "Préfixe d'envoi à la cantonade pour routeurs de relais 6à4" [RFC3068] pose de

sévères problèmes pratiques lorsque utilisée dans l'Internet. Le présent document demande que les RFC 3068 et 6732 soient passées au statut de Historique, comme défini au paragraphe 4.2.4 de la [RFC2026]. Il complète les lignes directrices de déploiement de la [RFC6343].

6à4 a été conçu pour aider à la transition de l'Internet de IPv4 à IPv6. Il a été un bon mécanisme pour expérimenter IPv6, mais à cause des forts taux d'échec vus avec l'envoi à la cantonade 6à4 [HUSTON], les utilisateurs finaux peuvent finir par désactiver IPv6 sur les hôtes ; il en a résulté que certains fournisseurs de contenu ont été réticents à rendre des contenus disponibles sur IPv6.

La [RFC6343] analyse en détails les problèmes de fonctionnement connus et décrit un ensemble de suggestions pour améliorer la fiabilité de 6à4, étant donnée la large présence des hôtes et équipements dans les locaux des utilisateurs qui le prennent en charge. L'avis de désactiver 6à4 par défaut a été largement adopté dans les systèmes d'exploitation récents, et les modes d'échec ont été généralement cachés aux utilisateurs par de nombreux navigateurs qui ont adopté l'approche "Happy Eyeballs" de la [RFC6555].

Néanmoins, une quantité mesurable de trafic 6à4 est toujours observée par les fournisseurs de contenu IPv6. Les utilisateurs restants qui réussissent l'envoi 6à4 à la cantonade sont probablement sur des hôtes qui utilisent le tableau de politique obsolète de la [RFC3484] (qui préfère 6à4 à IPv4) et fonctionnent sans Happy Eyeballs. De plus, ils doivent avoir un chemin jusqu'à un relais d'envoi à la cantonade opérationnel et ils doivent accéder à un hôte IPv6 qui a un chemin sur un relais de retour opérationnel.

Cependant, l'expérience montre que les échecs de fonctionnement causés par l'envoi 6à4 à la cantonade ont continué en dépit de l'avis de la RFC 6343 qui est disponible.

1.1 Travaux en rapport

La [RFC5969] "Déploiement rapide de IPv6 sur infrastructures IPv4 (6rd) -- Spécification du protocole" s'appuie explicitement sur le mécanisme 6à4, utilisant un préfixe de fournisseur de service au lieu de 2002::/16. Cependant, le modèle de déploiement se fonde sur la prise en charge du fournisseur de service de telle sorte que 6rd évite les problèmes observés avec 6à4 à la cantonade.

Le cadre pour "Tunnels 6 à 4 gérés par le fournisseur" [RFC6732] est destiné à aider un fournisseur de service à gérer les tunnels de 6à4 en envoi à la cantonade. Ce cadre n'existe qu'à cause des problèmes observés avec l'envoi à la cantonade 6à4.

2. Conventions

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].

Dans le présent document, le mot "déconseille" et ses dérivés n'est utilisé que dans son sens générique de "critique ou désapprobation expresse" et n'a aucune signification normative spécifique. Une fonction déconseillée peut exister dans l'Internet pendant de nombreuses années pour permettre la rétro compatibilité.

3. Problèmes de fonctionnement de 6à4

6à4 est un mécanisme conçu pour isoler des îlots IPv6 pour leur permettre de se joindre mutuellement en utilisant le tunnelage automatique IPv6 sur IPv4. Pour atteindre l'Internet IPv6 natif, le mécanisme utilise des routeurs relais dans les deux directions vers l'avant et vers l'arrière. Le mécanisme est pris en charge dans de nombreuses mises en œuvre IPv6. Avec le déploiement accru d'IPv6, le mécanisme s'est révélé présenter un certain nombre d'inconvénients.

Dans la direction vers l'avant, un nœud 6à4 va envoyer du trafic IPv6 encapsulé dans IPv4 à un relais 6à4 qui est connecté aux deux nuages 6à4 et IPv6 natif. Dans la direction inverse, un chemin 2002::/16 est injecté dans le domaine d'acheminement IPv6 natif pour attirer le trafic provenant des nœuds IPv6 natif jusqu'à un routeur relais 6à4. Il est prévu que le trafic utilise des relais différents dans les directions vers l'avant et vers l'arrière.

Un modèle de développement 6à4, décrit au paragraphe 5.2 de la RFC 3056, suggère qu'un routeur 6à4 devrait avoir un ensemble de connexions gérées (via des connexions BGP) à un ensemble de routeurs relais 6à4. Bien que cela rende le chemin vers l'avant plus contrôlé, cela ne garantit pas un chemin inverse fonctionnel. Dans tous les cas, ce modèle a la même charge opérationnelle que les tunnels configurés manuellement et n'a vu aucun développement dans l'Internet public.

La RFC 3068 ajoute une extension qui permet l'utilisation d'une adresse bien connue d'envoi IPv4 à la cantonade pour atteindre le plus proche relais 6à4 vers l'avant. Cependant, ce mécanisme d'envoi à la cantonade pose un certain nombre de problèmes de fonctionnement, qui sont décrits en détail à la Section 3 de la [RFC6343]. Le présent document est destiné à déconseiller le mécanisme d'envoi à la cantonade.

L'utilisation d'homologue à homologue du mécanisme 6à4 existe dans l'Internet, probablement à l'insu de nombreux opérateurs. Cet usage est sans dommage pour les tiers et ne dépend pas du mécanisme d'envoi à la cantonade 6à4 que le présent document déconseille.

4. Désapprobation

Le présent document déconseille formellement le mécanisme de transition 6à4 d'envoi à la cantonade défini dans la [RFC3068] et l'adresse IPv4 d'envoi à la cantonade associée 192.88.99.1. Il n'est plus considéré en dernier ressort comme un service utile.

Le préfixe 192.88.99.0/24 NE DOIT PAS être réalloué pour d'autre usage excepté par une future action de normalisation de l'IETF.

Le mécanisme de base d'envoi à la cantonade 6à4 défini dans la [RFC3056] et le préfixe IPv6 6à4 associé 2002::/16 ne sont pas déconseillés. Les règles de choix d'adresse par défaut spécifiées dans la [RFC6724] ne sont pas modifiées.

En l'absence d'envoi à la cantonade 6à4, la [RFC6732] "Tunnels 6 à 4 gérés par le fournisseur" ne sera plus nécessaire, de sorte qu'elle est aussi déconseillée par ce document.

Les références incidentes à 6à4 devraient être revues et éventuellement retirées des autres documents de l'IETF si et quand ils seront mis à jour. Ces documents incluent les RFC 3162, RFC 3178, RFC 3790, RFC 4191, RFC 4213, RFC 4389, RFC 4779, RFC 4852, RFC 4891, RFC 4903, RFC 5157, RFC 5245, RFC 5375, RFC 5971, RFC 6071, et RFC 6890.

5. Recommandations de mise en œuvre

Il N'EST PAS RECOMMANDÉ d'inclure le mécanisme de transition 6à4 d'envoi à la cantonade dans les nouvelles mises en œuvre. Si il est inclus dans une mise en œuvre, le mécanisme 6à4 d'envoi à la cantonade DOIT être désactivé par défaut.

Dans les mises en œuvre d'hôtes, 6à4 en envoi individuel DOIT aussi être désactivé par défaut. Tous les hôtes qui utilisent 6à4 DOIVENT prendre en charge la politique de choix d'adresse IPv6 décrite dans la [RFC6724].

Dans les mises en œuvre de routeur, 6à4 DOIT être désactivé par défaut. En particulier, permettre la transmission IPv6 sur un appareil NE DOIT PAS activer automatiquement 6à4.

6. Recommandations de fonctionnement

Le présent document n'implique pas une recommandation d'un filtrage généralisé du trafic ou des chemins pour 6à4 ou même 6à4 en envoi à la cantonade. Il recommande simplement qu'il n'y ait pas d'autres déploiements du mécanisme de 6à4 en envoi à la cantonade, des appels pour les déploiements actuels de 6à4 pour évaluer l'efficacité de la poursuite de l'utilisation du mécanisme de 6à4 en envoi à la cantonade, et il fait des recommandations destinées à empêcher toute utilisation de 6à4 d'entraver un plus large déploiement et utilisation de IPv6 natif sur l'Internet global.

Les réseaux NE DEVRAIENT PAS exclure les paquets dont l'adresse de source est 192.88.99.1, parce que c'est le trafic 6à4 normal d'un relais de retour 6to4 quelque part sur l'Internet. Cela inclut de s'assurer que le trafic provenant d'un relais de retour local 6à4 avec une adresse de source de 192.88.99.1 est permis à travers les filtres anti usurpation d'identité (comme ceux décrits dans la [RFC2827] et la [RFC3704]) ou par les vérifications de transmission en envoi individuel sur le chemin inverse (uRPF) de la [RFC5635].

Les lignes directrices de la Section 4 de la [RFC6343] restent valides pour ceux qui choisissent de continuer à faire de l'envoi à la cantonade 6à4 en dépit de cette désapprobation.

Les opérateurs actuels de relais d'envoi à la cantonade 6à4 avec l'adresse IPv4 192.88.99.1 DEVRAIENT revoir les

informations de la [RFC6343] et le présent document, et examiner ensuite attentivement si le relais d'envoi à la cantonade 6à4 pourra être arrêté lorsque le trafic diminuera. Les fournisseurs de service Internet qui ne gèrent pas de relais d'envoi à la cantonade mais fournissent à leurs clients un chemin pour 192.88.99.1 DEVRAIENT vérifier que cela ne conduit pas en fait à un relais opérationnel d'envoi à la cantonade, comme expliqué au paragraphe 4.2.1 de la [RFC6343]. De plus, les fournisseurs d'accès Internet et autres opérateurs de réseaux NE DOIVENT PAS générer de chemin pour 192.88.99.1, sauf si ils font fonctionner activement et surveillent un service de relais 6à4 à la cantonade comme précisé au paragraphe 4.2.1 de la [RFC6343].

Les opérateurs d'un relais de retour 6à4 qui répondent au préfixe IPv6 2002::/16 DEVRAIENT revoir les informations de la [RFC6343] et du présent document, et regarder attentivement si le relais de retour pourra être arrêté lorsque le trafic diminuera. Pour éviter les confusions, noter que rien dans la conception de 6à4 ne suppose ni n'exige que les paquets de retour soient traités par le même relais que les paquets sortants. Comme exposé au paragraphe 4.5 de la RFC 6343, les fournisseurs de contenu peuvent choisir de continuer à faire fonctionner un relais de retour pour le bénéfice de leurs propres clients 6à4 résiduels. Les fournisseurs d'accès Internet DEVRAIENT annoncer le préfixe IPv6 2002::/16 à leurs propres clients si et seulement si cela conduit à un relais de retour fonctionnant correctement comme décrit dans la RFC 6343. Les fournisseurs de service seulement IPv6, y compris ceux qui gèrent un service NAT64 [RFC6146], sont avisés que leurs propres clients ont besoin d'un chemin pour un tel relais pour le cas où un utilisateur 6à4 résiduel desservi par un fournisseur de service différent tenterait de communiquer avec eux.

Les opérateurs de "tunnels 6 à 4 gérés par le fournisseur" [RFC6732] DEVRAIENT considérer attentivement quand ce service pourra être arrêté lorsque le trafic diminuera.

7. Considérations relatives à l'IANA

Le document créant les "Registres d'adresses IPv4 d'utilisation particulière" [RFC6890] de l'IANA incluait le préfixe d'envoi à la cantonade de relais 6à4 (192.88.99.0/24) au Tableau 10. Selon ce document, IANA a marqué le préfixe 192.88.99.0/24 (défini à l'origine par la [RFC3068]) comme "Déconseillé (Relais 6à4 d'envoi à la cantonade)" et a ajouté une référence à la présente RFC. Les valeurs booléennes pour le bloc d'adresses 192.88.99.0/24 ont été supprimées. Une redélégation de ce préfixe pour toute utilisation exigera des justifications via une action de normalisation de l'IETF [RFC5226].

8. Considérations sur la sécurité

Il n'y a aucune nouvelles considérations sur la sécurité qui relèvent du présent document. Les questions générales de sécurité des tunnels figurent dans la [RFC6169] et celles plus spécifiques de 6à4 dans les [RFC3964] et [RFC6324].

9. Références

9.1 Références normatives

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. DOI 10.17487/RFC2026 *(Remplace* RFC1602, RFC1871) (*MàJ par* RFC3667, 3668, 3932, 3979, 3978, 5378, 6410, 8179)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997, DOI 10.17487/RFC2119.

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. DOI 10.17487/RFC2827 (*MàJ par* RFC3704) (BCP0038)

[RFC3056] B. Carpenter, K. Moore, "Connexion des domaines IPv6 via des nuages IPv4", février 2001. DOI 10.17487/RFC3056 *(P.S.)*

[RFC3068] C. Huitema, "Préfixe d'envoi à la cantonade pour routeurs de relais 6à4", juin 2001. DOI 10.17487/RFC3068 *(P.S.)*

[RFC3704] F. Baker, P. Savola, "Filtrage d'entrée pour réseaux à rattachement multiples", mars 2004. (BCP0084) DOI 10.17487/RFC3704.

[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. DOI 10.17487/RFC5226 (*Remplace* RFC2434 *; remplacée par* RFC8126)

[RFC6146] M. Bagnulo, P. Matthews, I. van Beijnum, "NAT64 à états pleins : Traduction d'adresse et protocole réseau de clients IPv6 en serveurs IPv4", avril 2011. DOI 10.17487/RFC6146 *(P.S.)*

[RFC6724] D. Thaler, R. Draves, A. Matsumoto, T. Chown, "Choix de l'adresse par défaut pour IPv6", septembre 2012. DOI 10.17487/RFC6724 (*Remplace la* RFC3484) *(P.S.)*

[RFC6890] M. Cotton et autres, "Registres d'adresses IP d'utilisation particulière", BCP0153, avril 2013. DOI 10.17487/RFC6890 (*Remplace* RFC4773, RFC5156, RFC5735, RFC5736 ; *MàJ par* RFC8190)

9.2 Références pour information

[HUSTON] Huston, G., "Flailing IPv6", The ISP Column, décembre 2010, < http://www.potaroo.net/ispcol/2010-12/6to4fail.html >.

[RFC3484] R. Draves, "Choix d'adresse par défaut pour le protocole Internet version 6 (IPv6)", février 2003. (*Remplacée par la* RFC6724) *(P.S.)*

[RFC3964] P. Savola, C. Patel, "Considérations de sécurité pour 6à4", décembre 2004. DOI 10.17487/RFC3964 *(Information)*

[RFC5635] W. Kumari, D. McPherson, "Filtrage de trou noir déclanché à distance avec transmission en envoi individuel sur le chemin inverse (uRPF)", août 2009. DOI 10.17487/RFC5635 *(Information)*

[RFC5969] W. Townsley, O. Troan, "Déploiement rapide de IPv6 sur infrastructures IPv4 (6rd) -- Spécification du protocole", août 2010. DOI 10.17487/RFC5969 *(PS)*

[RFC6169] S. Krishnan, D. Thaler, J. Hoagland, "Problèmes de sécurité avec le tunnelage IP", avril 2011. DOI 10.17487/RFC6169 *(Information)*

[RFC6324] G. Nakibly, F. Templin, "Attaque de boucle d'acheminement utilisant les tunnels automatiques IPv6 : position du problème et atténuations proposées", août 2011. DOI 10.17487/RFC6324 *(Information)*

[RFC6343] B. Carpenter, "Lignes directrices et conseils pour le déploiement de 6 à 4", août 2011. DOI 10.17487/RFC6343 *(Information)*

[RFC6555] D. Wing, A. Yourtchenko, "Algorithme Happy Eyeballs : pour le succès des hôtes à double pile", avril 2012. DOI 10.17487/RFC6555 *(P.S. ; remplacée par* RFC8305)

[RFC6732] V. Kuarsingh, Y. Lee, O. Vautrin, "Tunnels 6 à 4 gérés par le fournisseur", septembre 2012. DOI 10.17487/RFC6732. *(Information)*

Remerciements

Les auteurs tiennent à remercier Tore Anderson, Mark Andrews, Dmitry Anipko, Jack Bates, Cameron Byrne, Ben Campbell, Lorenzo Colitti, Gert Doering, Nick Hilliard, Philip Homburg, Ray Hunter, Joel Jaeggli, Victor Kuarsingh, Kurt Erik Lindqvist, Jason Livingood, Jeroen Massar, Keith Moore, Tom Petch, Daniel Roesen, Mark Townsley, et James Woodyatt de leurs contributions et des discussions sur ce sujet.

Un merci spécial à Fred Baker, David Farmer, Wes George, et Geoff Huston pou leurs contributions significatives.

Un grand merci à Gunter Van de Velde qui a documenté les dommanges causés par les tunnels non gérés et qui a stimulé la création de ce document.

Adresse des auteurs

Ole Troan
Cisco
Oslo
Norway
mél : ot@cisco.com

Brian Carpenter (editor)
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand
mél : brian.e.carpenter@gmail.com