Source address routing eXtension (SAR-X)

Etienne Gallet de Santerre, Laurent Toutain

Source Address Routing eXtension (SAR-X)

Etienne Gallet de Santerre — Laurent Toutain

TELECOM Bretagne - site de Rennes

RÉSUMÉ. *Devant la quantité grandissante de sites pratiquant le multihoming, le besoin de simplifier le procédé et de résoudre ses problèmes se fait plus pressant. Dans cet article, nous proposerons de résoudre le problème du choix de l'adresse source en étendant les protocoles de routage actuels à une sélection de la route par défaut en fonction de l'adresse source du paquet.*

ABSTRACT. *As more and more sites are interested in being multihomed, it is necessary to find simplier solutions to solve current multihoming problems. In this article, we will present an extension to current routing protocol allowing to solve ingress filtering problem in an easy way by taking into account the source address in the routing decision.*

MOTS-CLÉS : *Multihoming, IPv6, routage, adresse source, filtrage*

KEYWORDS: *Multihoming, IPv6, routing, source address, ingress filtering*

1. Introduction

Afin d'offrir une connectivité permanente et une fiabilité plus importante, de plus en plus de sites pratiquent le multihoming. C'est-à-dire qu'ils se connectent via différents Fournisseurs d'Accès Internet (FAI).

Les entreprises, particulièrement celles offrant un service, utilisent ce procédé dans le but de pouvoir communiquer en permanence avec l'extérieur et ne peuvent se permettre une perte de leur connectivité.

En IPv4, un préfixe indépendant des Fournisseurs d'Accès Internet (FAI) est délégué au site souhaitant faire du multihoming. Ce préfixe, annoncé par les différents FAIs du site dans le coeur de réseau, vient saturer les tables de routage déjà surchargées.

L'IPv6 permet de résoudre ce problème d'agrégation en allouant différentes adresses globales à chaque interface, chaque adresse globale appartenant à un FAI différent. Si cela semble intéressant pour diminuer la taille des tables de routage du coeur de réseau, d'autres problèmes importants se posent.
Notamment, le problème du choix de l'adresse source. En effet, (Ferguson *et al.,* 2000) indique que pour des raisons de sécurité un paquet sortant d'un site doit avoir une adresse source appartenant au FAI, faute de quoi, il sera rejeté.

Dans cet article, nous allons présenter brièvement différentes façons de faire du multihoming en IPv6 et des solutions en cours de développement. Puis, nous expliquerons en détail notre solution permettant de s'affranchir du choix de l'adresse source tout en permettant l'agrégation des préfixes et nous préciserons les avantages de cette solution. Nous conclurons alors sur les évolutions envisageables de ce procédé.

2. Les différents mécanismes de multihoming en IPv6

2.1. *Allocation d'un préfixe indépendant du fournisseur*

L'allocation d'un préfixe indépendant du fournisseur est la technique utilisée en IPv4 pour les sites multi-homés. De tels sites se voient attribuer un numéro d'AS (Autonomous System) ainsi qu'un préfixe global directement par un RIR (Regional Internet Registry). Le préfixe ainsi alloué est indépendant de ceux des FAI du site. Ce préfixe est donc annoncé par tous les fournisseur d'accès du site via BGP dans le coeur de réseau.
Cette solution présente un inconvénient majeur, relevé dans (T. Bu *et al.,* 2004), qui est d'encombrer encore plus les tables de routage d'internet déjà très surchargées ; d'autant plus que le nombre de sites pratiquant le multihoming est croissant.

2.2. *Utilisation de plusieurs adresses*

Grâce à l'IPv6, il est possible de configurer plusieurs adresses pour une interface. Ainsi, une adresse est attribuée aux machines pour chaque FAI du site. Ainsi aucun nouveau préfixe n'est annoncé n'est annoncé au coeur de réseau en plus de celui des FAI.

Les machines ont donc plusieurs adresses ; se pose alors le choix de l'adresse source. Effectivement, (Ferguson *et al.,* 2000) spécifie qu'un paquet émis depuis une machine d'un réseau vers l'extérieur de ce réseau doit posséder une adresse source correspondant au FAI de sortie ; c'est ce qu'on appelle l'*ingress filtering*. Ainsi un paquet ayant une adresse source de préfixe x (délégué par un fournisseur X) arrivant sur un routeur de bordure connecté à un fournisseur Y (déléguant un préfixe y) sera jeté pour des mesures de sécurité (pour éviter l'usurpation d'adresse IP).

Une approche pour résoudre ce problème d'*ingress filtering* et donc de résoudre le problème du choix de l'adresse source est la séparation des rôles de localisation et d'identification de l'adresse IP. Une des adresses de la machine est choisie pour identifier la machine, tandis que l'ensemble des adresses allouées peuvent servir de localisateur.

Nous allons maintenant présenter brièvement deux types de solutions qui sont actuellement à l'étude ; d'une part, une solution de type *réécriture d'adresse* et d'autre part, une solution de type *encapsulation*.

- La ***réécriture d'adresse*** consiste en la modification de l'en-tête IPv6, au niveau d'un routeur sur le trajet du paquet (la machine émettrice, le routeur de sortie du site ou un autre routeur), pour modifier l'adresse source du paquet et la faire correspondre au préfixe appartenant au FAI de sortie. Les seuls bits à changer sont ceux correspondant au préfixe délégué dans le site. Ainsi l'adresse de sortie est correcte et le paquet n'est pas jeté. Cependant, une correspondance doit être établie au niveau du (ou des) routeur effectuant le changement d'adresse pour reconnaître les paquets ayant subi une modification de l'adresse source et éventuellement faire l'opération inverse. Un exemple de cette solution est décrite dans (Vogt, 2007)

- Le ***processus d'encapsulation*** permet quant à lui de créer des tunnels entre deux routeurs du réseau servant respectivement de localisateur pour la machine source et pour la machine destination du paquet envoyé. Plusieurs localisateurs peuvent exister pour une machine. Ainsi, pour joindre un ordinateur donné, une requête est faite pour établir vers quel localisateur envoyé le paquet. Comme un tunnel est créé entre deux localisateurs, une nouvelle encapsulation IPv6 est ajoutée avec l'adresse du localisateur en adresse source, ce qui permet d'avoir toujours une adresse cohérente au niveau du FAI de sortie. Un procédé d'encapsulation est défini dans (Farinacci *et al.,* 2007) .

Ces solutions répondent effectivement au problème de l'adresse source et de l'*ingress filtering* mais elles impliquent des modifications au niveau du coeur de réseau : le *processus d'encapsulation* nécessite d'établir des tables de correspondances entre une destination et ses localisateurs, ainsi qu'un moyen de récupérer ces cor-

respondances, tandis que la *réécriture d'adresse* impose aux machines pratiquant ce procédé, ainsi qu'aux machines source et destination de conserver un contexte de la communication afin de voir les modifications apportées et les inverser au besoin.

La solution que nous proposons n'intervient qu'au niveau du réseau terminal et étend le protocole de routage du site pour prendre en compte l'adresse source du paquet dans la décision de routage ; elle ne modifie en rien le paquet, ni l'architecture et le fonctionnement du coeur de réseau.

3. Fonctionnement de SAR-X (Source Address Routing eXtension)

L'idée principale de cette extension est de router un paquet à destination d'un site externe jusqu'au FAI de sortie correspondant à l'adresse source du paquet émis. Le principe de SAR-X est très simple et il a l'avantage de n'entraîner aucun changement au niveau de la machine terminale ni dans le comportement du coeur de réseau internet. Les changements nécessaires au bon fonctionnement de SAR-X s'effectuent essentiellement au niveau des routeurs de bordure du site (c'est-à-dire aux routeurs rattachés aux FAI) et éventuellement à tous les routeurs du site.

Actuellement, lorsqu'un paquet est reçu par un routeur, si la destination du paquet est connu, le paquet est retransmis au prochain routeur conformément à la table de routage, sinon, le paquet est transmis sur la route par défaut du routeur. SAR-X donne la possibilité de choisir cette route par défaut en fonction de l'adresse source du paquet.

Le protocole de routage du site doit être modifié pour annoncer, en plus de la table de routage classique, une table spécifique contenant le préfixe global délégué par le FAI, le coût pour aller jusqu'au routeur de sortie du FAI le plus proche et le prochain saut à qui transmettre le paquet.

3.1. *diffusion des différentes routes par défaut*

Dans les protocoles de routage actuels, tous les routeurs annoncent les préfixes des liens auxquels ils sont directement connectés et le coût associé à chaque lien. Après traitement de ces messages, chaque routeur peut construire sa table de routage avec les préfixes des liens, leur coût et le prochain saut associés.

Avec SAR-X, une autre information est distribué par les routeurs de bordures et relayés par tous les routeurs (ceux utilisant SAR-X). Chaque routeur de bordure annonce à ses voisins, dans une option SAR-X d'un message de l'IGP (*Interior Gateway Protocol*), le préfixe global délégué par le FAI, un coût nul et leur adresse IP en tant que prochain saut.

Les routeurs du site acceptant de traiter cette option (donc, les routeurs utilisant SAR-X), utilisent ces informations pour compléter leur table de routage. Plus préci-

sément, une route par défaut est associé au préfixe et au prochain saut spécifiés dans cette option du message de l'IGP. Ensuite, ce préfixe, le coût de la route incrémenté (d'une unité pour un protocole de routage de type vecteur de distance ou du coût du lien ayant reçu l'information pour un protocole de type état de lien) et l'adresse du routeur sont spécifiés dans une option SAR-X et envoyé aux voisins.

Après un temps de convergence, tous les routeurs SAR-X ont une table de routage classique, ainsi qu'une table des routes par défaut associées à leur préfixe.

3.2. *Traitement du paquet*

Pour simplifier la compréhension de SAR-X, nous allons considérer dans cette section que tous les routeurs du site utilisent SAR-X.

Un paquet est envoyé par une machine interne au site à une destination externe. Comme la machine ne connaît pas directement le préfixe de la destination, le paquet est transmis sur la route par défaut de la machine. La passerelle par défaut de la machine reçoit alors le paquet et essaye de trouver une correspondance optimal pour le préfixe de l'adresse destination. Comme il s'agit d'une adresse externe au site, aucune correspondance n'est trouvé. Le routeur doit donc envoyer le paquet sur sa route par défaut.

Puisqu'il en possède plusieurs, le routeur va comparer les préfixes associés à ces routes par défaut à l'adresse source du paquet pour essayer de trouver le préfixe qui s'en rapproche le plus. Une fois la correspondance trouvée, le paquet est envoyé au prochain saut spécifié dans la table des routes par défaut.

Ce procédé est répété sur tous les routeurs SAR-X jusqu'à ce que le paquet soit dirigé vers le routeur de sortie du FAI ayant délivré le préfixe de l'adresse source.

Figure 1. *réseau SAR-X*

Dans l'exemple de la Figure 1, les deux FAI du site annoncent leur préfixe aux autres routeurs en plus des informations de routage classiques. Avec ces informations, chaque routeur peut, dans un premier temps, remplir sa table de routage classique, puis sa table des routes par défaut. Ils savent alors comment joindre tous les liens du site et comment atteindre le routeur de sortie qui acceptera l'adresse source du paquet.

Les tables des routes par défaut des différents routeurs sont listées ci-dessous :

R_1

prefix	Next hop	cost
α : :/48	R_A	1
β : :/52	R_2	3

R_2

prefix	Next hop	cost
α : :/48	R_1	2
β : :/52	R_3	2

R_3

prefix	Next hop	cost
α : :/48	R_2	3
β : :/52	R_B	1

R_A

prefix	Next hop	cost
α : :/48	if_{out}	0
β : :/52	R_1	4

R_B

prefix	Next hop	cost
α : :/48	R_3	4
β : :/52	if_{out}	0

- La source S veut envoyer un paquet à la destination D en dehors du site (γ :1 : :1). Comme S ne connaît pas le préfixe γ, le paquet est envoyé à la passerelle par défaut (supposons le routeur R_3) en utilisant une de ses adresses source (nous supposerons α :3 : :1).

- R_3 compare l'adresse destination du paquet avec les réseaux connus de sa table de routage. Aucune correspondance n'étant trouvé, le routeur cherche une correspondance dans la table des routes par défaut pour le préfixe de l'adresse source. Une correspondance est trouvé (préfixe : α : :/48 - prochain saut : R_2 - coût : 3) alors le paquet et transmis au prochain saut spécifié dans la table.

- R_2 traite le paquet de la même manière que R_3 et trouve, dans sa table de routes par défaut que le prochain saut est R_1. Le paquet lui est donc transmis.

- Le même processus est effectué au niveau de R_1 qui transmet alors le paquet à R_A.

- Le paquet de préfixe α pour son adresse source, quitte le site via le FAI A qui a délégué ce préfixe. L'*ingress filtering* ne bloque pas le paquet.

3.3. *Scénaio de déploiement de SAR-X*

3.3.1. *Plusieurs zones indépendantes de routeurs SAR-X existent dans le site*

Dans ce scénario, chaque routeur de bordure fonctionne avec SAR-X et est connecté à au moins un autre routeur SAR-X, mais tout les routeurs de bordures ne peuvent pas être liés par des routeurs SAR-X successifs.

Une source du site envoie un paquet à une destination externe. Dans un premier temps routé classiquement, le paquet est ensuite reçu par un routeur SAR-X. Comme la destination source est inconnue, une correspondance est cherchée dans la table des routes par défaut. Cependant comme des zones SAR-X indépendantes existent, le routeur ne connaît pas tous les préfixes du site. Il y a donc une possibilité qu'aucune correspondance ne soit trouvée. Le paquet est alors routé de manière classique jusqu'au routeur de sortie qui va rejeter le paquet à cause de l'*ingress filtering*.

Ce scénario n'apporte donc clairement aucune amélioration au fonctionnement actuel du routage, mais il montre que cela ne perturbe pas le fonctionnement du routage. On peut également en déduire qu'une condition nécessaire pour que SAR-X soit efficace est que tous les routeurs SAR-X aient connaissance de tous les préfixes du site et de leur routeur de bordure correspondant.

3.3.2. *Tous les routeurs de bordure appartiennent à une même zone SAR-X*

Tous les routeurs n'utilisent pas SAR-X, mais il est possible d'aller d'un routeur de bordure à un autre via des routeurs implémentant SAR-X.

Avec cette architecture, tous les routeurs SAR-X connaissent tous les préfixes du site et le routeur de sortie associé à chaque préfixe. Un paquet envoyé par une machine du site vers une destination externe au site va nécessairement être traité par un routeur SAR-X. Le paquet est alors transmis sur un chemin menant vers le routeur de bordure du FAI qui a délégué le préfixe de l'adresse source.

Si ce scénario à l'avantage d'affranchir le routage du problème de l'*ingress filtering*, on peut lui reprocher le fait que le chemin utilisé pour aller de la source jusqu'au routeur de sortie n'est pas nécessairement le plus court. Le pire cas étant un routage classique jusqu'à un mauvais routeur de bordure (en considération de l'adresse source) qui va alors le renvoyer vers le routeur correct grâce à SAR-X. Le temps de transit du paquet est donc augmenté, mais considérant que le paquet est au final transmis et non pas rejeté, l'évolution apportée par l'utilisation de SAR-X reste positive.

3.3.3. *Tous les routeurs du site utilisent SAR-X*

Tous les routeurs utilisent SAR-X, donc connaissent tous les préfixes du site et les routeurs de bordure associés.

Un paquet envoyé du site vers l'extérieur est immédiatement pris en charge par un routeur SAR-X. Donc le paquet est directement transmis sur un chemin conduisant au routeur de bordure du FAI qui a délivré le préfixe de l'adresse source du paquet. De plus, le chemin utilisé pour aller de la source jusqu'au routeur de sortie est le plus court possible puisque la construction de la table des routes par défaut s'effectue en tenant compte du coût pour atteindre le routeur de sortie.

Dans ce dernier scénario, non seulement le problème de l'*ingress filtering* et donc du choix de l'adresse source est résolu, mais le routage est aussi optimal qu'avec les protocoles de routage actuels.

4. Conclusion

Les solutions telles que (Farinacci *et al.,* 2007) ou (Vogt, 2007) parviennent à résoudre nombre de problèmes liés au multihoming mais impliquent des changements conséquents dans l'architecture actuelle, notamment dans le coeur de réseau.

SAR-X au contraire permet de répondre au problème posé par l'*ingess filtering* de manière simple en ne modifiant le fonctionnement que du site terminal. Il assure également une agrégabilité des préfixes au niveau du coeur de réseau. De plus, son déploiement peut se faire progressivement pour parvenir à une utilisation optimale.

Enfin, l'utilisation conjointe de SAR-X avec d'autres solutions répondant à d'autres problématiques liées au multihoming telles que la survie de la session sont à l'étude. Notamment SHIM6 (E. Nordmark, 2007), qui crée un contexte de connection entre deux machines communicantes et permet la survie de la session. Le but étant de parvenir à un résultat offrant le maximum de bénéfices pour les sites multi-homés.

5. Bibliographie

E. Nordmark M. B., « "Shim6 : Level 3 Multihoming Shim Protocol for IPv6" », October, 2007. draft-ietf-shim6-proto-09.

Farinacci D., Fuller V., Oran D., Meyer D., « "Locator/ID Separation Protocol (LISP" », November, 2007. draft-farinacci-lisp-05 (work in progress).

Ferguson P., Senie D., « "Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing" », May, 2000. RFC2827.

T. Bu L. G., Towsley D., « "On characterizing BGP routing table growth" », *Computer Networks*, 2004.

Vogt C., « "Six/One : A Solution for Routing and Addressing in IPv6" », November, 2007. draft-vogt-rrg-six-one-01 (work in progress).