

Groupe de travail Réseau
Request for Comments : 4191
 Catégorie : En cours de normalisation
 Traduction Claude Brière de L'Isle

R. Draves
 D. Thaler
 Microsoft
 novembre 2005

Préférences en matière de routeur par défaut et chemins plus spécifiques

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la 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 (2005). Tous droits réservés.

Résumé

Le présent document décrit une extension facultative aux messages d'annonce de routeur pour communiquer les préférences de routeur par défaut et les chemins plus spécifiques des routeurs aux hôtes. Cela améliore la capacité des hôtes à prendre un routeur approprié, en particulier lorsque l'hôte est multi rattachement et que les routeurs sont sur des liaisons différentes. Les valeurs de préférence et les chemins spécifiques annoncés aux hôtes exigent une configuration administrative ; ils ne sont pas automatiquement déduits des tableaux d'acheminement.

Table des Matières

1. Introduction.....	1
1.1 Conventions de langage.....	2
2. Formats de message.....	2
2.1 Valeurs de préférence.....	2
2.2 Changements en format de message d'annonce de routeur.....	3
2.3 Option Informations de chemin	3
3. Modèle conceptuel d'un hôte.....	4
3.1 Structures de données conceptuelles pour les hôtes.....	4
3.2 Algorithme d'envoi conceptuel pour les hôtes.....	5
3.3 Gestion de l'antémémoire de destination.....	5
3.4 Configurabilité du client.....	5
3.5 Vérification de l'accessibilité du routeur.....	5
3.6 Exemple.....	6
4. Configuration du routeur.....	6
4.1 Lignes directrices pour les administrateurs.....	6
5. Exemples.....	7
5.1 Meilleur routeur pour ::/0 contre routeur le moins probable pour rediriger.....	7
5.2 Hôte multi rattachement et réseau isolé.....	7
6. Considérations sur la sécurité.....	8
7. Considérations relatives à l'IANA.....	8
8. Remerciements.....	8
9. Références normatives.....	8
10. Références pour information.....	9
Adresse des auteurs.....	9
Déclaration complète de droits de reproduction.....	9

1. Introduction

La découverte de voisin [RFC2461] spécifie un modèle conceptuel pour les hôtes qui comporte une liste de routeurs par défaut et une liste de préfixes. Les hôtes envoient des messages de sollicitation de routeur et reçoivent des messages d'annonce de routeur de la part des routeurs. Les hôtes remplissent leur liste de routeurs par défaut et leur listes de préfixes sur la base des informations des messages d'annonce de routeur. Un algorithme conceptuel d'envoi utilise la liste des préfixes pour déterminer si une adresse de destination est sur la liaison et utilise la liste des routeurs par défaut pour choisir

un routeur pour les destinations hors liaison.

Dans certaines topologies de réseau où l'hôte a plusieurs routeurs sur sa liste de routeurs par défaut, le choix d'un routeur pour une destination hors liaison est important. Dans certaines situations, un routeur peut fournir de bien meilleures performances qu'un autre pour une destination. Dans d'autres situations, choisir le mauvais routeur peut résulter en l'échec de la communication. (La Section 5 donne des exemples spécifiques de ces scénarios.)

Le présent document décrit une extension facultative au message d'annonce de routeur de découverte de voisin pour communiquer les préférences de routeur par défaut et les chemins plus spécifiques des routeurs aux hôtes. Cela améliore la capacité des hôtes à prendre un routeur approprié pour une destination hors liaison.

Noter que comme ces procédures ne sont applicables qu'aux hôtes, l'algorithme de transmission utilisé par les routeurs (incluant les hôtes à capacité de transmission IP) n'est pas affecté.

La découverte de voisin fournit un message Redirect que les routeurs peuvent utiliser pour corriger le choix de routeur d'un hôte. Un routeur peut envoyer un message Redirect à un hôte pour lui dire d'utiliser un routeur différent pour une certaine destination. Cependant, la fonction Redirect se limite à une seule liaison. Un routeur sur une liaison ne peut pas rediriger un hôte sur un routeur d'une autre liaison. Donc, les messages Redirect n'aident pas les hôtes multi rattachement (à travers plusieurs interfaces) à choisir un routeur approprié.

Les hôtes multi rattachement sont un scénario à l'importance croissante, en particulier avec IPv6. En plus d'une connexion de réseau filaire, comme Ethernet, les hôtes peuvent avoir une ou plusieurs connexions sans fil, comme 802.11 ou Bluetooth. En plus de la connexion physique au réseau, les hôtes peuvent avoir des connexions réseau virtuelles ou tunnelées. Par exemple, en plus d'une connexion directe à l'Internet public, un hôte peut avoir un tunnel dans un réseau d'entreprise privé. Certains scénarios de transition à IPv6 peuvent ajouter des tunnels supplémentaires. Par exemple, des hôtes peuvent avoir des connexions réseau 6à4 [RFC3056] ou de tunnel configuré [RFC2893].

Le présent document exige que les valeurs de préférence et les chemins spécifiques annoncés aux hôtes reçoivent une configuration administrative explicite. Elles ne sont pas automatiquement déduites des tableaux d'acheminement. En particulier, les valeurs de préférence ne sont pas des métriques d'acheminement et il n'est pas recommandé que les routeurs ouvrent leurs tableaux d'acheminement entiers aux hôtes.

On utilise les messages d'annonce de routeur plutôt que tout autre protocole comme RIP [RFC2080], parce que l'annonce de routeur est un protocole standard existant et stable pour la communication de routeur à hôte. Porter ces informations sur du trafic existant de messages des routeurs aux hôtes réduit les frais généraux du réseau. La découverte de voisin partage avec la découverte d'écouter de diffusion groupée la propriété que tous deux définissent comme interactions d'hôte à routeur, tout en protégeant l'hôte contre l'obligation de participer à des interactions plus générales de routeur à routeur. De plus, RIP ne convient pas parce il ne porte pas les durées de vie de chemins de sorte qu'il requiert un trafic de messages fréquents avec de plus gros frais généraux de traitement.

Les mécanismes spécifiés ici sont rétro compatibles, de sorte que les hôtes qui ne les mettent pas en œuvre continuent de fonctionner comme ils le faisaient antérieurement.

1.1 Conventions de langage

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. Formats de message

2.1 Valeurs de préférence

Les préférences de routeur par défaut et les préférences de chemins plus spécifiques sont codées de la même façon.

Les valeurs de préférence sont codées comme entier signé sur deux bits, comme suit :

01 : haute

00 : moyenne (par défaut)

11 : faible

10 : réservé – NE DOIT PAS être envoyé

Noter que les mises en œuvre peuvent traiter la valeur comme un entier signé de deux bits.

Avoir juste trois valeurs renforce le fait que ce ne sont pas des métriques et il n'apparaîtra pas que plus de valeurs soient nécessaires pour des scénarios raisonnables.

2.2 Changements en format de message d'annonce de routeur

Les changements au paragraphe 4.2 de la découverte de voisin [RFC2461] et au paragraphe 7.1 de la [RFC3775] sont les suivants :

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Code   |   Somme de contrôle   |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Limite act bond | M | O | H | Prf | Rsv |   Durée de vie de routeur   |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Durée d'accessibilité         |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Temporisateur de retransmission |
+-----+-----+-----+-----+-----+-----+-----+
|   Options ...   |
+-----+-----+-----+-----+-----+-----+-----+

```

Champs :

Prf (Préférence de routeur par défaut) : entier signé de deux bits. Indique si on préfère ce routeur aux autres routeurs par défaut. Si la durée de vie du routeur est zéro, la valeur de préférence DOIT être réglée à (00) par l'envoyeur et DOIT être ignorée par le receveur. Si la valeur Réserve (10) est reçue, le receveur DOIT traiter la valeur comme si c'était (00).

Rsv (Réserve) : champ de 3 bits non utilisés. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Options possibles :

Informations de chemin : ces options spécifient des préfixes qui sont accessibles via le routeur.

Discussion : Noter qu'en plus de la valeur de préférence dans l'en-tête de message, une annonce de routeur peut aussi contenir une option Informations de chemin pour ::/0, avec une valeur de préférence et une durée de vie. Coder une valeur de préférence dans l'en-tête d'annonce de routeur présente des avantages :

1. Cela permet une distinction entre "le meilleur routeur pour le chemin par défaut" et "le routeur le moins probable pour rediriger le trafic commun", comme décrit au paragraphe 5.1.
2. Lorsque le meilleur routeur pour le chemin par défaut est aussi le routeur le moins probable pour rediriger le trafic commun (ce qui sera le cas courant) le codage de la valeur de préférence dans l'en-tête de message est plus efficace que d'envoyer une option séparée.

2.3 Option Informations de chemin

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Longueur   | Longueurpréfixe | Rsv | Prf | Rsv |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Durée de vie de chemin         |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Préfixe (longueur variable)     |
~
~
+-----+-----+-----+-----+-----+-----+-----+

```

Champs :

Type : 24

Longueur : entier non signé de 8 bits. La longueur de l'option (incluant les champs Type et Longueur) en unités de 8 octets. Le champ Longueur est 1, 2, ou 3 selon la longueur de préfixe. Si Longueur de préfixe est supérieur à 64, Longueur doit être 3. Si Longueur de préfixe est supérieur à 0, Longueur doit alors être 2 ou 3. Si Longueur de préfixe est zéro, Longueur doit alors être 1, 2, ou 3.

Longueur de préfixe : entier non signé de 8 bits. Le nombre de bits en tête dans le préfixe qui sont valides. Les valeurs vont de 0 à 128. Le champ Préfixe est de 0, 8, ou 16 octets selon la longueur.

Prf (Préférence de chemin) : entier signé de deux bits. La préférence de chemin indique si on préfère le routeur associé à ce préfixe plutôt que les autres, lorsque plusieurs préfixes identiques (pour des routeurs différents) ont été reçus. Si la valeur Réserve (10) est reçue, l'option Informations de chemin DOIT être ignorée.

Rsv (réserve) : champs de trois bits non utilisés. Ils DOIVENT être initialisés à zéro par l'expéditeur et DOIVENT être ignorés par le receveur.

Durée de vie de chemin : entier non signé de 32 bits. La durée en secondes (par rapport à l'heure d'envoi du paquet) pendant laquelle le préfixe est valide pour la détermination de chemin. Une valeur toute de bits à un (0xffffffff) représente l'infini.

Préfixe : champ de longueur variable qui contient une adresse IP ou un préfixe d'une adresse IP. Le champ Longueur de préfixe contient le nombre de bits en tête valides dans le préfixe. Les bits dans le préfixe après la longueur de préfixe (si il y en a) sont réservés et DOIVENT être initialisés à zéro par l'expéditeur et ignorés par le receveur.

Les routeurs NE DOIVENT PAS inclure deux options Informations de chemin avec le même préfixe et longueur de préfixe dans la même annonce de routeur.

Discussion : il y a plusieurs raisons d'utiliser une nouvelle option Informations de chemin plutôt que d'utiliser des bits fanions pour surcharger l'option existante d'informations de préfixe :

1. les préfixes ne vont normalement se montrer que dans une option, pas les deux, de sorte qu'une nouvelle option n'introduit pas de duplication ;
2. l'option Informations de chemin fait normalement 16 octets tandis que l'option Informations de préfixe fait 32 octets ;
3. utiliser une nouvelle option peut améliorer la rétro compatibilité avec certaines mises en œuvre d'hôte.

3. Modèle conceptuel d'un hôte

Il y a trois modèles conceptuels possibles pour une mise en œuvre d'hôte de préférences de routeur par défaut et de chemins plus spécifiques, correspondant à différents niveaux de prise en charge. On les appelle type A, type B, et type C.

3.1 Structures de données conceptuelles pour les hôtes

Les hôtes de type A ignorent les préférences de routeur par défaut et les chemins plus spécifiques. Ils utilisent les structures de données conceptuelles décrites dans la découverte de voisin [RFC2461].

Les hôtes de type B utilisent la liste de routeurs par défaut augmentée des valeurs de préférence, mais ignorent toutes les options d'informations de chemins. Ils utilisent la valeur de préférence de routeur par défaut dans l'en-tête d'annonce de routeur. Ils ignorent les options d'informations de chemin.

Les hôtes de type C utilisent un tableau d'acheminement au lieu d'une liste de routeurs par défaut. (Le tableau d'acheminement peut aussi englober la liste de préfixes, mais cela sort du domaine d'application du présent document.) Les entrées dans le tableau d'acheminement ont un préfixe, une longueur de préfixe, une valeur de préférence, une durée de vie, et un routeur de prochain bond. Les hôtes de type C utilisent la valeur de préférence de routeur par défaut dans l'en-tête d'annonce de routeur et les options d'informations de routeur.

Lorsque un hôte de type C reçoit une annonce de routeur, il modifie son tableau d'acheminements comme suit. Lorsque il traite une annonce de routeur, un hôte de type C met d'abord à jour un chemin `::/0` sur la base de la durée de vie de routeur et la préférence de routeur par défaut dans l'en-tête de message d'annonce de routeur. Ensuite, lorsque l'hôte traite les options Informations de routeur dans le corps du message d'annonce de routeur, il met à jour son tableau d'acheminements pour chacune de ces options. Les valeurs de préférence de routeur et de durée de vie dans une option Informations de chemin `::/0` outrepassent les valeurs de préférence et de durée de vie dans l'en-tête d'annonce de routeur. La mise à jour de

chaque chemin est faite comme suit. Un chemin est localisé dans le tableau d'acheminements sur la base du préfixe, de la longueur de préfixe, et du routeur de prochain bond. Si la durée de vie du chemin reçu est zéro, le chemin est retiré du tableau d'acheminements si il y est présent. Si la durée de vie d'un chemin n'est pas zéro, le chemin est ajouté au tableau d'acheminements si il n'y est pas présent et la durée de vie et la préférence du chemin sont mises à jour si le chemin est déjà présent.

Par exemple, supposons des hôtes qui reçoivent une annonce de routeur d'un routeur X avec une durée de vie de routeur de 100 secondes et une préférence de routeur par défaut de moyen. Le corps de l'annonce de routeur contient une option d'informations de chemin pour `::/0` avec une durée de vie de chemin de 200 secondes et une préférence de chemin de faible. Après le traitement de l'annonce de routeur, un hôte de type A va avoir une entrée pour le routeur X dans sa liste des routeurs par défaut avec une durée de vie de 100 secondes. Si un hôte de type B reçoit la même annonce de routeur, il va avoir une entrée pour le routeur X dans sa liste des routeurs par défaut avec une préférence moyenne et une durée de vie de 100 secondes. Un hôte de type C aura une entrée dans son tableau d'acheminements pour `::/0 -> routeur X`, avec une préférence faible et une durée de vie de 200 secondes. Durant le traitement de l'annonce de routeur, un hôte de type C PEUT avoir un état transitoire, dans lequel il a une entrée dans son tableau d'acheminements pour `::/0 -> routeur X` avec une préférence moyenne et une durée de vie de 100 secondes.

3.2 Algorithme d'envoi conceptuel pour les hôtes

Les hôtes de type A utilisent l'algorithme d'envoi conceptuel décrit dans la découverte de voisin [RFC2461].

Lorsque un hôte de type B fait la détermination du prochain bond et consulte sa liste des routeurs par défaut, il préfère principalement les routeurs accessibles à ceux qui ne le sont pas, et secondairement utilise les valeurs de préférence de routeur. Si l'hôte n'a pas d'information sur l'accessibilité du routeur, il suppose que le routeur est accessible.

Lorsque un hôte de type C fait la détermination de prochain bond et consulte son tableau d'acheminements pour une destination hors liaison, il cherche dans son tableau d'acheminement pour trouver le chemin avec le plus long préfixe qui correspond à la destination, en utilisant les valeurs de préférence de chemin pour le départage si plusieurs chemins correspondent avec la même longueur de préfixe. Si le meilleur chemin pointe sur un routeur non accessible, ce routeur est mémorisé pour l'algorithme décrit au paragraphe 3.5, et le meilleur chemin suivant est consulté. Cette vérification est répétée jusqu'à ce qu'un chemin correspondant soit trouvé qui pointe sur un routeur accessible, ou qu'il ne reste plus de chemin qui corresponde. Là encore, si l'hôte n'a pas d'information sur l'accessibilité du routeur, il supposera l'accessibilité.

Si il n'y a pas de chemin qui corresponde à la destination (c'est-à-dire, pas de chemin par défaut et pas de chemin plus spécifique) un hôte de type C DEVRAIT éliminer le paquet et rapporter un "Destination inaccessible/Pas de chemin" comme erreur de destination à la couche supérieure.

3.3 Gestion de l'antémémoire de destination

Lorsque un hôte de type C traite une annonce de routeur et met à jour son tableau d'acheminements conceptuel, il DOIT invalider ou supprimer les entrées d'antémémoire de destination et refaire la détermination de prochain bond pour les destinations affectées par les changements du tableau d'acheminements.

3.4 Configurabilité du client

Les hôtes de type B et C PEUVENT être configurables avec des valeurs de préférence qui outrepassent les valeurs des annonces de routeur reçues. Ceci est particulièrement utile pour traiter avec les routeurs qui peuvent ne pas prendre en charge les préférences.

3.5 Vérification de l'accessibilité du routeur

Lorsque un hôte évite d'utiliser tout routeur X non accessible et envoie à la place un paquet de données à un autre routeur Y, et que l'hôte aurait utilisé le routeur X si il avait été accessible, l'hôte DEVRAIT alors sonder l'accessibilité de chacun de ces routeurs X en envoyant une seule sollicitation de voisin à l'adresse de ce routeur. Un hôte NE DOIT PAS sonder l'accessibilité d'un routeur en l'absence de trafic utile que l'hôte aurait envoyé au routeur si il avait été accessible. Dans tous les cas, ces sondages DOIVENT être limités à pas plus d'un par minute et par routeur.

Cette exigence permet à l'hôte de découvrir quand le routeur X devient accessible et de commencer à utiliser le routeur X à ce moment. Autrement, l'hôte peut ne pas remarquer l'accessibilité du routeur X et continuer d'utiliser le moins désirable routeur Y jusqu'à ce que la prochaine annonce de routeur soit envoyée par X. Noter que le routeur peut avoir été

inaccessible pour des raisons autres que d'être hors circuit (par exemple, un commutateur sur le chemin peut être hors service) de sorte qu'il peut se passer jusqu'à 30 minutes (la période maximum d'annonce) avant que la prochaine annonce de routeur soit envoyée.

Pour un hôte de type A (suivant l'algorithme de la [RFC2461]) aucun sondage n'est nécessaire car tous les routeurs sont également préférables. Par ailleurs, un hôte de type B ou C sonde explicitement les routeurs préférables inaccessibles, pour savoir quand ils deviennent à nouveau accessibles.

3.6 Exemple

Supposons un hôte de type C qui a quatre entrées dans son tableau d'acheminements :

::/0 -> routeur W avec une préférence moyenne,

2002::/16 -> routeur X avec une préférence moyenne,

2001:db8::/32-> routeur Y avec une préférence haute,

2001:db8::/32-> routeur Z avec une préférence faible.

et l'hôte envoie à 2001:db8::1, une destination hors liaison. Si tous les routeurs sont accessibles, l'hôte va alors choisir le routeur Y. Si le routeur Y n'est pas accessible, le routeur Z va alors être choisi et l'accessibilité du routeur Y sera sondée. Si les routeurs Y et Z ne sont pas accessibles, le routeur W va alors être choisi et l'accessibilité des routeurs Y et Z sera vérifiée. Si les routeurs W, Y, et Z ne sont pas accessibles, l'hôte devrait alors utiliser Y tout en vérifiant l'accessibilité de W et Z. Le routeur X ne sera jamais choisi parce que son préfixe ne correspond pas à la destination.

4. Configuration du routeur

Les routeurs NE DEVRAIENT PAS annoncer des préférences ou chemins par défaut. En particulier, ils NE DEVRAIENT PAS "communiquer" tout leur tableau d'acheminements aux hôtes.

Les routeurs PEUVENT avoir un mode de configuration dans lequel une annonce d'un préfixe spécifique dépend d'une condition spécifique, comme un état de fonctionnement d'une liaison ou la présence du même préfixe ou d'un autre dans le tableau d'acheminements installé par une autre source, comme un protocole d'acheminement dynamique. Si cela est, les mises en œuvre de routeur DEVRAIENT s'assurer que les annonces de préfixes aux hôtes sont découplées de la dynamique du tableau d'acheminement pour empêcher une charge excessive sur les hôtes durant les périodes d'instabilité de l'acheminement. En particulier, des chemins non stables NE DEVRAIENT PAS être annoncés aux hôtes tant que leur stabilité n'est pas améliorée.

Les routeurs NE DEVRAIENT PAS envoyer plus de 17 options d'informations de chemin dans les annonces de routeur par liaison. Cette limite arbitraire est destinée à renforcer l'idée que des chemins relativement peu nombreux et choisis avec soin devraient être annoncés aux hôtes.

Les valeurs de préférence (préférences de routeur par défaut et préférences de chemin) NE DEVRAIENT PAS être des métriques d'acheminement ou être automatiquement déduites de métriques : les valeurs de préférence DEVRAIENT être configurées.

Les informations contenues dans les annonces de routeur peuvent changer par l'action de la gestion du système. Par exemple, la durée de vie ou la préférence des chemins annoncés peuvent changer, ou de nouveaux chemins pourraient être ajoutés. Dans ce cas, le routeur PEUT transmettre jusqu'à MAX_INITIAL_RTR_ADVERTISEMENTS annonces non sollicitées, en utilisant les mêmes règles que dans la [RFC2461]. Lorsque elle cesse d'être une interface d'annonce et d'envoi d'annonces de routeur avec une durée de vie de routeur de zéro, l'annonce de routeur DEVRAIT aussi régler la durée de vie de chemin à zéro dans toutes les options d'informations de chemin.

4.1 Lignes directrices pour les administrateurs

Les valeurs de préférence haute et faible (qui ne sont pas par défaut) ne devraient être utilisées que lorsque quelqu'un qui a connaissance à la fois des routeurs et de la topologie du réseau les configure explicitement. Par exemple, ce pourrait être un administrateur réseau commun, ou ce pourrait être une demande de consommateur à des administrateurs différents qui gèrent les routeurs.

Une exception à cette règle générale est que l'administrateur d'un routeur qui n'a pas de connexion à l'Internet, ou est connecté à travers un pare-feu qui bloque le trafic général, devrait configurer le routeur à annoncer une préférence de routeur par défaut faible.

De plus, l'administrateur d'un routeur devrait configurer le routeur à annoncer un chemin spécifique du site pour le préfixe du ou des réseaux auxquels le routeur appartient. L'administrateur peut aussi configurer le routeur à annoncer les chemins spécifiques pour les sous réseaux directement connectés et tous préfixes plus courts pour les réseaux auxquels appartient le routeur.

Par exemple, si un utilisateur établit un tunnel dans un réseau d'entreprise derrière un pare-feu, le routeur d'accès sur l'extrémité réseau d'entreprise du tunnel devrait s'annoncer comme routeur par défaut, mais avec une préférence faible. De plus, le routeur d'entreprise devrait annoncer un chemin spécifique pour le préfixe spécifique du site d'entreprise. Le résultat net est que les destinations dans le réseau d'entreprise seront accessibles via le tunnel, et les destinations générales de l'Internet seront accessibles via le fournisseur d'accès Internet de rattachement. Sans ces mécanismes, la machine de rattachement pourrait choisir d'envoyer le trafic Internet dans le réseau d'entreprise ou le trafic d'entreprise dans l'Internet, conduisant à l'échec des communications à cause du pare-feu.

On notera que l'administrateur de réseau qui règle les préférences et/ou les chemins plus spécifiques dans les annonces d'acheminement ne sait normalement pas quelles sortes de nœuds (type A, B, et/ou C) seront connectés à ses liaisons. Cela exige que l'administrateur configure les réglages qui vont fonctionner de façon optimale sans considération de la sorte de nœuds qui y seront rattachés. Voici deux exemples de la façon de le faire.

5. Exemples

5.1 Meilleur routeur pour `::/0` contre routeur le moins probable pour rediriger

Le meilleur routeur pour le chemin par défaut est le routeur avec le meilleur chemin vers l'Internet le plus large. Le routeur qui a la plus faible probabilité de rediriger le trafic dépend de l'usage du trafic réel. Les deux concepts peuvent être différents lorsque la majorité des communications a besoin en fait de passer par un autre routeur.

Par exemple, considérons une situation dans laquelle on a une liaison avec deux routeurs, X et Y. Le routeur X est le meilleur pour `2002::/16` (c'est notre passerelle de site `6à4`). Le routeur Y est le meilleur pour `::/0` (il connecte à l'Internet IPv6 natif). Le routeur X transmet le trafic IPv6 natif au routeur Y ; le routeur Y transmet le trafic `6à4` au routeur X. Si la plupart du trafic provenant de ce site est envoyé aux destinations `2002::/16`, le routeur X est celui qui a le moins de chances de rediriger.

Pour faire bien fonctionner les hôtes de type A, les deux routeurs devraient s'annoncer comme routeurs par défaut. En particulier, si le routeur Y tombe en panne, les hôtes de type A devraient envoyer le trafic au routeur X pour conserver la connectivité `6à4`, donc le routeur X et le routeur Y doivent être des routeurs par défaut.

Pour faire bien fonctionner les hôtes de type B, le routeur X devrait s'annoncer avec une haute préférence de routeur par défaut. Cela va amener les hôtes de type B à préférer le routeur X, minimisant le nombre de redirections.

Pour faire bien fonctionner les hôtes de type C, le routeur X devrait de plus annoncer le chemin `::/0` avec une préférence faible et le chemin `2002::/16` avec une préférence moyenne. Un hôte de type C va finir avec trois chemins dans son tableau d'acheminement : `::/0 -> routeur X` (faible), `::/0 -> routeur Y` (moyenne), `2002::/16 -> routeur X` (moyenne). Il va envoyer le trafic `6à4` au routeur X et les autres trafics au routeur Y. Les hôtes de type C ne causeront aucune redirection.

Noter que lorsque les hôtes de type C traitent l'annonce de routeur provenant du routeur X, la préférence faible pour `::/0` outrepassa la préférence haute de routeur par défaut. Si le chemin spécifique `::/0` n'était pas présent, un hôte de type C appliquerait alors la préférence de routeur par défaut de haute à son chemin `::/0` vers le routeur X.

5.2 Hôte multi rattachement et réseau isolé

Dans un autre scénario, un hôte multi rattachement est connecté à l'Internet via un routeur X sur une liaison et à un réseau isolé via un routeur Y sur une autre liaison. L'hôte multi rattachement peut avoir un tunnel dans un réseau d'entreprise protégé par un pare-feu, ou il peut être directement connecté à un réseau isolé.

Dans cette situation, un hôte multi rattachement de type A (qui n'a pas de préférence de routeur par défaut ni de chemin plus spécifique) n'aura aucun moyen de choisir intelligemment entre les routeurs X et Y sur sa liste des routeurs par défaut. Les utilisateurs de l'hôte vont voir des échecs de connectivité imprévisibles, selon l'adresse de destination et le choix du routeur.

Si les routeurs sont configurés de façon appropriée, un hôte de type B multi rattachements dans cette même situation aurait une connectivité Internet stable, mais n'aurait aucune connectivité avec le réseau d'essai isolé.

Si les routeurs sont configurés de façon appropriée, un hôte de type C multi rattachements dans cette même situation peut correctement choisir entre les routeurs X et Y. Par exemple, le routeur Y sur le réseau isolé devrait annoncer une option d'informations de chemin pour le préfixe de réseau isolé. Il pourrait ne pas du tout s'annoncer lui-même comme routeur par défaut (durée de vie de routeur de zéro) ou il pourrait s'annoncer comme routeur par défaut avec une préférence faible. Le routeur X devrait s'annoncer comme routeur par défaut avec la préférence moyenne.

6. Considérations sur la sécurité

Un nœud malveillant pourrait envoyer des messages d'annonce de routeur, spécifiant une préférence haute de routeur par défaut ou portant des chemins spécifiques, avec pour effet de tirer du trafic hors des routeurs légitimes. Cependant, un nœud malveillant pourrait facilement obtenir le même effet d'autres façons.

Par exemple, il pourrait fabriquer des messages d'annonce de routeur avec une durée de vie de routeur de zéro à partir des autres routeurs, causant l'arrêt par les hôtes de l'utilisation des autres chemins. En annonçant un préfixe spécifique, cette attaque pourrait être réalisée de façon à être moins remarquée. Cependant, cette attaque n'a pas d'impact significatif sur la sécurité de l'infrastructure de l'Internet.

Un nœud malveillant pourrait aussi inclure un durée de vie infinie dans une option d'informations de chemin, causant la persistance indéfinie du chemin. Une attaque similaire existe déjà avec l'option d'informations de préfixe dans la RFC 2461, où un nœud malveillant cause l'apparition d'un préfixe comme en liaison de façon infinie, résultant en un manque de connectivité si il ne l'est pas. À l'opposé, une durée de vie infinie dans une option d'informations de chemin va causer la poursuite infinie de la vérification de l'accessibilité d'un routeur, mais ne va pas résulter en un manque de connectivité.

De même, un nœud malveillant pourrait aussi essayer de surcharger les hôtes avec un grand nombre de chemins dans l'option d'informations de chemin, ou avec de très fréquentes annonces de chemins. Là encore, cette même attaque existe déjà avec les options d'informations de préfixes.

La [RFC3756] donne plus de détails sur les modèles de confiance, et dans le groupe de travail SEND sur la sécurisation des messages de découverte de routeur des travaux sont en cours qui vont régler ces problèmes.

7. Considérations relatives à l'IANA

Le paragraphe 2.3 définit une nouvelle option de découverte de voisin [RFC2461], l'option Informations de chemin, à qui a été allouée la valeur 24 au sein de l'espace de numérotation des formats d'option de découverte de voisin IPv6.

8. Remerciements

Les auteurs tiennent à remercier de leurs contributions Balash Akbari, Steve Deering, Robert Elz, Tony Hain, Bob Hinden, Christian Huitema, JINMEI Tatuya, Erik Nordmark, Pekka Savola, Kresimir Segaric, et Brian Zill. Les diagrammes de paquets sont déduits de la découverte de voisin [RFC2461].

9. 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](#))
- [RFC2461] T. Narten, E. Nordmark, W. Simpson, "[Découverte de voisins pour IP version 6](#) (IPv6)", décembre 1998. (Obsolète, voir [RFC4861](#)) (D.S.)
- [RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. (P.S.) (Obs., voir [RFC6275](#))

10. Références pour information

- [RFC2080] G. Malkin, R. Minnear, "[RIPng pour IPv6](#)", janvier 1997. (P.S.)
- [RFC2893] R. Gilligan, E. Nordmark, "Mécanismes de transition pour les hôtes et routeurs IPv6", août 2000. (Obs., voir [RFC4213](#))
- [RFC3056] B. Carpenter, K. Moore, "Connexion des [domaines IPv6 via des nuages IPv4](#)", février 2001. (P.S.)
- [RFC3756] P. Nikander, éd., "[Modèles de confiance et menaces](#) pour la découverte de voisin IPv6 (ND)", mai 2004. (Information)

Adresse des auteurs

Richard Draves
Microsoft Research
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 706 2268
mél : richdr@microsoft.com

Dave Thaler
Microsoft
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 703 8835
mél : dthaler@microsoft.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à 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 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 la Administrative Support Activity (IASA) de l'IETF