Groupe de travail Réseau
Request for Comments : 2894
Catégorie : En cours de normalisation

M. Crawford, Fermilab
août 2000
Traduction Claude Brière de L'Isle

Dénumérotation de routeur pour IPv6

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Note de l'IESG :
Le présent document définit des mécanismes pour informer un ensemble de routeurs des opérations de dénumérotation qu'ils vont effectuer, y compris un mode de fonctionnement dans des environnements dans lesquels le nombre exact de ces routeurs n'est pas connu. Une information fiable de tous les routeurs lorsque le nombre réel de routeurs est inconnu est un problème difficile. L'expérience de la mise en œuvre et du fonctionnement seront nécessaires pour pleinement comprendre les aspects d'applicabilité et d'adaptabilité des mécanismes définis dans ce document lorsque le nombre de routeurs est inconnu.

Résumé
La découverte de voisin IPv6 et l'autoconfiguration d'adresse rendent plus pratiques l'allocation initiale des préfixes d'adresse aux hôtes. À côté du problème de la survie des connexions à travers un événement de dénumérotation, ces deux mécanismes simplifient aussi la reconfiguration des hôtes lorsque l'ensemble des préfixes valides change.

Le présent document définit un mécanisme appelé dénumérotation de routeur (RR, *Router Renumbering*) qui permet de configurer les préfixes d'adresses sur les routeurs et de les reconfigurer presque aussi facilement que fonctionne la combinaison de la découverte de voisin et l'autoconfiguration d'adresse pour les hôtes. Il donne le moyen au gestionnaire de réseau de faire les mises à jour des préfixes utilisés et annoncés par les routeurs IPv6 sur tout un site.

Table des Matières

1. Vue fonctionnelle d'ensemble

Les paquets de commande de dénumérotation de routeur contiennent une séquence d'opérations de contrôle de préfixe (PCO, *Prefix Control Operation*). Chaque PCO spécifie une opération, un Match-Prefix, et zéro, un ou plusieurs Use-Prefix. Un routeur traite chaque PCO à la suite, vérifiant sur chacune de ses interfaces une adresse ou préfixe qui corresponde au Match-Prefix. Pour chaque interface sur laquelle est trouvée une correspondance, l'opération est appliquée. L'opération est ADD, CHANGE, ou SET-GLOBAL pour ordonner au routeur, respectivement d'ajouter le Use-Prefix à l'ensemble de préfixes configurés, retirer le préfixe qui correspond au Match-Prefix et le remplacer par le Use-Prefix, ou remplacer tous les préfixes de portée globale par le Use-Prefix. Si l'ensemble de Use-Prefix dans la PCO est vide, l'opération ADD ne fait rien et les deux autres se réduisent à des suppressions.

Des informations supplémentaires pour chaque Use-Prefix sont incluses dans l'opération de contrôle de préfixe : les durées de vie valide et préférée à inclure dans les options d'information de préfixe d'annonce de routeur [RFC2461], et les fanions L et A pour la même option, ou une indication qu'elles sont à copier du préfixe qui correspondait au Match-Prefix.

Il est possible d'ordonner aux routeurs de créer de nouveaux préfixes en combinant les Use-Prefix dans une PCO avec une portion du préfixe existant qui correspondait au Match-Prefix. Cela simplifie certaines opérations dont on estime qu'elles sont parmi les plus courantes. Pour chaque Use-Prefix, la PCO spécifie un certain nombre de bits qui devraient être copiés de l'adresse ou préfixe existant qui correspondait au Match-Prefix et ajoutés au use-prefix avant de configurer le nouveau préfixe sur l'interface. Les bits copiés sont zéro, un ou plusieurs bits des positions immédiatement après la longueur du Use-Prefix. Si des informations de sous-réseau sont dans la même portion des préfixes ancien et nouveau, cette synthèse permet à une seule opération de contrôle de préfixe de définir un nouveau préfixe global sur chaque routeur d'un site, tout en préservant la structure de sous-réseau.

À cause de la puissance du mécanisme de dénumérotation de routeur, chaque message RR comporte un numéro de séquence pour se garder contre les répétitions, et il doit être authentifié et son intégrité doit être vérifiée. Chaque opération de contrôle de préfixe est idempotente et pourrait ainsi être retransmise pour améliorer la fiabilité, tant que le numéro de séquence est en cours, sans se soucier de traitements multiples. Cependant, des combinaisons non idempotentes de PCO peuvent facilement être construites et des messages contenant de telles combinaisons ne pourraient pas être retraités en toute sécurité. Donc, il est exigé de tous les routeurs qu'ils se préservent contre le traitement plus d'une fois du message RR. Pour permettre une vérification fiable que les commandes ont été reçues et traitées par les routeurs, un mécanisme est inclus pour la notification de commande dupliquée à la station de gestion.

Un gestionnaire de réseau pourrait éventuellement vouloir effectuer plus de dénumérotation, ou exercer un contrôle plus détaillé, que ce que peut exprimer un seul paquet de dénumérotation de routeur sur le support disponible. Le mécanisme RR est très puissant lorsque les paquets RR sont en diffusion groupée, de sorte que la fragmentation IP est indésirable. Pour cette raison, chaque paquet RR contient un "numéro de segment". Tous les paquets RR qui ont un numéro de séquence supérieur ou égal à la plus forte valeur vue sont valides et doivent être traités. Cependant, un routeur doit garder trace des numéros de segment des messages RR déjà traités et éviter de retraiter un message dont le numéro de séquence et le numéro de segment correspondent à un message traité antérieurement. (Cette liste de numéros de segment traités est remise à zéro lorsque est vu un plus fort numéro de séquence.)

Le numéro de segment n'impose pas d'ordre au traitement des paquets. Si on désire une séquence spécifique des opérations, elle peut être réalisée en ordonnant les PCO en un seul message de commande RR ou par le champ Numéro de séquence.

Il y a un fanion "Essai" qui indique que tous les routeurs devraient simuler le traitement du message RR et ne pas effectuer une reconfiguration réelle. Un fanion "Rapport" distinct ordonne aux routeurs de renvoyer un message Résultat de dénumérotation de routeur à la source de la commande RR pour indiquer le résultat réel ou simulé des opérations du message de commande RR.

L'effet ou l'effet simulé d'un message de commande RR peut aussi faire l'objet d'un rapport au gestionnaire du réseau par de moyens qui sortent du domaine d'application du présent document, concernant la valeur du fanion "Rapport".

2. Définitions

2.1 Terminologie

Adresse
Ce terme se réfère toujours à une adresse IPv6 de 128 bits [RFC2373]. Lorsque on se réfère aux bits au sein d'une adresse, ils sont numérotés de 0 à 127, le bit 0 étant le premier bit du préfixe Format.

Préfixe
Un préfixe peut être vu comme une adresse plus une longueur, cette dernière étant un entier dans la gamme de 0 à 128, qui indique combien de bits de tête sont significatifs. Lorsque on se réfère aux bits au sein d'un préfixe, ils sont numérotés de la même façon que les bits d'une adresse. Par exemple, les bits significatifs d'un préfixe de longueur L sont les bits numérotés de 0 à L-1, inclus.

Correspondance
Une adresse A "correspond" à un préfixe P dont la longueur est L si les L premiers bits de A sont identiques aux L premiers bits de P. (Chaque adresse correspond à un préfixe de longueur 0.) Un préfixe P1 de longueur L1 correspond à un préfixe P2 de longueur L2 si L1 ≥ L2 et si les L2 premiers bits de P1 et P2 sont identiques.

Opération de contrôle de préfixe
C'est la plus petite unité individuelle d'opération de dénumérotation de routeur. Un paquet de commande de dénumérotation de routeur comporte zéro, une ou plusieurs d'entre elles, chacune comportant une condition correspondante, appelée partie Match-Prefix, et zéro, une ou plusieurs spécifications de substitution, appelées parties Use-Prefix.

Match-Prefix
C'est un préfixe auquel un routeur compare les adresses et les préfixes configurés à ses interfaces.

Use-Prefix
C'est le préfixe et les informations associées qui sont à configurer à une interface de routeur lorsque certaines conditions sont satisfaites.

Préfixe satisfait
C'est le préfixe ou adresse existant qui a satisfait à un Match-Prefix.

Nouveau préfixe
C'est un préfixe construit à partir d'un Use-Prefix, incluant éventuellement certains des préfixes satisfaits.

Numéro de séquence enregistré
Le plus fort numéro de séquence trouvé dans un message DOIT être enregistré dans une mémoire non volatile.

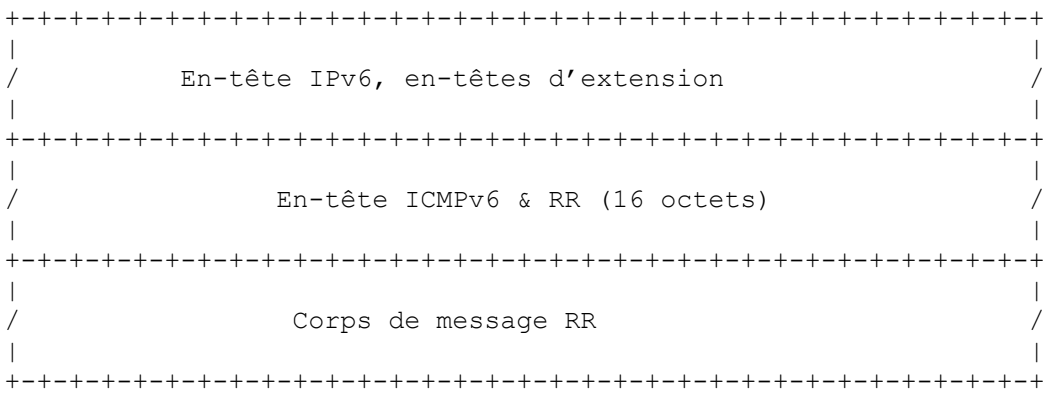
Noter que "correspondance" est une relation transitive mais non symétrique. Si deux préfixes correspondent l'un à l'autre, ils sont identiques.

2.2 Exigences

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Format de message

Il y a deux types de messages de dénumérotation de routeur : les commandes, qui sont envoyées aux routeurs, et les résultats, qui sont envoyés par les routeurs. Un troisième type de message est utilisé pour synchroniser un rétablissement de numéro de séquence enregistré avec l'annulation de clés de chiffrement. Les trois types de messages sont distingués par le champ "Code" ICMPv6 et diffèrent par le contenu du champ "Corps de message".



Format du message de dénumérotation de routeur

Les messages de dénumérotation de routeur sont portés dans les paquets ICMPv6 avec le type = 138. Le message RR comporte un en-tête RR, qui contient l'en-tête ICMPv6, les numéros de séquence et de segment et d'autres informations, et le corps de message RR, de longueur variable.

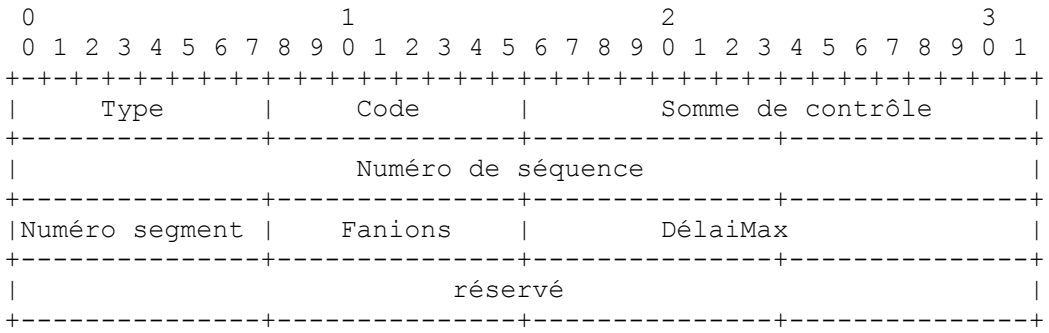
Tous les champs marqués "réservé" ou "res" DOIVENT être réglés à zéro à l'émission d'un message RR, et ignorés à réception.

Toutes les mises en œuvre qui génèrent des messages de commande de dénumérotation de routeur DOIVENT prendre en charge leur envoi à l'adresse de diffusion groupée Tous routeurs avec des portées de liaison et de site, et aux adresses d'envoi individuel de format liaison locale et site local. Tous les routeurs DOIVENT être capables de recevoir les commandes RR envoyées à ces adresses de diffusion groupée et à toutes leurs adresses d'envoi individuel de liaison locale et de site local. Les mises en œuvre DEVRAIENT prendre en charge l'envoi et la réception des messages RR adressés aux autres adresses d'envoi individuel. Une mise en œuvre qui est à la fois envoyeur et receveur de commandes RR DEVRAIT prendre en charge l'utilisation de l'adresse d'envoi en diffusion groupée Tous routeurs avec portée de nœud.

L'authentification des données et la protection de l'intégrité de message DOIVENT être fournies pour tous les messages de commande de dénumérotation de routeur par les moyens appropriés de sécurité IP [RFC2401]. L'assurance de l'intégrité doit inclure l'adresse de destination IPv6, l'en-tête RR et le corps de message. Voir la section 7, "Considérations pour la sécurité".

L'utilisation de l'authentification pour les messages de résultat de dénumérotation de routeur est RECOMMANDÉE.

3.1 En-tête de dénumérotation de routeur



Champs :
Type : 138 (décimal) ; valeur du type ICMPv6 allouée à la dénumérotation de routeur

Code : 0 pour une commande de dénumérotation de routeur
1 pour un résultat de dénumérotation de routeur
255 pour une remise à zéro de numéro de séquence (décrite à la section 5).

Somme de contrôle : somme de contrôle ICMPv6, comme spécifié dans la [RFC2463]. La somme de contrôle couvre le pseudo en-tête IPv6 et tous les champs du message RR à partir du champ Type.

Numéro de séquence : entier non signé de 32 bits. Le numéro de séquence DOIT être non décroissant entre les remises à zéro de numéro de séquence.

Numéro de segment : champ d'entier non signé de 8 bits qui numérote les différents messages RR valides ayant le même numéro de séquence. Aucun ordre des messages RR n'est imposé par le numéro de segment.

Fanions : combinaison de fanions de un bit. Cinq sont définis et trois sont réservés.

Les fanions T, R, A et S ont une signification définie dans un message de commande RR. Dans un message Résultat, ils DOIVENT être copiés de la commande correspondante. Le fanion P n'a de signification que dans un message Résultat et DOIT être à zéro dans une commande émise et ignoré dans une commande reçue.

T commande d'essai
0 indique que la configuration du routeur est à modifier ;
1 indique un message "Essai" : le traitement doit être simulé et aucun changement de configuration n'est à faire.

R Résultat exigé
0 indique qu'un message Résultat NE DOIT PAS être envoyé (mais d'autres formes d'enregistrement ne sont pas exclues) ;
1 indique que le routeur DOIT envoyer un message Résultat à l'achèvement du traitement du message Commande.

A Toutes interfaces
0 indique que la commande NE DOIT PAS être appliquée aux interfaces qui sont fermées administrativement ;
1 indique que la commande DOIT être appliquée à toutes les interfaces sans considération du statut de fermeture administrative.

S Site spécifique : ce fanion DOIT être ignoré sauf si le routeur traite les interfaces comme appartenant à des "sites" différents.
0 indique que la commande DOIT être appliquée aux interfaces sans considération du site auquel elles appartiennent ;
1 indique que la commande DOIT être appliquée aux seules interfaces qui appartiennent au même site que l'interface à laquelle la commande est adressée. Si l'adresse de destination est appropriée pour les interfaces qui appartiennent à plus d'un site, la commande DOIT alors être appliquée seulement aux interfaces qui appartiennent au même site que l'interface sur laquelle la commande a été reçue.

P *(Processed previously)* Traité précédemment
0 indique que le message Résultat contient le rapport complet du traitement de la commande ;
1 indique que le message Commande a été traité précédemment (et n'est pas un essai) et que le routeur qui répond ne le traite pas à nouveau. Ce message Résultat PEUT avoir un corps vide.

DélaiMax : champ d'entier non signé de 16 bits qui spécifie le délai maximum, en millisecondes, dont un routeur DOIT retarder l'envoi de toute réponse à cette commande. Les mises en œuvre PEUVENT générer un retard aléatoire entre 0 et DélaiMax millisecondes avec une granularité plus fine que 1 ms.

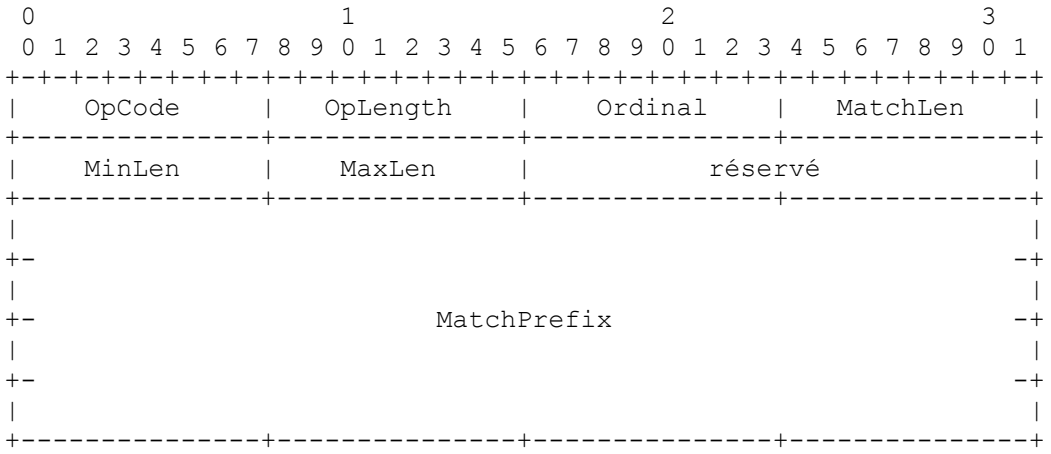
3.2 Corps de message – message de commande

Le corps d'un message Commande RR est une séquence de zéro, une ou plusieurs opérations de contrôle de préfixe, chacune étant de longueur variable. La fin de la séquence PEUT être déduite de la longueur IPv6 et des longueurs des en-têtes d'extension qui précèdent l'en-tête ICMPv6.

3.2.1 Opération de contrôle de préfixe

Une opération de contrôle de préfixe a une partie Match-Prefix de 24 octets, suivie par zéro, une ou plusieurs parties Use-Prefix de 32 octets chacune.

3.2.1.1 Partie Match-Prefix



Champs :

OpCode : entier non signé de 8 bits qui spécifie l'opération à effectuer lorsque le MatchPrefix associé correspond à l'adresse ou préfixe d'une interface. Les valeurs sont :
1 : opération ADD
2 : opération CHANGE
3 : opération SET-GLOBAL

OpLength : longueur totale de cette opération de contrôle de préfixe, en unités de 8 octets. Une OpLength valide va toujours être de la forme 4N+3, avec N égal au nombre de parties UsePrefix (éventuellement zéro).

Ordinal champ de 8 bits qui DOIT avoir une valeur différente dans chaque opération de contrôle de préfixe contenue dans un certain message Commande RR. Il n'y a pas d'autre contrainte sur la valeur.

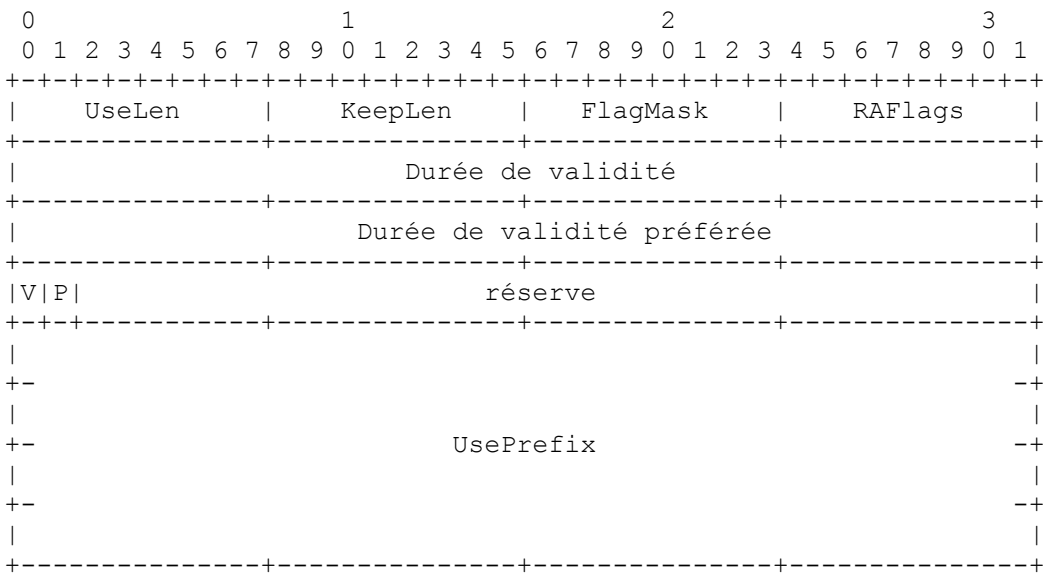
MatchLen entier non signé de 8 bits entre 0 et 128 inclus qui spécifie le nombre de bits initiaux du MatchPrefix qui sont significatifs dans la correspondance.

MinLen entier non signé de 8 bits qui spécifie la longueur minimum que tout préfixe configuré doit avoir afin d'être éligible à la confrontation à MatchPrefix.

MaxLen entier non signé de 8 bits qui spécifie la longueur maximum que doit avoir tout préfixe configuré afin d'être éligible à la confrontation à MatchPrefix.

MatchPrefix préfixe de 128 bits à comparer au préfixe ou adresse de chaque interface.

3.2.1.2 Partie Use-Prefix



Champs :

UseLen entier non signé de 8 bits inférieur ou égal à 128 qui spécifie le nombre de bits initiaux de UsePrefix à utiliser pour créer un nouveau préfixe pour une interface.

KeepLen entier non signé de 8 bits inférieur ou égal à (128 - UseLen) qui spécifie le nombre de bits du préfixe ou adresse qui correspondent au Match-Prefix associé qui devraient être conservés dans le nouveau préfixe. Les bits conservés sont ceux des positions de UseLen à (UseLen+KeepLen - 1) dans l'adresse ou préfixe qui correspond, et ils sont copiés sur les mêmes positions dans le nouveau préfixe.

FlagMask gabarit de 8 bits. Un bit 1 dans toute position signifie que le bit fanion correspondant dans une option d'information de préfixe d'annonce de routeur (RA, *Router Advertisement*) devrait être établi à partir du champ RAFlags dans cette partie Use-Prefix. Un bit 0 dans le FlagMask signifie que le bit fanion RA pour le nouveau préfixe devrait être copié du bit fanion RA correspondant du préfixe satisfait.

RAFlags champ de 8 bits qui, sous le contrôle du champ FlagMask, peut être utilisé pour initialiser les fanions dans les options d'information de préfixe d'annonce de routeur [RFC2461] qui annonce le nouveau préfixe. Noter que seuls deux fanions ont une signification définie aujourd'hui : les fanions L (en-liaison) et A (configuration autonome). Ces fanions occupent les deux positions des bit les plus à gauche dans le champ RAFlags, correspondant à leur position dans l'option d'information de préfixe.

Durée de validité entier non signé de 32 bits qui est le nombre de secondes pendant lequel le nouveau préfixe sera valide [RFC2461].

Durée de validité préférée entier non signé de 32 bits qui est le nombre de secondes pendant lequel le nouveau préfixe sera préféré [RFC2461].

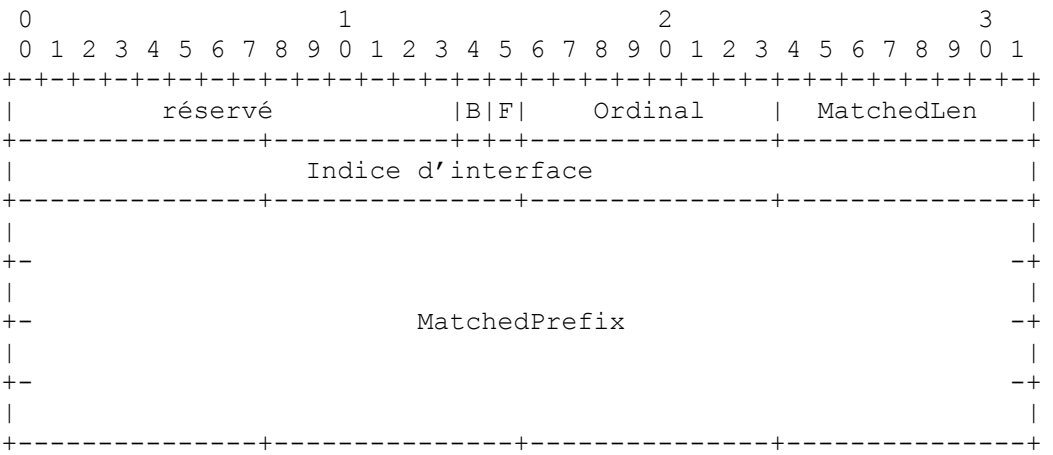
V fanion de 1 bit qui indique que la durée de validité du nouveau préfixe DOIT être effectivement décrémentée en temps réel.

P fanion de 1 bit qui indique que la durée de validité préférée du nouveau préfixe DOIT être effectivement décrémentée en temps réel.

UsePrefix le Use-prefix de 128 bits qui devient, ou est utilisé pour former (si KeepLen n'est pas zéro) le nouveau préfixe. Il NE DOIT PAS avoir la forme d'une adresse de diffusion groupée ou de liaison locale [RFC2373].

3.3 Corps de message – message de résultat

Le corps d'un message Résultat RR est une séquence de zéro, un ou plusieurs rapports de correspondance de 24 octets. Un message Commande RR avec le fanion "R" établi va obtenir un message Résultat RR contenant un rapport de correspondance pour chaque opération de contrôle de préfixe, pour chaque préfixe différent auquel il correspond sur chaque interface. Le rapport de correspondance a le format suivant :



Champs :

B fanion d'un bit qui, lorsque établi, indique qu'un ou plusieurs champs dans la PCO associée étaient hors limite. La vérification des limites est décrite au paragraphe 4.2.

F fanion d'un bit qui, lorsque établi, indique qu'une ou plusieurs parties Use-Prefix provenant de la PCO associée

n'ont pas été honorées par le routeur à cause d'une tentative de formation d'un format de préfixe interdit, tel qu'une adresse de diffusion groupée ou de bouclage.

Ordinal copié de la PCO dont le MatchPrefix correspondait au MatchedPrefix sur l'interface indiquée par InterfaceIndex.

MatchedLen longueur du préfixe satisfait.

InterfaceIndex désignation numérique par le routeur de l'interface sur laquelle MatchedPrefix a été configuré. Ce DOIT être la même que la valeur de ipv6IfIndex qui désigne cet indice dans le groupe général de la MIB IPv6 SNMP [RFC2466].

Il est possible qu'un message Résultat soit plus grand que le message Commande qui l'obtient. Un tel message Résultat peut devoir être fragmenté pour la transmission. Si il en est ainsi, il DEVRAIT être fragmenté au minimum exigé de la MTU IPv6 [RFC2460].

4. Traitement du message

Le traitement des messages de résultat de dénumérotation de routeur reçus est entièrement défini par la mise en œuvre. Une mise en œuvre de traitement d'un message Commande peut varier par les détails de la procédure établie ci-après, pour autant que le résultat n'est pas affecté.

Le traitement des messages de commande de dénumérotation de routeur reçus consiste en trois parties conceptuelles : la vérification de l'en-tête, la vérification des limites, et l'exécution.

4.1 Vérification d'en-tête

La somme de contrôle et le type ICMPv6 sont supposés avoir été vérifiés avant qu'un module de dénumérotation de routeur reçoive une commande à exécuter. Dans un environnement de mise en œuvre où ce pourrait n'être pas le cas, ces vérifications DOIVENT être faites à ce moment du traitement.

Si la longueur ICMPv6 déduite de la longueur IPv6 est inférieure à 16 octets, le message DOIT être éliminé et DEVRAIT faire l'objet d'une signalisation à la gestion de réseau.

Si le champ Code ICMPv6 indique un message Résultat, un routeur qui n'est pas source de messages Commande RR DOIT éliminer le message et NE DEVRAIT PAS le signaler à la gestion du réseau.

Si l'adresse de destination IPv6 n'est ni l'adresse de diffusion groupée Tous routeurs de la [RFC2373] ni une des adresses d'envoi individuel du routeur receveur, le message DOIT être éliminé et DEVRAIT faire l'objet d'une signalisation à la gestion de réseau.

Ensuite, le numéro de séquence est comparé au numéro de séquence enregistré. (Si aucun message RR n'a été reçu ni accepté depuis l'initialisation du système, le numéro de séquence enregistré est zéro.) Cette comparaison est faite avec les deux numéros considérés comme des entiers non signés, et non comme des numéros de série du style DNS. Si le numéro de séquence est inférieur au numéro de séquence enregistré, le message DOIT être éliminé et DEVRAIT faire l'objet d'une signalisation à la gestion de réseau.

Finalement, si le numéro de séquence dans le message est supérieur au numéro de séquence enregistré ou si le fanion T est établi, sauter la vérification des limites. Autrement, le numéro de segment DOIT maintenant être vérifié. Si un message correctement authentifié avec le même numéro de séquence et le même numéro de segment n'a pas déjà été traité, passer à la vérification de limites. Autrement, cette commande est un double est non une commande d'essai. Si le fanion R n'est pas établi, le message dupliqué DOIT être éliminé et NE DEVRAIT PAS faire l'objet d'une signalisation à la gestion de réseau. Si R est établi, un message Résultat RR avec le fanion P établi DOIT être programmé pour transmission à l'adresse de source de la commande après un délai aléatoire uniformément distribué entre 0 et DélaiMax millisecondes. Le corps de ce message Résultat DOIT soit être vide, soit être une copie sauvegardée du corps du message Résultat générée par le traitement du message précédent avec les mêmes numéro de séquence et numéro de segment. Après la programmation du message Résultat, la commande DOIT être éliminée sans autre traitement.

4.2 Vérification des limites

Si le numéro de séquence est supérieur au numéro de séquence enregistré, alors la liste des numéros de segment traités et

l'ensemble des messages Résultat sauvegardés, s'il en est, DOIVENT être éliminés et le numéro de séquence enregistré DOIT être mis à jour à la valeur utilisée dans le message en cours, sans considération des erreurs de traitement.

Ensuite, si le champ Code ICMPv6 indique une remise à zéro du numéro de séquence, passer à la section 5.

À ce point, si T est établi dans l'en-tête RR et si R n'est pas établi, le message PEUT être éliminé sans autre traitement.

Si le fanion R est établi, commencer à construire un message Résultat RR. L'en-tête RR du message Résultat est complètement déterminé à ce moment, sauf la somme de contrôle.

Les valeurs des champs suivants d'une PCO DOIVENT être vérifiés pour s'assurer qu'ils sont dans les limites appropriées :

OpCode doit avoir une valeur définie.

OpLength doit être de la forme 4N+3 et être cohérent avec la longueur du paquet Commande et le décalage de la PCO au sein du paquet.

MatchLen doit être entre 0 et 128 inclus.

UseLen, KeepLen dans chaque partie Use-Prefix doit être entre 0 et 128 inclus, comme doit l'être la somme des deux.

Si un de ces champs est hors gamme dans une PCO, la PCO entière NE DOIT être effectuée sur aucune interface. Si le fanion R est établi dans l'en-tête RR on ajoute alors au message RR Résultat un rapport de correspondance avec le fanion B établi, le fanion F à zéro, le champ Ordinal copié de la PCO, et tous les autres champs à zéro. Ce rapport de correspondance DOIT être inclus une seule fois, et non une fois par interface.

Noter que les limites de MinLen et MaxLen n'ont pas besoin d'être explicitement vérifiées, même si certaines combinaisons de valeurs vont rendre toute correspondance impossible.

4.3 Exécution

Pour chaque interface de routeur applicable, comme il est déterminé par les fanions A et S, les opérations de contrôle de préfixe dans un message de commande RR doivent être effectuées dans l'ordre de leur apparition. L'ordre relatif du traitement des PCO parmi les différentes interfaces n'est pas spécifié.

Si le fanion T est établi, créer une copie de chaque configuration d'interface sur laquelle opérer, parce que le résultat du traitement d'une PCO peut affecter le traitement des PCO suivantes. Noter que si toutes les opérations sont effectuées sur une interface avant de traiter une autre interface, seule une copie de configuration d'interface sera exigée à la fois.

Pour chaque interface et pour chaque opération de contrôle de préfixe, chaque préfixe configuré sur cette interface avec une longueur d'une valeur entre MinLen et MaxLen dans la PCO est vérifiée pour déterminer si elle correspond (comme défini au paragraphe 2.1) au MatchPrefix de la PCO. Les préfixes configurés sont vérifiés dans un ordre arbitraire. Tout nouveau préfixe configuré sur une interface par l'effet d'une certaine PCO NE DOIT PAS être vérifié contre cette PCO, mais DOIT être vérifié par rapport à toutes les PCO suivantes dans le même message de commande RR.

Sous certaines conditions, les adresses sur une interface sont aussi vérifiées pour voir si une d'entre elles correspond au MatchPrefix. Si, et seulement si, un préfixe configuré "P", ayant une longueur entre MinLen et MaxLen inclus, ne correspond pas au MatchPrefix "M", mais si M correspond bien à P (cela peut arriver si M est plus long que P) alors ces adresses sur cette interface qui correspond à P DOIVENT être vérifiées pour déterminer si une d'entre elles correspond à M. Si une de ces adresses correspond bien à M, traiter la PCO comme si P correspondait à M, mais lorsque on forme de nouveaux préfixes, si KeepLen est différent de zéro, les bits sont copiés de l'adresse. Ce cas particulier permet à une PCO d'être facilement ciblée sur une seule interface spécifique dans un réseau.

Si P ne correspond pas à M, le traitement est terminé pour cette combinaison de PCO, interface et préfixe. On continue avec un autre préfixe sur la même interface si il y a d'autres préfixes qui n'ont pas été vérifiés par rapport à cette PCO et n'ont pas été créés par l'action de cette PCO. Si il ne reste plus de tels préfixes sur l'interface en cours, on continue le traitement avec la PCO suivante sur la même interface, ou avec une autre interface.

Si P correspond à M, soit directement, soit parce qu'une adresse configurée qui correspond à P correspond aussi à M, P est alors le préfixe correspondant. On effectue les étapes suivantes.

Si la commande a le fanion R établi, ajouter un rapport de correspondance au message Résultat en cours de construction.

Si le OpCode est CHANGE, marquer P à supprimer de l'interface en cours.

Si le OpCode est SET-GLOBAL, marquer à supprimer tous les préfixes de portée globale sur l'interface en cours.

Si il y a des parties Use-Prefix dans la PCO en cours, former les nouveaux préfixes. Éliminer tout nouveau préfixe qui a un format interdit, et si le fanion R est établi dans la commande, établir le fanion F dans le rapport de correspondance pour cette PCO et cette interface. Les formats de préfixe interdit incluent, au minimum, les adresses de diffusion groupée, les adresses inspécifiées et de bouclage [RFC2373]. Toute mise en œuvre PEUT interdire, ou permettre au gestionnaire de réseau d'interdire aussi les autres formats.

Pour chaque nouveau préfixe qui est déjà configuré sur l'interface courante, ôter le marquage "à supprimer" du préfixe et mettre à jour la durée de vie et les fanions RA. Pour chaque nouveau préfixe qui n'est pas déjà configuré, ajouter le préfixe et, si c'est approprié, configurer une adresse avec ce préfixe.

Supprimer tout préfixe qui serait encore marqué "à supprimer", ainsi que toute adresse qui correspondrait à ces préfixes mais pas à un préfixe qui ne serait pas marqué "à supprimer".

Après traitement de toutes les opérations de contrôle de préfixe sur toutes les interfaces, une mise en œuvre DOIT enregistrer le numéro de segment du paquet dans une liste associée au numéro de séquence.

Si la commande a le fanion R établi, calculer la somme de contrôle et programmer la transmission du message Résultat après un intervalle de temps aléatoire uniformément distribué entre 0 et DélaiMax millisecondes. Cet intervalle DEVRAIT commencer à la conclusion du traitement, et non à son début. Une copie du message Résultat PEUT être sauvegardée pour être retransmise en réponse à une commande dupliquée.

4.4 Résumé des effets

Les seuls paramètres de découverte de voisin [RFC2461] qui puissent être affectés par la dénumérotation de routeur sont les suivants :

- Les adresses et les préfixes annoncés d'un routeur, y compris les longueurs de préfixe.

- Les bits fanions (L et A, et tous ceux qui pourraient être définis à l'avenir) et les durées de validité et de validité préférée qui apparaissent dans une option d'information de préfixe d'annonce de routeur.

- La propriété non désignée des durées de vie qui spécifie si ce sont des valeurs fixes ou des valeurs décrémentées en temps réel.

Les autres informations internes de routeur, comme le temps jusque à la prochaine annonce de routeur non sollicitée ou les variables de MIB qui PEUVENT être affectées en tant que de besoin.

Tous les changements de configuration résultant de la dénumérotation de routeur DEVRAIENT être sauvegardés dans une mémorisation non volatile où cette facilité existe. Le problème de la restauration appropriée des durées de vie de préfixe à partir d'une mémorisation non volatile existe indépendamment de la dénumérotation de routeur et mérite une grande attention, mais sort du domaine d'application du présent document.

5. Rétablissement de numéro de séquence

Il peut se révéler nécessaire en pratique de rétablir le numéro de séquence enregistré d'un routeur. Ce n'est une opération sûre que lorsque toutes les clés de chiffrement utilisées précédemment pour authentifier les commandes RR sont arrivées à expiration ou ont été révoquées. Pour cette raison, le message de remise à zéro de numéro de séquence est défini pour accomplir ces deux fonctions.

Lorsque une remise à zéro de numéro de séquence (SNR, *Sequence Number Reset*) a été authentifiée et a réussi la vérification d'en-tête, le routeur DOIT invalider toutes les clés qui avaient été utilisées pour authentifier les commandes RR précédentes, y compris la clé qui a authentifié la SNR elle-même. Il DOIT ensuite éliminer tous les messages Résultat RR sauvegardés, éliminer la liste des numéros de segment enregistrée et remettre le numéro de séquence enregistré à zéro.

Si le routeur n'a pas d'autre clé d'authentification inutilisée déjà disponible pour que la dénumérotation de routeur l'utilise, il DEVRAIT établir une ou plusieurs nouvelles clés valides. Les détails de ce processus vont dépendre de si on utilise un

chiffrement manuel ou un protocole de gestion de clé. Dans l'un et l'autre cas, si aucune clé n'est disponible, aucune nouvelle commande ne peut être traitée.

Un message SNR DEVRAIT ne contenir aucune PCO, car elle serait ignorée. Si et seulement si le fanion R est établi dans le message SNR, un routeur DOIT répondre par un message Résultat ne contenant pas de rapport de correspondance. L'en-tête et la transmission du Résultat sont décrits à la Section 3.

L'invalidation des clés d'authentification causée par un message SNR valide va faire que les copies retransmises de ce message seront ignorées.

6. Considérations relatives à l'IANA

Suivant les politiques mentionnées dans la [RFC2434], de nouvelles valeurs du champ Code dans l'en-tête Dénumérotation de routeur (paragraphe 3.1) et le champ OpCode de la partie Match-Prefix (paragraphe 3.2.1.1) sont à allouer uniquement par consensus de l'IETF.

7. Considérations pour la sécurité

Le mécanisme de dénumérotation de routeur proposé ici est très puissant et la prévention de l'usurpation d'identité est importante. La répétition de vieux messages doit, en général, être empêchée (même si une petite classe de messages existe pour laquelle la répétition serait sans dommage). Ce qui constitue un algorithme d'authentification suffisamment fort peut changer avec le temps, mais les algorithmes devraient être choisis pour être assez forts contre les attaques courantes de récupération de clés et de contrefaçon.

Les clés d'authentification doivent être aussi bien protégées que toute autre méthode d'accès qui permet la reconfiguration des routeurs d'un site. La distribution des clés ne doit pas les exposer ou permettre leur altération, et la validité des clés doit être limitée en termes de temps et de nombre de messages authentifiés.

Noter que bien que la remise à zéro du numéro de séquence enregistré exige l'annulation des clés d'authentification utilisées précédemment, l'introduction de nouvelles clés et l'expiration des vieilles clés n'exige pas de remettre à zéro le numéro de séquence enregistré.

7.1 Politique de sécurité et entrées de base de données d'association

La base de données de sécurité (SPD, *Security Policy Database*) [RFC2401] d'un routeur qui met en œuvre la présente spécification DOIT causer l'élimination des paquets entrants de commande de dénumérotation de routeur ou l'application de IPsec. (La détermination de "éliminer" ou "appliquer" PEUT se fonder sur l'adresse de source.) Les entrées résultantes de base de données d'association de sécurité (SAD, *Security Association Database*) DOIVENT assurer l'authentification et la protection d'intégrité de l'adresse de destination, de l'en-tête RR et du corps de message, et la longueur du corps impliquée par la longueur IPv6 et les en-têtes d'extension présents. Ces exigences sont satisfaites par l'utilisation de l'en-tête d'authentification [RFC2402] en mode transport ou tunnel, ou de l'encapsulation de charge utile de sécurité [RFC2406] en mode tunnel avec l'authentification non NULLE. L'algorithme d'authentification IPsec de mise en œuvre obligatoire (autre que NUL) semble assez fort pour la dénumérotation de routeur au moment de cette rédaction.

Noter que, pour que SPD distingue la dénumérotation de routeur des autres paquets ICMP, cela exige l'utilisation du champ Type ICMP comme sélecteur. Ceci est cohérent, bien qu'elle ne le mentionne pas, avec la spécification de l'architecture de sécurité [RFC2401].

Au moment de cette rédaction, il n'existe pas de protocole de gestion de clé de diffusion groupée pour IPsec et aucun n'est en préparation. Des associations de sécurité configurées manuellement vont donc être de règle. L'occurrence de "de trafic" dans le tableau ci-dessous serait donc plus réaliste avec un caractère générique ou une gamme fixe. L'utilisation d'un petit ensemble de clés partagées par station de gestion suffit, pour autant que la distribution et la mémorisation des clés soient suffisamment sécurisées.

Un ensemble suffisant d'entrées de SPD pour le trafic entrant pourrait retenir :

Champ	entrée de SPD	entrée de SAD
Source	caractère générique	de trafic
Destination	caractère générique	de SPD
Transport	ICMPv6	de SPD
Type ICMP	Rtr. Renum	de SPD
Action	Appliquer IPsec	
SA Spec	Mode AH/transport	

ou il pourrait y avoir une entrée pour chaque station de gestion et/ou pour chaque adresse d'envoi individuel du routeur et pour chaque adresse de diffusion groupée Tous routeurs définie, et une entrée finale de caractère générique pour éliminer tous les autres messages RR entrants.

La SPD et la SAD sont des bases de données conceptuelles par interface. Ce fait peut être exploité pour permettre une gestion partagée d'un routeur frontière, par exemple, ou pour éliminer tout le trafic de dénumérotation de routeur qui arrive sur des tunnels.

8. Conseils de mise en œuvre et d'usage pour la fiabilité

Les utilisateurs de la dénumérotation de routeur (RR) vont vouloir être sûrs que chaque message non trivial atteint chacun des routeurs prévus. L'exploitation bien considérée des caractéristiques de retransmission et de direction de réponse de la dénumérotation de routeur devrait rendre cet objectif réalisable avec un fort degré de confiance même dans un réseau d'une fiabilité minimale.

Dans un certain nombre de cas, probablement la majorité, la station de gestion du réseau va connaître l'ensemble complet des routeurs sous son contrôle. Les commandes peuvent être retransmises, avec le fanion "R" (Réponse exigée) établi dans l'en-tête RR, jusqu'à ce que des résultats aient été collectés de tous les routeurs. Si des associations de sécurité en envoi individuel (ou les moyens de les créer) sont disponibles, la station de gestion peut passer de la transmission en diffusion groupée à l'envoi individuel lorsque le nombre de routeur non encore entendus est convenablement faible.

Pour conserver une liste des routeurs gérés, la station de gestion peut employer une des différentes méthodes automatiques qui peuvent être plus pratiques que l'entrée manuelle dans un grand réseau. Les commandes RR "Essai" en diffusion groupée peuvent être envoyées périodiquement et leurs résultats archivés, ou bien la station de gestion peut utiliser SNMP pour "parler" dans un protocole d'acheminement d'état de liaison tel que OSPF [RFC1850]. (Dans le cas de OSPF, en gros un routeur par zone devrait être examiné pour construire une liste complète des routeurs.)

Dans un grand réseau dynamique où l'ensemble des routeurs gérés n'est pas connu mais où on désire une exécution fiable, on décrit une méthode adaptable pour réaliser la confiance dans la livraison. Rien dans cette section n'affecte le format ou le contenu des messages de dénumérotation de routeur, ni leur traitement par les routeurs.

Une station de gestion qui met en œuvre ces mécanismes de fiabilité DOIT alerter un opérateur qui tente de commencer un ensemble de commandes de dénumérotation de routeur lors de la retransmission non achevée d'un jeu précédent, mais DEVRAIT permettre à l'opérateur d'outrepasser l'avertissement.

8.1 Aperçu et définitions

L'ensemble de routeurs gérés avec la dénumérotation de routeur est considéré comme un ensemble de populations, chaque population ayant une probabilité caractéristique d'aller-retour de livraison réussie d'une paire Commande/Résultat. L'objectif est d'estimer une limite inférieure, P, sur la probabilité d'aller-retour pour l'ensemble complet. Avec cette estimation et d'autres données sur les réponses aux retransmissions de la commande, un niveau de confiance peut être calculé pour l'hypothèse où tous les routeurs sont connus.

Si la vraie probabilité d'une communication aller-retour réussie avec un routeur géré était une constante, p, pour tous les routeurs gérés, une estimation P de p pourrait alors être déduite de l'une ou l'autre de ces statistiques :

Le ratio attendu Nombre de routeurs connus après (N + 1) transmissions sur Nombre de ceux connus après N est (1 - p).

Lorsque N différents routeurs sont connus après M transmissions d'une commande, le nombre total attendu de messages Résultat reçus est pNM. Si R est le nombre de Résultats en fait reçus, alors P = R/MN.

Les deux méthodes ne sont pas équivalentes. La première pose des problèmes numériques lorsque le nombre de routeurs restant à connaître devient faible, de sorte que l'estimation P = R/MN devrait être utilisée.

Comme la probabilité d'aller-retour n'est pas supposée être uniforme dans la réalité, et que les unités moins fiables sont plus importantes pour une estimation de limite inférieure mais seront plus probablement manquées dans l'échantillonnage, l'échantillon à partir duquel P est calculé est biaisé à l'égard des routeurs les moins fiables. Après le N ième intervalle de transmission, N > 2, négliger tous les routeurs connus dans les intervalles de 1 à F de l'estimation de fiabilité, où F est le plus grand entier inférieur à un demi de N. Par exemple, après cinq intervalles, seuls les routeurs déjà connus dans les intervalles de trois à cinq seront comptés.

Une station de gestion qui met en œuvre les méthodes de cette section devrait permettre à l'utilisateur de spécifier les paramètres suivants, et de les prendre par défaut aux valeurs indiquées.

Ct Intervalle de confiance de livraison de la cible, par défaut 0,999.

Pp Estimation initiale pessimiste de la limite inférieure de la probabilité d'aller-retour, P, pour empêcher une terminaison prématurée (voir ci-dessous). Par défaut 0,75.

Ti Intervalle initial entre les retransmissions de commande. Par défaut 4 secondes. DélaiMax millisecondes (voir au paragraphe 3.1) doivent être ajoutées au temporisateur de retransmission. La connaissance du temps de traitement des routeurs pour les commandes RR peut influencer le réglage de Ti. Ti+DélaiMax est aussi la durée minimum que la station de gestion doit attendre les résultats après chaque transmission avant de calculer un nouveau niveau de confiance. La phrase "fin du N ième intervalle" signifie une durée de Ti+DélaiMax après la N ième transmission d'une commande.

Tu Limite supérieure de la période entre les retransmissions de commande. Par défaut 512 secondes.

Les variables suivantes, dont certaines sont une fonction du compteur de retransmissions N, sont utilisées dans le paragraphe suivant.

T(N) Le temps entre les transmissions de commandes N et N+1 est V*T(N) + DélaiMax, où V est aléatoire et à peu près uniforme dans la gamme [0,75 à 1,0]. T(1) = Ti et pour N > 1, T(N) = min(2*T(N-1), Tu).

M(N) Nombre cumulatif des routeurs distincts dont les réponses ont été reçues dans une des N premières transmissions de la commande.

F=F(N) FLOOR((N-1)/2). Tous les routeurs dont les réponses ont été reçues dans les F premiers intervalles seront effectivement omis de l'estimation de la probabilité d'aller-retour calculé au N ième intervalle.

R(N,F) Nombre total de messages Résultat RR, y compris les dupliqués, reçus à la fin du N ième intervalle des routeurs qui n'étaient PAS connus dans un des F premiers intervalles.

p(N) Estimation du plus mauvais cas de probabilité d'aller-retour de livraison.

c(N) Niveau de confiance calculé.

Un astérisque (*) est utilisé pour noter la multiplication et un signe d'omission (^) note l'élévation à la puissance.

Si la différence de fiabilité entre les parties "bonne" et "mauvaise" d'un réseau géré est très grande, les premières valeurs de c(N) seront trop élevées. Les retransmissions devraient continuer pendant au moins Nmin = log(1- Ct)/log(1-Pp) intervalles, sans considération de l'estimation actuelle de l'intervalle de confiance. (En fait, il n'est pas besoin de calculer p(N) et c(N) avant Nmin intervalles.)

8.2 Calculs

Soit A = N*(M(N)-M(F))/R(N,F) pour abréger, l'estimation de la probabilité d'aller-retour de livraison est p(N) = 1-Q, où Q est cette racine de l'équation Q^N - A*Q + (A-1) = 0 qui est entre 0 et 1. (Q = 1 est toujours une racine. Si N est impair, il y a aussi une racine négative.) Cela peut se résoudre numériquement, par exemple avec la méthode de Newton (voir les textes standard, par exemple [ANM]). L'approximation de premier ordre Q1 = 1 - 1/A peut aussi être utilisée comme point de départ de l'itération. Mais Q1 NE DEVRAIT PAS être utilisé comme solution d'approximation car il sous estime toujours Q, et donc surestime p(N), ce qui causerait une surestimation du niveau de confiance.

Si nécessaire, la racine parasite Q = 1 peut être divisée, laissant Q^(N-1) + Q^(N-2) + ... + Q - (A-1) = 0 comme équation à résoudre. Selon la méthode numérique utilisée, cela pourrait être désirable car il serait possible (mais très improbable) que

A=N et ainsi Q=1 serait une double racine de l'équation précédente.

Après que N > 2 (ou N ≥ Nmin) intervalles ont été achevés, calculer l'estimation de la limite inférieure de fiabilité p(N) = R(N,F)/((N-F)*(M(N) - M(F))).

Calculer l'estimation de l'intervalle de confiance c(N) = (1 - (1-p(N))^N)^(M(N) - M(F) + 1) qui est la probabilité bayésienne que M(N) soit le nombre de routeurs présents étant donné le nombre de réponses qui ont été collectées, par opposition à M(N)+1 ou tout nombre supérieur. On suppose que la probabilité a priori qu'il y ait K routeurs n'était pas supérieure à celle de K-1 routeurs, pour tout K > M(N).

Lorsque c(N) ≥ Ct et N ≥ Nmin, les retransmissions de la commande peuvent cesser. Autrement, une autre transmission devrait être programmée à l'instant V*T(N) + DélaiMax après la (N^{ième}) transmission précédente, ou V*T(N) après la conclusion du traitement des réponses à la N^{ième} transmission, quelque soit la dernière.

Un cas particulier mérite considération. Une division par zéro peut se produire lors du calcul de p. Cela ne peut arriver que lorsque aucun nouveau routeur n'a été vu dans les N-F derniers intervalles. Généralement, l'estimation de l'intervalle de confiance c(N) sera proche de un à ce moment là, mais dans un cas particulier comme celui d'un grand nombre de routeurs avec une communication fiable et un nombre beaucoup plus petit de routeurs avec une très mauvaise communication, l'estimation de l'intervalle de confiance peut quand même être inférieure à Ct lorsque le dénominateur de p disparaît. La mise en œuvre peut continuer, et devrait continuer si le nombre minimum de transmissions donné au paragraphe précédent n'a pas encore été atteint. Si de nouveaux routeurs sont vus, p(N) va à nouveau être non singulier.

Bien sûr, aucun schéma de retransmission limité ne peut complètement régler la possibilité de problèmes à long terme, comme celui d'une partition de réseau. On suppose que le gestionnaire de réseau est au courant de telles conditions lorsque elles existent.

8.3 Méthodes d'assurance supplémentaires

Comme dernier moyen de détecter les routeurs qui deviennent accessibles après des commandes de dénumérotation manquantes durant un partage de réseau étendu, une station de gestion PEUT adopter la stratégie suivante. Lorsque on effectue chaque nouvelle opération, on incrémente le numéro de séquence de plus de un.

Après qu'on estime l'opération achevée, on envoie périodiquement une commande RR "no-op" avec le fanion R (Résultat exigé) établi et un numéro de séquence inférieur de un au plus fort utilisé. Toute réponse à une telle commande ne peut venir que d'un routeur qu'a manqué la dernière opération. Un exemple d'un commande "no-op" convenable serait une opération ADD avec MatchLen = 0, MinLen = 0, MaxLen = 128, et pas de partie Use-Prefix.

Si des vieilles clés d'authentification ont été sauvegardées par la station de gestion, même la réapparition de routeurs qui ont manqué la remise à zéro de numéro de séquence peut être détectée par la transmission de commandes no-op avec les clés invalides et un numéro de séquence supérieur à ceux utilisés avant que la clé soit invalidée. Comme il n'y a pas d'autre moyens pour qu'une station de gestion distingue l'échec d'un routeur à recevoir une séquence entière de messages SNR répétés de la perte d'un seul message résultat SNR de ce routeur, c'est la façon RECOMMANDÉE pour vérifier la réception universelle d'une commande SNR.

9. Exemples d'utilisation

Cette section met en scène quelques exemples d'applications de dénumérotation de routeur. Les en-têtes d'extension, y compris les en-tête IPsec exigés, entre l'en-tête IPv6 et l'en-tête ICMPv6, ne sont pas présentés dans les exemples.

9.1 Entretien de préfixes de portée mondiale

Une utilisation simple du mécanisme de dénumérotation de routeur, et dont on suppose qu'elle est très courante, est la maintenance d'un ensemble de préfixes globaux avec une structure de sous-réseau qui correspond à celle des allocations d'adresse de site local du site. Dans l'état permanent, cela va servir à garder les durées de vie préférée et valide réglées à leurs valeurs désirées. Durant une transition de dénumérotation, des messages de commande similaires peuvent ajouter de nouveaux préfixes et/ou en supprimer de vieux. Une présentation du message Commande convenable suit. Les champs non mentionnés sont supposés réglés aux valeurs convenables. Cette commande suppose que toutes les interfaces de routeur à entretenir ont déjà des adresses de site local [RFC2373].

En-tête IPv6
Prochain en-tête = 58 (ICMPv6)
Adresse de source = (Station de gestion)
Adresse de destination = FF05::2 (Tous routeurs, portée de site local)

En-tête ICMPv6/RR
Type = 138 (Dénumérotation de routeur), Code = 0 (Commande)
Fanions = 60 hex (R, A)

Première (et seule) PCO:
Partie Match-Prefix
OpCode = 3 (SET-GLOBAL)
OpLength = 4 N + 3 (supposant N préfixes globaux)
Ordinal = 0 (arbitraire)
MatchLen = 10
MatchPrefix = FEC0::0

Première partie Use-Prefix
UseLen = 48 (Longueur de TLA ID + RES + NLA ID [RFC2373])
KeepLen = 16 (Longueur de SLA (sous-réseau) ID [RFC2373])
FlagMask, RAFlags, Durées de vie, fanions V & P -- comme désiré
UsePrefix = Premier préfixe global /48
. . .

N^{ième} partie Use-Prefix
UseLen = 48
KeepLen = 16
FlagMask, RAFlags, durées de vie, fanions V & P -- comme désiré
UsePrefix = Dernier préfixe global /48

Cela va causer l'établissement (ou la mise à jour) de N préfixes globaux sur chaque interface applicable. Sur chaque interface, le champ SLA ID (sous-réseau) de chaque préfixe global sera copié du préfixe site local existant.

9.2 Dénumérotation d'un sous-réseau

Un sous-réseau peut être dénuméroté en douceur en réglant les temporisateurs de durée de vie valide et préférée sur le vieux préfixe à une valeur courte et en les laissant arriver à expiration, tout en ajoutant concurremment le nouveau préfixe. Ultérieurement, le préfixe arrivé à expiration est supprimé. La première étape est décrite par la commande RR suivante.

En-tête IPv6
Nouvel en-tête = 58 (ICMPv6)
Adresse de source = (Station de gestion)
Adresse de destination = FF05::2 (Tous routeurs, portée de site local)

En-tête ICMPv6/RR
Type = 138 (Dénumérotation de routeur), Code = 0 (Commande)
Fanions = 60 hex (R, A)

Première (et seule) PCO :
Partie Match-Prefix
OpCode = 2 (CHANGE)
OpLength = 11 (reflète deux parties Use-Prefix)
Ordinal = 0 (arbitraire)
MatchLen = 64
MatchPrefix = vieux préfixe /64

Première partie Use-Prefix
UseLen = 0
KeepLen = 64 (cela conserve intacte la valeur du vieux préfixe)
FlagMask = 0, RAFlags = 0
Durée de validité = 28800 secondes (8 heures)
Durée de vie préférée = 7200 secondes (2 heures)

Fanion V = 1, Fanion P = 1
UsePrefix = 0::0

Seconde partie de Use-Prefix
UseLen = 64
KeepLen = 0
FlagMask = 0, RAFlags = 0
Durées de vie , fanions V & P -- comme désiré
UsePrefix = Nouveau préfixe /64

La seconde étape, la suppression du vieux préfixe, peut être faite par une commande RR avec la même partie de Match-Prefix (sauf pour une OpLength réduite de 11 à 3) et pas de partie Use-Prefix. On devrait résister à la tentation de régler KeepLen = 64 dans la seconde partie Use-Prefix ci-dessus, car cela ordonnerait au routeur d'éviter la configuration d'adresse.

10. Remerciements

Ce protocole a été conçu par Matt Crawford sur la base d'une idée de Robert Hinden et Geert Jan de Groot. De nombreux membres du groupe de travail IPNG ont contribué par d'utiles commentaires, en particulier les membres de l'équipe IPv6 de DIGITAL UNIX. Bill Sommerfeld a fourni sa précieuse expertise IPsec. La rigueur implacable de certains membres de l'IESG pourrait avoir amélioré la qualité finale de cette spécification.

11. Références

[ANM] Isaacson, E. and H. B. Keller, "Analysis of Numerical Methods", John Wiley & Sons, New York, 1966.

[RFC1850] F. Baker, R. Coltun, "Base de données d'informations de gestion OSPF version 2", novembre 1995. (*Obsolète, voir* RFC4750) *(D.S.)*

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

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC4291) *(PS)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303*)*

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226*)*

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par* 5095, 6564 *; D.S)*

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

[RFC2466] D. Haskin, S. Onishi, "Base de données d'information de gestion pour IP version 6 : groupe ICMPv6", décembre 1998. (*Obsolète, voir* RFC4293) *(P.S.)*

12. Adresse de l'auteur

Matt Crawford
Fermilab MS 368
PO Box 500
Batavia, IL 60510
USA
téléphone : +1 630 840 3461
mél : crawdad@fnal.gov

Appendice Déduction des estimations de fiabilité

Si une population S de taille k est échantillonnée de façon répétée avec une efficacité p, le nombre de membres attendu de S découverts d'abord sur le n^{ième} échantillon est m = [1 - (1-p)^n] * k

Le nombre total attendu de membres de S trouvé dans les échantillons, y compris les dupliqués, est r = n * p * k

Prendre le ratio de m sur r annule le facteur inconnu k et donne l'équation [1 - (1-p)^n] / p = nm/r qui peut être résolue pour p, qui est alors un estimateur de l'efficacité de l'échantillonnage. (Les propriétés statistiques de l'estimateur ne seront pas examinées ici.) Avec la substitution p = 1-q, cela devient la première équation du paragraphe 8.2.

Avec l'estimateur p et un compte m de membres de S découverts après n échantillonnages, on peut calculer à posteriori la probabilité que la vraie taille de S soit m+j, pour j ≥ 0. Soit Hj la notation de l'hypothèse que la vraie taille de S est m+j, et soit R le résultat que m membres ont été trouvés dans n échantillonnages. Alors,

P{R | Hj} = [(m+j)!/m!j!] * [1-(1-p)^n]^m * [(1-p)^n]^j

On s'intéresse à P{H0 | R}, mais pour le trouver on doit allouer des valeurs a priori à P{Hj}. Supposons que la taille de S est une distribution exponentielle P{Hj} / P{H0} = h^(-j) pour un h arbitraire dans (0, 1). La valeur de h sera éliminée du résultat.

La méthode bayésienne donne P{Hj | R} / P{H0 | R} = [(m+j)!/m!j!] * [h*(1-p)^n]^j

La réciproque de la somme sur j ≥ 0 de ces ratios est P{H0 | R} = [1-h*(1-p)^n] ^ (m+1) et l'estimation de l'intervalle de confiance du paragraphe 8.2 est la limite h -> 1 de cette expression.

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.