Groupe de travail Réseau
Request for Comments : 3971
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

J. Arkko, éd., Ericsson
J. Kempf, DoCoMo
B. Zill, Microsoft
P. Nikander, Ericsson
mars 2005

Découverte de voisin sécurisée (SEND)

Résumé
Les nœuds IPv6 utilisent le protocole de découverte de voisin (NDP, *Neighbor Discovery Protocol*) pour découvrir d'autres nœuds sur la liaison, pour déterminer leurs adresses de liaison locale afin de trouver des routeurs, et pour entretenir les informations d'accessibilité sur les chemins vers les voisins actifs. S'il n'est pas sécurisé, NDP est vulnérable à diverses attaques. Le présent document spécifie des mécanismes de sécurité pour NDP. À la différence des spécifications NDP d'origine, ces mécanismes n'utilisent pas IPsec.

Table of Contents

1. Introduction

IPv6 définit le protocole de découverte de voisin (NDP, *Neighbor Discovery Protocol*) dans les [RFC2461] et [RFC2462]. Les nœuds sur la même liaison utilisent NDP pour découvrir leur présence réciproque et leurs adresses de liaison locale, pour trouver les routeurs, et pour conserver les informations d'accessibilité sur les chemins vers les voisins actifs. NDP est utilisé par les hôtes et les routeurs. Ses fonctions incluent la découverte de voisin (ND, *Neighbor Discovery*) la découverte de routeur (RD, *Router Discovery*) l'auto configuration d'adresse, la résolution d'adresse, la détection d'inaccessibilité de voisin (NUD, *Neighbor Unreachability Detection*) la détection d'adresse dupliquée (DAD, *duplicate adresse detection*) et la redirection.

Les spécifications NDP d'origine proposaient l'utilisation de IPsec pour protéger les messages NDP. Cependant, les RFC n'ont pas donné d'instructions détaillées pour que l'utilisation d'IPsec le fasse. Dans cette application particulière, IPsec peut seulement être utilisé avec une configuration manuelle des associations de sécurité, à cause des problèmes d'amorçage pour utiliser IKE [ICMP-IKE], [RFC2409]. De plus, le nombre d'associations de sécurité configurées manuellement qui est nécessaire pour protéger NDP peut être très élevé [Manual SA], rendant cette approche impraticable pour presque tout. Le protocole SEND est conçu pour contrer les menaces contre NDP. Ces menaces sont décrites en détails dans la [RFC3756]. SEND est applicable dans les environnements où la sécurité physique sur la liaison n'est pas assurée (comme en sans fil) et où les attaques contre NDP sont un problème.

Le présent document est organisé comme suit . les sections 2 et 3, respectivement, définissent la terminologie et présentent une brève vue d'ensemble de NDP. La Section 4 décrit l'approche globale de la sécurisation de NDP. Cette approche implique l'utilisation de nouvelles options NDP pour porter des signatures fondées sur une clé publique. Un mécanisme de configuration zéro est utilisé pour montrer la propriété des adresses sur les nœuds individuels ; les routeurs sont certifiés par une ancre de confiance [RFC3280]. Les formats, procédures, et les mécanismes cryptographiques pour le mécanisme de configuration zéro sont décrits dans la spécification qui s'y consacre, la [RFC3972].

Les nouvelles options NDP requises sont exposées à la Section 5. La Section 6 décrit le mécanisme de distribution des chemins de certification pour établir une chaîne de délégation d'autorisation jusqu'à une ancre de confiance.

Finalement, la Section 8 expose la coexistence de NDP sécurisé et non sécurisé sur la même liaison, et la Section 9 expose les considérations sur la sécurité pour la découverte de voisin sécurisée (SEND, *SEcure Neighbor Discovery*).

L'utilisation de certificats d'identité provisionnés sur les hôtes d'extrémité pour autoriser l'utilisation d'une adresse sort du domaine d'application du présent document, tout comme la sécurité de NDP lorsque l'entité qui défend une adresse n'est pas la même que l'entité qui revendique cette adresse (aussi appelé "ND mandataire"). Ce sont des extensions à SEND qui pourront être traitées dans des documents séparés, si le besoin s'en fait sentir.

1.1 Spécification des exigences

Dans le présent document, plusieurs mots sont utilisés pour signifier les exigences de la spécification. Ces mots sont souvent en majuscules. Les mots clés "DOIT", "NE DOIT PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ",et "PEUT" sont à interpréter comme décrit dans la [RFC2119].

2. Termes

Découverte de délégation d'autorisation (ADD, *Authorization Delegation Discovery*) : processus par lequel les nœuds SEND peuvent acquérir un chemin de certification d'un nœud homologue jusqu'à une ancre de confiance.

Liste de révocation de certificat (CRL, *Certificate Revocation List*) : dans une méthode de révocation de certificat, une autorité produit périodiquement une structure de données signées appelée la liste de révocation de certificat. C'est une liste avec un horodatage qui identifie les certificats révoqués, signée par celui qui l'a produite, et rendue librement disponible dans un répertoire public.

Annonce de chemin de certification (CPA, *Certification Path Advertisement*) : message d'annonce utilisé dans le processus ADD.

Sollicitation de chemin de certification (CPS, *Certification Path Solicitation*) : message de sollicitation du processus ADD.

Adresse générée cryptographiquement (CGA, *Cryptographically Generated Address*) : technique décrite dans la [RFC3972] par laquelle une adresse IPv6 d'un nœud est générée de façon cryptographique en utilisant une fonction de hachage unidirectionnelle à partir de la clé publique du nœud et d'autres paramètres.

Règles de codage en métalangage distinctif (DER, *Distinguished Encoding Rules*) : schéma de codage pour des valeurs de données, définie dans [X.690].

Détection d'adresse dupliquée (DAD, *Duplicate Address Detection*) : mécanisme qui assure que deux nœuds IPv6 sur la même liaison n'utilisent pas la même adresse.

Nom de domaine complet (FQDN, *Fully Qualified Domain Name*) : un nom de domaine complet consiste en un nom d'hôte et de domaine, incluant le domaine de niveau supérieur.

Nom de domaine internationalisé (IDN, *Internationalized Domain Name*) : les noms de domaine internationalisés peuvent être utilisés pour représenter des noms de domaines qui contiennent des caractères en dehors de l'ensemble ASCII. Voir la [RFC3490].

Découverte de voisin (ND, *Neighbor Discovery*) : fonction de découverte de voisin du protocole de découverte de voisin (NDP, *Neighbor Discovery Protocol*). NDP contient d'autres fonctions que ND.

Protocole de découverte de voisin (NDP, *Neighbor Discovery Protocol*) : c'est le protocole de découverte de voisin IPv6 [RFC3280], [RFC3281], qui fait partie de ICMPv6 [RFC2463].

Détection d'inaccessibilité du voisin (NUD, *Neighbor Unreachability Detection*) : mécanisme utilisé pour retracer l'accessibilité des voisins.

Nœud non SEND : nœud IPv6 qui ne met pas en œuvre la présente spécification mais utilise seulement le protocole de découverte de voisin défini dans les RFC2461 et 2462, telles que mises à jour, sans sécurité.

Nom occasionnel *(Nonce)* : nombre aléatoire ou pseudo aléatoire imprévisible généré par un nœud et utilisé exactement une fois. Dans SEND, les noms occasionnels sont utilisés pour assurer qu'une annonce particulière est liée à la sollicitation qui l'a déclanchée.

Certificat d'autorisation de routeur : dans le certificat de clé publique X.509v3 [RFC3280] qui utilise le profil spécifié au paragraphe 6.3.1.

Nœud SEND : nœud IPv6 qui met en œuvre la présente spécification.

Découverte de routeur (RD, *Router Discovery*) : la découverte de routeur permet aux hôtes de découvrir quels routeurs existent sur la liaison, et quels préfixes de sous réseau sont disponibles. La découverte de routeur fait partie du protocole de découverte de voisin.

Ancre de confiance : les hôtes sont configurés avec un ensemble d'ancres de confiance pour protéger la découverte de routeurs. Une ancre de confiance est une entité en laquelle l'hôte a confiance pour autoriser les routeurs à agir comme routeurs. Une configuration d'ancre de confiance consiste en une clé publique et des paramètres associés (voir au paragraphe 6.5 l'explication détaillée de ces paramètres).

3. Vue d'ensemble de la découverte de voisin et de routeur

Le protocole de découverte de voisin a plusieurs fonctions. Beaucoup se concentrent sur quelques types de messages centraux, comme le message ICMPv6 Annonce de voisin. Dans cette section, on examine certaines de ces tâches et leurs effets afin de mieux comprendre comment les messages devraient être traités. Cette section n'est pas normative, et si la présente section et les RFC d'origine sur la découverte de voisin sont en conflit, les RFC d'origine, telles que mises à jour, ont la préséance.

Les principales fonctions de NDP sont les suivantes :

o La fonction de découverte de routeur permet aux hôtes IPv6 de découvrir les routeurs locaux sur une liaison rattachée. La découverte de routeur est décrite à la Section 6 de la [RFC2461]. Le principal objet de la découverte de routeur est de

trouver les routeurs voisins qui acceptent de transmettre les paquets au nom des hôtes. La découverte de préfixe de sous réseau implique de déterminer quelles destinations sont directement sur une liaison ; cette information est nécessaire afin de savoir si un paquet devrait être envoyé à un routeur ou directement au nœud de destination.

- La fonction Redirect est utilisée pour rediriger automatiquement un hôte sur un meilleur routeur de premier bond, ou pour informer les hôtes qu'une destination est en fait un voisin (c'est-à-dire, sur la liaison). Redirect est spécifié à la Section 8 de la [RFC2461].

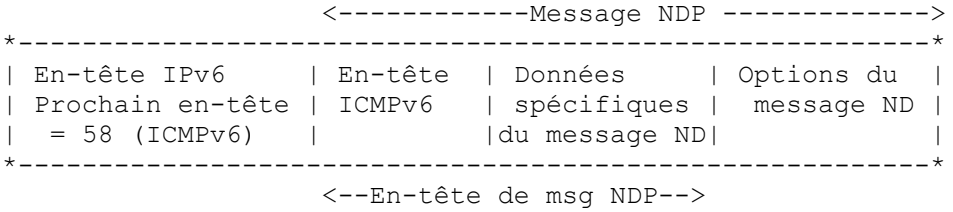
- L'autoconfiguration d'adresse est utilisée pour allouer automatiquement des adresses à un hôte [RFC2462]. Cela permet aux hôtes de fonctionner sans une configuration explicite à l'égard de la connexité IP. Le mécanisme d'autoconfiguration par défaut est sans état. Pour créer des adresses IP, les hôtes utilisent toute information de préfixe qui leur est livrée durant la découverte de routeur et ensuite, ils vérifient l'unicité des nouvelles adresses formées. Un mécanisme à états pleins, DHCPv6 [RFC3315], fournit des caractéristiques d'autoconfiguration supplémentaires.

- La détection d'adresse dupliquée (DAD) est utilisée pour prévenir les collisions d'adresses [RFC2462] : par exemple, durant l'autoconfiguration d'adresse. Un nœud qui a l'intention d'allouer une nouvelle adresse à une de ses interfaces lance d'abord la procédure de DAD pour vérifier qu'aucun autre nœud n'utilise la même adresse. Comme les règles interdisent d'utiliser une adresse jusqu'à ce elle ait été déclarée unique, aucun trafic de couche supérieure n'est possible avant que cette procédure soit terminée. Donc, empêcher les attaques contre DAD peut aider à s'assurer de la disponibilité des communications pour le nœud en question.

- La fonction de résolution d'adresse permet à un nœud sur la liaison de résoudre l'adresse IPv6 d'un autre nœud en l'adresse de couche liaison correspondante. La résolution d'adresse est définie au paragraphe 7.2 de la [RFC2461], et est utilisée aussi bien pour les hôtes que les routeurs. Là encore, aucun trafic de niveau supérieur ne peut s'écouler tant que l'envoyeur ne connaît pas l'adresse de couche liaison du nœud de destination ou du routeur de prochain bond. Noter que l'adresse de source de la couche de liaison sur les trames de couche liaison n'est pas confrontée aux informations apprises par la résolution d'adresse. Cela permet un ajout plus facile des éléments de réseau tels que les ponts et les mandataires et facilite les exigences de mise en œuvre de la pile, car moins d'informations sont à passer d'une couche à l'autre.

- La détection d'inaccessibilité de voisin (NUD) est utilisée pour retracer l'accessibilité des nœuds du voisinage, hôtes aussi bien que routeurs. NUD est défini au paragraphe 7.3 de la [RFC2461]. NUD est sensible à la sécurité, parce qu'un attaquant pourrait prétendre que l'accessibilité existe alors qu'en fait, elle n'existe pas.

Les messages NDP suivent le format de message ICMPv6. Toutes les fonctions de NDP sont réalisées par l'utilisation des messages Sollicitation de routeur (RS, *Router Solicitation*), Annonce de routeur (RA, *Router Advertisement*), Sollicitation de voisin (NS, *Neighbor Solicitation*), Annonce de voisin (NA, *Neigbhor Advertisement*), et Redirect. Un message NDP réel comporte un en-tête de message NDP, consistant en un en-tête ICMPv6 et des données spécifiques de message ND, et zéro, une ou plusieurs options NDP. Les options de message NDP sont formatées en format de Type-Longueur-Valeur.



4. Vue d'ensemble de la découverte de voisin sécurisée

Pour sécuriser les diverses fonctions de NDP, un ensemble de nouvelles options de découverte de voisin sont introduites. Elles sont utilisées pour protéger les messages NDP. La présente spécification introduit ces options, un processus d'autorisation de découverte de délégation, un mécanisme de preuve de possession d'adresse, et les exigences pour l'utilisation de ces composants dans NDP.

Les composants de la solution spécifiée dans ce document sont les suivantes :

- Les chemins de certification, ancrés sur les parties de confiance, sont supposés certifier l'autorité des routeurs. Un hôte doit être configuré avec une ancre de confiance avec laquelle le routeur a un chemin de certification avant que l'hôte puisse adopter le routeur comme son routeur par défaut. Les messages Sollicitation de chemin de certification et Annonce sont utilisés pour découvrir un chemin de certification pour l'ancre de confiance sans exiger que les messages réels de découverte de routeur portent de longs chemins de certification. La réception d'un message d'annonce de routeur protégé

pour lequel aucun chemin de certification n'est disponible déclanche le processus de découverte de délégation d'autorisation.

o Les adresses générées cryptographiquement sont utilisées pour s'assurer que l'envoyeur d'un message de découverte de voisin est le "propriétaire" de l'adresse revendiquée. Une paire de clés publique-privée est générée par tous les nœuds avant qu'ils puissent revendiquer une adresse. Une nouvelle option NDP, l'option CGA, est utilisée pour porter la clé publique et les paramètres associés.

La présente spécification permet aussi à un nœud d'utiliser des non CGA avec les certificats qui autorisent leur usage. Cependant, les détails d'une telle utilisation sortent du domaine d'application de cette spécification et feront l'objet de futurs travaux.

o Une nouvelle option NDP, l'option Signature RSA, est utilisée pour protéger tous les messages qui se rapportent à la découverte de voisin et de routeur.

Les signatures de clé publique protègent l'intégrité des messages et authentifient l'identité de leur envoyeur. L'autorité d'une clé publique est établie soit avec le processus de délégation d'autorisation, en utilisant des certificats, soit par le mécanisme de preuve de possession d'adresse, en utilisant des CGA, soit avec les deux, selon la configuration et le type du message protégé.

Note : RSA est obligatoire parce qu'avoir plusieurs algorithmes de signature romprait la compatibilité entre les mises en œuvre ou augmenterait la complexité de la mise en œuvre en forçant l'utilisation de plusieurs algorithmes et du mécanisme de choix entre eux. Un second algorithme de signature n'est nécessaire que comme mécanisme de secours, en cas de défaillance de RSA. Si cela arrivait, un algorithme de signature plus fort pourra être choisi, et SEND pourra être révisé. Les relations entre le nouvel algorithme et le SEND fondé sur RSA décrit dans le présent document seraient similaires à celles entre le SEND fondé sur RSA et la découverte de voisin sans SEND. Les informations signées avec le plus fort algorithme ont la préséance sur celles signées avec RSA, de la même façon que les informations signées avec RSA ont maintenant la préséance sur les informations non signées. Les mises en œuvre des spécifications actuelles et révisées resteront compatibles.

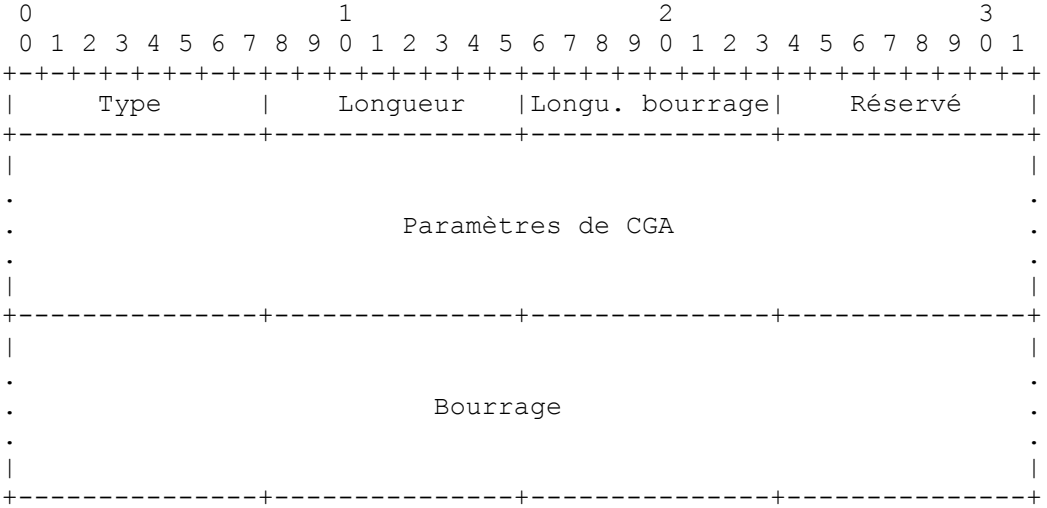
o Pour empêcher les attaques en répétition, deux nouvelles options de découverte de voisin, Horodatage et Nom occasionnel, sont introduites. Étant donné que les messages de découverte de voisin et de routeur sont dans certains cas envoyés à des adresses de diffusion groupée, l'option Horodatage offre une protection contre la répétition sans état préalablement établi ni numéros de séquence. Lorsque les messages sont utilisés dans des paires sollicitation-annonce, ils sont protégés avec l'option Nom occasionnel.

5. Options du protocole de découverte de voisin

Les options décrites dans cette section DOIVENT être prises en charge.

5.1 Option CGA

L'option CGA permet la vérification de la CGA de l'envoyeur. Le format de l'option CGA est décrit comme suit :



Type : 11

Longueur : longueur de l'option (incluant les champs Type, Longueur, Longueur de bourrage, Réservé, Paramètres de CGA, et Bourrage) en unités de 8 octets.

Longueur de bourrage : nombre d'octets de bourrage au delà de la fin du champ Paramètres de CGA mais dans la longueur spécifiée par le champ Longueur. Les octets de bourrage DOIVENT être réglés à zéro par l'envoyeur et ignorés à réception.

Réservé : champ de 8 bits réservé pour utilisation future. La valeur DOIT être initialisée à zéro par l'envoyeur et DOIT être ignorée par le receveur.

Paramètres de CGA : champ de longueur variable qui contient la structure de données des paramètres de CGA décrite à la Section 4 de la [RFC3972].

La présente spécification exige que si les deux options CGA et Signature sont présentes, la clé publique trouvée dans le champ Paramètres de CGA dans l'option CGA DOIT être celle référencée par le champ Hachage de clé dans l'option Signature RSA. Les paquets reçus avec deux clés différentes DOIVENT être éliminés en silence. Noter qu'une future extension pourrait fournir un mécanisme permettant au propriétaire d'une adresse d'être différent du signataire.

Bourrage : champ de longueur variable qui fait de la longueur de l'option un multiple de 8, contenant autant d'octets que spécifié dans le champ Longueur de bourrage.

5.1.1 Règles de traitement par l'envoyeur

Si le nœud a été configuré à utiliser SEND, l'option CGA DOIT être présente dans tous les messages Sollicitation de voisin et Annonce et DOIT être présente dans les messages Sollicitation de routeur sauf si ils sont envoyés avec l'adresse de source non spécifiée. L'option CGA PEUT être présente dans d'autres messages.

Un nœud qui envoie un message en utilisant l'option CGA DOIT construire le message comme suit :

Le champ Paramètre de CGA dans l'option CGA est rempli conformément aux règles présentées ci-dessus et dans la [RFC3972]. La clé publique dans le champ est tirée de la configuration utilisée pour générer la CGA, normalement d'une structure de données associée à l'adresse de source. L'adresse DOIT être construite comme spécifié à la Section 4 de la [RFC3972]. Selon le type de message, cette adresse apparaît dans différents endroits, comme suit :

Redirect : l'adresse DOIT être l'adresse de source du message.

Sollicitation de voisin : l'adresse DOIT être l'adresse cible pour les sollicitations envoyées pour la détection d'adresse dupliquée ; autrement elle DOIT être l'adresse de source du message.

Annonce de voisin : l'adresse DOIT être l'adresse de source du message.

Sollicitation de routeur : l'adresse DOIT être l'adresse de source du message. Noter que l'option CGA n'est pas utilisée lorsque l'adresse de source est l'adresse non spécifiée.

Annonce de routeur : l'adresse DOIT être l'adresse de source du message.

5.1.2 Règles de traitement pour le receveur

Les messages Sollicitation de voisin et Annonce sans l'option CGA DOIVENT être traités comme non sûrs (c'est-à-dire, traités de la même façon que les messages NDP envoyés par un nœud non SEND). Le traitement des messages non sûrs est spécifié à la Section 8. Noter que les nœuds SEND qui ne tentent pas d'interopérer avec les nœuds non SEND PEUVENT simplement éliminer les messages non sûrs.

Les messages Sollicitation de routeur sans l'option CGA DOIVENT aussi être traités comme non sûrs, sauf si l'adresse de source du message est l'adresse non spécifiée.

Les messages Redirect, Sollicitation de voisin, Annonce de voisin, Sollicitation de routeur, et Annonce de routeur qui contiennent une option CGA DOIVENT être vérifiés comme suit :

Si l'interface a été configurée à utiliser CGA, le nœud receveur DOIT vérifier l'adresse de source du paquet en utilisant

l'algorithme décrit à la Section 5 de la [RFC3972]. Les entrées de l'algorithme sont l'adresse revendiquée, comme défini au paragraphe précédent, et le champ Paramètres de CGA.

Si la vérification de CGA est réussie, le receveur poursuit avec une vérification cryptographique de la signature qui prend plus de temps. Noter que même si la vérification de CGA réussit, aucune réclamation sur la validité de l'utilisation ne peut être faite tant que la signature n'est pas vérifiée.

Un receveur qui ne prend pas en charge CGA ou n'a pas spécifié son utilisation pour une certaine interface peut quand même vérifier les paquets en utilisant les ancres de confiance, même si une CGA est utilisée sur un paquet. Dans un tel cas, la propriété CGA de l'adresse reste simplement non vérifiée.

5.1.3 Configuration

Tous les nœuds qui prennent en charge la vérification de l'option CGA DOIVENT enregistrer les informations de configuration suivantes :

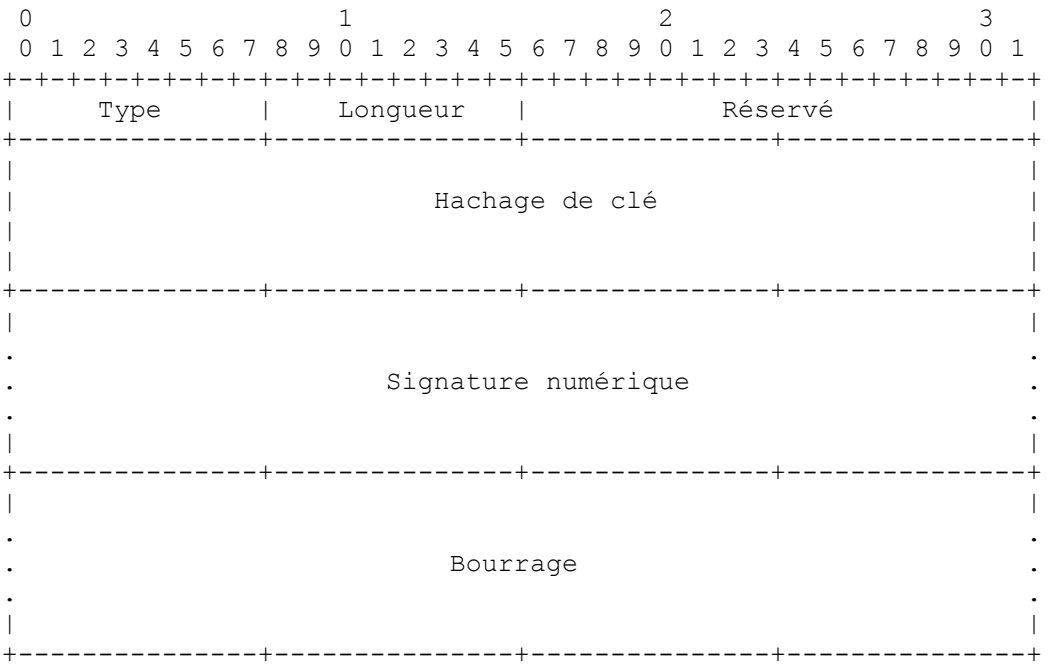
minbits : longueur de clé minimum acceptable pour les clés publiques utilisées dans la génération des CGA. Par défaut, ce DEVRAIT être 1024 bits. Les mises en œuvre PEUVENT aussi établir une limite supérieure à la quantité de calcul nécessaire lors de la vérification des paquets qui utilisent ces associations de sécurité. La limite supérieure DEVRAIT être d'au moins 2048 bits. Toutes les mises en œuvre devraient avoir une pratique cryptographique prudente pour déterminer les longueurs de clé appropriées.

Tous les nœuds qui prennent en charge l'envoi de l'option CGA DOIVENT enregistrer les informations de configuration suivantes :

Paramètres de CGA : toute information requise pour construire des CGA, comme décrit dans la [RFC3972].

5.2 Option Signature RSA

L'option Signature RSA permet que des signatures fondées sur une clé publique soient attachées à des messages NDP. Le format de l'option Signature RSA est décrit dans le diagramme suivant :



Type : 12

Longueur : longueur de l'option (incluant les champs Type, Longueur, Réservé, Hachage de clé, Signature numérique, et Bourrage) en unités de 8 octets.

Réservé : champ de 16 bits réservé pou une utilisation future. La valeur DOIT être initialisée à zéro par l'envoyeur, et DOIT être ignorée par le receveur.

Hachage de clé : champ de 128 bits qui contient les 128 bits de poids fort (les plus à gauche) d'un hachage SHA-1 [FIPS180-1] de la clé publique utilisée pour construire la signature. Le hachage SHA-1 est pris sur la présentation utilisée dans le champ Clé publique de la structure de données de paramètres de CGA portée dans l'option CGA. Son objet est d'associer la signature à une clé particulière connue du receveur. Une telle clé peut être mémorisée dans l'antémémoire de certificat du receveur ou être reçue dans l'option CGA dans le même message.

Signature numérique : champ de longueur variable qui contient une signature PKCS#1 v1.5, construite en utilisant la clé privée de l'envoyeur sur la séquence d'octets suivante :

1. La valeur d'étiquette de type de message CGA de 128 bits [RFC3972] pour SEND, 0x086F CA5E 10B2 00C9 9C8C E001 6427 7C08. (La valeur de l'étiquette a été générée au hasard par l'éditeur de cette spécification.).
2. Le champ Adresse de source de 128 bits provenant de l'en-tête IP.
3. Le champ Adresse de destination de 128 bits provenant de l'en-tête IP.
4. Les champs Type de 8 bits, Code de 8 bits, et Somme de contrôle de 16 bits provenant de l'en-tête ICMP.
5. L'en-tête de message NDP, commençant à l'octet qui suit le champ Somme de contrôle ICMP et qui continue jusqu'aux options NDP non incluses.
6. Toutes les options NDP qui précèdent l'option Signature RSA.

La valeur de la signature est calculée avec l'algorithme RSASSA-PKCS1-v1_5 et le hachage SHA-1, comme défini dans [PKCS1]. Ce champ commence après le champ Hachage de clé. La longueur du champ Signature numérique est déterminée par la longueur de l'option Signature RSA moins la longueur des autres champs (incluant le champ Bourrage de longueur variable).

Bourrage : ce champ de longueur variable contient le bourrage, long d'autant d'octets qu'il reste après la fin de la signature.

5.2.1 Règles de traitement pour les envoyeurs

Si le nœud a été configuré à utiliser SEND, les messages Sollicitation de voisin, Annonce de voisin, Annonce de routeur, et Redirect DOIVENT contenir l'option Signature RSA. Les messages Sollicitation de routeur non envoyés avec l'adresse de source non spécifiée DOIVENT contenir l'option Signature RSA.

Un nœud qui envoie un message avec l'option Signature RSA DOIT construire le message comme suit :

- Le message est construit entièrement, sans l'option Signature RSA.
- L'option Signature RSA est ajoutée comme dernière option dans le message.
- Les données à signer sont construites comme expliqué au paragraphe 5.2, sous la description du champ Signature numérique.
- Le message, sous la forme définie ci-dessus, est signé en utilisant la clé privée configurée, et la signature PKCS#1 v1.5 résultante est mise dans le champ Signature numérique.

5.2.2 Règles de traitement pour les receveurs

Les messages Sollicitation de voisin, Annonce de voisin, Annonce de routeur, et Redirect sans l'option Signature RSA DOIVENT être traités comme non sûrs (c'est-à-dire, traités de la même façon que les messages NDP envoyés par un nœud non SEND). Voir à la Section 8.
Les messages Sollicitation de routeur sans l'option Signature RSA DOIVENT aussi être traités comme non sûrs, sauf si l'adresse de source du message est l'adresse non spécifiée.
Les messages Redirect, Sollicitation de voisin, Annonce de voisin, Sollicitation de routeur, et Annonce de routeur qui contiennent une option Signature RSA DOIVENT être vérifiés comme suit :

- Le receveur DOIT ignorer toute option qui vient après la première option Signature RSA. (Les options sont ignorées pour les besoins de la vérification de signature et le traitement NDP.)
- Le champ Hachage de clé DOIT indiquer l'utilisation d'une clé publique connue, soit apprise d'une option CGA précédente dans le même message, soit connue par d'autres moyens.
- Le champ Signature numérique DOIT avoir un codage correct et NE DOIT PAS excéder la longueur de l'option Signature RSA moins le bourrage.
- La vérification de la signature numérique DOIT montrer que la signature a été calculée comme spécifié au paragraphe précédent.
- Si l'utilisation d'une ancre de confiance a été configurée, un chemin de certification valide (voir au paragraphe 6.3) entre l'ancre de confiance du receveur et la clé publique de l'envoyeur DOIT être connu.

Noter que le receveur peut vérifier juste la propriété CGA d'un paquet, même si, en plus de la CGA, l'envoyeur a utilisé une ancre de confiance.

Les messages qui ne satisfont pas aux vérifications ci-dessus DOIT être éliminés en silence si l'hôte a été configuré à accepter seulement les messages ND sûrs. Les messages PEUVENT être acceptés si l'hôte a été configuré à accepter les messages sécurisés et non sécurisés, mais ils DOIVENT être traités comme des messages non sûrs. Autrement, le receveur PEUT aussi éliminer en silence les paquets (par exemple, en réponse à une attaque apparente de déni de service par épuisement de CPU).

5.2.3 Configuration

Tous les nœuds qui prennent en charge la réception de l'option Signature RSA DOIVENT permettre que les informations suivantes soient configurées pour chaque type de message NDP :

Méthode d'autorisation : ce paramètre détermine la méthode par laquelle l'autorité de l'envoyeur est déterminée. Il peut avoir quatre valeurs :
- ancre de confiance : l'autorité de l'envoyeur est vérifiée comme décrit au paragraphe 6.3. L'envoyeur peut réclamer une autorisation supplémentaire grâce à l'utilisation des CGA, mais ce n'est ni exigé ni vérifié.
- CGA : la propriété de CGA de l'adresse de l'envoyeur est vérifiée comme décrit dans la [RFC3972]. L'envoyeur peut réclamer une autorité supplémentaire par une ancre de confiance, mais ce n'est ni exigé ni vérifié.
- ancre de confiance et CGA : l'ancre de confiance et la vérification de CGA sont toutes deux exigées.
- ancre de confiance ou CGA : l'ancre de confiance ou la vérification de CGA est exigée.

ancre : la ou les ancres de confiance permises, si la méthode d'autorisation n'est pas réglée à CGA.

Tous les nœuds qui prennent en charge l'envoi de l'option Signature RSA DOIVENT enregistrer les informations de configuration suivantes :

keypair : paire de clé publique/privée. Si la délégation d'autorisation est utilisée, un chemin de certification allant d'une ancre de confiance à cette paire de clés doit exister.

fanion CGA : fanion qui indique si une CGA est utilisée ou non. Ce fanion peut être par interface ou par nœud. (Noter que dans de futures extensions du protocole SEND, ce fanion pourrait aussi être par préfixe de sous réseau.)

5.2.4 Considérations de performances

La construction et la vérification de l'option Signature RSA est coûteuse en calcul. Dans le conteste de NDP, cependant, les hôtes n'ont normalement à effectuer que quelques opérations de signature lorsque ils entrent sur une liaison, quelques opérations lorsque ils trouvent un nouvel homologue en ligne avec lequel communiquer, ou la détection d'inaccessibilité de voisin avec les voisins existants.

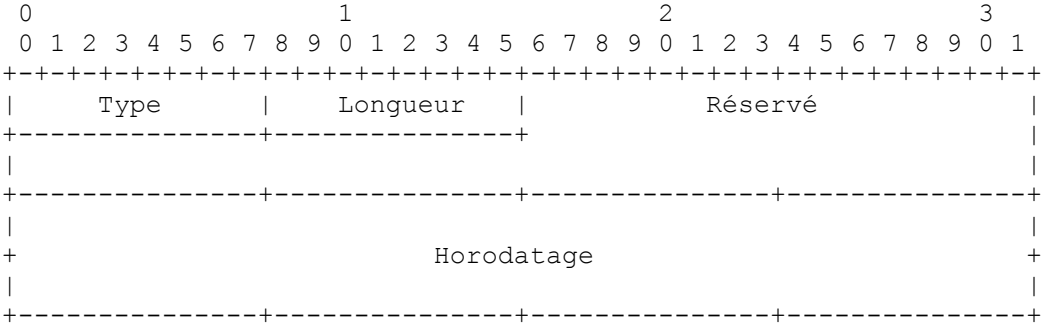
Les routeurs sont obligés d'effectuer un plus grand nombre d'opérations, en particulier lorsque la fréquence des annonces de routeur est élevée à cause des exigences de mobilité. Le nombre d'opérations de signature exigé est quand même de l'ordre de quelques douzaines par seconde, dont certaines peuvent être pré calculées comme on l'explique ci-dessous. Un grand nombre de sollicitations de routeur peut causer une plus forte demande d'opérations asymétriques, bien que le protocole NDP de base limite le taux d'envoi des réponses en diffusion groupée aux sollicitations.

Les signatures peuvent être pré calculées pour les annonces de voisin et de routeur non sollicitées (en diffusion groupée) si la programmation des annonces futures est connue. Normalement, les annonces de voisin sollicitées sont envoyées à l'adresse d'envoi individuel de laquelle la sollicitation a été envoyée. Étant donné que l'en-tête IPv6 est couvert par la signature, il n'est pas possible de pré calculer les annonces sollicitées.

5.3 Options Horodatage et Nom occasionnel

5.3.1 Option Horodatage

L'objet de l'option Horodatage est de s'assurer que des annonces non sollicitées et des redirections n'ont pas été répétées. Le format de cette option est décrit ci après :



Type : 13

Longueur : longueur de l'option (incluant les champs Type, Longueur, Réservé, et Horodatage) en unités de 8 octets ; c'est-à-dire, 2.

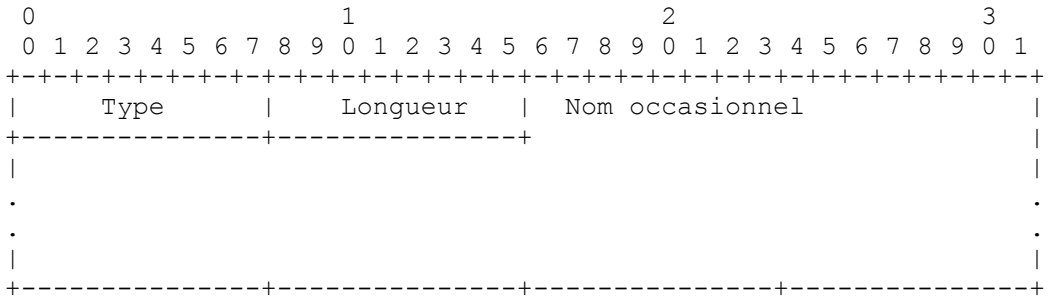
Réservé : champ de 48 bits réservé pour une utilisation future. La valeur DOIT être initialisée à zéro par l'envoyeur et DOIT être ignorée par le receveur.

Horodatage : champ contenant un entier non signé de 64 bits qui représente un horodatage. La valeur indique le nombre de secondes depuis le 1er janvier 1970, 00:00 UTC, en utilisant un format à virgule fixe. Dans ce format, le nombre entier de secondes est contenu dans les 48 premiers bits du champ, et les 16 bits restants indiquent le nombre de fractions de 1/64000 de seconde.

Note de mise en œuvre : ce format est compatible avec la représentation usuelle de l'heure sous UNIX, bien que le nombre de bits disponible pour la partie entière et la partie fractionnaire puisse varier.

5.3.2 Option Nom occasionnel

L'objet de l'option Nom occasionnel est de s'assurer qu'une annonce est une réponse fraîche à une sollicitation envoyée antérieurement par le nœud. Le format de cette option est décrit dans ce qui suit :



Type : 14

Longueur : longueur de l'option (incluant les champs Type, Longueur, et Nom occasionnel) en unités de 8 octets.

Nom occasionnel : champ contenant un nombre aléatoire choisi par l'envoyeur du message de sollicitation. La longueur du nombre aléatoire DOIT être d'au moins 6 octets. La longueur du nombre aléatoire DOIT être choisie de façon à ce que la longueur de l'option Nom occasionnel soit un multiple de 8 octets.

5.3.3 Règles de traitement pour l'envoyeur

Si le nœud a été configuré à utiliser SEND, tous les messages de sollicitation DOIVENT inclure un nom occasionnel. Lors de l'envoi d'une sollicitation, l'envoyeur DOIT mémoriser le nom occasionnel en interne afin qu'il puisse reconnaître toutes les réponses qui contiennent ce nom occasionnel particulier.

Si le nœud a été configuré à utiliser SEND, toutes les annonces envoyées en réponse à une sollicitation DOIVENT inclure un nom occasionnel, copié de la sollicitation reçue. Noter que les routeurs peuvent décider d'envoyer une annonce en diffusion groupée à tous les nœuds au lieu d'une réponse à un hôte spécifique. Dans un tel cas, le routeur PEUT quand même inclure la valeur de nom occasionnel pour l'hôte qui a déclanché l'annonce en diffusion groupée. (Omettre la valeur de nom occasionnel peut être cause que l'hôte ignore l'annonce du routeur, sauf si les horloges dans ces nœuds sont suffisamment synchronisées pour que la fonction d'horodatage soit correcte.)

Si le nœud a été configuré à utiliser SEND, tous les messages de sollicitation, d'annonce, et de redirection DOIVENT inclure un horodatage. Les envoyeurs DEVRAIENT régler le champ Horodatage à l'heure courante, conformément à leurs horloges en temps réel.

5.3.4 Règles de traitement pour le receveur

Le traitement des options Nom occasionnel et Horodatage dépend de si un paquet est une annonce sollicitée. Un système peut mettre en œuvre la distinction de diverses façons. Le paragraphe 5.3.4.1 définit les règles de traitement pour les annonces

sollicitées. Le paragraphe 5.3.4.2 définit les règles de traitement des autres messages.

De plus, les règles suivantes s'appliquent dans tous les cas :
- Les messages reçus sans au moins une option Horodatage et Nom occasionnel DOIVENT être traités comme non sûrs (c'est-à-dire, traités de la même façon que les messages NDP envoyés par un nœud non SEND).
- Les messages reçus avec l'option Signature RSA mais sans l'option Horodatage DOIVENT être éliminés en silence.
- Les messages Sollicitation reçus avec l'option Signature RSA mais sans l'option Nom occasionnel DOIVENT être éliminés en silence.
- Les annonces envoyées à une adresse de destination en envoi individuel avec l'option Signature RSA mais sans l'option Nom occasionnel DEVRAIENT être traités comme des annonces non sollicitées.
- Une mise en œuvre PEUT utiliser des mécanismes comme une antémémoire d'horodatage pour renforcer la résistance aux attaques de répétition. Lorsque il y a un très grand nombre de nœuds sur la même liaison, ou lorsque une attaque de remplissages d'antémémoire est en cours, il est possible que la mémoire tampon qui contient le plus récent horodatage d'envoyeur devienne pleine. Dans ce cas, le nœud DOIT retirer des entrées de la mémoire tampon ou refuser de nouvelles entrées demandées. La politique spécifique de choix des entrées à conserver est une décision de la mise en œuvre. Cependant, les politiques normales peuvent préférer les entrées existantes aux nouvelles, les CGA avec une valeur de Sec élevée à celles qui en ont de petites, et ainsi de suite. La question est brièvement discutée à l'Appendice B.
- Le receveur DOIT être prêt à recevoir les options Horodatage et Nom occasionnel dans n(importe quel ordre, conformément à la Section 9 de la [RFC2461].

5.3.4.1 Traitement des annonces sollicitées

Le receveur DOIT vérifier qu'il a récemment envoyée une sollicitation correspondante, et que l'annonce reçue contient une copie du nom occasionnel envoyé dans la sollicitation.

Si le message contient une option Nom occasionnel mais si la valeur du nom occasionnel n'est pas reconnue, le message DOIT être éliminé en silence.

Autrement, si le message ne contient pas l'option Nom occasionnel, il PEUT être considéré comme une annonce non sollicitée et traité conformément au paragraphe 5.3.4.2.

Si le message est accepté, le receveur DEVRAIT mémoriser l'heure de réception du message et l'horodatage du message, comme spécifié au paragraphe 5.3.4.2.

5.3.4.2 Traitement de tous les autres messages

Les receveurs DEVRAIENT être configurés avec une valeur de différence d'horodatage admise, un "facteur de confusion" pour les comparaisons, et un paramètre de dérive d'horloge admise. La valeur par défaut recommandée pour la différence admise est HORODATAGE_DELTA ; pour le facteur de confusion, HORODATAGE_FUZZ ; et pour la dérive d'horloge, HORODATAGE_DRIFT (voir au paragraphe 10.2).

Pour faciliter la vérification de l'horodatage, chaque nœud DEVRAIT mémoriser les informations suivantes pour chaque homologue :
- l'heure de réception du dernier message SEND reçu et accepté. C'est ce qui est appelé RDlast.
- l'horodatage du dernier message SEND reçu et accepté. C'est de qui est appelé TSlast.

Un message SEND accepté est tout message vérifié avec succès de Sollicitation de voisin, Annonce de voisin, Sollicitation de routeur, Annonce de routeur, ou Redirect provenant de l'homologue en question. L'option Signature RSA DOIT être utilisée dans un tel message avant qu'il puisse mettre à jour les variables ci-dessus.

Les receveurs DEVRAIENT alors vérifier le champ Horodatage comme suit :
- Lorsque un message est reçu d'un nouvel homologue (c'est-à-dire, qui n'est pas mémorisé dans la mémoire tampon) l'horodatage reçu, TSnew, est vérifié, et le paquet est accepté si l'horodatage est assez récent par rapport à l'heure de réception du paquet, Rdnew : -Delta < (RDnew - TSnew) < +Delta
  Les valeurs de RDnew et TSnew DEVRAIENT être mémorisées dans la mémoire tampon comme RDlast et TSlast.
- Si l'horodatage n'est PAS dans les limites mais si le message est une Sollicitation de voisin à laquelle le receveur devrait répondre, le receveur DEVRAIT répondre au message. Cependant,même si il répond au message, il NE DOIT PAS créer une entrée d'antémémoire de voisin. Cela permet aux nœuds qui ont de grosses différences d'horloge de continuer à communiquer en échangeant des paires NS/NA.
- Lorsque un message est reçu d'un homologue connu (c'est-à-dire, qui a déjà une entrée dans la mémoire tampon) l'horodatage est vérifié par rapport au message SEND reçu précédemment : TSnew + fuzz > TSlast + (RDnew - RDlast) x (1 - drift) - fuzz

Si cette inégalité n'est pas vérifiée, le receveur DEVRAIT éliminer en silence le message. Si, par ailleurs, l'inégalité est vérifiée, le receveur DEVRAIT traiter le message.

De plus, si l'inégalité est vérifiée et si TSnew > TSlast, le receveur DEVRAIT mettre à jour RDlast et TSlast. Autrement, le receveur NE DOIT PAS mettre à jour RDlast ou TSlast.

Comme les messages non sollicités peuvent être utilisés dans une attaque de déni de service pour faire que le receveur vérifie des signatures coûteuses en calcul, tous les nœuds DEVRAIENT appliquer un mécanisme pour empêcher une utilisation excessive de ressources pour le traitement de tels messages.

6. Découverte de délégation d'autorisation

NDP permet à un nœud de se configurer automatiquement sur la base des informations apprises peu après la connexion à une nouvelle liaison. Il est particulièrement facile de configurer des routeurs "félons" sur une liaison non sécurisée, et il est particulièrement difficile à un nœud de distinguer entre des sources valides et invalides d'informations de routeur, parce que le nœud a besoin de ces informations avant de communiquer avec des nœuds en dehors de la liaison.

Comme le nœud nouvellement connecté ne peut pas communiquer hors liaison, il ne peut pas être responsable de la recherche d'informations pour l'aider à valider le ou les routeurs. Cependant, étant donné un chemin de certification, le nœud peut vérifier les résultats de la recherche de quelqu'un d'autre et en conclure qu'un message particulier vient d'une source autorisée. Dans le cas normal, un routeur déjà connecté au delà de la liaison peut communiquer si nécessaire avec des nœuds hors liaison et construire un chemin de certification.

Le protocole sûr de découverte de voisin rend obligatoire un format de certificat et introduit deux nouveaux messages ICMPv6 utilisés entre hôtes et routeurs pour permettre à l'hôte d'apprendre un chemin de certification avec l'assistance du routeur.

6.1 Modèle d'autorisation

Pour protéger la découverte de routeur, SEND exige que les routeurs soient autorisés à agir comme routeurs. Cette autorisation est provisionnée dans les routeurs et dans les hôtes. Les routeurs reçoivent des certificats d'une ancre de confiance, et les hôtes sont configurés avec les ancres de confiance pour autoriser les routeurs. Ce provisionnement est spécifique de SEND et ne suppose pas que les certificats déjà déployés à d'autres fins puissent être utilisés.

L'autorisation pour les routeurs dans SEND est en deux étapes :

- Les routeurs sont autorisés à agir comme routeurs. Le routeur appartient à l'ensemble des routeurs de confiance pour l'ancre de confiance. Tous les routeurs de cet ensemble ont la même autorisation.
- Facultativement, les routeurs peuvent aussi être autorisés à annoncer un certain ensemble de préfixes de sous réseau. Un certain routeur reçoit un certain ensemble de préfixes de sous réseau à annoncer ; d'autres routeurs ont une autorisation d'annoncer d'autres préfixes de sous réseau. Les ancres de confiance peuvent aussi déléguer un certain ensemble de préfixes de sous réseau à quelqu'un (comme un FAI) qui, à son tour, délègue des parties de cet ensemble aux routeurs individuels.

Noter que tout en communiquant avec les hôtes, les routeurs présentent aussi normalement un certain nombre d'autres paramètres au delà de ceux présentés ci-dessus. Par exemple, les routeurs ont leurs propres adresses IP, les préfixes de sous réseau ont une durée de vie, et les routeurs contrôlent l'utilisation de l'autoconfiguration d'adresse à états pleins et sans état. Cependant, la capacité d'être un routeur et les préfixes de sous réseau sont les paramètres les plus fondamentaux à autoriser. Ceci parce que l'hôte a besoin de choisir un routeur qu'il utilise comme routeur par défaut, et parce que les préfixes de sous réseau annoncés ont un impact sur les adresses qu'utilise l'hôte. Les préfixes de sous réseau représentent aussi une revendication sur la localisation topologique du routeur dans le réseau.

Il faut faire attention si les certificats utilisés dans SEND sont aussi utilisés pour fournir une autorisation dans d'autres circonstances ; par exemple, avec les protocoles d'acheminement. Il est nécessaire de s'assurer que les informations d'autorisation sont appropriées pour toutes les applications. Les certificats SEND peuvent autoriser un ensemble plus large de préfixes de sous réseau que le routeur n'est autorisé à annoncer sur une certaine interface. Par exemple, SEND permet l'utilisation du préfixe nul, qui peut causer des problèmes de vérification ou d'acheminement dans d'autres applications. Il est RECOMMANDÉ que les certificats SEND qui contiennent le préfixe nul soient utilisés seulement pour SEND.

Noter que les hôtes d'extrémité n'ont pas besoin d'être provisionnés avec leurs propres clés publiques certifiées, tout comme les clients de la Toile aujourd'hui n'exigent pas que l'hôte d'extrémité soit provisionné avec des clés certifiées. Les clés publiques pour la génération de CGA n'ont pas besoin d'être certifiées, car ces clés tirent leur capacité d'autoriser des opérations sur la CGA du lien avec l'adresse.

6.2 Modèle de déploiement

Le modèle de déploiement pour les ancres de confiance peut être soit une infrastructure de clé publique à racine mondiale, soit un modèle de déploiement décentralisé plus local, similaire à celui actuellement utilisé pour TLS dans les serveurs de la Toile. Le modèle centralisé suppose une racine mondiale capable d'autoriser les routeurs et, facultativement, l'espace d'adresse qu'ils annoncent. Les hôtes finaux sont configurés avec les clés publiques de la racine mondiale. La racine mondiale pourrait fonctionner, par exemple, sous l'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) ou comme une coopérative entre les registraires régionaux de l'Internet (RIR). Cependant, une telle racine mondiale n'existe pas actuellement.

Dans le modèle décentralisé, les hôtes d'extrémité sont configurés avec une collection de clés publiques de confiance. Les clés publiques pourraient être produites en divers endroits ; par exemple, a) une clé publique pour la propre organisation de l'hôte d'extrémité, b) une clé publique pour le FAI de rattachement de l'hôte d'extrémité et pour les FAI avec lesquels le FAI de rattachement a un accord d'itinérance, ou c) des clés publiques pour les courtiers d'itinérance qui agissent comme intermédiaires pour les FAI qui ne veulent pas avoir leur propre autorité de certification.

Ce modèle décentralisé fonctionne même quand un nœud SEND est utilisé à la fois dans des réseaux qui ont des routeurs certifiés et dans des réseaux qui n'en ont pas. Comme exposé à la Section 8, un nœud SEND peut revenir à l'utilisation d'un routeur non SEND. Cela rend possible de commencer avec une ancre de confiance locale même si il n'y a pas d'ancre de confiance pour tous les réseaux possibles.

6.3 Format de certificat

Le chemin de certification d'un routeur se termine dans un certificat d'autorisation de routeur qui autorise un nœud IPv6 spécifique à agir comme un routeur. Parce que les chemins d'autorisation ne sont pas de pratique courante dans l'Internet au moment de cette rédaction, le chemin DOIT consister en certificats de clé publique (PKC, *Public Key Certificates*) standard, au sens de la [RFC3281]. Le chemin de certification DOIT commencer à l'identité d'une ancre de confiance partagée par l'hôte et le routeur. Cela permet à l'hôte d'ancrer la confiance en la clé publique du routeur dans l'ancre de confiance. Noter qu'il PEUT y avoir plusieurs certificats produits par une seule ancre de confiance.

6.3.1 Profil de certificat d'autorisation de routeur

Les certificats d'autorisation de routeur sont des certificats X.509v3, comme défini dans la [RFC3280], et DEVRAIENT contenir au moins une instance de l'extension X.509 pour les adresses IP, comme défini dans la [RFC3779]. Les certificats parents dans le chemin de certification DEVRAIENT contenir une ou plusieurs extensions X.509 d'adresse IP, un repli sur un tiers de confiance (comme le FAI de l'usager) qui a configuré le bloc d'adresse IP original pour le routeur en question, ou qui a délégué le droit de le faire. Les certificats pour les autorités délégantes intermédiaires DEVRAIENT contenir la ou les extensions X.509 d'adresse IP pour les sous délégations. Le certificat de routeur est signé par l'autorité délégante pour les préfixes de sous réseau que le routeur est autorisé à annoncer.

L'extension X.509 d'adresse IP DOIT contenir au moins un élément addressesOrRanges *(adresses ou gammes)*. Cet élément DOIT contenir un élément addressPrefix *(préfixe d'adresse)* contenant un préfixe d'adresse IPv6 pour un préfixe que le routeur ou l'entité intermédiaire est autorisée à acheminer. Si il est permis à l'entité d'acheminer tout préfixe, le préfixe d'adresse IPv6 utilisé est le préfixe nul, ::/0. L'élément addressFamily *(famille d'adresse)* de l'élément de séquence IPAddrBlocks *(blocs d'adresses IP)* DOIT contenir l'identifiant de famille d'adresse IPv6 (0002), comme spécifié dans la [RFC3779], pour les préfixes de sous réseau IPv6. Au lieu d'un élément addressPrefix, l'élément addressesOrRange PEUT contenir un élément addressRange pour une gamme de préfixes de sous réseau, si plus d'un préfixe est autorisé. L'extension X.509 d'adresse IP PEUT contenir des préfixes de sous réseau IPv6 supplémentaires, exprimés comme addressPrefix ou addressRange.

Un nœud qui reçoit un certificat d'autorisation de routeur DOIT d'abord vérifier si la signature du certificat a été générée par l'autorité délégante. Ensuite, le client DEVRAIT vérifier si toutes les entrées de addressPrefix ou addressRange dans le certificat du routeur sont contenues dans cette gamme d'adresses du certificat de l'autorité délégante, et si les entrées de addressPrefix correspondent à des entrées de addressPrefix dans le certificat de l'autorité délégante. Si un addressPrefix ou une addressRange n'est pas contenue dans les préfixes ou gammes de sous réseau de l'autorité délégante, le client PEUT tenter de prendre l'intersection des préfixes de gammes/sous réseaux et d'utiliser cette intersection. Si l'intersection est vide, le client NE DOIT PAS accepter le certificat. Si le addressPrefix manque dans le certificat ou est le préfixe nul, ::/0, on DEVRAIT utiliser le préfixe ou gamme parent. Si il n'y a pas de préfixe ou gamme parent, les préfixes de sous réseau qu'annonce le routeur sont dits être sans contrainte (voir au paragraphe 7.3). C'est-à-dire , il est permis au routeur d'annoncer tous les préfixes.

Les vérifications ci-dessus DEVRAIENT être faites pour tous les certificats dans le chemin. Si une des vérifications échoue, le client NE DOIT PAS accepter le certificat. Le client doit aussi effectuer la validation des préfixes de sous réseau annoncés

comme exposé au paragraphe 7.3.

Les hôtes DOIVENT vérifier le champ subjectPublicKeyInfo *(informations de clé publique du sujet)* dans le dernier certificat du chemin de certificat pour s'assurer que seules des clés publiques RSA sont utilisées pour tenter la validation des signatures de routeur. Les hôtes DOIVENT rejeter un certificat pour SEND si il ne contient pas une clé RSA.

Comme il est possible que certains certificats de clé publique utilisés avec SEND ne contiennent pas immédiatement l'élément d'extension X.509 d'adresse IP, une mise en œuvre PEUT contenir des facilités qui permettent d'assouplir les vérifications de préfixe et de gamme. Cependant, une telle option de configuration DEVRAIT être désactivée par défaut. Le système DEVRAIT avoir une configuration par défaut qui exige des vérifications rigoureuses des préfixes et des gammes.

Voici un exemple de chemin de certification. On suppose que isp_group_example.net est l'ancre de confiance. L'hôte a le certificat suivant :

Certificat 1 :
Producteur : isp_group_example.net
Validité : du 1er janvier 2004 au 31 décembre 2004
Sujet : isp_group_example.net
Extensions :
extension de délégation d'adresse IP :
Préfixes : P1, ..., Pk
... autres extensions éventuelles...
... autres paramètres de certificat ...

Lorsque l'hôte se rattache à une liaison desservie par le routeur_x.isp_foo_example.net, il reçoit le chemin de certification suivant :

Certificat 2 :
Producteur : isp_group_example.net
Validité : du 1er janvier 2004 au 31 décembre 2004
Sujet : isp_foo_example.net
Extensions:
extension de délégation d'adresse IP :
Préfixes : Q1, ..., Qk
... autres extensions éventuelles...
... autres paramètres de certificat ...

Certificat 3 :
Producteur : isp_foo_example.net
Validité : du 1er janvier 2004 au 31 décembre 2004
Sujet : routeur_x.isp_foo_example.net
Extensions:
extension de délégation d'adresse IP :
Préfixes R1, ..., Rk
... autres extensions éventuelles...
... autres paramètres de certificat ...

Lorsque les trois certificats sont traités, on effectue la validation usuelle de chemin de certificat de la [RFC3280]. Noter cependant, que lorsque un nœud vérifie les certificats reçus d'un routeur, il n'a normalement pas encore de connexion à l'Internet, de sorte qu'il n'est pas possible d'effectuer une vérification en ligne de liste de révocation de certificat (CRL) si nécessaire. Tant que cette vérification n'est pas faite, l'acceptation du certificat DOIT être considérée comme provisoire, et le nœud DOIT effectuer une vérification aussitôt qu'il a établi une connexion à l'Internet à travers le routeur. Si le routeur a été compromis, il pourrait interférer avec la vérification de CRL. Si les performances de la vérification de CRL devaient être perturbées ou si la vérification échoue, le nœud DEVRAIT immédiatement arrêter d'utiliser le routeur comme routeur par défaut et utiliser à la place un autre routeur sur la liaison.

De plus, les adresses IP dans l'extension de délégation DOIVENT être un sous ensemble des adresses IP dans l'extension de délégation du certificat du producteur. Ainsi, dans cet exemple, R1, ..., Rs doit être un sous ensemble de Q1,...,Qr, et Q1,...,Qr doit être un sous ensemble de P1,...,Pk. Si le chemin de certification est valide, alors router_foo.isp_foo_example.com est autorisé à acheminer les préfixes R1,...,Rs.

6.3.2 Aptitude des certificats d'identité standard

Comme le déploiement de l'extension d'adresse IP n'est pas courant par lui-même, un fournisseur de service réseau PEUT choisir de déployer des certificats d'identité standard sur le routeur pour fournie la clé publique du routeur pour les annonces de routeur signées.

Si il n'y a pas d'informations de préfixes plus loin sur le chemin de certification, un hôte interprètera un certificat d'identité standard comme permettant des annonces de préfixes sans contraintes.

Si les autres certificats contiennent des informations de préfixes, un certificat d'identité standard est interprété comme permettant ces préfixes de sous réseau.

6.4 Transport de certificat

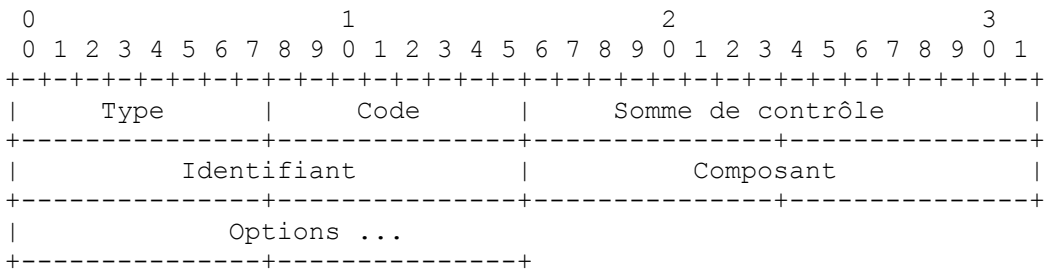
Le message Sollicitation de chemin de certification (CPS, *Certification Path Solicitation*) est envoyé par un hôte lorsque il souhaite demander un chemin de certification entre un routeur et une des ancres de confiance de l'hôte. Le message Annonce de chemin de certification (CPA, *Certification Path Advertisement*) est envoyé en réponse au message CPS. Ces messages sont gardés séparés du reste de la découverte de voisin et de routeur pour réduire les effets des informations potentiellement volumineuses de chemin de certification sur les autres messages.

Le processus de découverte de délégation d'autorisation (ADD, *Authorization Delegation Discovery*) n'exclut pas d'autres formes de découverte des chemins de certification. Par exemple, durant des mouvements rapides, des nœuds mobiles peuvent apprendre des informations (incluant des chemins de certification) sur le prochain routeur d'un routeur précédent, ou des nœuds peuvent être préconfigurés avec des chemins de certification à partir des partenaires d'itinérance.

Lorsque les hôtes sont eux-mêmes certifiés par une ancre de confiance, ces messages PEUVENT aussi être facultativement utilisés entre les hôtes pour acquérir le chemin de certification de l'homologue. Cependant, les détails d'un tel usage sortent du domaine d'application de la présente spécification.

6.4.1 Format de message Sollicitation de chemin de certification

Les hôtes envoient des sollicitations de chemin de certification afin de d'inviter les routeurs à générer des annonces de chemin de certification.



Champs IP :

Adresse de source : adresse d'envoi individuel de liaison locale allouée à l'interface d'envoi, ou à l'adresse non spécifiée si aucune adresse n'est allouée à l'interface d'envoi.

Adresse de destination : normalement l'adresse de diffusion groupé Tous-les-routeurs, l'adresse de diffusion groupée du nœud sollicité, ou l'adresse du routeur par défaut de l'hôte.

Limite de bonds : 255

Champs ICMP :

Type : 148

Code : 0

Somme de contrôle : somme de contrôle ICMP [RFC2463].

Identifiant : champ d'entier non signé de 16 bits, jouant le rôle d'identifiant pour aider à confronter les annonces aux

sollicitations. le champ Identifiant NE DOIT PAS être zéro, et sa valeur DEVRAIT être générée au hasard. Cette aléation ne doit pas être trop dure cryptographiquement, car son objet est seulement d'éviter des collisions.

Composant : champ d'entier non signé de 16 bits réglé à 65 535 si l'envoyeur cherche à restituer tous les certificats. Autrement, il est réglé à l'identifiant de composant correspondant au certificat que le receveur veut restituer (voir les paragraphes 6.4.2 et 6.4.6).

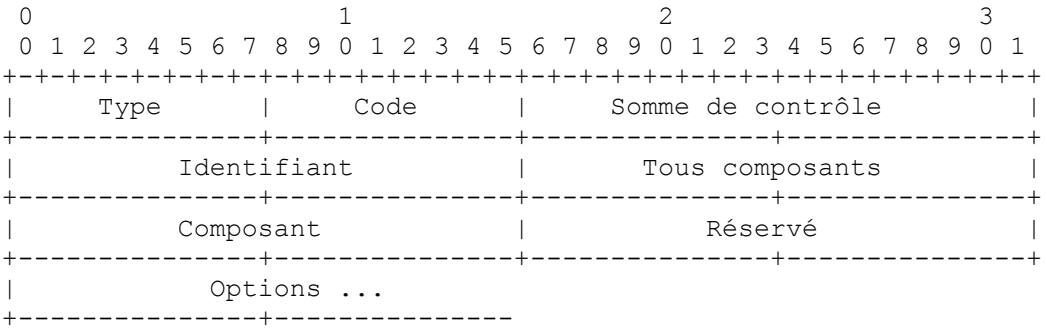
Options valides : ancre de confiance. Une ou plusieurs ancres de confiance que le client veut accepter. La première (ou la seule) option Ancre de confiance DOIT contenir un nom X.501 codé en DER ; voir le paragraphe 6.4.3. Si il y a plus d'une option Ancre de confiance, les options au delà de la première peuvent contenir tout type d'ancre de confiance.

De futures versions de ce protocole peuvent définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toutes les options qu'ils ne reconnaissent pas et continuer de traiter le message. Toutes les options incluses DOIVENT avoir une longueur supérieure à zéro.

Longueur ICMP (dérivée de la longueur IP) DOIT être de 8 octets ou plus.

6.4.2 Format de message Annonce de chemin de certification

Les routeurs envoient les messages Annonce de chemin de certification en réponse aux sollicitations de chemin de certification.



Champs IP :

Adresse de source : adresse d'envoi individuel de liaison locale allouée à l'interface de laquelle ce message est envoyé. Noter que les routeurs peuvent utiliser plusieurs adresses, et donc cette adresse n'est pas suffisante pour l'identification univoque des routeurs.

Adresse de destination : soit l'adresse de diffusion groupée du nœud sollicité du receveur, soit l'adresse de diffusion groupée Tous-les-nœuds de la portée de la liaison.

Limite de bonds : 255

Champs ICMP :

Type : 149

Code : 0

Somme de contrôle : somme de contrôle ICMP [RFC2463].

Identifiant : champ d'entier non signé de 16 bits, agissant comme un identifiant pour aider à confronter les annonces aux sollicitations. Le champ Identifiant DOIT être zéro pour les annonces envoyées à l'adresse de diffusion groupée Tous-les-nœuds et NE DOIT PAS être zéro pour les autres.

Tous composants : champ d'entier non signé de 16 bits, utilisé pour informer le receveur du nombre de certificats dans le chemin tout entier. une seule annonce DEVRAIT être coupée en plusieurs Composants envoyés séparément si il y a plus d'un certificat dans le chemin, afin d'éviter une fragmentation excessive à la couche IP. Les certificats individuels dans un chemin PEUVENT être mémorisés et utilisés comme reçus avant que tous les certificats soient arrivés ; ceci rend le protocole légèrement plus fiable et moins enclin aux attaques de déni de service. Des exemples de longueurs de paquet

de message Annonce de chemin de certification pour les chemins de certification normaux sont donnés à l'Appendice C.

Composant : champ d'entier non signé de 16 bits, utilisé pour informer le receveur du certificat qui est envoyé. Le premier message dans une annonce N-Composant a le champ Composant réglé à N-1, le second réglé à N-2, et ainsi de suite. Un zéro indique qu'il n'y a plus d'autres composants à venir dans cette annonce. L'envoi de composants de chemin DEVRAIT être ordonné de façon que le certificat après l'ancre de confiance soit envoyé en premier. Chaque certificat envoyé après le premier peut être vérifié avec les certificats envoyés antérieurement. Le certificat de l'envoyeur vient en dernier. Le certificat d'ancre de confiance NE DEVRAIT PAS être envoyé.

Réservé : champ non utilisé. Il DOIT être initialisé à zéro par l'envoyeur et DOIT être ignoré par le receveur.

Options valides : Certificat ; un certificat est fourni dans chaque option Certificat pour établir une partie d'un chemin de certification à une ancre de confiance. Le certificat de l'ancre de confiance lui-même NE DEVRAIT PAS être envoyé.

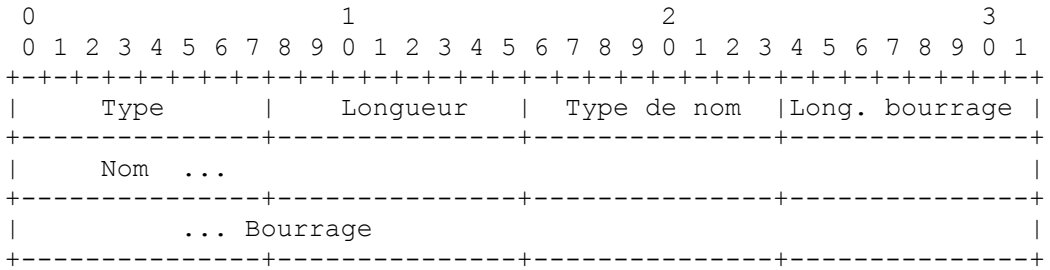
Ancre de confiance : zéro, une ou plusieurs options Ancre de confiances peuvent être incluses pour aider les receveurs à décider quelles annonces sont utiles pour eux. Si elles sont présentes, ces options DOIVENT apparaître dans le premier composant d'une annonce multi composants.

De futures versions de ce protocole pourront définir de nouveaux types d'option. Les receveurs DOIVENT ignorer en silence toute option qu'ils ne reconnaissent pas et continuer le traitement du message. Toutes les options incluses DOIVENT avoir une longueur supérieure à zéro.

La longueur ICMP (dérivée de la longueur IP) DOIT être de 8 octets ou plus.

6.4.3 Option Ancre de confiance

Le format de l'option Ancre de confiance est décrit ci-dessous :



Type : 15

Longueur : longueur de l'option (incluant les champs Type, Longueur, Type de nom, Longueur du bourrage, et Nom) en unîtes de 8 octets.

Type de nom : type du nom inclus dans le champ Nom. La présente spécification définit deux valeurs légales pour ce champ :
1 Nom X.501 codé en DER
2 FQDN

Longueur bourrage : nombre d'octets de bourrage au delà de la fin du champ Nom mais dans la longueur spécifiée par le champ Longueur. Les octets de bourrage DOIVENT être réglés à zéro par les envoyeurs et ignorés à réception.

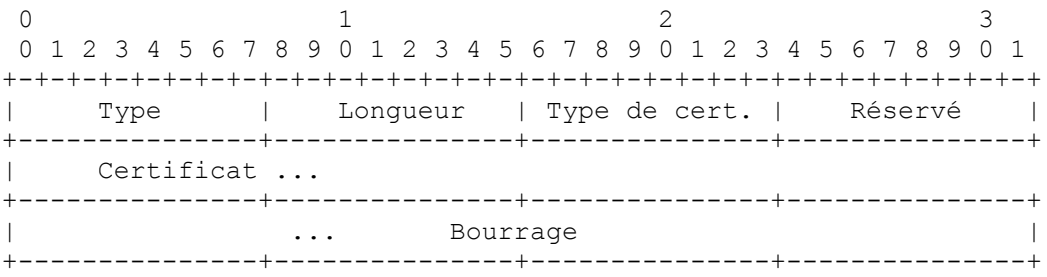
Nom : Lorsque le champ Type de nom est réglé à 1, le champ Nom contient un nom X.501 codé en DER qui identifie l'ancre de confiance. La valeur est codée comme défini dans [X.690] et la [RFC3280]. Lorsque le champ Type de nom est réglé à 2, le champ Nom contient un nom de domaine complet de l'ancre de confiance ; par exemple, "trustanchor.example.com". Le nom est mémorisé comme une chaîne, dans le format réseau du DNS, comme spécifié dans la [RFC1034]. De plus, les restrictions exposées au paragraphe 4.2.2.7 de la [RFC3280] s'appliquent. Dans le cas d'un FQDN, le champ Nom est un "nom de domaine qui ignore les IDN", comme défini dans la [RFC3490]. C'est-à-dire qu'il ne peut contenir que des caractères ASCII. Une mise en œuvre PEUT prendre en charge les noms de domaines internationalisés (IDN) en utilisant l'opération ToASCII ; voir plus d'informations dans la [RFC3490]. Tous les systèmes DOIVENT accepter les noms X.501 codés en DER. Les mises en œuvre PEUVENT prendre en charge le type de nom FQDN.

Bourrage : champ de longueur variable rendant la longueur d'option multiple de 8, qui commence après le champ précédent et

qui continue jusqu'à la fin de l'option, comme spécifié par le champ Longueur.

6.4.4 Option Certificat

Le format de l'option Certificat est décrit ci-dessous :



Type : 16

Longueur : longueur de l'option (incluant les champs Type, Longueur, Type de cert., Longueur de bourrage, et Certificat) en unités de 8 octets.

Type de cert. : type du certificat inclus dans le champ Certificat. La présente spécification définit seulement une valeur légale pour ce champ : 1 : Certificat X.509v3, comme spécifié ci-dessous.

Réservé : champ de 8 bits réservé pour une utilisation future. La valeur DOIT être initialisée à zéro par l'envoyeur et DOIT être ignorée par le receveur.

Certificat : lorsque le champ Type de certificat est réglé à 1, le champ Certificat contient un certificat X.509v3 [RFC3280], comme décrit au paragraphe 6.3.1.

Bourrage : champ de longueur variable faisant de la longueur de l'option un multiple de 8, commençant après la fin du codage ASN.1 du champ précédent [RFC3280], [RFC2409] et continuant jusqu'à la fin de l'option, comme spécifié par le champ Longueur.

6.4.5 Règles de traitement pour les routeurs

Un routeur DOIT éliminer en silence tous les messages de sollicitation de chemin de certification reçus qui ne se conforment pas au format de message défini au paragraphe 6.4.1. Le contenu du champ Réservé et de toutes les options non reconnues DOIT être ignoré. De futurs changements rétro compatibles du protocole pourront spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro compatibles pourront utiliser des valeurs de code différentes. Le contenu de toute option définie qui n'est pas spécifiée pour être utilisée avec les messages Sollicitation de routeur DOIT être ignoré, et le paquet traité de la façon normale. La seule option définie qui peut apparaître est l'option Ancre de confiance. Une sollicitation qui satisfait aux vérifications de validité est appelée une "sollicitation valide".

Les routeurs DEVRAIENT envoyer des annonces en réponse aux sollicitations valides reçues sur une interface d'annonce. Si l'adresse de source dans la sollicitation était l'adresse non spécifiée, le routeur DOIT envoyer la réponse à l'adresse de diffusion groupée Tous-les-nœuds de la portée de la liaison. Si l'adresse de source était une adresse d'envoi individuel, le routeur DOIT envoyer la réponse à l'adresse de diffusion groupée du nœud sollicité correspondant à l'adresse de source, sauf quand en charge, comme spécifié ci-dessous. Les routeurs NE DEVRAIENT PAS envoyer d'annonces de chemin de certification plus de MAX_CPA_RATE fois par seconde. Si il y a plus de sollicitations, le routeur DEVRAIT envoyer la réponse à l'adresse de diffusion groupée Tous-les-nœuds sans considération de l'adresse de source qui apparaît dans la sollicitation.

Dans une annonce, le routeur DEVRAIT inclure des options Certificat convenables afin qu'un chemin de certification puisse être établi jusqu'à l'ancre de confiance sollicitée (ou une de ses parties, si le champ Composant dans la sollicitation n'est pas égal à 65 535). Noter aussi qu'une seule annonce est coupée en composants envoyés séparément et ordonnés d'une façon particulière (voir au paragraphe 6.4.2) lorsque il y a plus d'un certificat dans le chemin.

L'ancre est identifiée par l'option Ancre de confiance. Si l'option Ancre de confiance est représentée comme un nom X.501 codé en DER, le nom doit alors être égal au champ Sujet dans le certificat de l'ancre. Si l'option Ancre de confiance est représenté comme un FQDN, le FQDN doit être égal à un FQDN dans le champ subjectAltName du certificat de l'ancre. Le routeur DEVRAIT inclure la ou les options Ancre de confiance dans l'annonce pour laquelle le chemin de certification s'est trouvé.

Si le routeur ne réussit pas à trouver un chemin pour l'ancre demandée, il DEVRAIT envoyer une annonce sans aucun certificat. Dans ce cas, le routeur DEVRAIT inclure l'option Ancre de confiances qui était sollicitée.

6.4.6 Règles de traitement pour les hôtes

Un hôte DOIT éliminer en silence tout message d'annonce de chemin de certification reçu qui ne se conforme pas au format de message défini au paragraphe 6.4.2. Le contenu du champ Réservé, et toute option non reconnue, DOIVENT être ignorés. De futurs changements rétro compatibles du protocole POURRONT spécifier le contenu du champ Réservé ou ajouter de nouvelles options ; les changements non rétro compatibles DOIVENT utiliser des valeurs de code différentes. Le contenu de toutes les options non spécifiées pour être utilisées avec les messages d'annonce de chemin de certification DOIVENT être ignorées, et le paquet traité de la façon normale. Les seules options définies qui peuvent apparaître sont les options Certificat et Ancre de confiance. Une annonce qui satisfait aux vérifications de validité est appelée une "annonce valide".

Les hôtes DEVRAIENT mémoriser les chemins de certification restitués dans les messages de découverte de chemin de certification si ils commencent par une ancre qui est de confiance pour l'hôte. Les chemins de certification DOIVENT être vérifiés, comme défini au paragraphe 6.3, avant de les mémoriser. Les routeurs envoient les certificats un par un, en commençant par l'ancre de confiance de la fin du chemin.

Note : sauf pour permettre les pertes de message et le réarrangement pour des besoins temporaires, les hôtes peuvent ne pas mémoriser les certificats reçus dans une annonce de chemin de certification sauf si ils contiennent un certificat qui peut être immédiatement vérifié soit par rapport à l'ancre de confiance, soit par rapport à un certificat qui a été vérifié antérieurement. Cette mesure est destinée à empêcher les attaques de déni de service, par lesquelles un attaquant inonde un hôte avec des certificats que l'hôte ne peut pas valider et remplissent la mémoire de stockage des certificats.

Noter que la mise en antémémoire de ces informations, et les résultats de vérification impliqués entre rattachements de réseau à utiliser sur plusieurs rattachements au réseau, peut aider à améliorer les performances. Mais les vérifications périodiques de révocation de certificat sont quand même nécessaires, même avec des résultats en antémémoire, pour s'assurer que le certificat est encore valide.

L'hôte DEVRAIT récupérer un chemin de certification lorsque une annonce de routeur a été reçue avec une clé publique qui n'est pas disponible à partir d'un certificat dans l'antémémoire de l'hôte, ou lorsque il n'y a pas de chemin de certification jusqu'à une des ancres de confiance de l'hôte. Dans ces situations, l'hôte PEUT envoyer un message Sollicitation de chemin de certification pour récupérer le chemin. Si il n'y a pas de réponse dans les CPS_RETRY secondes, le message devrait être réessayé. L'intervalle d'attente pour chaque retransmission suivante DOIT augmenter de façon exponentielle, en doublant à chaque fois. Si il n'y a pas de réponse après CPS_RETRY_MAX secondes, l'hôte abandonne le processus de restitution de chemin de certification. Si l'hôte reçoit seulement une partie d'un chemin de certification dans les CPS_RETRY_FRAGMENTS secondes de la réception de la première partie, il PEUT en plus transmettre un message Sollicitation de chemin de certification avec le champ Composant réglé à une valeur non égale à 65 535. Ce message peut être retransmis en utilisant le même processus que pour le message initial. Si il manque plusieurs certificats, des messages CPS supplémentaires peuvent être envoyés après avoir reçu une réponse pour le premier. Cependant, le processus de restitution complet ne peut durer au plus que CPS_RETRY_MAX secondes.

Les sollicitations de chemin de certification NE DEVRAIENT PAS être envoyées si l'hôte a un chemin de certification actuellement valide entre un routeur accessible et une ancre de confiance.

Lorsque il sollicite des certificats pour un routeur, un hôte DOIT envoyer des sollicitations de chemin de certification soit à l'adresse de diffusion groupée Tous-les-routeurs, si il n'a pas encore choisi un routeur par défaut, soit à l'adresse IP du routeur par défaut, si un routeur par défaut a déjà été choisi.

Si deux hôtes veulent établir la confiance avec les messages CPS et CPA, le message CPS DEVRAIT être envoyés à l'adresse de diffusion groupée du nœud sollicité du receveur. L'annonce DEVRAIT être envoyée comme spécifié ci-dessus pour les routeurs. Cependant, les détails exacts sortent du domaine d'application de cette spécification.

Lorsque il traite les annonces possibles envoyées en réponse à une sollicitation, l'hôte PEUT préférer traiter d'abord les annonces avec la même valeur de champ Identifiant que celle de cette sollicitation. Cela rend plus difficiles les attaques de déni de service contre le mécanisme (voir au paragraphe 9.3).

6.5 Configuration

Les hôtes d'extrémité sont configurés avec un ensemble d'ancres de confiance afin de protéger la découverte de routeur. Une configuration d'ancre de confiance consiste en les éléments suivants :

- o un algorithme de signature de clé publique et la clé publique associée, qui peut facultativement inclure des paramètres ;
- o un nom comme décrit au paragraphe 6.4.3 ;
- o un identifiant de clé publique facultatif ;
- o une liste facultative des gammes d'adresses pour lesquelles l'ancre de confiance est autorisée.

Si l'hôte a été configuré à utiliser SEND, il DEVRAIT posséder les informations ci-dessus pour au moins une ancre de confiance.

Les routeurs sont configurés avec une collection de chemins de certification et une collection de certificats contenant des clés certifiées, jusqu'à la clé et le certificat pour le routeur lui-même. Les clés certifiées sont exigées pour les routeurs afin qu'un chemin de certification puisse être établi entre le certificat du routeur et la clé publique d'une ancre de confiance.

Si le routeur a été configuré à utiliser SEND, il devrait être configuré avec sa propre paire de clé et certificat, et avec au moins un chemin de certification.

7. Adressage

7.1 CGA

Par défaut, un nœud à capacité SEND DEVRAIT utiliser seulement des CGA pour ses propres adresses. D'autres types d'adresses PEUVENT être utilisés pour des essais, des diagnostics, ou pour d'autres objets. Cependant, le présent document ne décrit pas comment choisir entre les différents types d'adresses pour les différentes communications. Un choix dynamique peut être fourni par une API, comme celle définie dans la [RFC5014].

7.2. Adresses redirigées

Si les champs Adresse cible et Adresse de destination dans le message ICMP Redirect sont égaux, alors ce message est utilisé pour informer les hôtes qu'une destination est, en fait, un voisin. Dans ce cas, le receveur DOIT vérifier que cette adresse tombe dans la gamme définie par le certificat du routeur. Les messages Redirect qui échouent à cette vérification DOIVENT être traités comme non sûrs, comme décrit au paragraphe 7.3.

Noter que les règles de base de NDP empêchent un hôte d'accepter un message Redirect provenant d'un routeur que l'hôte n'utilise pas pour atteindre la destination mentionnée dans le Redirect. Cela empêche un attaquant de tromper un nœud en redirigeant le trafic lorsque l'attaquant n'est pas le routeur par défaut.

7.3 Préfixes de sous réseau annoncés

Le certificat de routeur définit la ou les gammes d'adresses qu'il lui est permis d'annoncer en toute sécurité. Un routeur PEUT, cependant, annoncer une combinaison de préfixes de sous réseaux certifiés et non certifiés. Les préfixes de sous réseau non certifiés sont traités comme non sûrs (c'est-à-dire, traités de la même façon que les annonces de routeur non sécurisées envoyées par des routeurs non SEND). Le traitement des messages non sûrs est spécifié à la Section 8. Noter que les nœuds SEND qui ne tentent pas d'interopérer avec des nœuds non SEND PEUVENT simplement éliminer les informations non sûres. Les préfixes de sous réseau certifiés entrent dans les deux catégories suivantes :

Contraints : si l'opérateur du réseau veut contraindre les routeurs à qui il est permis d'acheminer des préfixes de sous réseau particuliers, les routeurs devraient être configurés avec des certificats qui ont les préfixes de sous réseau mentionnés dans l'extension de préfixes. Ces routeurs DEVRAIENT annoncer les préfixes de sous réseau qu'ils sont certifiés pour acheminer, ou un sous ensemble de ceux-ci.

Non contraints : les opérateurs de réseau qui ne veulent pas contraindre les routeurs de cette façon devraient configurer les routeurs avec des certificats contenant soit le préfixe nul, soit pas d'extension de préfixe du tout.

Lors du traitement de l'option Informations de préfixe dans une annonce de routeur, les nœuds DEVRAIENT vérifier que le préfixe spécifié dans cette option entre dans la gamme définie par le certificat, si le certificat contient une extension de préfixe. Les options qui échouent à cette vérification sont traitées comme contenant des préfixes de sous réseau non certifiés.

Les nœuds DEVRAIENT utiliser un des préfixes de sous réseau certifiés pour l'autoconfiguration sans état. Si aucun des préfixes de sous réseau annoncés ne correspond, l'hôte DEVRAIT utiliser un routeur annonceur différent comme son routeur par défaut, si il en est un disponible. Si le nœud effectue une autoconfiguration à états pleins, il DEVRAIT vérifier l'adresse fournie par le serveur DHCP par rapport aux préfixes de sous réseau certifiés et NE DEVRAIT PAS utiliser l'adresse si le préfixe n'est pas certifié.

7.4 Limitations

La présente spécification ne traite pas de la protection des paquets NDP pour les nœuds configurés avec une adresse statique (par exemple, PREFIX::1). De futures spécifications d'autorisation fondée sur le chemin de certification sont nécessaires pour ces nœuds. La présente spécification ne s'applique pas non plus aux adresses générées par l'autoconfiguration d'adresse IPv6 sans état à partir d'identifiants d'interface fixes (comme EUI-64).

Il sort du domaine d'application de la présente spécification de décrire l'utilisation de l'autorisation de l'ancre de confiance entre des nœuds qui ont des adresses qui changent de façon dynamique. Ces adresses peuvent être le résultat d'une autoconfiguration d'adresse à états pleins ou sans état, ou peuvent avoir résulté de l'utilisation des adresses de la [RFC3041]. Si la méthode de la CGA n'est pas utilisée, les nœuds sont obligés d'échanger les chemins de certification qui se terminent par un certificat qui autorise un nœud à utiliser une adresse IP ayant un identifiant d'interface particulier. La présente spécification ne spécifie pas le format de ces certificats, car il n'y a actuellement que peu de cas où ils sont fournis par la couche de liaison, et il appartient à la couche de liaison de fournir la certification de l'identifiant d'interface. Ceci pourra faire l'objet d'une future spécification. Il sort aussi du domaine d'application de cette spécification de décrire comment fonctionne l'autoconfiguration d'adresse à états pleins avec la méthode de la CGA.

L'adresse de cible dans une annonce de voisin est obligatoirement égale à l'adresse de source du paquet, sauf dans la découverte de voisin par un mandataire, qui n'est pas prise en charge par la présente spécification.

8. Questions de transition

Durant la transition vers les liaisons sécurisées, ou comme considération de politique, les opérateurs de réseaux peuvent vouloir faire fonctionner une certaine liaison avec un mélange de nœuds acceptant des messages sécurisé et non sécurisés. Les nœuds qui prennent en charge SEND DEVRAIENT accepter l'utilisation de messages NDP sécurisés et non sécurisés en même temps.

Dans un environnement mixte, les nœuds SEND reçoivent des messages sécurisés et non sécurisés mais donnent la priorité à ceux qui sont sécurisés. Ici, les messages "sécurisés" sont ceux qui contiennent une option Signature valide, comme spécifié ci-dessus et les messages "non sécurisés" sont ceux qui ne contiennent pas d'option Signature.

Un nœud SEND DEVRAIT avoir une option de configuration qui lui fasse ignorer tous les messages Sollicitation et Annonce de voisin, Sollicitation et Annonce de routeur, et Redirect non sécurisés. Ceci peut être utilisé pour mettre en application des réseaux seulement SEND. Par défaut, cette option de configuration DEVRAIT être que les messages sécurisés et non sécurisés sont tous deux permis.

Un nœud SEND PEUT aussi avoir une option de configuration par laquelle il désactive complètement l'utilisation de SEND, même pour les messages qu'il envoie lui-même. Cette option de configuration DEVRAIT être désactivée par défaut ; c'est-à-dire que SEND est utilisé. Les nœuds NDP purs (non SEND) n'enverront évidemment que des messages non sécurisés. Selon la [RFC2461], de tels nœuds vont ignorer les options inconnues et vont traiter les messages sûrs de la même façon que ceux qui ne le sont pas. Les nœuds sûrs et non sûrs partagent les mêmes ressources réseau, comme les préfixes de sous réseau et les espaces d'adresses.

Les nœuds SEND configurés à utiliser SEND au moins dans leurs propres messages se comportent dans un environnement mixte comme expliqué ci-dessous. SEND adhère aux règles définies pour le protocole NDP de base, avec les exceptions suivantes :

- o Toutes les sollicitations envoyées par un nœud SEND DOIVENT être sécurisées.
- o Les annonces non sollicitées envoyées par un nœud SEND DOIVENT être sécurisées.
- o Un nœud SEND DOIT envoyer une annonce sécurisée en réponse à une sollicitation sécurisée. Les annonces envoyées en réponse à une sollicitation non sûre DOIVENT être quand même sécurisées, mais NE DOIVENT PAS contenir l'option Nom occasionnel.
- o Un nœud SEND qui utilise la méthode d'autorisation de CGA pour protéger les sollicitations de voisin DEVRAIT effectuer la détection d'adresse dupliquée comme suit. Si la détection d'adresse dupliquée indique que l'adresse tentée est déjà utilisée, le nœud génère une nouvelle tentative de CGA. Si après trois tentatives consécutives aucune adresse non unique n'est générée, il enregistre une erreur système et abandonne ses tentatives de générer une adresse pour cette interface.
  Lorsque il effectue la détection d'adresse dupliquée pour la première tentative d'adresse, le nœud accepte les annonces et sollicitations de voisin aussi bien sécurisées que non sécurisées reçues en réponse aux sollicitations de voisin. Lorsque il effectue la détection d'adresse dupliquée pour la seconde ou la troisième tentative, il ignore les annonces et sollicitations de voisin non sûres. (Les implications de ceci pour la sécurité sont discutées au paragraphe 9.2.3 et dans la [RFC3972].)
- o Le nœud PEUT avoir une option de configuration par laquelle il ignore les annonces non sûres, même lorsque il effectue la

détection d'adresse dupliquée pour la première tentative d'adresse. Cette option de configuration DEVRAIT être désactivée par défaut. C'est un mécanisme de récupération pour les cas où des attaques contre la première adresse deviendraient courantes.

- Les entrées d'antémémoire de voisin, de liste de préfixe et de liste de routeur par défaut DOIVENT avoir un fanion sécurisé/non sécurisé qui indique si le message qui a causé la création ou la dernière mise à jour de l'entrée était sécurisée ou non. Les messages non sûrs reçus NE DOIVENT PAS causer de changements aux entrées sécurisées existantes dans l'antémémoire de voisin, la liste des préfixes ou la liste des routeurs par défaut. Les messages sûrs reçus DOIVENT causer une mise à jour des entrées correspondantes, qui DOIVENT être étiquetées comme étant sécurisées.
- Les sollicitations de voisin pour les besoins de la détection d'inaccessibilité de voisin (NUD) DOIVENT être envoyées à l'adresse de diffusion groupée Nœuds-sollicités de ce voisin si l'entrée n'est pas sécurisée avec SEND. Des confirmations de couche supérieure sur les entrées d'antémémoire de voisin non sûres NE DEVRAIENT PAS mettre à jour l'état de l'antémémoire de voisin de PÉRIMÉ à ACCESSIBLE sur un nœud SEND si l'entrée d'antémémoire de voisin n'a jamais été antérieurement ACCESSIBLE. Cela assure que si une usurpation d'entrée d'un hôte SEND valide est créée par un attaquant non SEND sans avoir été sollicité, la NUD sera faite avec l'entrée pour transmission des données dans les cinq secondes d'utilisation. Par suite, en mode mixte, les attaquants ne peuvent prendre le contrôle d'une entrée d'antémémoire de voisin d'un nœud SEND pendant plus longtemps que si (a) le nœud SEND n'était pas en communication avec le nœud victime, de sorte qu'il n'y a pas d'entrée sécurisée pour lui, et (b) le nœud SEND n'est pas actuellement sur la liaison (ou est dans l'incapacité de répondre).
- L'algorithme d'envoi conceptuel est modifié afin qu'un routeur non sûr ne soit choisi que si il n'y a pas de routeur SEND accessible pour le préfixe. C'est-à-dire que l'algorithme pour choisir un routeur par défaut favorise les routeurs SEND accessibles par rapport aux non SEND.
- Un nœud PEUT adopter un routeur qui envoie des messages non sûrs, ou un routeur pour lequel des messages sécurisés ont été reçus mais pour lequel les vérifications de sécurité complètes n'ont pas encore été achevées, alors que les vérification de sécurité sont en cours. Les vérifications de sécurité incluent dans ce cas les vérifications de sollicitation de chemin de certification, de certificat, de CRL, et de signature RA. Un nœud PEUT aussi adopter un routeur qui envoie des messages non sûrs si un routeur connu pour être sécurisé devient inaccessible, mais comme l'inaccessibilité peut être le résultat d'une attaque, il DEVRAIT tenter de trouver un routeur connu pour être sûr, aussitôt que possible. Noter que bien que ceci puisse accélérer le rattachement à un nouveau réseau, accepter un routeur qui envoie des messages non sûrs ou pour lequel les vérifications de sécurité ne sont pas achevées livre le nœud à de possibles attaques. Les nœuds qui choisissent d'accepter de tels routeurs le font à leurs risques et périls. Le nœud DEVRAIT, en tout cas, préférer un routeur connu pour être sûr dès qu'il en est un de disponible avec des vérifications de sécurité complètes.

9. Considérations sur la sécurité

9.1 Menaces sur la liaison locale non couvertes par SEND

SEND n'assure pas la confidentialité des communications NDP.

SEND ne compense pas une couche de liaison non sûre. Par exemple, il n'est pas assuré que les paquets de charge utile viennent réellement de l'homologue pour lequel on a fait NDP.

Il ne peut pas y avoir de lien cryptographique dans SEND entre l'adresse de trame de la couche de liaison et l'adresse IPv6. Une couche de liaison non sûre peut permettre à des nœuds d'usurper l'adresse de couche de liaison d'autres nœuds. Un attaquant pourrait perturber le service IP en envoyant une annonce de voisin sur une couche de liaison non sécurisée, avec l'adresse de source de couche de liaison sur la trame réglée à l'adresse de source d'une victime, une adresse CGA valide et une signature valide correspondant à lui-même, et une extension d'adresse de couche liaison cible correspondant à la victime. L'attaquant pourrait alors bombarder la victime de flux de trafic dans une attaque de DoS. Ceci ne peut pas être empêché juste en sécurisant la couche de liaison.

Même sur une couche de liaison sécurisée, SEND n'exige pas que les adresses sur la couche de liaison et les annonces de voisin correspondent. Cependant, il est RECOMMANDÉ d'effectuer ces vérifications si la technologie de la couche de liaison le permet.

Avant de participer à la découverte de voisin et à la détection d'adresse dupliquée, les nœuds doivent s'abonner au groupe de diffusion groupée Tous-les-nœuds à portée de la liaison et au groupe de diffusion groupée Nœud-sollicité pour les adresses qu'ils revendiquent comme leurs selon la [RFC2461]. S'abonner à un groupe de diffusion groupée exige que le nœud utilise MLD [RFC2710]. MLD ne contient pas de disposition pour la sécurité. Un attaquant pourrait envoyer un message MLD Done pour désabonner une victime de l'adresse de diffusion groupée Nœud-Sollicité. Cependant, la victime devrait être capable de détecter cette attaque parce que le routeur envoie une interrogation spécifique d'adresse de diffusion groupée pour déterminer si les écoutants sont toujours sur l'adresse, et à ce moment la victime peut répondre pour éviter d'être éliminé du groupe. Cette technique va fonctionner si le routeur sur la liaison n'a pas été compromis. D'autres attaques utilisant MLD sont possibles, mais leur but principal conduit à du trafic supplémentaire (mais pas nécessairement envahissant).

9.2 Comment SEND compte les menaces sur NDP

Le protocole SEND est conçu pour contrer les menaces qui pèsent sur NDP, comme précisé dans la [RFC3756]. Les paragraphes qui suivent contiennent un retour sur les menaces contre le protocole SEND, pour illustrer quel aspect du protocole contre chaque menace.

9.2.1 Usurpation d'identité de sollicitation/annonce de voisin

Cette menace est définie au paragraphe 4.1.1 de la [RFC3756]. La menace est qu'un message usurpé puisse causer une fausse entrée dans l'antémémoire de voisins d'un nœud. Il y a deux cas :

1. Les entrées faites comme effet collatéral d'une sollicitation de voisin ou d'une sollicitation de routeur. Un routeur qui reçoit une sollicitation de routeur avec une extension d'adresse cible de couche liaison et une adresse de source IPv6 inégales à l'adresse non spécifiée insère une entrée pour l'adresse IPv6 dans son antémémoire de voisins. Aussi, un nœud qui effectue la détection d'adresse dupliquée (DAD) et qui reçoit une sollicitation de voisin pour la même adresse considère la situation comme une collision et cesse de solliciter pour cette adresse. Dans l'un et l'autre cas, SEND contre ces menaces en exigeant que les options Signature RSA et CGA soient présentes dans ces sollicitations. Les nœuds SEND peuvent envoyer des messages Sollicitation de routeur avec une adresse de source CGA et une option CGA, que le routeur peut vérifier, afin que le lien de l'antémémoire de voisin soit correct. Si un nœud SEND doit envoyer une sollicitation de routeur avec l'adresse non spécifiée, le routeur ne va pas mettre à jour son antémémoire de voisins, conformément au NDP de base.
2. Les entrées faites par suite d'un message annonce de voisin. SEND contre cette menace en exigeant que les options Signature RSA et CGA soient présentes dans ces annonces.

Voir aussi au paragraphe 9.2.5 une discussion sur la protection contre les répétitions et les horodatages.

9.2.2 Échec de la détection d'inaccessibilité du voisin

Cette attaque est décrite au paragraphe 4.1.2 de la [RFC3756]. SEND la contre en exigeant qu'un nœud qui répond aux sollicitations de voisin envoyées comme sondes de NUD inclue une option Signature RSA et une preuve d'autorisation d'utiliser l'identifiant d'interface dans l'adresse sondée. Si ces pré requis ne sont pas satisfaits, le nœud qui effectue la NUD élimine les réponses.

9.2.3 Attaques de DoS par la détection d'adresse dupliquée

Cette attaque est décrite au paragraphe 4.1.3 de la [RFC3756]. SEND contre cette attaque en exigeant que les annonces de voisin envoyées en réponse à la DAD incluent une option Signature RSA et la preuve de l'autorisation d'utiliser l'identifiant d'interface dans l'adresse à vérifier. Si ces pré requis ne sont pas satisfaits, le nœud effectuant la DAD élimine les réponses.

Lorsque un nœud SEND effectue une DAD, il peut écouter les collisions d'adresse des nœuds non SEND pour la première adresse qu'il génère, mais pas pour les tentatives suivantes. Cela protège le nœud SEND des attaques de DoS avec DAD par des nœuds non SEND ou par des attaquants qui font semblant d'être des nœuds non SEND, au prix d'une collision d'adresse potentielle entre un nœud SEND et un nœud non SEND. La probabilité et les effets d'une telle collision d'adresse sont discutés dans la [RFC3972].

9.2.4 Attaques par sollicitations et annonces de routeur

Ces attaques sont décrites aux paragraphes 4.2.1, 4.2.4, 4.2.5, 4.2.6, et 4.2.7 de la [RFC3756]. SEND les contre en exigeant que les annonces de routeur contiennent une option Signature RSA, et que la signature soit calculée en utilisant la clé publique d'un nœud qui peut prouver son autorisation d'acheminer les préfixes de sous réseau contenus dans toute option Informations de préfixe. Le routeur prouve son autorisation en montrant un certificat qui contient le préfixe spécifique ou une indication que le routeur est autorisé à acheminer tout préfixe. Une annonce de routeur sans ces protections est éliminée.

SEND ne protège pas contre les attaques en force brute sur le routeur, comme les attaques de DoS, ou contre la compromission du routeur, comme décrit aux paragraphes 4.4.2 et 4.4.3 de la [RFC3756].

9.2.5 Attaques en répétition

Cette attaque est décrite au paragraphe 4.3.1 de la [RFC3756]. SEND protège contre les attaques dans les transactions Sollicitation de routeur/Annonce de routeur et Sollicitation de voisin/Annonce de voisin en incluant une option Nom occasionnel dans la sollicitation et en exigeant que l'annonce comporte une option correspondante. Avec les signatures, cela forme un protocole de défi-réponse.

SEND protège contre les attaques à partir des messages non sollicités comme les annonces de voisin, les annonces de routeur, et les Redirect en incluant une option Horodatage. Les questions de sécurité suivantes ne sont pertinentes que pour les messages non sollicités :

- Un fenêtre de vulnérabilité pour les attaques en répétition existe jusqu'à l'arrivée à expiration de l'horodatage. Cependant, une telle vulnérabilité n'est utile pour des attaquants que si les paramètres annoncés changent durant la fenêtre. Bien que certains paramètres (comme la durée de vie restante d'un préfixe) changent souvent, les changements radicaux ne surviennent que dans le contexte d'un cas particulier, comme le passage sur une nouvelle adresse de couche liaison du fait de la rupture d'un adaptateur d'interface. Les nœuds SEND sont aussi protégés contre les attaques en répétition tant qu'ils mettent en mémoire l'état créé par le message qui contient l'horodatage. L'état mis en antémémoire permet au nœud de se protéger contre les messages répétés. Cependant, une fois que le nœud a purgé l'état pour n'importe quelle raison, un attaquant peut recréer l'état en répétant un vieux message pendant que l'horodatage est encore valide. Comme la plupart des nœuds SEND vont probablement utiliser des horodatages à gros grain, comme expliqué au paragraphe 5.3.1, ceci peut affecter certains nœuds.
- Les attaques contre les protocoles de synchronisation horaire comme [NTP] peuvent être cause que les nœuds SEND ont une valeur d'horodatage incorrecte. Ceci peut être utilisé pour lancer des attaques en répétition, même en dehors de la fenêtre normale de vulnérabilité. Pour se protéger contre ces attaques, il est recommandé que les nœuds SEND gardent des horloges à alimentation indépendante ou appliquent des mesures de sécurité convenables pour les protocoles de synchronisation de l'heure.

9.2.6 Attaques de DoS par la découverte de voisin

Cette attaque est décrite au paragraphe 4.3.2 de la [RFC3756]. L'attaquant bombarde le routeur avec des paquets pour des adresses fictives sur la liaison, causant l'occupation du routeur à effectuer les sollicitations de voisin pour des adresses qui n'existent pas. SEND ne traite pas cette menace parce qu'elle peut être traitée par des techniques comme la limitation du taux des sollicitations de voisin, restreignant la quantité d'état Réservé pour les sollicitations non résolues, et une gestion adroite de l'antémémoire. Ce sont toutes des techniques impliquées dans la mise en œuvre de la découverte de voisin sur le routeur.

9.3 Attaques contre SEND lui-même

Les CGA ont une valeur de hachage de 59 bits. La sécurité du mécanisme de CGA a été exposée dans la [RFC3972].

Certaines attaques de déni de service se font contre NDP et SEND lui-même. Par exemple, un attaquant peut essayer de produire un nombre très élevé de paquets qu'un hôte ou routeur victime va devoir vérifier en utilisant des méthodes asymétriques. Bien que des sauvegardes soient nécessaires pour empêcher une utilisation excessive de ressources, ceci peut quand même rendre SEND non opérationnel. Lorsque la protection des CGA est utilisée, SEND traite les attaques de DoS en utilisant le processus de vérification décrit au paragraphe 5.2.2. Dans ce processus, une simple vérification du hachage de la propriété de CGA de l'adresse est effectuée avant la plus coûteuse vérification de signature. Cependant, même si la vérification de CGA réussit, aucune réclamation sur la validité du message ne peut être faite tant que la signature n'a pas été vérifiée.

Lorsque des ancres de confiance et des certificats sont utilisés pour la validation d'adresse dans SEND, les défenses ne sont pas aussi efficaces. Les mises en œuvre DEVRAIT garder trace des ressources dédiées au traitement des paquets reçus avec l'option Signature RSA et commencer à éliminer sélectivement des paquets si trop de ressources sont dépensées. Les mises en œuvre PEUVENT aussi commencer à éliminer les paquets qui ne sont pas protégés par une CGA. Le processus de découverte de délégation d'autorisation peut aussi être vulnérable aux attaques de déni de service. Une attaque peut cibler un routeur en demandant qu'un grand nombre de chemins de certification soient découverts pour différentes ancres de confiance. Les routeurs DEVRAIENT se défendre contre de telles attaques en mettant en antémémoire les informations découvertes (incluant les réponses négatives) et en limitant le nombre de processus de découverte différents dans lesquels ils s'engagent.

Les attaquants peuvent aussi cibler des hôtes en envoyant un grand nombre de chemins de certification inutiles, forçant les hôtes à dépenser inutilement sur eux des ressource de mémoire et de vérification. Les hôtes peuvent se défendre contre cette attaque en limitant la quantité de ressources dédiées aux chemins de certification et leur vérification. Les hôtes DEVRAIENT aussi donner des priorités aux annonces envoyées en réponse aux sollicitations qu'ils ont envoyées sur des annonces non sollicitées.

10 Valeurs du protocole

10.1 Constantes

Constantes des hôtes :
CPS_RETRY : 1 seconde

CPS_RETRY_FRAGMENTS : 2 secondes
CPS_RETRY_MAX : 15 secondes

Constante de routeur :
MAX_CPA_RATE : 10 fois par seconde

10.2 Variables

HORODATAGE_DELTA : 300 secondes (5 minutes)
HORODATAGE_FUZZ : 1 seconde
HORODATAGE_DRIFT : 1 % (0,01)

11. Considérations relatives à l'IANA

Le présent document définit deux nouveaux types de message ICMP, utilisés dans la découverte de délégation d'autorisation. Ces messages doivent recevoir les numéros de type ICMPv6 de la gamme de message d'information :
- Le message Sollicitation de chemin de certification (148), décrit au paragraphe 6.4.1.
- Le message Annonce de chemin de certification (149), décrit au paragraphe 6.4.2.

Le présent document définit six nouvelles options du protocole de découverte de voisin [RFC2461] qui doivent recevoir les valeurs de Type d'option dans l'espace de numéros d'option pour les messages du protocole de découverte de voisin :
- L'option CGA (11), décrite au paragraphe 5.1.
- L'option Signature RSA (12), décrite au paragraphe 5.2.
- L'option Horodatage (13), décrite au paragraphe 5.3.1.
- L'option Nom occasionnel (14), décrite au paragraphe 5.3.2.
- L'option Ancre de confiance (15), décrite au paragraphe 6.4.3.
- L'option Certificat (16), décrite au paragraphe 6.4.4.

Le présent document définit une nouvelle valeur de 128 bits dans l'espace de noms de type de message CGA [RFC3972], 0x086F CA5E 10B2 00C9 9C8C E001 6427 7C08.

Le présent document définit un nouvel espace de noms pour le champ Type de nom dans l'option Ancre de confiance. De futures valeurs de ce champ pourront être allouées par action de normalisation [RFC2434]. Les valeurs actuelles pour ce champ sont :
1 : Nom X.501 codé en DER
2 : FQDN

Un autre nouvel espace de noms est alloué pour le champ Type de certificat dans l'option Certificat. De futures valeurs de ce champ pourront être allouées par action de normalisation [RFC2434]. Les valeurs actuelles pour ce champ sont :
1 : Certificat X.509v3

12. Références

12.1 Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987.

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

[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)

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

[RFC2462] S. Thomson, T. Narten, "Autoconfiguration d'adresse IPv6 sans état", décembre 1998. (*Obsolète, voir* RFC4862) *(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.)*

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3281] S. Farrell et R. Housley, "Profil de certificat d'attribut Internet pour l'autorisation", avril 2002. *(Remplacée par* RFC5755)

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

[RFC3779] C. Lynn, S. Kent, K. Seo, "ExtensionsX.509 pour les adresses IP et les identifiants d'AS", juin 2004. *(P.S.)*

[RFC3972] T. Aura, "Adresses générées cryptographiquement (CGA)", mars 2005. (*MàJ par* RFC4581, RFC4982) *(P.S.)*

[X.690] Union Internationale des Télécommunications, "Information Technology- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", Recommandation UIT-T X.690, juillet 2002.

[PKCS1] RSA Laboratories, "RSA Encryption Standard, Version 2.1", PKCS1, November 2002.

[FIPS180-1] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1, avril 1995, <http://www.itl.nist.gov/fipspubs/fip180-1.htm>.

12.2 Références pour information

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2710] S. Deering, W. Fenner et B. Haberman, "Découverte d'écouteur de diffusion groupée (MLD) pour IPv6", octobre 1999.

[RFC3041] T. Narten, R. Draves, "Extensions de confidentialité pour l'auto-configuration d'adresse sans état dans IPv6", janvier 2001. (*Obsolète, voir* RFC4941) *(P.S.)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227)

[RFC3756] P. Nikander, éd., "Modèles de confiance et menaces pour la découverte de voisin IPv6 (ND)", mai 2004. *(Information)*

[RFC5014] E. Nordmark et autres, "API de prises IPv6 pour la sélection d'adresse de source", septembre 2007.*(Information)*

[ICMP-IKE] Arkko, J., "Effects of ICMPv6 on IKE and IPsec Policies", Travail en cours, mars 2003.

[Manual SA] Arkko, J., "Manual SA Configuration for IPv6 Link Local Messages", Travail en cours, juin 2002.

[NTP] Bishop, M., "A Security Analysis of the NTP Protocol", SixthAnnual Computer Security Conference Proceedings, décembre 1990.

Appendice A Contributeurs et remerciements

Tuomas Aura a contribué à la spécification du mécanisme de transition à la Section 8. Jonathan Trostle a contribué à l'exemple de chemin de certification au paragraphe 6.3.1. Bill Sommerfeld a été impliqué dans beaucoup du travail de conception précoce.

Les auteurs tiennent aussi à remercier Tuomas Aura, Bill Sommerfeld, Erik Nordmark, Gabriel Montenegro, Pasi Eronen, Greg Daley, Jon Wood, Julien Laganier, Francis Dupont, Pekka Savola, Wenxiao He, Valtteri Niemi, Mike Roe, Russ Housley, Thomas Narten, et Steven Bellovin pour les discussions intéressantes sur ces problèmes et pour leurs retours sur le protocole SEND.

Appendice B Gestion d'antémémoire

Dans cette section, on esquisse un algorithme de gestion d'antémémoire qui permet à un nœud de rester partiellement fonctionnel même sous une attaque de DoS consistant à remplir l'antémémoire. Cet appendice est pour information, et les mises en œuvre réelles DEVRAIENT utiliser des algorithmes différents afin d'éviter les dangers d'un code mono culturel.

Il y a au moins deux scénarios distincts d'attaque en rapport avec l'antémémoire :

1. Il y a un certain nombre de nœuds sur une liaison, et quelqu'un lance une attaque de remplissage d'antémémoire. Le but est ici de s'assurer que les nœuds peuvent continuer à communiquer même si l'attaque se déroule.

2. Il y a déjà une attaque de remplissage d'antémémoire en cours, et un nouveau nœud arrive sur la liaison. Le but est ici de rendre possible au nouveau nœud de se rattacher au réseau, en dépit de l'attaque.

Comme l'intention est de limiter les dommages aux entrées existantes valides dans l'antémémoire, il est clairement meilleur d'être très sélectif dans l'élimination des entrées. Réduire la valeur du Delta d'horodatage est très discriminatoire pour les nœuds qui ont une grande différence d'horloge, car un attaquant peut réduire sa différence d'horloge à sa discrétion. Éliminer les entrées anciennes juste parce que leur différence d'horloge est grande semble donc une mauvaise approche.

Il est raisonnable d'avoir des espaces d'antémémoire séparés pour les entrées nouvelles et anciennes, et en cas d'attaque, les nouvelles entrées en antémémoire seront plus directement éliminées. On pourrait retracer le trafic et ne permettre qu'aux entrées nouvelles raisonnables qui reçoivent du trafic authentique d'être converties en anciennes entrées d'antémémoire. Bien qu'un tel schéma puisse rendre les attaques plus dures, cela ne va pas les empêcher complètement. Par exemple, un attaquant pourrait envoyer un petit trafic (c'est-à-dire, un ping ou un syn TCP) après chaque NS pour tromper la victime en lui faisant promouvoir son entrée d'antémémoire dans l'antémémoire des anciennes. Pour contrer cela, le nœud peut être plus intelligent en gardant ses entrées d'antémémoire que ce ne serait en ayant juste une frontière noir/blanc ancien/nouveau.

La distinction du paramètre Sec des paramètres de CGA lorsque on force la sortie des entrées d'antémémoire – en gardant de préférence les entrées avec de plus grands paramètres Sec – paraît aussi être une approche possible, car les CGA avec de plus forts paramètres Sec sont plus difficiles à usurper.

Appendice C Taille de message portant des certificats

Dans un exemple de scénario utilisant SEND, un essai de découverte de délégation d'autorisation a été fait avec un chemin de certification de 4. Trois certificats sont envoyés en utilisant des messages d'annonce de chemin de certification, car le certificat de l'ancre de confiance est déjà connu des deux parties. Avec une longueur de clé de 1024 bits, les longueurs de certificat dans l'essai vont de 864 à 888 octets ; la variation est due à la différence des noms des producteurs de certificats et des extensions de préfixe d'adresse. Les différents certificats avaient entre 1 et 4 extensions de préfixe d'adresse .

Les trois messages d'annonce de chemin de certification vont de 1 050 à 1 066 octets sur une couche de liaison Ethernet. Le certificat lui-même tient la plus grande partie du paquet. Le reste est l'option Ancre de confiance, l'en-tête ICMP, l'en-tête IPv6, et l'en-tête de couche liaison.

Adresses des auteurs

Jari Arkko
Ericsson
Jorvas 02420
Finland
mél : jari.arkko@ericsson.com

James Kempf
DoCoMo Communications Labs USA
181 Metro Drive
San Jose, CA 94043
USA
mél : kempf@docomolabs-usa.com

Brian Zill
Microsoft Research
One Microsoft Way
Redmond, WA 98052
USA
mél : bzill@microsoft.com

Pekka Nikander
Ericsson
Jorvas 02420
Finland
mél : Pekka.Nikander@nomadiclab.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait 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 Identifiant 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 actuellement fourni par l'Internet Society.